DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

YONATHAN GAMBIN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA ELECTRÓNICA

COLOMBIA

2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

YONATHAN GAMBIN

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

Presentado a:

MSc. Jose Ignacio Cardona

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA ELECTRÓNICA

COLOMBIA

2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá, 30 de noviembre de 2020 (30, 11, 2020)

Dedico este trabajo a mis queridos padres por todo su sacrificio y esfuerzo apoyándome todos estos años para poder salir adelante con mi carrera.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

ACL: Una lista de control de acceso o ACL (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores.

DHCP: Reduce en gran medida los errores que se producen cuando las direcciones IP se asignan de forma manual, y puede estirar las direcciones IP al limitar el tiempo que un dispositivo puede mantener una dirección IP individual.

DNS: La sigla DNS proviene de la expresión inglesa Domain Name System: es decir, Sistema de Nombres de Dominio. Se trata de un método de denominación empleado para nombrar a los dispositivos que se conectan a una red a través del IP (Internet Protocol o Protocolo de Internet).

LAN: Una red local es la interconexión de varios computadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de unos pocos kilómetros.

MÁSCARA DE SUBRED: La máscara de subred es particularmente necesaria al momento de señalar la dirección de red correspondiente a cada subred, y que es la que se encuentra referenciada en la tabla de enrutamiento.

OSPF: Open Shortest Path First (OSPF), camino más corto primero, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP),

PROTOCOLOS DE RED: Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red.

ROUTER: Dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras.

SWITCH: Dispositivo de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection).

RESUMEN

El desarrollo del presente trabajo consiste en la administración de dos redes utilizando el software cisco Packet Tracer. Inicialmente se diseña la topología de las redes; seguidamente, se configura la primera red para que admita la conectividad IPv4 e IPv6 para los hots soportados, el enrutamiento entre VLAN, DHCP, Etherchannel y port-security. La segunda red se configura el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), las listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. A medida que se realicen las configuraciones se verificaran que las conexiones y la comunicación entre los dispositivos.

Palabras clave: Administración, Enrutamiento, Protocolos, Red.

ABSTRACT

The development of this work consists of the administration of two networks using the Cisco Packet Tracer software. Initially, the network topology is designed; then the first network is configured to support IPv4 and IPv6 connectivity for supported hots, inter-VLAN routing, DHCP, Etherchannel, and port-security. The second network is configured with the OSPF dynamic routing protocol, the dynamic host configuration protocol (DHCP), the static and dynamic network address translation (NAT), the access control lists (ACL) and the time protocol network (NTP) server / client. As the configurations are made, the connections and communication between the devices will be verified.

Keywords: Administration, Routing, Protocols, Network.

INTRODUCCIÓN

Este proyecto tendrá como objetivo la administración de dos redes, por medio del programa de Cisco Packet Tracer. Inicialmente se identificarán las prácticas o los laboratorios. Se realizará una revisión bibliográfica sobre los protocolos de red para el desarrollo de cada uno de estos. se realizará el desarrollo de cada topología, con las configuraciones de los dispositivos y la verificación de las mismas.

Para esto se redactará el respectivo informe de laboratorio que contarán con el procedimiento que nos permitirá realizar los dos escenarios, permitiendo así que el estudiante tenga el conocimiento y pueda ponerlo en práctica.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Configurar dos redes LAN por medio de la herramienta de simulación cisco packet tracer

2.2 OBJETIVOS ESPECÍFICOS

- Investigar sobre los protocolos de enrutamiento y comandos.
- Realizar y configurar las topologías de las redes a administrar.
- Validar los resultados mediante los comandos necesarios.

3. DESARROLLO DEL PROYECTO

3.1 ESCENARIO 1

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

Topología

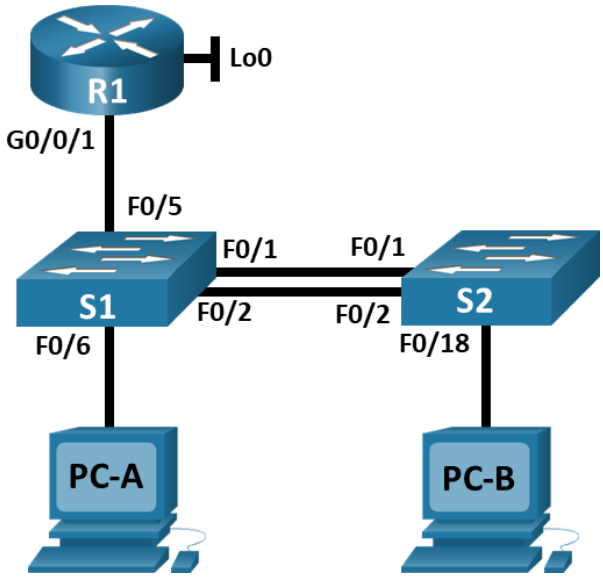


Figura 1 Topología del primer escenario

Para realizar la topología de la red, tal como se muestra en la Figura 1, inicialmente agregamos a la pantalla principal del programa un router 2901 y agregamos dos switch 2960 y dos PC's, estos dispositivos se conectan puertos seriales, como podemos observar en la topología de la red.

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

Tabla 1. Asignación de las VLAN a crear en el desarrollo del primer escenario

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

Tabla 2 Asignación de Direcciones en los dispositivos del primer escenario

PARTE 1: INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BÁSICOS DE LOS DISPOSITIVOS

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

Es importante borrar las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos, por medio de la ejecución de los siguientes comandos tal como se muestra para cada uno de los dispositivos de la red que tenemos en la figura 1.

R1

Router>enable
Router#erase
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete

Router#

Router#reload

Proceed with reload? [confirm]

S1

Switch>enable
Switch#erase sta
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete

Switch#

Switch#reload

Proceed with reload? [confirm]

S2

Switch>enable
Switch#erase sta
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete

Switch#

Switch#reload

Proceed with reload? [confirm]

Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Paso 1: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes líneas de comandos y además se crean las subinterfaces, encapsulándolas con su VLAN y asignando los direccionamientos IPv4 e IPv6, además se genera una clave de cifrado RSA, se configuran las medidas de seguridad, así como la transferencia de autenticación por medio de SSH.

Tarea	Especificación
Desactivar la búsqueda DNS	Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin privilege 15 secret admin1pass

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #El acceso no autorizado está prohibido#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1(config)#interface gi0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description LAN to VLAN2 R1(config-subif)#ip add 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shutdown R1(config-if)#no shutdown R1(config-subif)#exit
	R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#ip add 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#description LAN to VLAN3 R1(config-subif)#no shutdown R1(config-subif)#exit
	R1(config)#interface gi0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#ip add 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64

	R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#description LAN to VLAN4 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gi0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#exit
	R1(config)#interface gi0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	R1(config)#interface lo0 R1(config-if)#description LAN to Loopback0 R1(config-if)#ip add 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 add 2001:db8:acad:209::1/64 R1(config-if)#ipv6 add FE80::1 link-local R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa

Tabla 3 Configuraciones básicas en R1 del primer escenario con su respectivo comando

Paso 2: Configure S1 y S2.

Las tareas de configuración incluyen las siguientes líneas de comandos y además se crean las subinterfaces, encapsulándolas con su VLAN y asignando los direccionamientos IPv4 e IPv6, además se genera una clave de cifrado RSA, se configuran las medidas de seguridad, así como la transferencia de autenticación por medio de SSH.

Tarea	Especificación
Desactivar la búsqueda DNS.	S1(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass

Contraseña de acceso a la consola	S1(config)#line con 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)# banner motd #El acceso no autorizado esta prohibido#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 4 S1(config-if)#ip add 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 add 2001:db8:acad:c::98/64 S1(config-if)#ipv6 add fe80::98 link-local S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97

Tabla 4 Configuraciones básicas en S1 con su respectivo comando

Configuración S2.

Tarea	Especificación
Desactivar la búsqueda DNS.	S2(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1

Nombre de dominio	S2(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S2(config)#line con 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S2(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#username admin privilege 15 secret admin1pass S2(config)#line vty 0 15 S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)#line vty 0 15 S2(config-line)#login local S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd #El acceso no autorizado está prohibido#
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S2(config)#interface vlan 4 S2(config-if)#ip add 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 add 2001:db8:acad:c::99/64 S2(config-if)#ipv6 add fe80::99 link-local S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97

Tabla 5 Configuraciones básicas en S2 con su respectivo comando

Realizar las configuraciones anteriores es importante por ello son básicas y siempre se realizan al inicio de administrar cualquier red y configurar los dispositivos que pertenezcan a esta.

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

Paso 1: Configurar S1

La configuración del S1 que se realiza para configurar la infraestructura de la red, incluye crear las VLAN y al mismo tiempo asignarle un nombre para luego ingresar a las interfaces y configurarlas en modo trunk para que su acceso y comunicación por medio de la VLAN nativa 6 para las interfaces fa0/1, fa0/2 y fa0/5, luego procedemos a crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, Configuramos el puerto de acceso de host para VLAN 2, luego hay que configurar la seguridad del puerto en los puertos de acceso que sería la interface fa0/6 y por ultimo hay que proteger todas las interfaces no utilizadas.

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1#configure terminal S1(config)#interface fa0/1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1#configure terminal S1(config)#interface fa0/2 S1(config-if)#switchport trunk encapsulation dot1q

	S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 2 mode active S1(config)#exit S1(config#interface port-channel 2 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	S1(config)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shutdown S1(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso	S1(config)#interface fa0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	S1(config)#interface range fa0/3-4, fa0/7-24, gi0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#shutdown

Tabla 6 Configuración de la infraestructura (vlan, trunking, etherchannel) de red en S1 con su respectivo comando

Paso 2: Configure el S2

Entre las tareas de configuración de S2 se incluyen las mismas configuraciones que se describieron anteriormente.

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#interface range fa0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#interface port-channel 2 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit S2(config)#interface range fa0/1-2 channel-group 2 mode passive S2(config-if-range)#no shutdown S2(config)#interface port-channel 2 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit S2(config)#interface range fa0/1-2 channel-group 2 mode passive S2(config-if-range)#no shutdown

Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit
Configure port-security en los access ports	S2(config)#interface fa0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	S2(config)#interface range fa0/3-17, fa0/19-24, gi0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Puertos no utilizados S2(config-if-range)#shutdown

Tabla 7 Configuración de la infraestructura (vlan, trunking, etherchannel) de red en S2 con su respectivo comando

PARTE 3: CONFIGURAR SOPORTE DE HOST

Paso 1: Configure R1

Para realizar esta tercera parte de configurar el soporte de host en el router R1, como se le llamo en esta red, hay que primero ingresar la dirección ip route por defecto y así luego comenzar a configurar el protocolo DHCP que es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red, ya que una dirección IP es un número que identifica de forma única a un ordenador en la red y en este caso realizamos una configuración para que este proceso se haga automáticamente y no manualmente por medio de los siguientes que comandos.

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 lo0
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp pool vlan 2 R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.10 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-a.net R1(config)#default-router 10.19.8.1

Configurar DHCP IPv4 para VLAN 3	R1(config)#ip dhcp pool vlan 3 R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.10 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-b.net R1(config)#default-router 10.19.8.65

Tabla 8 Configuración del soporte de host en R1

Paso 4: Configurar los servidores

En este paso se configuran los equipos host PC-A y PC-B para que utilicen el protocolo DHCP para IPv4 y que se asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, se registrarán las configuraciones de red del host con el comando **ipconfig /all** en cada host de la red.

PC-A Network Configuration	
Descripción	CCNA-a.net
Dirección física	0000.0c89.3578
Dirección IP	10.19.8.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Tabla 9 Configuración del servidor PC-A

Configuración de red de PC-B	
Descripción	en blanco
Dirección física	00D0.BCDC.3ADB
Dirección IP	169.254.58.219
Máscara de subred	255.255.0.0
Gateway predeterminado	0.0.0.0
Gateway predeterminado IPv6	FE80::1

Tabla 10 Configuración del servidor PC-B

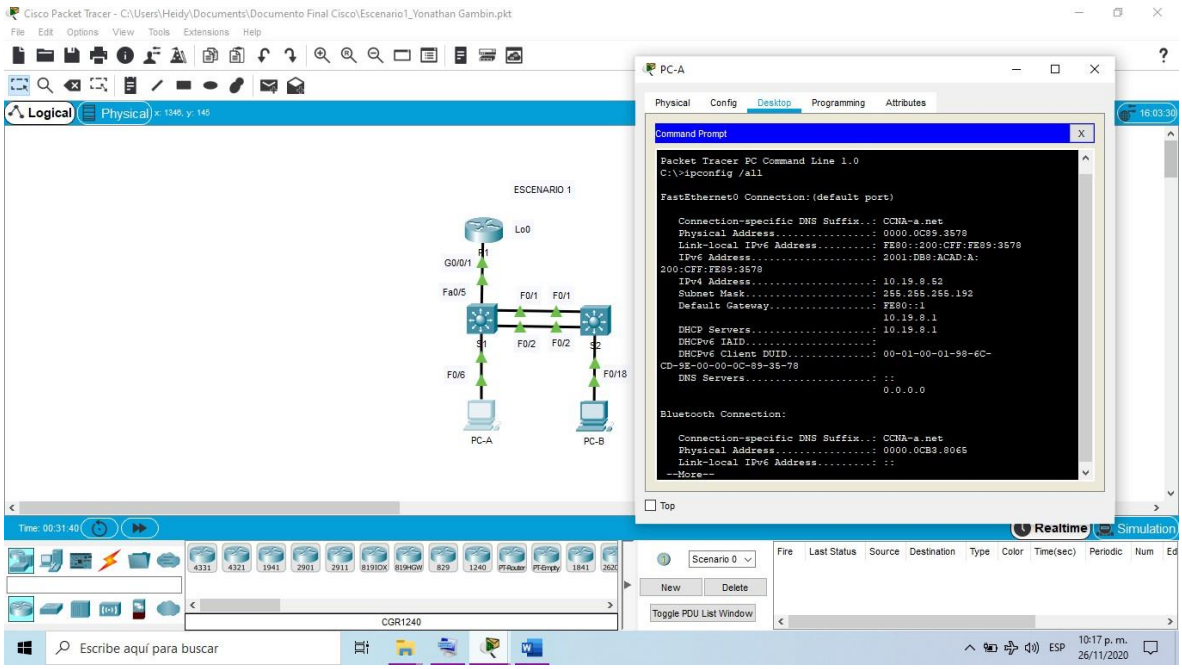


Figura 2 Verificación de la configuración de red de PC-A

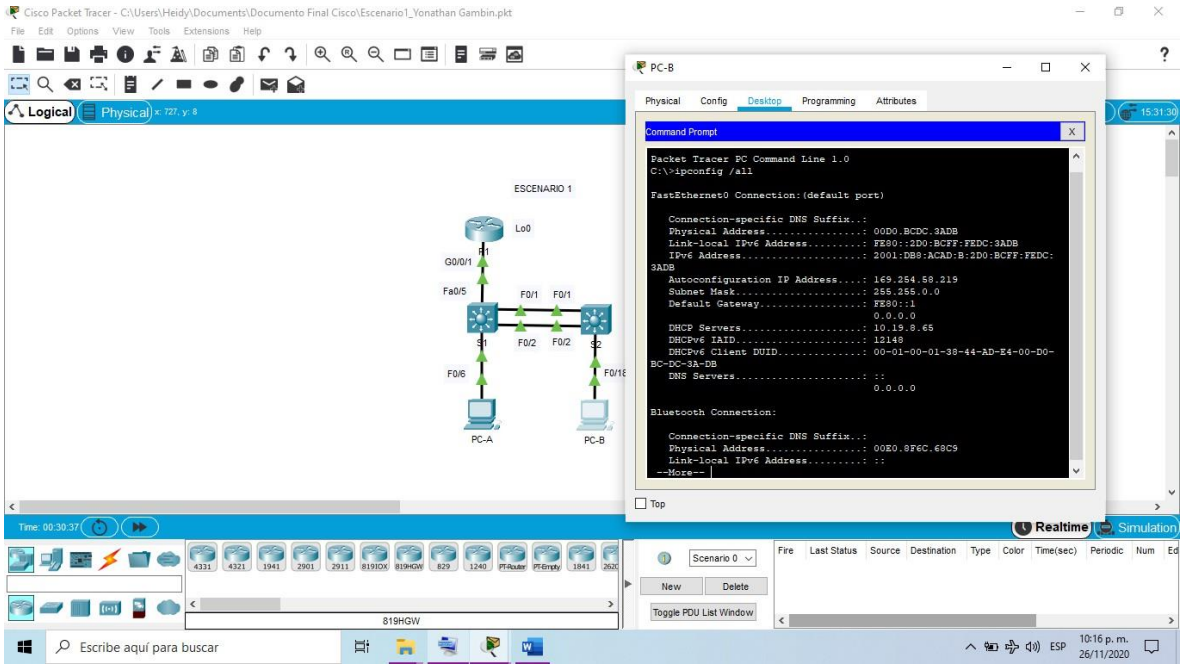


Figura 3 Verificación de la configuración de red de PC-B

En las imágenes anteriores se observa cómo después de realizar las configuraciones del protocoló DHCP podemos ingresar a la ventana CLI de cada host y por medio del comando ipconfig /all identificar la dirección IPv4 e IPv6 que se genero a automáticamente.

