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

CARLOS ANDRES ARRIETA MADERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

SUCRE (SINCELEJO)

2021

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

CARLOS ANDRES ARRIETA MADERA

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

Presentado a:

MSc. JAVIER RICARDO VASQUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

SUCRE (SINCELEJO)

2021

Nota de Aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Sucre (Sincelejo), 29 de noviembre de 2021 (17, 11, 2021)

AGRADECIMIENTOS

Agradecerles a mi padre y a mi madre, por ser los principales creyentes en mi sueño, por confiar y creer en que yo si sería capaz de lograrlo, gracias a esa inspiración era que podía seguir adelante cada día sin importar lo difícil de la situación, por los consejos que me dieron en momentos difíciles y por los principios que me enseñaron desde niño ya que gracias a eso soy el hombre que soy y espero ser un gran profesional.

Agradecerles a todas las personas que me brindaron su apoyo con las actividades que hice para poder financiar mis estudios, a mis amigos y compañeros que estuvieron a mi lado cuando necesité un apoyo moral para poder seguir adelante muchas gracias por todo.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

GATEWAY: Considerado como un dispositivo en red que actúa como un punto de entrada de una red a otras redes. Es el enlace que conecta dos ordenadores a Internet. La pasarela actúa como portal entre dos programas y como medio de comunicación entre los protocolos que les permite compartir datos en los mismos dispositivos informáticos o entre diferentes sistemas informáticos.

INTERFAZ: La conexión física y funcional que se establece entre dos aparatos, dispositivos o sistemas que funcionan independientemente uno del otro

RED: Es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat,

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).

OSPF: Protocolo de encaminamiento, basado en estado de enlace, que utiliza el costo de las interfaces del router y usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos, permitiendo la autenticación de actualizaciones de ruteo, máscaras de subred de longitud variable y resumen de rutas

RESUMEN

En el presente informe se realizan las configuraciones que requieren dos redes pequeñas; principalmente comenzamos con los parámetros básicos que debe tener cualquier dispositivo, se diseña el esquema de direccionamiento IPv4 para las LAN propuestas, se configuran para que admitirá conectividad IPv4 e IPv6 y además se establecen los protocolos de configuración de hosts dinámicos (DHCP), el protocolo de routing dinámico OSPF y 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 con el fin poner en práctica los conocimientos adquiridos y aprender a administrar de forma segura las redes.

Palabras clave: Conectividad, Configuración, Seguridad, Red, Protocolo.

ABSTRACT

In this report, the configurations that require two small networks are made; We mainly start with the basic parameters that any device must have, the IPv4 addressing scheme for the proposed LANs is designed, they are configured to support IPv4 and IPv6 connectivity and also the dynamic host configuration protocols (DHCP) are established, the protocol of OSPF dynamic routing and dynamic and static network address translation (NAT), access control lists (ACL) and the server / client network time protocol (NTP) in order to put into practice the acquired knowledge and learn to securely manage networks.

Keywords: Connectivity, Configuration, Security, Network, Protocol

INTRODUCCIÓN

En el presente informe tendrá como objetivo identificar las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de Routers y switches, mediante el uso de comandos especializados en gestión de redes y compatibles con el protocolo SMNP. Inicialmente se identificarán las herramientas de simulación y laboratorios de acceso remoto con el fin de establecer dos escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento. Se construirán las topologías de red, se diseñará un esquema de direccionamiento IP para la LAN1 y la LAN2, se configurarán los aspectos básicos de los dispositivos de la Red propuesta, los ajustes básicos de seguridad en el R1 y S1, se configurarán los hosts, por último, se verificará la conectividad entre los equipos por medio del comando ping, permitiendo así que el estudiante tenga el conocimiento y pueda ponerlo en práctica.

DESARROLLO

1.1 ESCENARIO 1

En este primer scenario se configuran los dispositivos de una red pequeña, un router, un switch y equipos PC, se diseña el esquema de direccionamiento IPv4 para las LAN propuestas.

Figura 1 Topología del escenario.

Fuente: Guía Prueba de habilidades prácticas CCNA.

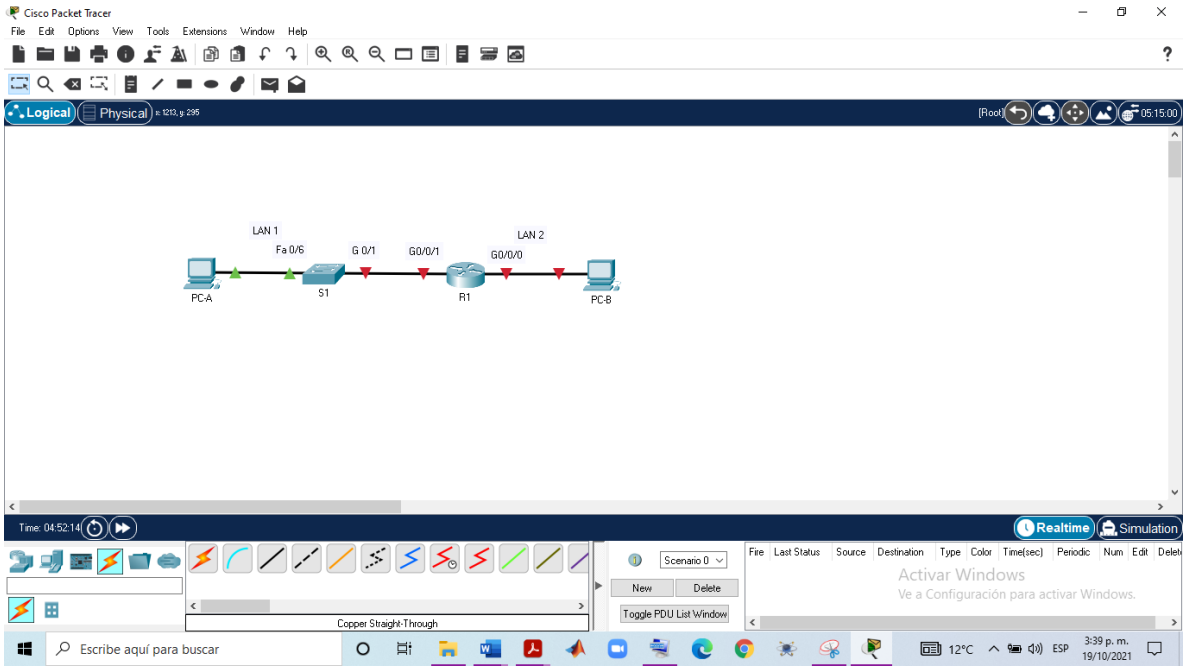
Para el desarrollo de este escenario se instala el entorno de simulación de Packet Tracer versión 8.0. Se crea la topología de red con los siguientes dispositivos: Un Router Cisco ISR4331, un Switch Cisco 2960-24T y dos PCs Cisco PC-PT.

Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

Se construye la red de acuerdo con la topología lógica que se plantea en la figura 1, se cablea conforme se indica en la topología utilizando el cable Ethernet directo (Copper Straight – Through)

Figura 2 Simulacion de escenario 1 en el software cisco packet tarcer.



Fuente: propia.

Parte 2: Desarrolle el esquema de direccionamiento IP

El esquema de direccionamiento IP, para IPv4 comienza creando las dos subredes con la cantidad requerida de hosts. Se realiza con el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula. Mi cedula es 95.536.320 por lo que el direccionamiento queda 192.168.20.0

La dirección IP 192.168.20.0/24 es un tipo de IP a la clase C, entonces su máscara de subred por defecto es 255.255.255.0.

Tabla 1 Direccionamiento IPv4

IP original 192.168.20.0					
N° Subredes	Dirección de Subred	Primera red útil	Ultima red útil	broadcatch	Marcara

1	192.168.20.0	192.168.20.1	192.168.20.126	192.168.20.127	255.255.255.128
2	192.168.20.128	192.168.20.129	192.168.20.190	192.168.20.191	255.255.255.192

Fuente: Guía Prueba de habilidades prácticas CCNA.

Tabla 2 Direccionamiento de los dispositivos

Item	Requerimiento
Dirección de Red	192.168.20.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.20.1
R1 G0/0/0	192.168.2.129
S1 SVI	192.168.20.2
PC-A	192.168.20.126
PC-B	192.168.20.190

Fuente: Guía Prueba de habilidades prácticas CCNA.

Parte 3: Configure aspectos básicos

Configuraciones básicas del Router R1, se realizan en modo de configuración global aplicando los siguientes comandos:

Paso 1: configurar los ajustes básicos

Tabla 3 Configuraciones básicas en R1

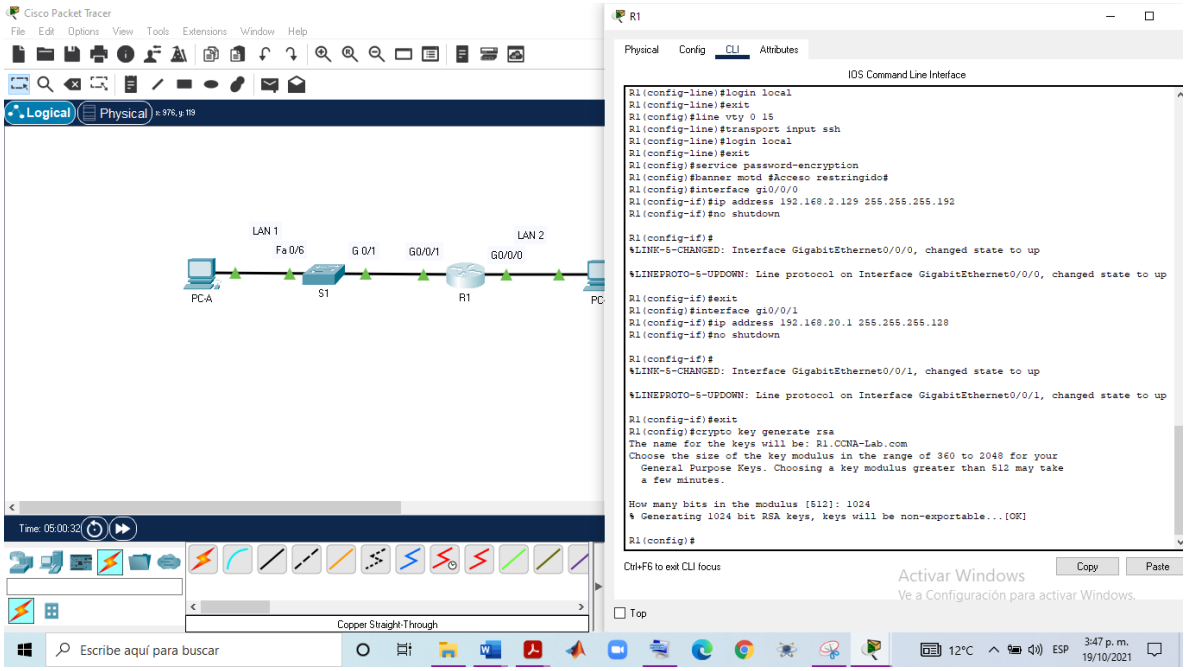
Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass

Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin privilege 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 15 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 #Acceso restringido#
Configurar interfaz G0/0/0	R1(config)#interface gi0/0/0 R1(config-subif)#ip address 192.168.2.129 255.255.255.192 R1(config-subif)#no shutdown R1(config-subif)#exit
Configurar interfaz G0/0/1	R1(config)#interface gi0/0/1 R1(config-subif)#ip address 192.168.20.1 255.255.255.128 R1(config-subif)#no shutdown R1(config-subif)#exit

Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa 1024 The name for the keys will be: R1.CCNA-Lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable... [OK]

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 3 Configuraciones básicas en R1



Fuente: Propia.

