PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ANGELA ROCIO SILVA ALVARADO

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

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ANGELA ROCIO SILVA ALVARADO

Diplomado de opción de grado presentado para optar el título de INGENIERO SISTEMAS

DIRECTOR:
JUAN CARLOS VESGA FERREIRA

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

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

TUNJA-BOYACÀ, 22 de Julio de 2020

AGRADECIMIENTOS

Primero que todo quiero agradecerle A Dios, por darme la fuerza, sabiduría para continuar con la carrera que tanto había soñado,

A mi mamá que me apoyo en momentos, que ya no tenía para el otro semestre me animo, a que siguiera adelante y que en ningun momento desistiera por mal que estuviera la situación.

Quiero agradecer a un Amigo que fue la principal persona, que vio en mí, mis capacidades y las ganas de sacar adelante la carrera de ingeniería de sistemas. Y si no hubiera sido por él nunca lo hubiera pensado.

A todas mis amigas que siempre ha estado pendientes de que cuando terminaba la carrera Gracias Amigas.

y muy especialmente a todas las personas que creen en mí.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Interfaces: se utiliza para en informática para nombrar las conexión funcional entre dos sistemas, programas, dispositivos o componentes de cualquier tipo, que proporciona una comunicación de distintos niveles, permitiendo el intercambio de informacion.

Enrrutamiento: se conoce como el nombre de enrutamiento (routing) el proceso que permite que los paquetes IP enviados por el host origen lleguen al host destino de forma adecuada. En su viaje entre ambos host los paquetes han de atravesar un numero indefinido de host o dispositivos de red intermedios.

Servidor:es una aplicación en ejecución capaz de atender las peticiones de un cliente y devolver una respuesta en con cordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como “servidor”

Host: se usa en informática para referirse a las computadoras u otros dispositivos (tables, móviles,portatiles) conectados a una red que proveen y utilizan servicios de ella. También es descrito como el lugar donde reside un sitio web, un anfitrión de internet tiene por lo general una direccion de internet única llamada “direccion IP ” y un nombre de dominio único o nombre de anfitrión(host name)

Mascara sub red: es la direccion que te asigna tu IPS empresa que da el acceso a internet como telefonía, y sirve para identificarte dentro de internet cuando te conectas, pero la IP por si sola tampoco sirve para identificarte en la red. A esta direccion la vas a tener que acompañar siempre de la máscara9 de subred. A efectos prácticos se trata de otra IP, pero cuya numeración casi siempre va a estar compuesta por ceros y 255.

Router: es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red, se encarga de establecer la ruta que designara a cada paquete de datos dentro de una red informática.

Switch: es un dispositivo de interconexión utilizado para conectar equipos de red formando lo que se conoce como una red de área local (LAN) cuyas especificaciones técnicas siguen el estándar conocido como ethernet. Es importante tener claro que un switch NO proporciona por si solo conectividad con otras redes, y obviamente tan poco conectividad con internet.

RESUMEN

En el tiempo del proceso de aprendizaje y del desarrollo de la simulación del escenario 1 para el programa de ingeniería de sistemas de las Unad, se desarrolló los modulos de cisco correspondiente a CCNA(Generalidades de Networking, mecanimos de comunicación y acceso a la red, comunicaciones sobre ethernet, Direccionamiento IP subnetting, comunicación en capas superior, enrutamiento estatico, enrrutamiento dinamico y comutacion, Vlans, direccionamiento ip dinamico y ACL, nat pat y gestion de equipos de networking). Llegando de esta manera al diplomado buscando adquirir y dar a conocer el proceso de configuración del dispositivos de la simulación de los escenarios, permitiendo la conectividad de las PC con el fin de realizar el ping de las dos PC. Analizando y configurando los requerimientos que son requeridos por la simulaciónes de los escenarios.

Palabras Clave: CISCO, CCNA, dinamico, Enrutamiento, Redes, Networking.

ABSTRACT

During the learning process and the development of the simulation of scenario 1 for the systems engineering program of the Unad, the cisco modules corresponding to CCNA (Generalities of Networking, communication mechanisms and network access, communications over ethernet, IP subnetting addressing, communication in higher layers, static routing, dynamic routing and commutation, Vlans, dynamic IP addressing and ACL, nat pat and management of networking equipment). Arriving in this way to the graduate seeking to acquire and publicize the process of configuring the devices of the simulation of the scenarios, allowing the connectivity of the PCs in order to ping the two PCs. Analyzing and configuring the requirements that are required by the simulation of the scenarios.

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

INTRODUCCIÓN

La simulación de la redes ha venido evolucionando, en cuanto a sus versiones de cisco Packet trecer, de acuerdo a esto nos permitè esta herramienta crear tipología de red, con multiplex representaciones visuales, y principalmente como herramienta didáctico que nos permite crear topologías, configurar dispositivos, insertar paquetes y simular una red. En focado en apoyar los protocolos de redes que se nos enseña en el curriculum de la certificación cisco.

Este trabajo se llevó a cabo con el fin de realizar un proceso paso a paso del scrip de la configuración, Para saber y poder implementar la simulación del escenario 1, aplicando la configuración iniciales, y el enrrutamiento para los Router, donde se le asigna nombre y protocolo de comunicación. Y por ende en esta primer simulación del encenario 1. Se realizo la configuración del Router y Switch 1 y 2 en este proceso se tuvo que tener en cuenta dos versiones tanto IPV4 y IPV6 para interconectar la PC -A y la Pc B, para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 Y se pueda realizar el ping.

Es muy importante garantizar la seguridad del router, a través de la creación de cuentas de usuarios y la asignación de contraseñas secretas para habilitar router, line de consola, línea terminal virtual.

En el encenario 2 se realizó la configuración de OPSF, primero se tuvo que inicializar los routers y los switches, luego se procede a configurar el R1, R2 y R3 paso a paso. Y Se configuro el S1 y S3 se realizó la conectividad en el mismo escenario que esta en el packet trecer.

Se configuro la seguridad del switch, las VLAN y el routing entre VLAN tanto del S1 y S3, y también el protocolo de routing dinamico OSPF, se implementó DHCP y NAT para ipv4 y por ultimo introducir el comando de CLI adecuado que se necesita para mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se reestableció.

ESCENARIO 1

Figura 1. Escenario 1

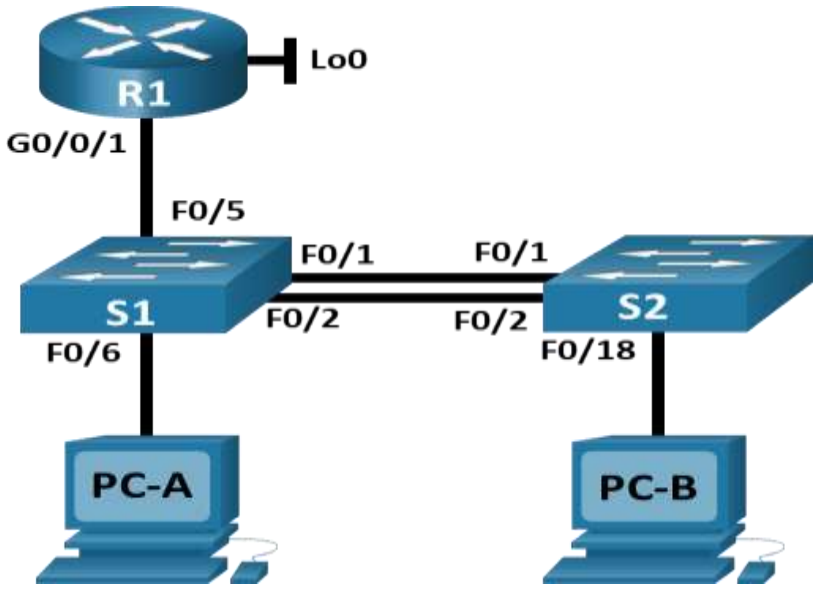
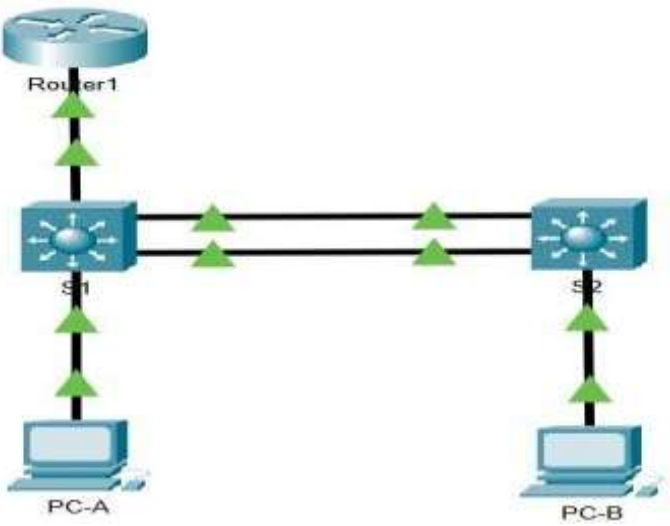


Figura 2. Simulación de escenario 1



1.1. Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.
Se procede a configurar cada uno de los enrutadores. 1, 2, 3, 4, 5
Se asignan nombre y protocolos de comunicación mediante EIGRP que fueron asignados.

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

Tabla 1. Nombre de la Vlan

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

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
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
	2001:db8:acad:a: :50 /64	fe80::2D0:BAFF:FEC8:8D78
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80 ::2D0:BAFF:FEC8:8D78

Tabla 2. Puerto de Enlace Predeterminado

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

Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

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

- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los disposit0ivos.6789

- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.
- Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Paso 2: Configurar R1

Tarea	Especificación
Desactivar la búsqueda DNS	R1 (config)# no ip domain-lookup R1#
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	ok
Configurar VTY solo aceptando SSH	ok
Cifrar las contraseñas de texto no cifrado	ok
Configure un MOTD Banner	ok
Habilitar el routing IPv6	ok
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. Falta este punto
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1
Generar una clave de cifrado RSA	Módulo de 1024 bits

Tabla 3. Configuracion R1

Las tareas de configuración para R1 incluyen las siguientes:

1.Desabilite la búsqueda DNS Si se desactiva la búsqueda DNS un router no podría resolver los nombres, lo cual provocaría posibles problemas cuando el router necesite una direccion IP para enviar un paquete (se desactiva cuando se hacen pruebas para que el Router no intente buscas una entrada DNS para un nombre que en realidad es un error de escritura).

R1 (config)# no ip domain-lookup Desactivar la búsqueda DNS (en este caso R1)

R1#

2.Asigne el nombre de dispositivo al Router (R1) para la asignación del R1 se utiliza el hostname con el fin de que establezca el nombre de Router a R1.

Router > enable Entrar al modo EXEC Privilegiado

Router# configure terminal Entrar al modo configuración Global

Enter configuration commands, one per line. End with CNTL/Z.

Router (config)# hostname R1 Configurar nombre del Router (en este caso R1)

R1 (config)#

3. Asigne el nombre del dominio en el router para el usuario ingrese a la direccion que es ccna-lab.com.

R1# configure terminal Entrar a Configure Termial

R1(config)# hostname <nombre-router> Se configura con hostname nombre-router

<nombre-router>(config)#ip domain-name ccna-lab.com Se coloca nombre -dominio

<nombre-router>(config)#exit Terminamos

4. Contraseña cifrada para el modo EXEC privilegiado para que el usuario ingrese con la contraseña que es ciscoenpass.

Router > enable

R1# configure terminal

R1(config)# enable password ciscoenpass

5. Asigne **ciscoenpass** como la contraseña de **consola 0** y habilite el inicio de la sesión. Y pueda ingresar a la consola con la contraseña que aparece y el login es para deshabilitar la autenticación. Pero esto no quiere decir que aumente la seguridad.

R1 (config)# line console 0

R1 (config-line)# password Ciscoenpass

R1(config-line)# login local

R1 (config-line)# exit

R1 (config)#

6. establecí la longitud mina para la contraseña realizando el siguiente comando. Quiere decir que solo puede ingresar con esa mina longitud de caracteres puede ser 8 o 10

R1(config)#security password min-length ? Configurar seguridad de la contraseña

<0-16> Minimum length of all user/enable passwords

R1(config)#enable password **ciscoenpass** Entramos en modo privilegiado para password como ciscoenpass

7. cree el usuario administrative en la base de datos local con el siguiente comando para que ingrese con el usuario y la contraseña.

Nombre de usuario: **admin**

Password: **admin1pass**

R1(config)#username admin password admin1pass

8. Asigne **cisco** como la contraseña de **VTY(Línea de tiempo virtual)** 0-4 y habilite el inicio de sesión estan habilitadas de 0 15 y son utilizadas para establecer la sesiones telnet.

R1(config)# line vty 0 4 Configurar line vty 0 4

R1(Config-line)# password ciscoenpass Ingresar password ciscoenpass

R1(config-line)# login local Hace que pida contraseña al acceder línea de tiempo virtual

R1(config-line)# exit

R1(config)#

9. luego encripte las contraseñas de texto no cifrado. Esta contraseña restringe el acceso a la configuracion.

R1#disable

R1>enable

Password: ciscoenpass

Password: ciscoenpass

Password: ciscoenpass

% Bad secrets

10. establecí configuración del MOTD banner de una sola línea. Este nos permite configurar el mensaje de entrada para todas las terminales conectadas.

R1(config)#banner motd Authorized Access only

R1#(config)# exit

R1#exit

11. Para habilitar enrrutamiento IPV6 en el R1 por medio del comando IPV6 unicast-routing. Se tiene que teclear el comando de interfaces se debe tener en cuenta que los puertos o interfaces de un router estan desactivado por defecto pero se active con el comando no shutdown.

R1#Configure terminal

R1(config)# ipv6 unicast-routing.

