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

ARLEY YAMID CASTAÑEDA CARDENAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
YOPAL
2022

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

ARLEY YAMID CASTAÑEDA CARDENAS

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

DIRECTOR:
Msc. HÉCTOR JULIAN PARRA MOGOLLÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
YOPAL
2022

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Yopal, 26 de junio de 2022

AGRADECIMIENTOS

Dando gracias primeramente a Dios, el presente trabajo es el resultado de mi gran esfuerzo con logros alcanzados en el proceso académico. Así mismo agradezco el empuje de cada uno de mis familiares e instructores que son guías para ejecutar los conocimientos adquiridos que son da grandes frutos para un buen crecimiento profesional en el hacer, saber y saber hacer.

Finalmente agradecer a todos los seres especiales que desde un principio se preocuparon por brindándome armonía y empuje para llegar a este punto.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DNS: (Domain Name System). Traductor de los nombres de los dominios tales como google.com a una dirección IP

VLAN: (Red de área local virtual). Son redes de area local que se agrupan de manera lógica no física, ofreciendo así una independencia y privacidad entre grupos de usuarios de la red.

IPV4: (Internet Protocol versión 4). Las direcciones IP son números de 32 bits y la estructura de una dirección IPv4 se denomina notación decimal punteada y se representa con cuatro números decimales entre 0 y 255. Las direcciones IPv4 son números asignados a los dispositivos individuales conectados a una red

IPV6: (Internet Protocol versión 6). Las direcciones IPv6 son de una longitud de 128 bits y son una cadena de valores hexadecimales. Cada cuatro bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Los grupos de cuatro dígitos hexadecimales se separan por dos puntos (:). Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas.

OSPF: (Open Shortest Path First). En español “El camino más corto primero” Protocolo de direccionamiento dinámico interior, sus funciones principales son el aprender, anunciar información de enrutamiento sobre subred Ip a los routers cercanos, elije a base a una métrica escoge la mejor ruta, si cambia alguna configuración o falla pasa a elige una nueva mejor ruta; haciendo un proceso de convergencia.

Packet Tracer: Es un simulador de redes reales, proporciona tres menús principales; agrega dispositivos y los conecta a través de cables o inalámbricos. Selecciona, elimina, inspecciona, etiqueta y agrupa componentes dentro una red. Administra red abriendo una red existente o de muestra, guarda y/o modifica perfil de usuario o preferencias.

RESUMEN

En este trabajo final es parte integral del diplomado de certificación Cisco, específicamente para el módulo CCNP (Cisco Certified Network Professional), donde se abordan varios temas de importancia relevante al momento de implementar la conmutación y conectividad entre diferentes hosts, dentro de las redes de Telecomunicaciones. Para esto se usan varios métodos de enrutamiento dinámico y estático según las necesidades específicas de cada escenario.

Los equipos de routing and switching para este informe son virtuales y no cuentan con la electrónica real de los componentes físicos; sin embargo, proporcionan una excelente opción para realizar pruebas y configuraciones en escenarios controlados que pueden exportarse fácilmente a los equipos reales.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In this final work, that is an integral part of the Cisco certification course, specifically for the CCNP (Cisco Certified Network Professional) module, where several topics of relevant importance are addressed when implementing switching and connectivity between different hosts, within networks of Telecommunications. For this, various dynamic and static routing methods are used according to the specific needs of each scenario.

The routing and switching equipment for this report is virtual and does not have the real electronics of the physical components; however, they provide an excellent option for testing and configuration in controlled scenarios that can be easily exported to real equipment.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

Las redes de datos constituyen la base fundamental de la civilización actual y son transversales a todas las áreas del conocimiento y la industria. Según Chaparro (1998), “Las tecnologías de la información y las telecomunicaciones están teniendo un profundo impacto en todos los sectores de la actividad humana, desde la producción, hasta la educación y los servicios de salud”. Por esta razón es pertinente y apropiado que el ingeniero de sistemas egresado de UNAD adquiera y desarrolle habilidades sólidas en este campo y las ponga en práctica en su vida profesional.

El siguiente trabajo individual y parte final del Diplomado de profundización Cisco (diseño e implementación de soluciones integradas LAN / WAN); en el cual se realizó la simulación de dos escenarios de redes de datos en donde se pretende poner a prueba las habilidades adquiridas a lo largo del diplomado y se realiza un paso a paso detallado de las diferentes configuraciones de los dispositivos de red.

En el primer escenario se deberá configurar varios dispositivos de una red pequeña; se debe configurar un Router, un swich y dos PCs, con un subnetting donde la LAN 1 se necesita para 100 host y una LAN2 para 50 hosts. Se debe tomar el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Estas actividades se realizaron con la ayuda de la herramienta Packet Tracert; la cual permite en un entorno controlado realizar el montaje y las pruebas requeridas antes de exportar las configuraciones a un entorno real. Los montajes se realizaron de acuerdo con la topología lógica que se plantea en la guía y constituyen un aprendizaje significativo para el ingeniero de sistemas.

DESARROLLO

1. ESCENARIO 1

Figura 1 Escenario 1

Fuente: Prueba de habilidades CCNA 2022

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Objetivos

Parte 1: Construir en el simulador la Red
Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1
Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

1.1 Parte 1: Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

1.2 Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1 Direccionamiento

Ítem	Requerimiento
Dirección de Red	192.168.33.0 Donde X corresponde a los últimosdos dígitos de su cédula.
Requerimiento de host Subred LAN1	100 host 192.168.33.0/25 para 126 Host usables
Requerimiento de host Subred LAN2	50 host 192.168.33.128/26 para 62 Host usables
R1 G0/0/1	Primera dirección de host de la subred LAN1 192.168.33.1/25
R1 G0/0/0	Primera dirección de host de la subred LAN2 192.168.33.129/26
S1 SVI	Segunda dirección de host de la subred LAN1 192.168.33.2/25
PC-A	Última dirección de host de la subred LAN1 192.168.33.126/25
PC-B	Última dirección de host de la subred LAN2 192.168.33.190/26

Fuente: Prueba de habilidades CCNA 2022

Tabla 2 Subneteo

LAN	# Total Host	# Hosts utilizables	Dirección de red	Mascara	Rango de host utilizable	Dirección Broadcast
1	128	126	192.168.33.0/25	255.255.255.128	192.168.33.1 - 192.168.33.126	192.168.33.127
2	64	62	192.168.33.128/26	25.255.255.192	192.168.33.129 - 192.168.33.190	192.168.33.191

Fuente: Propia

1.3 Parte 3: Configure aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

1.3.1 Paso 1: Configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 Configuración aspectos básicos 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 R1(config)#
Nombre de dominio	R1(config)#ip domain-name ccnalab.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 R1(config)#
Establecer la longitud mínima para lascontraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#user admin privilege 15 secret admin1pass Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTYpara que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit R1(config)#
Configurar VTY solo aceptando SSH	R1(config)#ip ssh version 2 Please create RSA keys (of at least 768 bits size) to enable SSH v2. R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #Esta prohibido el acceso no autorizado#
Configurar interfaz G0/0/0	R1(config)#interface giga 0/0/0 R1(config-if)#description R1 a PC-B R1(config-if)#ip address 192.168.33.129 255.255.255.192 R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

	R1(config-if)#exit R1(config)#
Configurar interfaz G0/0/1	R1(config)#interface giga 0/0/1 R1(config-if)#description R1 a S1 R1(config-if)#ip address 192.168.33.1 255.255.255.128 R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up R1(config-if)#exit R1(config)#
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa The name for the keys will be: R1.ccnalab.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] R1(config)#

