DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FREDY ALEXANDER ZAMUDIO

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

FREDY ALEXANDER ZAMUDIO

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

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 padres por su apoyo incondicional.

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.

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),

RIP: (Routing information protocolo, protocolo de información de encaminamiento) RIP es un protocolo de encaminamiento interno, es decir para la parte interna de la red, la que no está conectada al backbone de Internet.

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).

VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

RESUMEN

En el presente informe se aplican las competencias y habilidades que fueron adquiridas a lo largo del diplomado a través de la realización de dos escenarios de redes LAN en los que se configura la creación de VLAN y seguidamente se implementa el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), el protocolo de tiempo de red (NTP) servidor/cliente entre otros, según los requerimientos de cada red con el fin poner en práctica los conocimientos adquiridos para la solución de redes de comunicación.

Palabras clave: Administrar, Habilidades, Cisco, LAN, Protocolo.

ABSTRACT

In this report, the competencies and skills that were acquired throughout the course are applied through the realization of two LAN network scenarios in which the creation of VLANs is configured and then the dynamic routing protocol OSPF is implemented, the dynamic host configuration protocol (DHCP), the server / client network time protocol (NTP) among others, according to the requirements of each network in order to put into practice the knowledge acquired for the communication network solution.

Keywords: Manage, Skills, Cisco, LAN, Protocol.

INTRODUCCIÓN

Este informe tendrá como objetivo administrar dos redes LAN, las cuales están basados en requerimientos habituales en las organizaciones para realizar el transporte de la información y asimismo se desarrollarán con el fin de poner en práctica lo aprendido por medio del programa de Cisco Packet Tracer. Inicialmente se identificarán las redes, su topología y requerimientos de configuraciones en los dispositivos que conforman la red. Se realizará una investigación bibliográfica sobre los protocolos de red para el desarrollo de cada una de estas. se realizará el desarrollo de cada topología, con las configuraciones de los dispositivos y se verificación de las mismas.

Para esto se redactará el respectivo informe que contará con el procedimiento de realización de los dos escenarios, permitiendo así que el estudiante tenga el conocimiento y pueda ponerlo en práctica de una forma práctica y legible.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar la configuración de dos redes LAN por medio del software cisco packet tracer

2.2 OBJETIVOS ESPECÍFICOS

Identificar las herramientas de supervisión y protocolos de administración de red.

Realizar las topologías de las redes a administrar.

Configurar las topologías según los requerimientos indicados.

Evaluar el desempeño de routers y switches.

3. DESARROLLO DE LA PRUEBA DE HABILIDADES

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

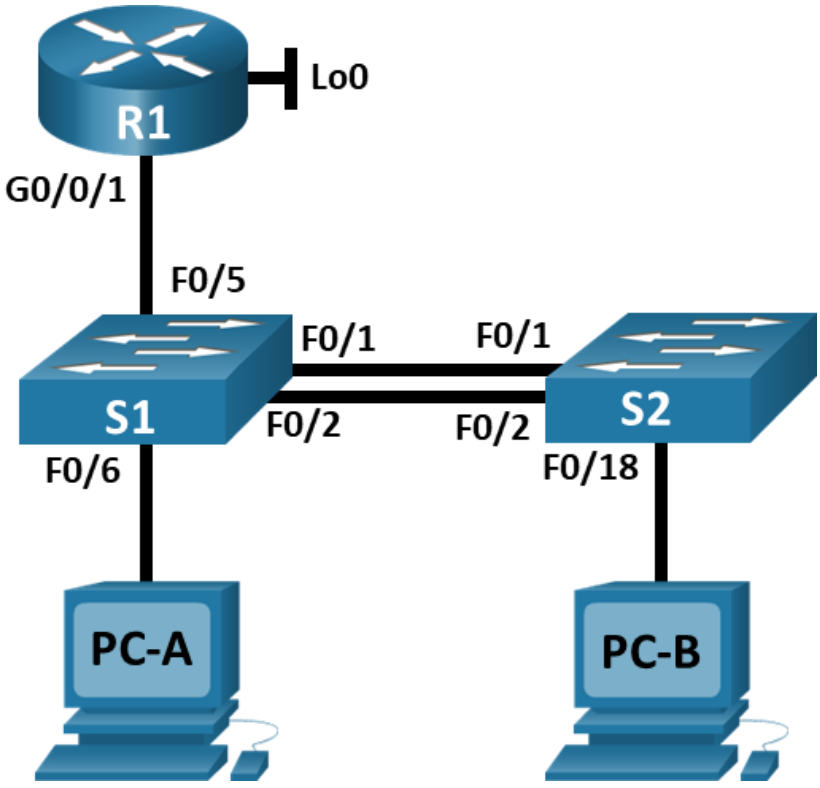


Figura 1 Topología del primer escenario

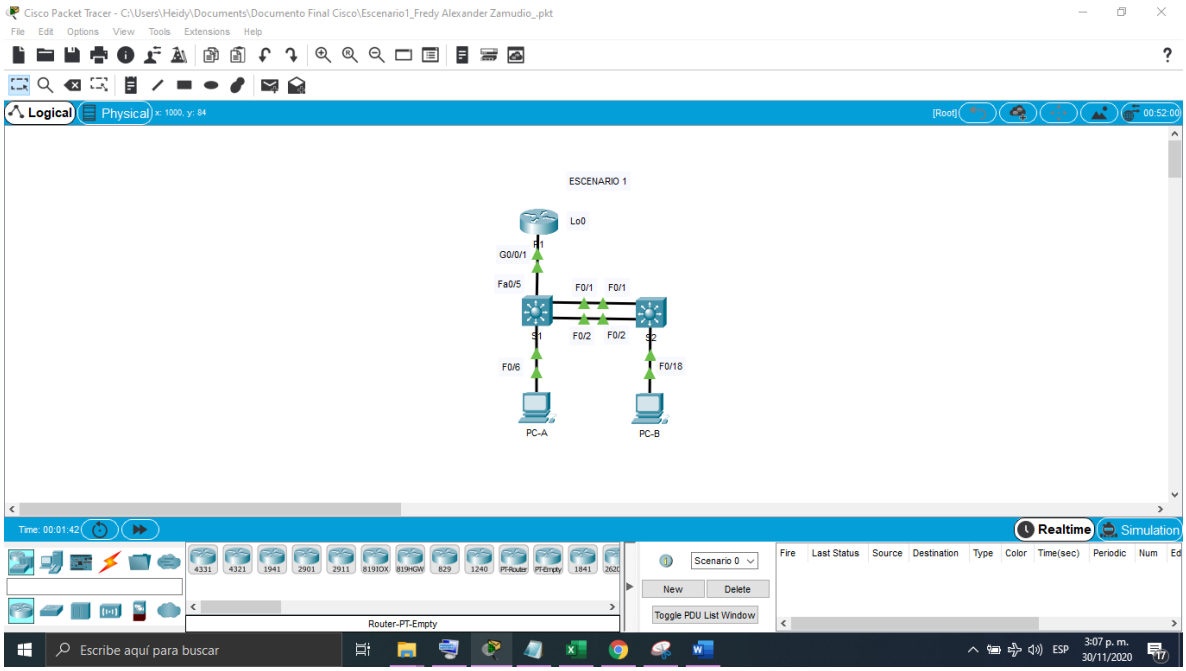


Figura 2 Topologia en la pantalla principal del software cisco packet tarcer

A continuación, se muestra la tabla 1, que nos muestra las VLAN que se van a crear con el correspondiente nombre que se le asignara

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

En la siguiente tabla, se encuentran las direcciones IPv4 e IPv6 correspondientes a cada dispositivo de la red y puerto de enlace de la misma.

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

EL procedimiento de desarrollo del escenario, se realiza por medio de las partes que encontramos a continuación

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 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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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 siguientes:

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

Las tareas de configuración para R1 incluyen las siguientes:

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

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	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

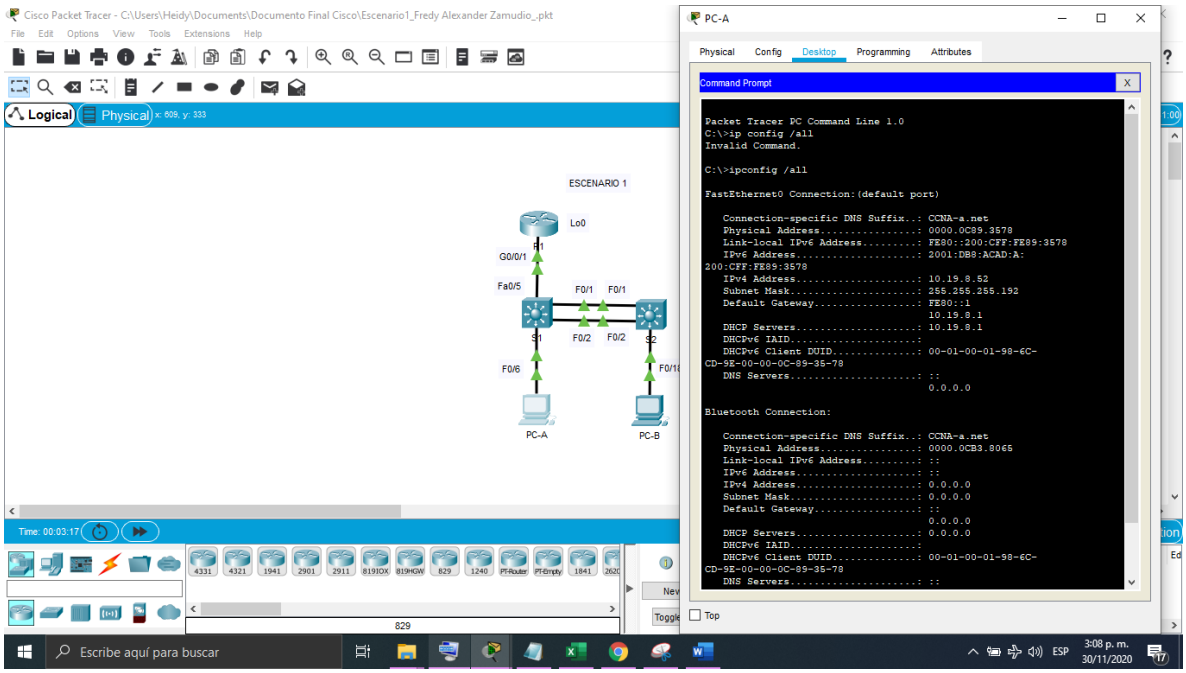


Figura 3 Verificación de la configuración de red de PC-A

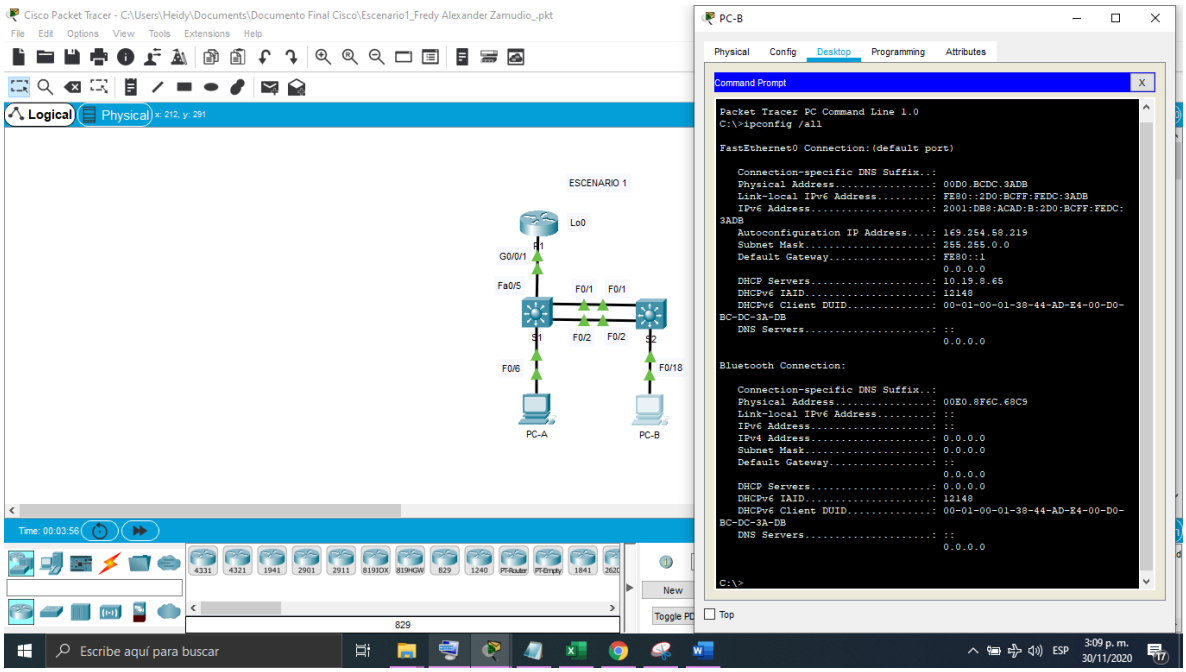


Figura 4 Verificación de la configuración de red de PC-B

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 5)
	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 5)
	R1, G0/0/1.3	Dirección	10.19.8.65	Reply from 10.19.8.65:bytes=32 time=3ms TL=255 (Ver figura 6)
	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 6)
	R1, G0/0/1.4	Dirección	10.19.8.97	Reply from 10.19.8.97: bytes=32 time=1ms TTL=255 (Ver figura 7)
	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 7)
	S1, VLAN 4	Dirección	10.19.8.98	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 8)
	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 8)
	S2, VLAN 4	Dirección	10.19.8.99	Reply from 10.19.8.99: bytes=32 time=3ms TTL=254 (Ver figura 9)
	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 9)

	PC-B	Dirección	169.254.58.219	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 10)
	PC-B	IPv6	2001:db8:acad:b: :50	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 10)
	R1 Bucle 0	Dirección	209.165.201.1	Reply from 209.165.201.1: bytes=32 time=6ms TTL=255 (Ver figura 11)
	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 (Ver figura 11)
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 12)
	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	Reply from 2001:DB8:ACAD:209::1: bytes=32 time=12ms TTL=255 (Ver figura 12)
	R1, G0/0/1.2	Dirección	10.19.8.1	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 13)
	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 13)
	R1, G0/0/1.3	Dirección	10.19.8.65	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 14)
	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 14)
	R1, G0/0/1.4	Dirección	10.19.8.97	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 15)
	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 15)
	S1, VLAN 4	Dirección	10.19.8.98	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 16)
	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254

				(Ver figura 16)
	S2, VLAN 4	Dirección	10.19.8.99	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 17)
	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254 (Ver figura 17)