R1(config#)exit

12. Realice la configuracion interfa R1 G0/0/1.2 10.19.8.1 /26 y subinterfaces.

R1(Config-if)# interface G0/0/1.2

R1 (Config-if)#ip address 10.19.8.1 255.255.255.0 2001:db8:acad:a: :1 /64

R1 (confing-if)#interface serial 0/0/1

R1 (confing-if)#no shutdown

R1(confing-if)# exit

12.1 Realice la configuracion R1 G0/0/1.3 10.19.8.65 /27 y subinterfaces

R1(Config-if)# interface G0/0/1.3

R1 (Config-if)#ip address 10.19.8.65 255.255.255.0

R1 (confing-if)#no shutdown

R1(confing-if)# exit

12.2 Realice la configuracion R1 G0/0/1.4 10.19.8.97 /29 y subinterfaces

R1(Config-if)# interface G0/0/1.4

R1 (Config-if)#ip address 10.19.8.97 255.255.255.0

R1 (confing-if)#no shutdown

R1(confing-if)# exit

13. Configurar el Loopback0 interface esta direccion nos permite dirigir el tráfico hacia ellos mismos esta crea un método de acceso directo para la aplicación y servicios TCP/IP que se ejecuta en el mismo dispositivo para que se comuniquen entre si

R1> enable

R1# Config t

R1(config)# int loopback0

R1(config-if)# ip address 209.165.201.1 255.255.255.252

R1(config)# exit

14. Generar una clave de cifrado RSA se podrá de cifrar mediante la clave sin cifrar, que sea con la clave pública.

Route> enable
R1# configure terminal
R1#(config)#ip domain-name ccna-lab.com
R1(config)# crypto key generate rsa general-Keys modulus 1024
R1#wr

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tarea	**Especificación**
Desactivar la búsqueda DNS.	ok

Tarea	Especificación
Nombre del switch	S1 o S2, según proceda
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	ok
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	ok
Cifrar las contraseñas de texto no cifrado	ok
Configurar un MOTD Banner	ok
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4

Tabla 4. Configure S1 y S2.

CONFIGURACION DEL S1

1. Desabilitar la búsqueda DNS para evitar que el Switch intente traducir los comandos incorrectamente introducidos como si fuera nombre del host.

switch (config)# no ip domain-lookup

switch#

2. Para configurar el nombre del switch

Switch > enable	Entrar al modo EXEC Privilegiado
Switch# configure terminal	Entrar al modo configuración Global
Switch (config)# hostname S1	Configurar nombre del Switch (en este caso S1)

S1 (config)#

Switch > enable	Entrar al modo EXEC Privilegiado
Switch# configure terminal	Entrar al modo configuración Global
Switch (config)# hostname S1	Configurar nombre del Switch (en este caso S2)
S2 (config)#	

3. asigne el nombre del dominio en el router.

S1# configure terminal	Entrar a Configure Termial
S1(config)# hostname <nombre-Switch>	Se configura con hostname nombre-switch
<nombre-switch>(config)#ip domain-name ccna-lab.com	
<nombre-switch>(config)#end	exit

S2# configure terminal	Entrar a Configure Termial
S2(config)# hostname <nombre-Switch>	Se configura con hostname nombre-switch
<nombre-switch>(config)#ip domain-name ccna-lab.com	
<nombre-switch>(config)#end	exit

4. Contraseña cifrada para el modo EXEC privilegiado.

Switch> enable
S1# configure terminal
S1(config)# enable password ciscoenpass

Switch> enable
S2# configure terminal
S2(config)# enable password ciscoenpass

5. Se Configura la contraseña de acceso a la consola.

S1(config)# line console 0
S1(config-line)#password **ciscoenpass**
S1(config-line)# login

S2(config)# exit

S2(config)# line console 0
S2(config-line)#password **ciscoenpass**
S2(config-line)# login
S2(config)# exit

6. Se Crea un usuario administrativo en la base de datos local.

Nombre de usuario: **admin**
Password: **admin1pass**
S1(config) #username admin password admin1pass
S2(config) # username admin password admin1pass

7. Se Configura el inicio de sesión en las líneas VTY para que use la base de datos local

S1(config)# line vty 0 4	Configurar line vty 0 4
S1(Config-line)# password ciscoenpass	Ingresar password ciscoenpass
S1(config-line)# login local línea de tiempo virtual	Hace que pida contraseña al acceder
S1(config-line)# exit	
S1(config)#	

S2(config)# line vty 0 4	Configurar line vty 0 4
S2(Config-line)# password ciscoenpass	Ingresar password ciscoenpass
S2(config-line)# login línea de tiempo virtual	Hace que pida contraseña al acceder
S2(config-line)# exit	
S2(config)#	

8. Se Configura las líneas VTY para que acepten únicamente las conexiones SSH.

Switch >enable
S1# configure terminal
S1 (config)# hostname **SSH**

SSH(config)# enable password **ciscoenpass**
SSH (config)# ip domain-name **ccna-lab.com**
SSH (config)# crypto key generate rsa general-Keys modulus 1024
SSH (config)# line VTY 0 15
SSH (config)# password ciscoenpass (esta será la contraseña para logearme a la seccion de SSH).
SSH (config-line)# login
SSH (config-line)# transport input ssh (activar solo la línea ssh en la línea de VTY).
SSH(config) #exit

Switch >enable
S2# configure terminal
S2 (config)# hotsname **SSH**
SSH(config)# enable password **ciscoenpass**
SSH (config)# ip domain-name **ccna-lab.com**
SSH (config)# crypto key generate rsa general-Keys modulus 1024
SSH (config)# line VTY 0 15
SSH (config)# password ciscoenpass(esta será la contraseña para logearme a la seccion de SSH).
SSH (config-line)# login
SSH (config-line)# transport input ssh(activar solo la línea ssh en la línea de VTY).

9. Cifrar las contraseñas de texto no cifrado.

S1#disable
S1>enable
Password: ciscoenpass
Password: ciscoenpass
Password: ciscoenpass
% Bad secrets
S2#disable
S2>enable
Password: ciscoenpass
Password: ciscoenpass
Password: ciscoenpass
% Bad secrets

10. Se Configura un MOTD Banner.

S1(config)# banner motd Authorized Access Only
S1(config)#exit
S1#exit

Switch > enable
S2# configure terminal
S2(config)# banner motd Authorized Access Only

11. Se Genera una clave de cifrado RSA.

Switch > enable
S1# configure terminal
S1(config)# crypto key generate rsa general-Keys modulus 1024

Switch > enable
S2# configure terminal
S2(config)# crypto key generate rsa general-Keys modulus 1024

12. Se Configura la interfaz de administración (SVI).

Switch > enable
S1# configure terminal
S1(config)# interface VLAN 98
S1(config-if)# ip address 10.19.8.98 255.255.0.0
S1 (config-if)# no shutdown
S1 (config-if)# end
S1 (config-if)# wr

Switch > enable
S2# configure terminal
S2(config)# interface VLAN 99
S2(config-if)# ip address 10.19.8.99 255.255.0.0
S2 (config-if)# no shutdown
S2 (config-if)# end
S2 (config-if)# wr

13. Se Configura el gateway predeterminado.

Switch > enable
S1# configure terminal

S1 (config)#ip default-gateway 10.19.8.97
S1 (config)# end
S1 (config-if)# wr

Switch > enable
S2# configure terminal
S2 (config)# ip default-gateway 10.19.8.97
S2 (config)# end
S2 (config-if)# wr

Paso 3: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tabla 5. Configurar S1

1. Se crea VLAN

S1 # configure terminal

S1(config)# VLAN 2 S1(config-

VLAN)# name Bikes

S1 # configure terminal

S1(config)# VLAN 3 S1(config-
VLAN)# name trikes

S1 # configure terminal
S1(config)# VLAN 4
S1(config-VLAN)# name Management
S1 # configure terminal
S1(config)# VLAN 5

S1(config-VLAN)# name Parking
S1 # configure terminal
S1(config)# VLAN 5
S1(config-VLAN)# name Native

2. Se Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5

Cuando se habilite el troncal en el puerto con el enlace en la interfaz con el comando switchport mode trunk, se configura automáticamente la encapsulación de 802.1Q.

S1(config)# interface F0/1
S1(config-if)# Switchport mode trunk
S1(config-if)#switchport trunk native vlan 98

S1(config)# interface F0/2
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 98

S1(config)# interface F0/5
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 98

3. Se Crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

S1(config)#interface range Fastethernet 0/1 – 2
S1(config-if-range)# channel-group 1 mode active
S1(config-if-range)#interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 2,3,4,5

4. Se Configura el puerto de acceso de host para VLAN 2

S1# configure terminal
S1(config)# interface range F0/6
S1(config-if-range)# switchport mode Access
S1(config-if-range)#switchport Access VLAN 2

5. Se Configura la seguridad del puerto en los puertos de acceso

S2# Configure terminal
S2(config)# interface fastethernet 0/1
S2(config-if)#switchport mode Access
S2(config-if)#switchport port-security máximum 3
S2(config-if)#end
S2(config)# interface fastethernet 0/2
S2(config-if)#switchport mode Access
S2(config-if)#switchport port-security máximum 3
S2(config-if)#end
S2(config)# interface fastethernet 0/5
S2(config-if)#switchport mode Access
S2(config-if)#switchport port-security máximum 3
S2(config-if)#end

6. Proteja todas las interfaces no utilizadas.

S1(config)#interface range f0/4-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport port-security Vlan5

S1(config-if-range)#description interface no use

S1(config-if-range)#no shutdown

S1(config-if-range)# interface range g0/1-2

S1(config-if-range)# switchport mode Access

S1(config-if-range)# switchport Access vlan 5

S1(config-if-range)#description interface no use

S1(config-if-range)#no shutdown

Paso4: Configure el S2.

Entre las tareas de configuración de S2 se incluyen las siguientes:

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18
Configure port-security en los access ports	permite 3 MAC addresses
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tabla 6. Configurar S1

1.Se crear VLAN

S2 # configure terminal

S2(config)# VLAN 2 S2(config-

VLAN)# name Bikes

S2 # configure terminal

S2(config)# VLAN 3 S2(config-

VLAN)# name trikes S2 #

configure terminal S2(config)#

VLAN 4

S2(config-VLAN)# name Management

S2 # configure terminal

S2(config)# VLAN 5

S2(config-VLAN)# name Parking

S2 # configure terminal

S2(config)# VLAN 5

S2(config-VLAN)# name Native

2. Se Crea troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5

Cuando se habilite el troncal en el puerto con el enlace en la interfaz con el comando switchport mode trunk, se configura automáticamente la encapsulación de 802.1Q.

S2(config)# interface F0/1
S2(config)# Switchport mode trunk
S2(config)#switchport trunk native vlan 99

S2(config)# interface F0/2
S2(config)# switchport mode trunk
S2(config)# switchport trunk native vlan 99

3. Se Crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

S2(config)#interface range Fastethernet 0/1 – 2

S2(config-if-range)# channel -group 1 mode active

S2(config-if-range)#interface port-channel 1

S2(config-if)# switchport mode trunk

S2(config-if)#switchport trunk allowed vlan 2,3,4,5

4. Se Configura el puerto de acceso de host para VLAN 3

S2# configure terminal
S2(config)# interface F0/18
S2(config-if-range)# switchport mode Access
S2(config-if-range)#switchport Access VLAN 3

5. Se Configura la seguridad del puerto en los puertos de acceso

S2# Configure terminal
S2(config)# interface fastethernet 0/1
S2(config-if)#switchport mode Access
S2(config-if)#switchport port-security máximum 3
S2(config-if)#end

6. Se Asegura todas las interfaces no utilizadas.
S2(config)#interface range f0/4-24
S2(config-range)#switchport mode Access
S2(config-range)#switchport Access Vlan5
S2(config-range)#description interface no use
S2(config-range)#no shutdown
S2(config-range)# interface range g0/1-2
S2(config-range)# switchport mode Access

S2(config-range)# switchport Access vlan 5
S2(config-range)#description interface no use
S2(config-range)#no shutdown

Parte 2: Configurar soporte de host

Paso 1: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
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

Tabla 7. Configurar R1

1. Se Configura Default Routing

Router> enable

R1# show ipv6 router

R1(config)#ip route 0.0.0.0.0.0.0.0

R1(config)#

Router> enable

R1# show ipv4 router

IPv6 Routing Table - default - 4 entries

2. Se Configura IPv4 DHCP para VLAN

R1# config t
R1(config)# ip routing
R1(config-if)# interface Vlan 2
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config)# End

3. Se Configura DHCP IPv4 para VLAN 3

R1# config t
R1(config)# ip routing
R1(config-if)# interface Vlan 3
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config)# End

R2# configure terminal Entrar a Configure Termial
R2(config)# hostname <nombre-Router> Se configura con hostname nombre-switch
<nombre-switch>(config)#ip domain-name ccna-lab.net
<nombre-switch>(config)#end

Paso 2: Configurar los servidores

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**.

