SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGÍAS CISCO

ANGEL ANDRES MORALES WATTS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
SAHAGUN
2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGÍAS CISCO

ANGEL ANDRES MORALES WATTS

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

DIRECTOR:
MSc. NANCY AMPARO GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
SAHAGUN
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

SAHAGUN, 30 de noviembre de 2021

AGRADECIMIENTOS

Quiero aprovechar este espacio para agradecer a cada una de las personas que han hecho realidad este sueño de ser Ingeniero.

En primer lugar, quiero darle gracias a Dios quien me permite dar este gran paso en la vida y también agradecer a mis padres que día a día han logrado motivarme para ser mejor cada día y me enseñaron esforzarme en cada cosa que hago. Quiero dar gracias a mi hermana que un día me hablo sobre la educación virtual en la UNAD y se esmeró en conseguir todo lo necesario para que entrara y terminara mi carrera como profesional.

Quiero agradecer a aquellas personas que sin esperar ninguna recompensa me ayudaron a entender temas complicado donde a veces sentía que no podía más para esas personas mis más sinceras gracias.

Gracias a todos esos tutores que me apoyaron y que aun en horarios fuera de su jornada de atención sacaban el espacio para darme un accesoria, ellos fueron aquellos que sin darse cuenta formaban una escalera que me llevaría a la victoria

CONTENIDO

Contenido

AGRADECIMIENTOS 4

CONTENIDO 5

LISTA DE TABLAS 8

LISTA DE FIGURAS 9

GLOSARIO 10

RESUMEN 11

INTRODUCCIÓN 12

Escenario 1 13

Parte 1: Construya la Red 13

Figura 1. Simulación de escenario 1 13

Parte 2: Desarrolle el esquema de direccionamiento IP 13

Tabla 1. Direccionamiento 13

Tabla 2. Enrutamiento 14

Parte 3: Configure aspectos básicos 14

Paso 1: configurar los ajustes básicos 14

Tabla 3. Configuración R1 14

Tabla 4. Configuración S1 16

Paso 2. Configurar los equipos 18

Tabla 5. PC-A Network Configuration 18

Tabla 6. PC-B Network Configuration 19

Figura 2. Configuración PC-A 19

Escenario 2 20

Topología 20

Parte 1: Inicializar dispositivos 21

Paso 1: Inicializar y volver a cargar los routers y los switches 21
Tabla 7. Inicialización de routers y switches 21
Parte 2: Configurar los parámetros básicos de los dispositivos 21
Paso 1: Configurar la computadora de Internet 21
Tabla 8. Configurar la computadora de Internet 21
Paso 2: Configurar R1 22
Tabla 9. Configuración R1 22
Paso 3: Configurar R2 24
Tabla 10. Configuración R2 24
Paso 4: Configurar R3 27
Tabla 11. Configuración R3 27
Paso 5: Configurar S1 29
Tabla 12. Configuración S1 29
Paso 6: Configurar el S3 30
Tabla 13. Configuración S3 30
Paso 7: Verificar la conectividad de la red 31
Tabla 14. Verificar la conectividad 31
Figura 4. Prueba de ping desde el Router 1 a el Router 2 32
Figura 5. Prueba de ping desde el Router 2 a el Router 3 32
Figura 6. Prueba de ping desde el PC de Internet a el Gateway 33
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 33
Paso 1: Configurar S1 33
Tabla 15. Configurar S1 33
Tabla 16. Configurar S3 35
Paso 3: Configurar R1 37
Tabla 17. Configurar R1 37
Tabla 18. Verificar la conectividad 38
Figura 7. Prueba de Ping desde S1 a la vlan 99 38
Figura 8. Prueba de Ping desde S3 a la vlan 99 39
Figura 9. Prueba de Ping desde S3 a la vlan 23 39
Parte 4: Configurar el protocolo de routing dinámico OSPF 40
Paso 1: Configurar OSPF en el R1 40
Tabla 19. Configurar OSPF en el R1 40
Paso 2: Configurar OSPF en el R2 41

Tabla 20. Configurar OSPF en el R2 41
Paso 3: Configurar OSPFv3 en el R2....42
Tabla 21. Configurar OSPFv3 en el R2....42
Paso 4: Verificar la información de OSPF 43
Tabla 21. Configurar OSPFv3 en el R2....43
Figura 10. Comando show ip protocols....43
Figura 11. show running-config | section ospf 44
Parte 5: Implementar DHCP y NAT para IPv4 44
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23....44
Tabla 22. Implementar DHCP y NAT para IPv4....44
Paso 2: Configurar la NAT estática y dinámica en el R2 46
Tabla 23. Configurar la NAT estática y dinámica en el R2....46
Paso 3: Verificar el protocolo DHCP y la NAT estática....48
Tabla 24. Verificar el protocolo DHCP y la NAT estática 48
Parte 6: Configurar NTP 49
Tabla 25. Configurar NTP....49
Figura 12. show ntp status....50
Parte 7: Configurar y verificar las listas de control de acceso (ACL)....51
Paso 1: Restringir el acceso a las líneas VTY en el R2 Configurar NTP....51
Tabla 26. Restringir el acceso a las líneas VTY en el R2 Configurar NTP....51
Figura 13. acceso por Telnet a las líneas de VTY....52
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente....54
Tabla 27. comando de CLI....54
CONCLUSIONES 56
BIBLIOGRÁFIA 57

LISTA DE TABLAS

Tabla 1. Direccionamiento 13
Tabla 2. Enrutamiento 14
Tabla 3. Configuración R1 14
Tabla 4. Configuración S1 16
Tabla 5. PC-A Network Configuration 18
Tabla 6. PC-B Network Configuration 19
Tabla 7. Inicialización de routers y switches 21
Tabla 8. Configurar la computadora de Internet 21
Tabla 9. Configuración R1 22
Tabla 10. Configuración R2 24
Tabla 11. Configuración R3 27
Tabla 12. Configuración S1 29
Tabla 13. Configuración S3 30
Tabla 14. Verificar la conectividad 31
Tabla 15. Configurar S1 33
Tabla 16. Configurar S3 35
Tabla 17. Configurar R1 37
Tabla 18. Verificar la conectividad 38
Tabla 19. Configurar OSPF en el R1 40
Tabla 20. Configurar OSPF en el R2 41
Tabla 21. Configurar OSPFv3 en el R2 42
Tabla 21. Configurar OSPFv3 en el R2 43
Tabla 22. Implementar DHCP y NAT para IPv4 44
Tabla 23. Configurar la NAT estática y dinámica en el R2 46
Tabla 24. Verificar el protocolo DHCP y la NAT estática 48
Tabla 25. Configurar NTP 49
Tabla 26. Restringir el acceso a las líneas VTY en el R2 Configurar NTP 51
Tabla 27. comando de CLI 54

LISTA DE FIGURAS

Figura 1. Simulación de escenario 1 13
Figura 2. Configuración PC-A 19
Figura 4. Prueba de ping desde el Router 1 a el Router 2 32
Figura 5. Prueba de ping desde el Router 2 a el Router 3 32
Figura 6. Prueba de ping desde el PC de Internet a el Gateway 33
Figura 7. Prueba de Ping desde S1 a la vlan 99 38
Figura 8. Prueba de Ping desde S3 a la vlan 99 39
Figura 9. Prueba de Ping desde S3 a la vlan 23 39
Figura 10. Comando show ip protocols 43
Figura 11. show running-config | section ospf 44
Figura 12. show ntp status 50
Figura 13. acceso por Telnet a las líneas de VTY 52

GLOSARIO

Enrutamiento: El enrutamiento o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. ... El enrutado en sentido estricto se refiere al enrutado IP y se opone al bridging.

SUBNETTING: De acuerdo con la definición simple de subnetting, esta es la división de una red dentro de varias subredes. Por ejemplo, el subnetting les permite a las redes administrativas dividir su propia red empresarial en subredes sin darle a conocer esto a la internet

Mascara de red: Una máscara de red consiste en una máscara de 32 bits que se utiliza para dividir una dirección IP en subredes y especificar los hosts disponibles de la red. Con esta máscara de red, siempre se asignan automáticamente dos bits.[1] Este término también se utiliza para definir la clase y el rango de (Desconocido, s.f.) las direcciones de protocolo de Internet.

Topología: La topología de red se define como un mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como «conjunto de nodos interconectados». Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente depende del tipo de red en cuestión.

DNS: El DNS, o sistema de nombres de dominio, traduce los nombres de dominios aptos para lectura humana (por ejemplo, www.amazon.com) a direcciones IP aptas para lectura por parte de máquinas (por ejemplo, 192.0.2.44).

OSPF: es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP).
IPv6: obedece a la sexta y más reciente versión del Protocolo de Internet, pretende reemplazar la escasez de direcciones que tiene el actual IPv4 (cuarta versión)

IPv4: es un número de 32 bits que identifica de forma exclusiva una interfaz de red en un sistema, tal como se explica en Aplicación de las direcciones IP a las interfaces de red.

NAT: Podemos decir que son las siglas de Network Address Translator, o en español traductor de direcciones de red. Su función es precisamente esa, traducir las direcciones para que sean posibles las conexiones.

RESUMEN

El siguiente trabajo muestra las habilidades adquiridas durante el diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN) en el cual se desarrollaron dos escenarios en donde se aplicaron servicios como DHCP y protocolos de enrutamiento.

En el primer escenario se realizó el Subneteo de las redes en donde se aplicaron los conocimientos sobre mascaras variables, permitiendo así tener una segmentación de red de acuerdo con los parámetros solicitados y así proceder con la configuración de los dispositivos.

Para el escenario numero dos se realizó la configuración de los equipos de red bajo la consola de comando de CISCO, en donde se empleó el protocolo IPv6 y el protocolo IPv4. Además, de esto se realizó el enrutamiento mediante el protocolo OSPF permitiendo una conmutación más ágil debido a que este protocolo permite escoger la ruta más rápida de acuerdo con los recursos para enviar los datos

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes.