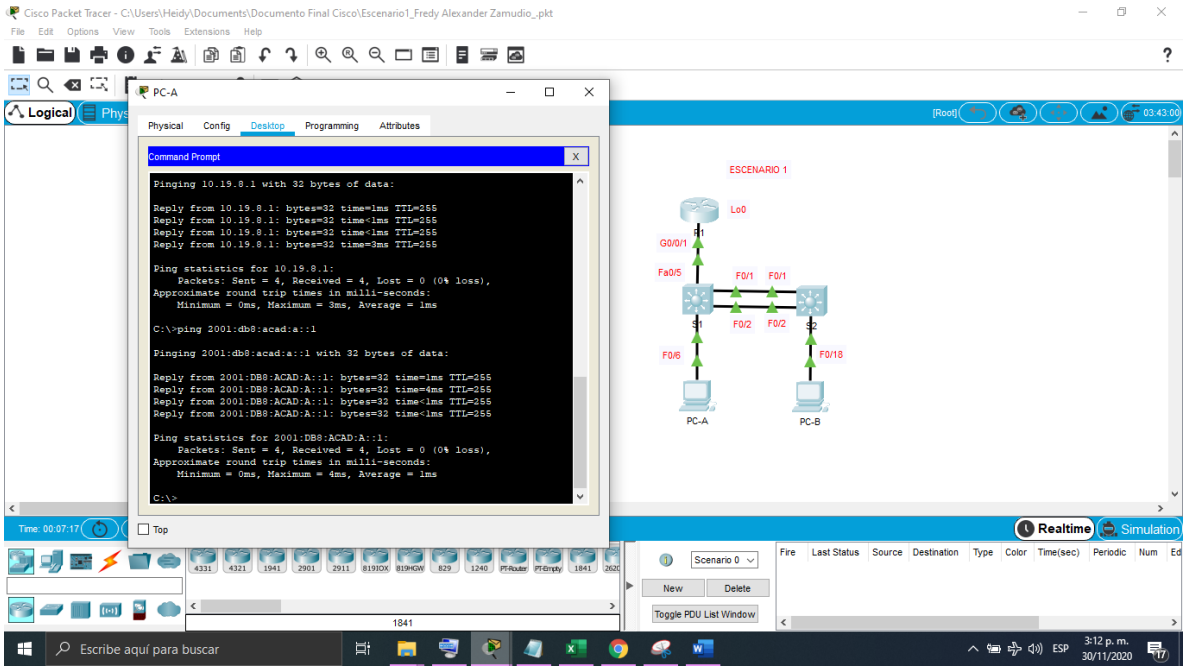


Figura 5 Verificación de conectividad en PC-A a R1 G0/0/1.2

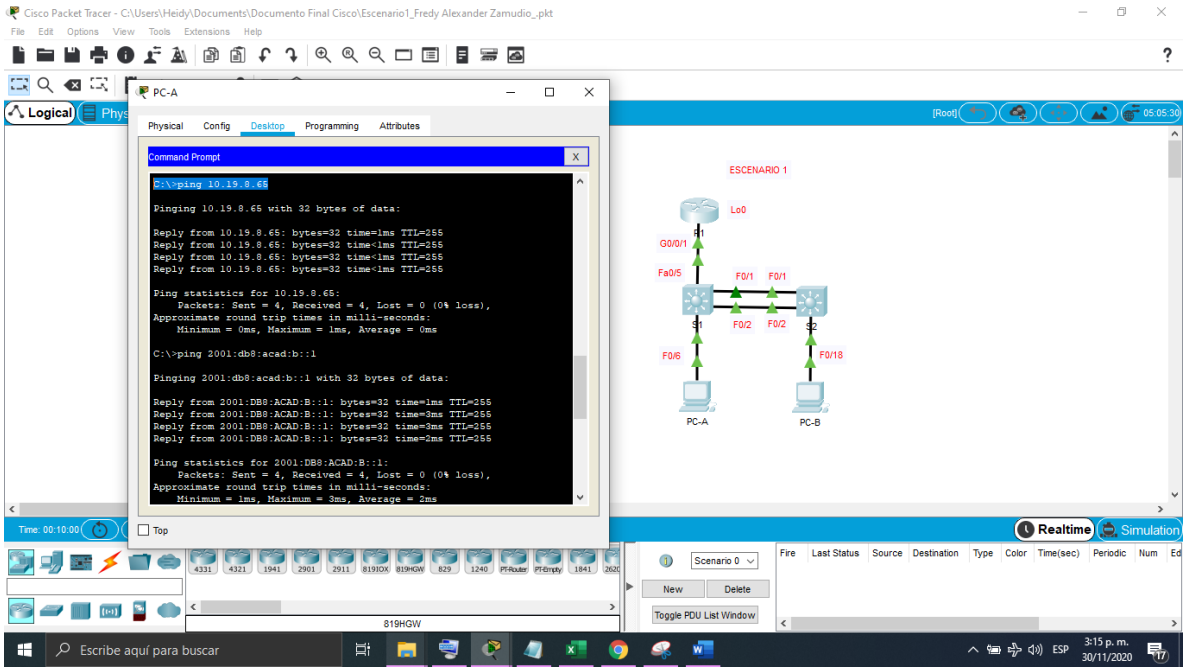


Figura 6 Verificación de conectividad en PC-A a R1 G0/0/1.3

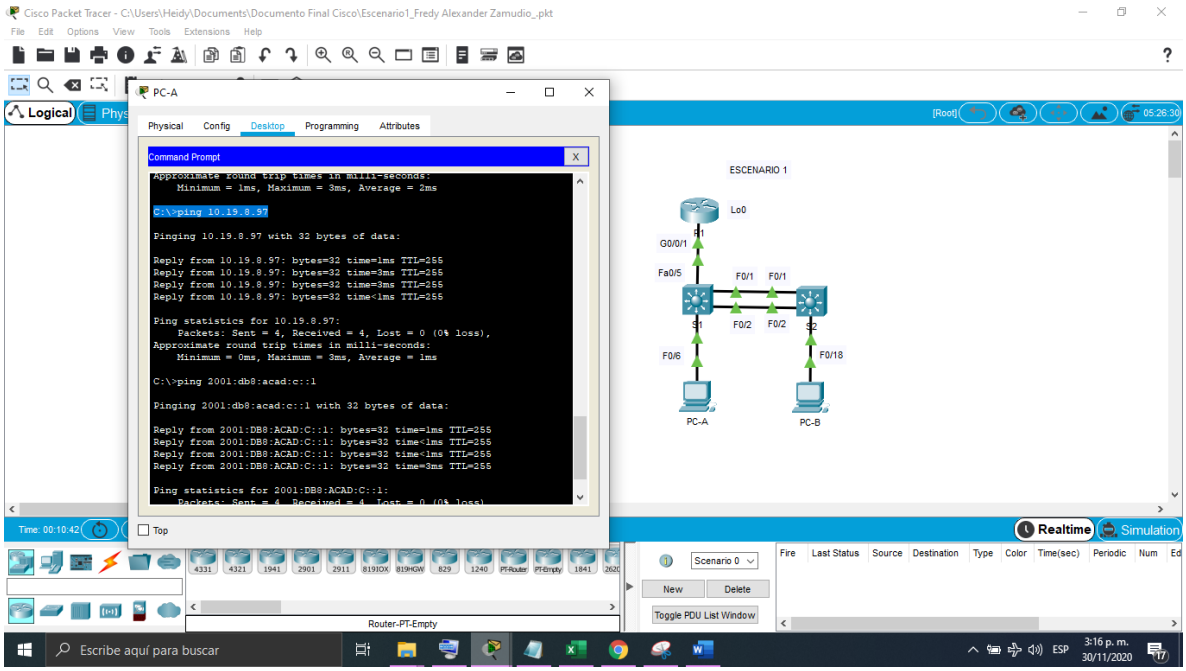


Figura 7 Verificación de conectividad en PC-A a R1 G0/0/1.4

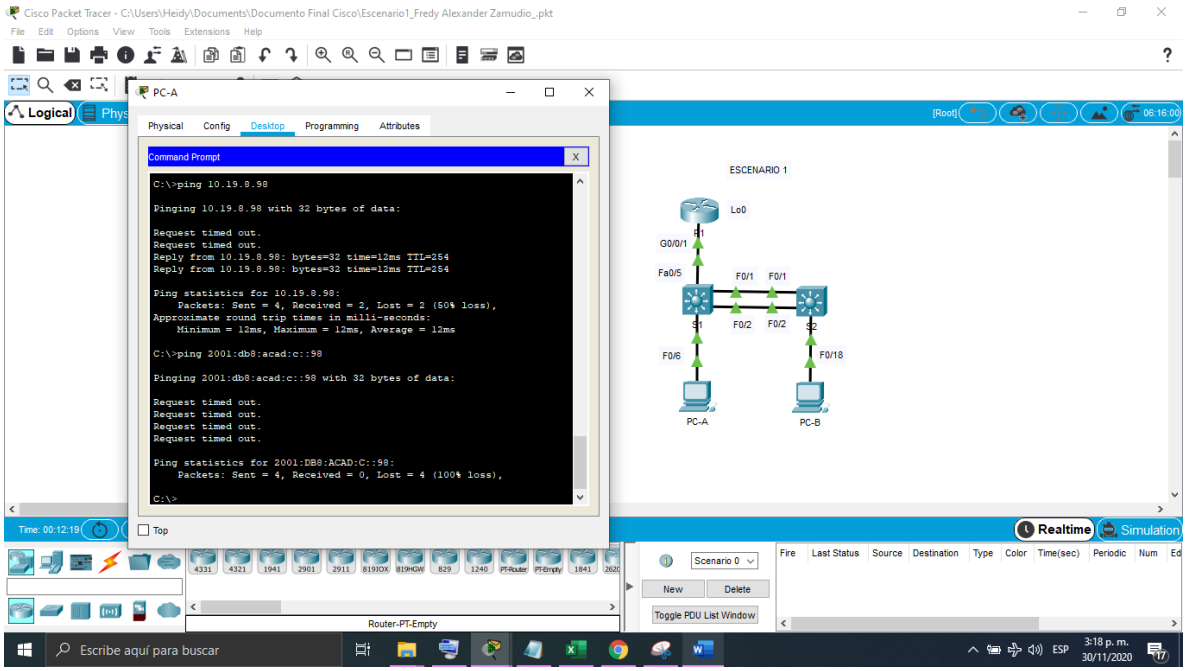


Figura 8 Verificación de conectividad en PC-A a S1 VLAN 4

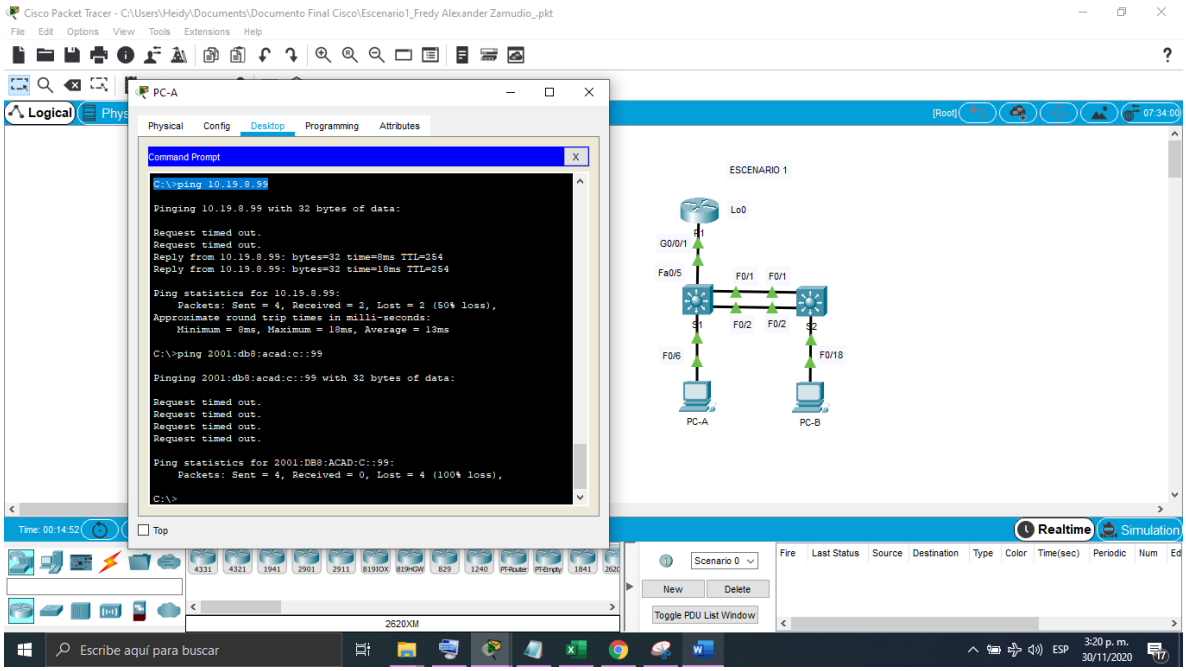


Figura 9 Verificación de conectividad en PC-A a S2 VLAN 4

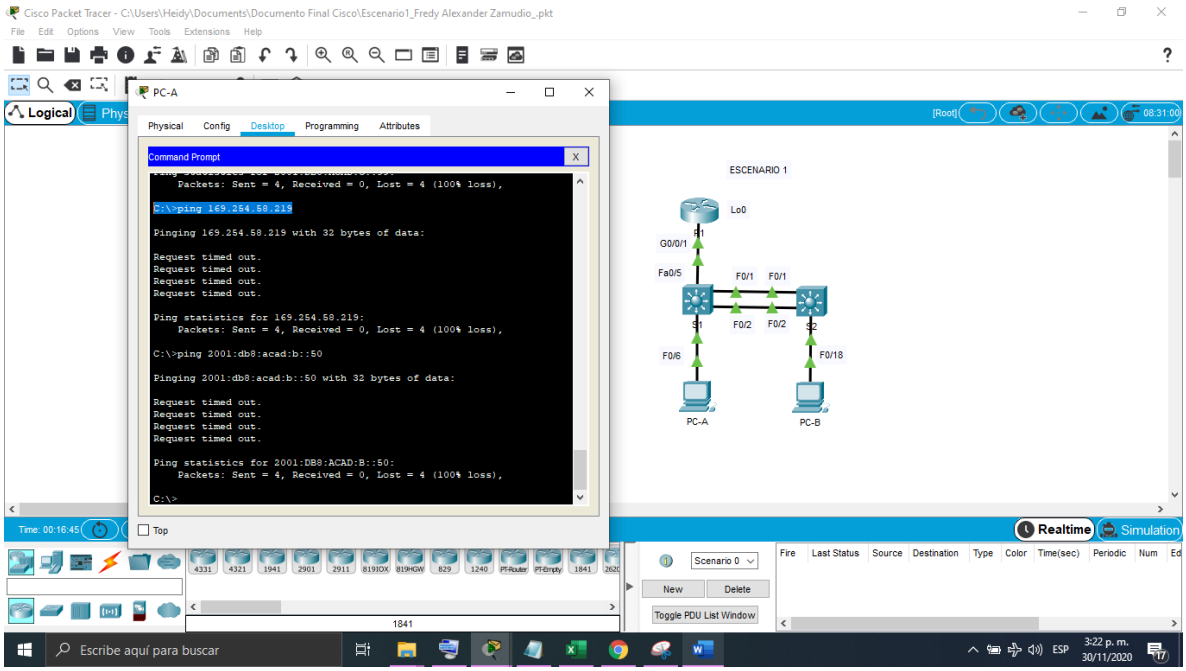


Figura 10 Verificación de conectividad en PC-A a PC-B

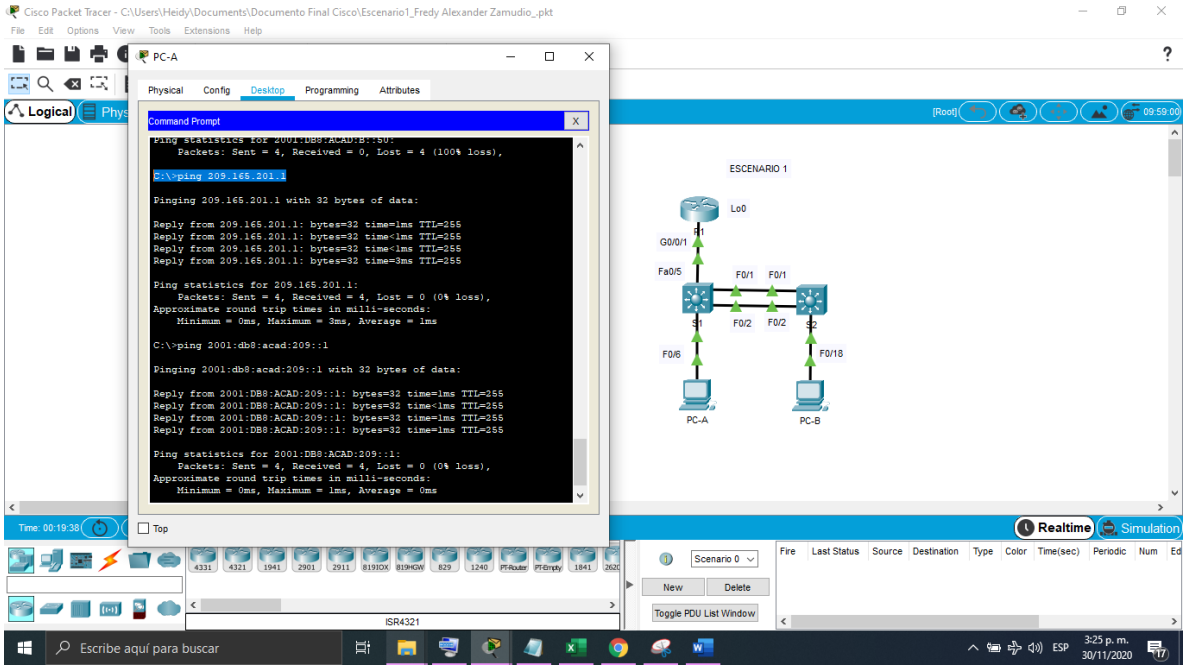


Figura 11 Verificación de conectividad en PC-A a R1 bucle 0

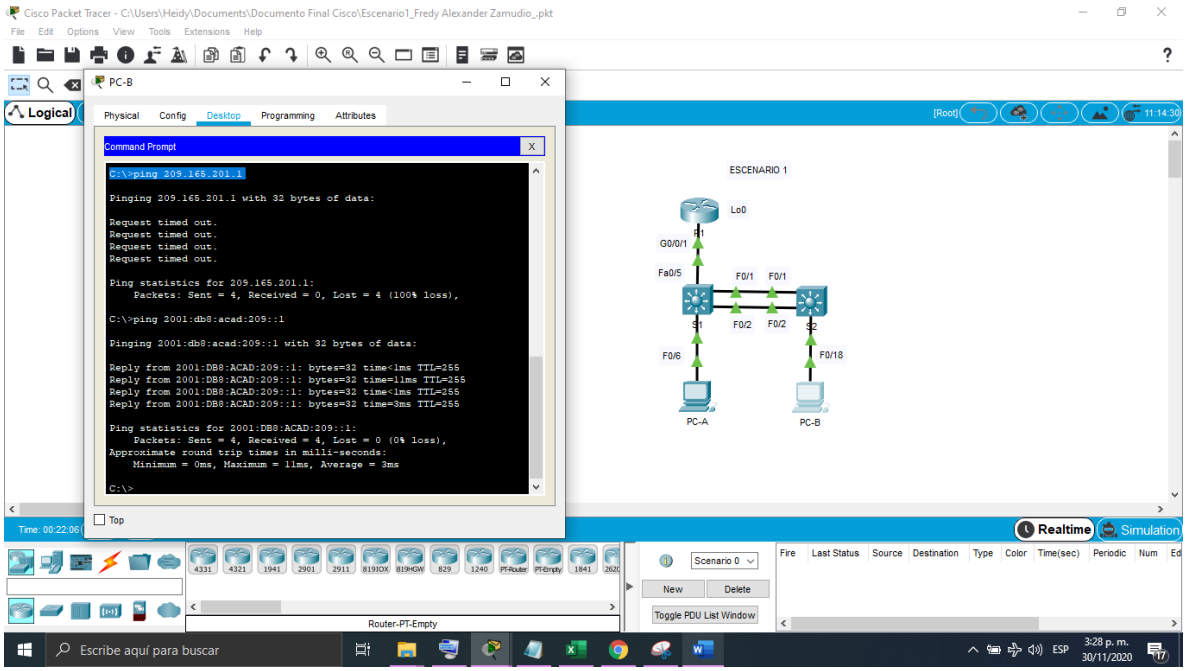


Figura 12 Verificación de conectividad en PC-B a R1 bucle 0

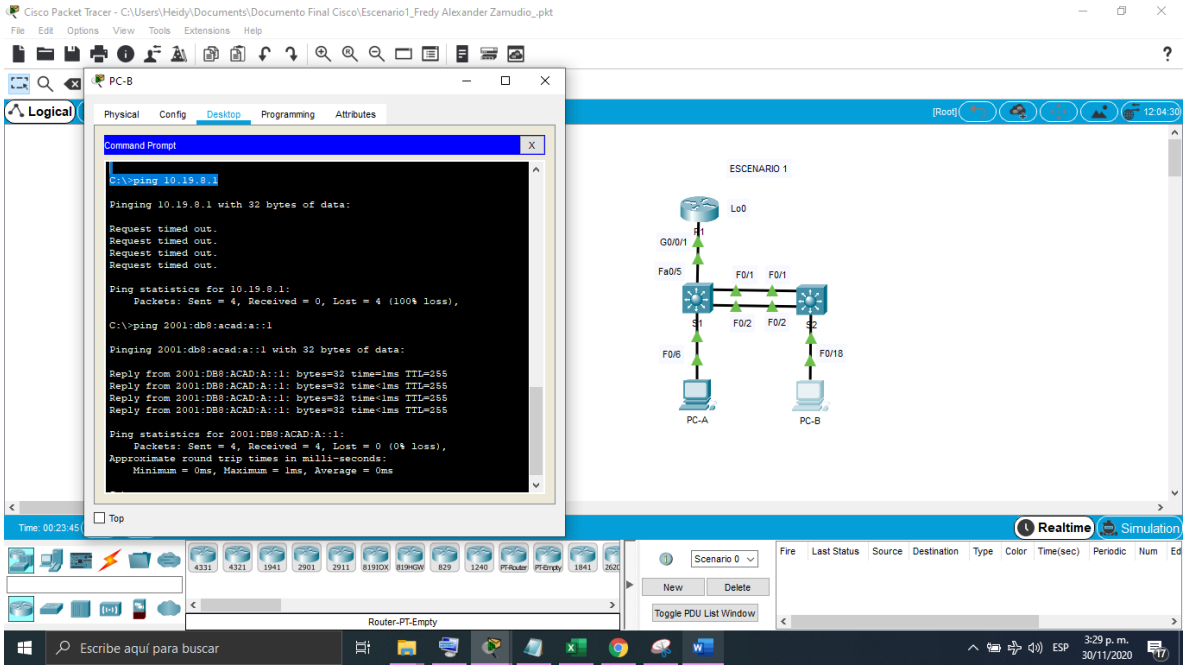


Figura 13 Verificación de conectividad en PC-B a R1 G0/0/1.2

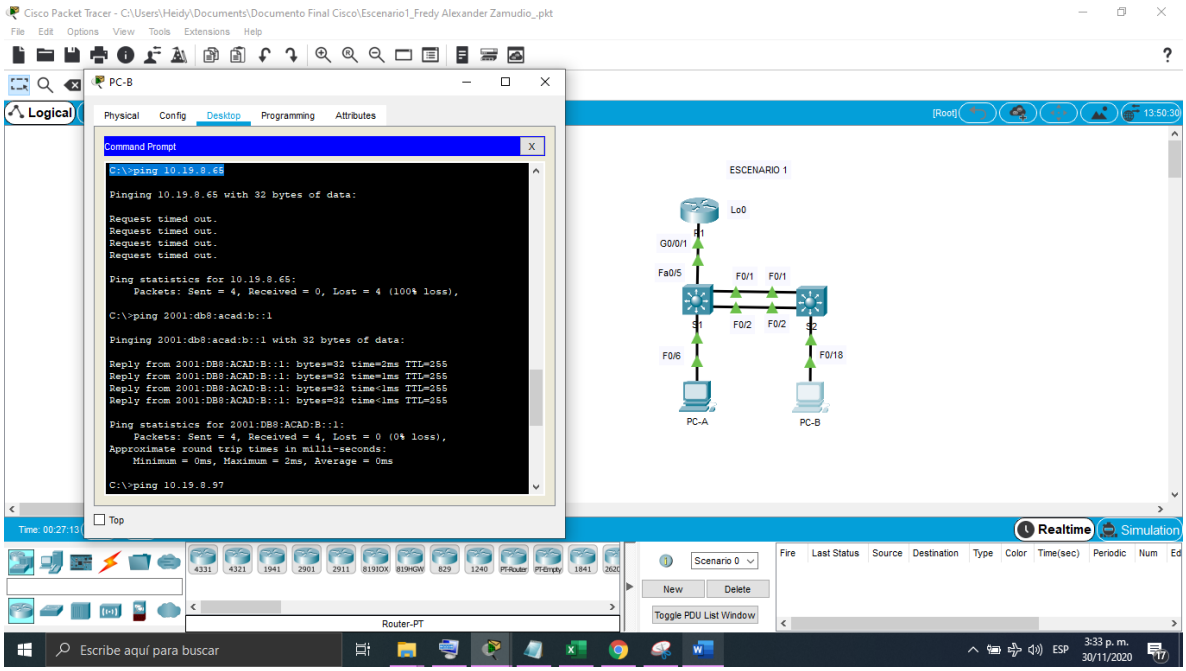