PC-A Network Configuration	
Descripción	Microsoft wi-fi Direct Virtual adapter #3
Dirección física	B2-FC-36-E5-0A-7F
Dirección IP	192.168.0.1
Máscara de subred	255.255.255.0
Gateway predeterminado	192.168.0.1
Gateway predeterminado IPv6	145816630

Configuración de red de PC-A	
Descripción	Microsoft wi-fi direct virtual adapter #3
Dirección física	B2-FC-36-E5-0A-7F
Dirección IP	192.168.0.1
Máscara de subred	255.255.255.0
Gateway predeterminado	192.168.0.1
Gateway predeterminado IPv6	145816630

Tabla 8. Configurar de los Servidores

Parte 3: 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	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	si
		IPv6	2001:db8:acad:a: :1	no
	R1, G0/0/1.3	Dirección	10.19.8.65	no
		IPv6	2001:db8:acad:b: :1	no
	R1, G0/0/1.4	Dirección	10.19.8.97	no
		IPv6	2001:db8:acad:c: :1	no
	S1, VLAN 4	Dirección	10.19.8.98	no
		IPv6	2001:db8:acad:c: :98	no
	S2, VLAN 4	Dirección	10.19.8.99.	no
		IPv6	2001:db8:acad:c: :99	no

Desde	A	de Internet	Dirección IP	Resultados de ping
	PC-B	Dirección	IP address Will vary.	Si
		IPv6	2001:db8:acad:b: :50	si
	R1 Bucle 0	Dirección	209.165.201.1	no
		IPv6	2001:db8:acad:209: :1	no
PC-B	R1 Bucle 0	Dirección	209.165.201.1	no
		IPv6	2001:db8:acad:209: :1	no
	R1, G0/0/1.2	Dirección	10.19.8.1	si
		IPv6	2001:db8:acad:a: :1	no
	R1, G0/0/1.3	Dirección	10.19.8.65	no
		IPv6	2001:db8:acad:b: :1	no
	R1, G0/0/1.4	Dirección	10.19.8.97	no
		IPv6	2001:db8:acad:c: :1	no
	S1, VLAN 4	Dirección	10.19.8.98	si
		IPv6	2001:db8:acad:c: :98	si
	S2, VLAN 4	Dirección	10.19.8.99.	
		IPv6	2001:db8:acad:c: :99	

Tabla 9. Probar y Verificar la conectividad de extremo a extremo

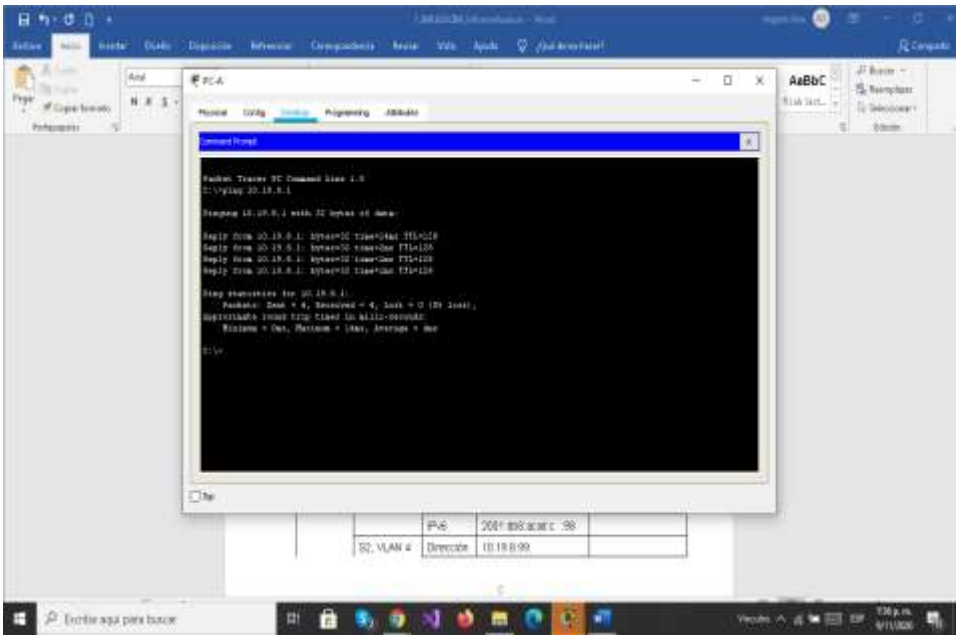


Figura.3 ping de Comprobación.

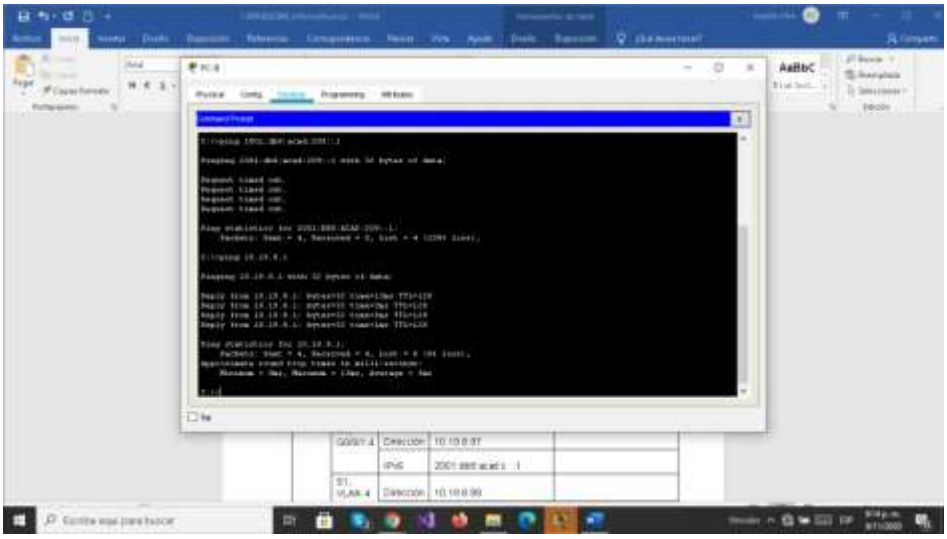


Figura .4 ping de Comprobación

Escenario 2

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

Figura 15. Escenario 2

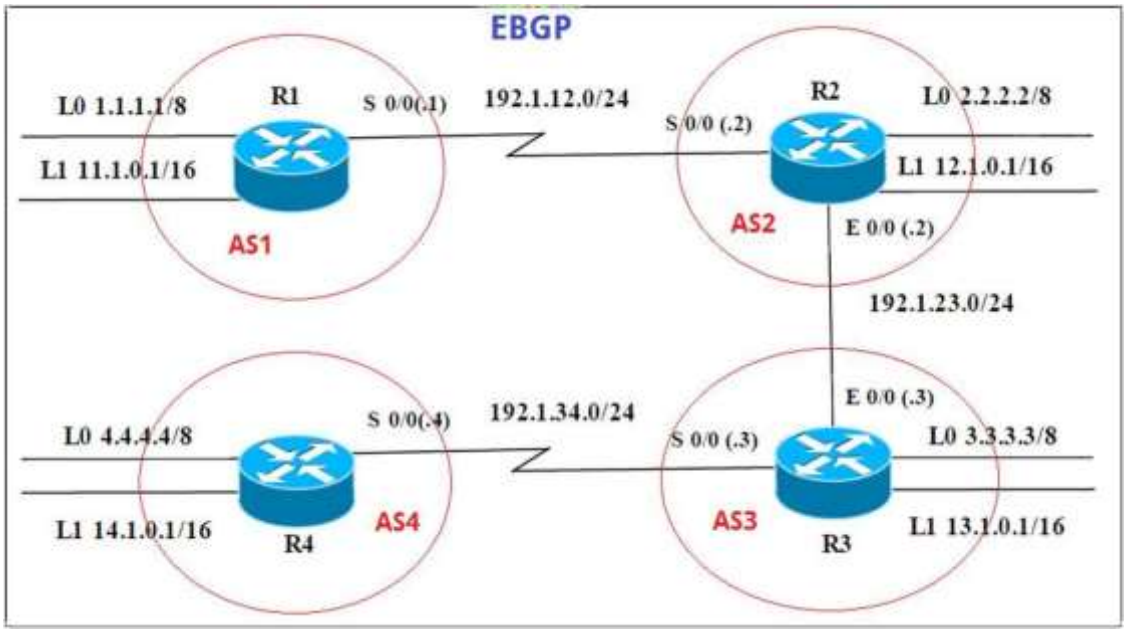
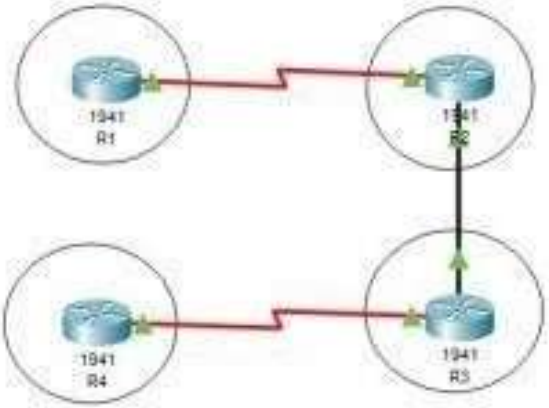
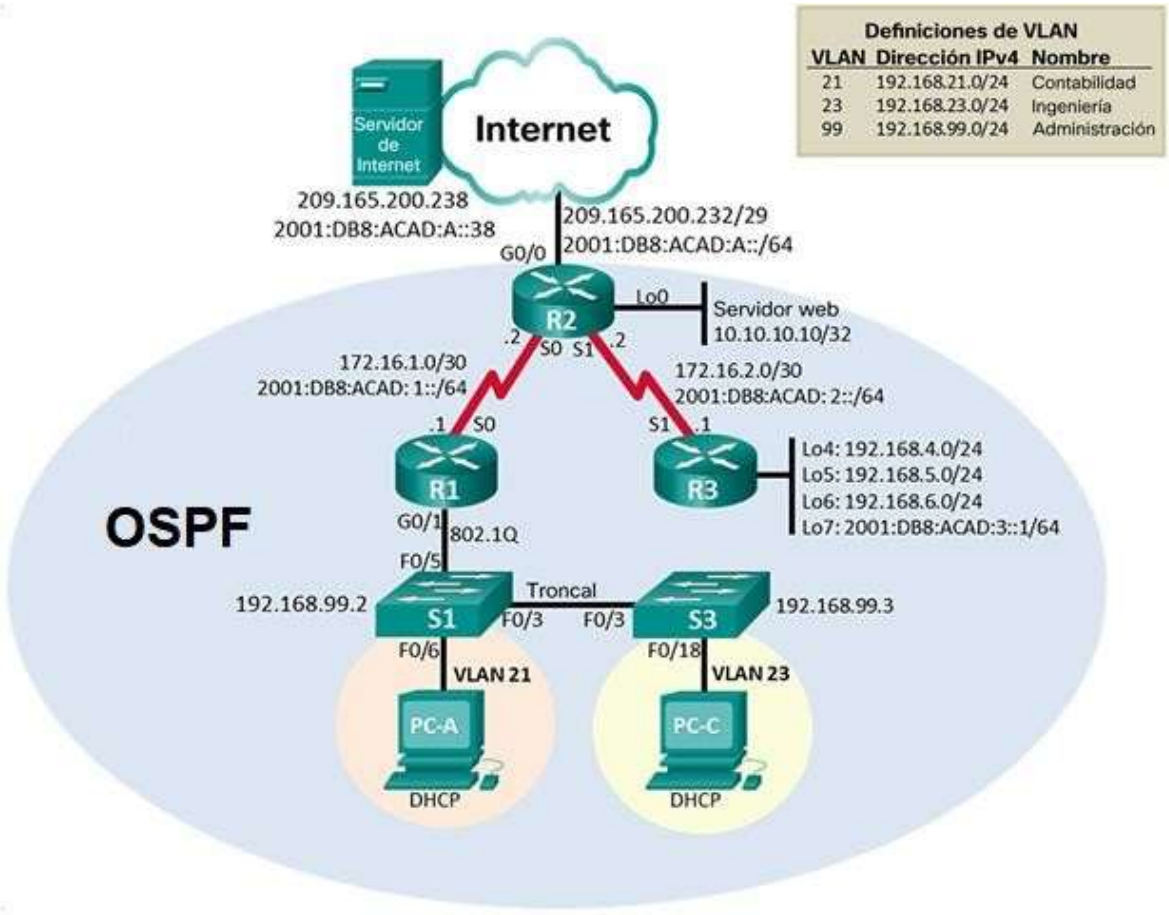


Figura 16. Simulación del escenario 2





Parte 1: Inicializar dispositivos

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

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

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

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

Tabla 10. Inicializar y volver a cargar los routers y los switches

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.232
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 11. Configurar la Computadora 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.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)# no ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	Class R1(config)# enable secret class
Contraseña de acceso a la consola	Cisco R1#configure terminal R1(config)#line console 0 R1(config-line)# password cisco R1(config-line)#login R1(config-line)# exit ok
Contraseña de acceso Telnet	R1#configure terminal R1(config)#line vty 0 15 R1(config-line)# password cisco R1(config-line)#login R1(config-line)# exit ok
Cifrar las contraseñas de texto no cifrado	R1#configure terminal R1(config)# service password-encryption ok
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)# banner motd #Se prohíbe el acceso no autorizado# ok

Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz R1# configure terminal R1(config)# interface S0/0/0 R1(config)#description connection to R2 R1(config-if)# ip add 172.16.1.0 255.255.255.252 R1(config-if)# ipv6 add 2001:DB8:ACAD:A::a/64 R1(config-if)# clock rate 128000 R1(config-if)# no shutdown ok
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 R1 (config)# ip route 0.0.0.0 0.0.0.0 s0/0/0 R1 (config)# ipv6 route ::/0 s0/0/0 ok

Tabla 12. Configurar R1

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)# no ip domain-lookup ok
Nombre del router	R2
Contraseña de exec privilegiado cifrada	Class R2(config)# enable secret class ok
Contraseña de acceso a la consola	Cisco R2#configure terminal R2(config)#line console 0 R2(config-line)# password cisco R2(config-line)#login R2(config-line)# exit ok
Contraseña de acceso Telnet	Cisco R2#configure terminal R2(config)#line vty 0 15 R2(config-line)# password cisco R2(config-line)#login R2(config-line)# exit ok
Cifrar las contraseñas de texto no cifrado	R2#configure terminal R2(config-line)# service password-encryption ok
Habilitar el servidor HTTP	R2(config)# ip http server R2(config)#ip http secure-server R2(config)#ip http authentication local Este comando no es soportado packe trecer
Mensaje MOTD	Se prohíbe el acceso no autorizado. R2(config)# banner motd #Se prohíbe el acceso no autorizado# ok

Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R2# configure terminal Router(config)# interface S0/0/0 R2(config-if)# description connection to R1 Router(config-if)# ip address 172.16.2.0 255.255.255.252 R2(config-if)# ipv6 address 2001:db8:acad:1::2/64 R2(config-if)# no shutdown R2(config-if)# exit ok
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dire acción disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz R2# configure terminal R2(config)# interface S0/0/1 R2(config-if)# description connection to R3 R2(config-if)# ip address 172.16.1.2 255.255.255.252 R2(config-if)# ipv6 address 2001:db8:acad:2::2/64 R2(config-if)# clock rate 128000 R2(config-if)# no shutdown R2(config-if)# exit ok

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz R2# configure terminal R2(config)# interface G0/0 R2(config-if)# description connection to internet R2(config-if)# ip address 209.165.200.232 255.255.255.248 R2(config-if)# ipv6 address 2001:db8:acad:a::1/64 R2(config-if)# no shutdown ok
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. R2(config)# interface loopback 0 R2(config-if)# ip address 10.10.10.10 255.255.255.0 R2(config-if)#description servidor web simulado R2(config-if)# exit ok
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 ok

Tabla 13. Configurar R2

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)# no ip domain-lookup
Nombre del router	Router(config)# Host R3
Contraseña de exec privilegiado cifrada	Class R3(config)# enable secret class ok
Contraseña de acceso a la consola	Cisco R3#configure terminal R3(config)#line console 0 R3(config-line)# password cisco R3(config-line)#login R3(config-line)# exit ok
Contraseña de acceso Telnet	Cisco R3#configure terminal R3(config)#line vty 0 15 R3(config-line)# password cisco R3(config-line)#login R3(config-line)# exit ok
Cifrar las contraseñas de texto no cifrado	R3#configure terminal R3(config)# service password-encryption ok
Mensaje MOTD	Se prohíbe el acceso no autorizado. R3(config)# banner motd #Se prohíbe el acceso no autorizado# ok