Fuente: Prueba de habilidades CCNA 2022

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 4 Configuración aspectos básicos S1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1 S1(config)#
Nombre de dominio	S1(config)# ip domain-name ccnalab.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 S1(config)#
Crear un usuario administrativo en la base de datos local	S1(config)#user admin privilege 15 secret admin1pass Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit S1(config)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#ip ssh version 2 Please create RSA keys (of at least 768 bits size) to enable SSH v2. S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit S1(config)#
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #Esta prohibido el acceso no autorizado#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa The name for the keys will be:

	S1.ccnalab.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]
Configurar la interfaz de administración (SVI)	S1(config)#vlan 1 *Mar 1 1:4:8.975: %SSH-5-ENABLED: SSH 2 has been enabled S1(config-vlan)#exit S1(config)#interface vlan 1 S1(config-if)#no shutdown S1(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up S1(config-if)#ip address 192.168.33.2 255.255.255.128 S1(config-if)#exit S1(config)#
Configuración del gateway predeterminado	S1(config)#ip default-gateway 192.168.33.1

Fuente: Prueba de habilidades CCNA 2022

1.3.2 Paso 2. Configurar los equipos

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 5 Configuración de Red PC-A

PC-A Network Configuration	
Descripción	PC-A
Dirección física	0060.70E3.AACA
Dirección IP	192.168.33.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.33.1

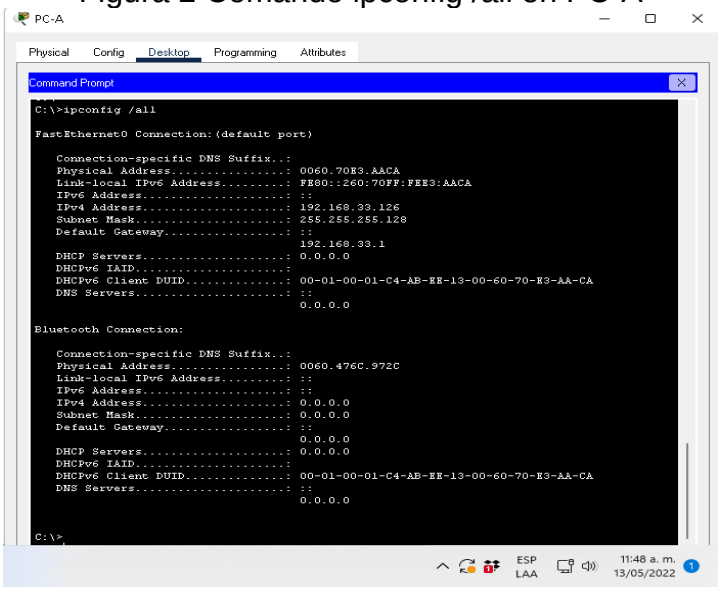
Fuente: Prueba de habilidades CCNA 2022

Tabla 6 Configuración de Red PC-B

PC-B Network Configuration	
Descripción	PC-B
Dirección física	0002.161D.4B5B
Dirección IP	192.168.33.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.33.129