Figura 14 Verificación de conectividad en PC-B a R1 G0/0/1.3

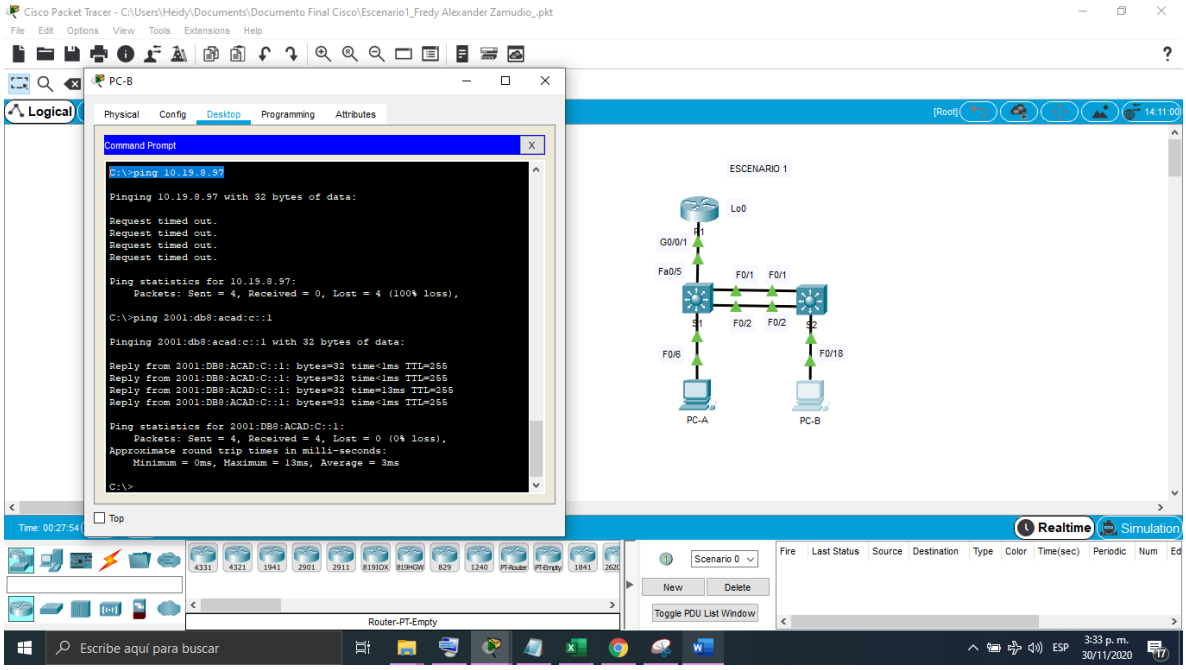


Figura 15 Verificación de conectividad en PC-B a R1 G0/0/1.4

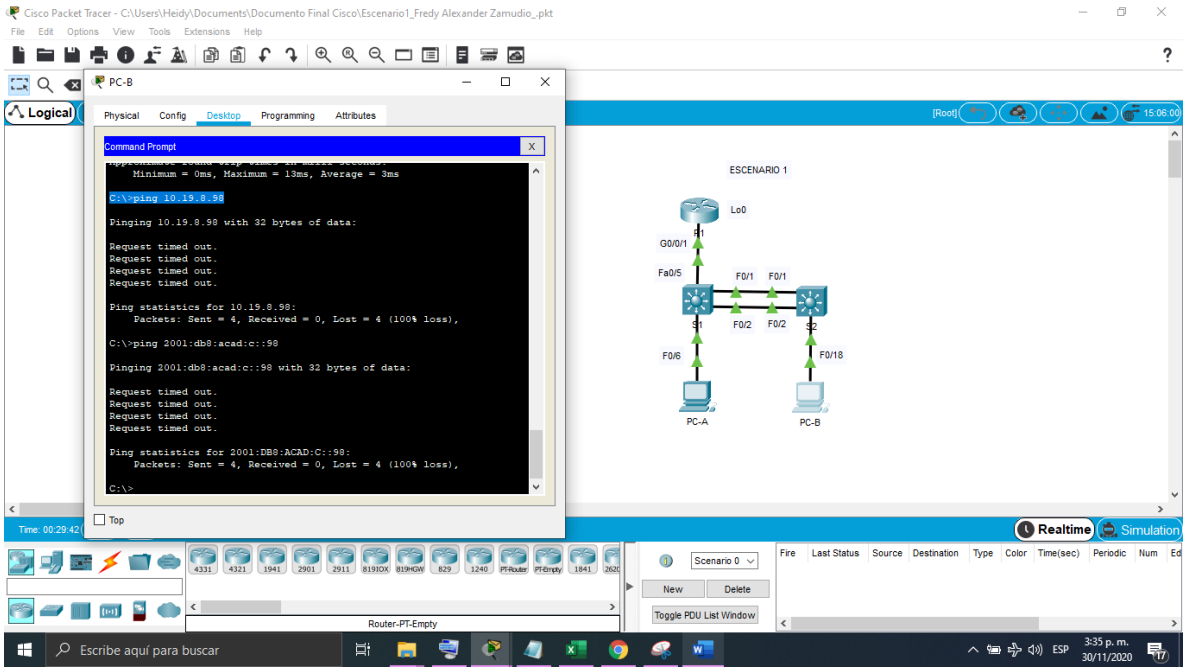


Figura 16 Verificación de conectividad en PC-B a S1 VLAN 4

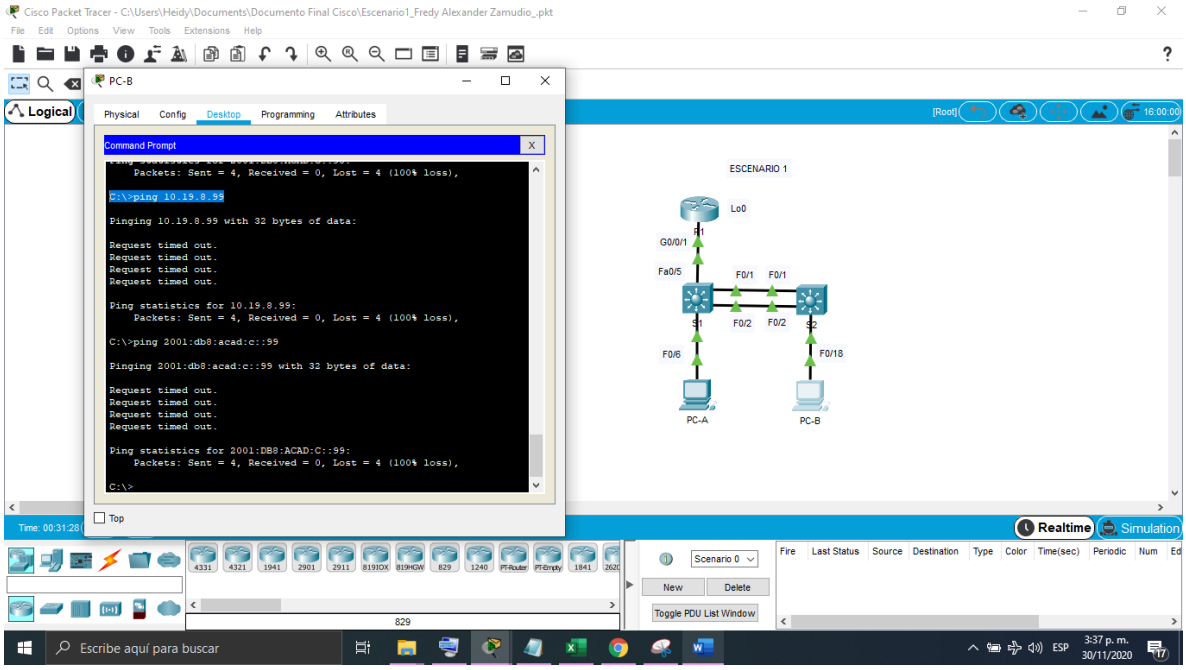


Figura 17 Verificación de conectividad en PC-B a S2 VLAN 4

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

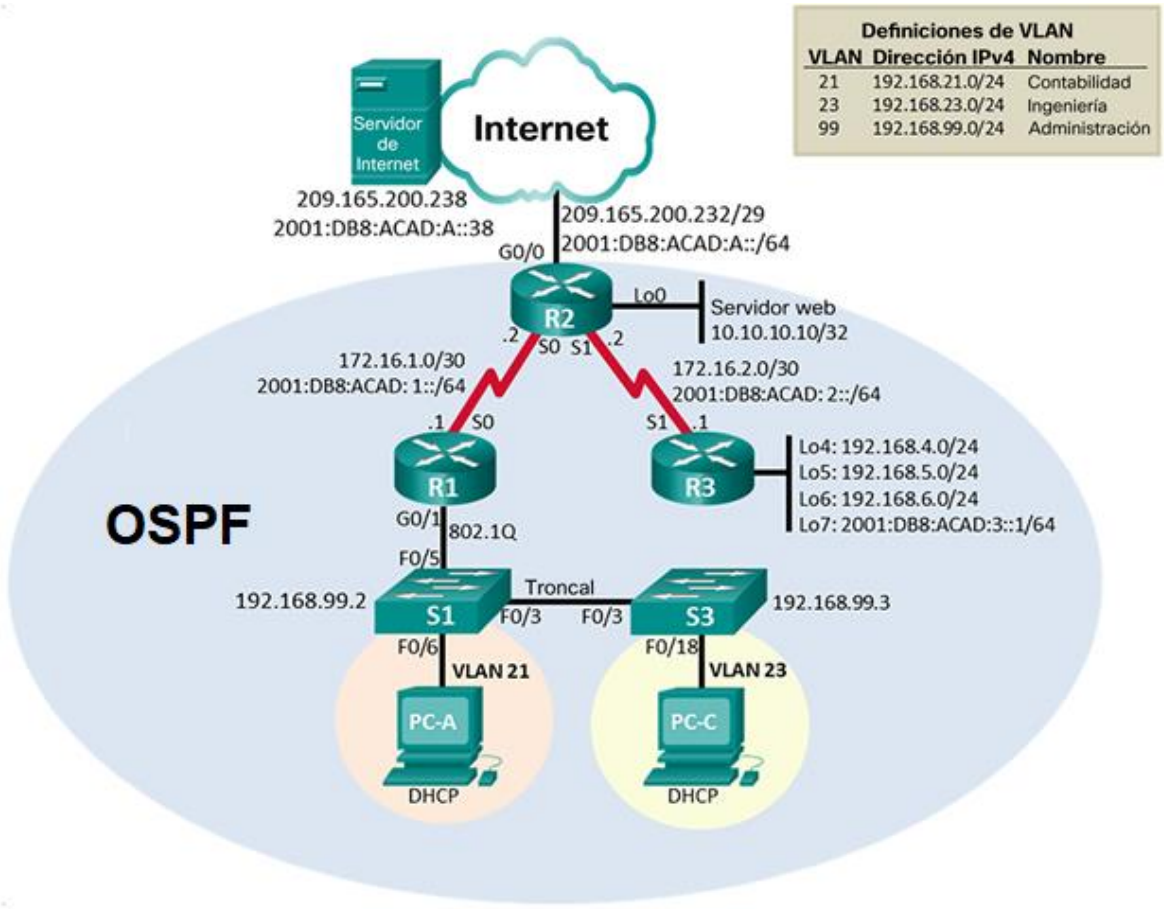


Figura 18 Topología del segundo escenario

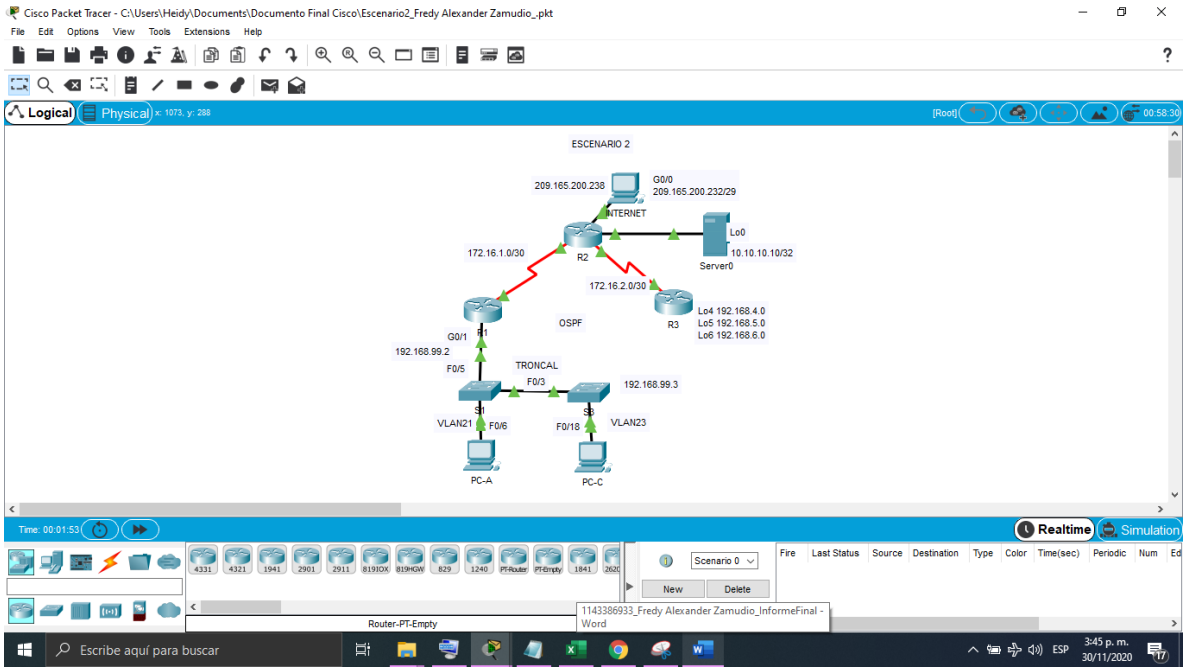


Figura 19 Topología realizada en la pantalla principal del software cisco packet tracer

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 y por medio de los siguientes comandos.se realizan las configuraciones de formateo y reinicio tanto en los Routers como en los Switch.

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

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

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

Tabla 12 Indicaciones para configurar la computadora red internet

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13 Configuraciones básicas de R1 en el segundo escenario

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

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	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 incluye las siguientes tareas:

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

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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 15 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:

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

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	172.16.1.2	R1#ping 172.16.1.2 Success rate is 100 percent(5/5), round-trip min/avg/max = 1/9/38 ms (Ver figura 20)
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 21)
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 22)