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. 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	Reply from 10.19.8.1: bytes=32 time=3ms TL=255 (Ver figura 4)
	R1, G0/0/1.2	IPv6	2001:db8:acad:a: :1	Reply from 2001:db8:acad:a::1: bytes=32 time=1ms TL=255 (Ver figura 4)
	R1, G0/0/1.3	Dirección	10.19.8.65	Reply from 10.19.8.65:bytes=32 time=3ms TL=255 (Ver figura 5)
	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	Reply from 2001:DB8:ACAD:B::1: bytes=32 time=1ms TTL=255 (Ver figura 5)
	R1, G0/0/1.4	Dirección	10.19.8.97	Reply from 10.19.8.97: bytes=32 time=1ms TTL=255 (Ver figura 6)
	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 (Ver figura 6)
	S1, VLAN 4	Dirección	10.19.8.98	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 7)
	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	Request timed out. (Ver figura 7)
	S2, VLAN 4	Dirección	10.19.8.99	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254

				(Ver figura 8)
	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 8)
PC-A	PC-B	Dirección	169.254.58.219.	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 9)
	PC-B	IPv6	2001:db8:acad:b: :50	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 9)
	R1 Bucle 0	Dirección	209.165.201.1	Reply from 209.165.201.1: bytes=32 time=6ms TTL=255 (Ver figura 10)
	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 (Ver figura 10)
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 11)
	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	Reply from 2001:DB8:ACAD:209::1: bytes=32 time=12ms TTL=255 (Ver figura 11)
	R1, G0/0/1.2	Dirección	10.19.8.1	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 12)
	R1, G0/0/1.2	IPv6	2001:db8:acad:a: :1	Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 (Ver figura 12)
	R1, G0/0/1.3	Dirección	10.19.8.65	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 13)
	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 (Ver figura 13)
	R1, G0/0/1.4	Dirección	10.19.8.97	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 14)
	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 (Ver figura 14)

	S1, VLAN 4	Dirección	10.19.8.98	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 15)
	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 15)
	S2, VLAN 4	Dirección	10.19.8.99	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 16)
	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 16)

Por medio de las siguientes imágenes podemos observar que la conexión es satisfactoria y todo esto solo ingresando el comando ping seguido de la dirección IP con la que queremos hacer comunicación.