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R3# configure terminal Router(config)# interface S0/0/1 R3(config-if)# description connetion to R2 Router(config-if)# ip address 172.16.1.2 255.255.255.252 R3(config-if)# ipv6 address 2001:db8:acad:1::2/64 R3(config-if)# no shutdown R3(config-if)# exit ok
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# interface loopback 4 R3(config-if)# ip address 192.168.4.0 255.255.255.0 R2(config-if)# exit ok
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# interface loopback 5 R3(config-if)# ip address 192.168.5.0 255.255.255.0 R2(config-if)# exit ok
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# interface loopback 6 R3(config-if)# ip address 192.168.6.0 255.255.255.0 R2(config-if)# exit ok

Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)# interface loopback 7 R3(config-if)# ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)# exit ok
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

Tabla 14. Configurar R3

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)# host S1
Contraseña de exec privilegiado cifrada	Class S1(config)# enable secret class ok
Contraseña de acceso a la consola	Cisco S1#configure terminal S1(config)#line console 0 S1(config-line)# password cisco S1(config-line)#login S1(config-line)# exit ok
Contraseña de acceso Telnet	Cisco S1#configure terminal S1(config)#line vty 0 15 S1(config-line)# password cisco S1(config-line)#login S1(config-line)# exit ok
Cifrar las contraseñas de texto no cifrado	S1#configure terminal S1(config)# service password-encryption ok

Mensaje MOTD	Se prohíbe el acceso no autorizado. S1(config)# banner motd #Se prohibe el acceso no autorizado# ok

Tabla 15. Configurar S1

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)# no ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	Class S3(config)# enable secret class ok
Contraseña de acceso a la consola	Cisco S3#configure terminal S3(config)#line console 0 S3(config-line)# password cisco S3(config-line)#login S3(config-line)# exit ok
Contraseña de acceso Telnet	Cisco S3#configure terminal S3(config)#line vty 0 15 S3(config-line)# password cisco S3(config-line)#login S3(config-line)# exit ok
Cifrar las contraseñas de texto no cifrado	S3#configure terminal S3(config)# service password-encryption ok
Mensaje MOTD	Se prohíbe el acceso no autorizado. S3(config)# banner motd #Se prohibe el acceso no autorizado# ok

Tabla 16. Configurar S3

Paso 7: Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.0	No exitoso
R2	R3, S0/0/1	172.16.2.0	exitoso
PC de Internet	Gateway predeterminado	209.165.200.232	No exitoso

Tabla 17. Verificación la conectividad de la red

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

Comando R1

R1>enable
Password: cisco
Password:class
R1#ping 172.16.1.0

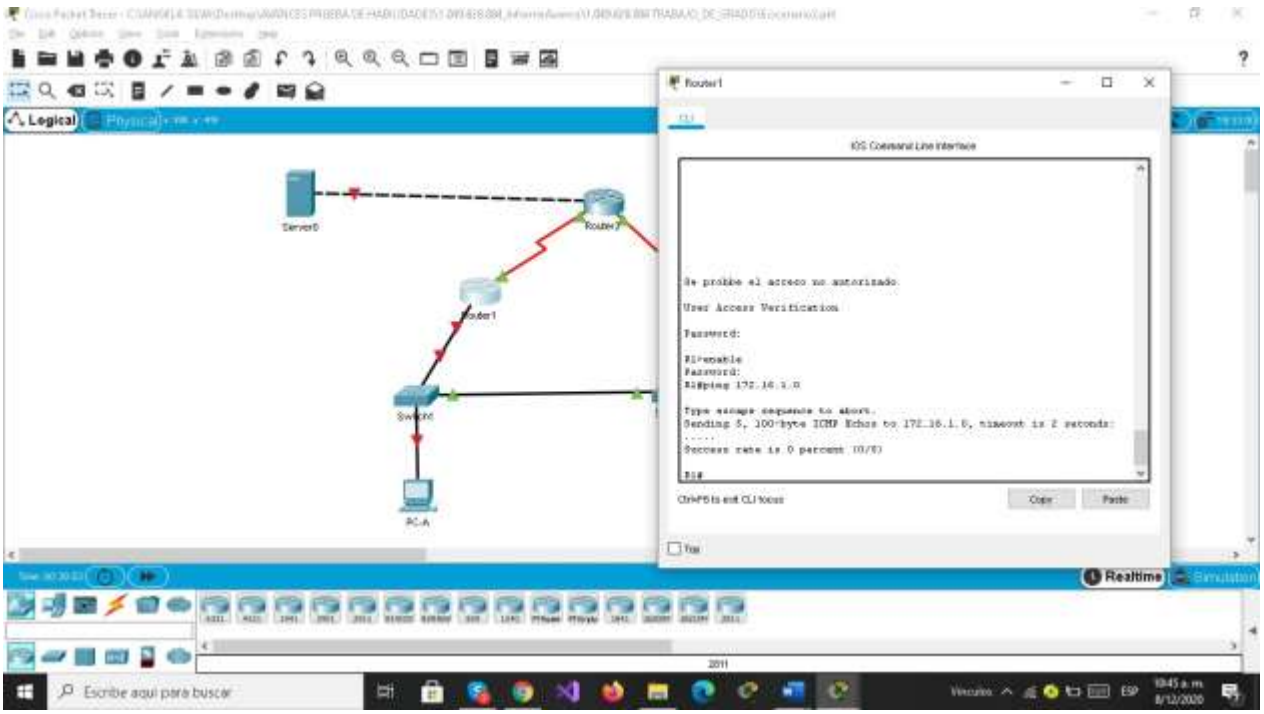


Figura 17. Conectividad de Ping R1 al R2

Comando R2
R1>enable
Password: cisco
Password:class
R1#ping 172.16.2.0

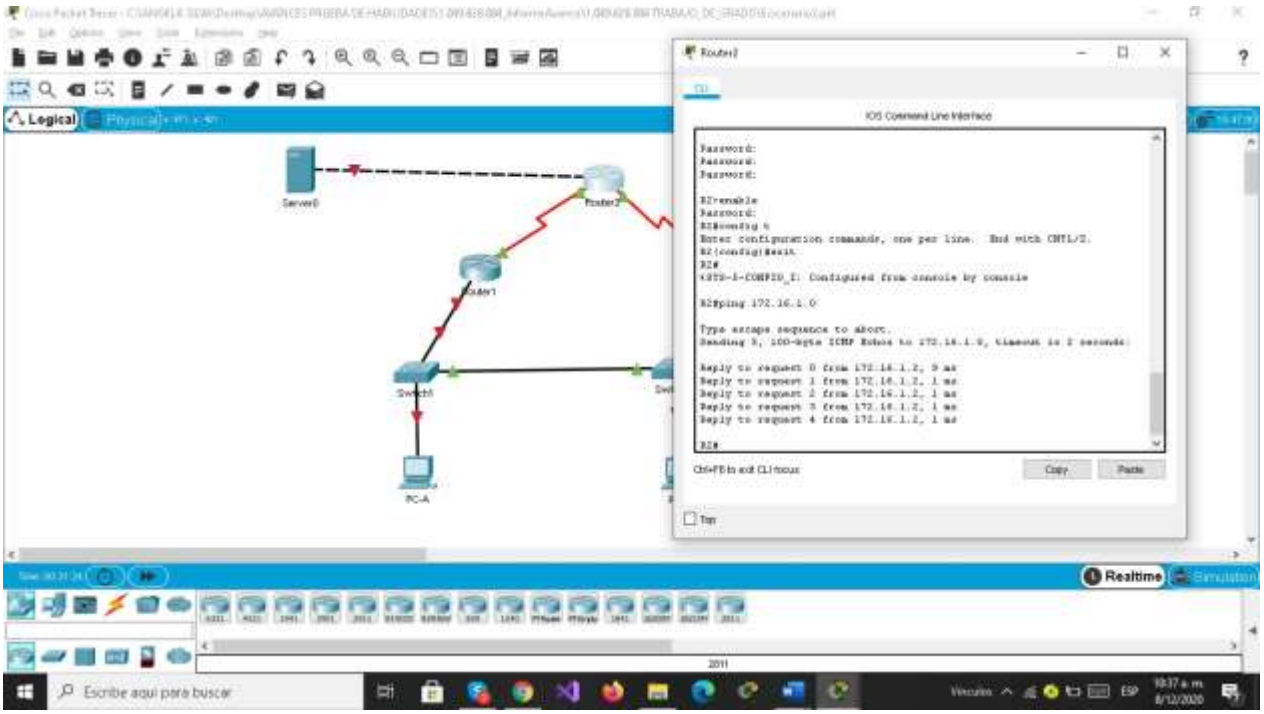


Figura 18. Conectividad de Ping R2 al R3

Comando para Pc Internet

Ingresar símbolo del sistema e ingrese Ping.

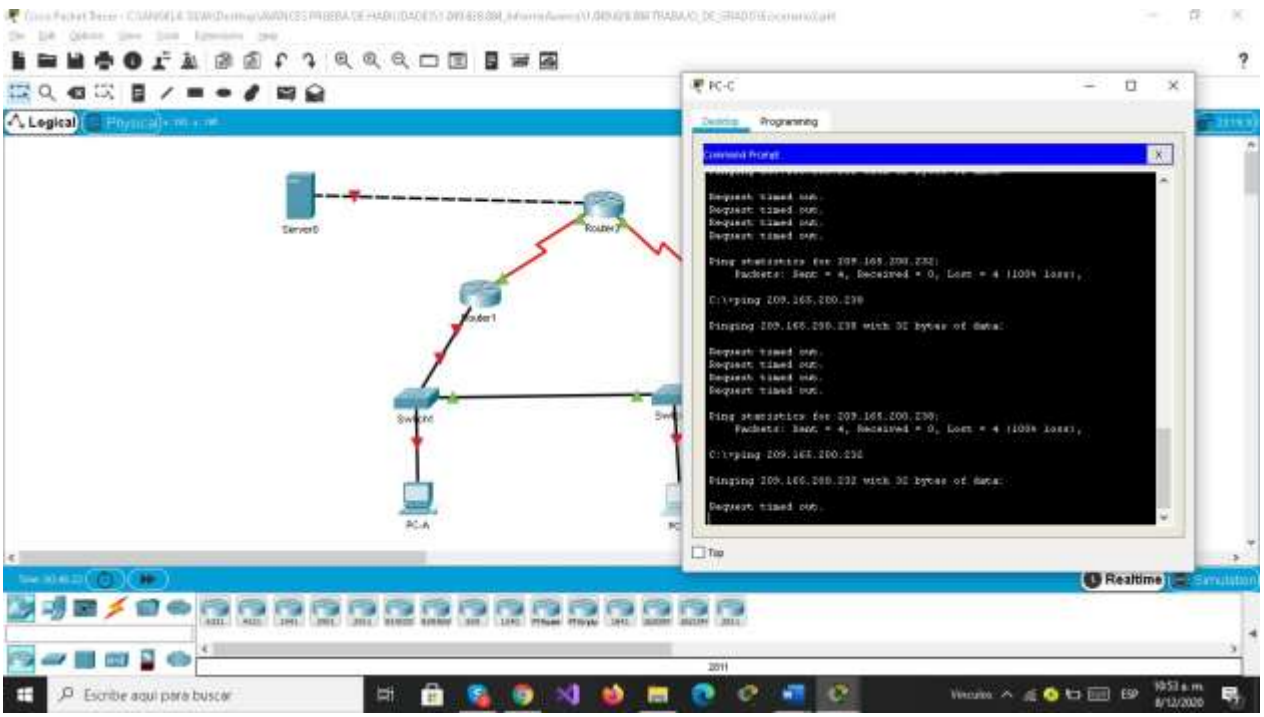


Figura 19. Conectividad de PC internet a Gateway predeterminado

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican. S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config)#exit S1(config)#Vlan 23 S1(config-vlan)#name Ingenieria S1(config)#exit S1(config)#Vlan 99 S1(config-vlan)# name Administracion S1(config)#exit ok
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-if)#ip address 192.168.99.2 255.255.255.0 S1(config)#no shutdown ok
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config-if)#ip default-gateway 192.168.99.2 ok

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#configure terminal S1(config)#interface F0/3 S1(config)# switchport mode trunk S1(config)# switchport trunk native vlan 1 S1(config)#exit ok
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config)#configure terminal S1(config)#interface F0/5 S1(config)# switchport mode trunk S1(config)# switchport trunk native vlan 1 S1(config)#exit ok
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)#configure terminal S1(config-if-range)#interface range f0/1-2, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config)#exit ok
Asignar F0/6 a la VLAN 21	S1(config)#interface range f0/6 S1(config-range)# switchport access vlan 21 S1(config-range)#exit ok
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if)#shutdown

Tabla 18. Configurar S1

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. S3(config)#vlan 21 S3(config)#name Contabilidad S3(config)#exit S3(config)#Vlan 23 S3(config)#name Ingenieria S3(config)#exit S3(config)#Vlan 99 S3(config)# name Administracion S3(config)#exit ok
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)#ip address 192.168.99.3 255.255.255.0 S3(config)#no shutdown S3(config)# ok
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 209.165.200.225 ok

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3(config)#configure terminal S3(config)#interface F0/3 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native vlan 1 S3(config-if)#exit ok
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-range)# switchport mode access S3(config-range)#exit ok
Asignar F0/18 a la VLAN 21	S3(config)#interface range f0/18 S3(config-range)# switchport access vlan 21 S3(config-range)#exit ok
Apagar todos los puertos sin usar	S3(config)# int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-range)#shutdown

Tabla 19. Configurar S3

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/0.1.	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 vlan 21 R1(config-subif)# encapsulation dot1q 21 R1(config-subif)# ip address 192.168.21.0 255.255.255.0 ok
Configurar la subinterfaz 802.1Q .23 en G0/0.1	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 vlan 23 R1(config-subif)# encapsulation dot1q 23 R1(config-subif)# ip address 192.168.23.0 255.255.255.0 ok
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz. R1(config)#interface g0/1.99 R1(config-subif)# description vlan 99 R1(config-subif)# encapsulation dot1q 99 R1(config-subif)# ip address 192.168.99.0 255.255.255.0 ok
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shut