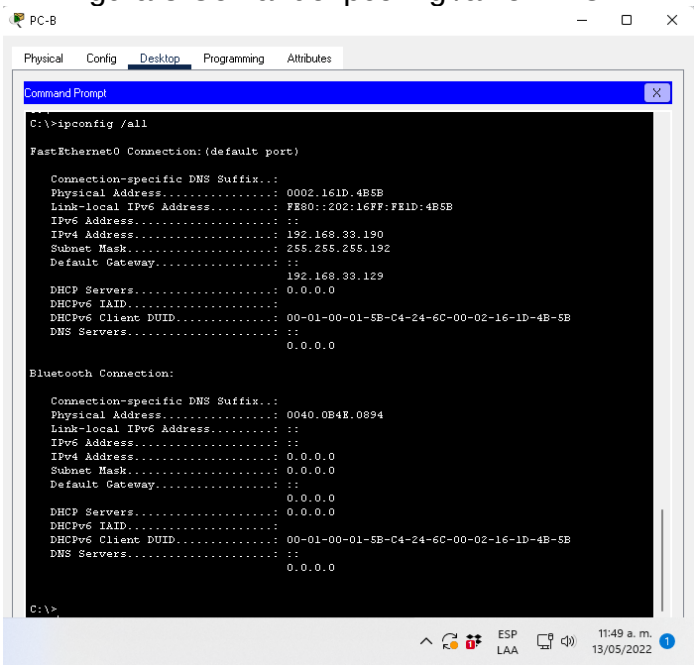
Fuente: Prueba de habilidades CCNA 2022

Figura 2 Comando ipconfig /all en PC-A



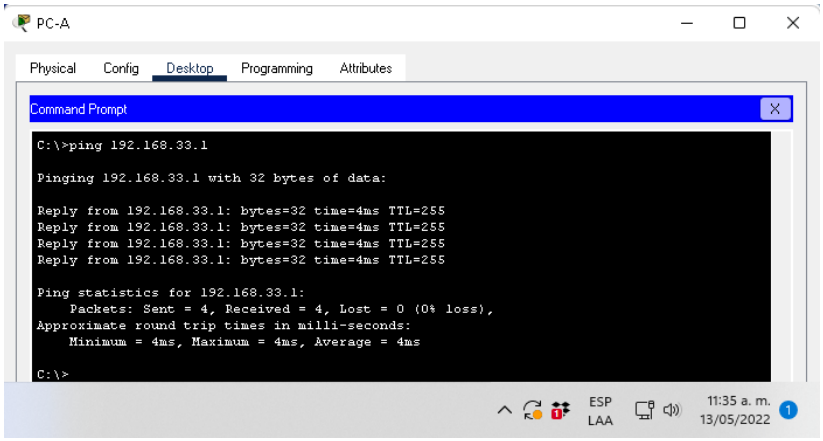
Fuente: Propia

Figura 3 Comando ipconfig /all en PC-B



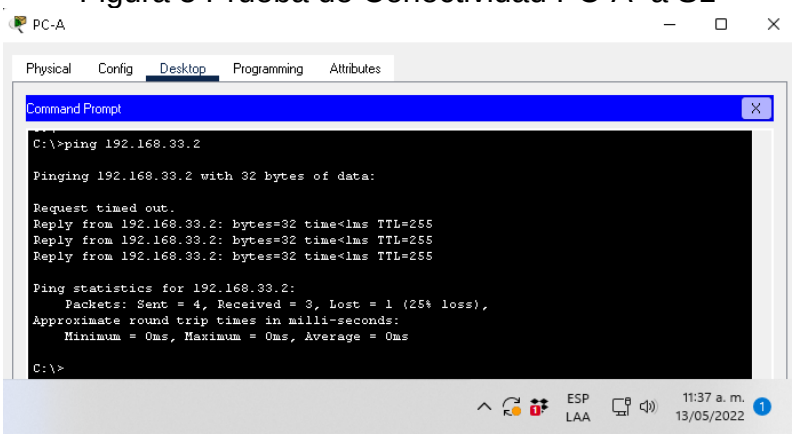
Fuente: Propia

Figura 4 Prueba de Conectividad PC-A a R1



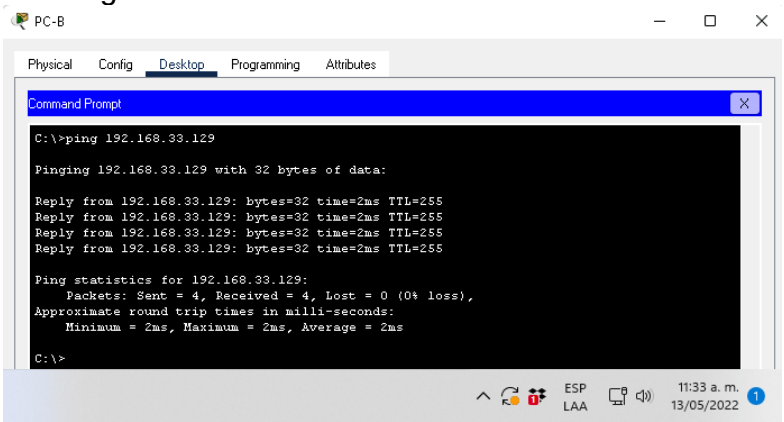
Fuente: Propia

Figura 5 Prueba de Conectividad PC-A a S1



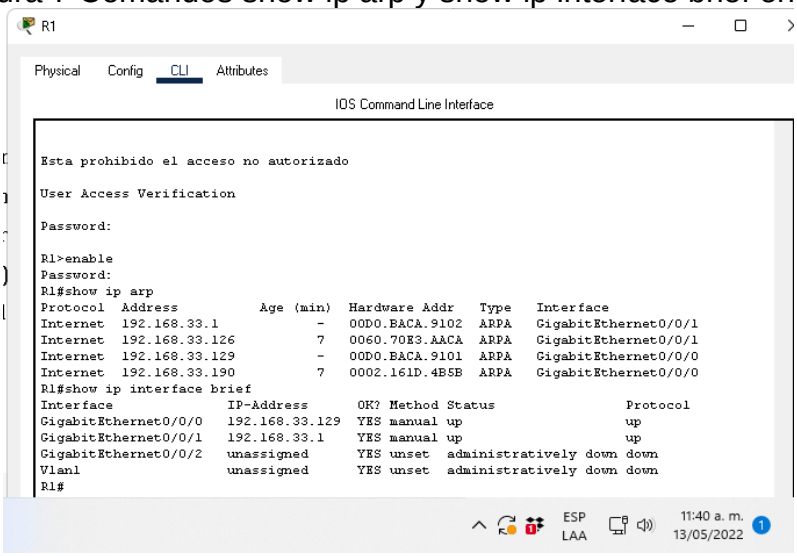
Fuente: Propia

Figura 6 Prueba de Conectividad PC-B a R1



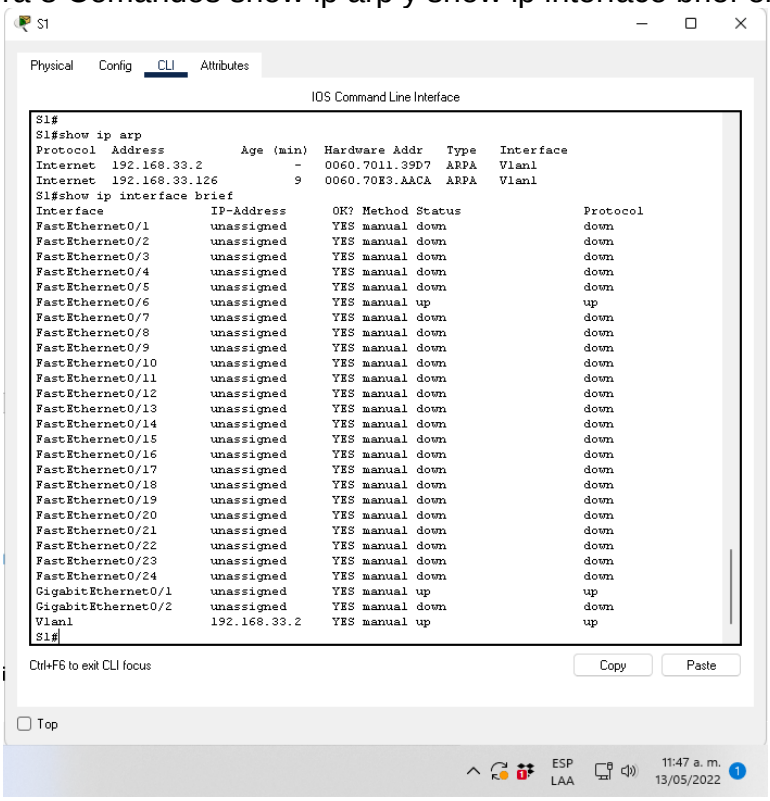
Fuente: Propia

Figura 7 Comandos show ip arp y show ip interface brief en R1



Fuente: Propia

Figura 8 Comandos show ip arp y show ip interface brief en S1

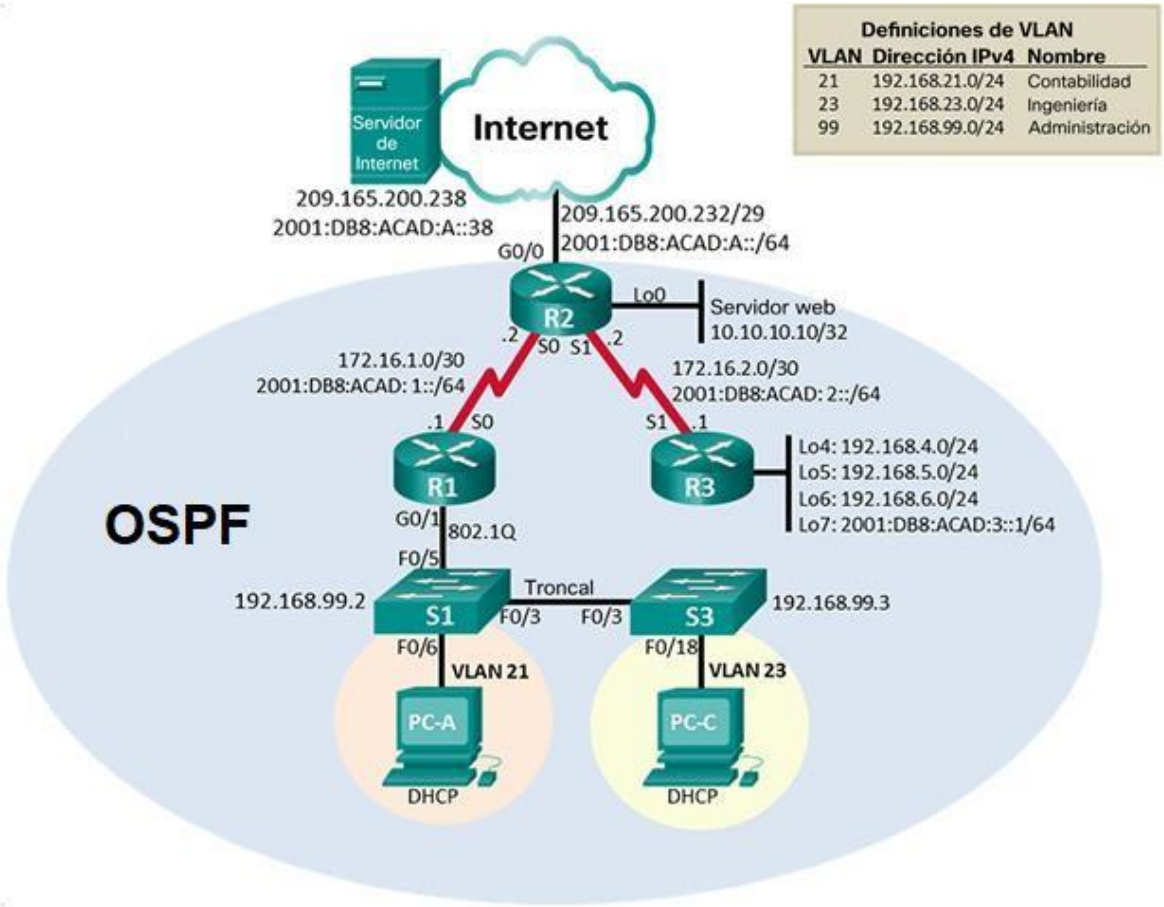


Fuente: Propia

2. ESCENARIO 2

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

Figura 9 Topología Escenario 2



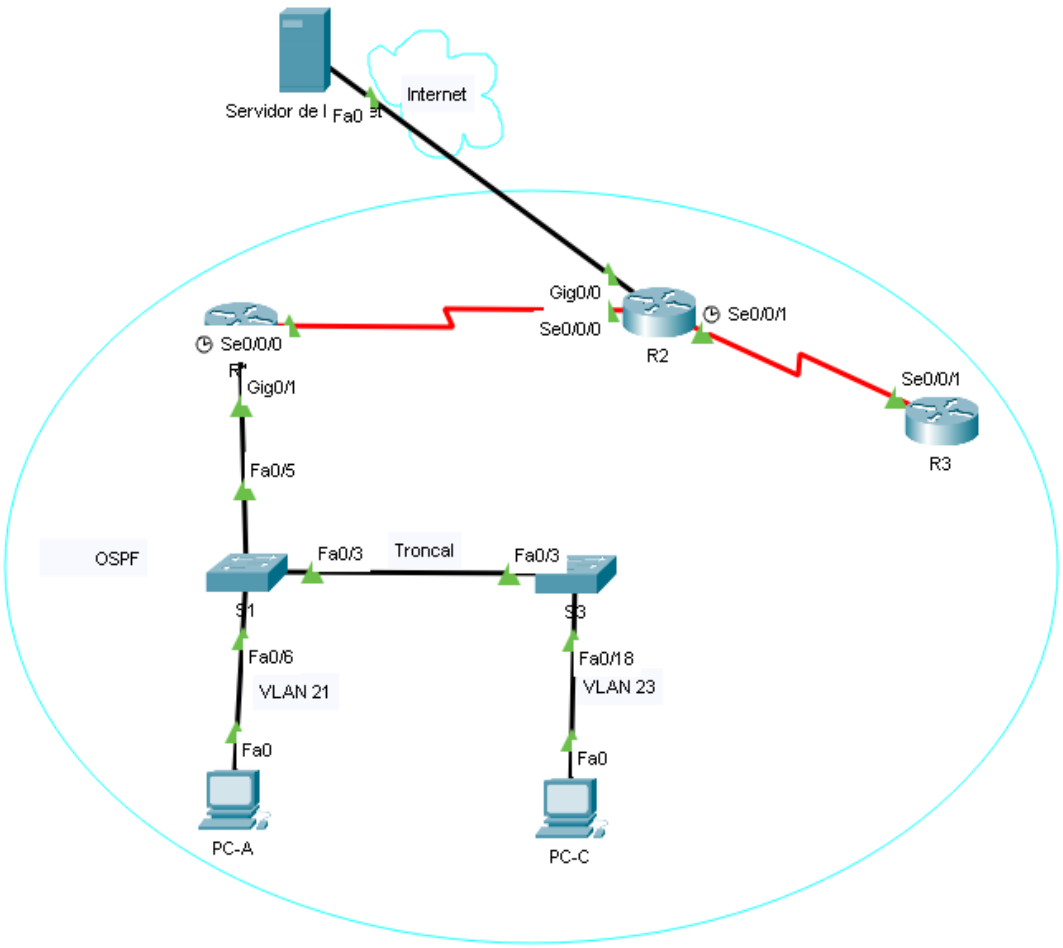
Fuente: Prueba de habilidades CCNA 2022

2.1 Parte 1: Inicializar dispositivos

2.1.1 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.

Figura 10 Simulación Packet Tracer Escenario 2



Fuente: Propia

Tabla 7 Iniciar y volver a cargar configuración de routers y switches Escenario 2

Tarea	Comando de IOS
Eliminar el archivo startup-config detodos los routers	Router>enable Router#erase startup-config

	Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Router#
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm] System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 2010 by cisco Systems, Inc.
Eliminar el archivo startup-config de todos los switches y eliminar la base dedatos de VLAN anterior	Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch#
Volver a cargar ambos switches	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 %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch#
Verificar que la base de datos de VLAN noesté en la memoria flash en ambos switches	Switch>enable Switch#show flash Directory of flash:/ 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free) Switch#

Fuente: Prueba de habilidades CCNA 2022

2.2 Parte 2: Configurar los parámetros básicos de los dispositivos

2.2.1 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):

Tabla 8 Configuración del servidor de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Prueba de habilidades CCNA 2022

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

2.2.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9 Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router(config)#hostname R1

	R1(config)#
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class R1(config)#
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#
Mensaje MOTD	R1(config)#banner motd #Se prohibe el acceso no autorizado.# R1(config)#