ABSTRACT

The following work shows the skills acquired during the Cisco in-depth diploma (design and implementation of integrated LAN / WAN solutions) in which two scenarios were developed where services such as DHCP and routing protocols were applied.

In the first scenario, the Subnetting of the networks was carried out where the knowledge about variable masks was applied, thus allowing to have a network segmentation according to the requested parameters and thus proceed with the configuration of the devices.

For scenario number two, the configuration of the network equipment was carried out under the CISCO command console, where the IPv6 protocol and the IPv4 protocol were used. In addition, the routing was carried out using the OSPF protocol, allowing a more agile switching because this protocol allows choosing the fastest route according to the resources to send the data.

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

INTRODUCCIÓN

En el siguiente trabajo se desarrollará en un entorno simulado la red de dos escenarios donde se pondrán en práctica lo aprendido durante el diplomado de cisco CCNA, abarcando temáticas como el Subneteo, los protocolos OSPF, NAT, IPV4, IPV6 y seguridad en dispositivos.

Para el primer escenario se realizará una segmentación de la red de acuerdo con los lineamientos establecidos, esto utilizando una dirección IPv4 con máscara 24 la cual fue dividida según los hosts que solicitaron. Obteniendo de esta manera una red con máscara variable y se aplicaran los protocolos de seguridad mediante la encriptación que ofrece CISCO

Para el segundo escenario se realiza la simulación de una red con protocolo de internet versión 6 y el protocolo de internet versión 4 donde se implementará protocolos de seguridad tanto de acceso como de envío de paquetes. estas configuraciones se realizarán tanto en los router como en los switches.

También se realizará la configuración del protocolo de enrutamiento OSFP que nos permitirá tener una comunicación más fluida de acuerdo con los recursos que tengan los dispositivos identificando las redes que estén directamente conectadas a el router.

Se habilitará el servicio DHCP en el router R1 quien tendrá una subinterfaz las cuales tendrán asignadas las VLAN que se crearon en cada uno de los switches con el fin de tener un control de las redes según los cargos que ocupen los usuarios conectados a esta.

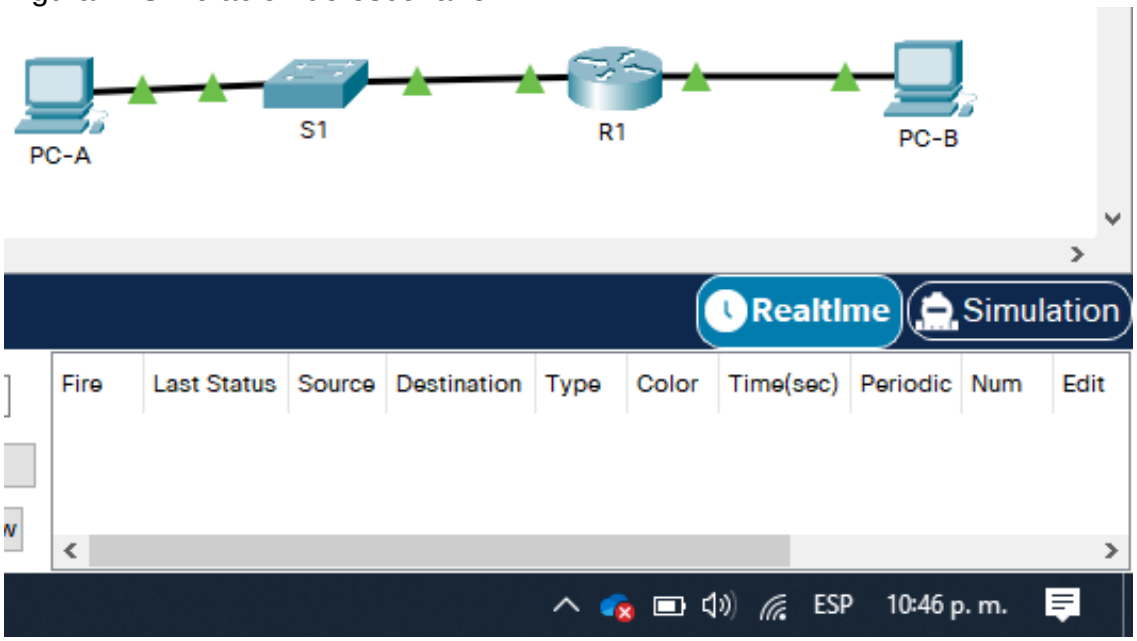
De igual forma, con el fin de proteger los datos de la organización se implementa una NAT (Network Address Translation) que permite traducir la red LAN privada a una red global,evitando que personas ajenas tengan conocimiento sobre nuestra infraestructura para evitar posibles ataques.

Escenario 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, cableeconforme se indica en la topología, y conecte los equipos de cómputo.

Figura 1. Simulación de escenario 1



Fuente Propia

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 tablade direccionamiento.

Cada estudiante tomará el direccionamiento 192.168.51.0 donde X corresponde a los últimos dos dígitos desu cédula.

Tabla 1. Direccionamiento

Ítem	Requerimiento
Dirección de Red	192.168.51.0

Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.51.129/26
R1 G0/0/0	192.168.51.1/25
S1 SVI	192.168.51.2/25
PC-A	192.168.51.126/25
PC-B	192.168.51.190/26

Fuente Propia

Tabla 2. Enrutamiento

Dispositivo	Puerto	Dirección ip	Mascara	Puerta de enlace
R1	G0/0/1	192.168.51.129/26	255.255.255.192	
	R1 G0/0/0	192.168.51.1/25	255.255.255.128	
S1 SVI	VLAN 1	192.168.51.2/25	255.255.255.128	192.168.51.1/25
PC-A		192.168.51.126/25	255.255.255.128	192.168.51.1/25
PC-B		192.168.51.190/26	255.255.255.192	192.168.51.129/26

Fuente Propia

Parte 3: Configure aspectos básicos

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

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC	ciscoenpass

privilegiado	
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para lascontraseñas	10 caracteres
Crear un usuario administrativo en la base dedatos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTYpara que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente Propia

Código para R1

Router>enable →Inicio al modo privilegiado
Router#configure terminal→Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1→ Asigno el nombre R1 al Router
R1(config)#no ip domain-lookup→Desactivo la búsqueda DNS
R1(config)#ip domain-name ccna-lab.com→Asigno el nombre de dominio
R1(config)#enable password ciscoenpass →Asigno contraseña modo privilegiado
R1(config)#line console 0→Ingreso a la línea consola
R1(config-line)#password ciscoconpass→Asigno contraseña al acceso a consola
R1(config-line)#login→Habilito la contraseña

R1(config-line)#exit→Salida de la línea de consola
R1(config)#username admin privilege 15 secret admin1pass→Crear un usuario administrativo en la base de datos local
R1(config)#line vty 0 15→Configure inicio de sesión en líneas VTY
R1(config-line)#login local→Configurar el inicio de sesión en las líneas VTY para que use la base de datos local
R1(config-line)#transport input ssh →Configuráramos VTY solo aceptando SSH
R1(config-line)#exit
R1(config)#service password-encryption→Cifrar las contraseñas de texto no cifrado
R1(config)#banner motd $Alerta!!! Prohibido el Acceso a Personal no Autorizado$→Configure un MOTD Banner
R1(config)#interface g0/0/0 →Ingresamos a la interfaz g0/0/0
R1(config-if)#ip address 192.168.51.1 255.255.255.128--- asignamos la dirección IP a la interfaz
R1(config-if)#no shutdown→encendemos la interfaz
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
R1(config-if)#interface g0/0/1→Ingresamos a la interfaz g0/0/1
R1(config-if)#ip address 192.168.51.129 255.255.255.128→asignamos la dirección IP a la interfaz
R1(config-if)#no shutdown→encendemos la interfaz
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
R1(config)#crypto key generate rsa general-keys modulus 1024→ Módulo de 1024 bits
The name for the keys will be: R1.ccna-lab.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:19:27.539: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1#copy running-config startup-config → Guardamos la configuración
Destination filename [startup-config]?
Building configuration...
[OK]

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 4. Configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	S1

Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para queuse la base de datos local	
Configurar las líneas VTY para que acepten únicamentelas conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.

Fuente Propia

Código para S1
Switch>enable→ Inicio al modo privilegiado
Switch #configure terminal → Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config)#hostname S1→ Asigno el nombre R1 al Router
S1(config)#no ip domain-lookup→ Desactivo la búsqueda DNS
S1(config)#ip domain-name ccna-lab.com→ Asigno el nombre de dominio
S1(config)#enable password ciscoenpass→ Asigno contraseña modo privilegiado
S1(config)#line console 0→ Ingreso a la línea consola
S1(config-line)#password ciscoconpass→ Asigno contraseña al acceso a consola
S1(config-line)#login→ Habilito la contraseña
S1(config-line)#exit→ Salida de la línea de consola
S1(config)#username admin privilege 15 secret admin1pass→ Crear un usuario administrativo en la base de datos local
S1(config)#line vty 0 15→ Ingresamos a la interfaz VTY
S1(config-line)#login local→ Habilito la contraseña local
S1(config-line)#transport input ssh→ Configuráramos VTY solo aceptando SSH
S1(config-line)#exit→ Salida de la línea VTY

S1(config)#service password-encryption→ Cifrar las contraseñas de texto no cifrado
S1(config)#banner motd $Alerta!!! Prohibido el Acceso a Personal no Autorizado$→ Configure un MOTD Banner
S1(config-if)#interface vlan 1→ Ingresamos a la Interface VLAN 1
S1(config-if)#ip address 192.168.51.2 255.255.255.128→Asignamos una IP
S1(config)# ip default-gateway 192.168.1.1→asignamos la puerta de enlace
S1(config)#crypto key generate rsa general-keys modulus 1024→ Módulo de 1024 bits
The name for the keys will be: S1.ccna-lab.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:19:27.539: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1#copy running-config startup-config → Guardamos la configuración
Destination filename [startup-config]?
Building configuration...
[OK]