Tabla 20. Configurar R1

Paso 4: Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.0	No exitoso
S3	R1, dirección VLAN 99	192.168.99.0	No exitoso
S1	R1, dirección VLAN 21	192.168.21.0	No exitoso
S3	R1, dirección VLAN 23	192.168.23.0	No exitoso

Tabla 21. Verificacion la conectividad de red

Ping en S1

S1> enable

Password: class

S1#ping 192.168.99.0

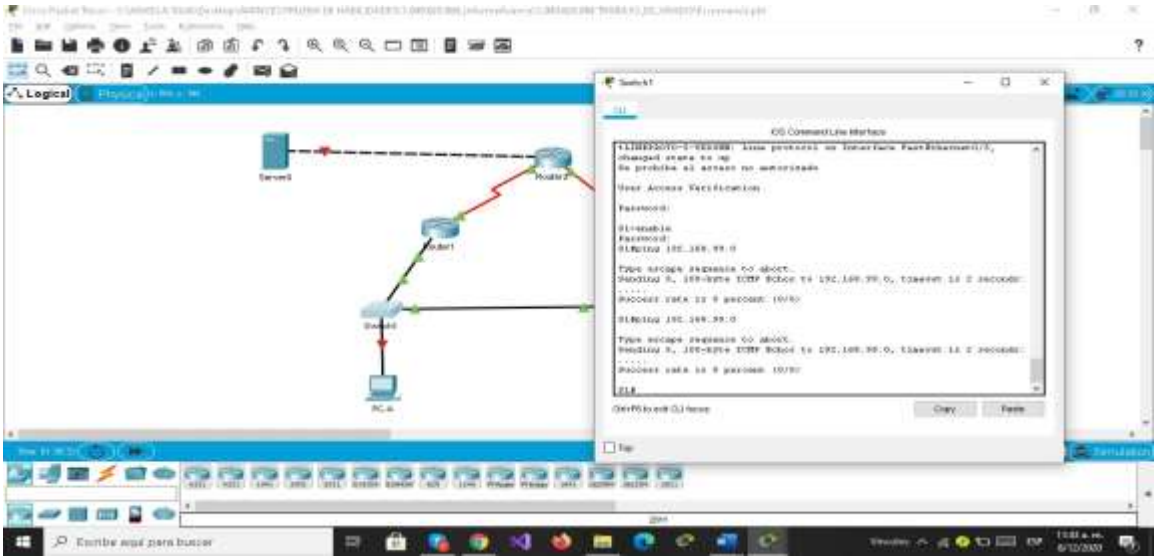


Figura 20. Conectividad de ping S1 al R1

S3>enable

Password: class

S3#ping 192.168.99.0

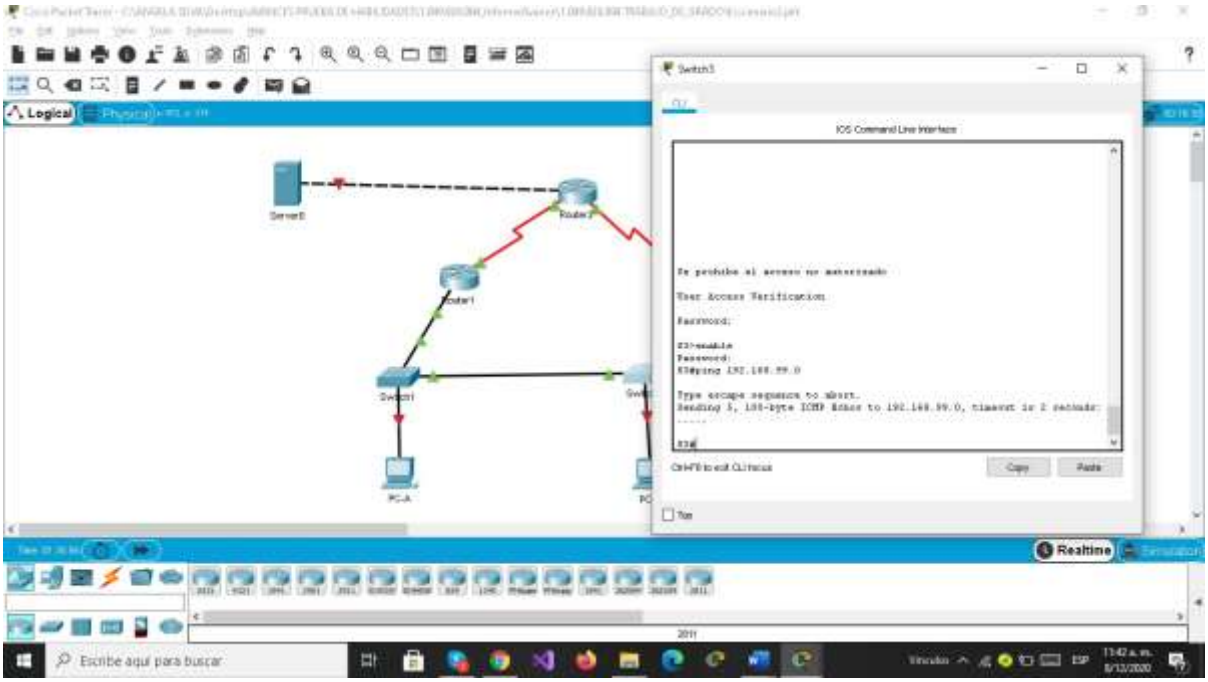


Figura 21. Conectividad de ping S3 al R1

S1> enable
Password: class
S1#ping 192.168.21.0

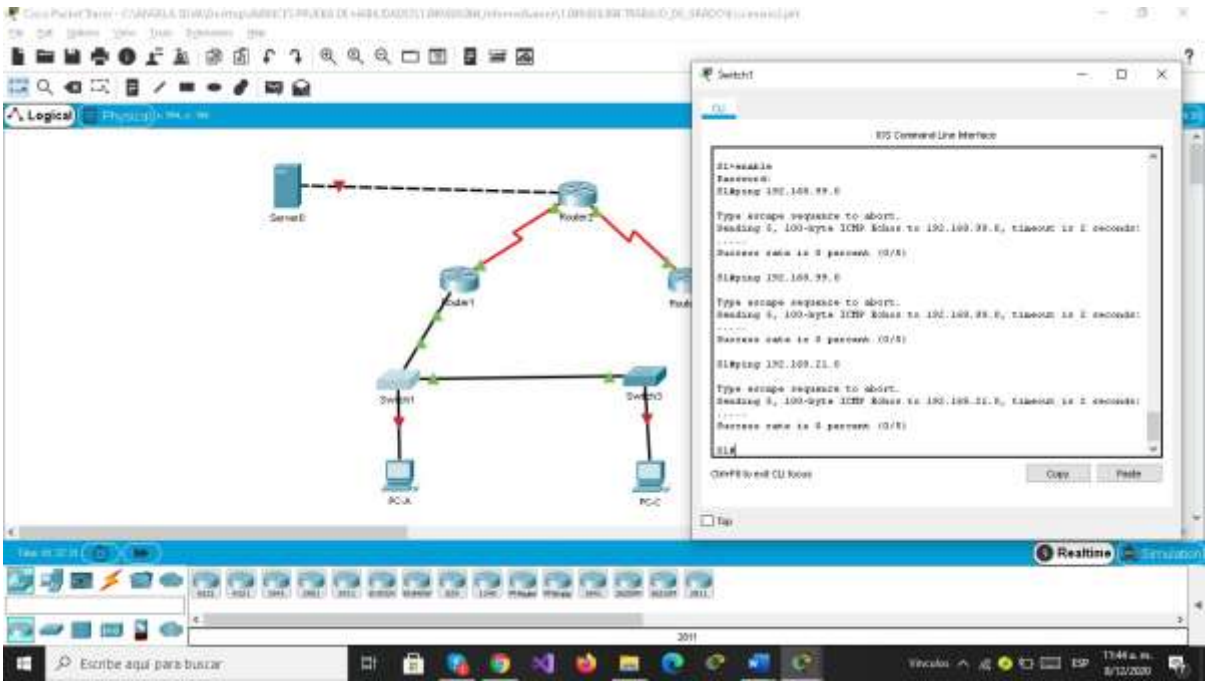


Figura 22. Conectividad de ping S1 al R1

S3>enable
Password: class
S3#ping 192.168.23.0

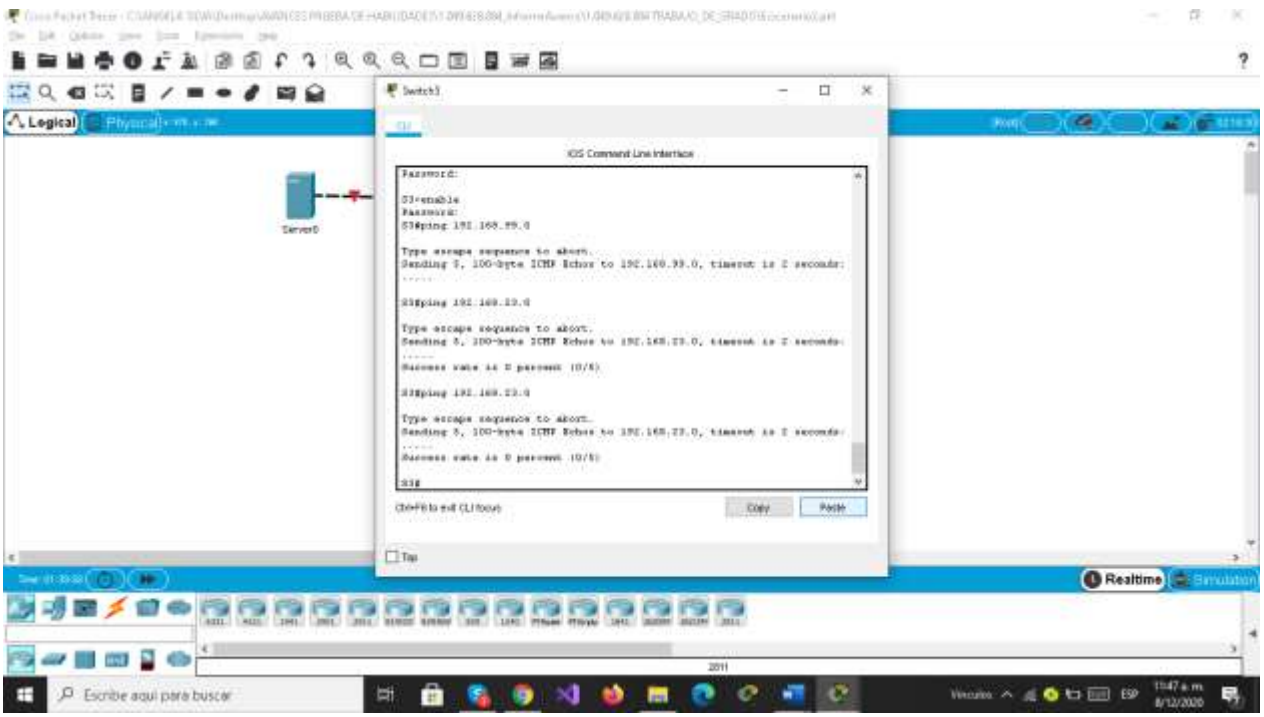


Figura 23. Conectividad de ping S3 al R1

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 1	R1(config)# router ospf 1 ok
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config)# network 172.16.1.0 255.255.255.0 area 0 ok

	R1(config)#router eigrp 10 R1(config)# passive-interface g0/0 R1(config)#router eigrp 10 R1(config)# passive-interface g0/1.21 R1(config)#router eigrp 10 R1(config)# passive-interface g0/1.23 R1(config)#router eigrp 10 R1(config)# passive-interface S0/0/0 R1(config)#router eigrp 10 R1(config)# passive-interface S0/0/1
Establecer todas las interfaces LAN como pasivas	ok

Tabla 22. Configurar OSPF en el R1

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)# router ospf 1
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config)# network 172.16.1.0 255.255.255.0 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config)# router ospf 0 R2(config)# passive-interface loopback0 ok
Desactive la sumarización automática.	R2(config)# router rip R2(config-router)# no auto-summary R2(config-router)# exit ok

Tabla 23. Configurar OSPF en el R2

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)# router ospf 0
Anunciar redes IPv4 conectadas directamente	R2(config)# network 172.16.1.0 255.255.255.0 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R2(config)#ip router ospf 0 R2(config)# passive-interface loopback0
Desactive la sumarización automática.	R2(config)# router rip R2(config-router)# no auto-summary R2(config-router)# exit OK

Tabla 23. Configurar v3 en el R2

Paso 4: Verificar la información de OSPF

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

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R1# show ip OSPF
¿Qué comando muestra solo las rutas OSPF?	R1# Show ip router OSPF
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1# Show run OSPF