Interfaz S0/0/0	R1(config)#interface s0/0/0 Establezca la descripción R1(config-if)#description R1 a R2 Establecer la dirección IPv4 R1(config-if)#ip address 172.16.1.1 255.255.255.252 Establecer la dirección IPv6 R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 Establecer la frecuencia de reloj en 128000 R1(config-if)#clock rate 128000 Activar la interfaz R1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down R1(config-if)#exit R1(config)#
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

	Configurar una ruta IPv6 predeterminada de S0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Fuente: Prueba de habilidades CCNA 2022

Nota: Todavía no configure G0/1.

2.2.3 Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10 Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#
Nombre del router	R2 Router(config)#hostname R2 R2(config)#
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class R2(config)#
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#passwor cisco R2(config-line)#login R2(config-line)#exit R2(config)#
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit R2(config)#
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption R2(config)#
Habilitar el servidor HTTP	R2(config)#ip http server (funciona en equipo real)
Mensaje MOTD	R2(config)#banner motd #Se prohibe el acceso no autorizado.#

	R2(config)#
Interfaz S0/0/0	R2(config)#interface s0/0/0 Establezca la descripción R2(config-if)#description R2 a R1 Establezca la dirección IPv4. R2(config-if)#ip address 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. R2(config-if)#ipv6 address 2001:DB8:ACAD:A::2/64 Activar la interfaz R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#interface s0/0/1 Establecer la descripción R2(config-if)#description R2 a R3 Establezca la dirección IPv4. R2(config-if)#ip address 172.16.2.2 255.255.255.252 Establezca la dirección IPv6. R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 Establecer la frecuencia de reloj en 128000. R2(config-if)#clock rate 128000 Activar la interfaz R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. R2(config)#interface g0/0 R2(config-if)#description R2 a Internet Establezca la dirección IPv4. R2(config-if)#ip address 209.165.200.233 255.255.255.248 Establezca la dirección IPv6. R2(config-if)#ipv6 address

	2001:DB8:ACAD:A::3/64 Activar la interfaz R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. R2(config-if)#description Web Simulado Establezca la dirección IPv4. R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ipv6 route ::/0 g0/0

Fuente: Prueba de habilidades CCNA 2022

2.2.4 Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 11 Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router(config)#hostname R3 R3(config)#
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class R3(config)#
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit