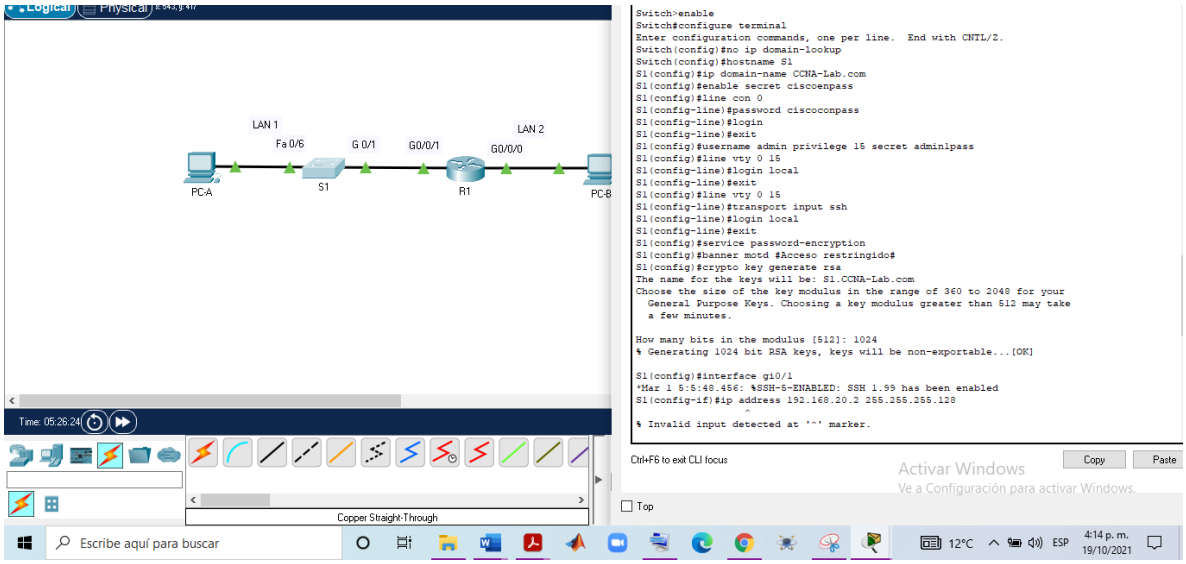
Configuraciones básicas del Switch S1, se realizan en modo de configuración global aplicando los siguientes comandos:

Tabla 4 Configuraciones básicas en S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line 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	R1(config)#banner motd #Acceso restringido#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S1(config)#interface gi0/1 S1(config-if)#ip address 192.168.20.2 255.255.255.128 S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 192.168.20.1 S1(config)#do write

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

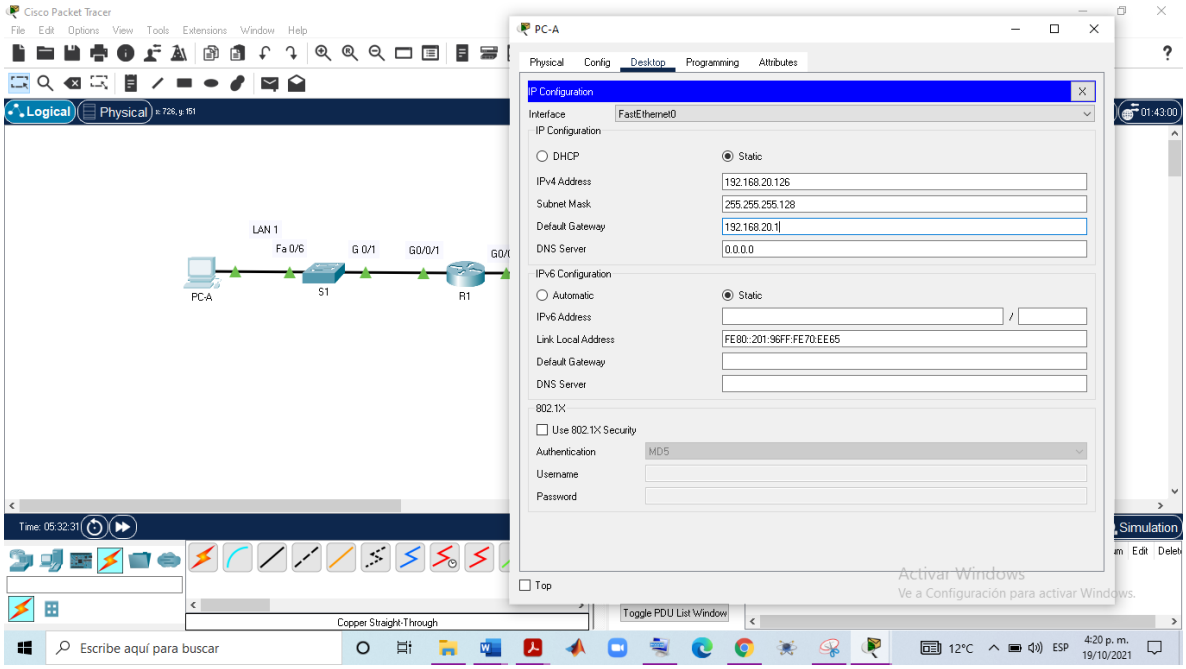
Figura 4 Configuraciones básicas en S1



Fuente: Propia.

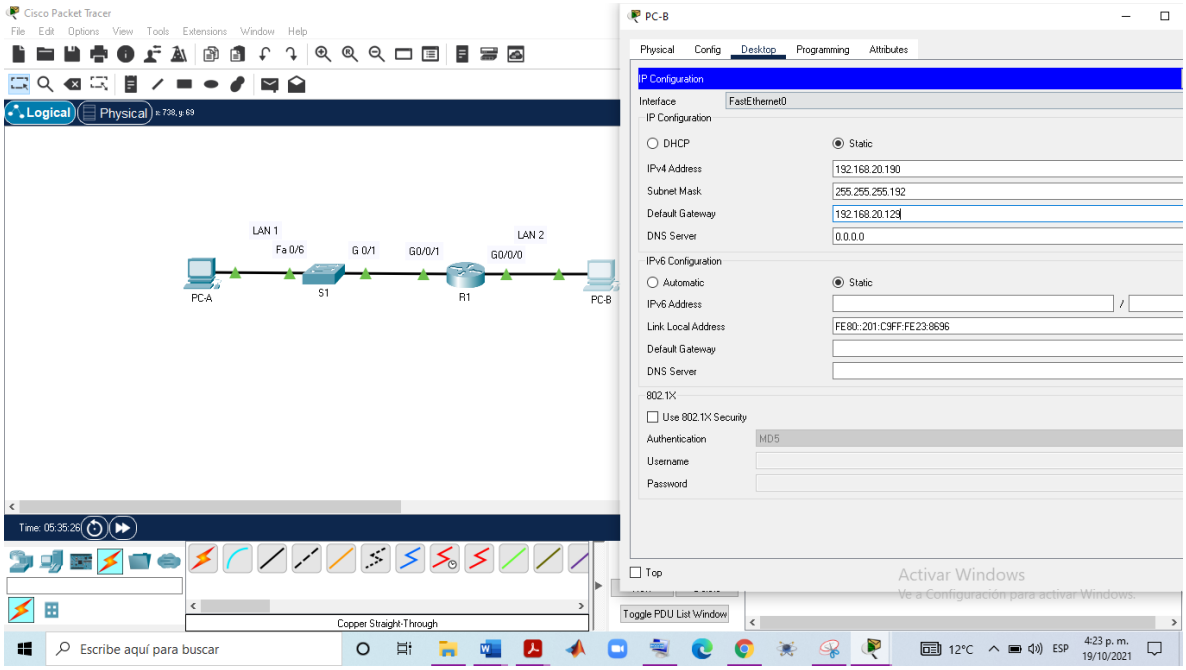
Paso 2. Configurar los equipos host PC-A y PC-B.

Figura 5 Configuración IP de PC-A



Fuente: Propia.

Figura 6 Configuración IP de PC-B



Fuente: Propia.

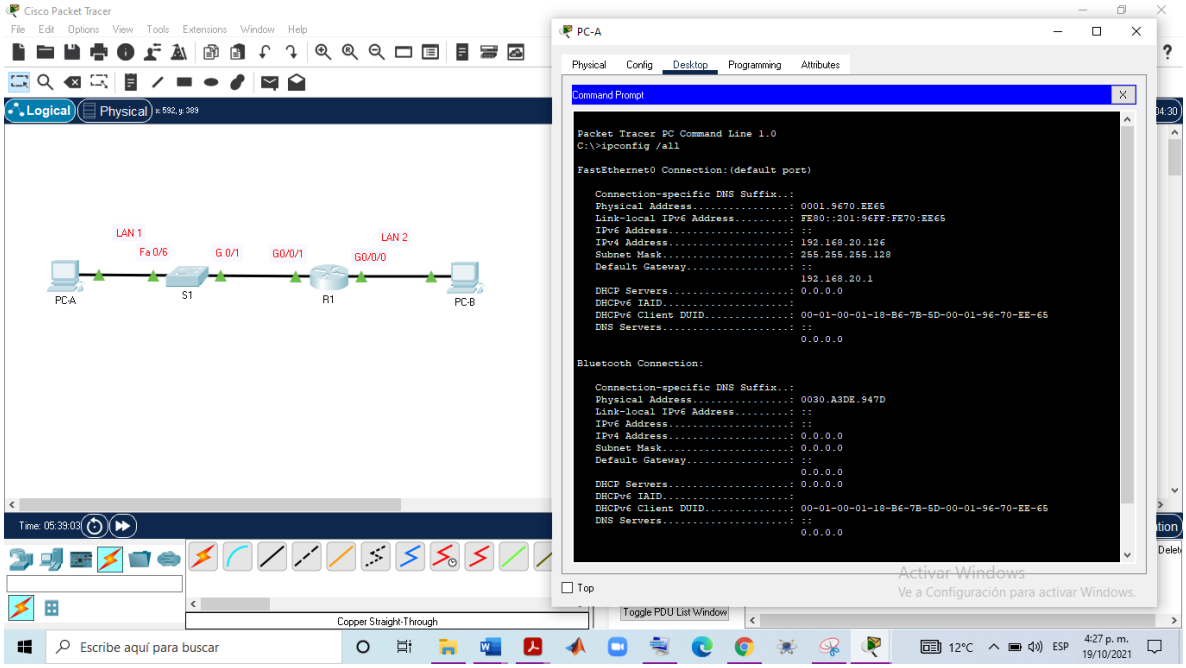
Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 5 Configuración del servidor PC-A

PC-A Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	0001.9670.EE65
Dirección IP	192.168.20.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.20.1

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 7 Verificación de la configuración de red de PC-A



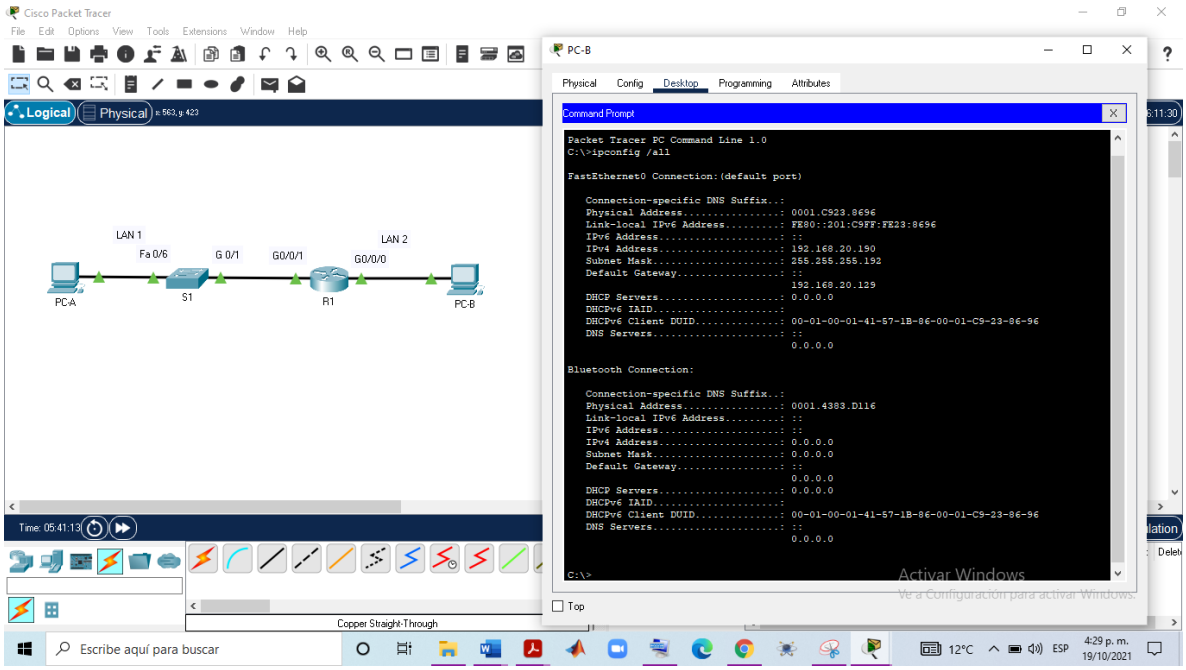
Fuente: Propia.

Tabla 6 Configuración del servidor PC-B

PC-B Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	0001.C923.8696
Dirección IP	192.168.20.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.20.129

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 8 Verificación de la configuración de red de PC-B

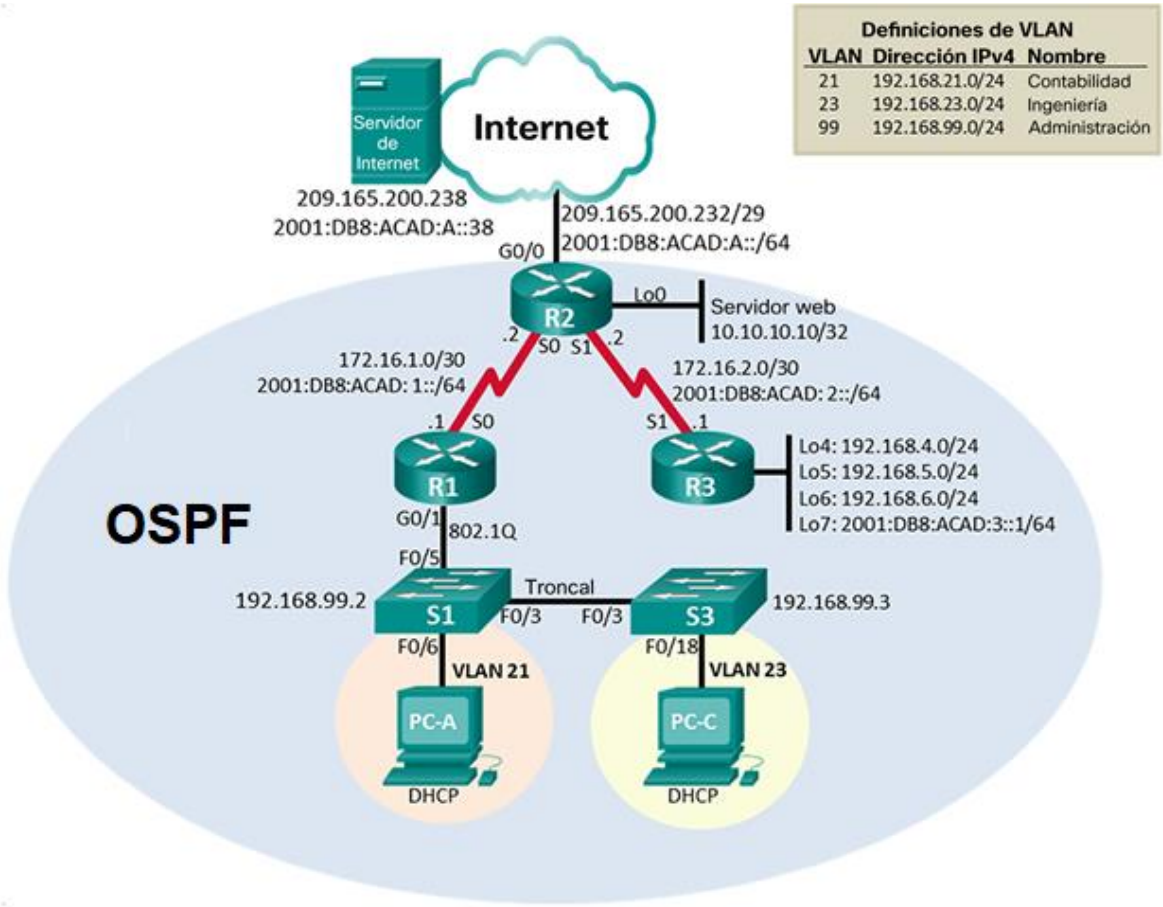


Fuente: Propia.