Tabla 17 Verificación de conectividad de la red

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

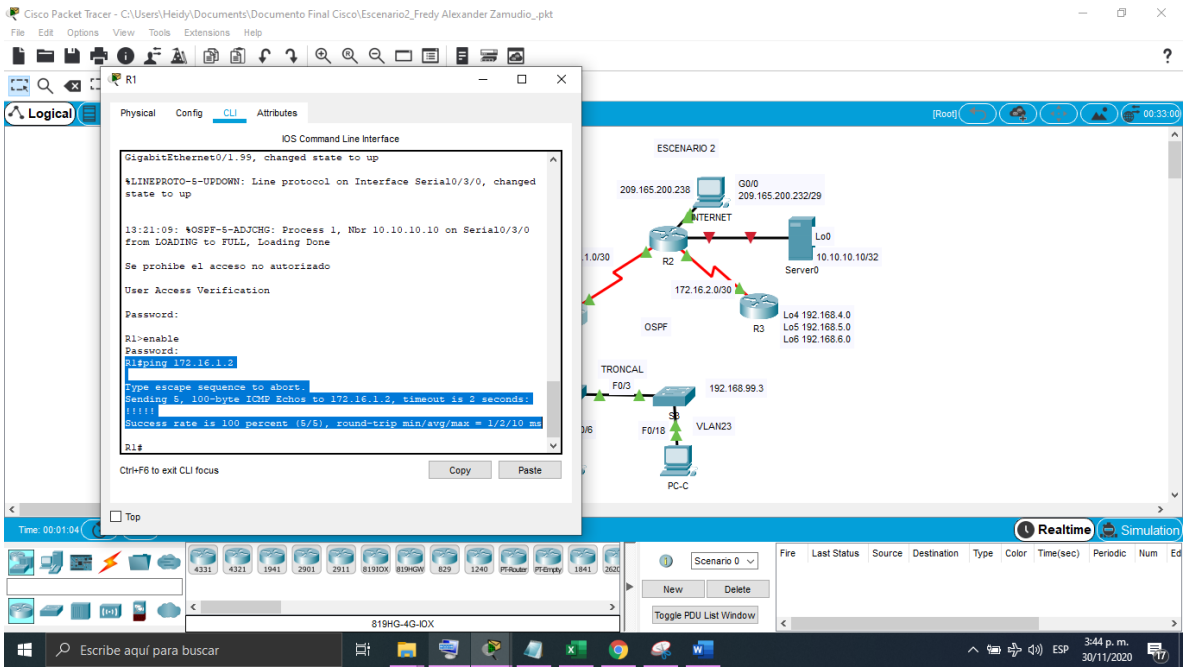


Figura 20 Verificación de conexión de red desde R1 a R2 S0/0/0

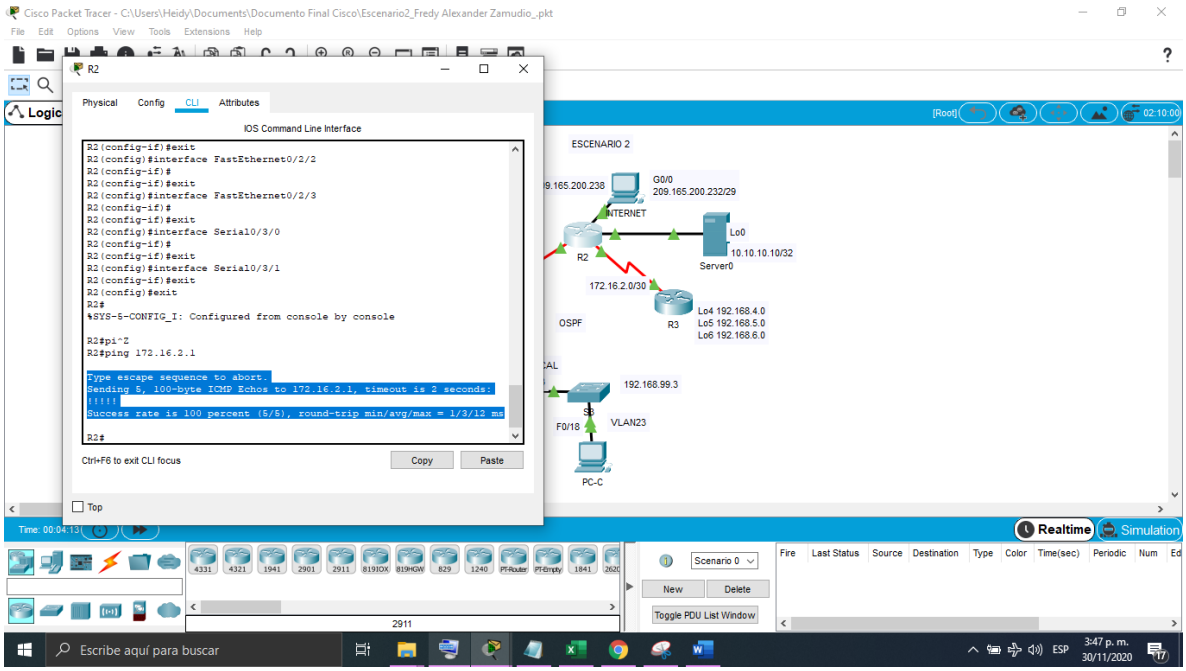


Figura 21 Verificación de conexión de red desde R2 a R3

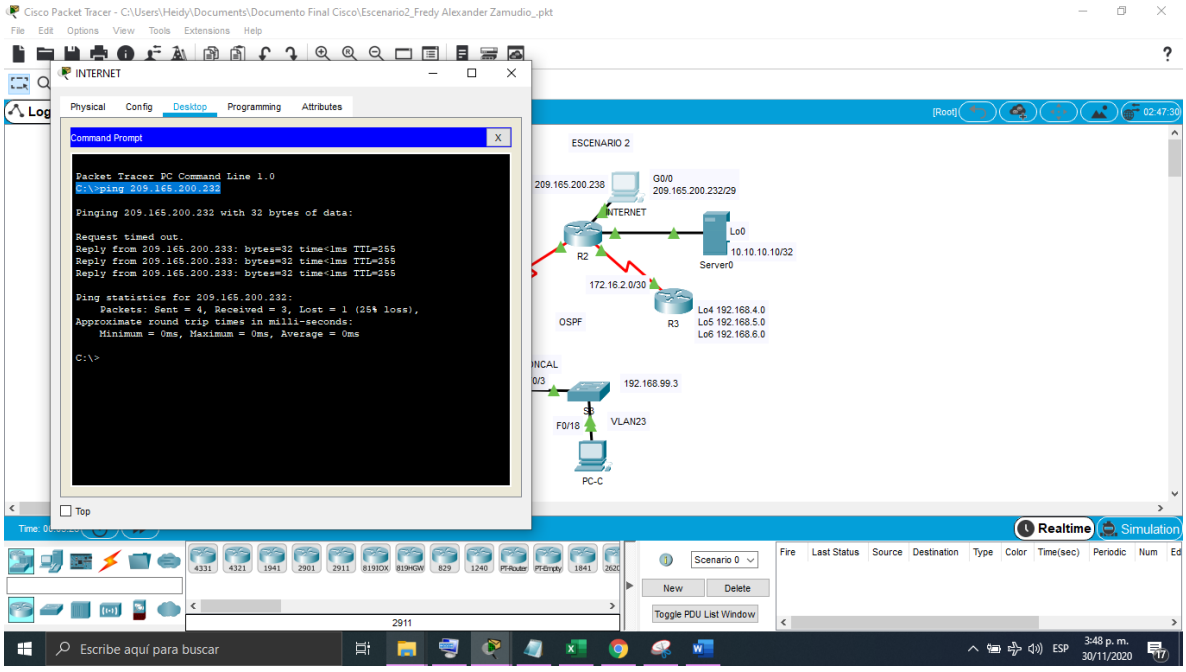


Figura 22 Verificación de conexión de red desde PC Internet a gateway predeterminado

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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

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	S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name 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 21	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 19 Configuración de la seguridad del switch y el routing entre las vlan de S3 con su respectivo comando

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 G0/1	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 20 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

Utilice el comando **ping** para probar la conectividad entre los switches y el R1 y 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	192.168.99.1	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 21 Verificación de conectividad de la red

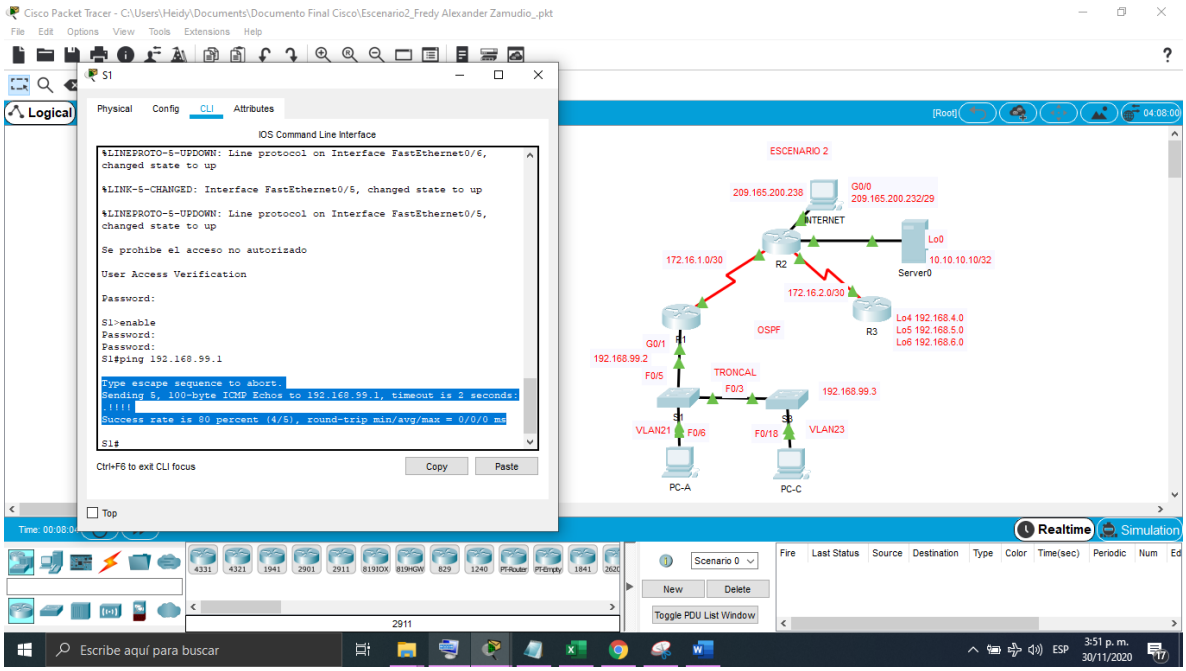


Figura 23 Verificación de conexión de red desde S1 a R1 dirección VLAN 99

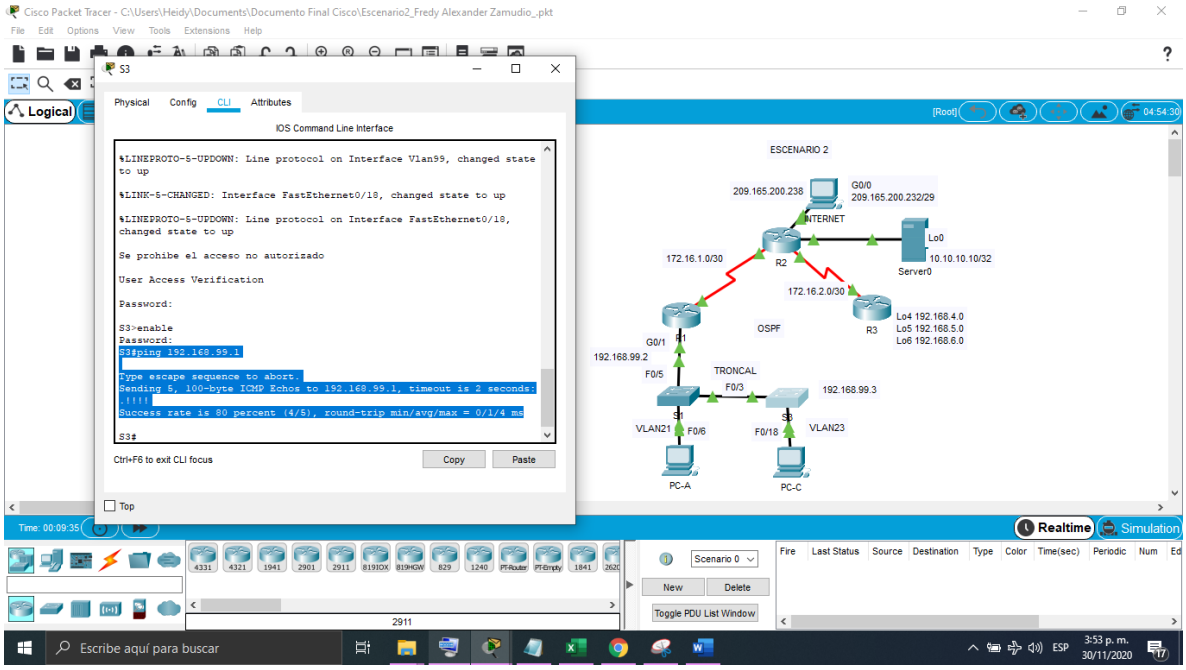


Figura 24 Verificación de conexión de red desde S3 a R1 dirección VLAN 99

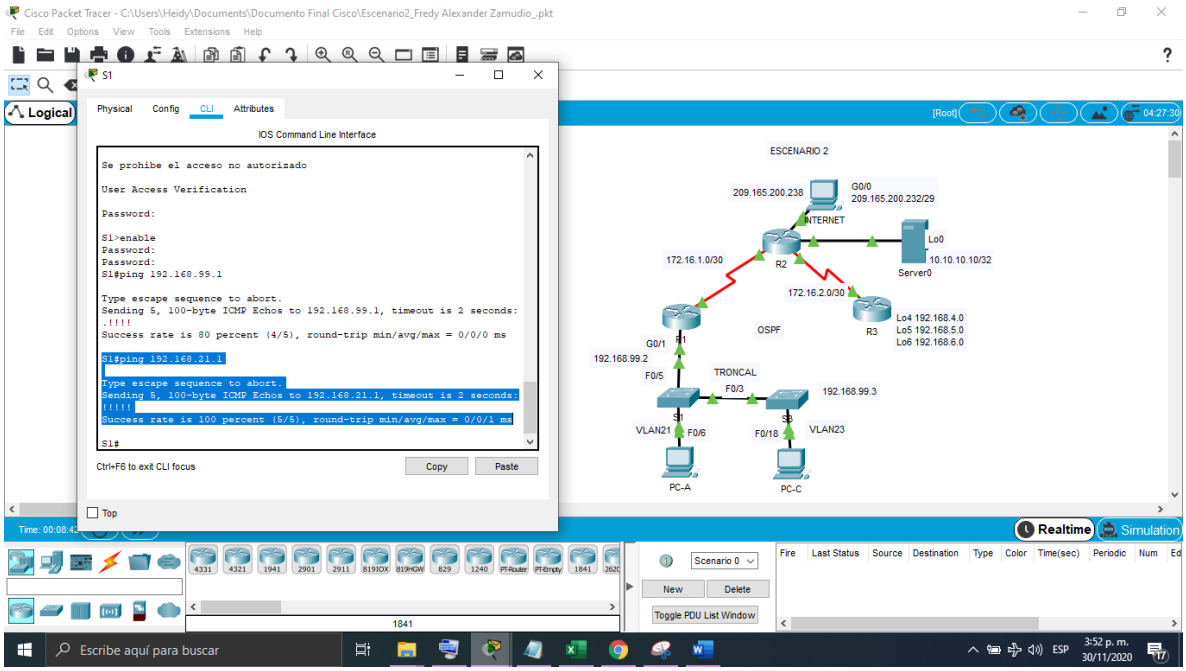


Figura 25 Verificación de conexión de red desde S1 a R1 dirección VLAN 21

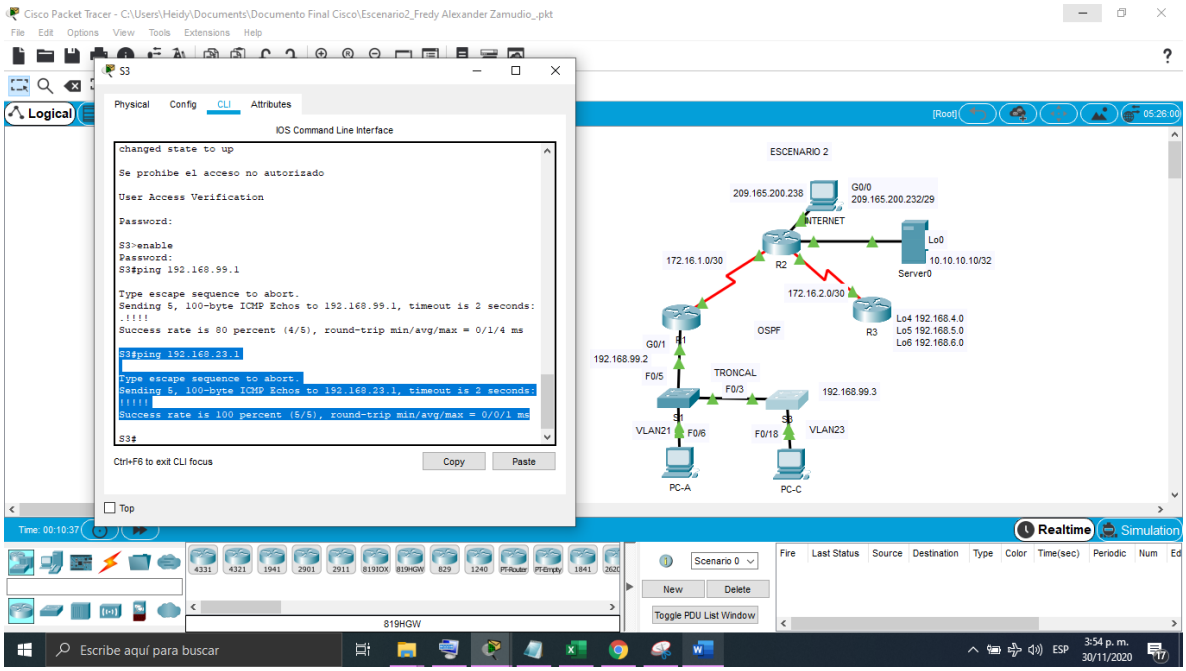


Figura 26 Verificación de conexión de red desde S3 a R1 dirección VLAN 23

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes

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 22 Configuración OSPF en el R1 con su respectivo comando

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

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 23 Configuración OSPF en el R2 con su respectivo comando

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas

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 24 Configuración OSPF en el R3 con su respectivo comando

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 protocols R2#Show ip protocols R3#Show ip protocols (Ver figura 27,28,29)
¿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 33,34,35)