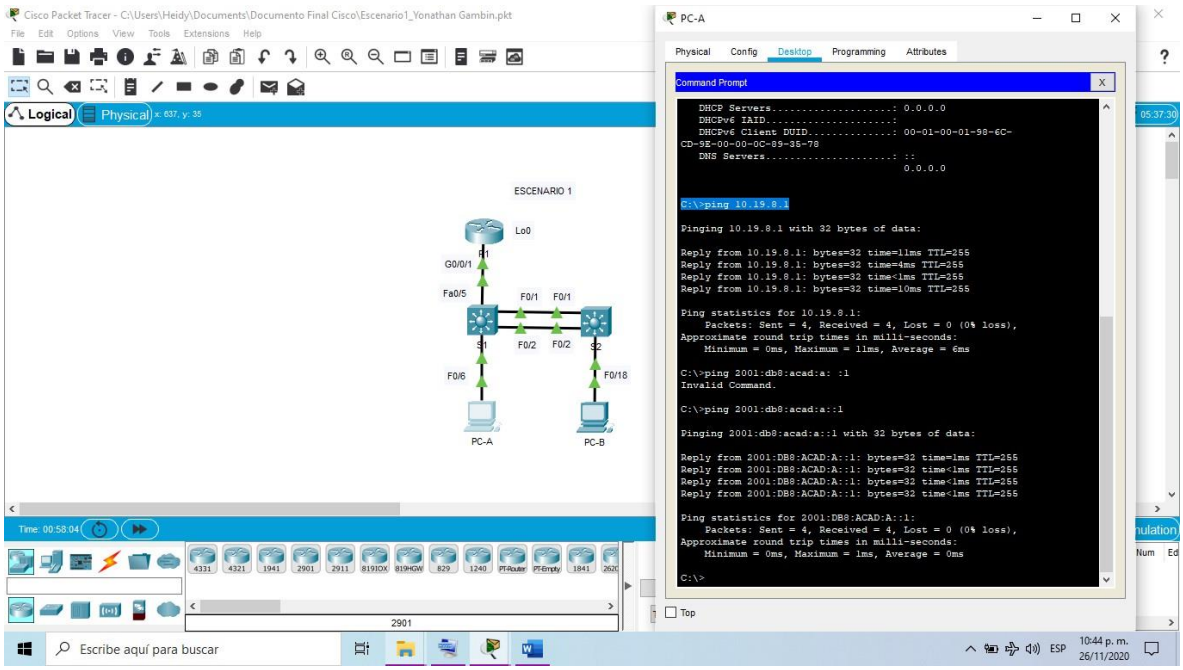


Figura 4 Verificación de conectividad en PC-A a R1 G0/0/1.2

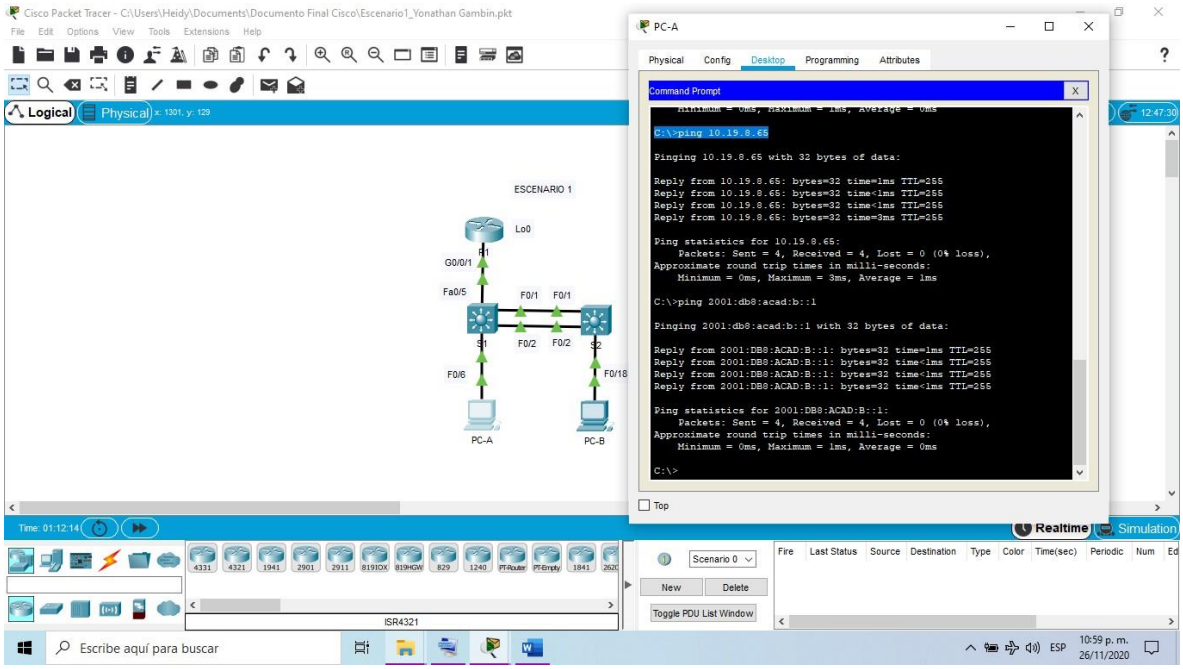


Figura 5 Verificación de conectividad en PC-A a R1 G0/0/1.3

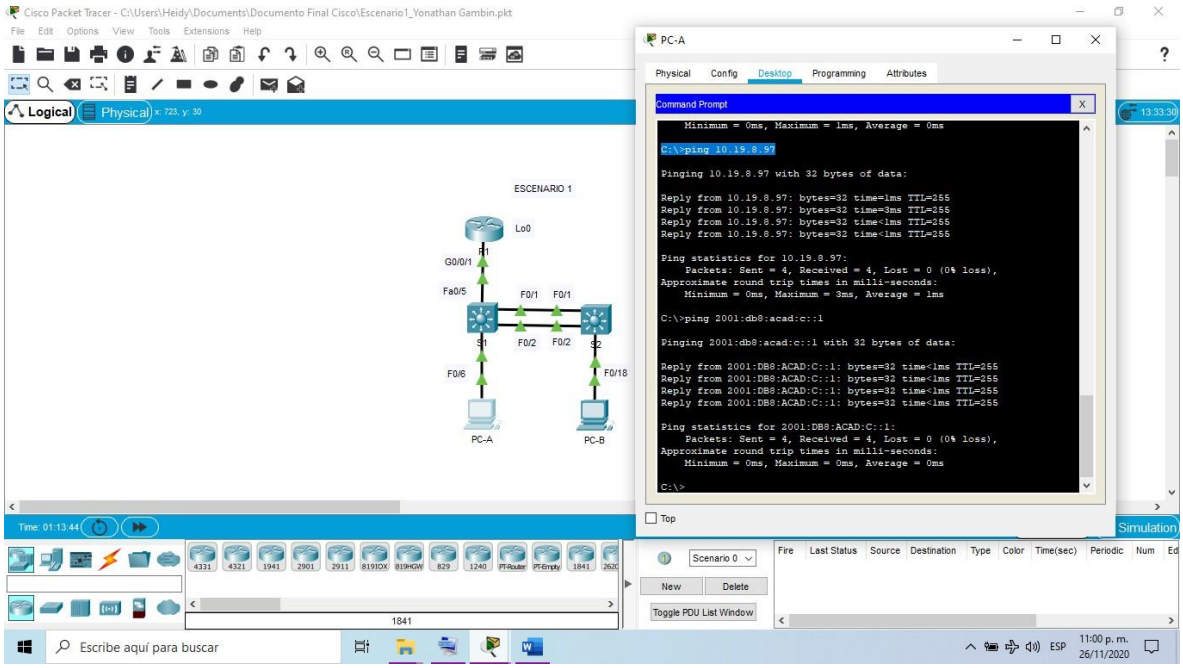


Figura 6 Verificación de conectividad en PC-A a R1 G0/0/1.4

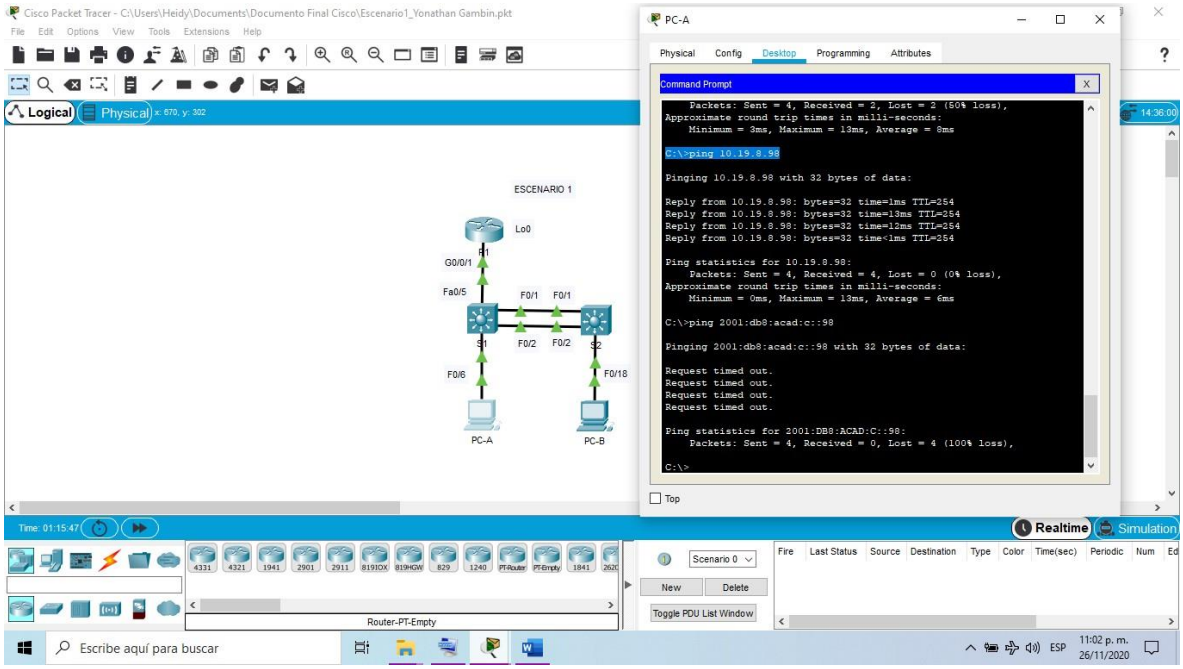


Figura 7 Verificación de conectividad en PC-A a S1 VLAN 4

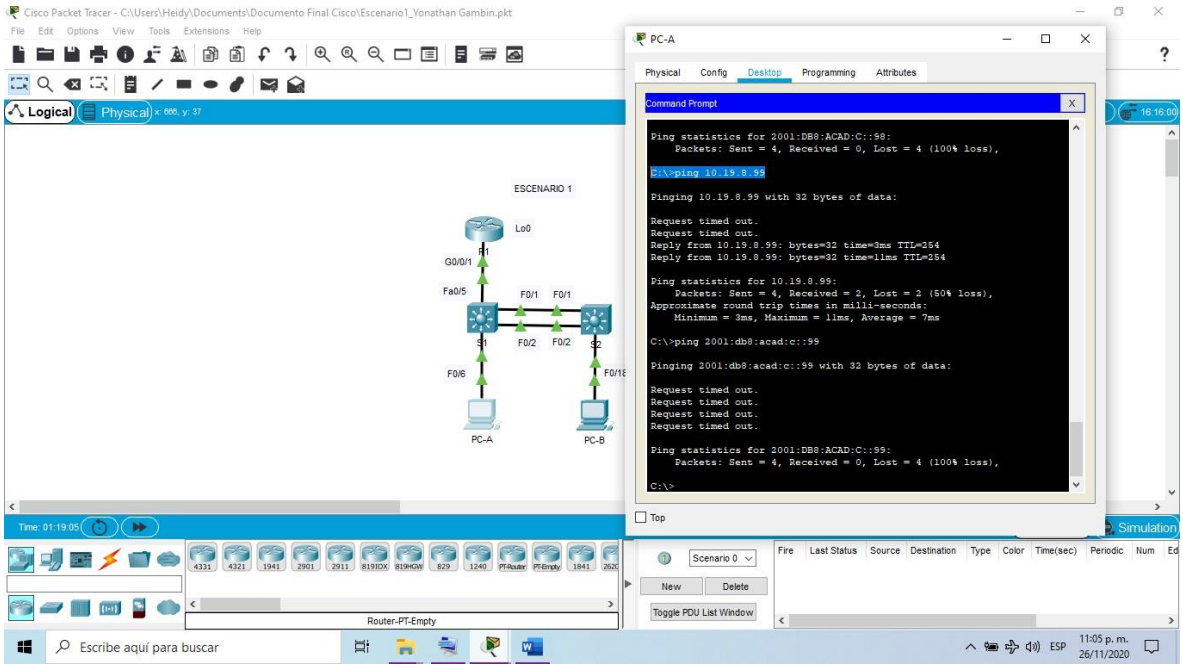


Figura 8 Verificación de conectividad en PC-A a S2 VLAN 4

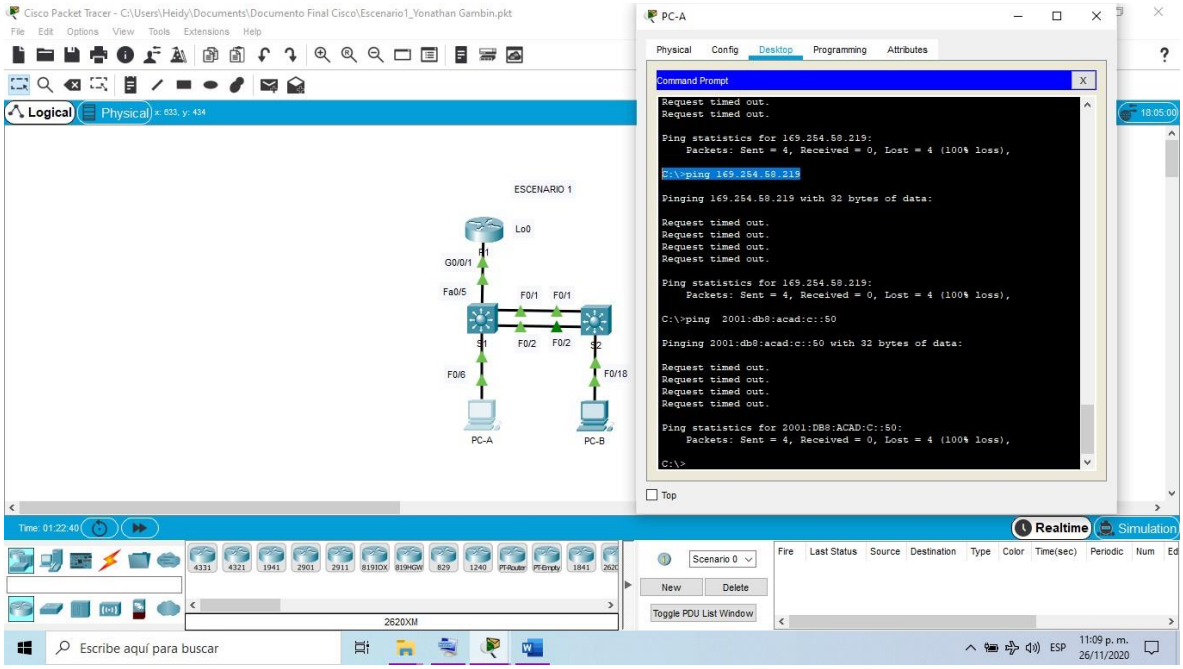


Figura 9 Verificación de conectividad en PC-A a PC-B

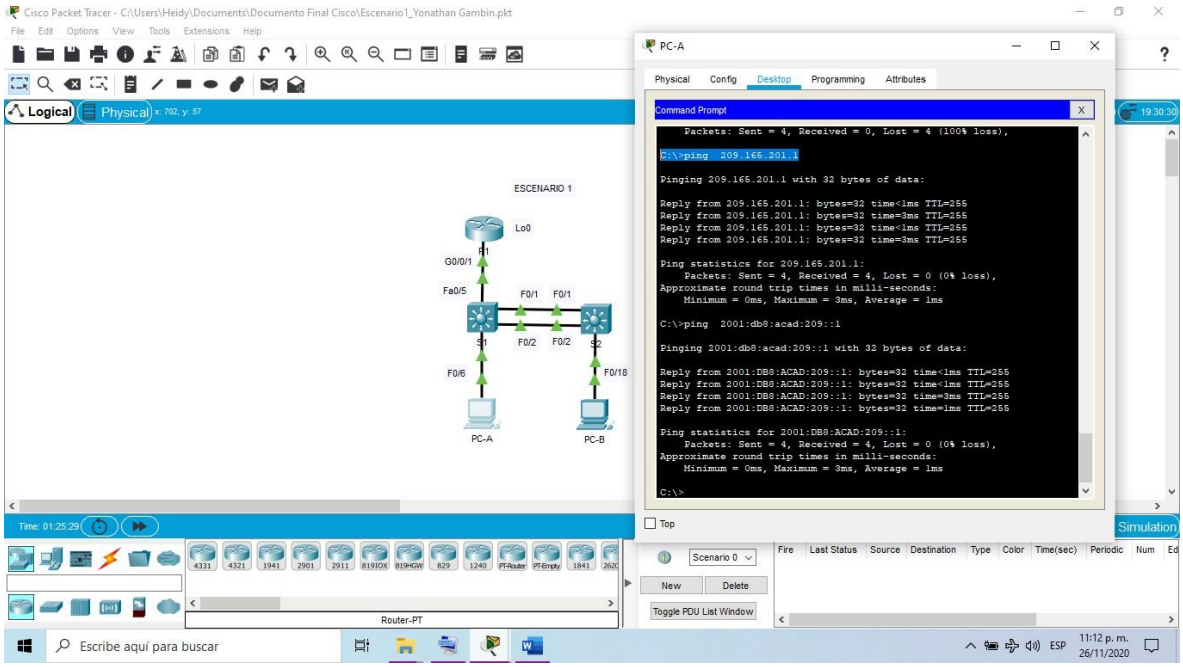


Figura 10 Verificación de conectividad en PC-A a R1 bucle 0

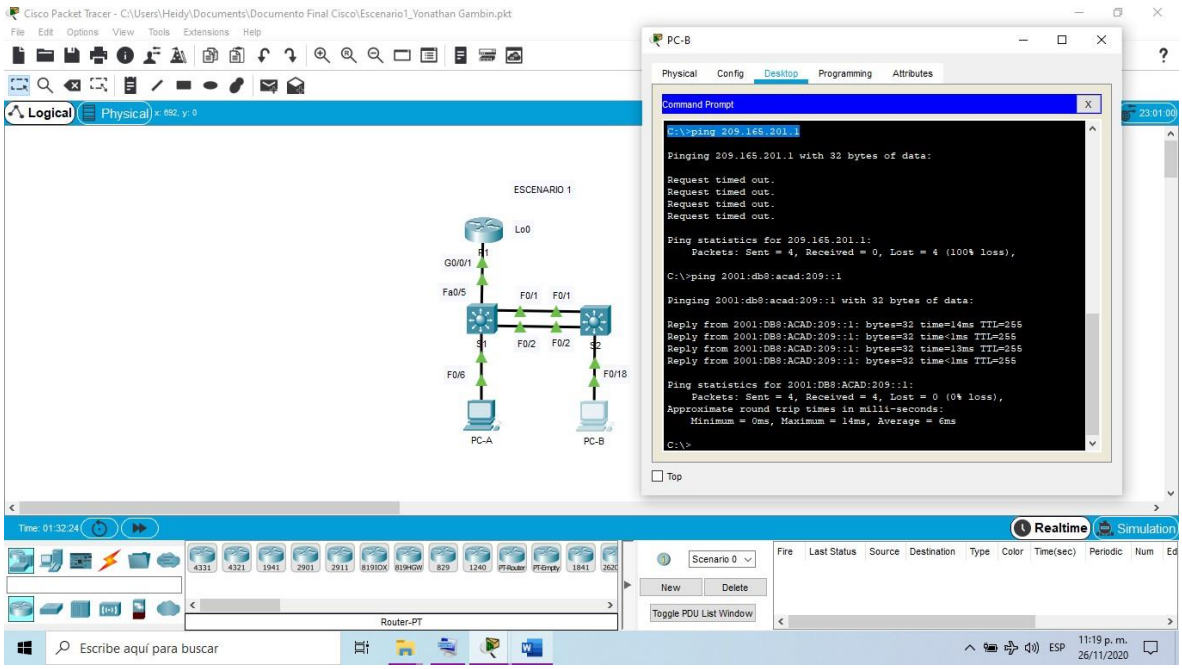


Figura 11 Verificación de conectividad en PC-B a R1 bucle 0

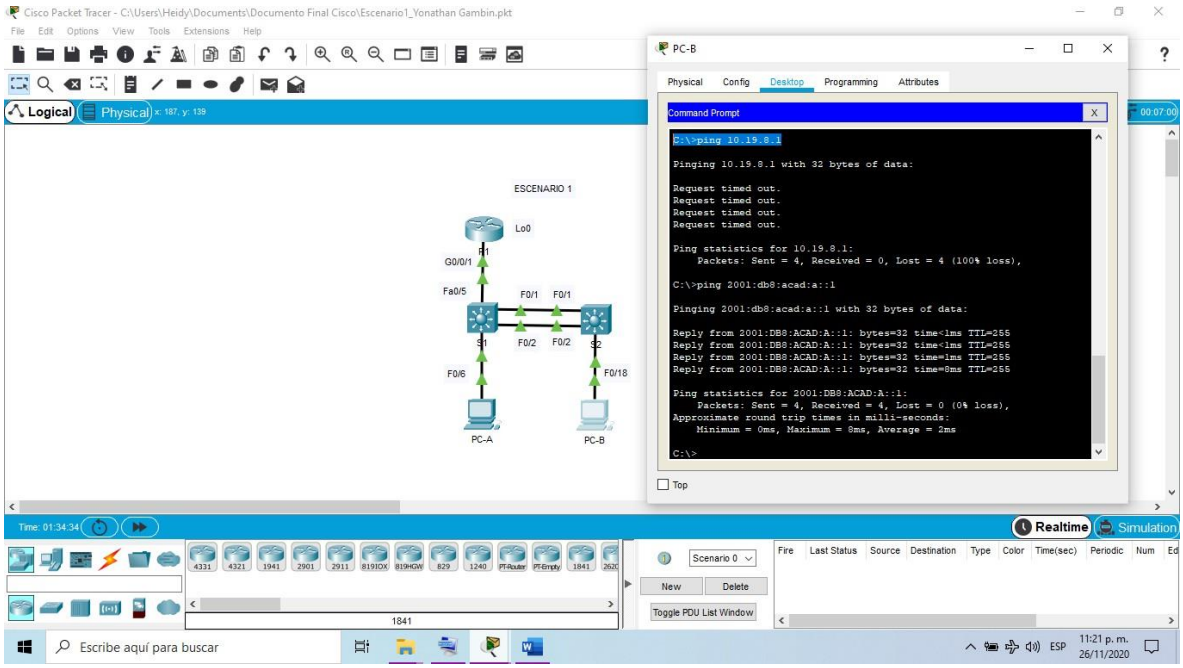


Figura 12 Verificación de conectividad en PC-B a R1 G0/0/1.2

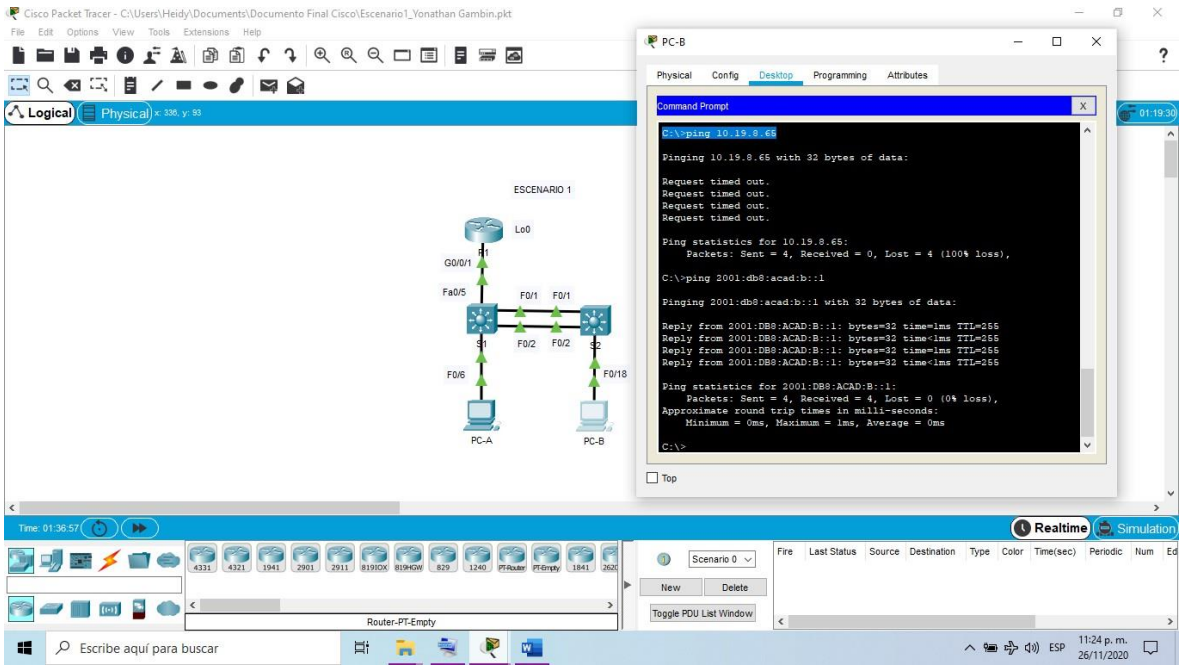


Figura 13 Verificación de conectividad en PC-B a R1 G0/0/1.3

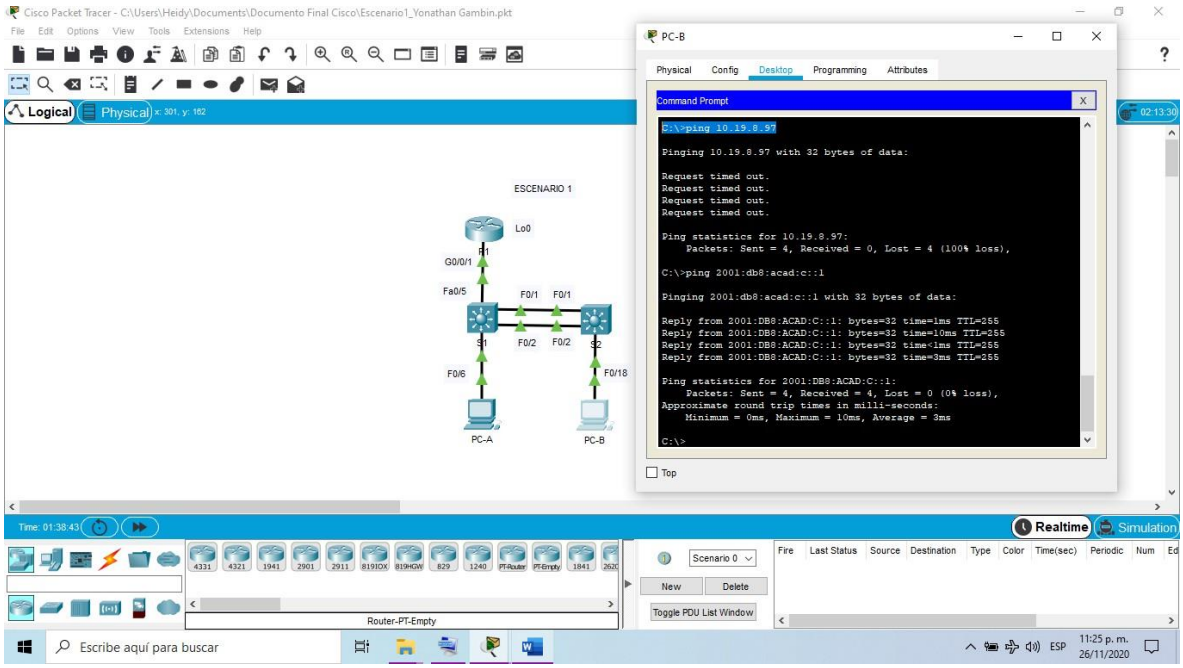


Figura 14 Verificación de conectividad en PC-B a R1 G0/0/1.4

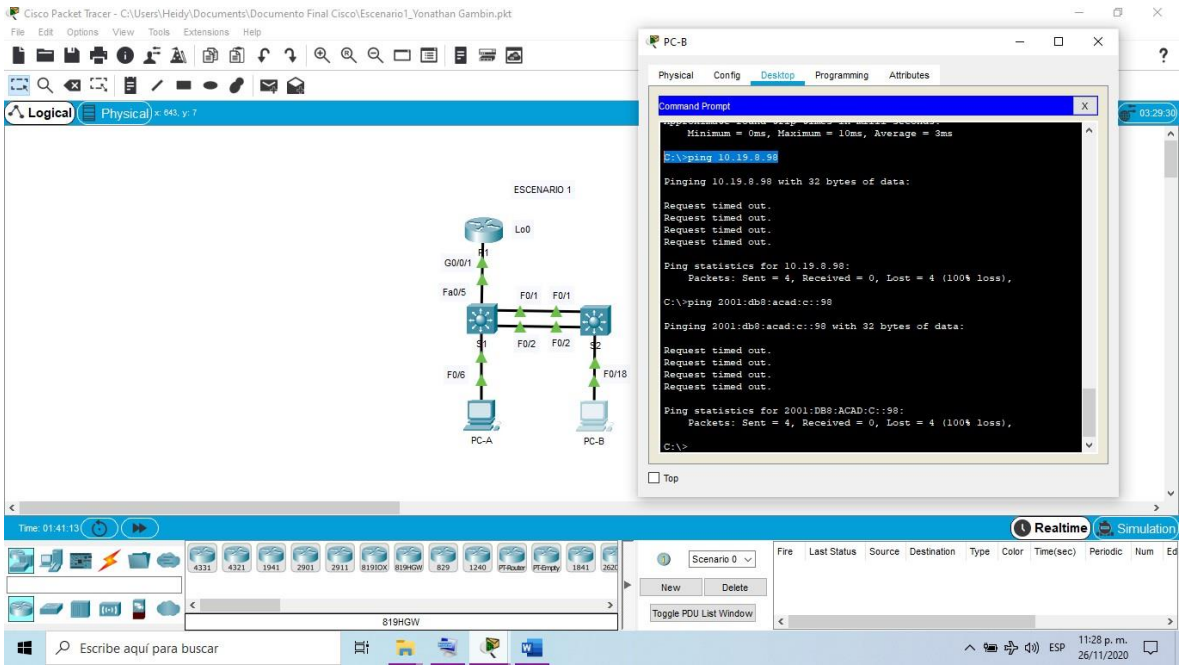


Figura 15 Verificación de conectividad en PC-B a S1 VLAN 4

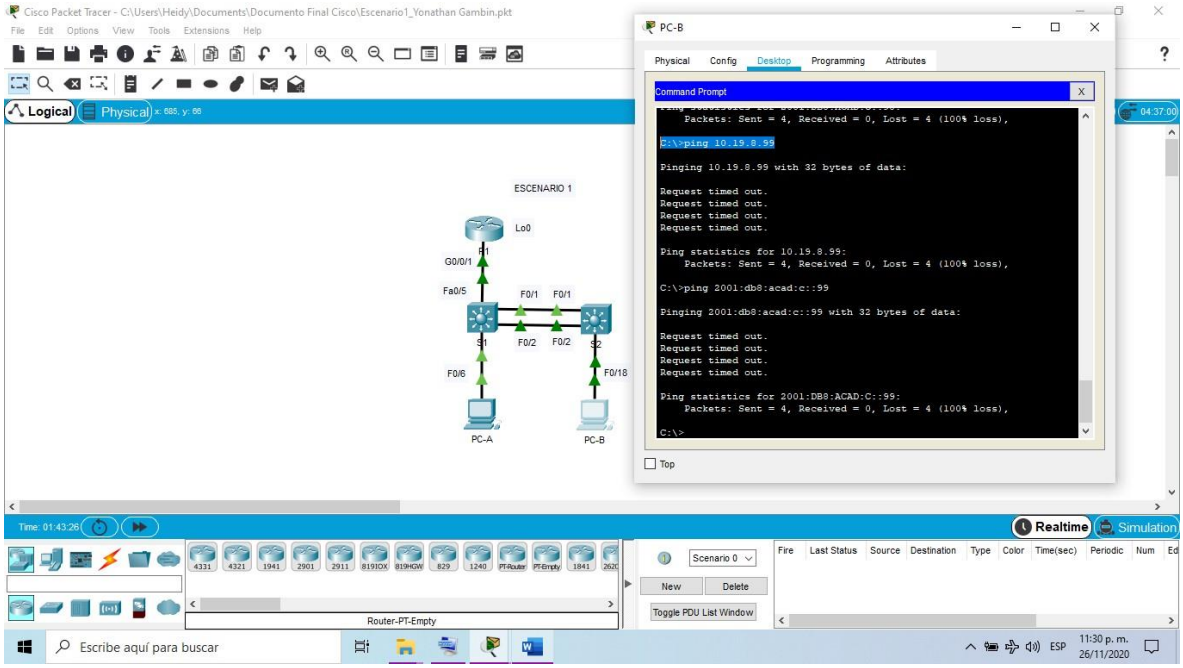


Figura 16 Verificación de conectividad en PC-B a S2 VLAN 4

3.2 ESCENARIO 2

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

Topología

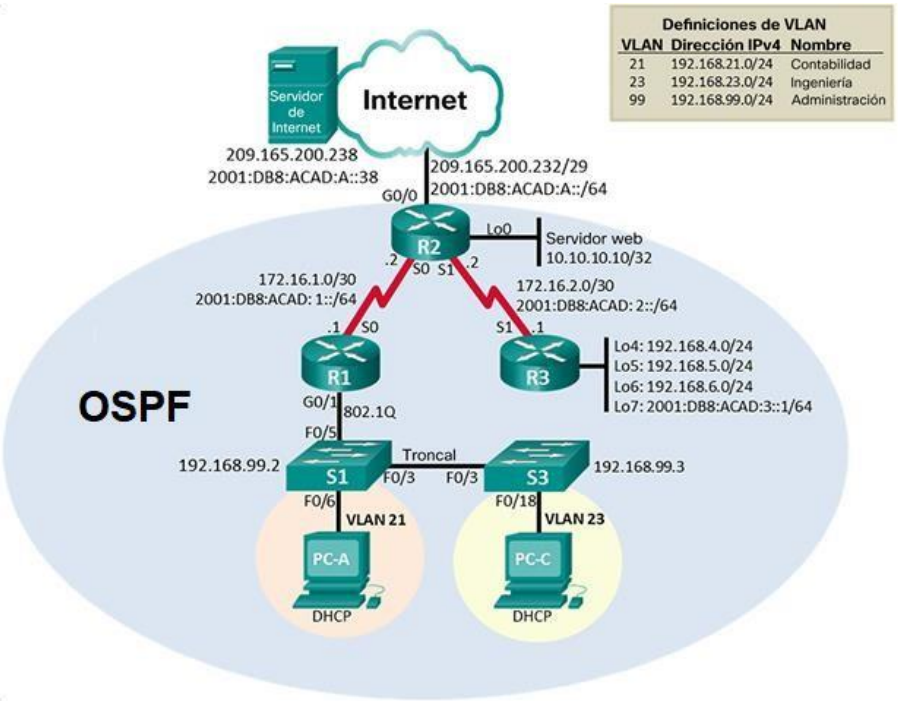


Figura 17 Topología del segundo escenario

Para realizar la topología de la red, tal como se muestra en la Figura 17, inicialmente agregamos a la pantalla principal del programa tres router 2901 y agregamos los módulos HWIC-2T y HWIC-4ESW a cada router para poder hacer comunicación entre ellos. Para ello primero debemos apagar cada router, luego agregar los módulos y volver a encender los router, por último, se conectan los dispositivos por los puertos serial s0/3/0 y s0/3/1, como podemos observar en la topología de la red.

PARTE 1: INICIALIZAR DISPOSITIVOS

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

Hay que eliminar las configuraciones de inicio y volver a cargar los dispositivos. Por ello se realizan las configuraciones de formateo y reinicio tanto en los Routers como en los Switch tal como aparecen en la tabla 11.

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

Tabla 11 Verificación inicial de las configuraciones de los dispositivos del segundo escenario

PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

Paso 1: Configurar la computadora de Internet

Configurar la computadora de internet que se observa en la topología con las direcciones IPv4 e IPv6 que aparecen en la tabla 12, además de configurar también la mascara de subred y la puerta de enlace.

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 12 Indicaciones para configurar la computadora red internet

Paso 2: Configurar R1

Las configuraciones básicas son importantes primero porque mediante la asignación de un nombre por medio del comando hostname nuestros dispositivos se podrán identificar en este caso le colocamos R1 a este dispositivo y no se cometerán erros además en estas configuraciones se establecen las contraseñas que son la principal defensa contra el acceso no autorizado a los dispositivos de red. Cada dispositivo debe tener contraseñas configuradas a nivel local para limitar el acceso y desde el inicio tener una red segura.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login

Cifrar las contraseñas de texto no cifrado	R1(config)n#service password-encryption
Mensaje MOTD	R1(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/0	R1(config)#interface s0/3/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config)#interface s0/3/0 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 serial s0/3/0 R1(config)#ipv6 route ::/0 serial s0/3/0

Tabla 13 Configuraciones básicas de R1 en el segundo escenario

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

Se lleva a cabo la misma configuración anterior le asignamos un nombre por medio del comando hostname y para este dispositivo será R2 se establecen las contraseñas que son la principal defensa contra el acceso no autorizado a los dispositivos de red y la respectiva asignación de las direcciones IP que vienen en la figura 17 para las interfaces según corresponda.

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	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#password cisco
Contraseña de acceso Telnet	R2(config)#password cisco

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)#interface s0/3/0 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config)#interface s0/3/0 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
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 12800 R2(config-if)#no shutdown R2(config)#interface s0/3/1 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#interface g0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#no shutdown R2(config)#interface g0/0 R2(config-if)#ipv6 address 2001:DB8:ACAD:/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no shutdown
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Tabla 14 Configuraciones básicas en R1 del segundo escenario con su respectivo comando

Paso 4: Configurar R3

La configuración del R3 es la misma que se realice en los dispositivos anteriores R1 y R2, pero con diferente configuración de las direcciones IP, ya que estas se realizan según la topología de la red de la figura 17.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R3(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#password cisco
Contraseña de acceso Telnet	R3(config)#password cisco
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 s0/3/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#clock rate 128000 R3(config-if)#no shutdown R3(config)#interface s0/3/1 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 192.168.4.0 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.0 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.0 255.255.255.0

	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