1.2 ESCENARIO 2

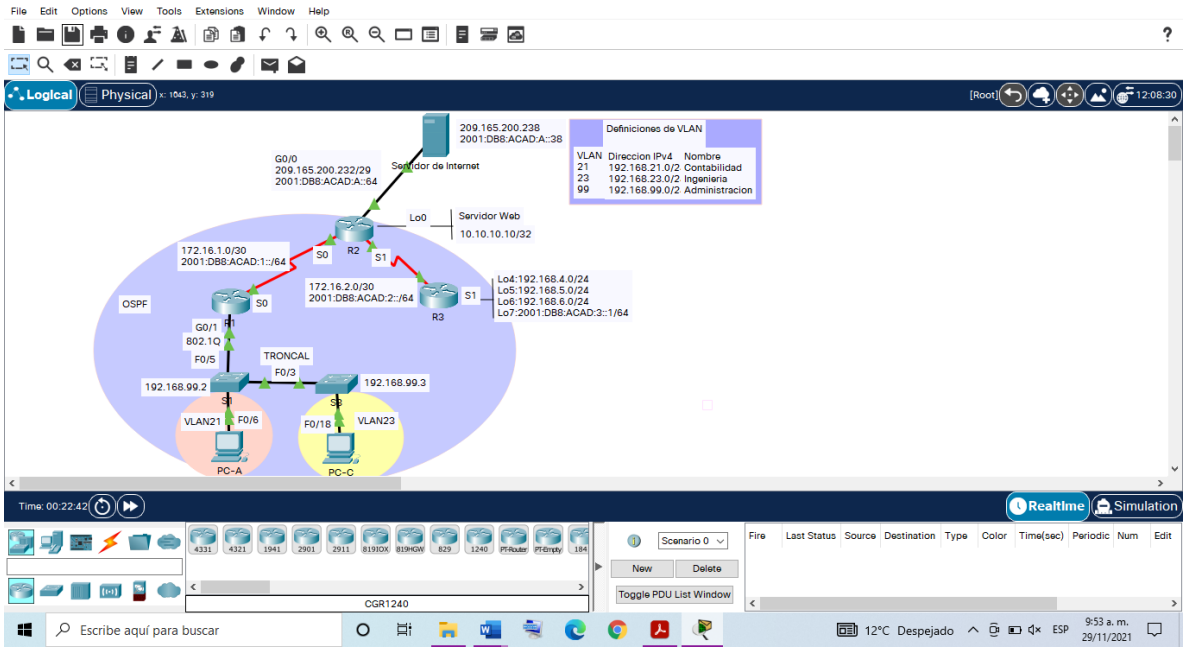
Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de 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.

Figura 9 Topología del segundo escenario.



Fuente: Guía Prueba de habilidades prácticas CCNA.

Figura 10 Simulación de escenario 2 en el software cisco Packet Tracer.



Fuente: Propia.

Parte 1: Inicializar Dispositivos

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

Primero revisamos si hay previas configuraciones en los dispositivos, de ser así 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.

Ingresamos a cada dispositivo dando doble clic y a través de la ventana (CLI), ingresamos el comando enable, que permite cambiar el modo EXEC del usuario al modo EXEC privilegiado donde si podemos realizar las configuraciones del dispositivo, luego ingresamos el comando erase startup-config para eliminar el contenido de la NVRAM y por último ingresamos el comando Reload para reiniciar el dispositivo.

Tabla 7 Inicialización de los Routers y Switchs

Tarea	Comando de ios
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Continue? [confirm] [Enter] [OK] Erase of nvram: complete
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm] [Enter]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [Enter] [OK] Erase of nvram: complete Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm] [Enter]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# show vlan brief

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

En la siguiente tabla, se encuentran las direcciones IPv4 e IPv6 correspondientes a la computadora de internet.

Tabla 8 Direcciones IPv4 e IPv6 para configurar en la computadora

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

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Puede ser necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes: (Todavía no es recomendable configurar la interfaz G0/1)

Tabla 9 Configuraciones básicas de R1

Tarea	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

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 3: Configurar R2

Tabla 10 Configuraciones básicas en R2

Tarea	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-line)#enable secret class
Contraseña de acceso a la consola	R2(config)# line console 0 R2(config)#password cisco R2(config-line)# login
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config)#password cisco R2(config-line)# login
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)# description Conexion Servidor R2(config-if)#ip address 209.165.200.225 255.255.255.248 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 0.0.0.0 172.16.1.1 R2(config)# ipv6 route ::/0 2001:DB8:ACAD:1::1 R2(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.1 R2(config)# ipv6 route ::/0 2001:DB8:ACAD:2::1 R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.238 R2(config)# ipv6 route ::/0 2001:BD8:ACAD:A::38

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 4: Configurar R3

Tabla 11 Configuraciones básicas de R3

Tarea	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)# line console 0 R3(config)#password cisco R3(config-line)# login
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config)#password cisco R3(config-line)# login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/1	R3(config)#interface s0/3/1 R3(config)# description Conexion a R2 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)#description Interfaz virtual (para pruebas, en este caso el 4)
	R3(config-if)#ip address 192.168.4.1 255.255.255.0
	R3(config-if)#no shutdown

Interfaz loopback 5	R3(config)#interface loopback 5

	R3(config)# description Interfaz virtual (para pruebas, en este caso el 5) R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#no shutdown

Interfaz loopback 6	R3(config)#interface loopback 6
	R3(config)#description Interfaz virtual (para pruebas, en este caso el 6)
	R3(config-if)#ip address 192.168.6.1 255.255.255.0
	R3(config-if)#no shutdown

Interfaz loopback 7	R3(config)#interface loopback 7
	R3(config)#description Interfaz virtual (para pruebas, en este caso el 7)
	R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
	R3(config-if)#no shutdown

Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R3(config)#ipv6 route ::/0 2001:DB8:ACAD:2::2

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 5: Configurar S1

Tabla 12 Configuraciones básicas de S1

Tarea	**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)# line console 0 S1(config)#password cisco S1(config-line)# login
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config)#password cisco S1(config-line)# login

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd $Se prohibe el acceso no autorizado$

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 6: Configurar el S3

Tabla 13 Configuraciones básicas de S3

Tarea	**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)# line console 0 S3(config)#password cisco S3(config-line)# login
Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config)#password cisco S3(config-line)# login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd $Se prohibe el acceso no autorizado$

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 7: Verificar la conectividad de la red

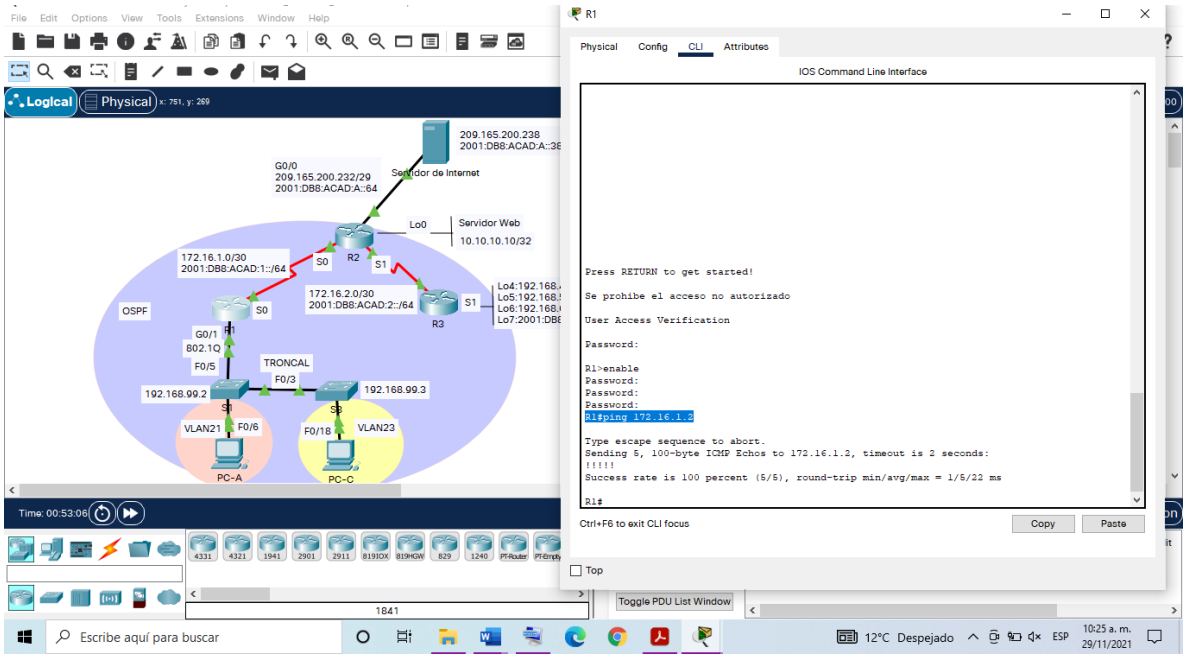
Utilice el comando ping para probar la conectividad entre los dispositivos de red. Y ademas utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 14 Verificación de conectividad de la red

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
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
PC de Internet	Gateway predeterminado	209.165.200.225	>ping 209.165.200.225 Reply from 209.165.200.225: bytes=32 time<1ms TTL=255

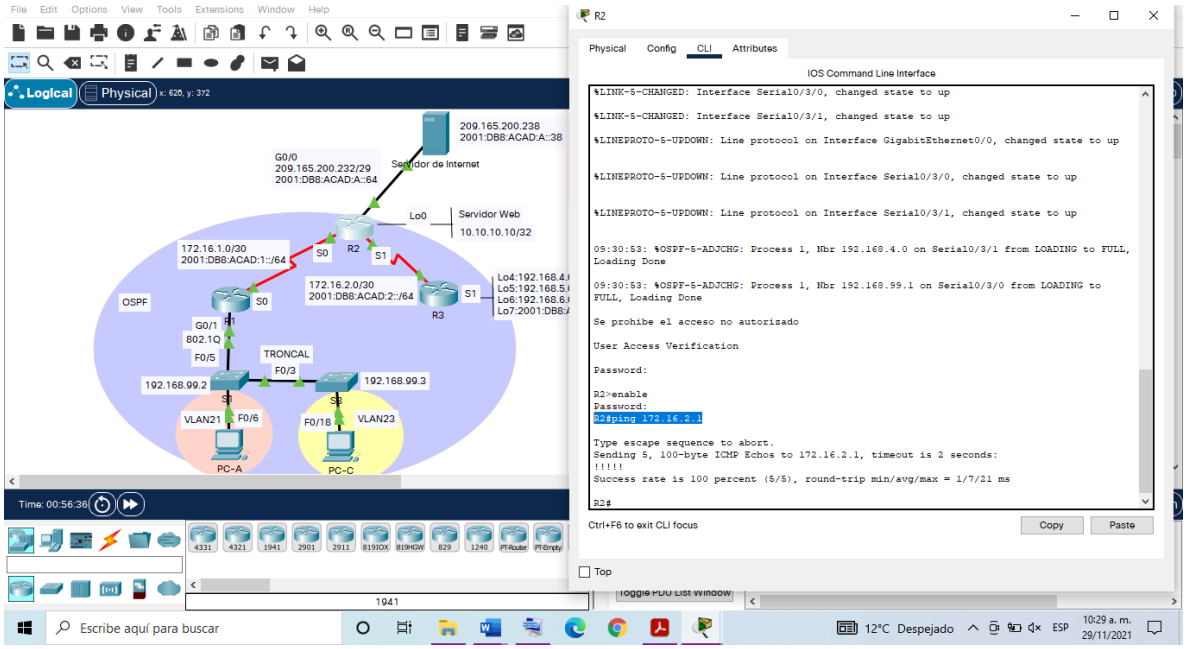
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 11 Verificación de conectividad desde R1 a R2.