	R3(config)#
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#
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	Establecer la descripción R3(config)#interface s0/0/1 R3(config-if)#description R3 a R2 Establezca la dirección IPv4. R3(config-if)#ip address 172.16.2.1 255.255.255.252 Establezca la dirección IPv6. R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 Activar la interfaz R3(config-if)#no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. R3(config)#interface loopback 4 R3(config-if)# %LINK-5-CHANGED: Interface Loopback4, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#
Interfaz loopback 5	Establezca la dirección IPv4. R3(config)#interface loopback 5 R3(config-if)# %LINK-5-CHANGED: Interface Loopback5,

	changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#
Interfaz loopback 6	Establezca la dirección IPv4. R3(config)#interface loopback 6 R3(config-if)# %LINK-5-CHANGED: Interface Loopback6, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#
Interfaz loopback 7	Establezca la dirección IPv6. R3(config)#interface loopback 7 R3(config-if)# %LINK-5-CHANGED: Interface Loopback7, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R3(config)#ip route 0.0.0.0 0.0.0.0 g0/0 Configure una ruta IPv6 predeterminada de G0/0. R3(config)#ipv6 route ::/0 g0/0

Fuente: Prueba de habilidades CCNA 2022

2.2.5 Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12 Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#
Nombre del switch	Switch(config)#hostname S1 S1(config)#
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class S1(config)#
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit S1(config)#
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit S1(config)#
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: Prueba de habilidades CCNA 2022

2.2.6 Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#
Nombre del switch	Switch(config)#hostname S3 S3(config)#
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class S3(config)#
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit S3(config)#
Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit S3(config)#
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: Prueba de habilidades CCNA 2022

2.2.7 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:

Tabla 14 Ping entre los dispositivos de red

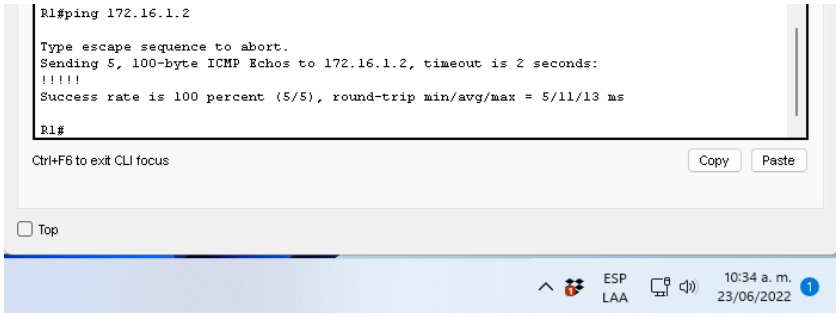
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2

			Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/14 ms
R2	R3, S0/0/1	172.16.2.1	R2#ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/16 ms
PC de Internet	Gateway predeterminado	209.165.200.233	C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time=2ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 2ms, Average = 0ms

Fuente: Prueba de habilidades CCNA 2022

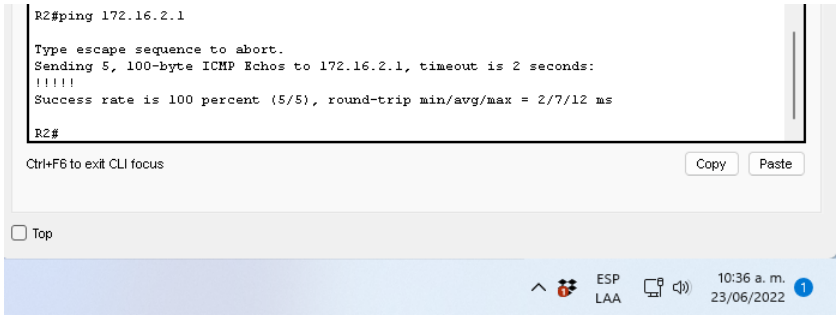
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicencorrectamente.

Figura 11 Ping del R1 al R2



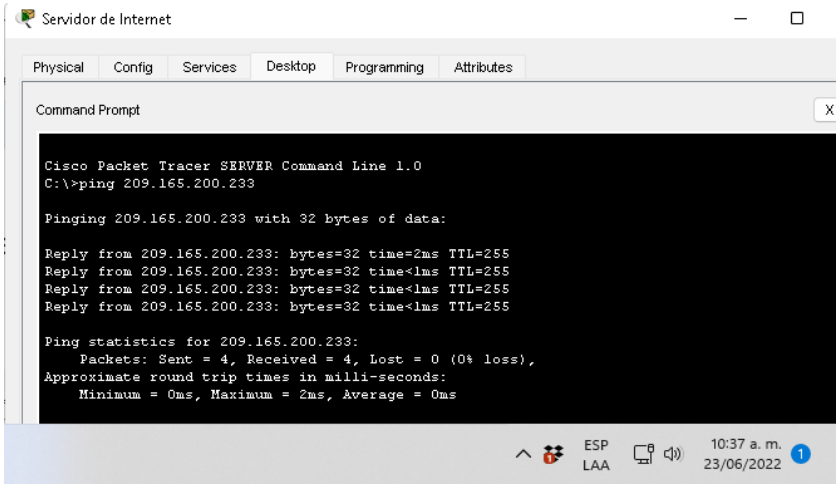
Fuente: Propia

Figura 12 Ping del R2 al R3



Fuente: Propia

Figura 13 Ping Equipo de Internet a Gateway



Fuente: Propia

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

2.3.1 Paso 1: Configura S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14 Configuración seguridad para S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1#confi term Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit S1(config)#
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up

	S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#
Asignar el gateway predeterminado	S1(config-if)#ip default-gateway 192.168.99.1 S1(config)#
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1S1(config-if)#
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit S1(config)#
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#exit S1(config)#
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#
Apagar todos los puertos sin usar	S1(config)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit S1(config)#

Fuente: Prueba de habilidades CCNA 2022

2.3.2 Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15 Configuración seguridad para S3

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 Administracion S3(config-vlan)#exit S3(config)#
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)#
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1 S3(config)#
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit S3(config)#
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range fa0/1- 2,fa0/4-17,gi0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit S3(config)#
Asignar F0/18 a la VLAN 23 (Se corrige así aparece en la topología)	S3(config)#interface f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 S3(config-if)#exit S3(config)#
Apagar todos los puertos sin usar	S3(config)#interface range f0/1-2,f0/4-17,f0/19-24,g0/1-2 S3(config-if-range)#shutdown

Fuente: Prueba de habilidades CCNA 2022

2.3.3 Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16 Configuración seguridad para R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21

	R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit R1(config)#
Configurar la subinterfaz 802.1Q .23 enG0/1	R1(config)#interface g0/1.23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#
Configurar la subinterfaz 802.1Q .99 enG0/1	R1(config)#interface g0/1.99 R1(config-subif)#description LAN de Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#
Activar la interfaz G0/1	R1(config)#interface g0/1 R1(config-if)#no shutdown

Fuente: Prueba de habilidades CCNA 2022

2.3.4 Paso 4: Verificar la conectividad de la red

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

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

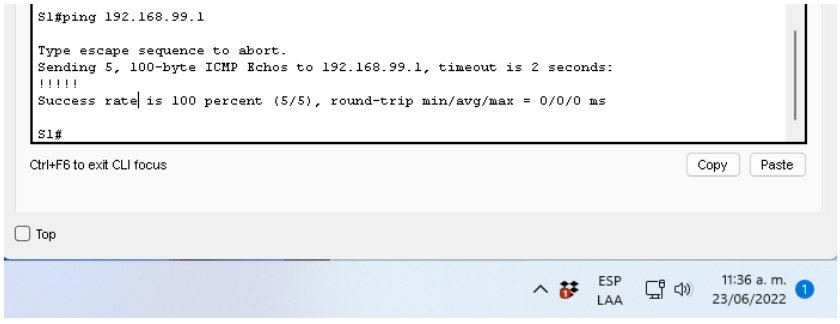
Tabla 17 Ping entre switches y el R1

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! 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 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! 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 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! 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 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