Tabla 15 Configuraciones básicas de R3 en el segundo escenario con su respectivo comando

Paso 5: Configurar S1

Primero hay que cambiar el nombre de usuario, primero nos aparecerá switch>, por lo que colocamos el comando enable para cambiar de usuario en modo normal a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado switch#. Y de esta forma entramos al modo de configuraciones con el comando configure terminal, continuamos escribiendo los comandos tal como se muestran en la tabla 16.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S1(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#password cisco
Contraseña de acceso Telnet	S1(config)#password cisco
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd $Se prohibe el acceso no autorizado$

Tabla 16 Configuraciones básicas de S1 en el segundo escenario con su respectivo comando

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas que son iguales a las configuraciones realizadas en el dispositivo anterior S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S3(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#password cisco
Contraseña de acceso Telnet	S3(config)#password cisco
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd $Se prohibe el acceso no autorizado$

Tabla 17 Configuraciones básicas de S3 en el segundo escenario con su respectivo comando

Paso 7: Verificar la conectividad de la red

Realizar este paso de verificar la conectividad de la red, se realiza ingresando el comando **ping** en la ventana CLI sin entrar en el modo de configuración del dispositivo.

Hay que tener en cuenta que si queremos establecer conectividad y esta falla hay que revisar por medio del comando show run, un comando que nos permite visualizar todas las configuraciones realizadas en los dispositivos e identificar la falla y corregirla.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2 Success rate is 100 percent(5/5), round-trip min/avg/max = 1/9/38 ms (Ver figura 18)
R2	R3, S0/0/1	172.16.2.1	R2#ping 172.16.2.1 Success rate is 100 percent(5/5) round-trip min/avg/max = 1/2/8 ms (Ver figura 19)
PC de Internet	Gateway predeterminado	209.165.200.232	>ping 209.165.200.232

			Reply from 209.165.200.232: bytes=32 time<1ms TTL=255 (Ver figura 20)

Tabla 18 Verificación de conectividad de la red

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

En la figura 18, 19 y 20 podemos observar cómo se escribió el comando ping en cada dispositivo según la dirección que correspondía en la tabla 18, en los dispositivos R1 Y R2 este comando se escribió en la Ventana CLI mientras que en el PC de internet ingresamos a la ventana command prompt y allí escribimos el comando ping y seguidamente la dirección IP con la que queremos probar conectividad.

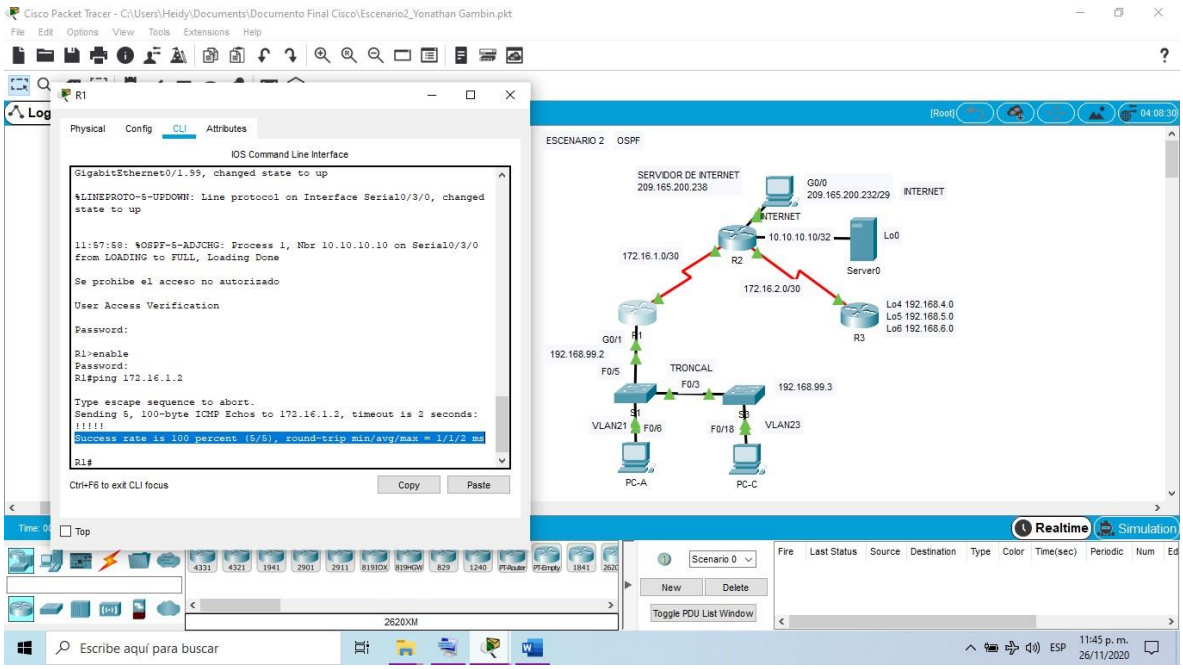


Figura 18 Verificación de conexión de red desde R1 a R2 S0/0/0

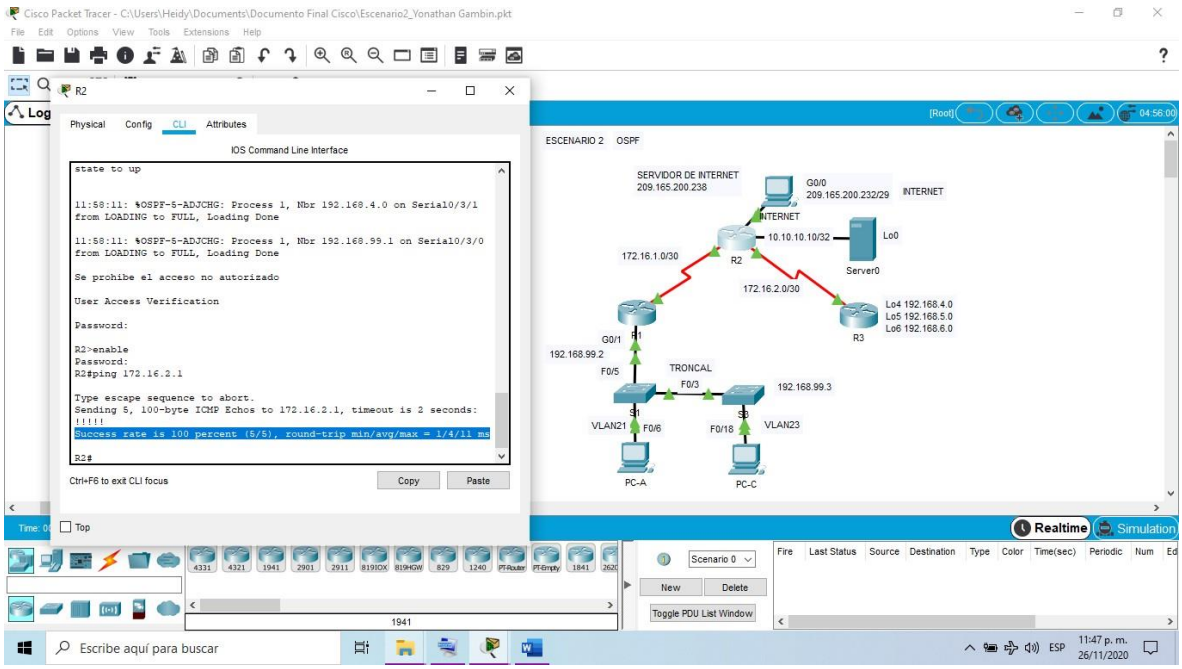


Figura 19 Verificación de conexión de red desde R2 a R3

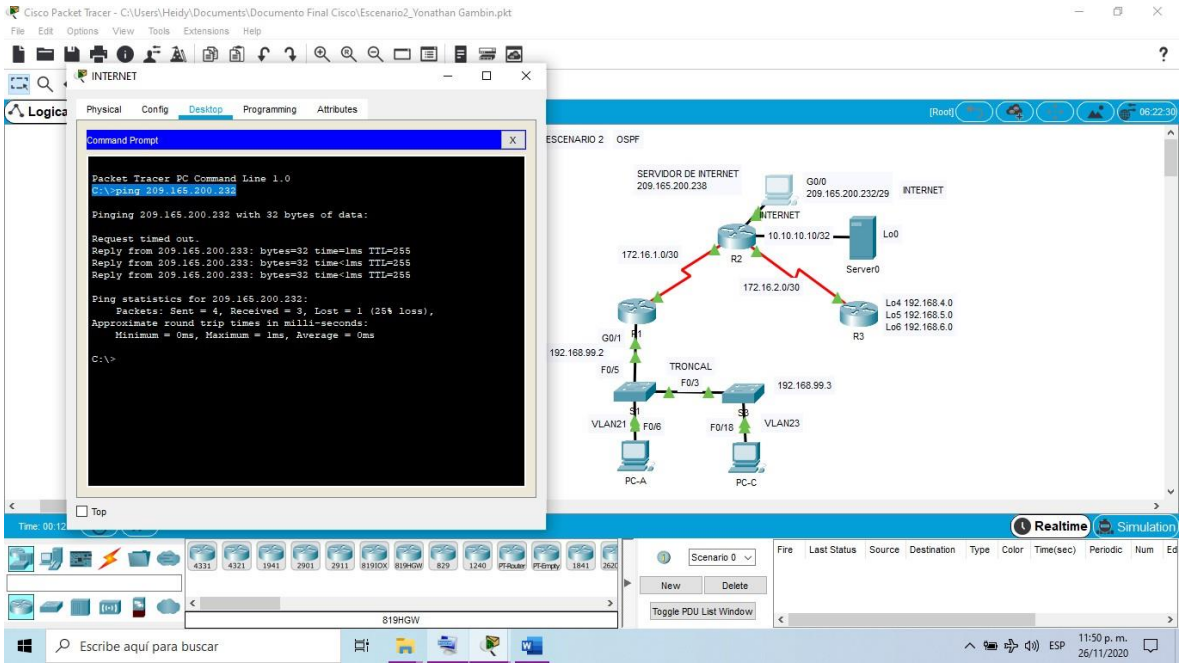


Figura 20 Verificación de conexión de red desde PC Internet a gateway predeterminado

PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

Paso 1: Configurar S1

La configuración del S1 que se realiza para configurar la infraestructura de la red, incluye crear las VLAN y al mismo tiempo asignarle un nombre para luego ingresar a las interfaces y configurarlas como puertos de acceso y en modo trunk a cada interfaz que estén involucradas con este dispositivo y asignamos el Gateway o puerta de enlace para que establecer comunicación más adelante

Tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name ingeniería S1(config-vlan)#vlan 99 S1(config-vlan)#name administración S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config-if)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#interface fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S1(config-if-rangen)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if)#interface fa0/6

	S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#no shutdown
Apagar todos los puertos sin usar	S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S1(config-if-range)#shutdown

Tabla 19 Configuración de la seguridad del switch y el routing entre las vlan de S1 con su respectivo comando

Paso 2: Configurar el S3

Igual que en switch S1 se crean las VLAN y al mismo tiempo asignarle un nombre para luego ingresar a las interfaces y configurarlas como puertos de acceso y en modo trunk a cada interfaz que estén involucradas con este dispositivo. Realizamos el proceso para S3, excepto que en este caso configuramos la interfaz F0/18 como puerto de acceso a la vlan 23.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingeniería S3(config-vlan)#vlan 99 S3(config-vlan)#name administración S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S3(config-if)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if)#interface fa0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 S3(config-if-range)#no shutdown
Apagar todos los puertos sin usar	S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S3(config-if-range)#shutdown

Tabla 20 Configuración de la seguridad del switch y el routing entre las vlan de S3 con su respectivo comando

Paso 3: Configurar R1

En esta parte configuramos la interfaz G0/1 de R1, la vamos a dividir en subinterfaces para el acceso de las vlan 99, 21, 23.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface g0/1.21 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)# interface g0/1.23 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)# interface g0/1.99 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0

Activar la interfaz G0/1	R1(config-subif)# interface g0/1 R1(config-subif)#no shutdown

Tabla 21 Configuración de la seguridad del switch y el routing entre las vlan de R1 con su respectivo comando

Paso 4: Verificar la conectividad de la red

Realizar este paso de verificar la conectividad de la red, se realiza ingresando el comando ping en la ventana CLI sin entrar en el modo de configuración del dispositivo.