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. PC-A Network Configuration

PC-A Network Configuration	
Descripción	PC-A
Dirección física	0001.9638.570B
Dirección IP	192.168.51.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.51.1

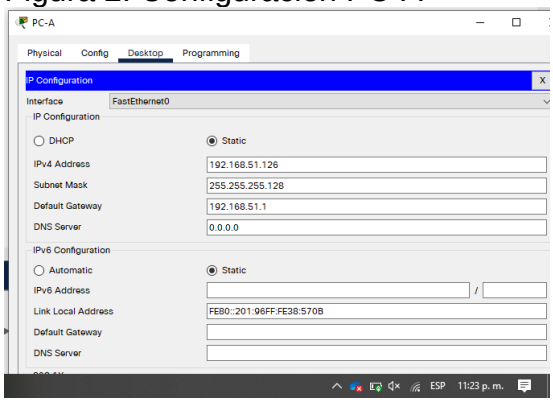
Fuente Propia

Tabla 6. PC-B Network Configuration

PC-B Network Configuration	
Descripción	PC-B
Dirección física	0007.EC79.D115
Dirección IP	192.168.51.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.51.129

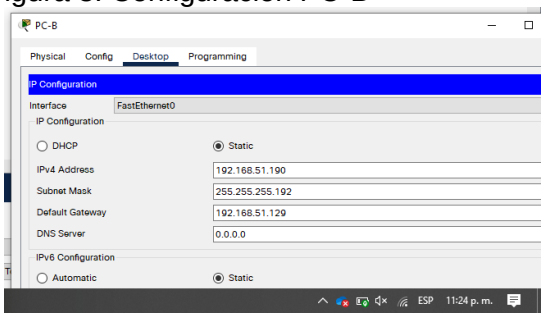
Fuente Propia

Figura 2. Configuración PC-A



Fuente propia

igura 3. Configuración PC-B

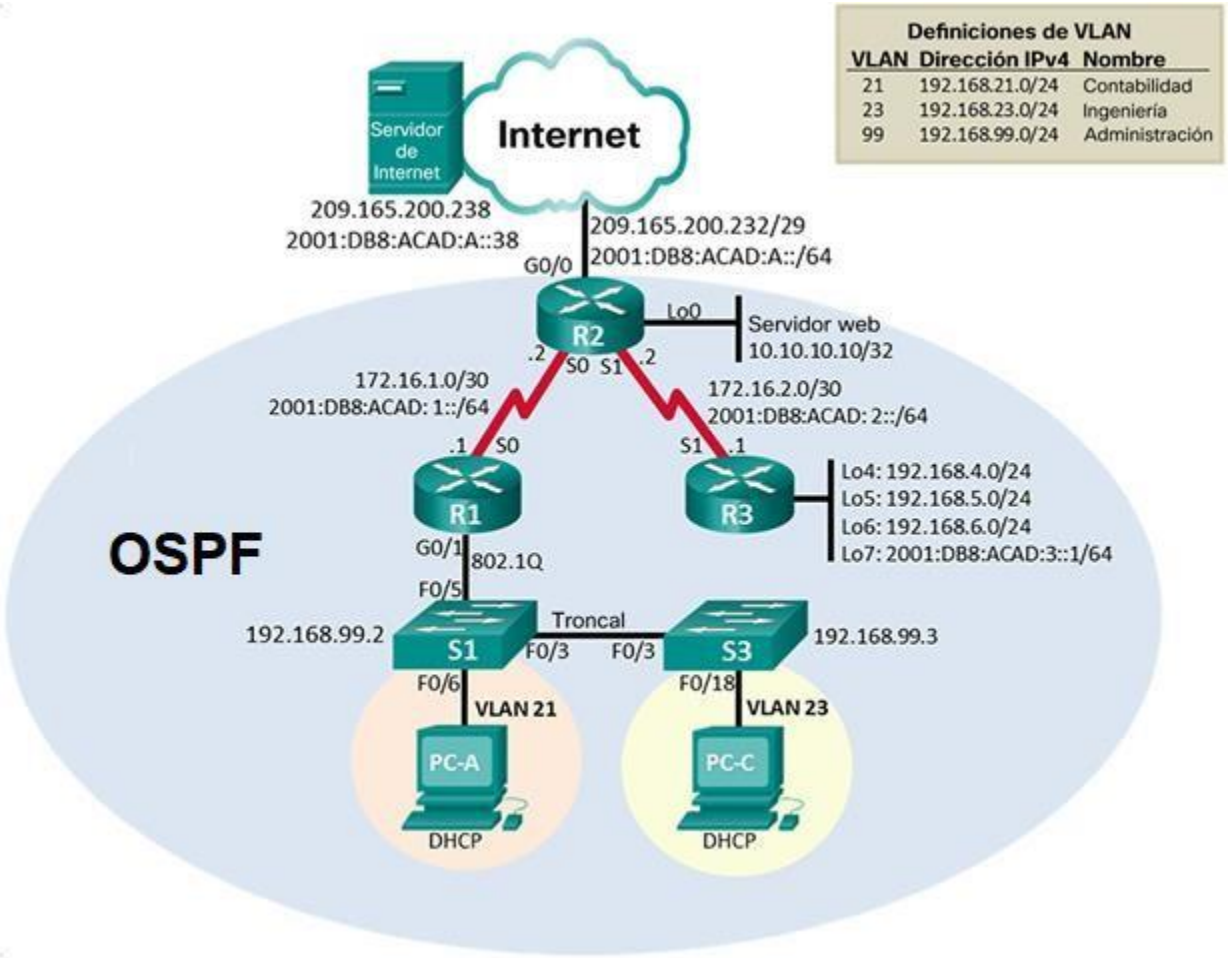


Fuente Propia

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.

Topología



Fuente Propia

Parte 1: Inicializar dispositivos

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

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

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

Tabla 7. Inicialización de routers y switches

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

Fuente Propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Tabla 8. Configurar la computadora 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:2::1

Fuente Propia

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(config)#no ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco
Cifrar las contraseñas de texto no cifrado	R|(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Fuente Propia

Linea de Comando

Router>enable→ Inicio al modo privilegiado
Router#configure terminal→ Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup→Desactivo la búsqueda DNS
Router(config)#hostname R1→ Asigno el nombre R1 al Router
R1(config)#enable secret class→ Asigno contraseña modo privilegiado
R1(config)#line console 0→ Ingreso a la línea consola
R1(config-line)#password cisco→ Asigno contraseña al acceso
R1(config-line)#login→ Habilito la contraseña
R1(config-line)#line vty 0 15→ Ingreso a la línea VTY
R1(config-line)#password cisco→ Asigno contraseña al acceso
R1(config-line)#login→ Habilito la contraseña
R1(config-line)#service password-encryption→ Cifrar las contraseñas de texto no cifrado
R1(config)#banner motd $Se prohíbe el acceso no autorizado.$ → Configure un MOTD Banner
R1(config)#ipv6 unicast-routing →Habilitamos la configuración IPv6 en el router
R1(config)#interface s0/0/0→ Ingresamos a la interfaz s0/0/0
R1(config-if)#description conexcion R1 A R2→ Agregamos una descripción
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64→ asignamos la dirección IPv6
R1(config-if)#ip address 172.16.1.1 255.255.255.252→ asignamos la dirección IPv4
R1(config-if)#no shutdown →Encendemos la interface
R1(config-if)#clock rate 128000→Establecemos la frecuencia de reloj en 128000
R1(config-if)#exit→Salimos de la Interface
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2→ Configuramos una ruta IPv4 predeterminada
R1(config)#ipv6 route ::/0 2001:db8:acad:1::2→ Configuramos una ruta IPv6 predeterminada
R1(config)#exit→salimos de la configuración
R1#copy running-config startup-config→ Guardamos las Configuraciones
Destination filename [startup-config]?
Building configuration...
[OK]

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(config)#no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Fuente propia

Línea de Comando

Router>enable→ Inicio al modo privilegiado
Router#configure terminal→ Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup→ Desactivo la búsqueda DNS
Router(config)#hostname R2→ Asigno el nombre R2 al Router R2(config)#enable secret class→ Asigno contraseña modo privilegiado
R2(config)#line console 0→ Ingreso a la línea consola
R2(config-line)#password cisco→ Asigno contraseña al acceso
R2(config-line)#login→ Habilito la contraseña
R2(config-line)#line vty 0 15→ Ingreso a la línea VTY
R2(config-line)#password cisco→ Asigno contraseña al acceso
R2(config-line)#login→ Habilito la contraseña
R2(config-line)#exit
R2(config)#service password-encryption→ Cifrar las contraseñas de texto no cifrado
R2(config)#banner motd $Se prohbe el acceso no autorizado.$ → Configure un MOTD Banner
R2(config)#ipv6 unicast-routing→ Habilitamos la configuración IPv6 en el router
R2(config)#interface s0/0/0→ Ingresamos a la interfaz s0/0/0
R2(config-if)#description conexion R2 A R1→ Agregamos una descripción
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64→ asignamos la dirección IPv6
R2(config-if)#ip address 172.16.1.2 255.255.255.252→ asignamos la dirección IPv4
R2(config-if)#no shutdown→ Encendemos la interface
R2(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2(config-if)#interface s0/0/1→ Ingresamos a la interfaz s0/0/1
R2(config-if)#description conexion R2 A R3→ Agregamos una descripción
R2(config-if)#ip address 172.16.2.2 255.255.255.252→ asignamos la dirección IPv4
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64→ asignamos la dirección IPv6
R2(config-if)#clock rate 128000→ Establecemos la frecuencia de reloj en 128000
R2(config-if)#interface g0/0→ Ingresamos a la g0/0
R2(config-if)#description conexion R2 A Internet→ Agregamos una descripción
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64→ asignamos la dirección IPv6
R2(config-if)#ip address 209.165.200.233 255.255.255.248→ asignamos la dirección IPv4
R2(config-if)#no shutdown→ Encendemos la interface
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#interface loopback 0 → Ingresamos a la loopback 0
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#description servidor web simulado→ Agregamos una descripción
R2(config-if)#ip address 10.10.10.10 255.255.255.255→ asignamos la dirección IPv4
R2(config-if)#exit→
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.238→ Configuramos una ruta IPv4 predeterminada
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:A::38→ Configuramos una ruta IPv6 predeterminada
R2(config)#exit→
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#copy running-config startup-config →
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Conexión