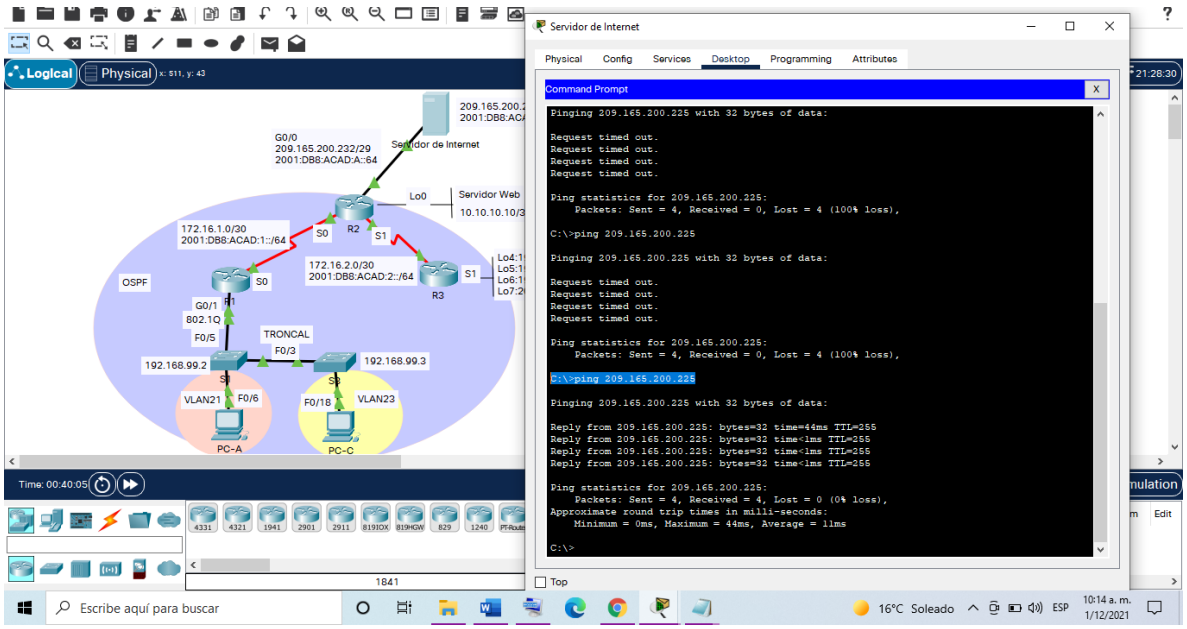
Fuente: Propia.

Figura 12 Verificación de conectividad desde R2 a R3. Fuente: propia



Fuente: Propia.

Figura 13 Verificación de conectividad desde PC de Internet a Gateway.



Fuente: Propia.

Es importante tener en cuenta de que aveces es necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

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

Paso 1: Configurar S1

Tabla 15 Configuración de la seguridad entre las vlan de S1.

Tarea	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

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 2: Configurar el S3

Tabla 16 Configuración de la seguridad entre las vlan de S3.

Tarea	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

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17 Configuración de la seguridad entre las vlan de R1.

Tarea	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 R1(config)#description LAN de contabilidad VLAN 21
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 R1(config)#description LAN de Ingeniería VLAN 23
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 R1(config)#description LAN de Administración VLAN 99
Activar la interfaz G0/1	R1(config-subif)# interface g0/1 R1(config-subif)#no shutdown

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 4: Verificar la conectividad de la red

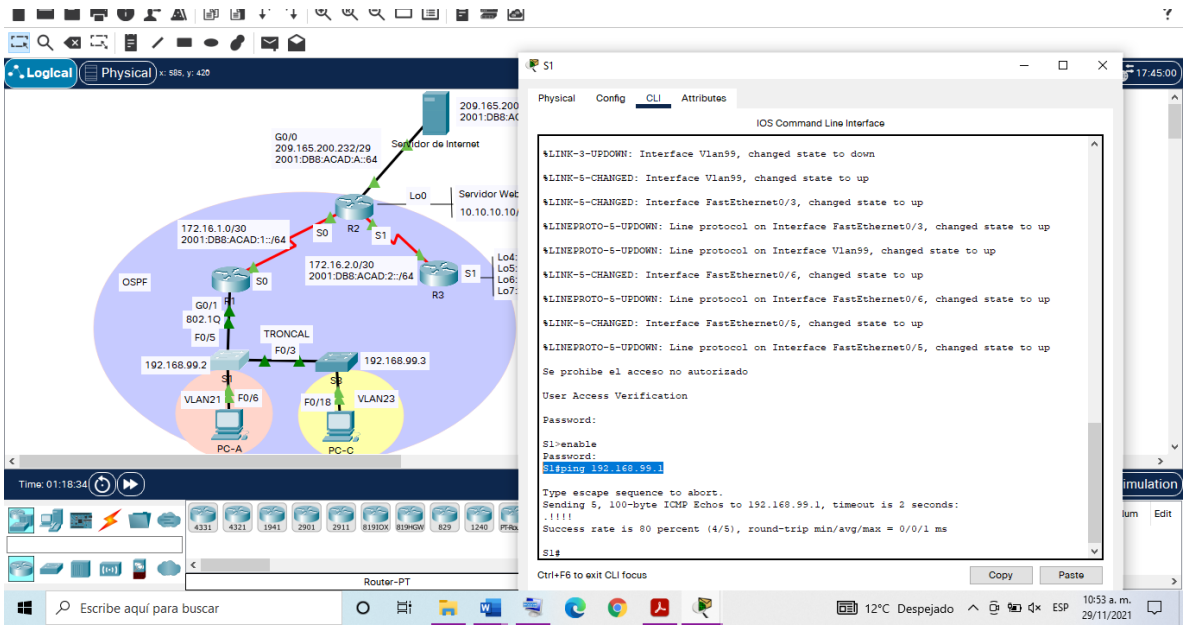
Utilice el comando ping para probar la conectividad entre los switches y el R1 y utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 18 Verificación de conectividad de la red

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
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
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
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

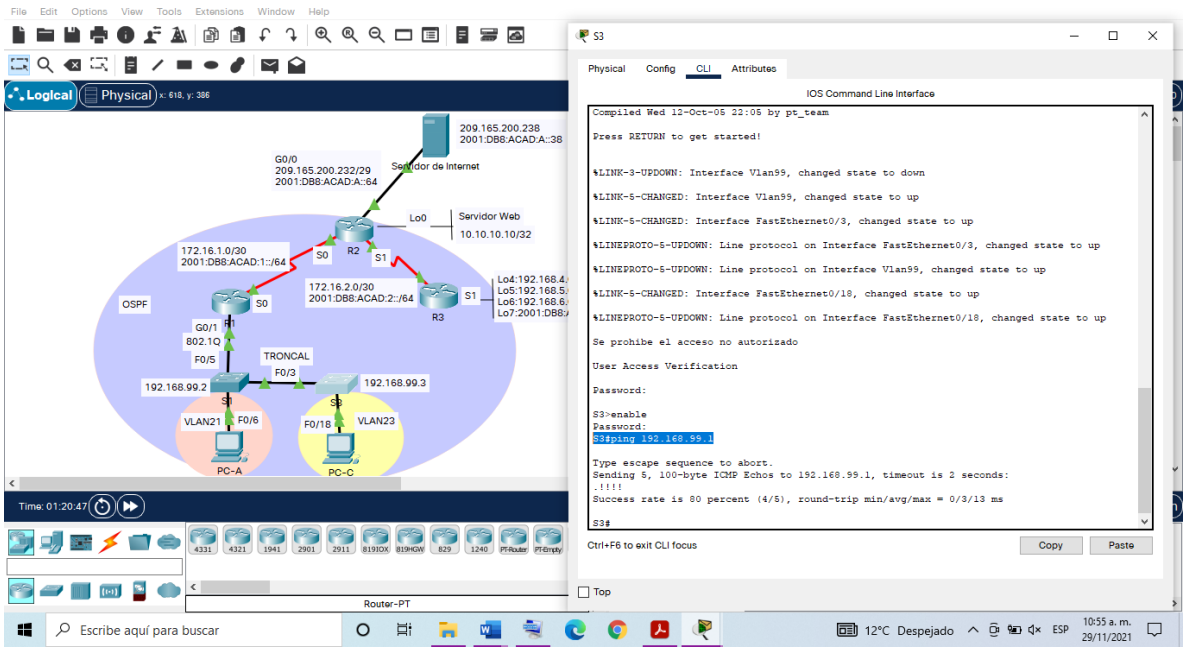
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Al aplicar las configuraciones se ve que la administración de la red va tomando forma y consistencia de la red, por ello es importante ir verificando que el constantemente el procedimiento para obtener el resultado final esta quedando correctamente, a través de las figuras siguientes, se observa que realizan que un seguimiento satisfactorio de las configuraciones realizadas hasta el momento del en la red. Figura 14 Verificación de conectividad desde S1 a R1 (VLAN99).



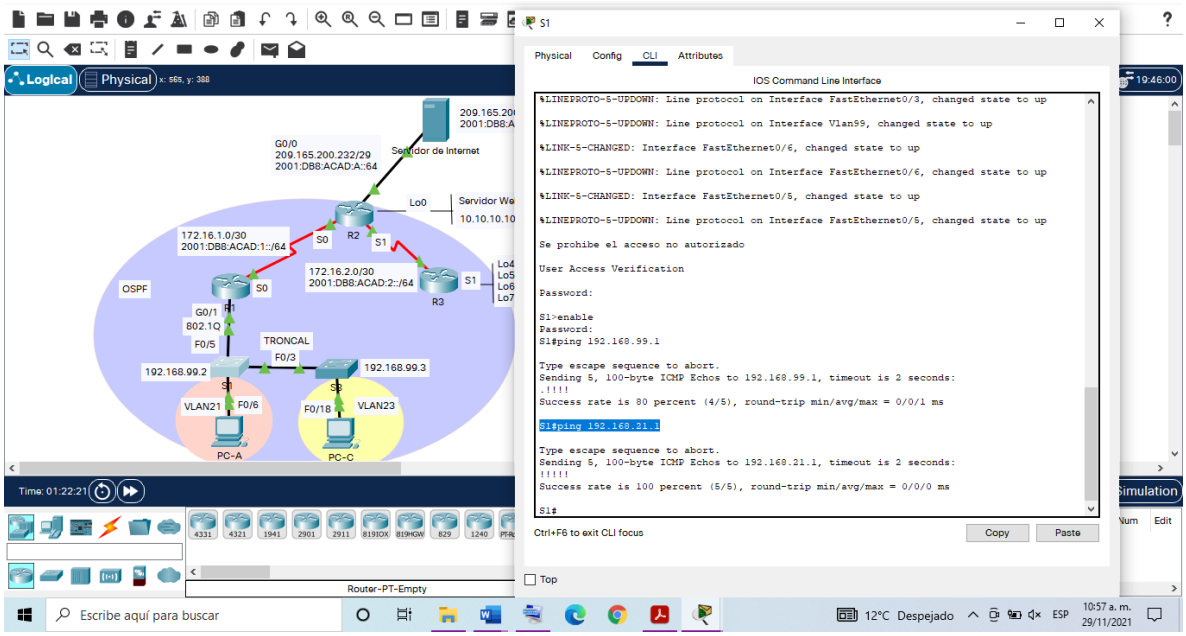
Fuente: Propia

Figura 15 Verificación de conectividad desde S3 a R1 (VLAN99).



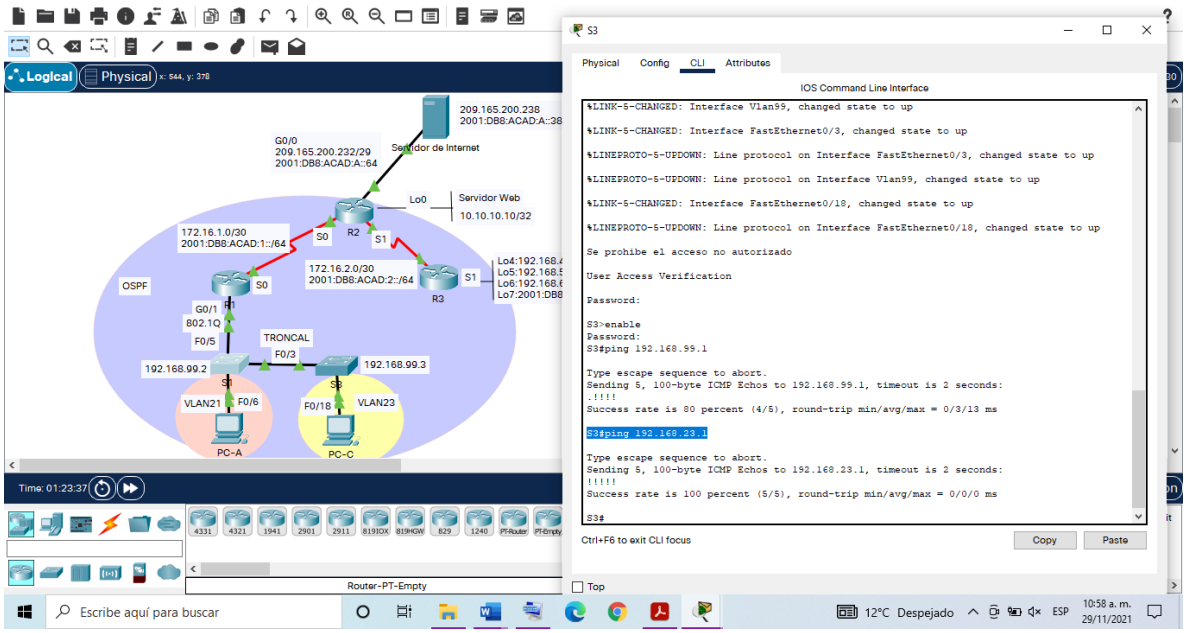
Fuente: Propia

Figura 16 Verificación de conectividad desde S1 a R1 (VLAN21).