Hay que tener en cuenta que si queremos establecer conectividad y esta falla hay que revisar por medio del comando show run, un comando que nos permite visualizar todas las configuraciones realizadas en los dispositivos e identificar la falla y corregirla.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 21)
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 22)
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 23)
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 24)

Tabla 22 Verificación de conectividad de la red

Primero verificamos conectividad desde S1 a R1 a la dirección de la vlan 99, para ello ingresamos a S1 colocamos ping y seguidamente la dirección IP.

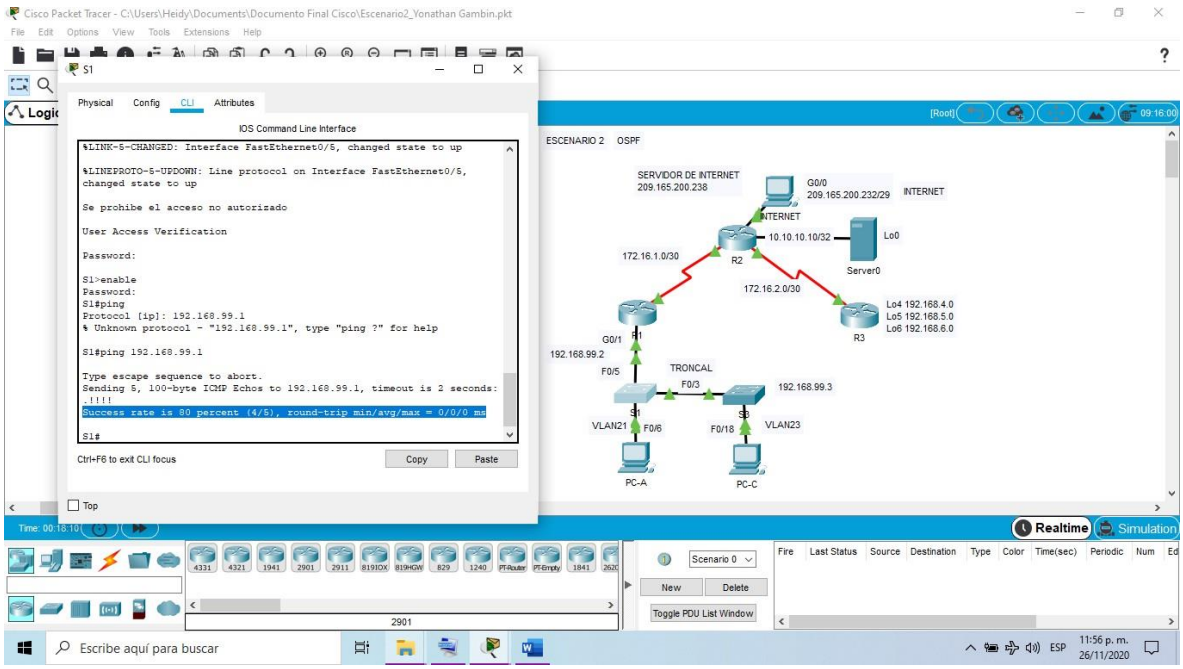


Figura 21 Verificación de conexión de red desde S1 a R1 dirección VLAN 99

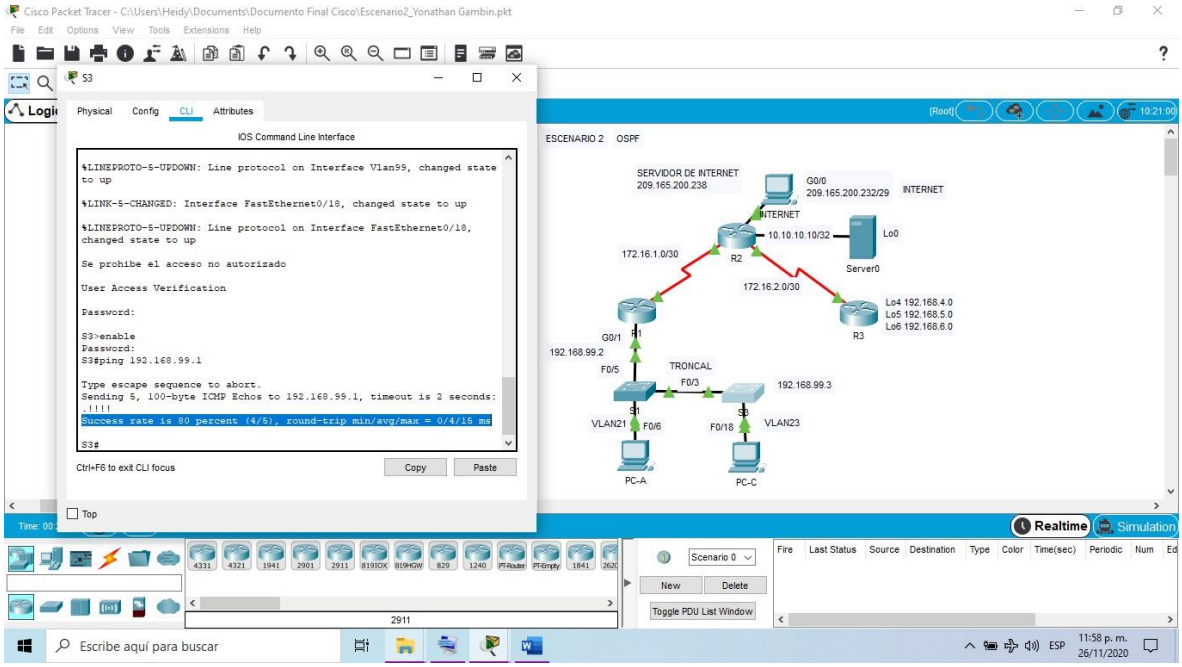


Figura 22 Verificación de conexión de red desde S3 a R1 dirección VLAN 99

Ahora verificamos conectividad desde S3 a R1 a la dirección de la vlan 99, para ello ingresamos a S1 colocamos ping y seguidamente la dirección IP.

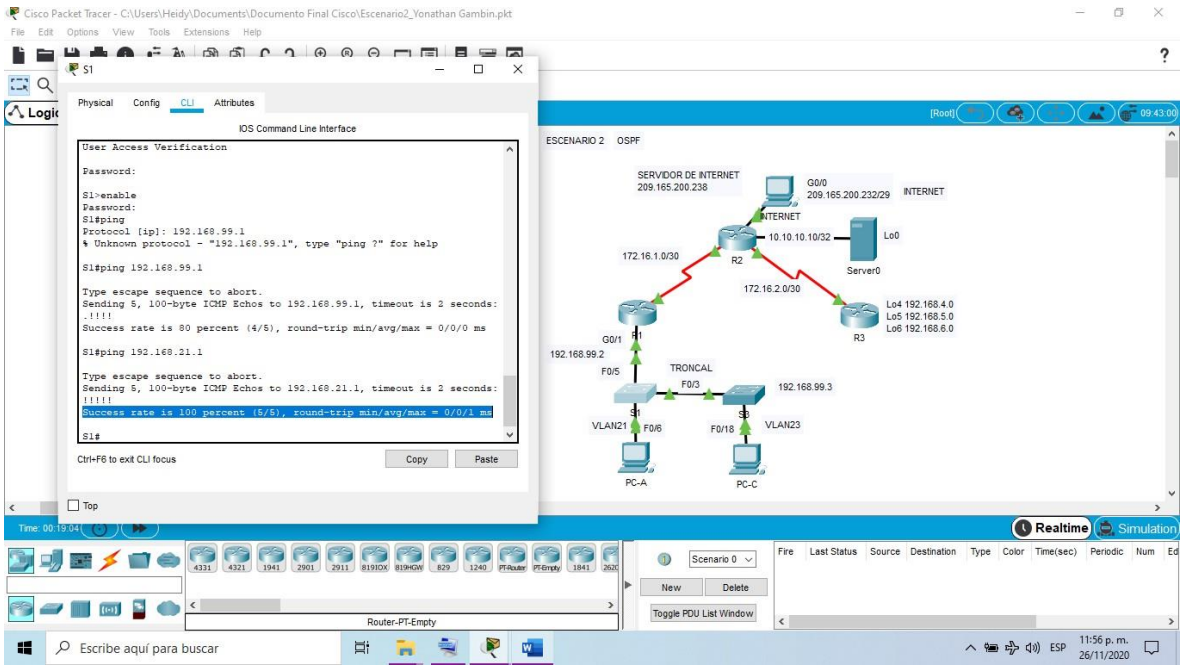


Figura 23 Verificación de conexión de red desde S1 a R1 dirección VLAN 21

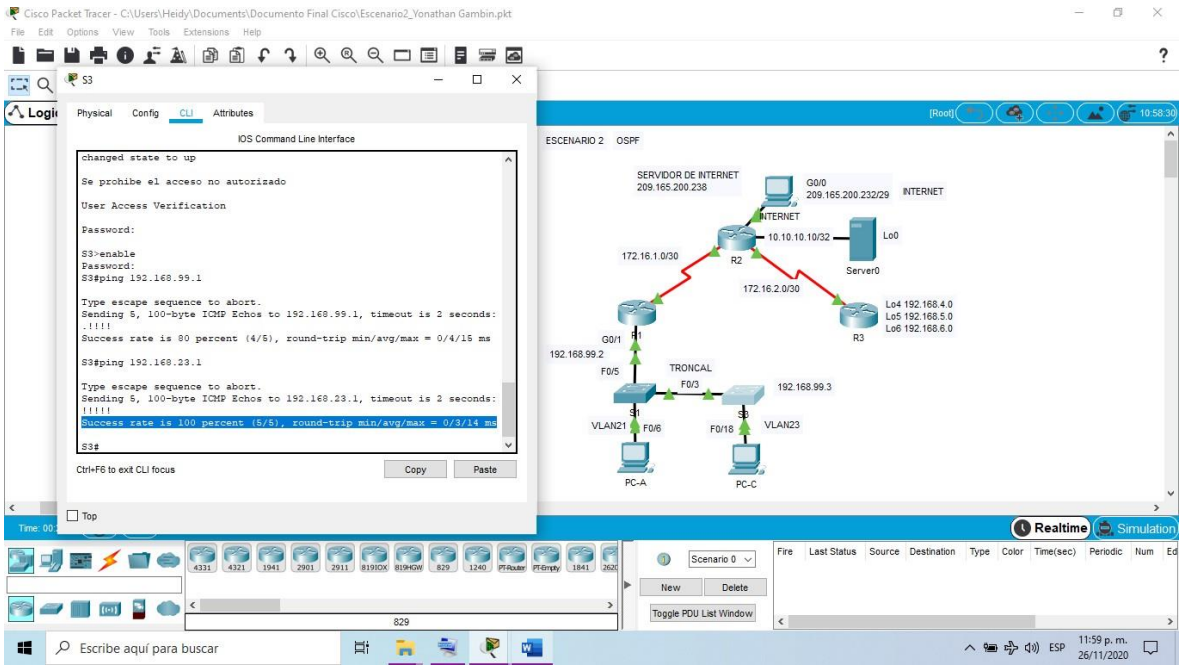


Figura 24 Verificación de conexión de red desde S3 a R1 dirección VLAN 23

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

Paso 1: Configurar OSPF en el R1

El protocolo Open Shortest Path First (OSPF), este protocolo significa abrir el camino más corto primero, es un protocolo de red para encaminamiento jerárquico que calcula la ruta más corta para realizar la comunicación entre los dispositivos de la red, por medio de los siguientes comandos y configuraciones.

Router(config)#router ospf xxx

Router(config-router)#network d.d.d.d m.m.m.m area zzz

Donde

- xxx es un número o identificativo de proceso que ejecuta OSPF interno para el router, que puede valer por ejemplo “1”. Para este caso le colocaremos 1
- d.d.d.d son direcciones base de red de redes directamente conectadas,
- m.m.m.m es una wildcard, es decir tiene el significado inverso de la máscara, 1’s en vez de 0’s Para este caso le colocaremos la máscara de red 0.0.0.255
- zzz es el identificador del área, para el backbone debe ser 0. Para este caso le colocaremos el área 0

Elemento o tarea de configuración	Especificación
Configurar OSPF area 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.255 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 23 Configuración OSPF en el R1 con su respectivo comando

Paso 2: Configurar OSPF en el R2

La configuración en el dispositivo R2 son las mimas que se realizaron en la configuración anterior R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF area 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)#network 172.16.2.0 0.0.0.255 area 0 R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 192.168.4.0 0.0.0.255 area 0 R2(config-router)#network 192.168.5.0 0.0.0.255 area 0 R2(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo4 R2(config-router)#passive-interface lo5 R2(config-router)#passive-interface lo6
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 24 Configuración OSPF en el R2 con su respectivo comando

Paso 3: Configurar OSPFv3 en el R3

La configuración en el dispositivo R3 son las mimas que se realizaron en la configuración anterior R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF area 0	R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.255 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0

	R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 25 Configuración OSPF en el R3 con su respectivo comando

Paso 4: Verificar la información de OSPF

Verificamos el protocolo OSPF para saber que está funcionando como se espera. Introducimos el comando que aparece en la tabla 26 escribiéndolo en la ventana CLI.

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 protocols R2#Show ip protocols R3#Show ip protocols (Ver figura 25,26,27)
¿Qué comando muestra solo las rutas OSPF?	R1#Show ip route ospf R2#Show ip route ospf R3#Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#Show run R2#Show run R3#Show run (Ver figura 31,32,33)

Tabla 26 Verificar la información de OSPF con su respectivo comando

En las siguientes figuras podemos observar como se escribe cada comando y el resultado que se obtiene después de ejecutar cada uno de ellos.