Tabla 25 Verificar la información de OSPF con su respectivo comando

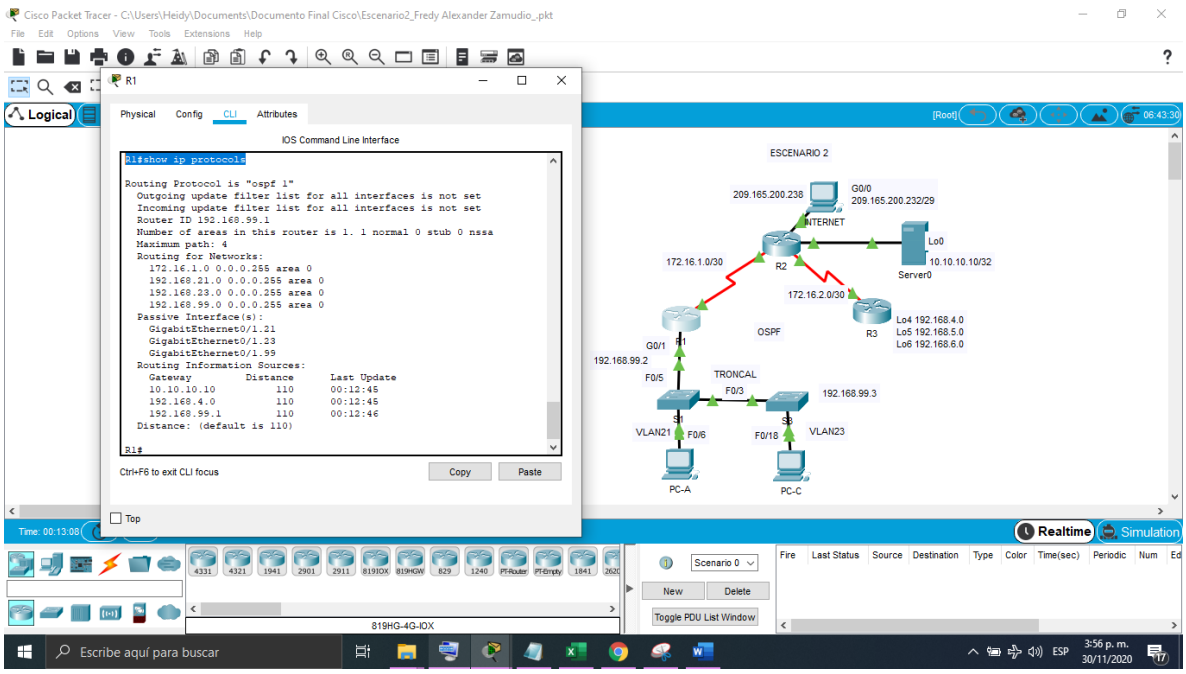


Figura 27 Verificar la información de OSPF en R1 usando el comando Show ip protocols

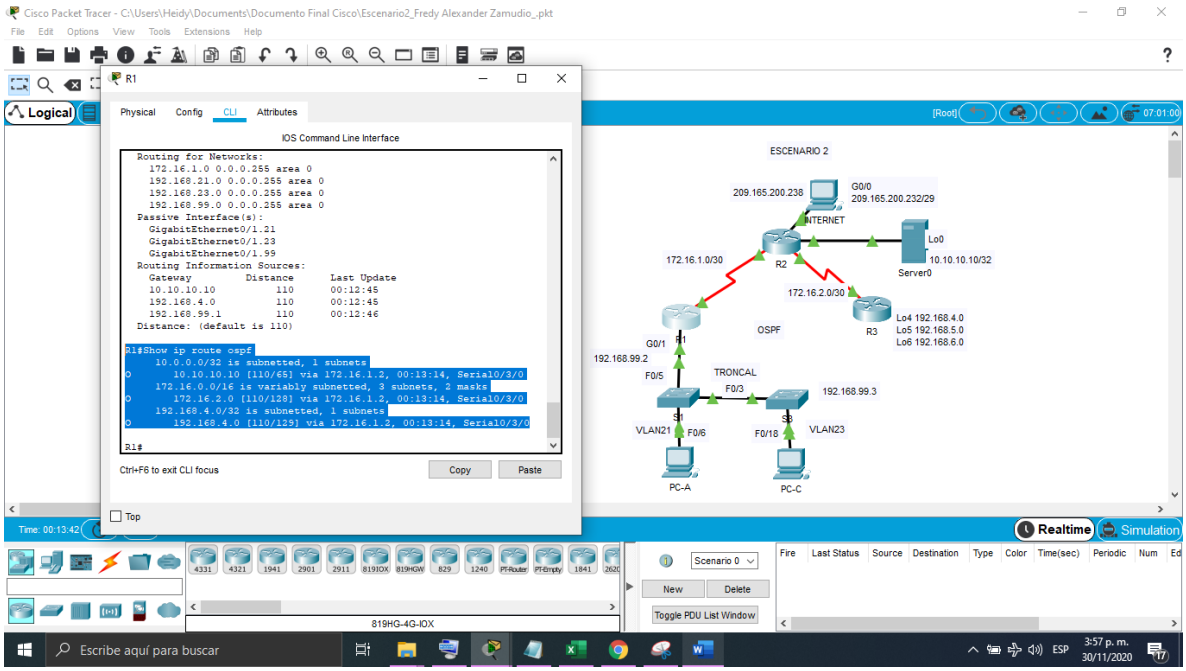


Figura 28 Verificar la información de OSPF en R1 usando el comando Show ip route ospf

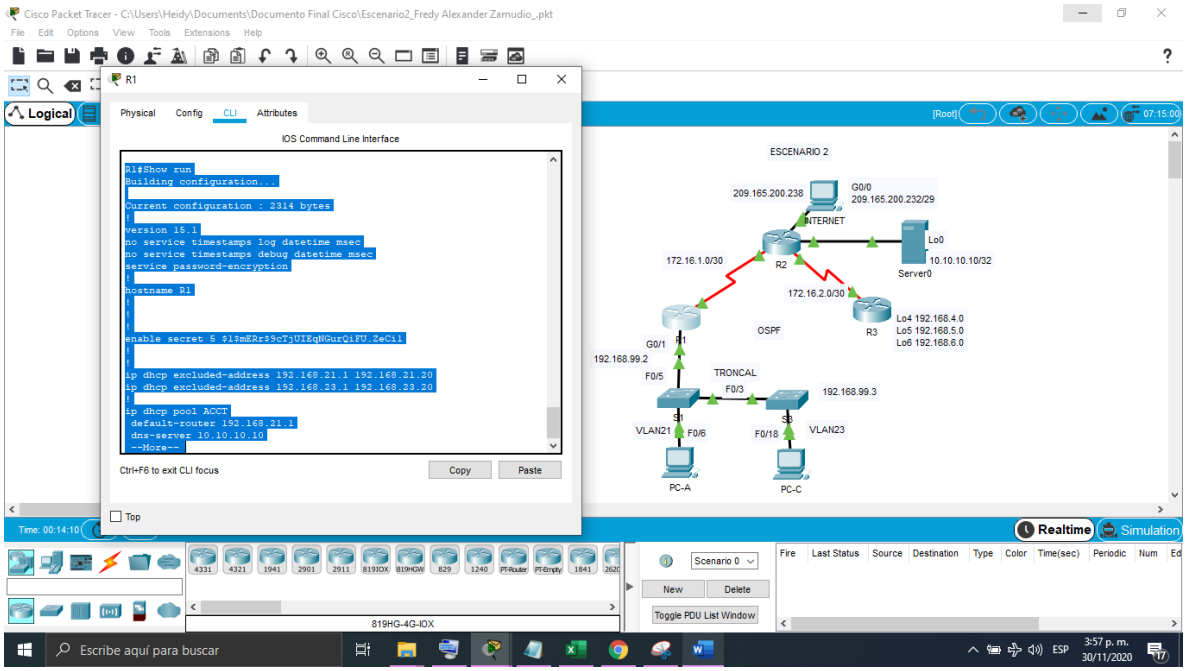


Figura 29 Verificar la información de OSPF en R1 usando el comando Show run

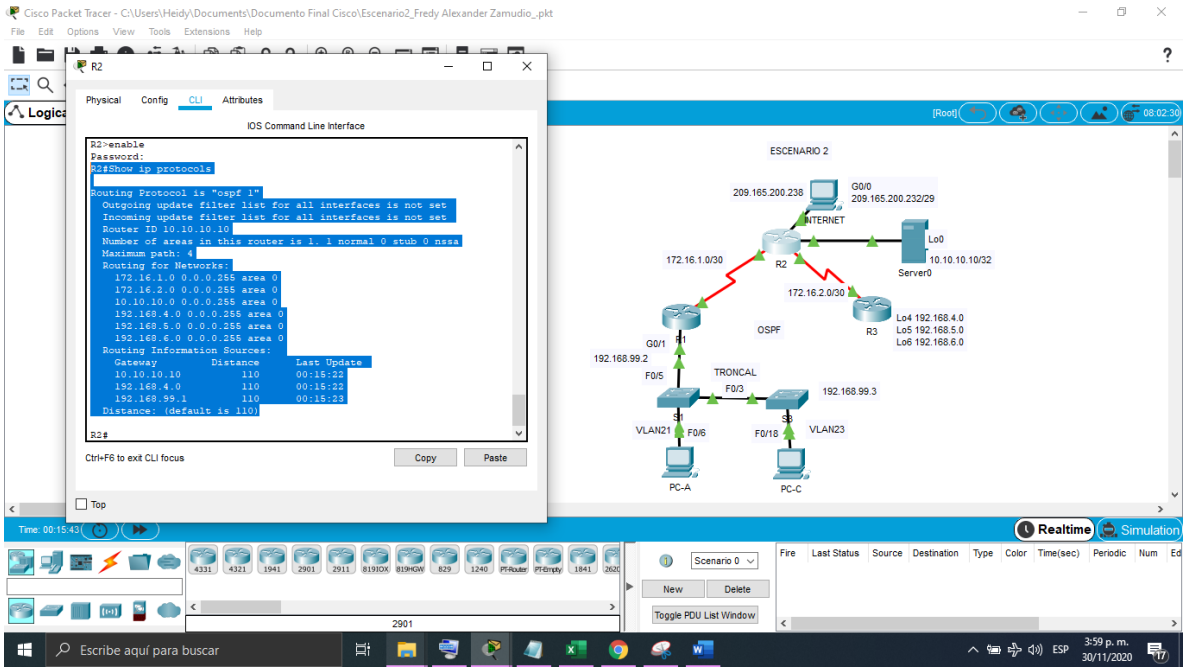


Figura 30 Verificar la información de OSPF en R2 usando el comando Show ip protocols

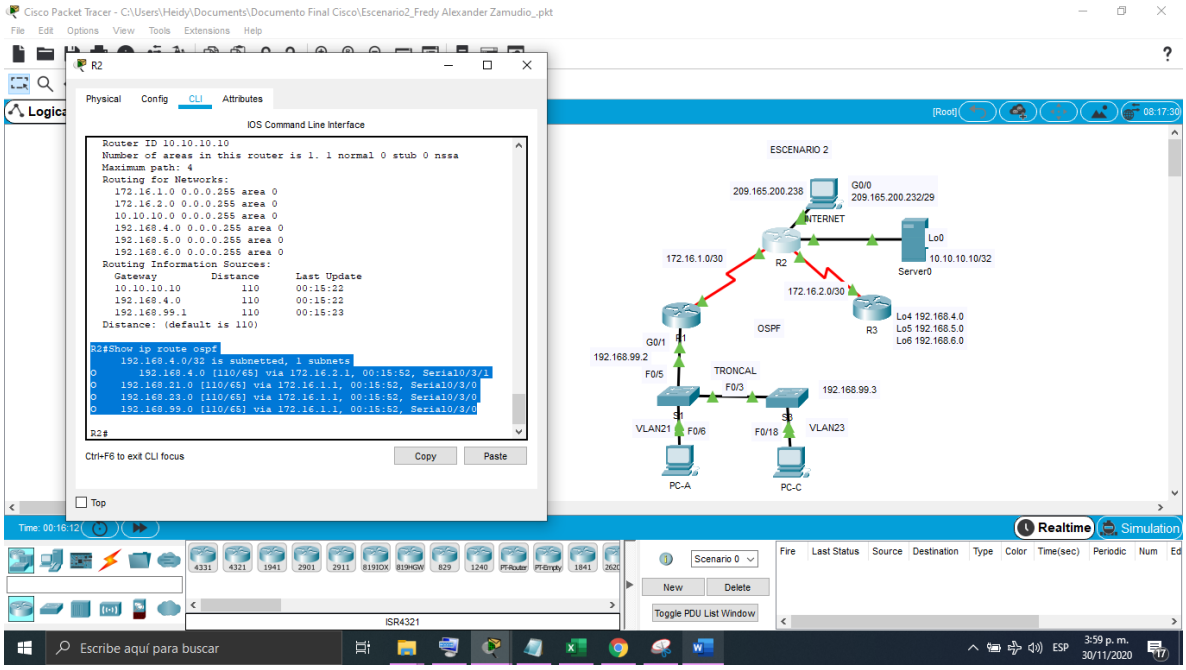


Figura 31 Verificar la información de OSPF en R2 usando el comando Show ip route ospf