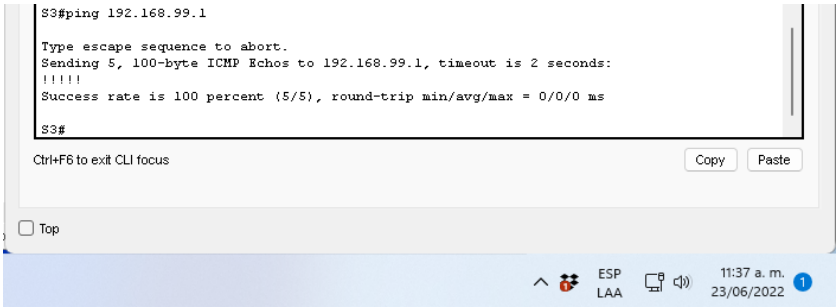
Fuente: Prueba de habilidades CCNA 2022

Figura 14 Ping desde S1 a R1, dirección VLAN 99



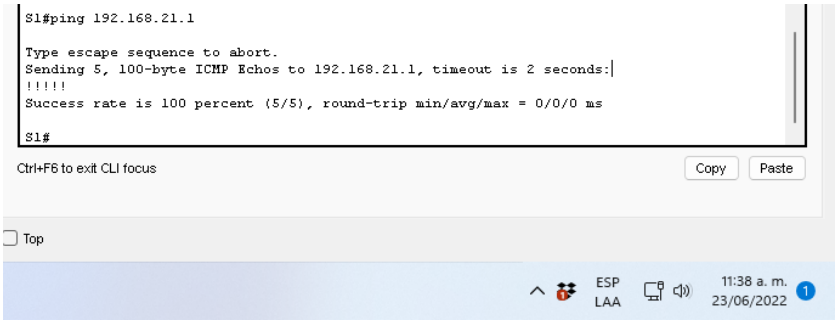
Fuente: Propia

Figura 15 Ping desde S3 a R1, dirección VLAN 99



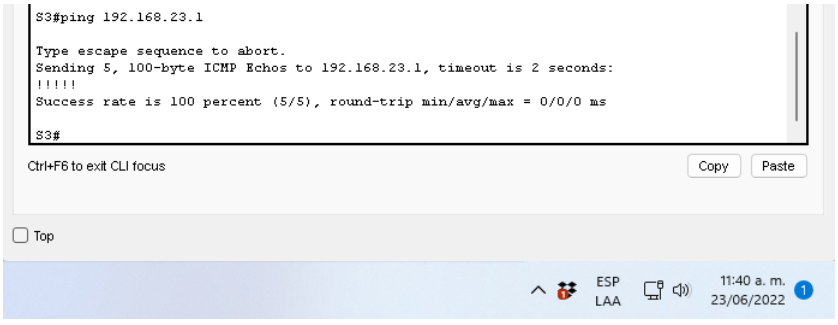
Fuente: Propia

Figura 16 Ping desde S1 a R1, dirección VLAN 21



Fuente: Propia

Figura 17 Ping desde S3 a R1, dirección VLAN 23



Fuente: Propia

2.4 Parte 4: Configurar el protocolo de routing dinámico OSPF

2.4.1 Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18 Configuración OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 R1(config-router)#
Desactive la sumarización automática	R1(config-router)#no auto-summary ^ % Invalid input detected at '^' marker. Comando Invalido sirve para configurar RIP

Fuente: Prueba de habilidades CCNA 2022

2.4.2 Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19 Configuración OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)# 03:50:16: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0 from LOADING to FULL, Loading Done

	R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 209.165.200.232 0.0.0.7 area 0 Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface Loopback0
Desactive la sumarización automática.	Comando Invalido sirve para configurar RIP

Fuente: Prueba de habilidades CCNA 2022

2.4.3 Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 20 Configuración OSPFv3 en el R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 1 R3(config-rtr)#router-id 1.1.1.1
Anunciar redes IPv4 conectadas directamente	R3(config-rtr)#interface s0/0/1 R3(config-if)#ipv6 ospf 1 area 0 R3(config-if)#exit R3(config)#
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config)#ipv6 router ospf 1 R3(config-rtr)#passive-interface Loopback4 R3(config-rtr)#passive-interface Loopback5 R3(config-rtr)#passive-interface Loopback6 R3(config-rtr)#passive-interface Loopback7 R3(config-rtr)#exit
Desactive la sumarización automática.	Comando Invalido sirve para configurar RIP

Fuente: Prueba de habilidades CCNA 2022

2.4.4 Paso 4: Verificar la información de OSPF

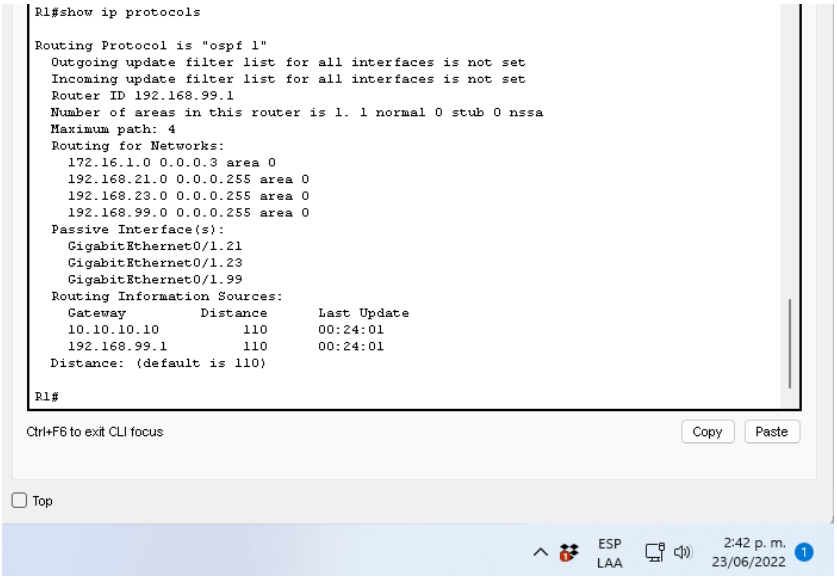
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 21 Verificación de información de OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID delrouter, las redes de routing y las interfaces pasivas configuradasen un router?	show ip protocols
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuraciónen ejecución?	show run