Tabla 24. Verificación la información de OSPF

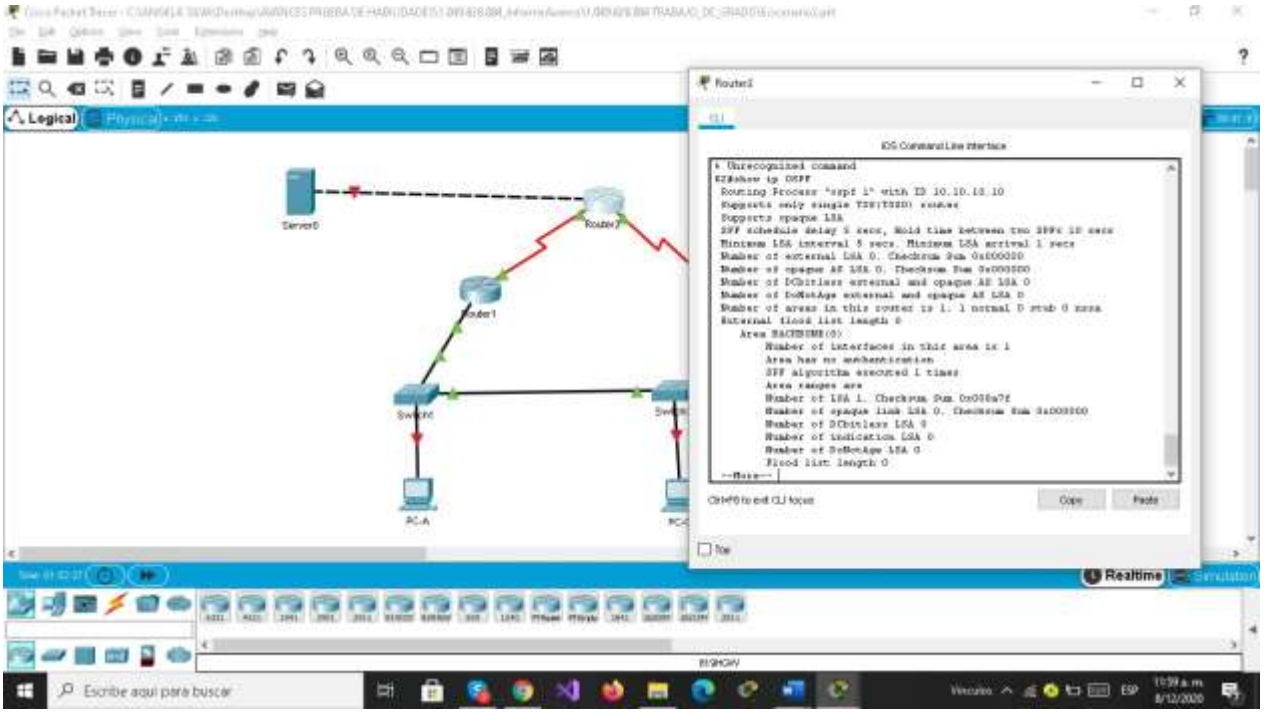


Figura 24 . Show protocols

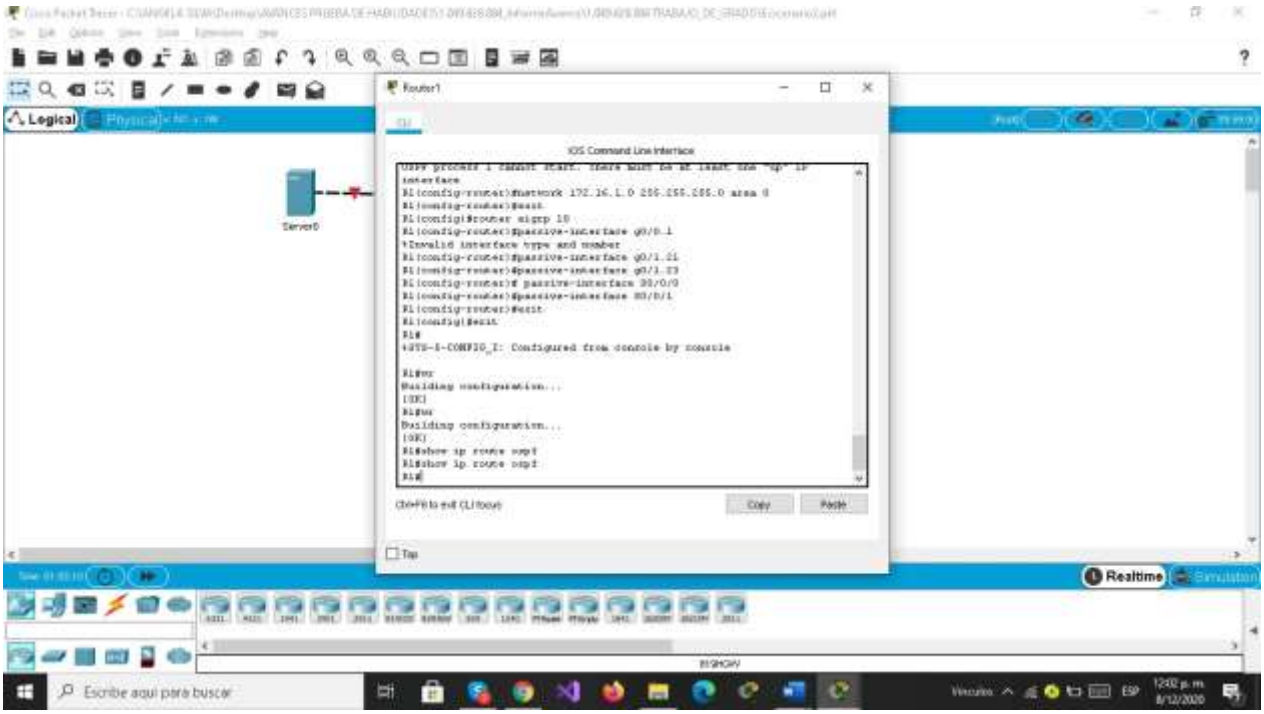


Figura 25. Show ip router OSPF

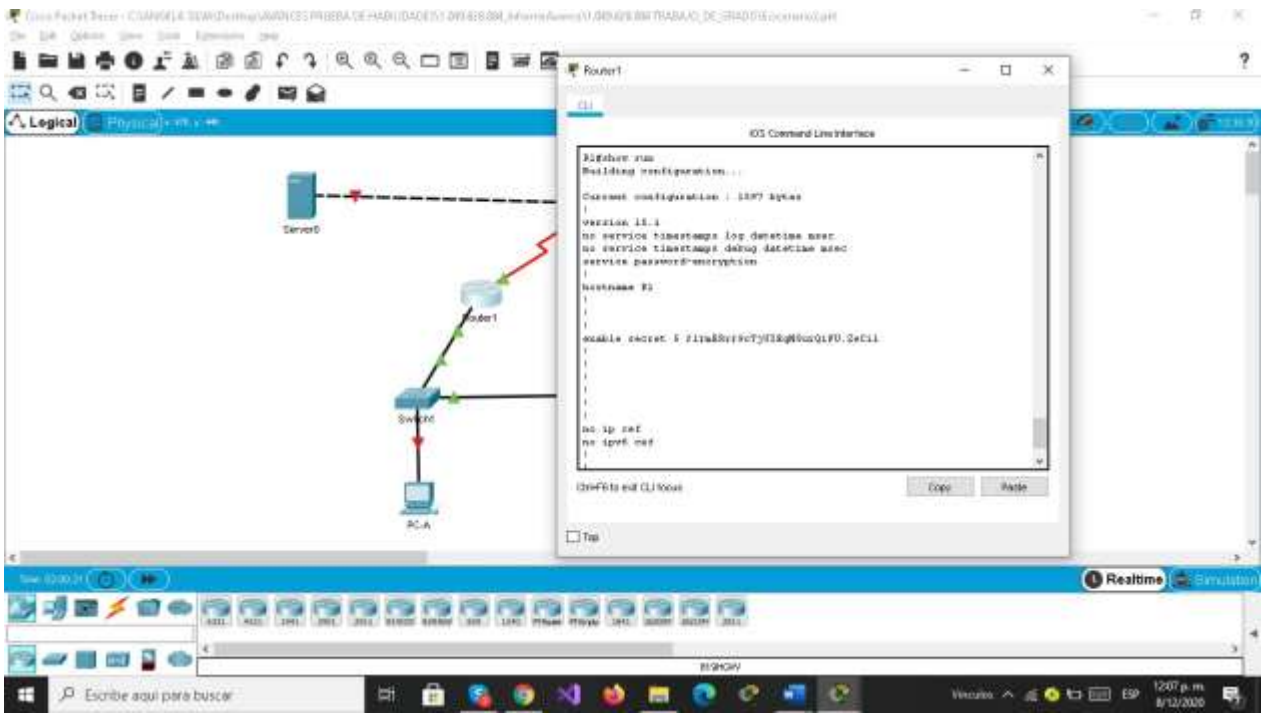


Figura 26. Show run OSPF

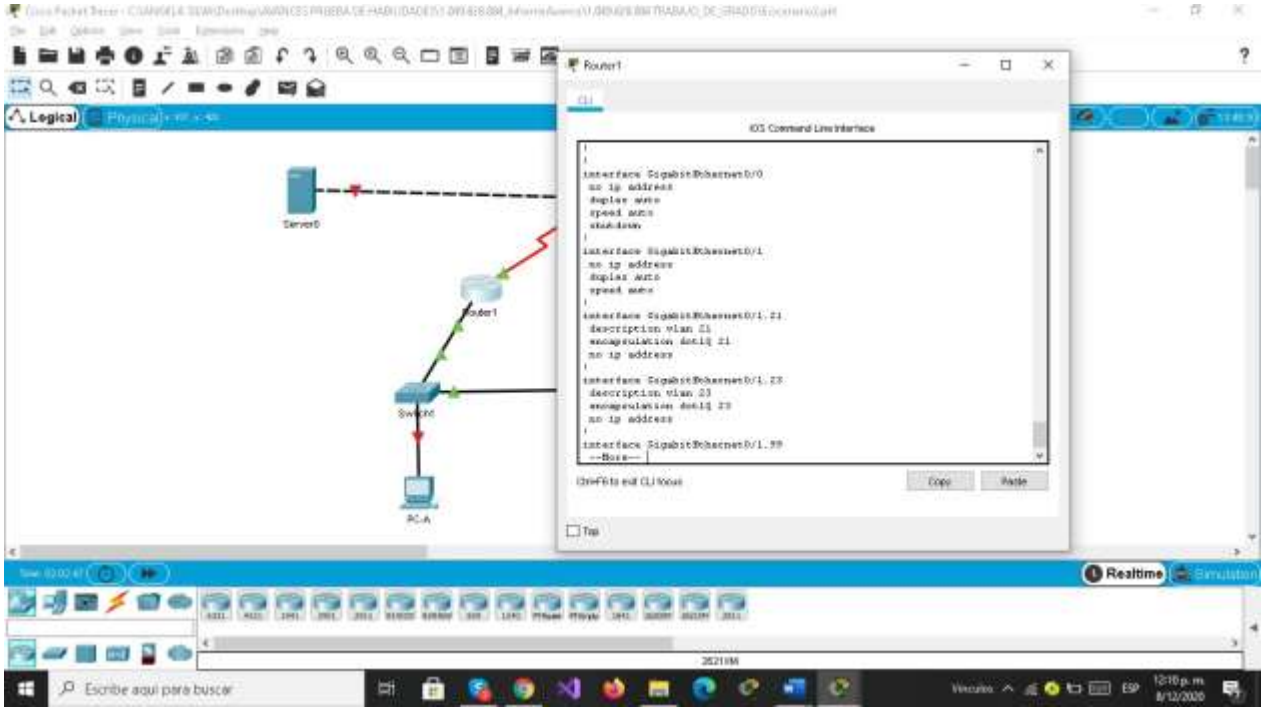


Figura 27. Show run OSPF

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1#(Config)ip dhcp excluded-address 192.168.21.2 192.168.21.20 ok
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1#(Config)ip dhcp excluded-address 192.168.23.2 192.168.23.20 ok
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) # network 192.168.21.0 255.255.255.0 R1#(dhcp-Config) #default-router 192.168.21.1 R1#(dhcp-Config) #dns-server 10.10.10.10 R1#(dhcp-Config) #domain-name ccna-sa.com ok
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1#(Config)ip dhcp pool ENGNR R1#(dhcp-Config) # network 192.168.23.0 255.255.255.0 R1#(dhcp-Config) #default-router 192.168.23.1 R1#(dhcp-Config) # dns-server 10.10.10.10 ok

Tabla 25. Configurar el R1 como servidor de DHCP para las vlan 21 y 23

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

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) #username webuser privilege 15 secret cisco12345 ok
Habilitar el servicio del servidor HTTP	R2(config)# ip http server ok
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)# aaa new-model R2(config)#aaa authentication login default local R2(config)#aaa authorization exec default local R2(config)# exit Este comando no son soportados en packe trecer pero en un servidor real deberia funcionar. ok

Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** R2(config)# ip nat inside source static 10.10.10.2 209.165.200.238 R2(config)#interface s0/0/0 R2(config)# ip address 10.10.10.0 255.255.255.252 ok
Asignar la interfaz interna y externa para la NAT estática.	R2(config-if)# interface s0/0/0 R2(config-if)#ip address 10.10.10.0 255.255.255.252 R2(config)# ip nat inside R2(config-if)#exit R2(config-if)# interface s0/0/0 R2(config-if)#ip address 209.165.200.238 255.255.255.252 R2(config)# ip nat outside R2(config-if)#exit ok
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)#ip nat inside source static 10.10.10.10 209.165.200.238 R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit R2Config)#access-list 1 permit 192.168.21.0 255.255.255.252 R2Config)#access-list 1 permit 192.168.23.0 255.255.255.252 R2Config)#access-list 1 permit 192.168.99.0 255.255.255.252 ok

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** R2Config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 ok
Definir la traducción de NAT dinámica	R2Config)# ip nat inside source list 1 pool INTERNET. ok

Tabla 26. Configurar la NAT estática y dinámica en el R2

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	El resultado es satisfactorio para PC-A
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	El resultado es satisfactorio para PC-C
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	El resultado es satisfactorio
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**	Los Pc no tienen comunicacion a internet utilizacion el comando http server porque en packet trecer es soportado para Activar el servidor web en R2. Pero Si utilizamos la direccion IP del servidor web en el navegador PC-A y PC-C temenos acceso a internet.