Tabla 11. Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

Fuente propia

Línea de Comando
Router>enable→ Inicio al modo privilegiado
Router#configure terminal Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup →Desactivo la búsqueda DNS
Router(config)#hostname R1→ Asigno el nombre R1 al Router
R1(config)#enable secret class→ Asigno contraseña modo privilegiado
R1(config)#line console 0→ Ingreso a la línea consola
R1(config-line)#password cisco→ Asigno contraseña al acceso
R1(config-line)#login→ Habilito la contraseña
R1(config-line)#line vty 0 15→ Ingreso a la línea VTY
R1(config-line)#password cisco→ Asigno contraseña al acceso
R1(config-line)#login→ Habilito la contraseña
R1(config-line)#exit
R1(config)#hostname R3
R3(config)#service password-encryption→ Cifrar las contraseñas de texto no
R3(config)#banner motd $Se prohbe el acceso no autorizado.$ → Configure un MOTD Banner
R3(config)#ipv6 unicast-routing Habilitamos la configuración IPv6 en el router
R3(config)#interface s0/0/0→ Ingresamos a la interfaz s0/0/0
R3(config-if)#interface s0/0/1
R3(config-if)#description conexion R3 A R2→ Agregamos una descripción
R3(config-if)#ipv6 address 2001:db8:acad:2::1/64→ asignamos la dirección IPv6
R3(config-if)#ip address 172.16.2.1 255.255.255.252 → asignamos la dirección IPv4

R3(config-if)#no shutdown →Encendemos la interface
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R3(config-if)#interface lo4 →Ingresamos a la interfaz lo4
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→ asignamos la dirección IPv4
R3(config-if)#interface lo5→Ingresamos a la interfaz lo5
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)#interface lo6→Ingresamos a la interfaz lo6

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)#interface lo7→Ingresamos a la interfaz lo7

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:2:31/64^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
^Z
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface lo7→Ingresamos a la interfaz lo7
R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 → Configuramos una ruta IPv4 predeterminada
R3(config)#ipv6 route ::/0 2001:db8:acad:2::2 Configuramos una ruta IPv6 predeterminada
R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.1 → Configuramos una ruta IPv4 predeterminada

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(config)#no ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente propia

Línea de Comando
Switch>ENABLE
Switch#configure terminal→ Inicio al modo privilegiado
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#no ip domain-lookup → Ingreso a modo de configuración
Switch(config)#hostname S2 → Asigno el nombre S2
S2(config)#enable secret class→ Asigno contraseña modo privilegiado
S2(config)#line console 0 → Ingreso a la línea consola
S2(config-line)#password cisco→ Asigno contraseña al acceso
S2(config-line)#login→ Habilito la contraseña
S2(config-line)#line vty 0 15→ Ingreso a la línea VTY
S2(config-line)#password cisco→ Asigno contraseña al acceso
S2(config-line)#login→ Habilito la contraseña
S2(config-line)#EXIT
S2(config)#service password-encryption→ Cifrar las contraseñas de texto no cifrado
S2(config)#banner motd $Se prohbe el acceso no autorizado.$ → Configure un MOTD Banner
S2(config)#EXIT
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#copy running-config startup-config→ Guardamos las Configuraciones
Destination filename [startup-config]?
Building configuration...
[OK]

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(config)#no ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente propia

Línea de Comando

Switch>enable→ Inicio al modo privilegiado
Switch#configure terminal→ Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup→Desactivo la búsqueda DNS
Switch(config)#hostname S3→ Asigno el nombre S3
S3(config)#enable secret class→ Asigno contraseña modo privilegiado
S3(config)#line console 0→ Ingreso a la línea consola
S3(config-line)#password cisco→ Asigno contraseña al acceso
S3(config-line)#login→ Habilito la contraseña
S3(config-line)#line vty 0 15→ Ingreso a la línea VTY
S3(config-line)#password cisco→ Asigno contraseña al acceso
S3(config-line)#login→ Habilito la contraseña
S3(config-line)#exit
S3(config)#service password-encryption→ Cifrar las contraseñas de texto no cifrado
S3(config)#banner motd $Se prohbe el acceso no autorizado.$ → Configure un MOTD Banner
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#copy running-config startup-config→ Guardamos las Configuraciones
Destination filename [startup-config]?
Building configuration...
[OK]
S3#

Paso 7: Verificar la conectividad de la red

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

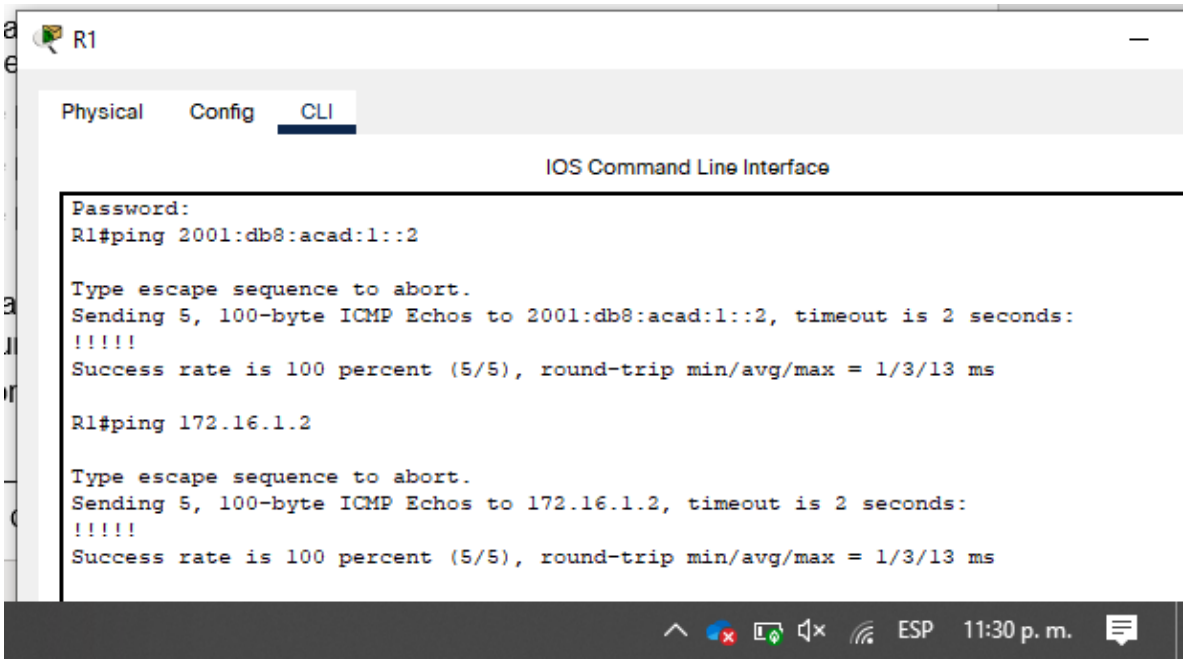
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 14. Verificar la conectividad

Des de	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	2001:db8:acad:1::2 y 172.16.1.2	Exitoso 5 enviado y 5 recibido
R2	R3, S0/0/1	2001:db8:acad:2::1 y 172.16.2.1	Exitoso 5 enviado y 5 recibido
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso 4 enviado y 4 recibido