Fuente: Propia

Figura 17 Verificación de conectividad desde S3 a R1 (VLAN21).



Fuente: Propia

Paso 5: Habilitar el envío de tráfico IPv6 en R1, R2 y R3.

Tenemos en cuenta de que, por defecto, IPv6 está desactivado en un dispositivo Cisco. El comando de configuración global ipv6 unicast-routing debe configurarse para que habilite al router el reenvío de paquetes IPv6) (Permite enrutar paquetes IPv6 entre las distintas interfaces del router)

Tabla 19 Habilitación tráfico IPv6 en R1, R2 y R3.

Tarea	Especificación
Habilitar el routing de unidifusión IPv6 en R1, R2 y R3.	R1#configure terminal R1(config)#ipv6 unicast-routing R1(config)#exit R2# configure terminal R2(config)#ipv6 unicast-routing R2(config)#exit R3# configure terminal R3(config)#ipv6 unicast-routing R3(config)#exit

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

(El escenario simulado en Packet Tracer no permite la inserción del comando no auto-78 summary).

Tabla 20 Configuración OSPF en el R1.

Tarea	Especificación
Configurar OSPF area 0	R1(config)#router ospf 1 R1(config)#router-id 1.1.1.1
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

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 2: Configurar OSPF en el R2

Tabla 21 Configuración OSPF en el R2.

Tarea	Especificación
Configurar OSPF area 0	R2(config)#router ospf 1 R2(config)#router-id 2.2.2.2
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	R2(config-router)#passive-interface lo4 R2(config-router)#passive-interface lo5 R2(config-router)#passive-interface lo6

(loopback) como pasiva	
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 3: Configurar OSPFv3 en el R3

Tabla 22 Configuración OSPF en el R3

Tarea	Especificación
Configurar OSPF area 0	R3(config)#router ospf 1 R3(config)#router-id 3.3.3.3
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 R3(config-router)#passive-interface lo7
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 4: Verificar la información de OSPF

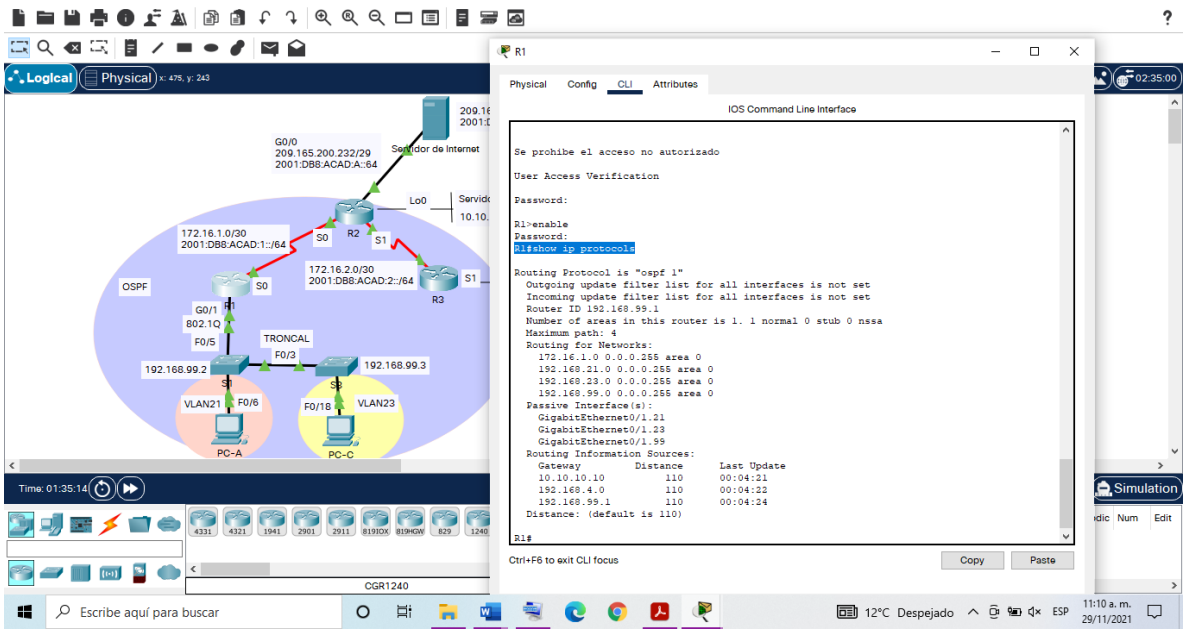
Verificamos que OSPF esté funcionando como se espera. Introduciendo el comando de CLI adecuado para obtener la siguiente información: Desde el modo de usuario y en R1, R2 y R3 se aplica los siguientes comandos:

Tabla 23 Verificar la información de OSPF

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
¿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-config | section router ospf R2#Show run-config | section router ospf R3#Show run-config | section router ospf

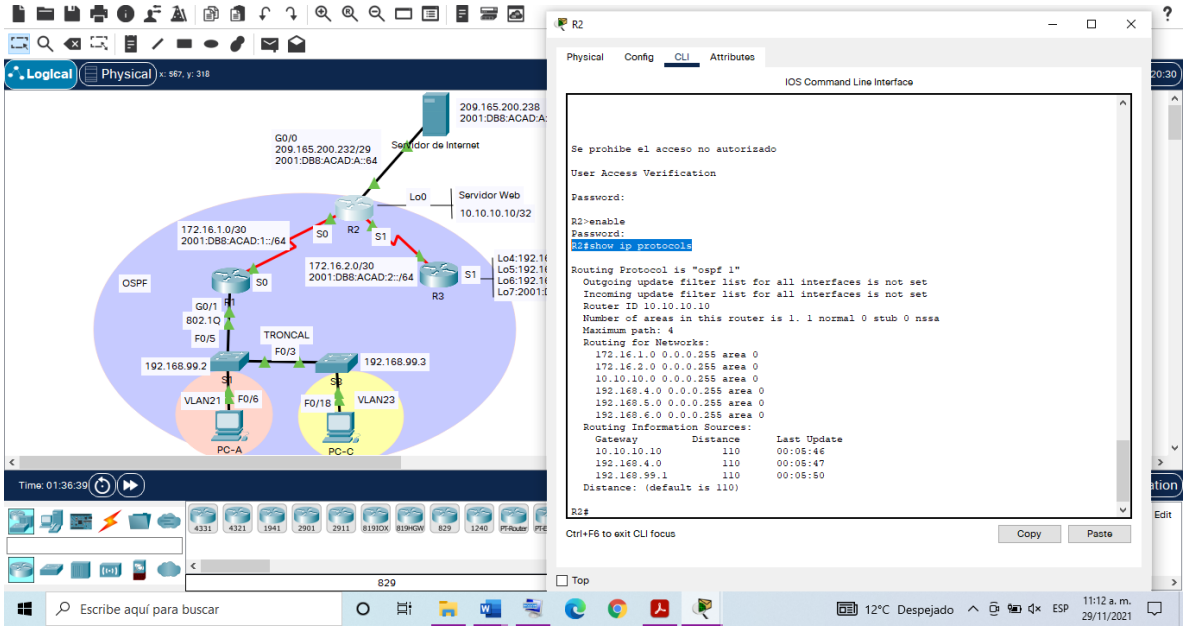
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 18 Comando show ip protocols en R1.



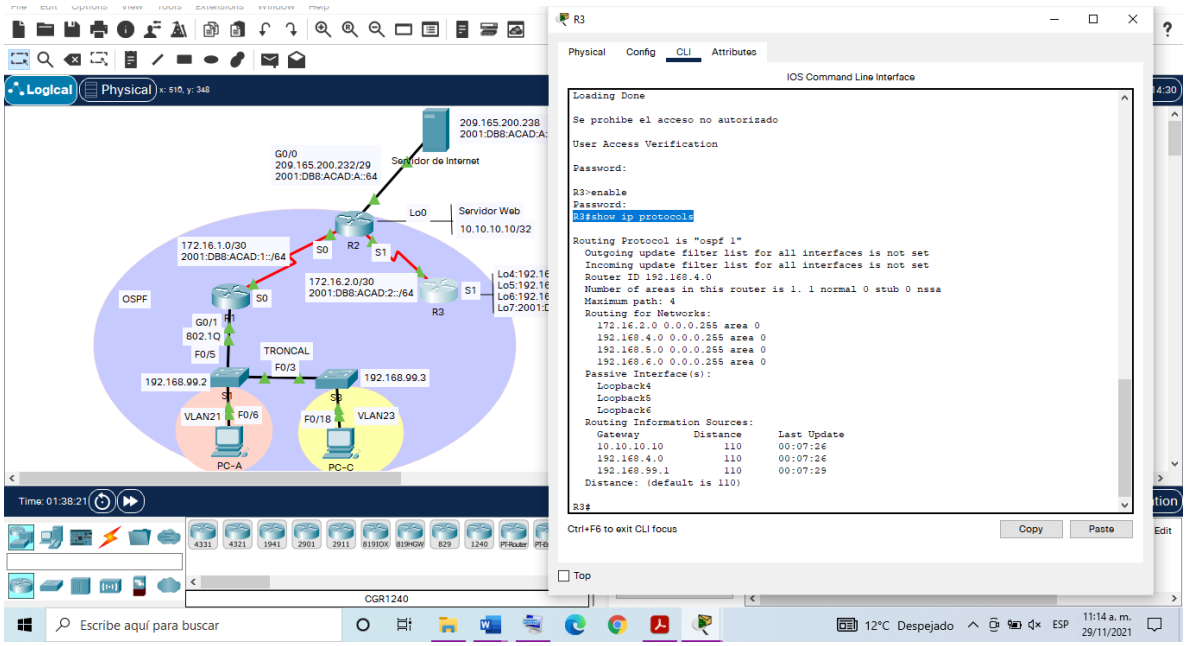
Fuente: Propia.

Figura 19 Comando show ip protocols en R2.



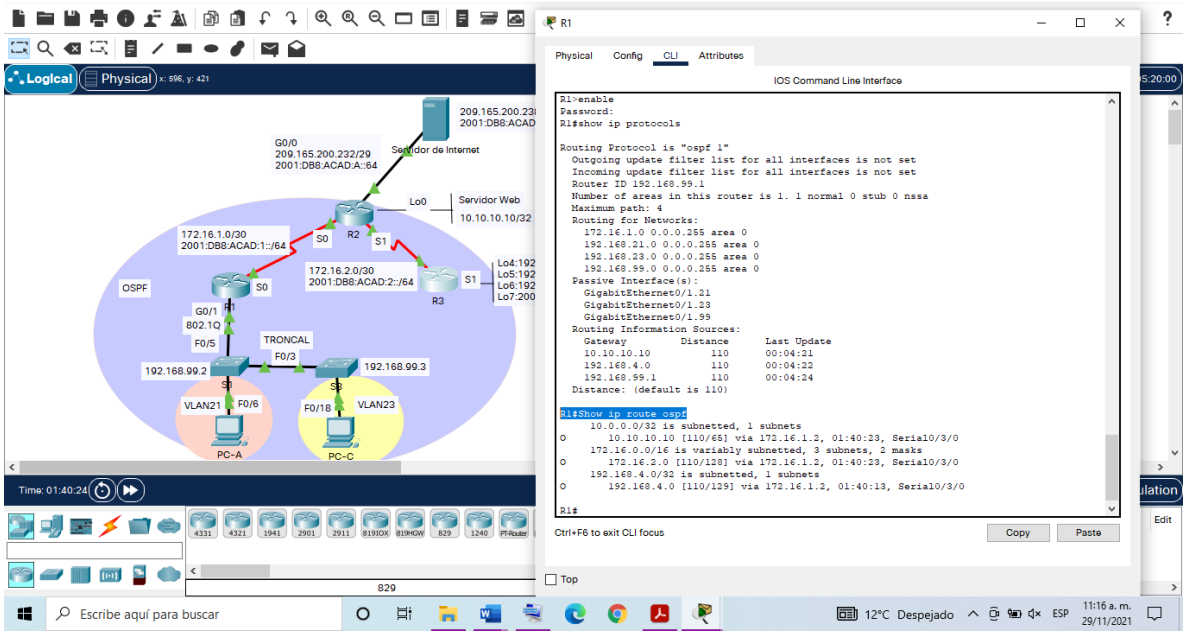
Fuente: Propia.

Figura 20 Comando show ip protocols en R3.