Tabla 27. Pruebas

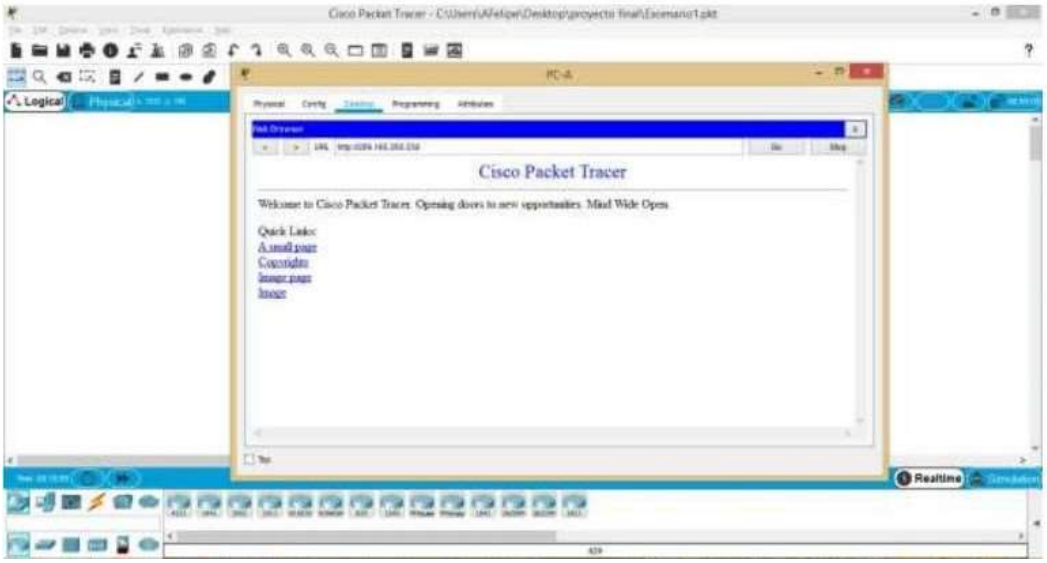


Figura 28. Conexión Internet desde PC-A utilizando la direccion IP del servidor de internet

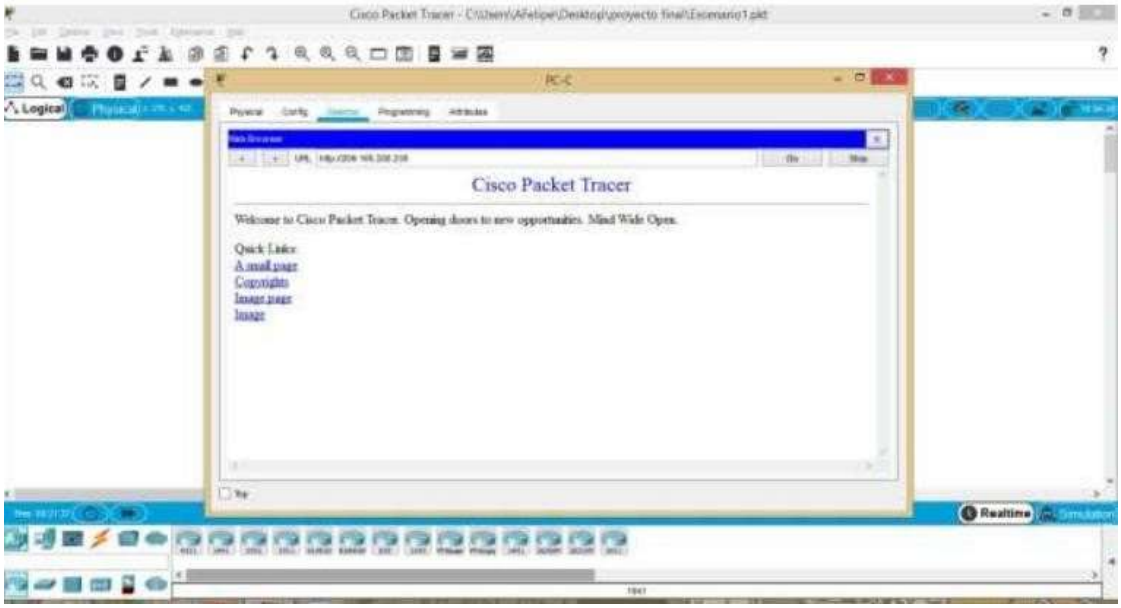


Figura 29. conexión internet desde PC-C utilizando la direccion IP del servidor de internet

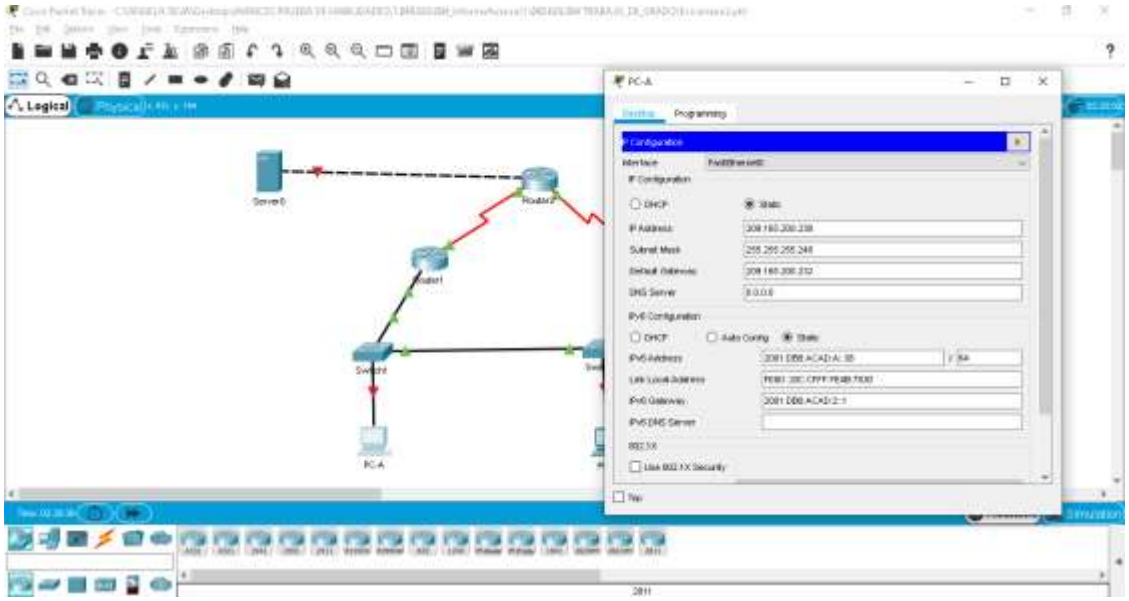


Figura 30 Verificación que la PC-A haya adquirido informacion de IP del servidor de DHCP

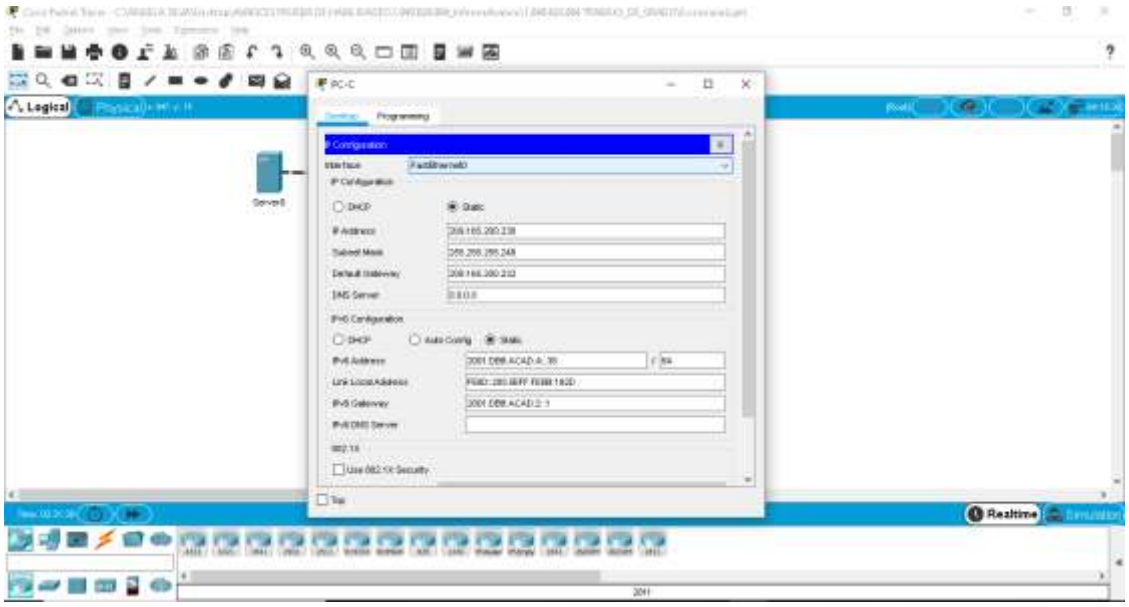


Figura 31 Verificación que la PC-C haya adquirido informacion de IP del servidor de DHCP

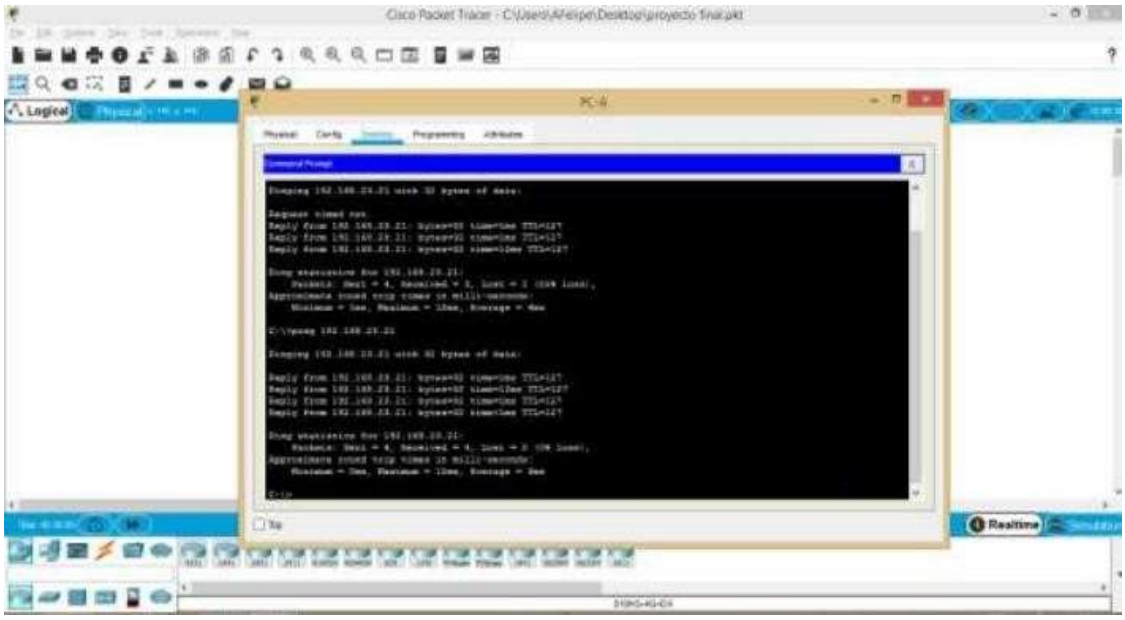


Figura 32 Verificar que la PC-A Pueda hacer ping a la PC-C

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2# clock set 9:00:00 5 marzo 2016.
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)# ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R2(config)#ntp server 172.16.1.0
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R2(config)#ntp update-calendar.
Verifique la configuración de NTP en R1.	R2#show ntp associations R2#show clock

Tabla 28. Configuración NTP

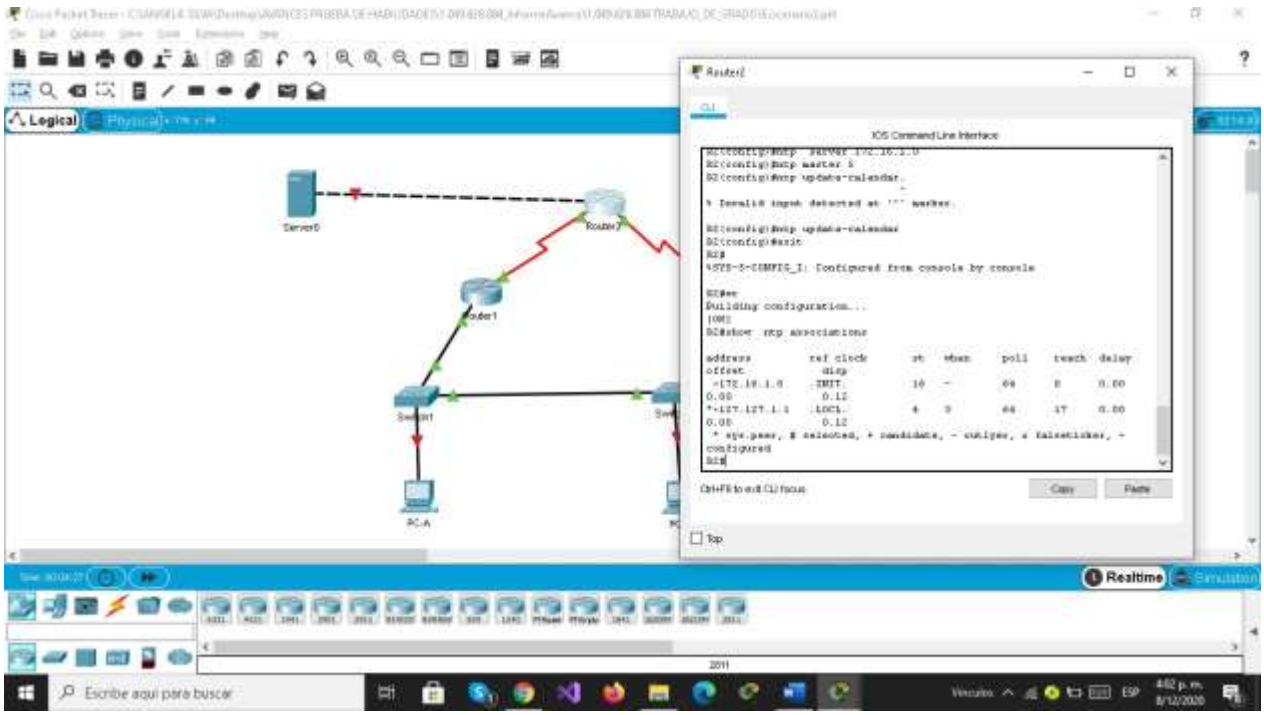


Figura 33. Verificación la configuración de NTP en R1.