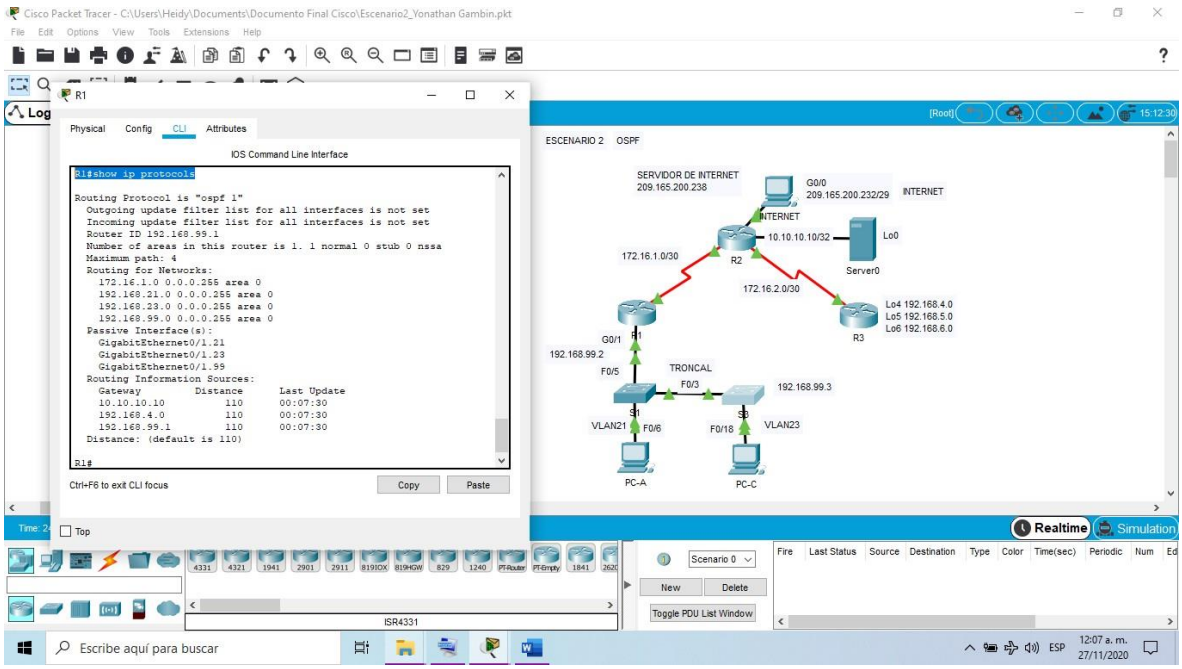


Figura 25 Verificar la información de OSPF en R1 usando el comando Show ip protocols

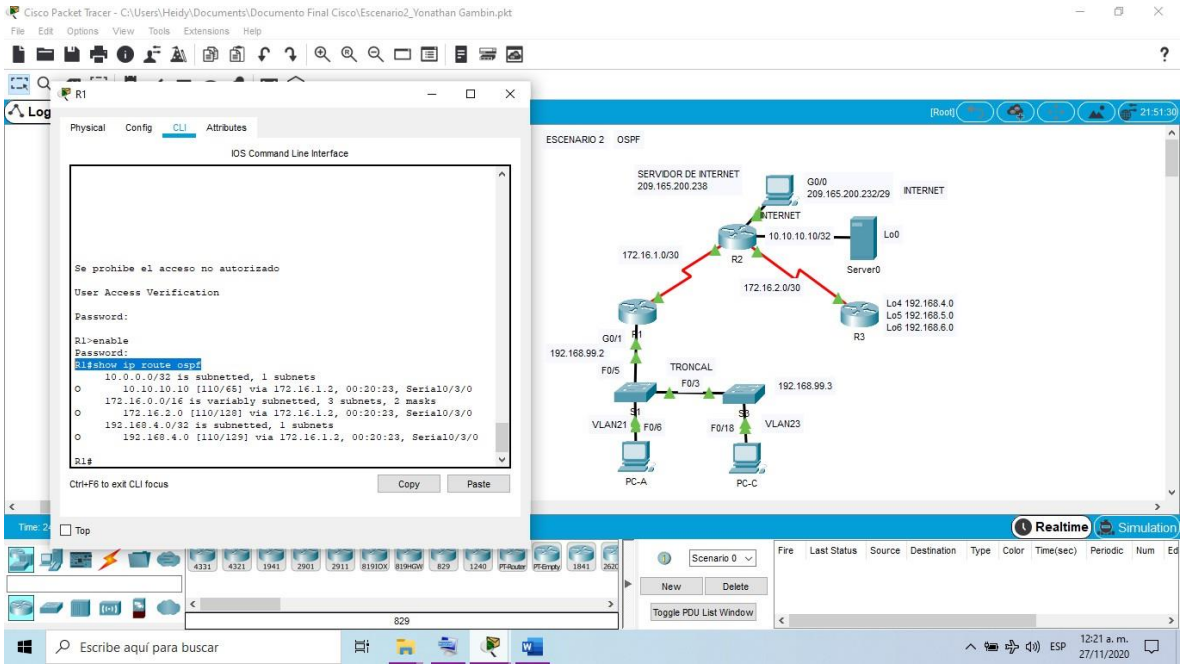


Figura 26 Verificar la información de OSPF en R1 usando el comando Show ip route ospf

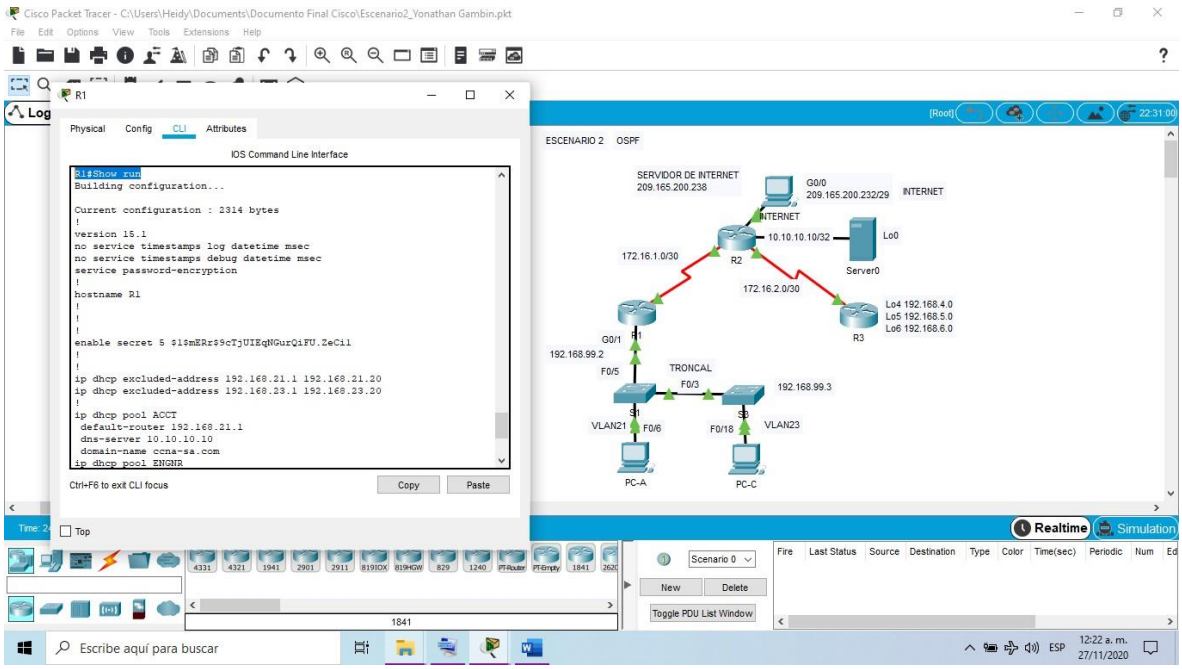


Figura 27 Verificar la información de OSPF en R1 usando el comando Show run

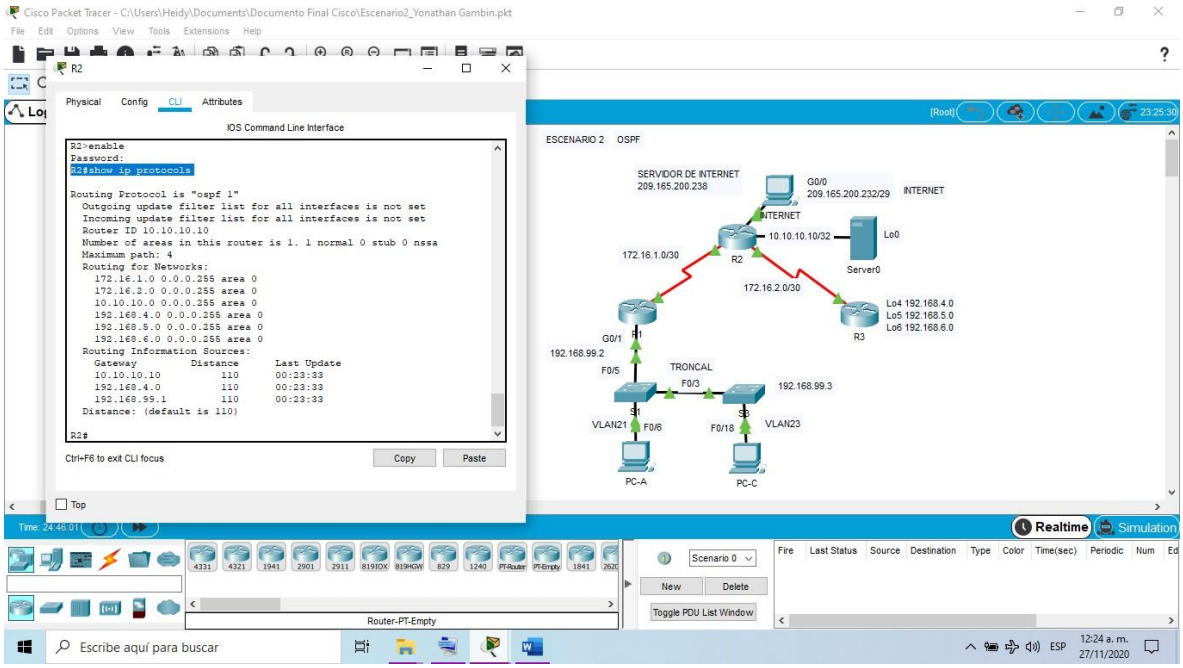


Figura 28 Verificar la información de OSPF en R2 usando el comando Show ip protocols

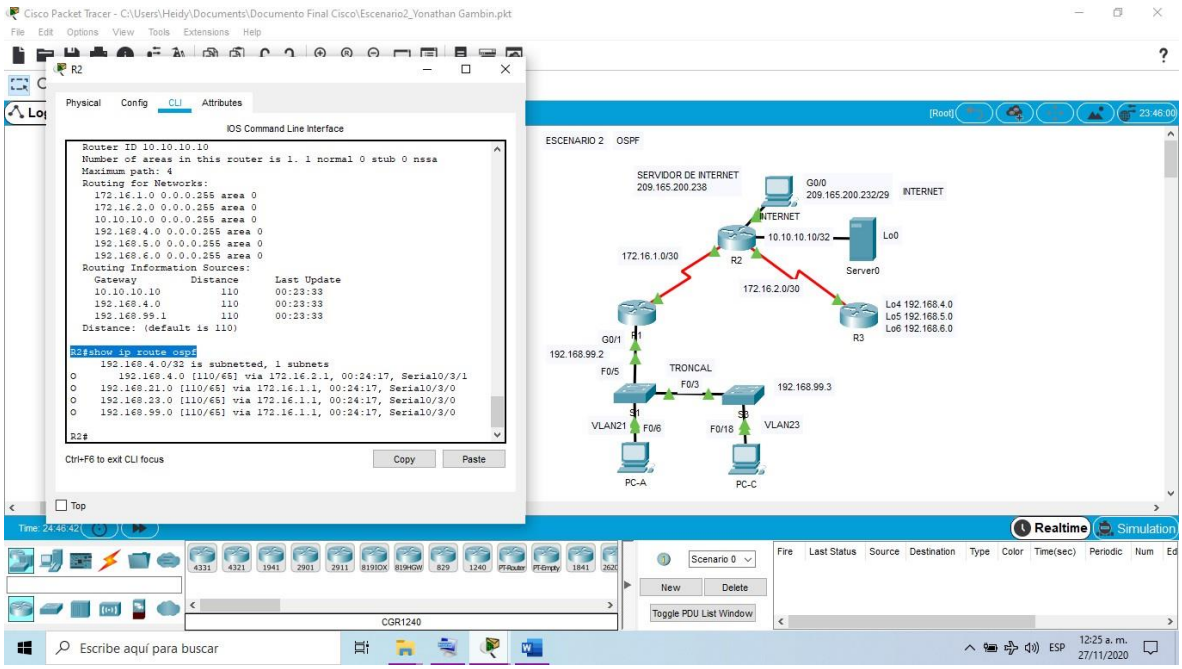


Figura 29 Verificar la información de OSPF en R2 usando el comando Show ip route ospf

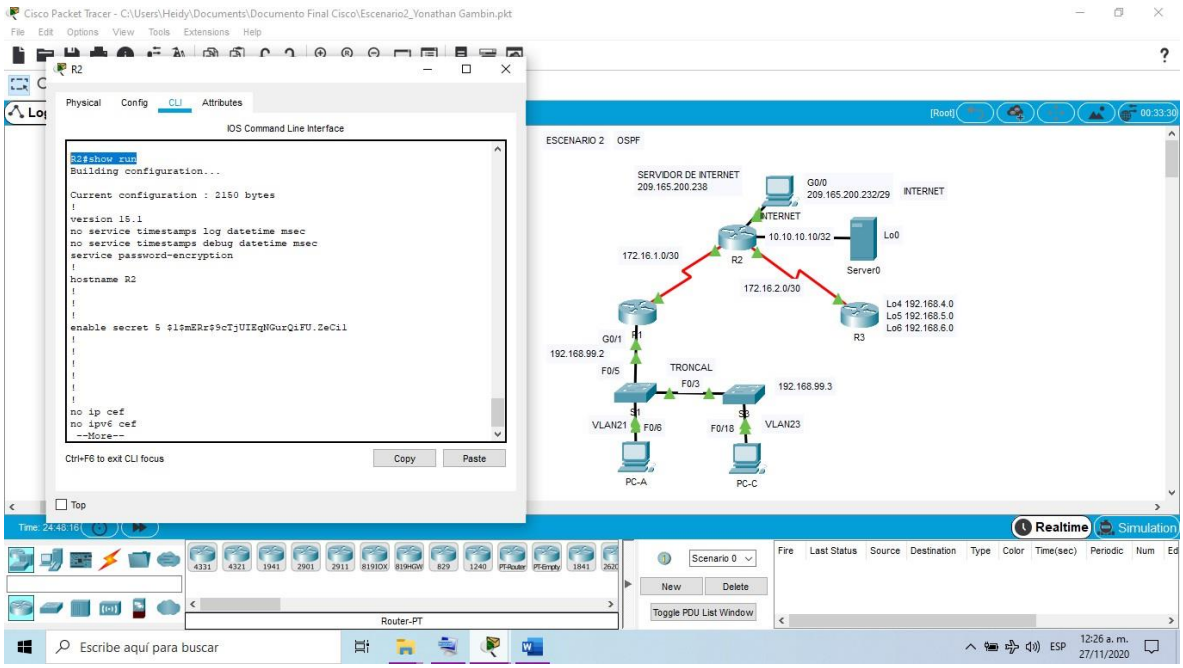


Figura 30 Verificar la información de OSPF en R2 usando el comando Show run

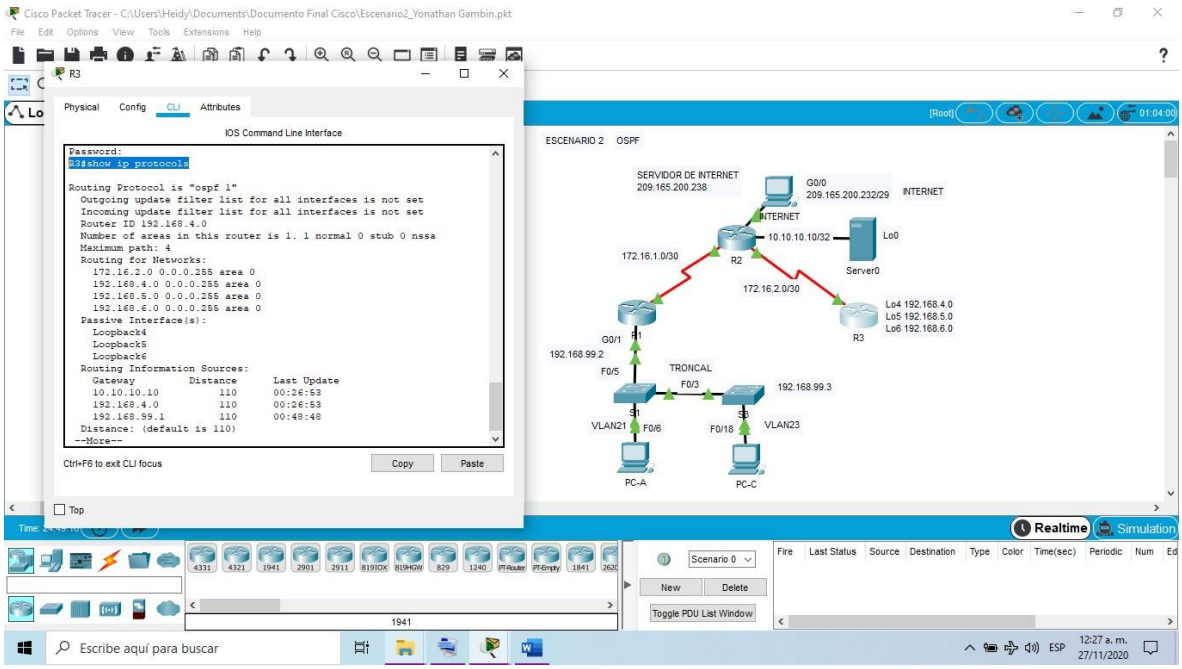


Figura 31 Verificar la información de OSPF en R3 usando el comando Show ip protocols