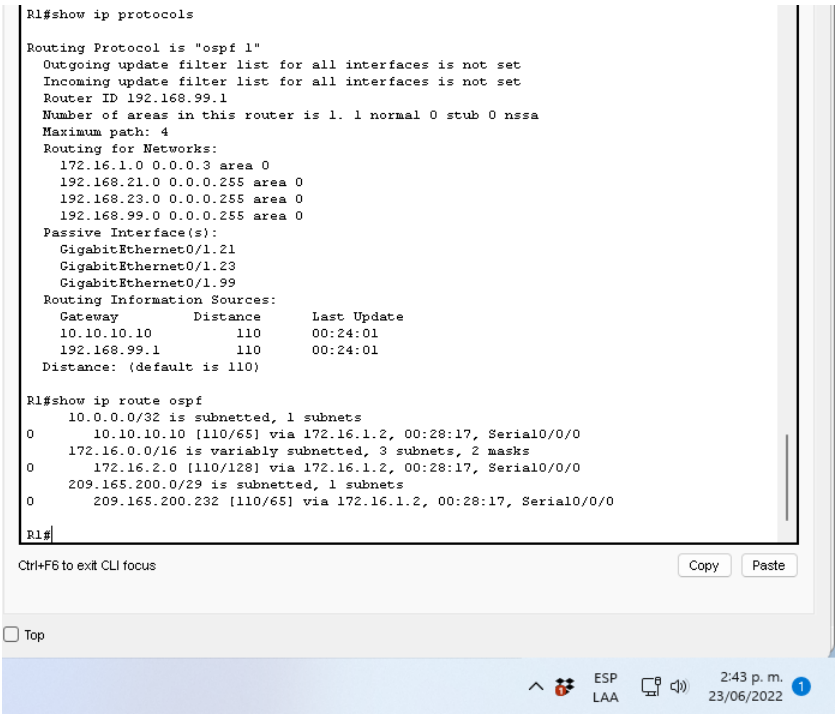
Fuente: Prueba de habilidades CCNA 2022

Figura 18 Ejecución de comando show ip protocols en R1



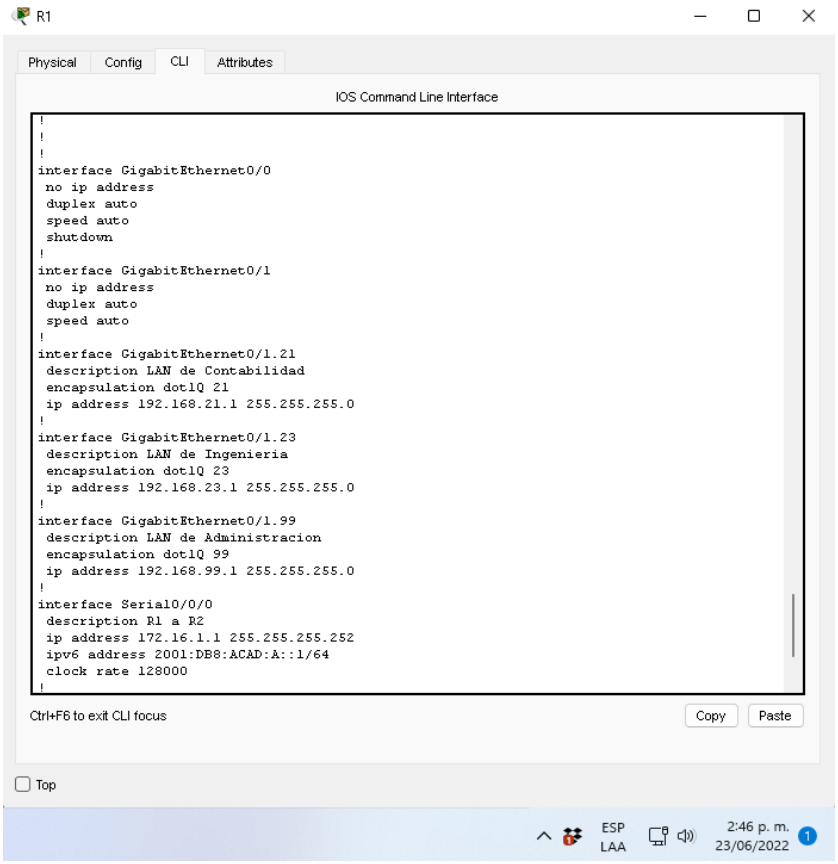
Fuente: Propia

Figura 19 Ejecución de comando show ip route ospf en R1



Fuente: Propia

Figura 20 Ejecución de comando show run en R1



Fuente: Propia

2.5 Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22 Configuración para R1 como servidor DCHP para VLAN 21 y 23

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP enla VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.21
Reservar las primeras 20 direcciones IP enla VLAN 23 para	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.21

configuraciones estáticas	
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT R1(config)#ip dhcp pool ACCT R1(dhcp-config)# Servidor DNS: 10.10.10.10 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 Nombre de dominio: ccna-sa.com R1(dhcp-config)#domain-name ccna-sa.com Establecer el gateway predeterminado R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR R1(config)#ip dhcp pool ENGRN Servidor DNS: 10.10.10.10 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 Nombre de dominio: ccna-sa.com R1(dhcp-config)#domain-name ccna-sa.com Establecer el gateway predeterminado R1(dhcp-config)#default-router 192.168.23.1

Fuente: Prueba de habilidades CCNA 2022

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23 Configuración NAT en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15

	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server (solo funciona en equipos reales)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local (solo funciona en equipos reales)
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 g0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/0/1 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 2(config)#access-list 1 permit 192.168.23.0 .0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 R2(config)#
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#

Fuente: Prueba de habilidades CCNA 2022

2.5.3 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 pingsse realicen correctamente.

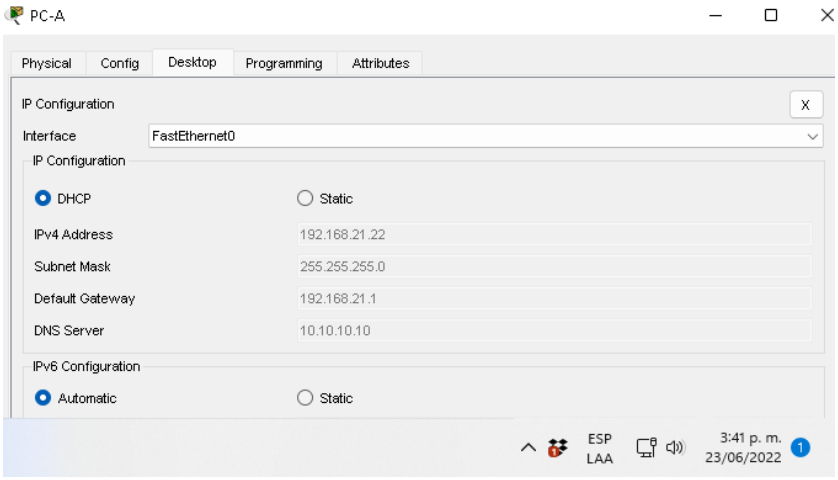
Tabla 24 Configuración DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ipv4 Address: 192.168.21.22 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.21.1 DNS Server: 10.10.10.10
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ipv4 Address: 192.168.23.22 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.23.1 DNS Server: 10.10.10.10
Verificar que la PC-A pueda hacer ping ala PC-C Nota: Quizá sea necesario deshabilitar elfirewall de la PC.	C:\>ping 192.168.23.22 Pinging 192.168.23.22 with 32 bytes of data: Request timed out. Reply from 192.168.23.22: bytes=32 time=1ms TTL=127 Reply from 192.168.23.22: bytes=32 time<1ms TTL=127 Reply from 192.168.23.22: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.23.22: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\>
Utilizar un navegador web en la computadora de Internet para acceder alservidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	Cisco Packet Tracer Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open. Quick Links: A small page Copyrights