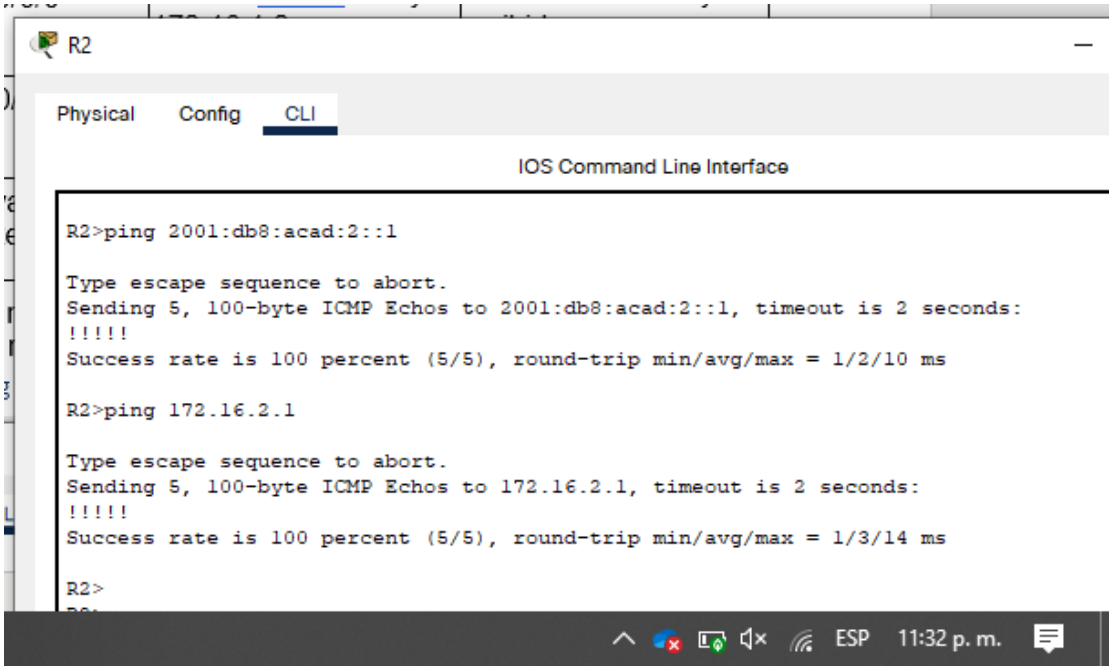
Fuente propia

Figura 4. Prueba de ping desde el Router 1 a el Router 2



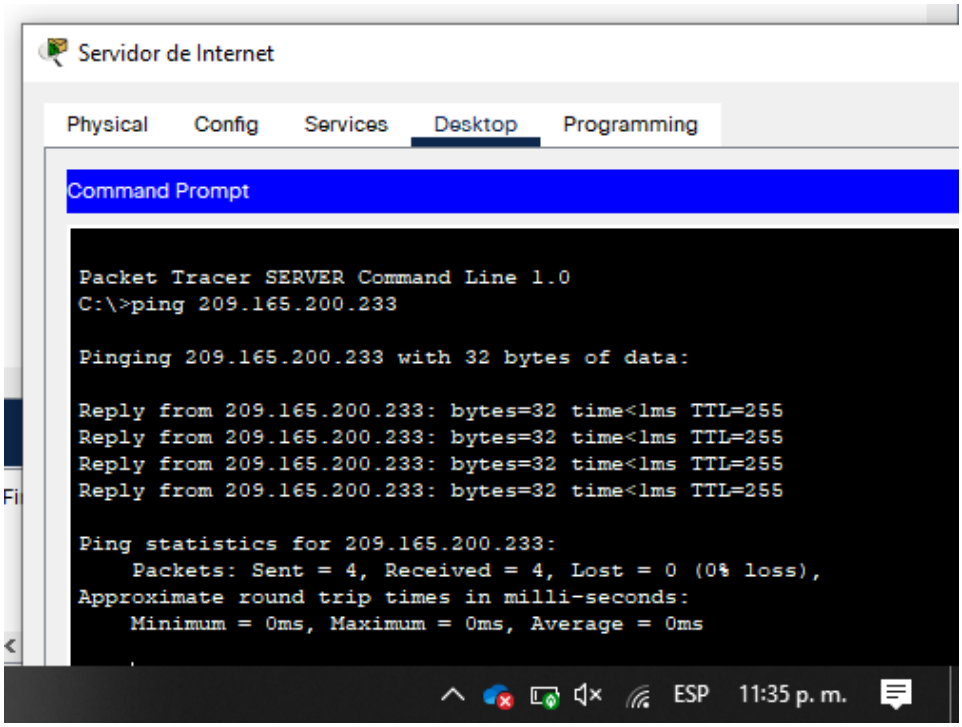
Fuente propia

Figura 5. Prueba de ping desde el Router 2 a el Router 3



Fuente propia

Figura 6. Prueba de ping desde el PC de Internet a el Gateway



Fuente propia

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 15. Configurar S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como elgateway predeterminado.

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	S2(config-if-range)#interface f0/6 S2(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S2(config-if)#int range f0/1-2, f0/4,f0/7-24, g0/1-2 S2(config-if-range)#shutdown

Fuente propia

Línea de Comando

S2#configure terminal → Inicio al modo privilegiado
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vlan 21 → Ingresamos a la VLAN
S2(config-vlan)#name Contabilidad→Asignamos nombre a la VLAN
S2(config-vlan)#vlan 23→ Ingresamos a la VLAN
S2(config-vlan)#name Ingenieria→Asignamos nombre a la VLAN
S2(config-vlan)#vlan 99→ Ingresamos a la VLAN
S2(config-vlan)#name administracion→Asignamos nombre a la VLAN
S2(config-vlan)#interface vlan 99→ Ingresamos a la interface de la VLAN 99
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S2(config-if)#ip address 192.168.99.2 255.255.255.0→ Asignamos una dirección IP
S2(config-if)#no shutdown→ Encendemos la Interface
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.99.1→ Asignamos la puerta de enlace
S2(config)#interface f0/3 → Ingresamos a la Interface
S2(config-if)#switchport mode trunk → cambiamos al modo de enlace troncal permanente
S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed

state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S2(config-if)#switchport trunk native vlan 1→Asignamos la VLAN 1
S2(config-if)#interface f0/5→ Ingresamos a la interface
S2(config-if)#switchport mode trunk→ cambiamos al modo de enlace troncal permanente
S2(config-if)#switchport trunk native vlan 1→Asignamos la VLAN 1
S2(config-if)#int range f0/1-2, f0/4,f0/6-24, g0/1-2→Seleccionamos varias interface
S2(config-if-range)#switchport mode access → cambia al modo de acceso permanente.
S2(config-if-range)#interface f0/6→ Ingresamos a la interface
S2(config-if)#switchport access vlan 21→ Asignamos la VLAN 1
S2(config-if)#int range f0/1-2, f0/4,f0/7-24, g0/1-2 Seleccionamos varias interface
S2(config-if-range)#shutdown→ Apagamos las Interfaces

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16. Configurar S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombrea cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama detopología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gatewaypredeterminado.
Forzar el enlace troncal en la interfazF0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	S3(config-if-range)#interface f0/18 S3(config-if)#switchport access vlan 21

Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-16,f0/17-24, g0/1-2 S3(config-if-range)#shutdown

Fuente propia

Línea de Comando

S3#configure terminal → Inicio al modo privilegiado
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 21→ Ingresamos a la VLAN
S3(config-vlan)#name Contabilidad→Asignamos nombre a la VLAN
S3(config-vlan)#vlan 23→ Ingresamos a la VLAN
S3(config-vlan)#name Ingenieria→Asignamos nombre a la VLAN
S3(config-vlan)#vlan 99→ Ingresamos a la VLAN
S3(config-vlan)#name administracion→Asignamos nombre a la VLAN
S3(config-vlan)#exit
S3(config)#interface vlan 99→ Ingresamos a la interface de la VLAN 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0→ Asignamos una dirección IP
S3(config-if)#no shutdown → Encendemos la Interface
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1→ Asignamos la puerta de enlace
S3(config)#interface f0/3→ Ingresamos a la Interface
S3(config-if)#switchport mode trunk→ cambiamos al modo de enlace troncal permanente
S3(config-if)#switchport trunk native vlan 1→Asignamos la VLAN 1
S3(config-if)#int range f0/1-2,f0/4-24, g0/1-2→Seleccionamos varias interface
S3(config-if-range)#switchport mode access → cambia al modo de acceso permanente.
S3(config-if-range)#interface f0/18→ Ingresamos a la interface
S3(config-if)#switchport access vlan 21→ Asignamos la VLAN
S3(config-if)#int range f0/1-2, f0/4-16,f0/17-24, g0/1-2→ Seleccionamos varias interface
S3(config-if-range)#shutdown→ Apagamos las Interfaces

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configurar R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	

Fuente propia

Línea de Comando

R1#configure terminal→ Inicio al modo privilegiado
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/1.21→ Ingresamos a la Subinterface
R1(config-subif)#encapsulation dot1Q 21→ protocolo que permite que el router tenga enlace troncal.
R1(config-subif)#ip address 192.168.21.1 255.255.255.0→ Asignamos una IP
R1(config-subif)#description vlan 21→ Agregamos una descripción
R1(config-subif)#interface g0/1.23→ Ingresamos a la Subinterface
R1(config-subif)#encapsulation dot1Q 23→ protocolo que permite que el router tenga enlace troncal.
R1(config-subif)#ip address 192.168.23.1 255.255.255.0→ Asignamos una IP
R1(config-subif)#description vlan 23→ Agregamos una descripción
R1(config-subif)#interface g0/1.99→ Ingresamos a la Subinterface
R1(config-subif)#encapsulation dot1Q 99→ protocolo que permite que el router tenga enlace troncal.
R1(config-subif)#ip address 192.168.99.1 255.255.255.0→ Asignamos una IP

R1(config-subif)#description vlan 99→ Agregamos una descripción
R1(config-subif)#interface g0/1 → Ingresamos a la Interface
R1(config-if)#no shutdown→Encendemos la Interface

Paso 4: Verificar la conectividad de la red

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

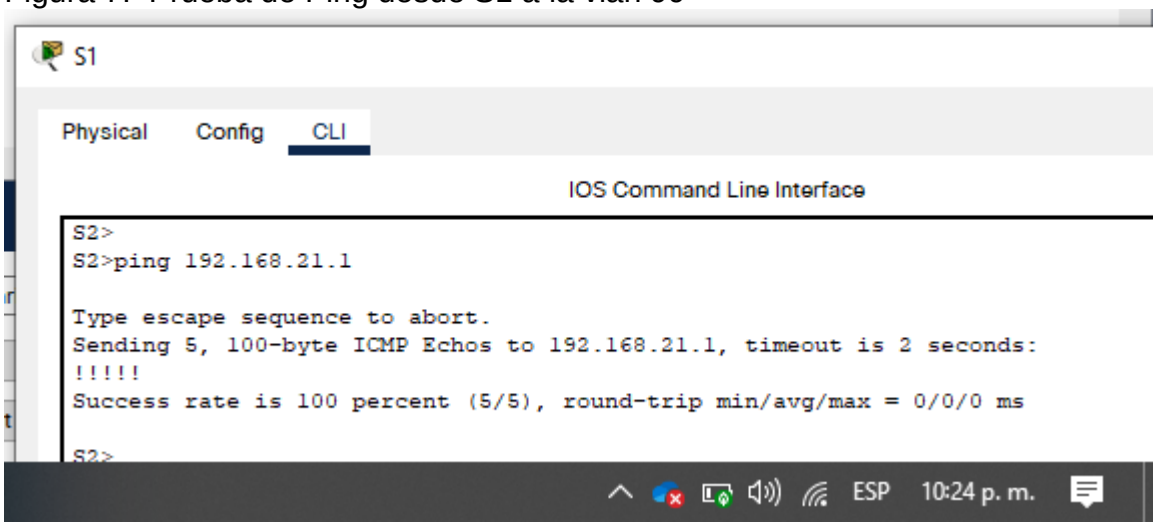
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 18. Verificar la conectividad