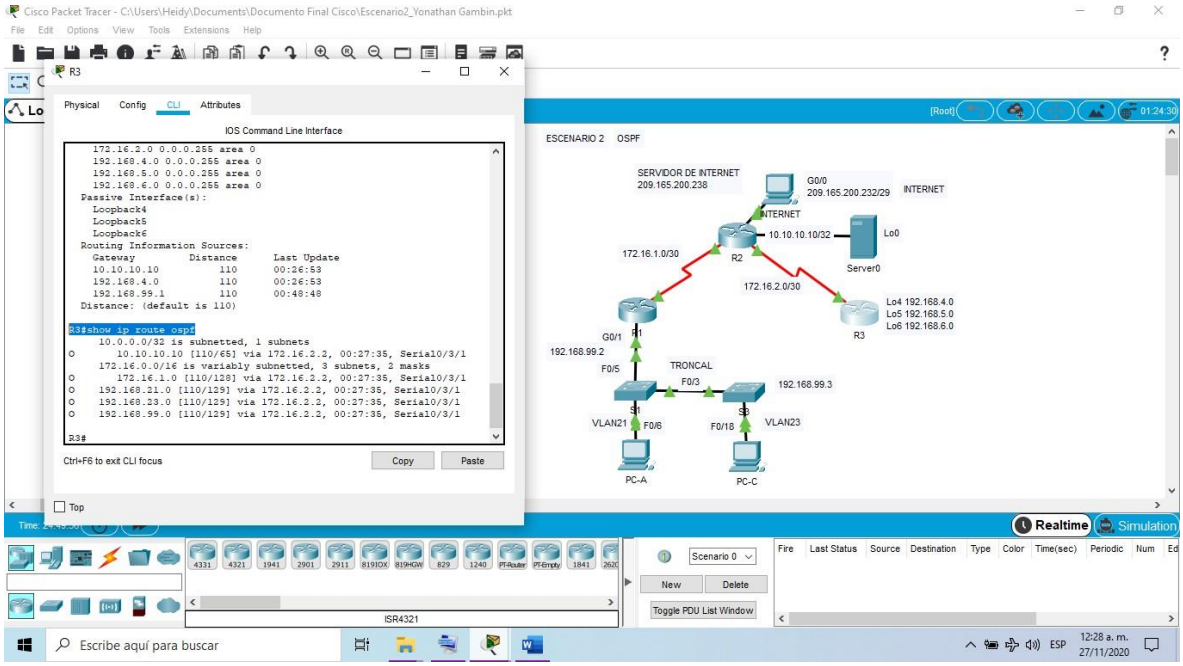


Figura 32 Verificar la información de OSPF en R3 usando el comando Show ip route ospf

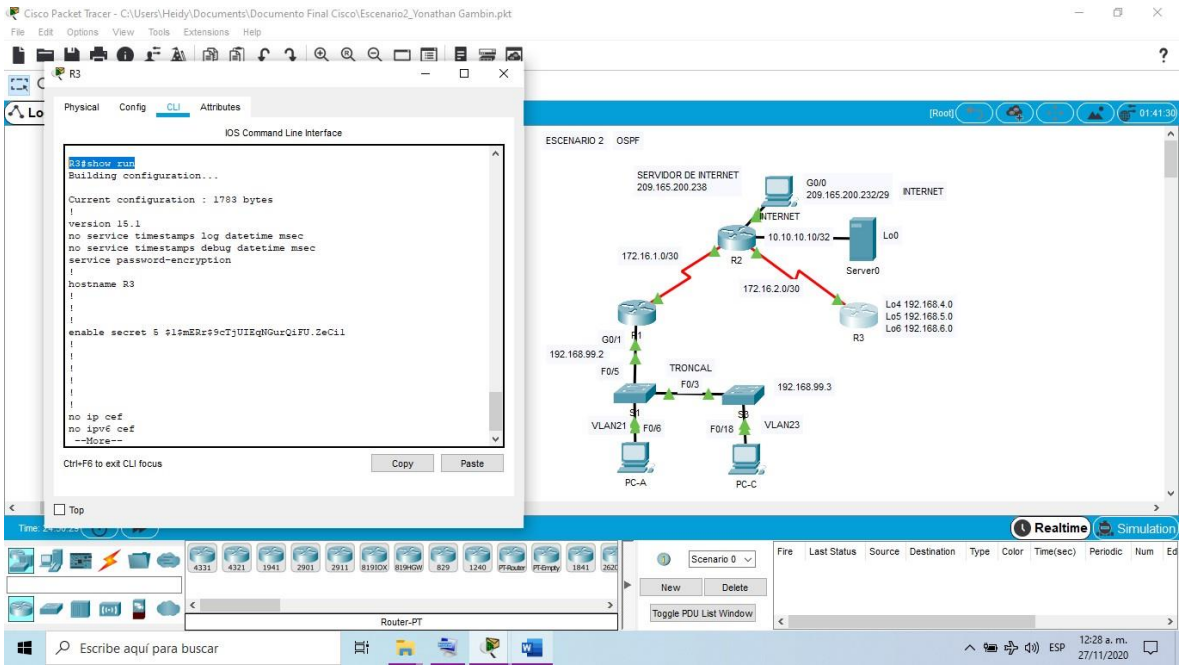


Figura 33 Verificar la información de OSPF en R3 usando el comando Show run

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

En esta parte configurar el protocolo DHCP (Dynamic Host Configuration Protocol) que es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red, ya que una dirección IP es un número que identifica de forma única a un ordenador en la red y en este caso realizamos una configuración para que este proceso se haga automáticamente y no manualmente como se realizó en el PC de Internet.

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

La configuración para R1 como servidor para la VLAN 21 y 23 se realiza por medio de los siguientes comandos, primero reservamos las primeras 20 direcciones IP en la VLAN 21 Y 23, Luego creamos un pool de DHCP para las dos VLAN.

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 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com R1(config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com R1(config)#default-router 192.168.23.1

Tabla 27 Configuración de R1 como servidor de DHCP para IPV4 con su respectivo comando

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

la NAT estática proporciona una asignación permanente entre una dirección local interna y una dirección global interna, la NAT dinámica permite la asignación automática de direcciones locales internas a direcciones globales internas. Por ello aquí veremos que para esta configuración la NAT estática y la NAT dinámica requiere que se configuren las interfaces interna y externa que participan en la NAT. Sin embargo, mientras que la NAT estática crea una asignación permanente a una única dirección, la NAT dinámica utiliza un conjunto de direcciones.

Esta configuración la realizamos por medio de crear una base de datos local con una cuenta de usuario y habilitamos el servidor HTTP, luego si creamos la NAT estática y la dinámica por medio de los comandos que aparecen en la table 28.

Elemento o tarea de configuración	especificación

Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Packet Tracer no procesa la configuraion 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
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gi0/1 R2(config)#ip nat outside R2(config)#interface fa0/6 R2(config)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Tabla 28 Configuración NAT en R2 para IPV4 con su respectivo comando

Paso 3: Verificar el protocolo DHCP y la NAT estática

Las configuraciones del protocolo DHCP y NAT estática es importante para llevar un control de las todas las configuraciones que se han ido realizando en esta red.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	request successful
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	request successful
Verificar que la PC-A pueda hacer ping a la PC-C	Successful

Nota: Quizá sea necesario deshabilitar el firewall de la PC.	
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	Successful

Tabla 29 Verificación del protocolo DHCP y NAT estática

PARTE 6: CONFIGURAR NTP

El Protocolo de tiempo de red (NTP, por sus siglas en inglés) sincroniza la hora de las computadoras en una red. Su Firebox puede usar el NTP para obtener automáticamente la hora correcta de los servidores NTP en Internet para configurar el reloj del sistema, lo que resulta importante para llevar un orden no solo interno si no también externo para quien acceda a la red.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R1 y R2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	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#show ntp associations R1#show clock

Tabla 30 Configuración NTP

En la figura 34 se muestra el resultado que nos muestra la ventana CLI de los routers cuando emitimos el comando #show ntp associations y #show clock.

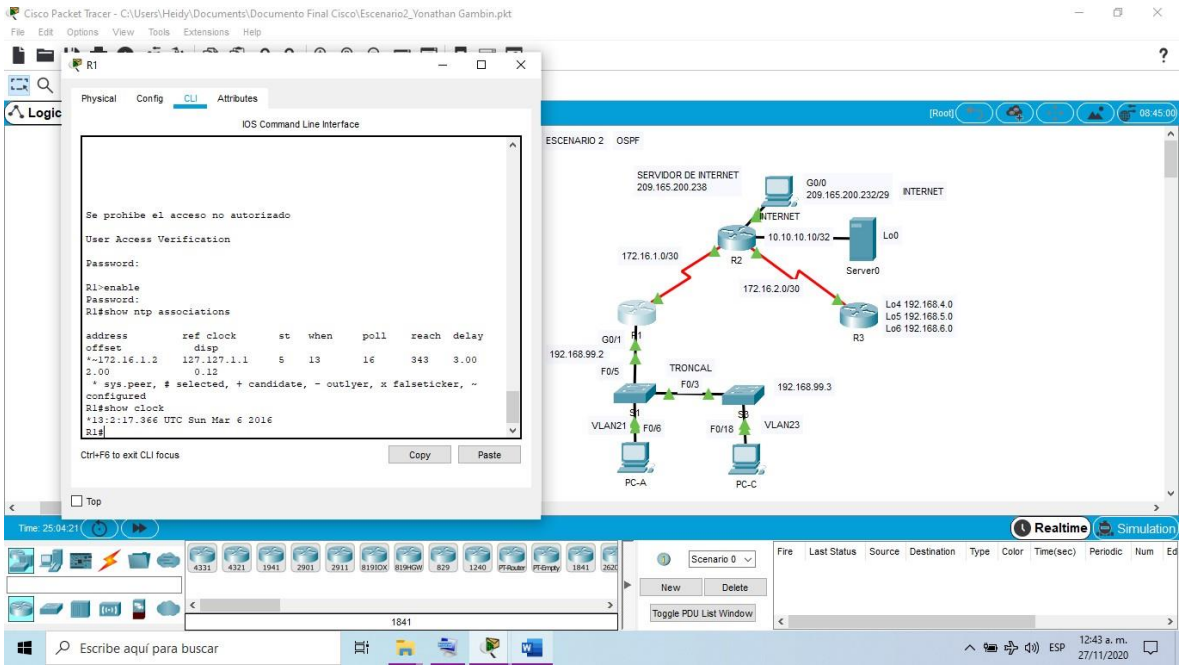


Figura 34 Verificación de la configuración NTP

PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

Es una serie de instrucciones que controlan que en un router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información y proporcionan un nivel básico de seguridad para el acceso a la red

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

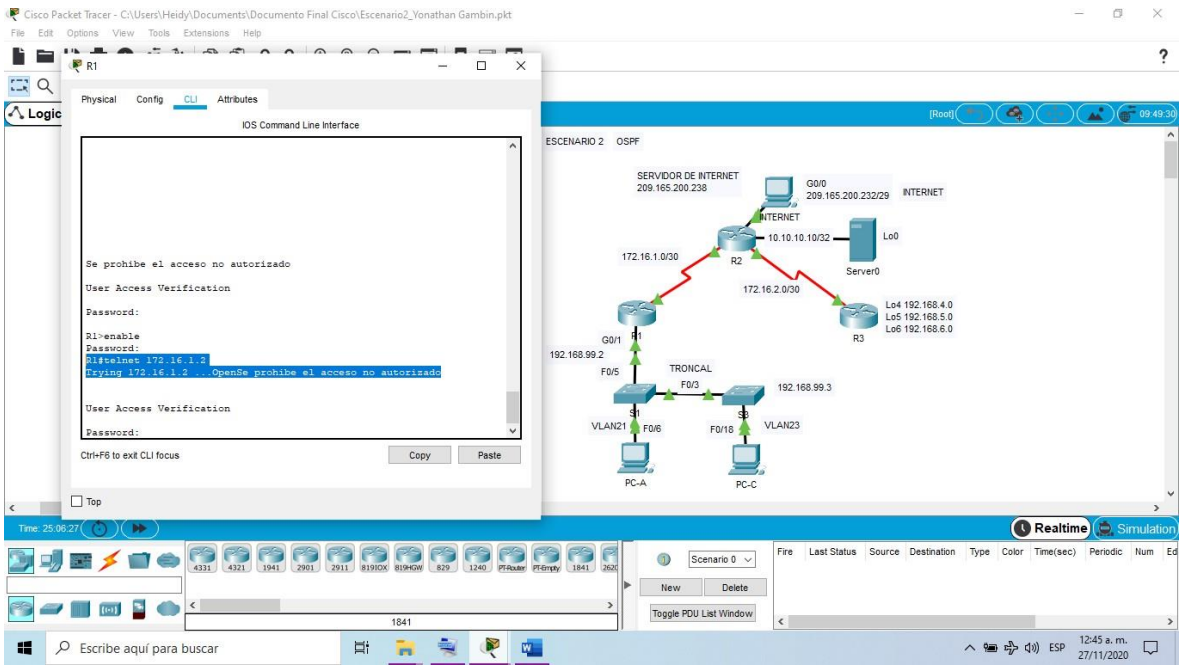
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R2, para restringir el acceso a las líneas de control de acceso.

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standart ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config-line)#line vty 0 4
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 R3#telnet 172.16.1.2

Tabla 31 configuración y verificación de las listas de control de acceso ACL

Verificamos, esta configuración por medio del comando, cuando ingresamos el código podemos ver como hace la verificación



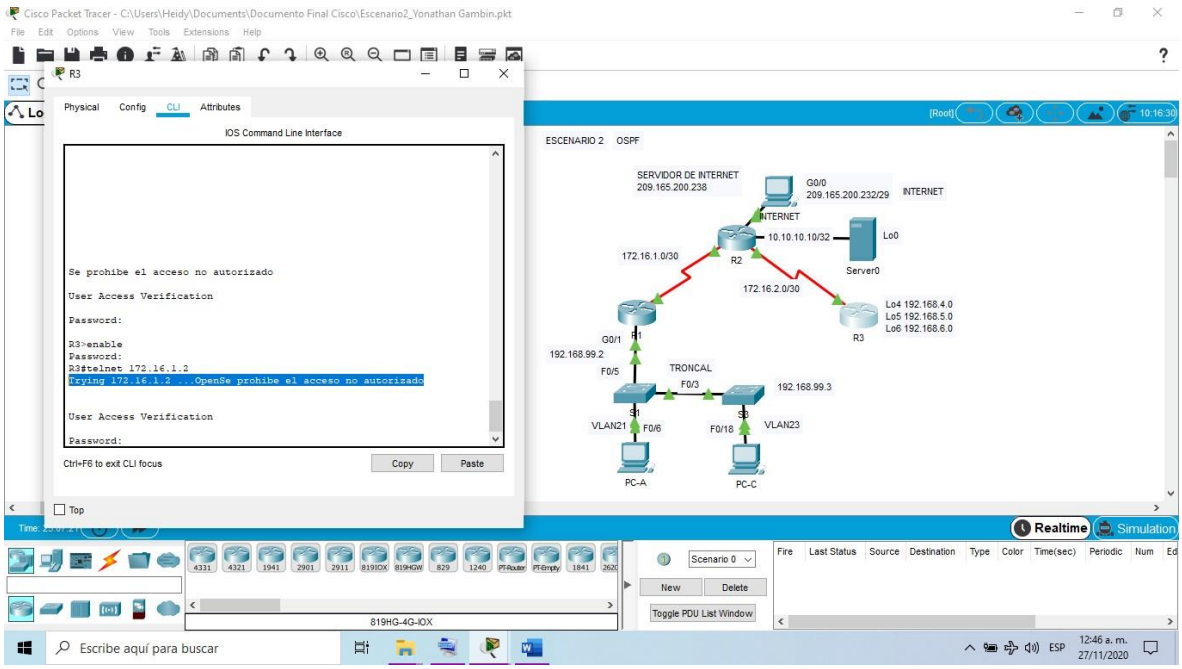


Figura 35 Verificación de la ACL en R1 y R3

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	#show ip access list
Restablecer los contadores de una lista de acceso	#clear ip
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	#show ip interface
¿Con qué comando se muestran las traducciones NAT?	#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	#clear ip nat translations

Tabla 32 Comandos para realizar las verificaciones de las configuraciones realizadas en los dispositivos de la red del segundo escenario

CONCLUSIONES

A partir del desarrollo de esta prueba de habilidades se aplicó cada uno de los conceptos y procedimientos vistos en el diplomado de cisco, utilizando el software cisco packet tracer como herramienta de simulación de los dos escenarios que se desarrollaron por su fácil comprensión del entorno y similitud con las configuraciones de una red de comunicaciones en cualquier aplicación de la vida, por ello se obtuvo no solamente un buen aprendizaje sino además buenos resultados de las configuraciones realizadas según los requerimientos de cada escenario.

Se manejaron distintos protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, como el protocolo de routing dinámico OSPF y Dynamic Host Configuration Protocol DHCP, a través de configurar el enrutamiento entre VLAN.

Se inspeccionaron cada una de las configuraciones realizadas en los dispositivos y su verificación de conectividad por medio de los comandos ping, traceroute, show ip route, entre otros, que facilitan además detectar los errores que se puedan cometer al realizar las configuraciones.

REFERENCIAS

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

ANEXOS

Anexo A Configuración de una red de forma segura.

CONFIGURACION DE UNA RED DE FORMA SEGURA

Yonathan Gambin
Universidad Nacional Abierta y a Distancia (UNAD) ygambing@unadvirtual.edu.co

Resumen

El desarrollo de este trabajo se centra en administrar una red pequeña por medio del software cisco Packet Tracer, que admita la conectividad IPv4 e IPv6 para los hots soportados, para así configurar el enrutamiento entre VLAN, DHCP, Etherchannel y port-security. con el fin de configurar de forma segura la red

Palabras clave: Administrar, DHCP, Seguridad, Red, VLAN.