	Image page Image

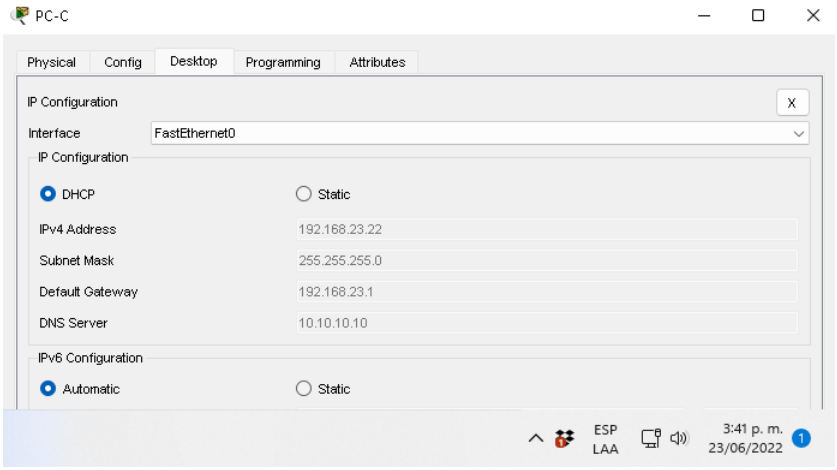
Fuente: Prueba de habilidades CCNA 2022

Figura 21 PC-A adquiere información de IP del servidor de DHCP



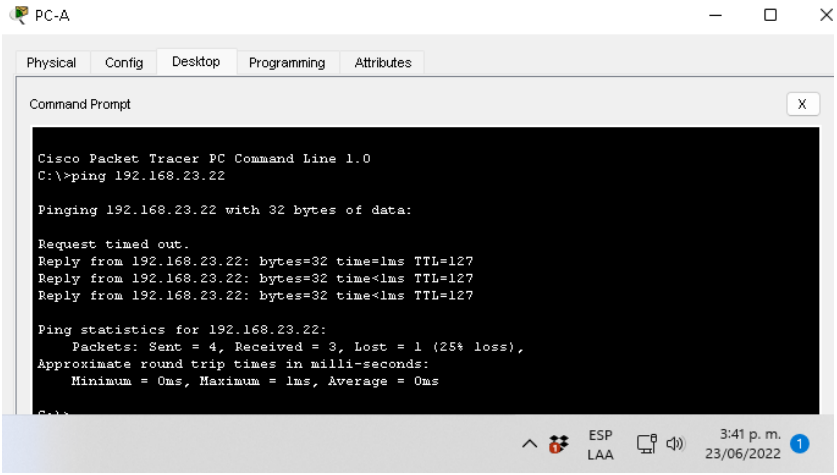
Fuente: Propia

Figura 22 PC-C haya adquiere información de IP del servidor de DHCP



Fuente: Propia

Figura 23 PC-A ping a la PC-C



Fuente: Propia

Figura 24 En la computadora de Internet accediendo al servidor web

Fuente: Propia

2.6 Parte 6: Configurar NTP

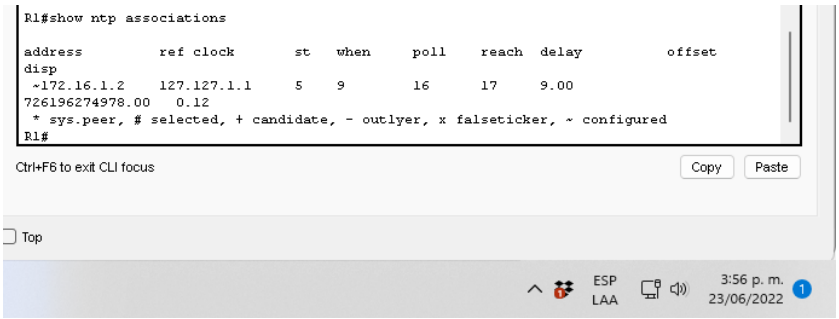
Tabla 25 Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m. R2#clock set 09:00:00 5 march 2016
Configure R2 como un maestro NTP.	Nivel de estrato: 5

	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2 R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con horaNTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 127.127.1.1 5 9 16 17 9.00 726196274978.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured R1#

Fuente: Prueba de habilidades CCNA 2022

Figura 25 Verificación del comando show ntp associations en R1



Fuente: Propia

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

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

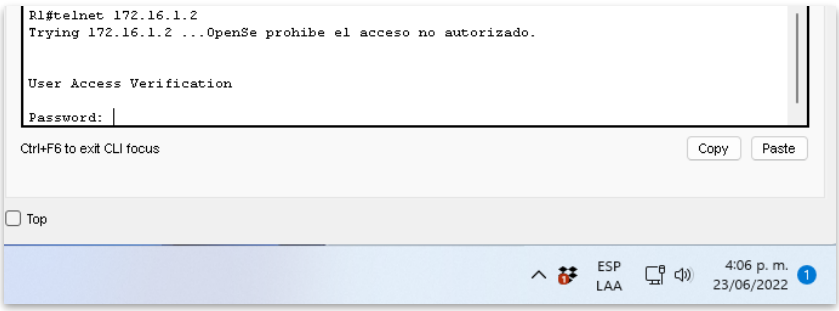
Tabla 26 Restricciones al acceso de las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1

Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado. User Access Verification Password:

Fuente: Prueba de habilidades CCNA 2022

Figura 26 Verificación acceso a Telnet 172.16.1.2



Fuente: Propia

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

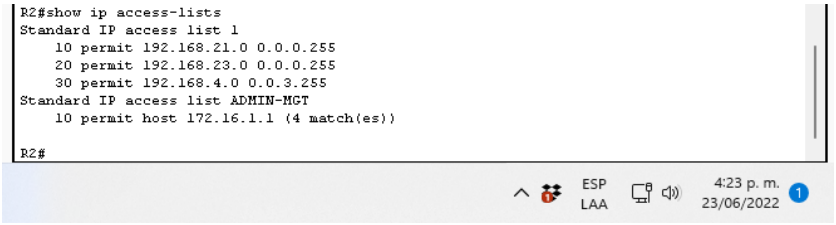
Tabla 27 Comandos CLI adecuados

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas poruna lista de acceso desde la última vez que se restableció	R2#show access-list R2#show ip access-list
Restablecer los contadores de una listade acceso	R2#clear ip access-list counters

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la direcciónen que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminarlas traducciones de NAT dinámicas?	R2#clear ip nat translation

Fuente: Prueba de habilidades CCNA 2022

Figura 27 Verificación comando show access-list

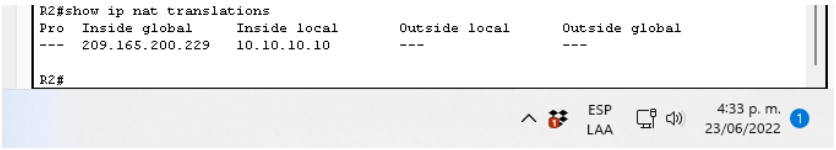


Fuente: Propia

Figura 28 Verificación comando show ip interface

Fuente: Propia

Figura 29 Verificación del comando show ip nat translations



Fuente: Propia

CONCLUSIONES

Este conjunto de simulaciones y configuraciones virtuales, permiten desarrollar las habilidades necesarias para la puesta en marcha y activación real de equipos en el ámbito profesional del ingeniero de Sistemas y proporcionan una experiencia de aprendizaje significativo para afrontar los retos en campo.

La herramienta del Packet Tracer hace muy didáctico y claro el funcionamiento de los equipos de red y permite realizar la configuración de las diferentes topologías; no solo las de este informe, donde se realizó de forma estructurada la conexión de dos redes LAN pequeñas a través de un dispositivo de Ruteo en el primer escenario. Allí se identificó en detalle el tamaño de las subredes y se realizaron pruebas de tráfico entre los diferentes dispositivos.

El segundo escenario es mucho más complejo y focaliza la atención no solo en la configuración de capa 2 y 3 del modelo OSI con enrutamiento dinámico OSPF, sino que además se dota a la red para conectividad sobre IPV4 e IPV6 respectivamente. Adicionalmente se configuran la seguridad de la red y el DHCP para cada subred.

Las configuraciones de seguridad, NAT y listas de acceso constituyeron un reto muy enriquecedor y permitieron poner a pruebas las habilidades desarrolladas a lo largo del diplomado.

BIBLIOGRÁFIA

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter8_Direccionamiento%20IP.pdf

CISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter9_Divisi%c3%b3n%20de%20redes%20IP%20en%20subredes.pdf

CISCO. (2019). Ethernet. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter5_Ethernet.pdf

CISCO. (2019). Capa de red. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter6_Capa%20de%20red.pdf