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso 5 enviado y 5 recibido
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso 5 enviado y 5 recibido
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso 5 enviado y 5 recibido
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso 5 enviado y 5 recibido

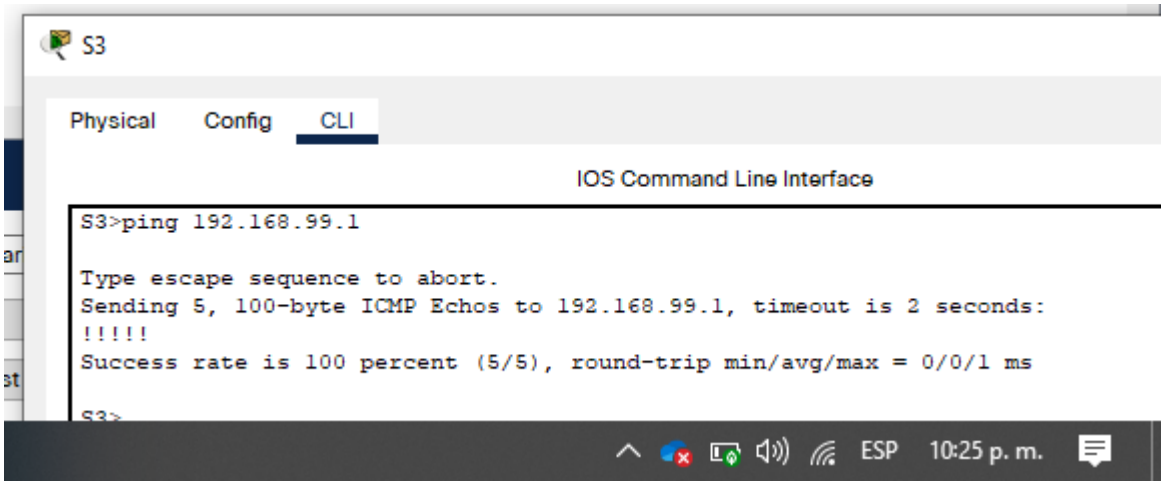
Fuente propia

Figura 7. Prueba de Ping desde S1 a la vlan 99



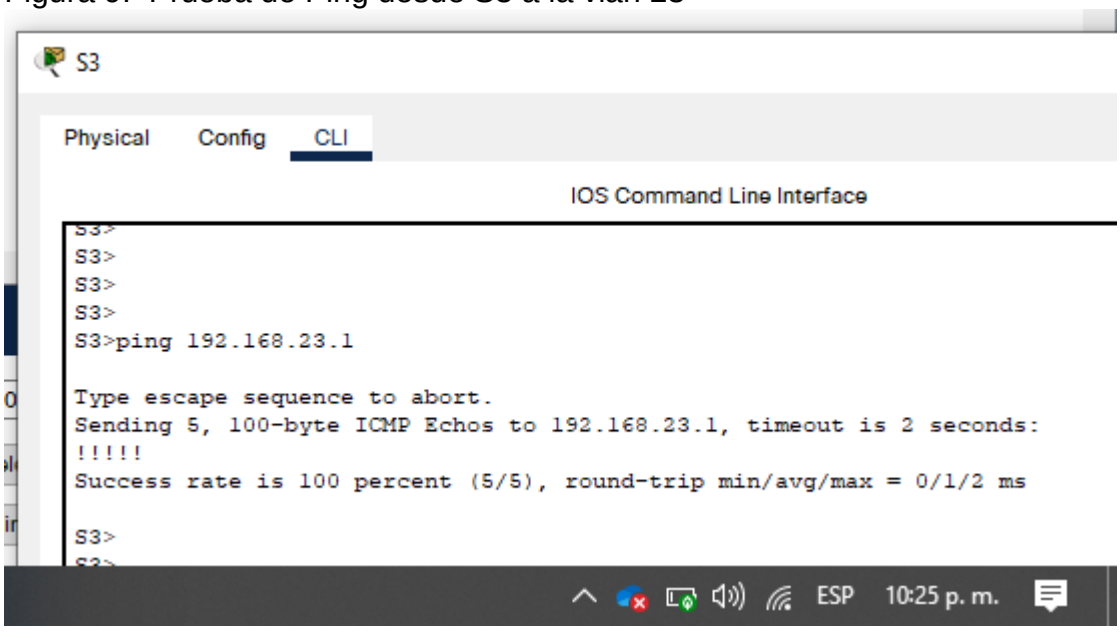
Fuente Propia

Figura 8. Prueba de Ping desde S3 a la vlan 99



Fuente Propia

Figura 9. Prueba de Ping desde S3 a la vlan 23



Fuente Propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 19. Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Fuente propia

Línea de Comando

R1>enable→ Inicio al modo privilegiado
R1#configure terminal → Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1 → Creamos el protocolo OSPF
R1(config-router)#router-id 1.1.1.1 → Asignamos un id al Protocolo
R1(config-router)#do show ip route connected → Verificamos las redes directamente Conectadas
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 → Anunciamos la red conectada
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0→ Anunciamos la red conectada
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0→ Anunciamos la red conectada
R1(config-router)#network 172.16.1.0 0.0.0.0 area 0→ Anunciamos la red conectada
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0→ Anunciamos la red conectada

R1(config-router)#passive-interface g0/1.21→ Establecemos la interface como pasivas
R1(config-router)#passive-interface g0/1.23→ Establecemos la interface como pasivas
R1(config-router)#passive-interface g0/1.99→ Establecemos la interface como pasivas
R1(config-router)#no auto-summary→ Desactiva la sumarización automática

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 20. Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Fuente propia

Línea de Comando

R2#configure terminal → Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1→ Creamos el protocolo OSPF
R2(config-router)#router-id 2.2.2.2→ Asignamos un id al Protocolo
R2(config-router)#do show ip route connected→ Verificamos las redes directamente Conectadas
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0→ Anunciamos la red conectada
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0→ Anunciamos la red conectada
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0→ Anunciamos la red conectada
R2(config-router)#passive-interface Loopback0→ Establecemos la interface como pasivas
R2(config-router)#no auto-summary→ Desactiva la sumarización automática

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 21. Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Fuente propia

Línea de Comando

R3#configure terminal→ Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1→ Creamos el protocolo OSPF
R3(config-router)#router-id 3.3.3.3 → Asignamos un id al Protocolo
R3(config-router)#do show ip route connected→ Verificamos las redes directamente Conectadas
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6
R3(config-router)#network 172.16.2.0 0.0.0.255 area 0→ Anunciamos la red conectada
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0→ Anunciamos la red conectada
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0→ Anunciamos la red conectada
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0→ Anunciamos la red conectada
R3(config-router)#passive-interface Loopback4→ Establecemos la interface LAN como pasivas
R3(config-router)#passive-interface Loopback5→ Establecemos la interface LAN como pasivas
R3(config-router)#passive-interface Loopback6→ Establecemos la interface LAN como pasivas
R3(config-router)#no auto-summary→ Desactiva la sumarización automática

Paso 4: Verificar la información de OSPF

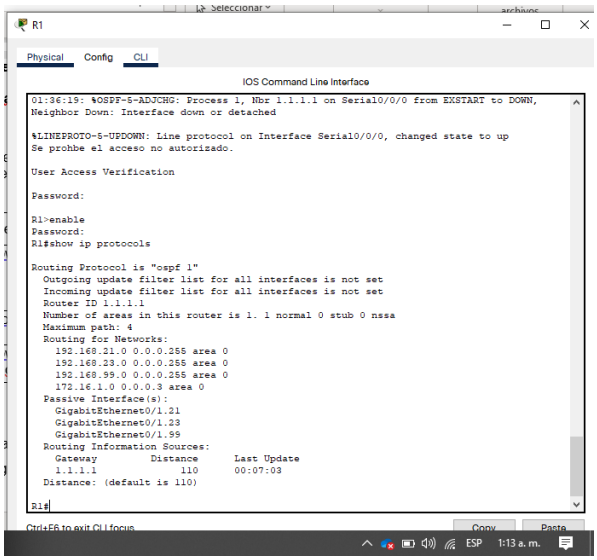
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 21. Configurar OSPFv3 en el R2

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
¿Qué comando muestra solo las rutas OSPF?	R1# show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show running-config | section ospf

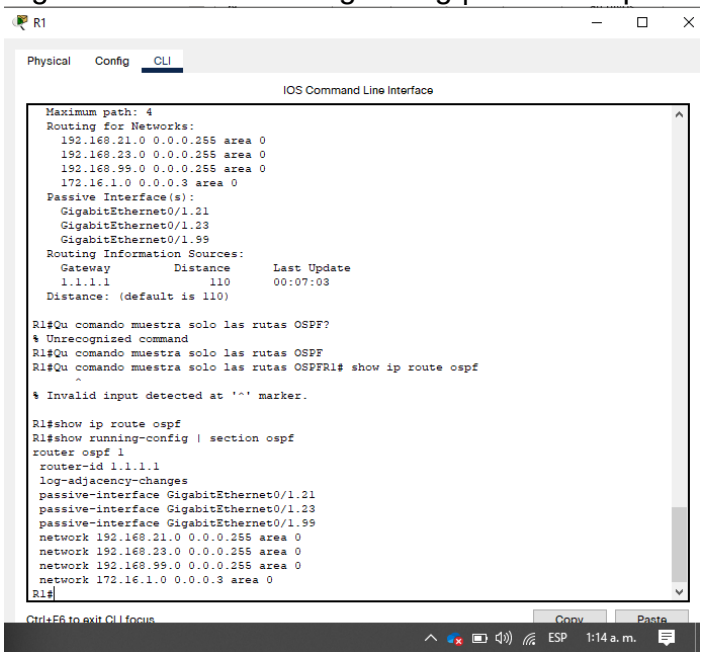
Fuente propia

Figura 10. Comando show ip protocols



Fuente propia

Figura 11. show running-config | section ospf



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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Implementar DHCP y NAT para IPv4