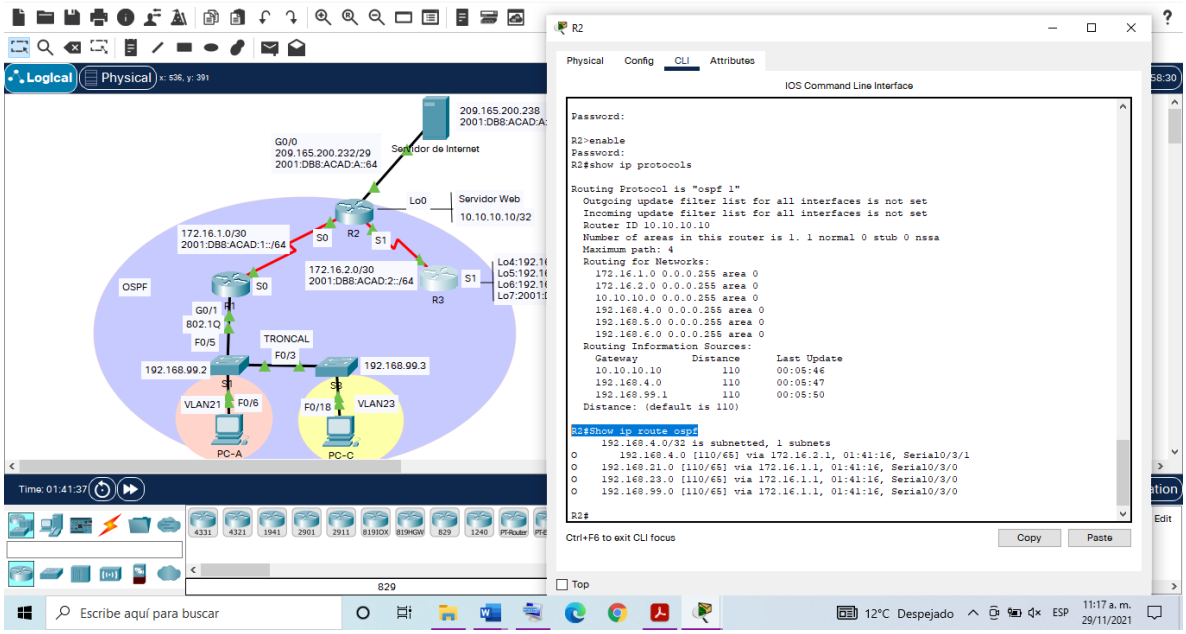
Fuente: Propia.

Figura 21 Comando show ip route ospf en R1.



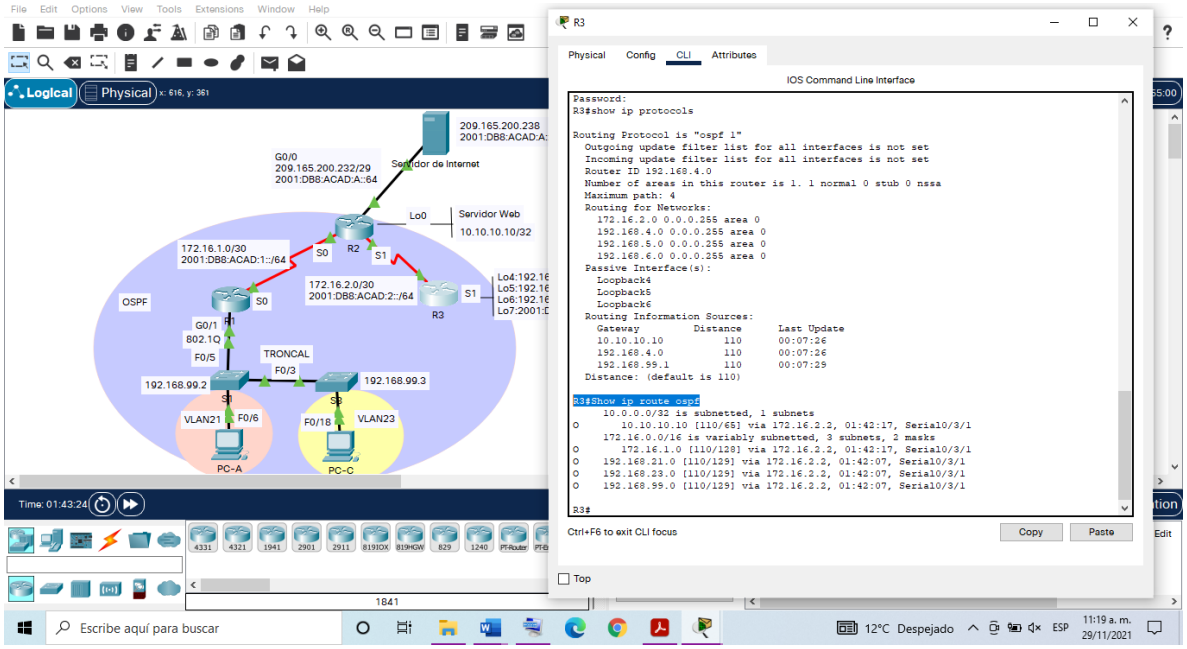
Fuente: Propia.

Figura 22 Comando show ip route ospf en R2.



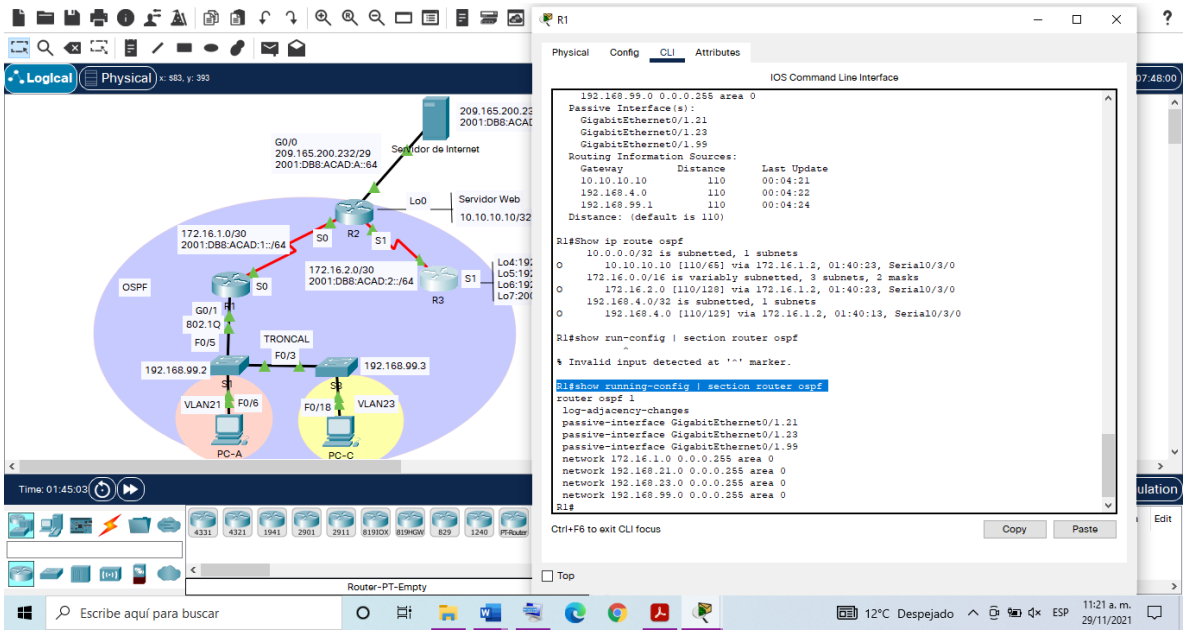
Fuente: Propia.

Figura 23 Comando show ip route ospf en R3



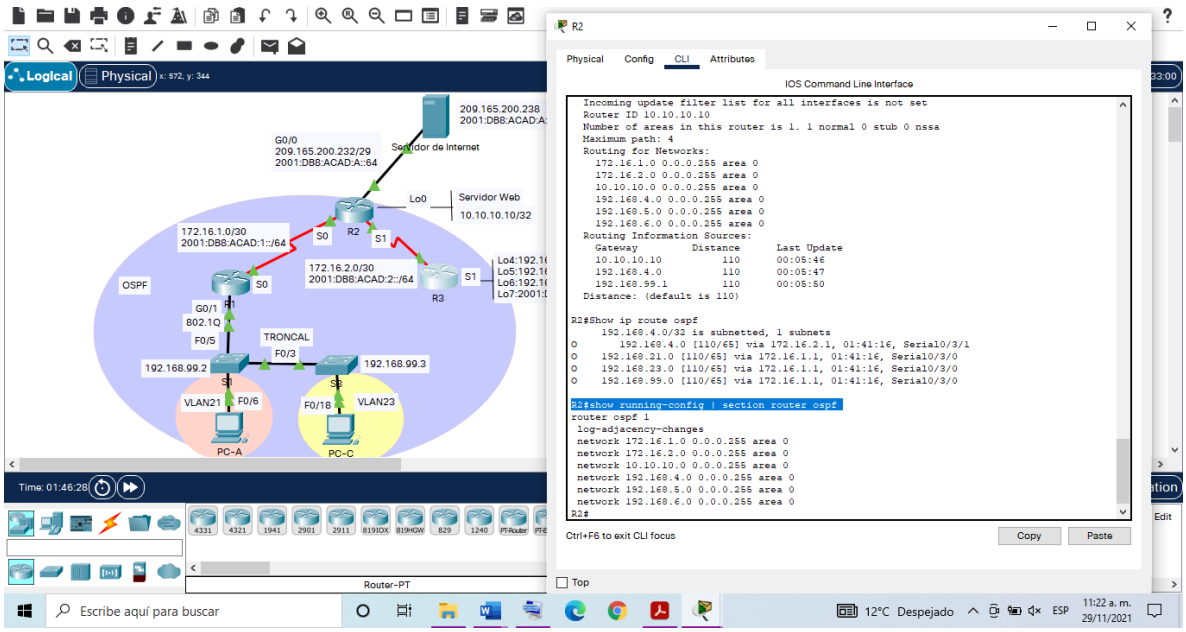
Fuente: Propia.

Figura 24 Comando show run-config | section router ospf en R1



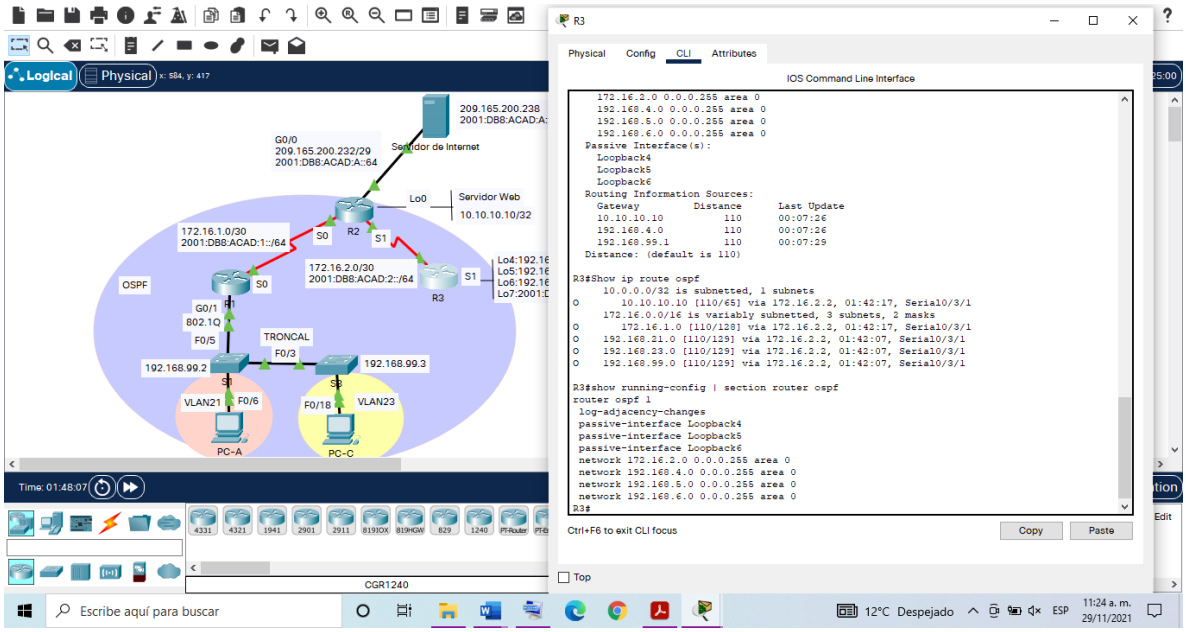
Fuente: Propia.

Figura 25 Comando show run-config | section router ospf en R2



Fuente: Propia.

Figura 26 Comando show run-config | section router ospf en R3



Fuente: Propia.