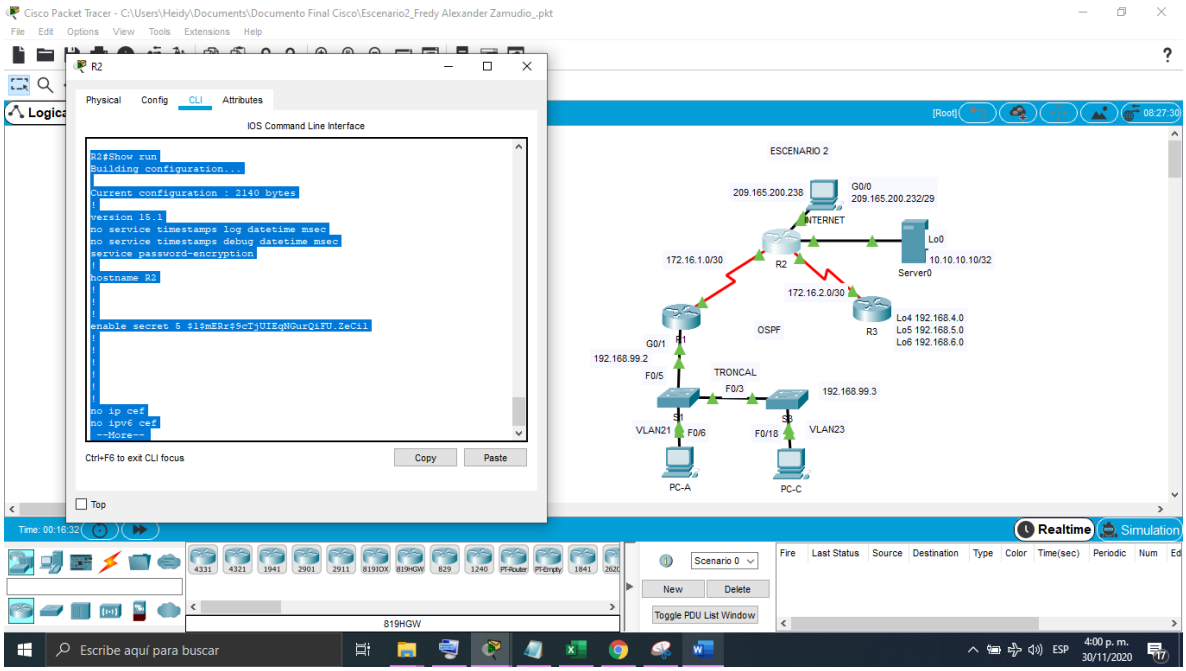


Figura 32 Verificar la información de OSPF en R2 usando el comando Show run

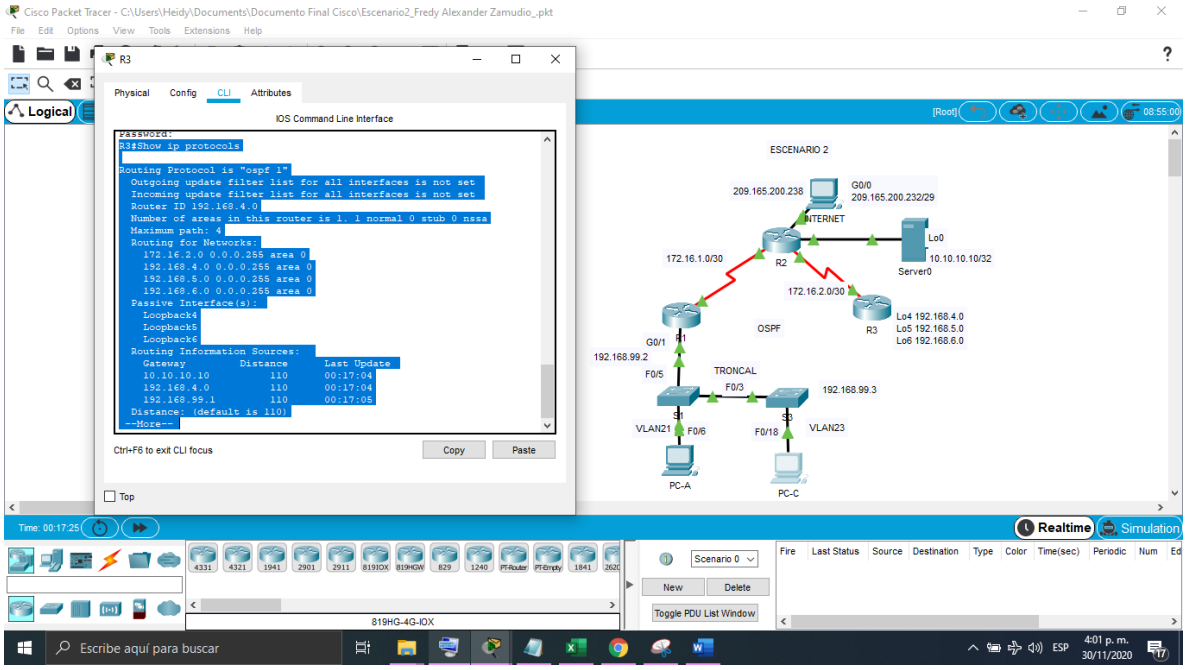


Figura 33 Verificar la información de OSPF en R3 usando el comando Show ip protocols

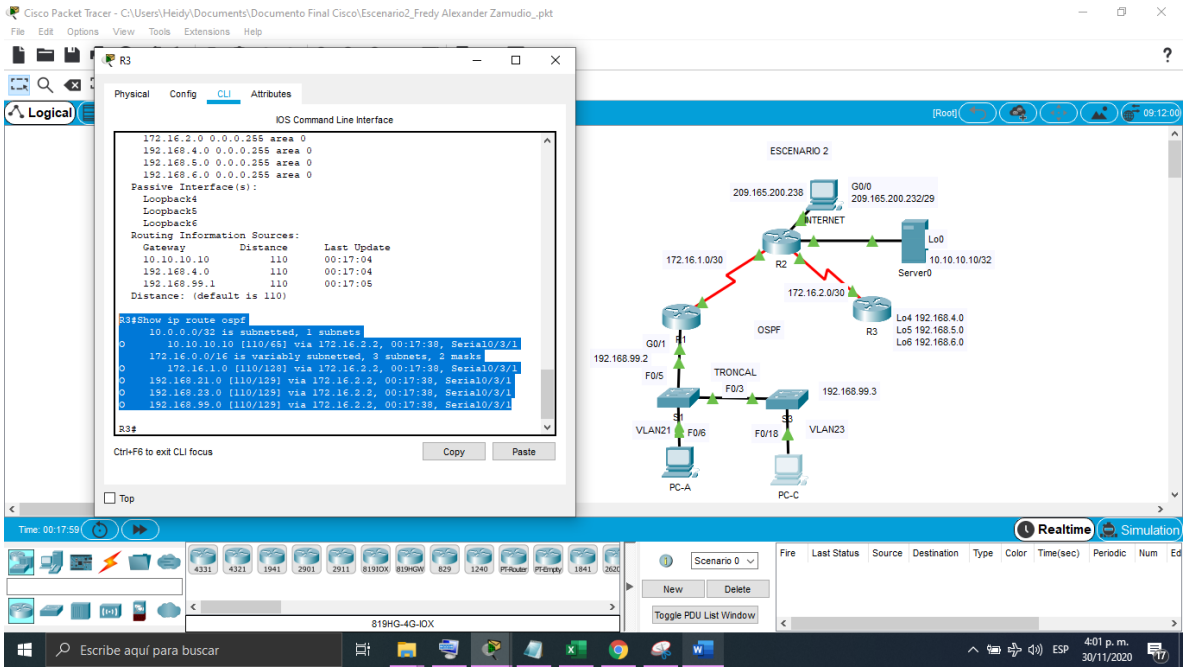


Figura 34 Verificar la información de OSPF en R3 usando el comando Show ip route ospf

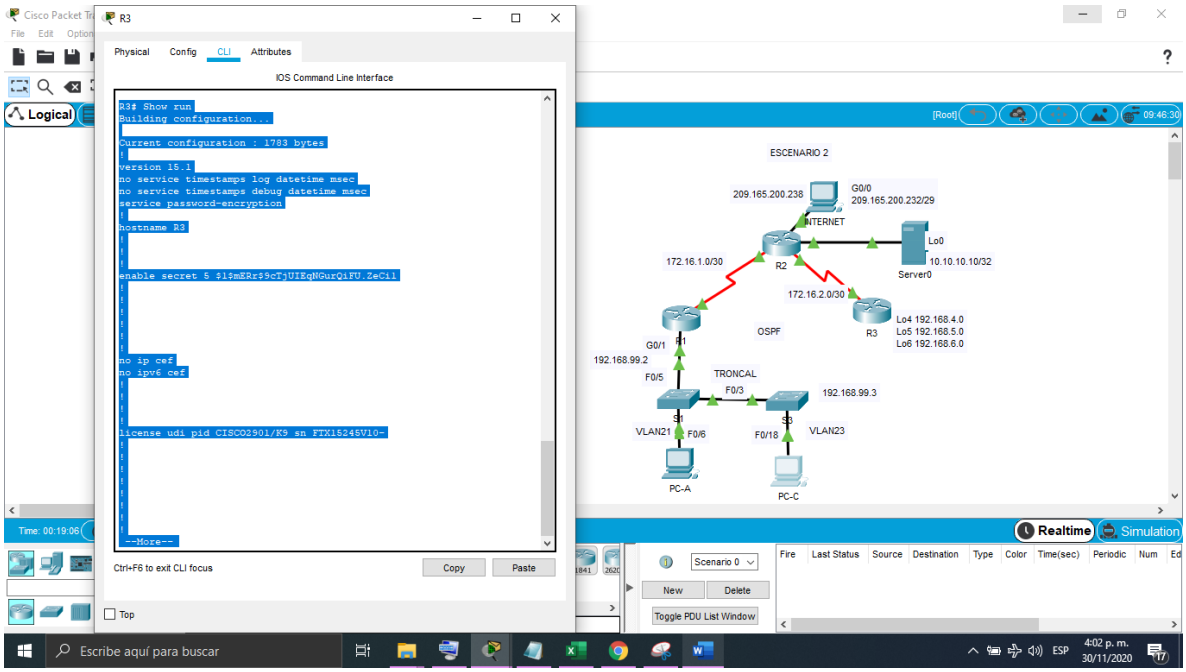


Figura 35 Verificar la información de OSPF en R3 usando el comando Show run

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

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

Las tareas de configuración para R1 incluyen las siguientes:

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 26 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 configuración del R2 incluye las siguientes tareas:

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 27 Configuración NAT en R2 para IPV4 con su respectivo comando

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	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 Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Successful
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 28 Verificación del protocolo DHCP y NAT estática

Parte 6: Configurar NTP

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 29 Configuración NTP

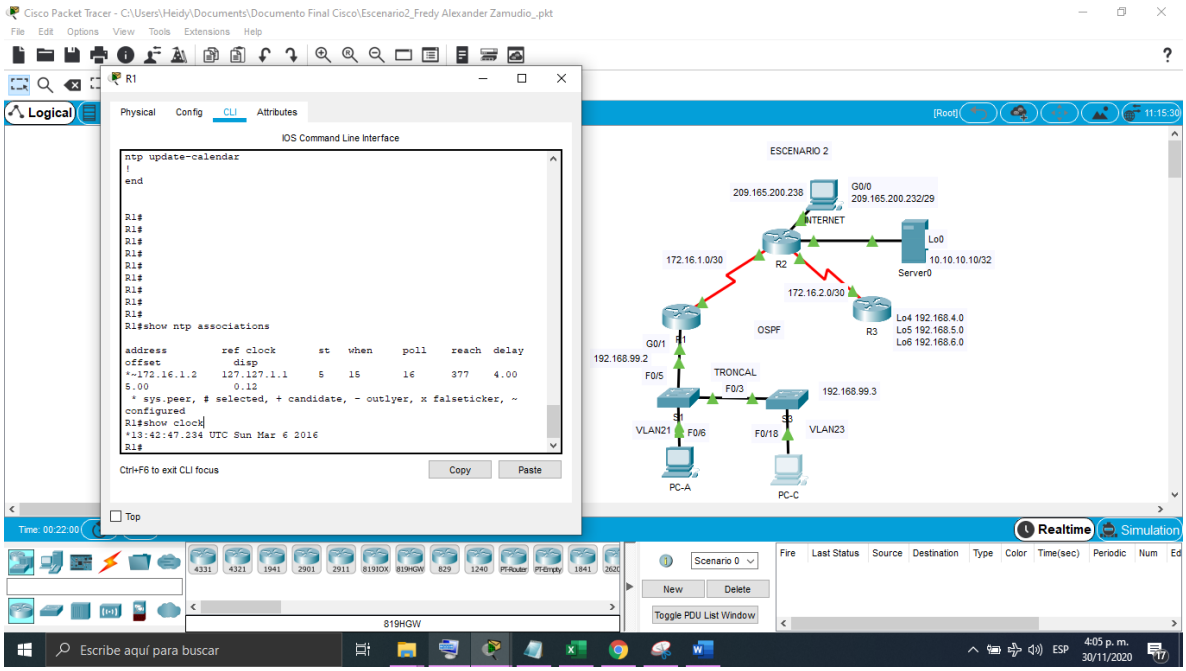


Figura 36 Verificación de la configuración NTP

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

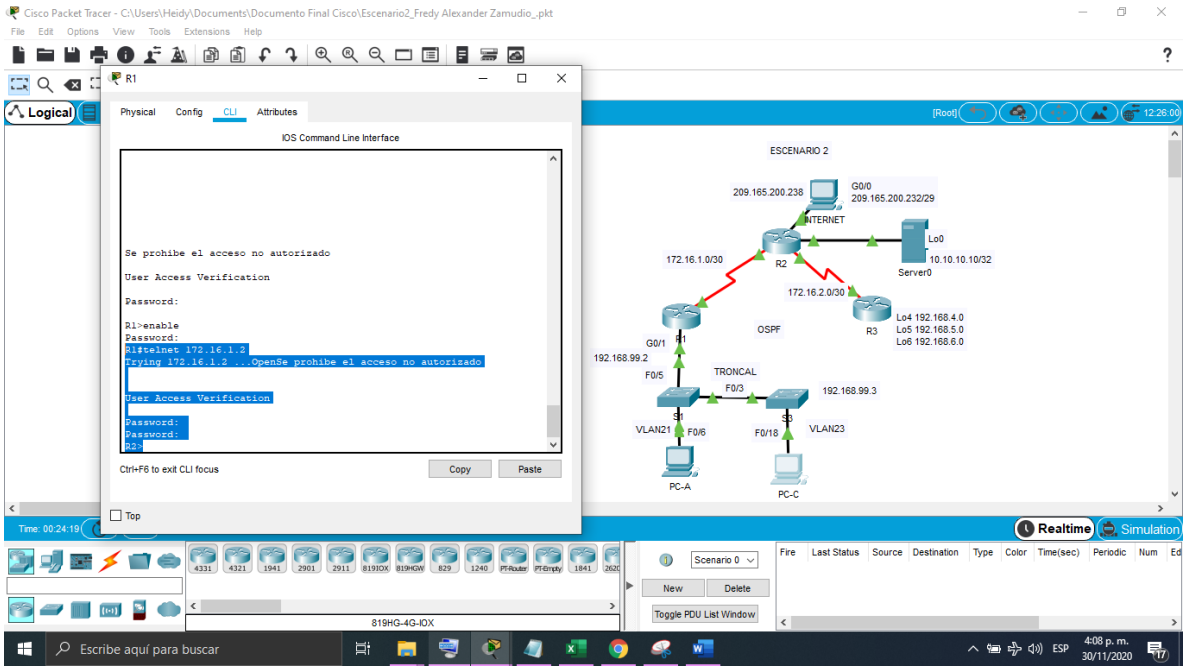
Paso 1: Restringir el acceso a las líneas VTY en el R2

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

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 30 configuración y verificación de las listas de control de acceso ACL



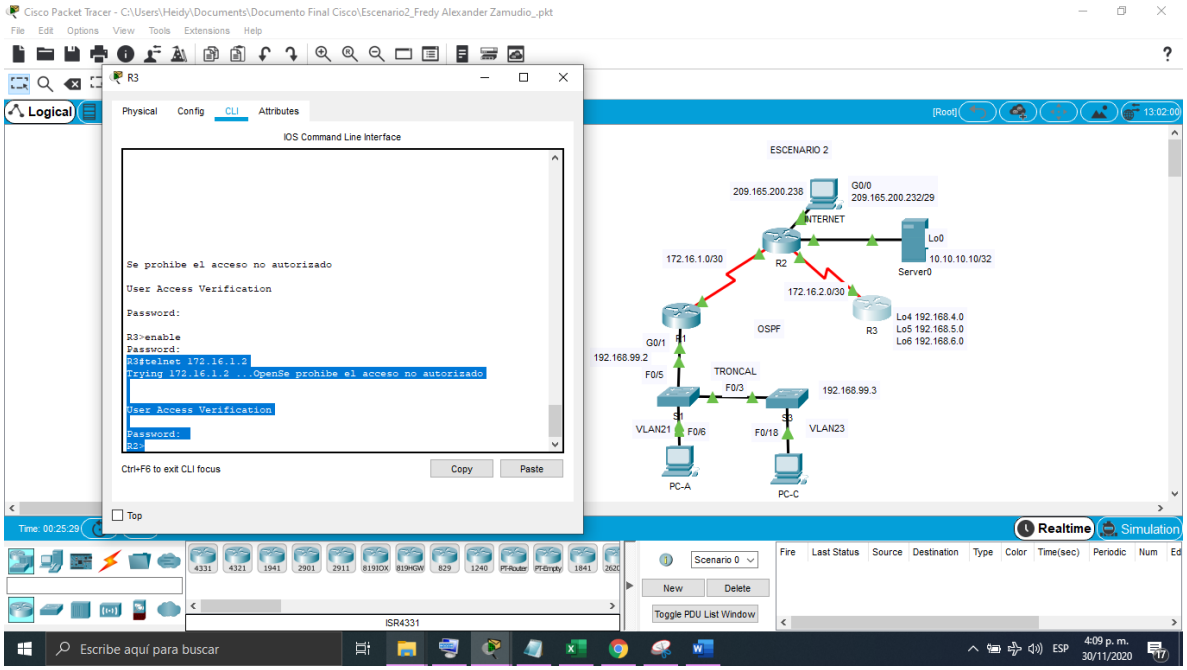


Figura 37 Verificación de la ACL en R1 y R3

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

CONCLUSIONES

Las configuraciones básicas que se realizan despues de la diseñar la topologia, son muy importantes primero porque le asignamos los parametros iniciales a cada dispositivo como un nombre por medio del comando hostname, contraseñas a los puertos de acceso y estas se encryptan para mayor seguridad limitando el acceso no autorizado para proteccion de la misma.