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP enla VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP enla 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.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna- sa.com Establecer el gateway predeterminado

Fuente propia

Línea de Comando

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 → Reserva direcciones IP
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20→ Reserva direcciones IP
R1(config)#interface g0/1.21→ Ingresamos a la subinterfaz
R1(config-subif)#ip dhcp pool ACCT → Habilitamos el servicio DHCP
R1(dhcp-config)#network 192.168.21.0 255.255.255.0 → Asignamos direccionamiento de red
R1(dhcp-config)#default-router 192.168.21.1→ Asignamos la puerta de enlace
R1(dhcp-config)#dns-server 10.10.10.10→ Asignamos los DNS
R1(dhcp-config)#domain-name ccna-sa.com→ Asignamos el dominio
R1(dhcp-config)#interface g0/1.23→ Ingresamos a la subinterfaz
R1(config-subif)#ip dhcp pool ENGNR→ Habilitamos el servicio DHCP
R1(dhcp-config)#network 192.168.23.0 255.255.255.0→ Asignamos direccionamiento de red
R1(dhcp-config)#default-router 192.168.23.1→ Asignamos la puerta de enlace
R1(dhcp-config)#dns-server 10.10.10.10→ Asignamos los DNS
R1(dhcp-config)#domain-name ccna-sa.com→ Asignamos el dominio
R1(dhcp-config)#

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23. Configurar la NAT estática y dinámica 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
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config-if)#ip nat outside
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
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
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool internet

Fuente propia

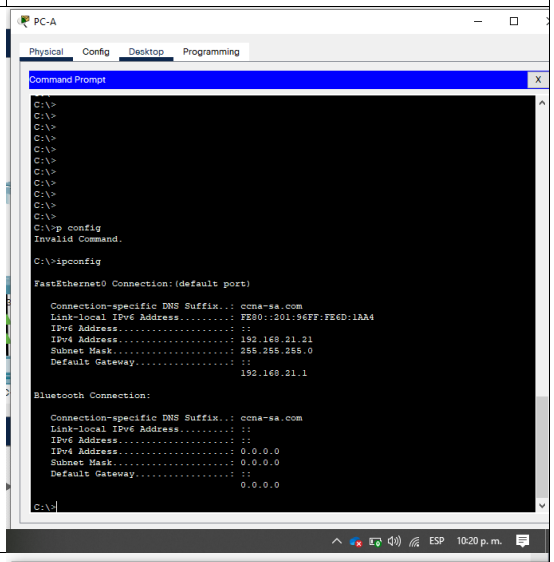
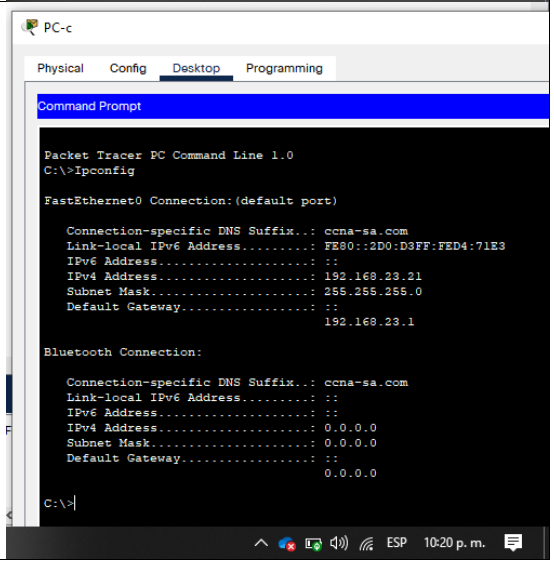
Línea de Comando

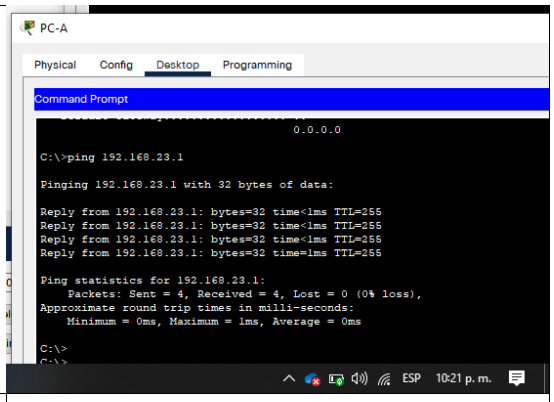
R2#configure terminal→ Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 secret 5 cisco12345→ Crear una base de datos local con una cuenta de usuario
R2(config)#ip http server→ Habilitar el servicio del servidor HTTP
R2(config)#ip http authentication local→ Configurar el servidor HTTP para utilizar la base de datos local para la autenticación
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237→ Crear una NAT estática al servidor web
R2(config)#interface g0/0→ Ingresamos a la Interface
R2(config-if)#ip nat outside→Configura la NAT hacia fuera
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255→ Permite el acceso a la dirección
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255→ Permite el acceso a la dirección
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255→ Permite el acceso a la dirección
R2(config)#ip nat pool internet 209.165.200.233 209.165.200.236 netmask 255.255.255.248→ Defina el pool de direcciones IP públicas utilizables.
R2(config)#ip nat inside source list 1 pool internet → Definir la traducción de NAT dinámica
R2(config)#

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. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	

Verificar que la PC-A pueda hacer ping ala PC-C Nota: Quizá sea necesario deshabilitar elfirewall de la PC.	
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	

Fuente propia

Parte 6: Configurar NTP

Tabla 25. Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con horaNTP.	
Verifique la configuración de NTP en R1.	

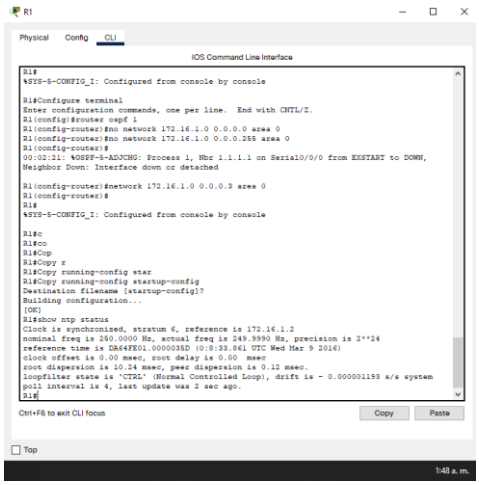
Fuente propia

Linea de Comando R2
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2#clock set 09:00:00 5 march 2016
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5

Línea de Comando R1

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ntp s
R1#show ntp status
Clock is synchronized, stratum 6, reference is 172.16.1.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is DA60373C.0000026E (9:11:24.622 UTC Sat Mar 5 2016)
clock offset is 1.00 msec, root delay is 2.00 msec
root dispersion is 10.20 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s
system poll interval is 4, last update was 16 sec ago.
R1#

Figura 12. show ntp status



Fuente propia

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

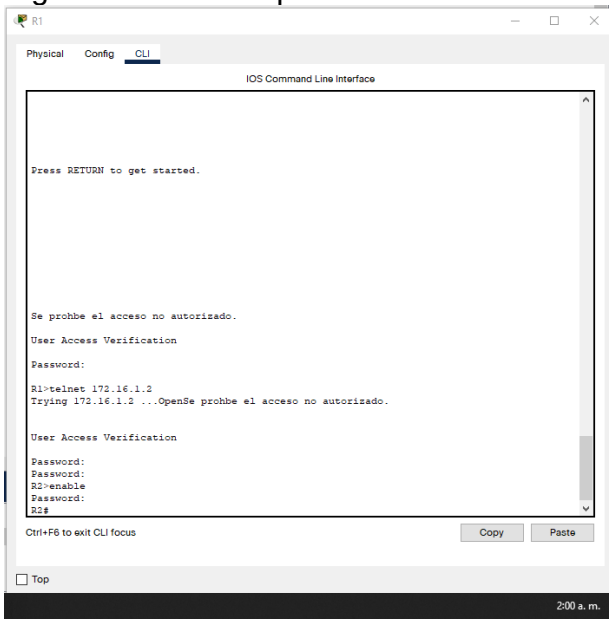
Paso 1: Restringir el acceso a las líneas VTY en el R2 Configurar NTP

Tabla 26. Restringir el acceso a las líneas VTY en el R2 Configurar NTP

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
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet R2(config-line)#
Verificar que la ACL funcione como se espera	Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1