Parte 5: Implementar dhcp y nat para IPV4

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

Tabla 24 Configuración de R1 como servidor de DHCP para IPV4

Tarea	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)#network 192.168.21.0 255.255.255.0 R1(config)#default-router 192.168.21.1 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(config)#network 192.168.23.0 255.255.255.0 R1(config)#default-router 192.168.23.1 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

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

Tabla 25 Configuración NAT en R2 para IPV4

Tarea	especificación

Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No aplica (El escenario simulado en Packet Tracer no permite la inserción del protocolo 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 No aplica (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP).
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 R2(config)#interface loopback 0 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 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.229 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

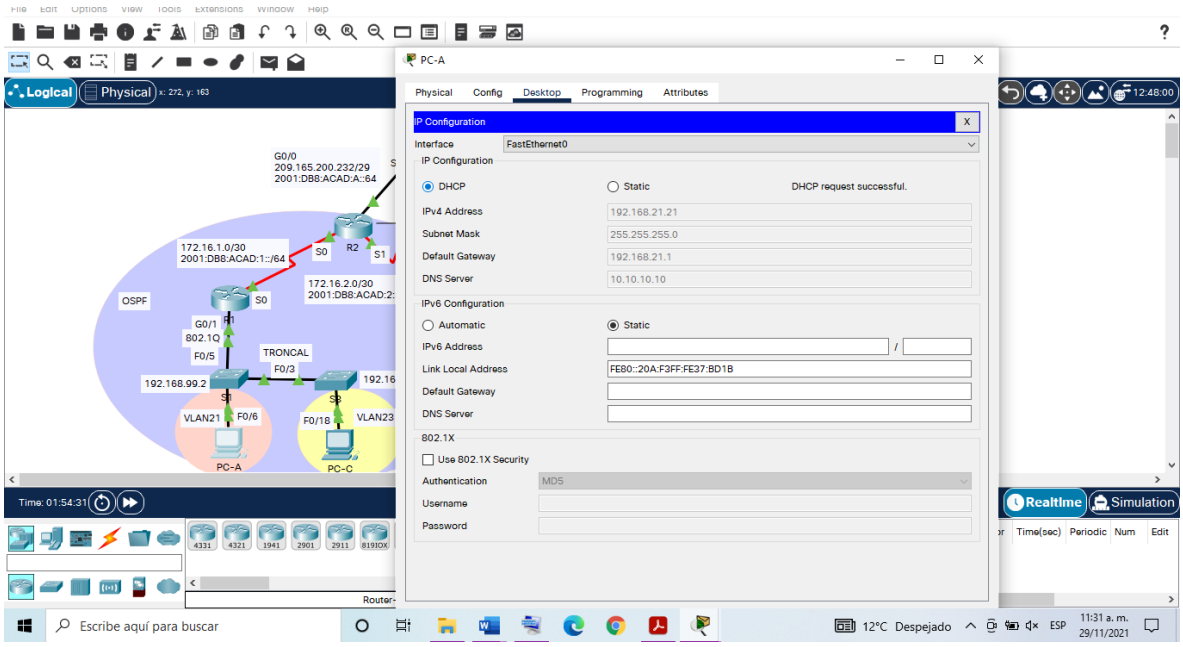
Por medio de las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 26 Verificación de protocolo DHCP y NAT estática.

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 Para este caso, al insertar la IP 209.165.200.229 no tiene acceso ya que en el ambiente de simulación el router no permite la habilitación del protocolo HTTP. Sin embargo, se aplica en el navegador la IP configurada en el servidor que es: 209.165.200.238 y se visualiza la información configurada en el archivo index.html del servidor.	Successful http://209.165.200.238

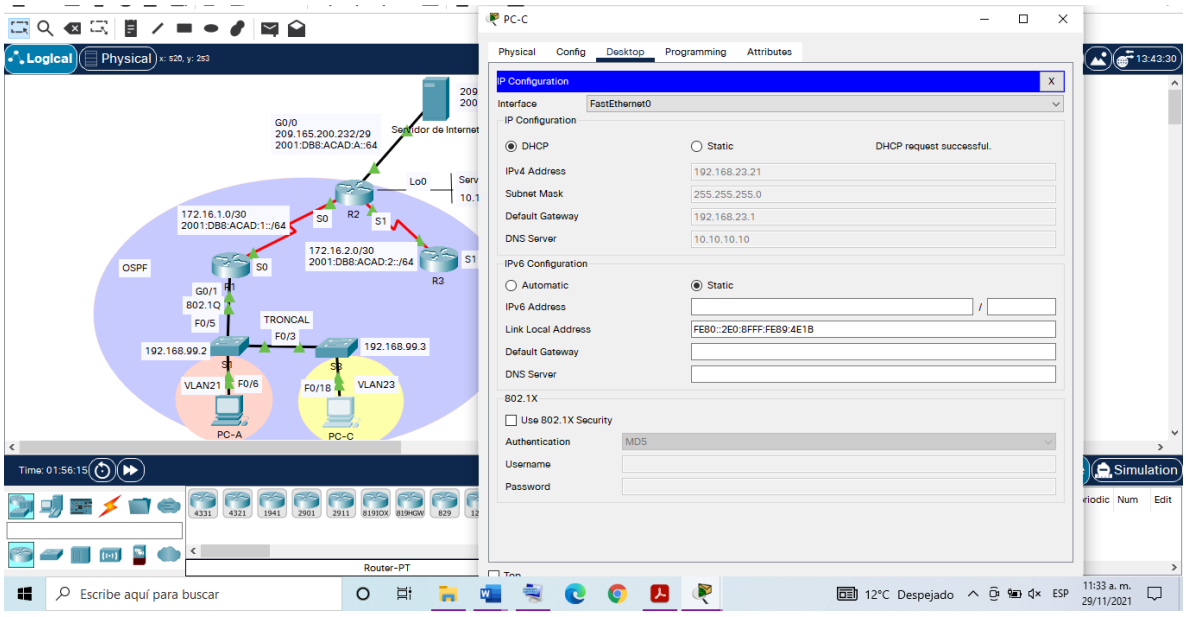
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 27 Verificación del protocolo DHCP en PC-A.



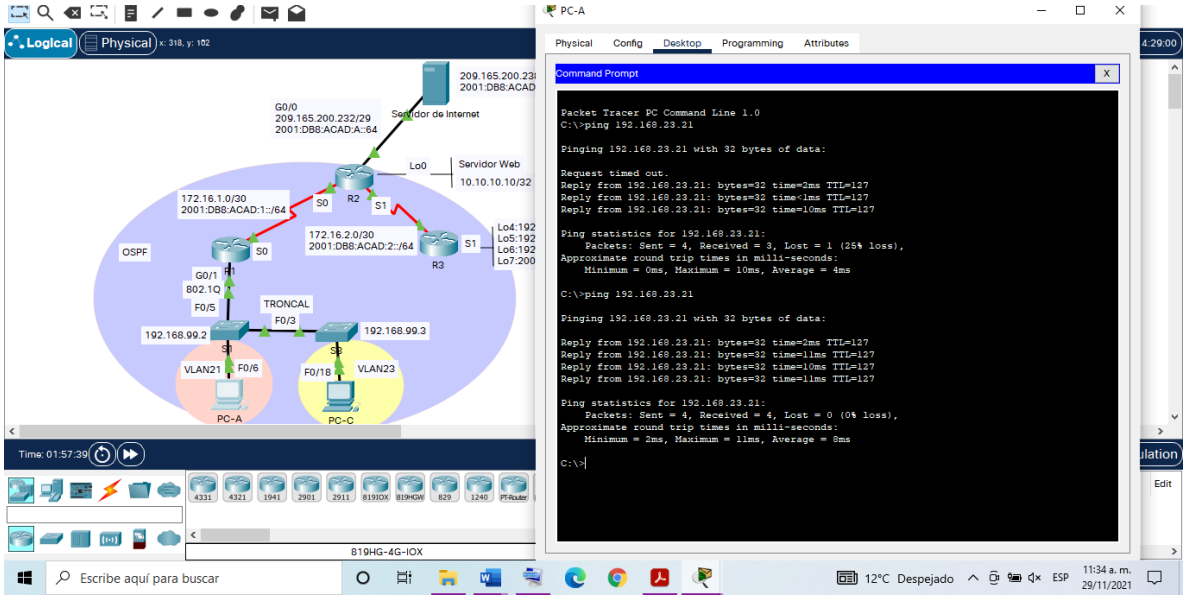
Fuente: Propia

Figura 28 Verificación del protocolo DHCP en PC-B.



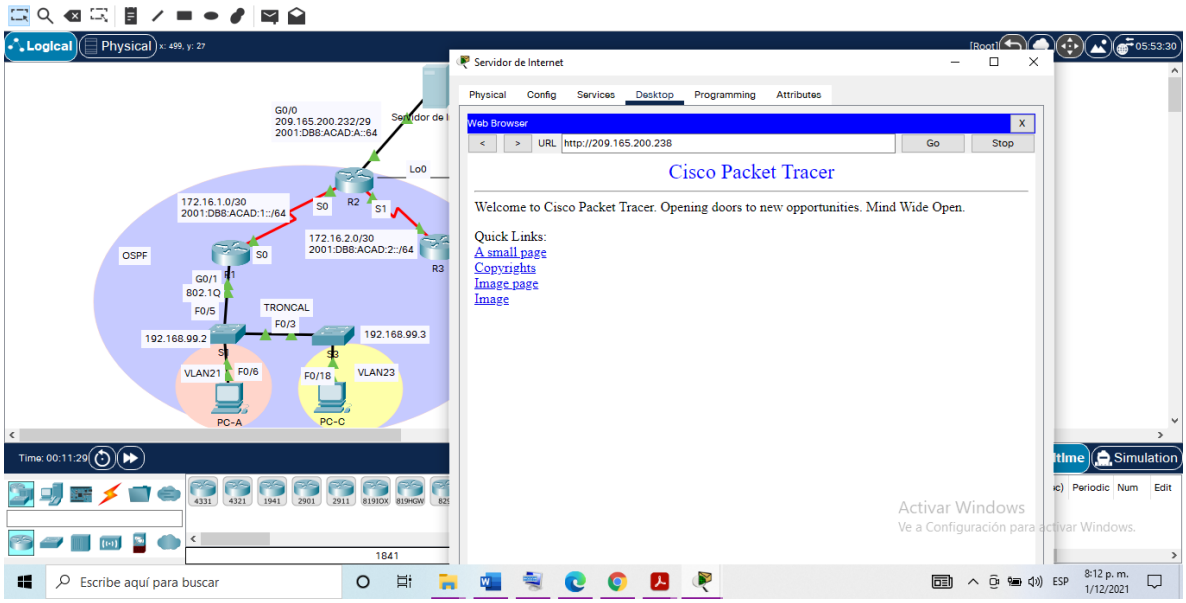
Fuente: Propia

Figura 29 Verificación de conexión entre PC-A y PC-C.



Fuente: Propia

Figura 30 Verificación de acceso al Servidor.



Fuente: Propia

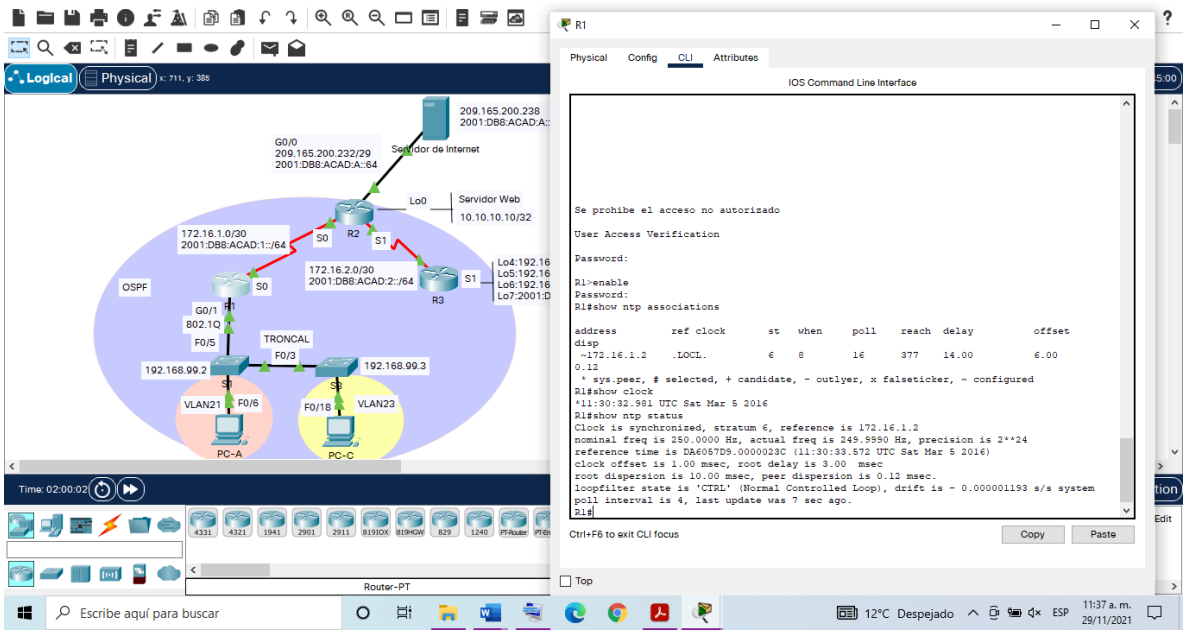
Parte 6: Configurar NTP

Tabla 27 Configuración NTP

Tarea	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 R1#show ntp status

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 31 Verificación de la configuración NTP en R1



Fuente: Propia

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

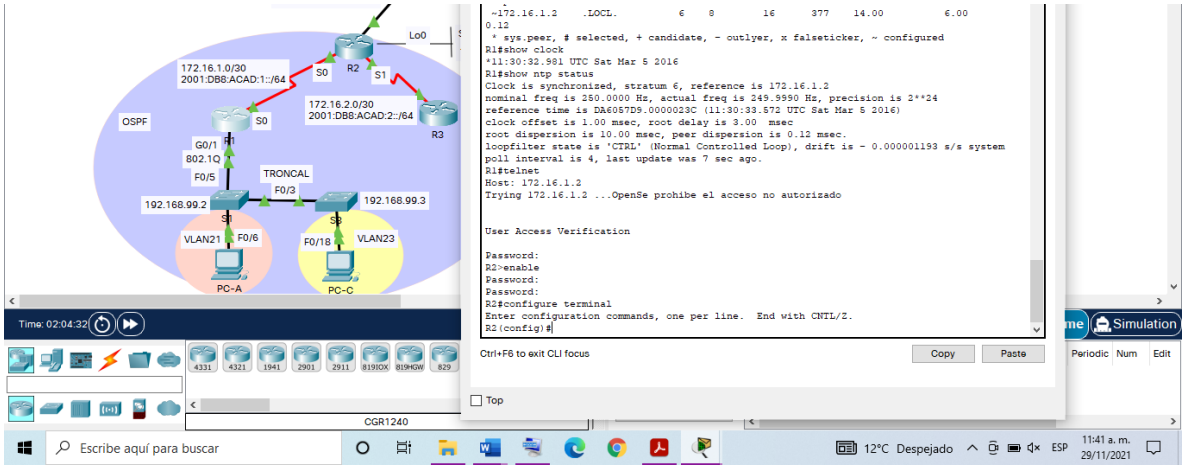
Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 28 Configuración y verificación de las listas de control de acceso ACL