Se comprendio como funciona le protocol DHCP (Dynamic Host Configuration Protocol), al configurar este protocolo nos proporciona las direcciones IP de los dispositivo de forma automatica lo que facilita este proceso tan tedioso sobre todo en redes mas grandes.

Ademas se manejo la configuracion NAT tanto dinamica como estatica, 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.

El Protocolo de tiempo de red (NTP, por sus siglas en inglés) sincroniza la hora de las computadoras en una red. Como se realize en el Segundo escenario siendo este interesante porque lo hace de forma automatica.

Se aplicaron 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 pudo verificar cada una de las configuraciones realizadas en los dispositivos y por medio de los comandos ping, traceroute, show ip route, entre otros.

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

Anexo A Articulo Científico

DESARROLLO DE UNA RED DE ACCESO SEGURA POR MEDIO DE LAS CONFIGURACIONES BASICAS

Fredy Alexander Zamudio
Universidad Nacional Abierta y a Distancia (UNAD) Zamudiogfreddy@gmail.com

Resumen

Este trabajo se centra en configurar una red para que su acceso sea seguro al solo realizar las configuraciones básicas de la misma por medio del software cisco Packet Tracer.

Palabras clave: Configuracion, Basico, Seguridad, Red, VLAN.

Abstract:

This work focuses on configuring a network so that access is secure by only performing basic network configurations using cisco Packet Tracer software.

Keywords— Configuration, Basic, Security, Network, VLAN

I. Introducción

Actualmente, la mayoría de usuarios disponemos en nuestra casa de un router wifi para conectarnos a Internet de forma inalámbrica, ya que es mucho más cómodo y, en el caso de dispositivos móviles, es la única forma de conectarse. Para asegurar nuestra privacidad, así como la capacidad de acceso a Internet, es muy necesario proteger nuestra red wifi, nuestra casa es una red pequeña comparada con una empresa en donde la red de comunicaciones sería mucho más grande y por lo tanto es más importante aún garantizar la seguridad de las redes que maneje esta, es 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 interconectará entre sí cada uno de los dispositivos. Se realizarán las configuraciones básicas de los switches y routers que le permitirán tener un acceso seguro y por último se verifica este procedimiento usando los comandos ping.

II. DESARROLLO DE UNA RED DE ACCESO SEGURO

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

A. Topología

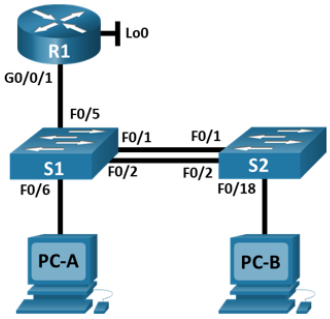


Figura 1. Topología

Para realizar la topología de la red, tal como se muestra en la figura 1, inicialmente agregamos a la pantalla principal del programa Packet Tracer el router 1941 y dos switch 2960 y 2 PC's, además los dispositivos se encuentran unidos por cable ethernet, y un cable de consola para configurar los dispositivos con cisco IOS mediante los puertos de consola. cómo podemos observar en la topología

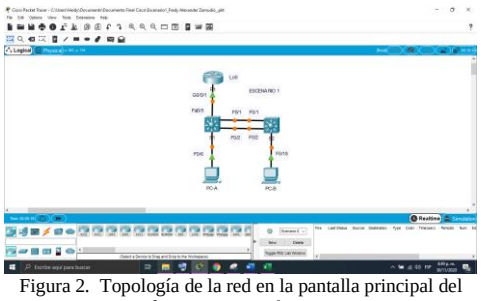


Figura 2. Topología de la red en la pantalla principal del software cisco packet tracer

B. Inicialización de los dispositivos

Para realizar esto, primero vamos a la pestaña CLI, allí

damos enter y volvemos a presionar enter para iniciar, nos aparecerá la línea de comando router> y switch> según corresponda, esto quiere decir usuario modo normal, en este usuario no podemos realizar ninguna configuración, por lo que comenzamos colocando el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado router# y switch#, como se muestra a continuación.

```
Router> enable
Router#
```

```
Switch> enable
Switch#
```

Luego verificamos que haya un archivo de configuración predeterminado limpio en el switch, emitiendo el comando del modo EXEC con privilegios show running-config. Si se guardó un archivo de configuración anteriormente, se debe eliminar.

```
Router> enable
Router#show running-config
```

```
Switch> enable
Switch#show running-config
```

Por medio del comando erase startup-config eliminamos los archivos y con el comando reload volverá a cargar los dispositivos.

```
Router# startup-config
Router# reload
```

```
Switch# startup-config
Switch# reload
```

A. Configuración los parámetros básicos en los dispositivos.

Comenzamos accediendo al router e ingrese al modo de configuración global, por medio de los siguientes comandos

```
Router> enable
Router#
```

Primero vamos a la pestaña CLI, allí damos enter y volvemos a presionar enter para iniciar, nos aparecerá la línea de comando router> que quiere decir usuario modo normal, en este usuario no podemos realizar ninguna configuración, por lo que comenzamos colocando el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado router#. Luego desactivamos la búsqueda de nombres de dominio, para esto simplemente colocamos el comando no ip domain lookup, después cambiamos el nombre de usuario, en este caso su nombre es router y lo cambiaremos por medio del comando hostname seguido del nombre que le colocaremos al router, en este caso R1.

Luego escribimos el comando service password-encryption para encriptar las contraseñas y le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class. También podemos agregar un mensaje que se mostrara al inicio de la línea de comando banner motd seguido el mensaje.

Otras configuraciones que se agregan son las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco después tenemos que escribir el comando login para que acepte y aplique las contraseñas. También se debe restringir el acceso del puerto de consola. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña. Para evitar que los mensajes de consola interrumpan los comandos, use la opción logging synchronous.

Se configuran las líneas de terminal virtual (vty) para que el router permita el acceso por Telnet. Si no configura una contraseña de vty, no podrá hacer Telnet al router.

```
Router> enable
Router#configure terminal
Router#no ip domain-lookup
Router(config)#service password-encryption
Router(config)#enable secret class
Router(config)#banner motd # Unauthorized Access is
strictly prohibited.#
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#loggin synchronous
Router(config-line)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
```

Despues de realizar esta configuración continuamos accediendo a los switches mediante la consola e ingrese al modo de configuración global.

```
Switch> enable
Switch#
```

Primero vamos a la pestaña CLI, allí damos enter y volvemos a presionar enter para iniciar, nos aparecerá la

línea de comando switch> que quiere decir usuario modo normal, en este usuario no podemos realizar ninguna configuración, por lo que comenzamos colocando el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado switch#. Luego desactivamos la búsqueda de nombres de dominio, para esto simplemente colocamos el comando no ip domain lookup, después cambiamos el nombre de usuario.

Luego escribimos el comando service password-encryption para encriptar las contraseñas y le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class. También podemos agregar un mensaje que se mostrara al inicio de la línea de comando banner motd seguido el mensaje. Otras configuraciones que se agregan son las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco después tenemos que escribir el comando login para que acepte y aplique las contraseñas. También se debe restringir el acceso del puerto de consola. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña. Para evitar que los mensajes de consola interrumpan los comandos, use la opción logging synchronous.

Se configuran las líneas de terminal virtual (vty) para que el switch permita el acceso por Telnet. Si no configura una contraseña de vty, no podrá hacer Telnet al switch.

```
Switch> enable
Switch#configure terminal
Switch#no ip domain-lookup
Switch(config)#service password-encryption
Switch(config)#enable secret class
Switch(config)#banner motd # Unauthorized Access is
strictly prohibited.#
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#loggin synchronous
Switch(config-line)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
```

I. RESULTADOS

A continuación, se muestran los resultados después de realizar estas configuraciones en cada dispositivo de la red.

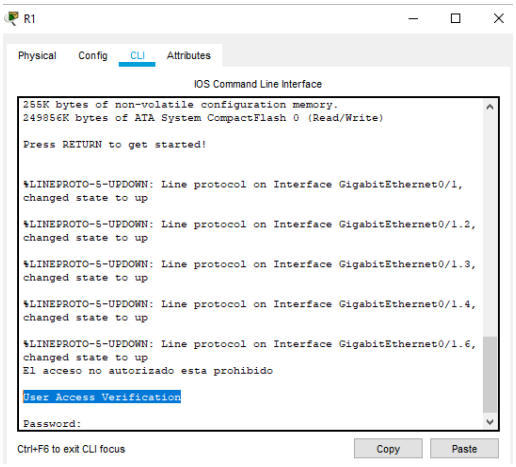


Figura 4. Ingreso al router R1

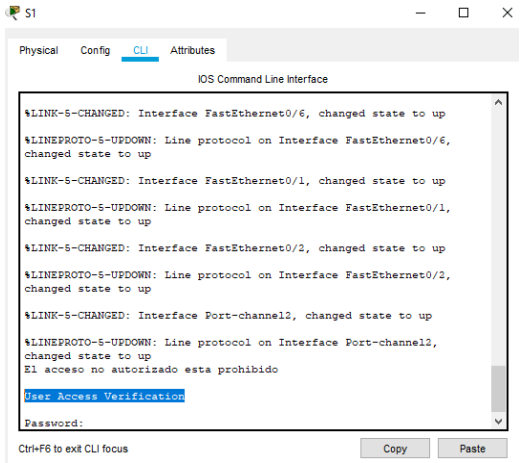


Figura 5. Ingreso al Switch S1

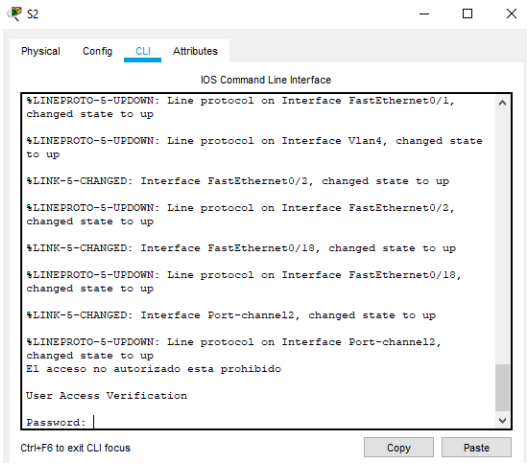


Figura 6. Ingreso al Switch S2

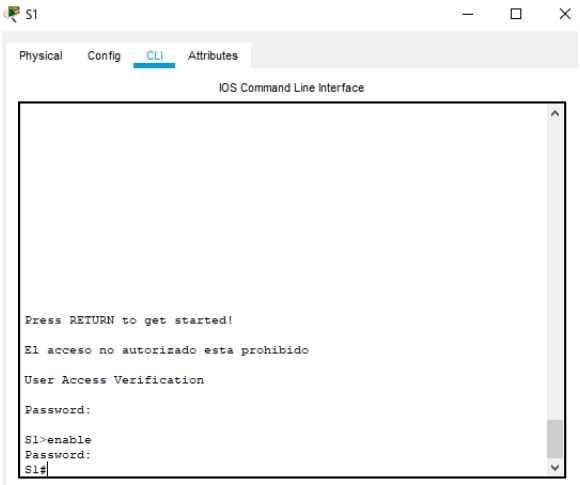


Figura 7. Ingreso al Switch S1 cuando ingresamos bien las contraseñas

Si ingresamos mal la contraseña más de tres veces, esta no nos deja ingresar y nos muestra el mensaje que configuramos inicialmente "El acceso no autorizado está prohibido" como podemos ver en la figura 8.

Como resultado de las configuraciones realizadas, es posible concluir que al realizar solo las configuraciones básicas después de la diseñar la topología, por medio de las contraseñas que se les asignan a los puertos de acceso y la se encriptación de estas los dispositivos y la red ya que quedan configurados para un acceso seguro para mayor seguridad limitando el acceso no autorizado y para protección de la misma.

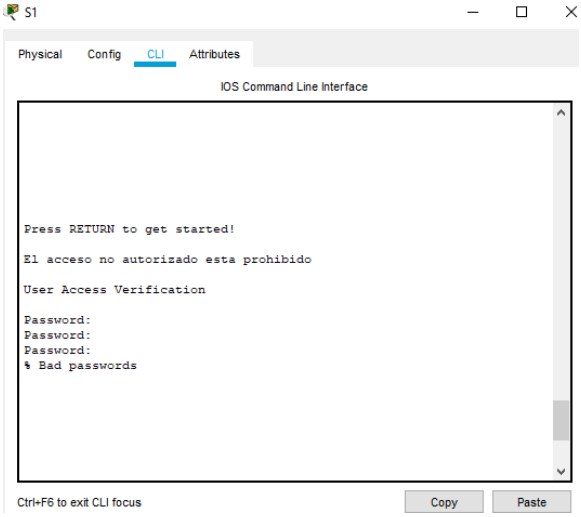


Figura 8. Resultado de ingresar tres veces mal la contraseña en S1

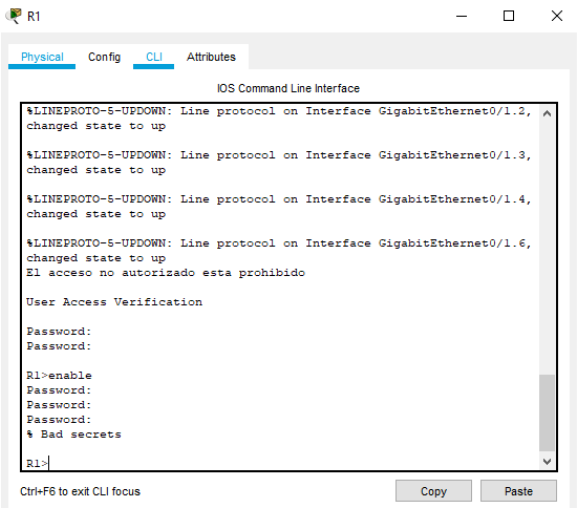


Figura 9. Resultado de ingresar la primera contraseña bien y la segunda no.

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

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-

[1] assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1
[2] 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
[3] 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