Abstract:

The development of this work is focused on managing a small network by means of cisco Packet Tracer software, which supports IPv4 and IPv6 connectivity for the supported hots, in order to configure the routing between VLAN, DHCP, Etherchannel and port-security. In order to securely configure the network

Keywords— Manage, DHCP, Security, Network, VLAN.

I. INTRODUCCIÓN

Garantizar la seguridad de las redes de comunicaciones se ha vuelto fundamental para las organizaciones, por ello este informe tendrá como objetivo la gestión de una red pequeña por medio del programa de Cisco Packet Tracer, inicialmente se realizará la topología de la red, donde se configurará e interconectará entre sí cada uno de los dispositivos.

Se realizarán las configuraciones básicas de los switches y routers para que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. Se realiza la configuración del enrutamiento entre VLAN, DHCP, Etherchannel, port-security y por último se verifica este procedimiento usando los comandos ping, traceroute, show ip route, entre otros.

II. PROCEDIMIENTO PARA CONFIGURAR UNA RED DE FORMA SEGURA

El procedimiento para llevar a cabo la configuración de cada uno de los dispositivos se describe a continuación.

A. Topología

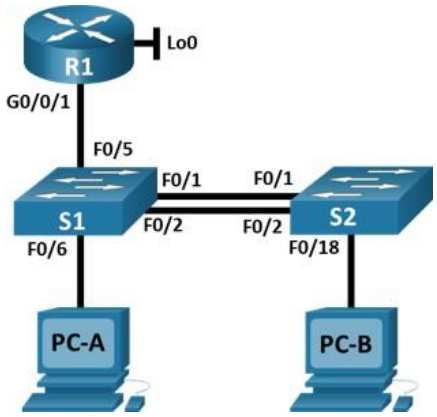


Figura 1. Topología

La topología de red, que se muestra en la Figura 1, Es una pequeña red compuesta por un router, dos switch y dos hosts para implementar esta topología en cisco packet tracer inicialmente agregamos a la pantalla principal del programa un router 2901 y se conectan los dispositivos por los puertos serial s0/3/0 y s0/3/1, como podemos observar en la topología de la red, seguidamente se agregan los switch y se realizan las conexiones por medio de puertos seriales al router y al host según corresponda.

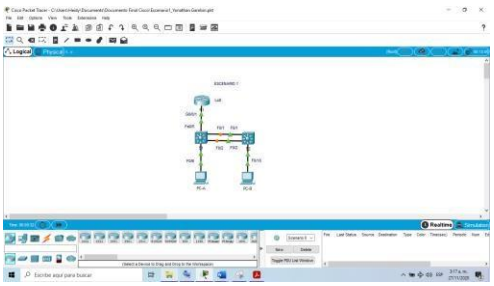


Figura 2. Topología en el software

A. Inicialización de los dispositivos

Borrar las configuraciones de inicio y las VLAN del router y del switch y volver a cargar los dispositivos, por medio de la ejecución de los siguientes comandos tal como se muestra para cada uno de los dispositivos de la red que tenemos en la figura 1.

R1

```
Router>enable
Router#erase
Router#erase startup-config
Erasing the nvram filesystem will remove all
configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
Router#reload
Proceed with reload? [confirm]
```

S1

```
Switch>enable
Switch#erase sta
Switch#erase startup-config
Erasing the nvram filesystem will remove all
configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
Switch#reload
Proceed with reload? [confirm]
```

S2

```
Switch>enable
Switch#erase sta
Switch#erase startup-config
Erasing the nvram filesystem will remove all
configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
Switch#reload
Proceed with reload? [confirm]
```

B. Configuración de R1

Las tareas de configuración para R1 incluyen las siguientes líneas de comandos y además se crean las subinterfaces, encapsulándolas con su VLAN y asignando los direccionamientos IPv4 e IPv6, además se genera una clave de cifrado RSA, se configuran las medidas de seguridad, así como la transferencia de autenticación por medio de SSH.

1) Ingresar a la pestaña CLI del router R1, donde inicialmente nos preguntara el sistema operativo del router, si queremos, usar el asistente de configuración, en este caso escribiremos no, ya que las configuraciones se harán manualmente.

2) Cambiar el nombre de usuario, primero nos aparecerá router>, por lo que colocamos el comando enable para cambiar de usuario en modo normal a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado router#.

3) Entrar en el modo de configuraciones con el comando configure terminal.

4) Desactivar la búsqueda de nombres de dominio, con el comando no ip domain lookup.

5) Cambiar el nombre del router por medio del comando hostname seguido del nombre que se le colocara, en este caso es R1 para el primer router, R2 para el segundo y R3 para el tercero.

6) Escribir el comando service password-encryption para encriptar las contraseñas.

7) Colocar una contraseña secreta que no se podrá visualizar por medio del comando enable secret seguido la contraseña cisco.

8) Restringir el acceso del puerto de consola y configurar las líneas de terminal virtual (vty) para que el router permita el acceso por Telnet, por medio de los comandos line console 0 y line vty 0 4, damos enter y colocamos la contraseña password cisco, después se ingresa el comando login para que aplique las contraseñas.

9) Configuración de las interfaces involucradas con cada dispositivo con su respectiva dirección IPv4 e IPv6

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R1

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#service password-encryption
R1(config)#enable secret class
R1(config)#line console 0
R1(config)#password cisco
R1(config)#login
R1(config)#line vty 0 4
R1(config)#password cisco
R1(config)#login
R1(config)#banner motd $Se prohibe el acceso no
```

```
autorizado$
R1(config)#interface s0/3/0
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config)#interface s0/3/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
R1(config-if)#no shutdown
R1(config)#ip route 0.0.0.0 0.0.0.0 serial s0/3/0
R1(config)#ipv6 route ::/0 serial s0/3/0
```

A. Configuración de S1 y S2

Las tareas de configuración para S1 y S2 incluyen las siguientes:

1) Ingresar a la pestaña CLI del switch, donde inicialmente nos preguntara el sistema operativo del switch, si queremos, usar el asistente de configuración, en este caso escribiremos no, ya que las configuraciones se harán manualmente.

2) Cambiar el nombre de usuario, primero nos aparecerá switch>, por lo que colocamos el comando enable para cambiar de usuario en modo normal a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado switch#.

3) Entrar en el modo de configuraciones con el comando configure terminal.

4) Desactivar la búsqueda de nombres de dominio, con el comando no ip domain lookup.

5) Cambiar el nombre del switch por medio del comando hostname seguido del nombre que se le colocara, en este caso es S1 para el primer switch y S2 para el segundo.

6) Escribir el comando service password-encryption para encriptar las contraseñas.

7) Colocar una contraseña secreta que no se podrá visualizar por medio del comando enable secret seguido la contraseña cisco.

8) Restringir el acceso del puerto de consola y configurar las líneas de terminal virtual (vty) para que el switch permita el acceso por Telnet, por medio de los comandos line console 0 y line vty 0 15, damos enter y colocamos la contraseña password cisco, después se ingresa el comando login para que aplique las contraseñas.

9) Configuración de las interfaces involucradas con cada dispositivo con su respectiva dirección IPv4 e IPv6

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de cada Switch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#service password-encryption
S1(config)#enable secret class
S1(config)#line console 0
S1(config)#password cisco
S1(config)#login
S1(config)#line vty 0 4
S1(config)#password cisco
S1(config)#login
S1(config)#banner motd $Se prohibe el acceso no
autorizado$
```

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S3
S2(config)#no ip domain-lookup
S2(config)#service password-encryption
S2(config)#enable secret class
S2(config)#line console 0
S2(config)#password cisco
S2(config)#login
S2(config)#line vty 0 4
S2(config)#password cisco
S2(config)#login
S2(config)#banner motd $Se prohibe el acceso no
autorizado$
S2(config)#crypto key generate rsa
S2(config)#interface vlan 4
S2(config-if)#ip add 10.19.8.99 255.255.255.248
S2(config-if)#ipv6 add 2001:db8:acad:c::99/64
S2(config-if)#ipv6 add fe80::99 link-local
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#ip default-gateway 10.19.8.97
```

Después de realizar las configuraciones básicas en los dispositivos es importante por medio del comando ping probar la conectividad entre los dispositivos de red.

B. Configurar de la infraestructura de red (vlan, trunking, etherchannel)

La configuración del S1 incluye las siguientes tareas:

```
S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#vlan 4
```

```
S1(config-vlan)#name Management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
```

Crear troncos 802.1Q que utilicen la VLAN 6 nativa

```
S1#configure terminal
S1(config)#interface fa0/1
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6

S1#configure terminal
S1(config)#interface fa0/2
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#exit

S1(config)#interface fa0/5
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#exit
```

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

```
S1(config)#interface range fa0/1-2
S1(config-if-range)#channel-group 2 mode active
S1(config)#exit
S1(config#interface port-channel 2
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config)#switchport trunk native vlan 6
```

Configurar el puerto de acceso de host para VLAN 2

```
S1(config)#interface fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#no shutdown
S1(config-if)#exit
```

Configurar la seguridad del puerto en los puertos de acceso

```
S1(config)#interface fa0/6
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
```

Proteja todas las interfaces no utilizadas

```
S1(config)#interface range fa0/3-4, fa0/7-24, gi0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#shutdown
```

La configuración del S2 incluye las siguientes tareas:

```
S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native
```

Crear troncos 802.1Q que utilicen la VLAN 6 nativa

```
S2(config)#interface range fa0/1-2
S2(config-if-range)#switchport trunk encapsulation dot1q
S2(config-if-range)#switchport mode trunk
S2(config)#interface port-channel 2
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#exit
S2(config)#interface range fa0/1-2
channel-group 2 mode passive
S2(config-if-range)#no shutdown
```

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

```
S2(config)#interface port-channel 2
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#exit
S2(config)#interface range fa0/1-2 channel-group 2 mode
passive
S2(config-if-range)#no shutdown
```

Configurar el puerto de acceso del host para la VLAN 3

```
S2(config)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#exit
```

Configure port-security en los access ports

```
S2(config)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3
```

Asegure todas las interfaces no utilizadas.

I. CONFIGURAR SOPORTE DE HOST

Esta configuración se realiza en R1

Configure Default Routing

```
R1(config)#ip route 0.0.0.0 0.0.0.0 lo0
```

Configurar IPv4 DHCP para VLAN 2

```
R1(config)#ip dhcp pool vlan 2
R1(config)#ip dhcp excluded-address 10.19.8.1
10.19.8.10
R1(config)#dns-server 10.10.10.10
R1(config)#domain-name ccna-a.net
R1(config)#default-router 10.19.8.1
```

Configurar DHCP IPv4 para VLAN 3

```
R1(config)#ip dhcp pool vlan 3
R1(config)#ip dhcp excluded-address 10.19.8.1
10.19.8.10
R1(config)#dns-server 10.10.10.10
R1(config)#domain-name ccna-b.net
R1(config)#default-router 10.19.8.65
```

Configurar 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

II. VERIFICAR DE CONEXIONES

Usando el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red. se verifica metódicamente la conectividad con cada dispositivo de red. Y dado el caso de que algún ping falle se toman medidas correctivas para establecer la conectividad si alguna de las pruebas falla.

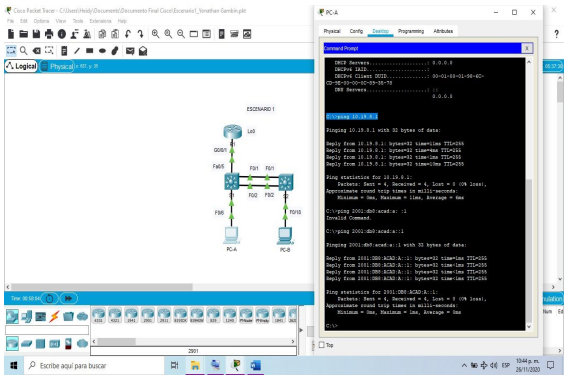


Figura 3. Verificación de la conectividad de red

III. RESULTADOS

A partir del procedimiento que se desarrolló, se obtuvo un buen resultado para continuar en trabajos futuros administrando una red mucho más grande. La metodología que se desarrollo fue buena debido a que establecer un orden secuencial permite que en las configuraciones que se realicen a la red ocurran pocas fallas.

A través de los comandos anteriores que pueden parecer básicos pero que son los más importantes, porque al realizar esta configuración inicial ya tenemos seguridad en nuestra red por medio de las contraseñas que se establecen a los puertos de acceso. A continuación, se muestran unas figuras en las que se muestra como al ingresar a cada dispositivo vemos como este nos pide ingresar las contraseñas demostrando que se configuro una red segura.

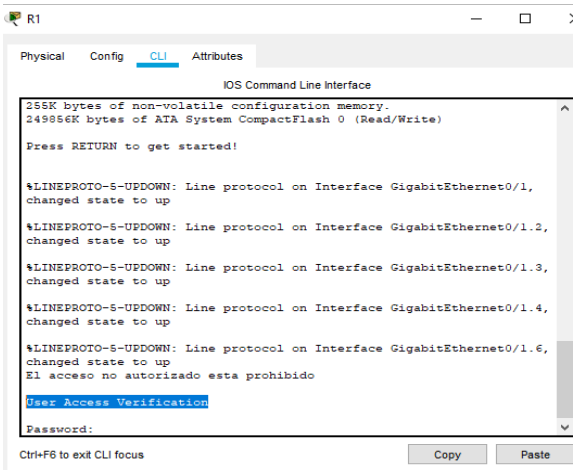


Figura 4. Ingreso al Router R1 después de las configuraciones básicas.

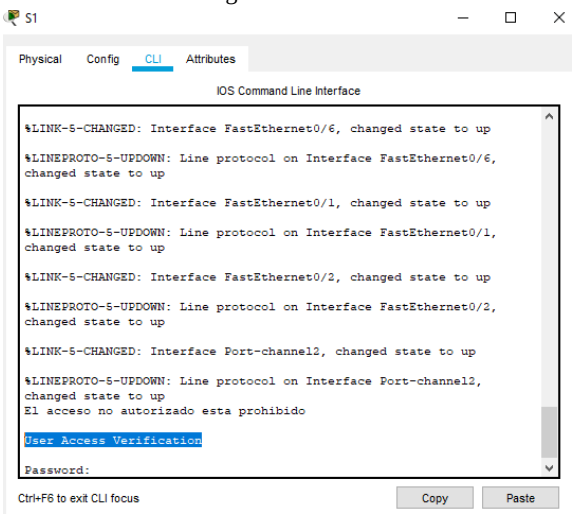


Figura 5. Ingreso al Switch S1 después de las configuraciones básicas

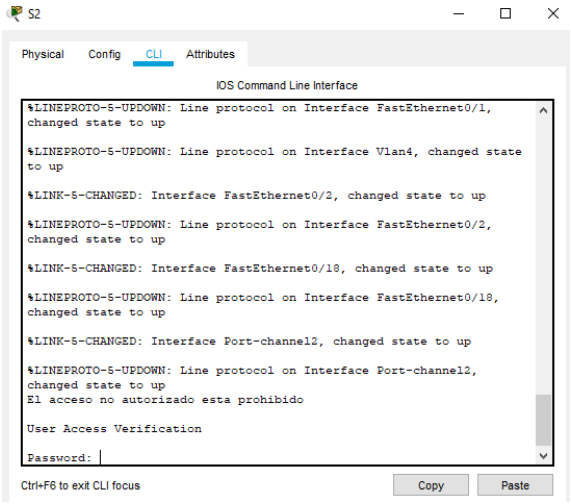


Figura 6. Ingreso al Switch S2 después de las configuraciones básicas

En la figura 7 se observa lo que ocurre si ingresamos mal la contraseña mal más de tres veces, esta no nos deja ingresar y nos muestra el mensaje que configuramos inicialmente "El acceso no autorizado está prohibido"

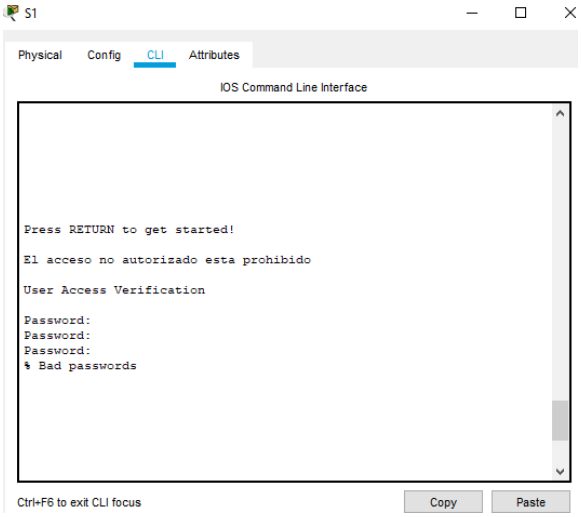


Figura 5. Resultado de ingresar tres veces mal la contraseña

I. Referencias

[1] CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

[2] CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

[3] CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

[4] CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

[5] CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

[6] UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

[7] CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

[8] CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

[9] CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

[10] CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

[11] CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1