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

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** R1(config)#ntp master 5 R1(config)#ip access-list standard ADMIN-MGT R1(config-std-nacl)#permit host 172.16.1.0 R1(config)#exit
Aplicar la ACL con nombre a las líneas VTY	R1(config)# line vty 0 4 R1(config-line)#access-class ADMIN-MGT in R1(config)#transport input telnet R1(config)# telnet 172.16.2.0

Permitir acceso por Telnet a las líneas de VTY	R1(config)# line vty 0 4 R1(config)#telnet 172.16.1.1
Verificar que la ACL funcione como se espera	R1#Show access-lists R1#show ip interface g0/0

Tabla 29. Restringir el acceso a las líneas VTY en el R2

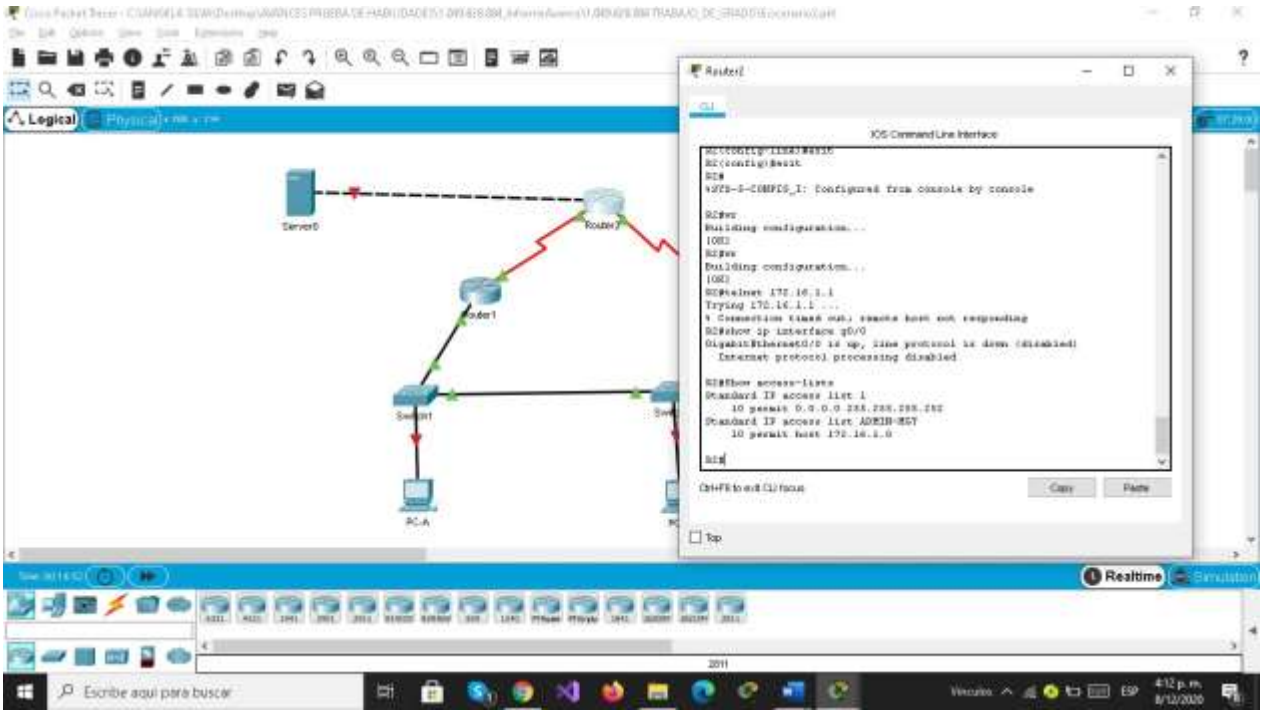


Figura 34 . Verificar que la ACL funcione como se espera

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

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show ip access-list Standard IP access list 1 21 permit 192.168.21.0 0.0.0.0.255 20 permit 192.168.23.0 0.0.0.0.255 99 permit 192.168.99 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1

Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters ^ % Invalid input detected at '^' marker. R2#clear ip ? bgp Clear BGP connections dhcp Delete items from the DHCP database nat Clear NAT ospf OSPF clear commands route Delete route table entries R2#clear ip
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2# show ip interface muestra la interfaz y las direccion
¿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. R2#show ip nat translations Pro Inside global Inside local Outside local Outside global.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

Tabla 30. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

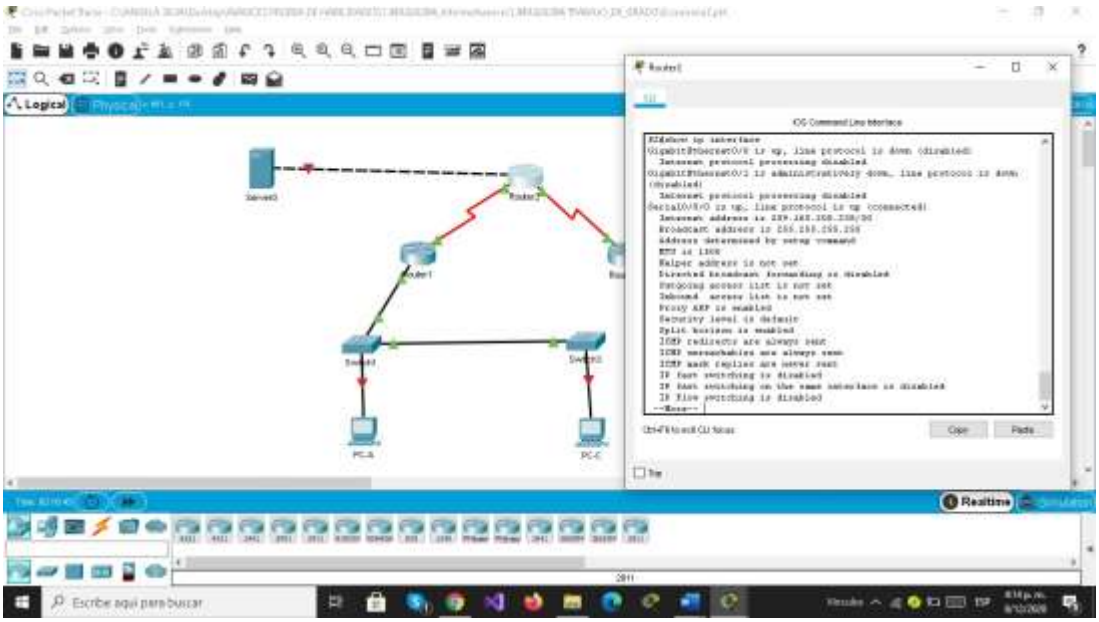


Figura 35. show ip interface

CONCLUSIONES

De acuerdo con los contenidos analizado por el primer escenario, podemos conceptualizar con claridad el termino de red, que no es más que un conjunto de equipos conectador por cables señales, ondas o cualquier otro método de transportes de datos, que comparte informacion, (archivos) y servicios como lo es acceso a internet .

El protocolo DHCP está diseñado fundamentalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP se encuentra activo en un servidor donde se centraliza la administración de las direcciones IP de la red.

Todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área. - Las listas de control de acceso desempeñan un gran papel como medida de seguridad lógica, ya que su cometido siempre es controlar el acceso a los recursos o activos del sistema.

Lograr que el estudiante reconozca el ámbito mediante este laboratorio se aplicaron concepto fundamentales estudiados en el módulo CCNA2 como lo es el protocolo de Routing dinamico, OSPFv3 para el caso de ipv4 respectivamente.

Hacer que el profesional aplique los conocimientos adquiridos a lo largo del curso de profundización Cisco CCNA I y II, y sobre todo relacionados con el protocolo de enrutamiento denominado OSPF, aplicado su configuracion básica a los dispositivos de red, configurando una prioridad de routers, desactivando las actualizaciones de enrutamiento en las interfaces adecuadas y verificando la conectividad entre los dispositivos de la topología.

Generar el uso de nuevas tecnologías con base en el caso de estudio entregado para su realización, se utilizó la herramienta de simulacion Cisco packet tracert, en el cual después de varios trabajos prácticos ya se logra contar con un mejor manejo y conocimiento como para montar una topología e interconectarlas de una manera más sencilla.

BIBLIOGRAFIA

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

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

ANEXOS

ANEXO1

https://drive.google.com/file/d/1yi3W_SFhBG1Ru0S2uVxi_IFP8SQUaxs/view?usp=sharing

PACKET TRECER ESCENARIO 2

Angela Roció Silva Alvarado

Universidad Nacional Abierta y A Distancia , anyelasilva99gmail.com

RESUMEN

Teniendo en cuenta el papel que se desempeña en la actualidad la tecnología en el desarrollo global de la economía a nivel mundial, hace que cada vez. Mas las organizaciones inviertan en una arquitectura tecnológica segura y robusta que le permita garantizar la seguridad, confiabilidad y disponibilidad de la informacion.

Es por ello que los escenarios de redes requieren un diseño basado en la implementación de protocolos de seguridad que garanticen una conectividad optima entre sus dispositivos.

Haciendo uso de las herramientas de simulacion PACKET TRECER, cisco. Se lleva a cabo la practica de los conocimientos adquiridos, mediante el desarrollo de dos escenarios, que plantea la configuracion de redes pequeñas, que deben permitir conectividad IPv4 A IPv6, Implementando configuraciones básicas de seguridad.

Abstract:

In this scientific article that was made with understanding the facility to understand about cisco. With which it is possible to design networks and carry out simulations on use. This free application is called packet thirteen and can be downloaded from the official cisco website. With this tool, all students, teachers, and professionals can test the operation of networks, cybersecurity and the internet of things. Packet trecer has an intuitive interface that facilitates its use when adding the different elements that make up the network. Being able to connect with each other and make very easy configurations. It offers us a great variety of functionalities, such as designing and building a network from scratch. Test new designs and red topologies. What packet thirteen gives us is something where the student can interact and perform network connectivity in real time.

Palabras clave: Vlan, Dns,ospf,ping

I. INTRODUCCIÓN

El objetivo del presente artículo es guiar a quienes se inician en la escritura científica, paso a paso en sus etapas, destacando los aspectos más relevantes.

La etapa final de una investigación es comunicar los resultados, de manera que éstos permitan integrar los conocimientos a la práctica profesional, es decir, se basa en los hallazgos de estudios científicos que deben tener validez, importancia, novedad y utilidad para el quehacer profesional.

Mediante el desarrollo del presente trabajo que busca afianzar los conocimientos adquiridos en el diplomado de profundización Cisco. A través de la configuracion de dos escenarios , el primero corresponde a una pequeña red, debe admitir tanto la conectividad IPv4 como IPV6 para los host soportados , el router y los switches deben administrarse de forma segura , realizandose configuracion de enrutamiento entre

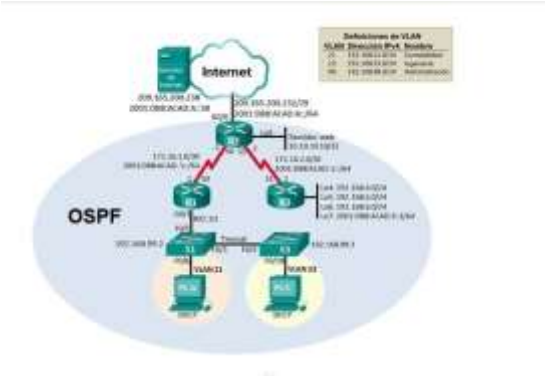
VLAN,DHCP. En el segundo escenario se implementa el protocolo de routing dinamico OSPF, el protocolo de configuracion de host dinamico , la traducción de direcciones de red dinámica y estatica (NAT) lista de control de acceso (ACL) y el protocolo de tiempo de red . teniendo en cuenta que uno de lo s factores primordiales en el diseño de una red es garantizar seguridad y disponibilidad , se hace necesario la configuracion adecuada de los dispositivos de red , a través de la implementación de protocolos seguros que permitan la comunicación necesaria, filtrando el trafico de red para optimizar los recursos.

II. METODOLOGÍA

Topología de red :

Con base en la topologia de red propuesta, se procede a realizar la configuracion física del primer escenario, en el cual corresponde a una red, en la que realiza la configuracion de los dispositivos; router, switches y dos Pc, los cuales deben admitir tanto la conectividad Ipv4 como Ipv6, igualmente, el router y los switches deben administrarse de forma segura, permite la configuración de enrutamiento entre vlan DHCP.

Figura1. Escenario 2



Configuracion de dispositivo :

Según los requerimientos del escenario 2, se procede a realizar la configuracion inicial de cada uno de los dispositivos como primer paso, borrar la configuracion de inicio del router y de los switches, asi como las vlan y se vuelve a cargar los dispositivos, verificando con el mensaje arrojado por los dispositivos que no tiene configuracion de inicio , posteriormente se realiza la configuracion de la verificación que admite ipv6 según sea necesario y se vuelven a cargar los switches . esta tarea se lleva a cabo mediante el uso de los comandos en la siguiente tabla:

Configuracion R1 :

Posteriormente a la inicialización de los dispositivos, se procede a realizar la configuraciones básicas de seguridad del router, que incluye las tareas descritas en la siguiente tabla.

Como primera medida se desactiva la búsqueda DNS, luego se asigna en el nombre del router en ese caso R1, se asigna nombre del dominio y se establece las contraseñas de acceso privilegiado, de consola con una longitud mínima de 10 catracteres sesión en la línea VTY se cifra la contraseña y se configura el mensaje de acceso prohibido no autorizado. 7

Posteriormente procedemos a habilitar el routing -ipv6 para enrutar paquete ipv6 entre las interfaces y sus interfaces desde el modo de configuracion global, habilitando el encapsulacion del trafico en cada una de ellas.

Figura 2. Tabla

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

Configuracio S1 y S3: Se realiza la configuracion básica de seguridad en los Switches , se asigna los nombres según la topologia (S1 y S3) se desactiva la búsqueda DNS, se asigna la contraseña de acceso privilegiado de consola y telnet , se crea el acceso no autorizado , se configura VTY solo aceptando la conexión segura , se configura la vlan, acorde con la tabla de direccionamiento IPv4 e IPv6 , se genera una clave de cifrado RSA , se configura la interfaz de administrador y se configura gateway predeterminado.

Figura 3. Configuracion S 1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)# host S1
Contraseña de exec privilegiado cifrada	Class S1(config)# enable secret class ok
Contraseña de acceso a la consola	Cisco S1#configure terminal S1(config)#line console 0 S1(config-line)# password cisco S1(config-line)#login S1(config-line)# exit ok
Contraseña de acceso Telnet	Cisco S1#configure terminal S1(config)#line vty 0 15 S1(config-line)# password cisco S1(config-line)#login S1(config-line)# exit ok

III. CONCLUSIONES

Siempre que se inicie la configuracion básica de los dispositivos de una red, es necesario realizar el borrado de configuracion inicial y el reinicio de los dispositivos con el objetivo de permitir una óptima configuracion de los mismos acordes al escenario planteado.

La implementación de la vlan permite optimizar el tráfico de la red y una mayor seguridad, dado que separan la red, lo cual disminuye la ocurrencia de ataques.

En el diseño de la topologia de red, es fundamental verificar el requerimiento de puertos seriales a utilizar en los routers, tipo de dispositivos a utilizar, cableado de red requerido y las comunicaciones permitidas y denegadas.

IV. REFERENCIAS

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

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

VI.