Tarea	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 R2(config)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config-line)#line vty 0 4 R2(config)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 R3#telnet 172.16.1.2

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 32 Verificación de que ACL funciona



Fuente: Propia

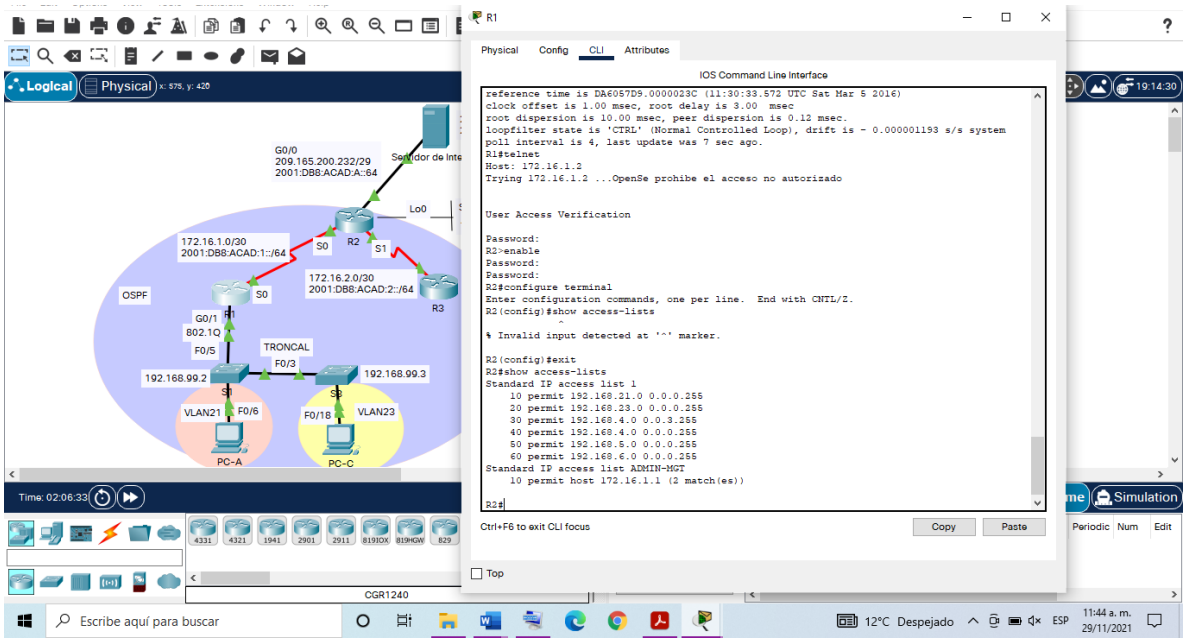
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

Tabla 29 Verificaciones de las configuraciones realizadas en la red

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	# show access-lists
Restablecer los contadores de una lista de acceso	# clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	# show ip interface | include Access #show running-config | include access
¿Con qué comando se muestran las traducciones NAT? Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.	#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	#clear ip nat translations

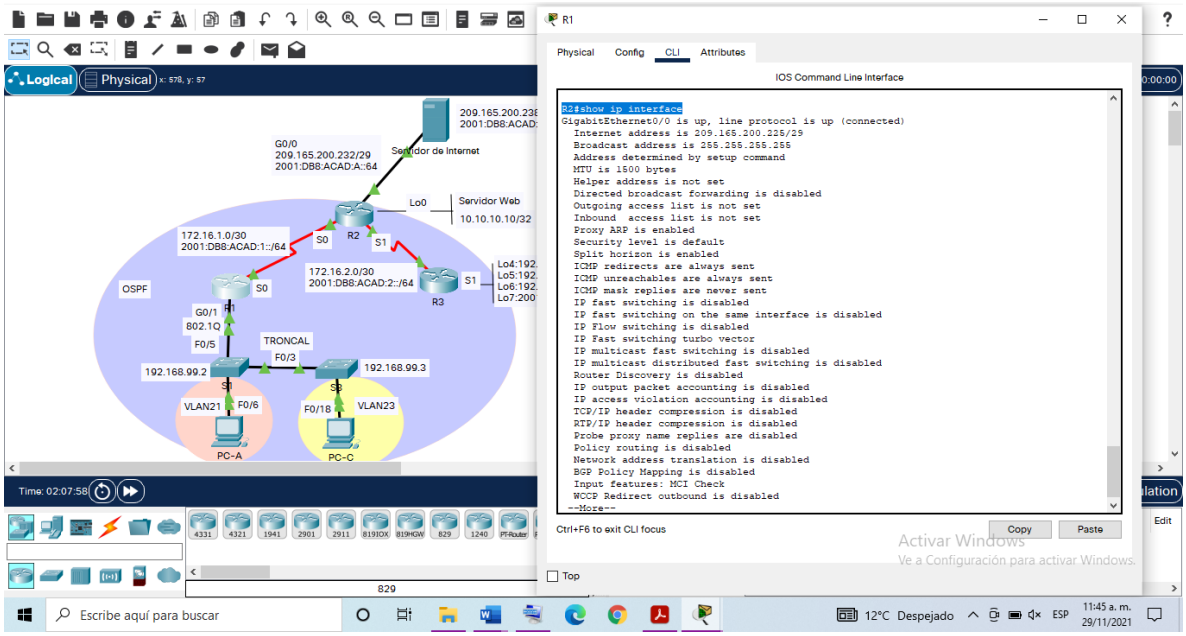
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 33 Verificación del comando show access-list en R2.



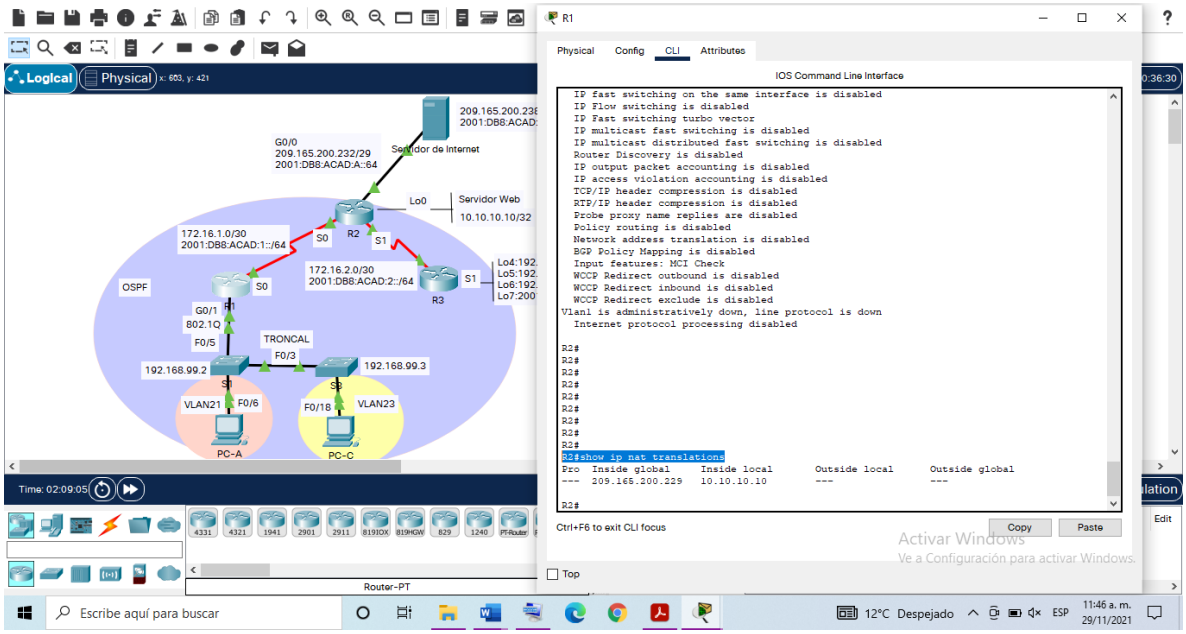
Fuente: Propia

Figura 34 Verificación del comando show ip interface.



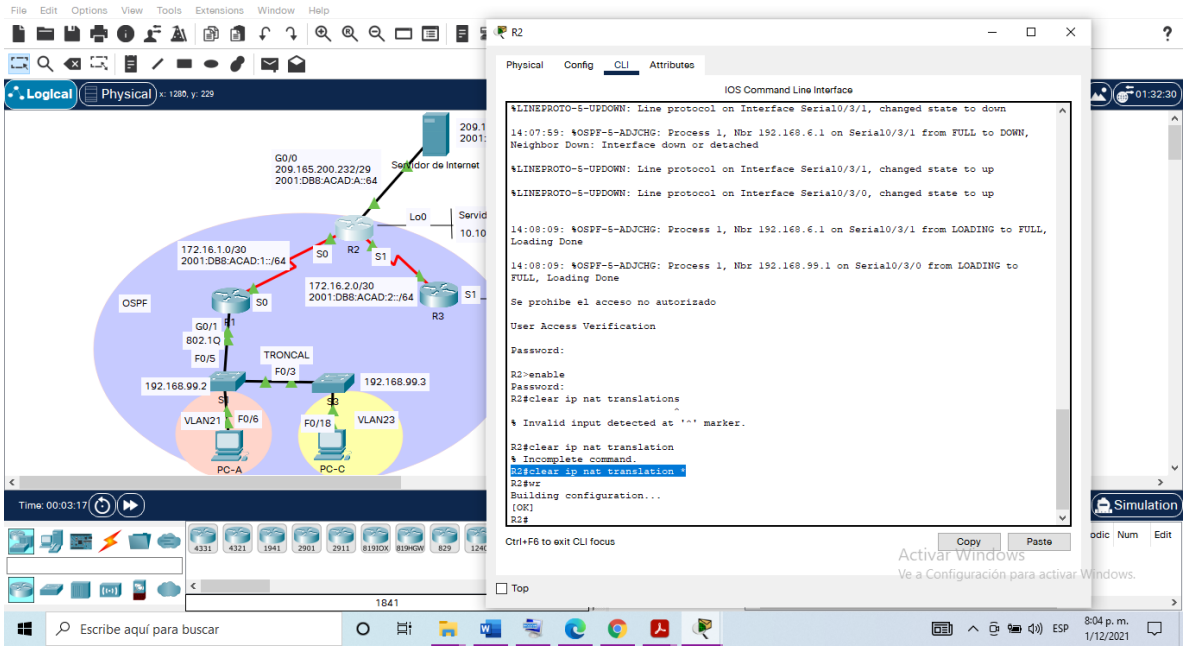
Fuente: Propia

Figura 35 Verificación del comando show ip nat translations.



Fuente: Propia

Figura 36 Comando para eliminar las traducciones de NAT dinámicas



Fuente: Propia

CONCLUSIONES

A partir del desarrollo del primer escenario, observe que es muy importante no solo conocerlo si no además aprenderlo, ya que estamos en una era digital; donde pequeñas, medianas y grandes empresas se están actualizando implementando redes, y es entonces allí cuando es beneficioso dividir en varias subredes ya que estas subredes además trabajan independientemente haciendo la transferencia de información más rápida. Y ahora con la aparición de IPv6, que abarca 128 bits y reemplazará a la versión IPv4 en los próximos años, porque se extiende el rango de direcciones dentro de una red.

Se toman como referencias los dispositivos de tecnología CISCO que permiten la implementación de redes ajustados a conectividad, seguridad, control de acceso, interoperabilidad y en este caso el direccionamiento IPv4.

En el segundo escenario se logró configurar de forma satisfactoria los distintos protocolos de red, observando que son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red como la topología del presente documento. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin. Dichas reglas de formateo determinan si los datos son recibidos correctamente o si son rechazados o ha habido algún tipo de problema en la transferencia de la información y asimismo adicionalmente seguridad a la red.

Para que una red basada en IP se comunique con otras redes, es necesaria la implementación de un protocolo de encaminamiento, como lo son RIP, EIGRP, OSPF, y BGP. Para el caso de redes que poseen subredes es óptimo la implementación del protocolo OSPF, ya que, permite la actualización de la tabla de enrutamiento en cada uno de los dispositivos de enrutamiento de cada una de las redes y a su vez, también permite resumir rutas de máscaras de subred de longitud

variable. Por lo tanto, la implementación de este protocolo de enrutamiento es se necesita conocer o fundamentar los parámetros de funcionamiento del protocolo, entender OSPF para poder aplicarlo en tecnologías inalámbricas, el desarrollo de este escenario me permitió comprender los escenarios actuales y emergentes dando herramientas claras de situaciones reales en mi vida profesional.

REFERENCIAS

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10