Fuente propia

Figura 13. acceso por Telnet a las líneas de VTY

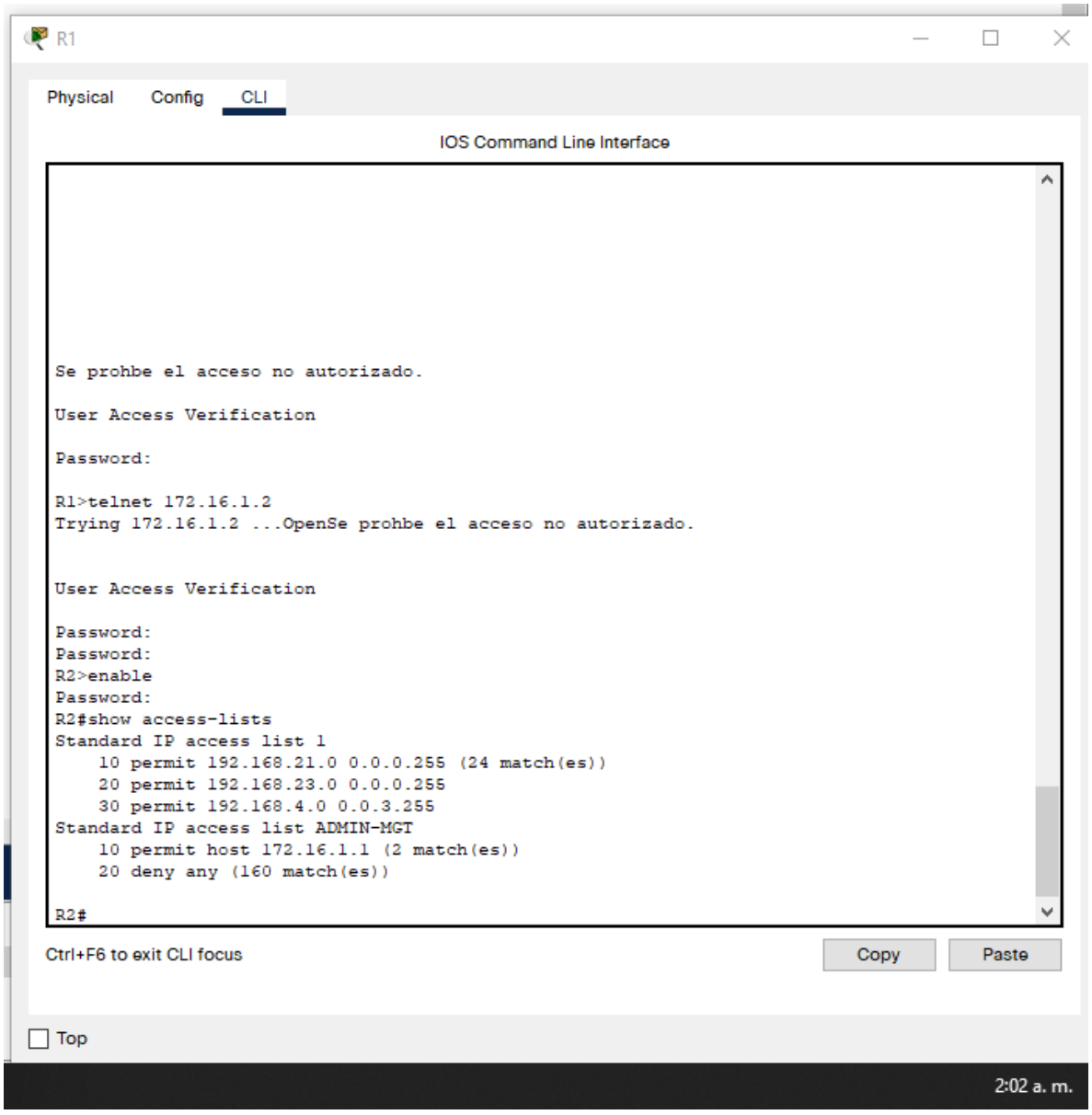


Fuente Propia

Línea de Comando

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip access-list standard  ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
```

Figura 14. show access-lists



Fuente propia

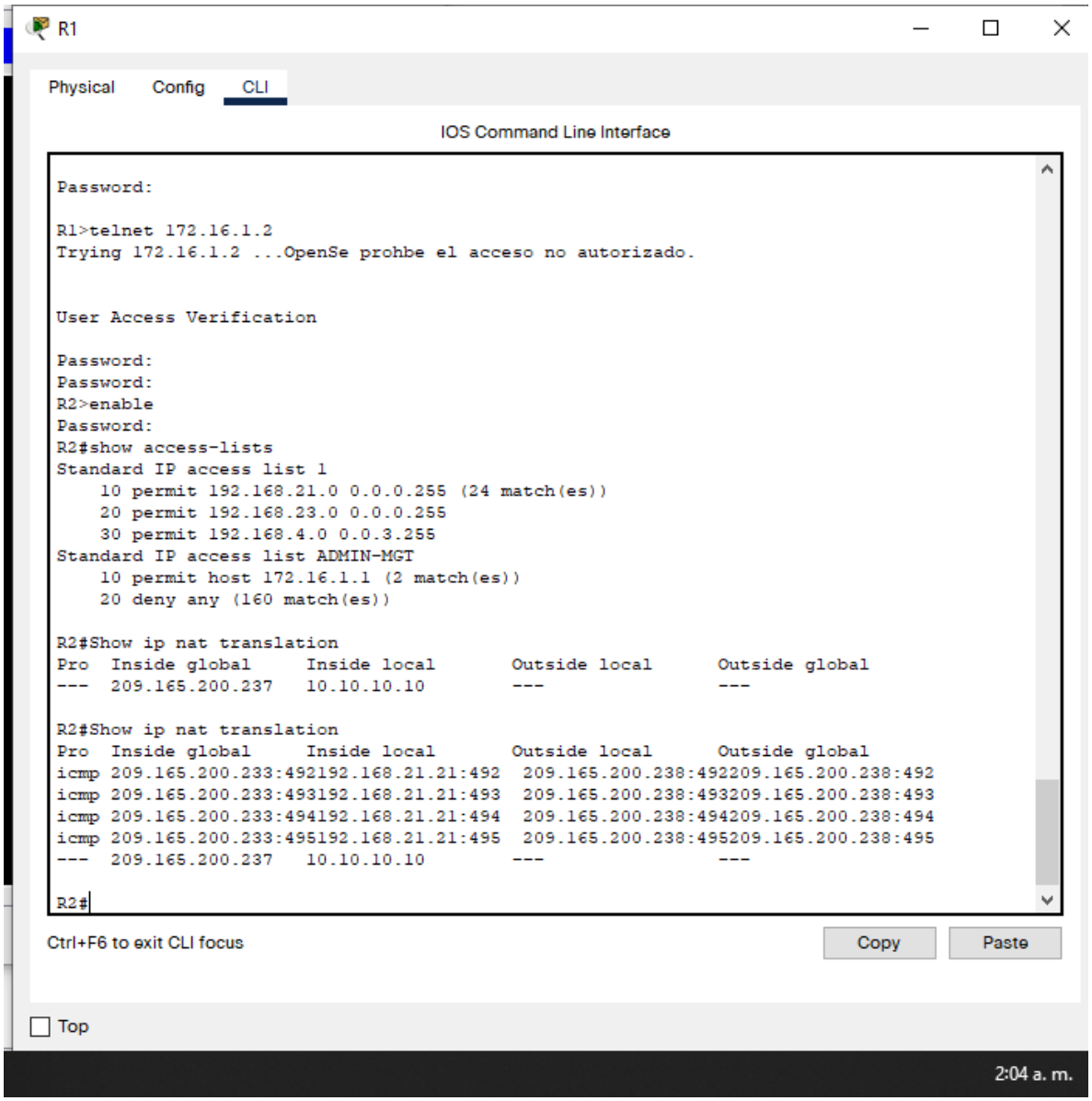
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 27. comando de CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas poruna lista de acceso desde la última vez que se restableció	Show ip Access-list
Restablecer los contadores de una listade acceso	Clear Access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la direcciónen que se aplica?	Show ip interface s0/0/0
¿Con qué comando se muestran lastraducciones NAT?	Nota: Las traducciones para la PC-A y la PC-C se agregarona 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 translation
¿Qué comando se utiliza para eliminarlas traducciones de NAT dinámicas?	Clear ip nat translation *

Fuente propia

Figura 14. Show ip nat translation



CONCLUSIONES

En el anterior trabajo se logra realizar dos simulaciones de red mediante el programa de Cisco Packet Tracer donde se aplicaron las habilidades aprendidas durante el diplomado de Cisco CCNA.

Para esta actividad se logró realizar la división de una red pequeña en donde por medio de máscara variable se asignó la red según los hosts que se necesitará, esto con el fin de tener un control de las IP asignadas mediante segmentos, de igual forma se realizan las configuraciones de seguridad a nivel de acceso a los dispositivos

También se evidencia la funcionalidad de el protocolo de enrutamiento OSFP que nos permite direccionar los paquetes por la ruta más ágil de acuerdo con los recursos que tengan los dispositivos.

Además, se implementa una NAT que permite la traducción de las redes LAN para la conexión de salida de internet de forma segura. Mediante listas de accesos con una máscara invertida

BIBLIOGRÁFIA

aws. (s.f.). Amazon . Obtenido de https://aws.amazon.com/es/route53/what-is-dns/

Desconocido. (s.f.). speedcheck. Obtenido de https://www.speedcheck.org/es/wiki/mascara-de-red/

irvingjuarez. (01 de 01 de 2021). platzi. Obtenido de https://platzi.com/tutoriales/1277-redes/9070-subnetting-que-es-y-como-funciona/?utm_source=google&utm_medium=cpc&utm_campaign=12915366154&utm_adgroup=&utm_content=&gclid=CjwKCAjw5c6LBhBdEiwAP9ejG0Kk7OCPAOYDtlMqGyg6CENedCyARlxxYdrpswklI3WoC91tly7u6hoCFIQQ

Wikipedia . (15 de 10 de 2021). Obtenido de https://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. Inge Cuc, 12(1), 86-93.

GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. Revista de Tecnología, 14(1), 127-138.

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In International Conference on Knowledge Management in Organizations (pp. 331-344). Springer, Cham.

BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. Revista UIS Ingenierías, 16(1), 75-84.

BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In 2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI) (pp. 1-5). IEEE.

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in

Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.