SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

CESAR ARMANDO CRUZ CRUZ

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

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

CESAR ARMANDO CRUZ CRUZ

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

TUTOR:
INGENIERO JAVIER RICARDO VASQUEZ

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

FACATATIVÁ, 28 de noviembre de 2021

AGRADECIMIENTOS

Doy gratitud a mis padres por darme su ejemplo de la constancia, la persistencia y la paciencia para lograr objetivos y metas, también agradezco a mi esposa por apoyarme y confiar en mí en este desafío que me trace y a mi hijo a quien le dedico este gran logro “nadie nos dijo que era fácil, pero tampoco nadie nos dijo que fuera imposible”.

CONTENIDO

LISTA DE TABLAS

TABLA DE FIGURAS

GLOSARIO

Tolerancia a fallas:

Una característica de la red que restringe el impacto de una falla en el acceso a la red y permite que una red se recupere rápidamente de dicha falla.

QoS:

Un mecanismo que permite administrar el flujo del tráfico en función de diversos requisitos a fin de garantizar la entrega confiable de cada tipo de tráfico.

BYOD:

Hace posible que los usuarios tengan la libertad de utilizar sus dispositivos personales para acceder a una red corporativa o de campus.

Red convergente:

Una red con la funcionalidad de entregar tráfico con distintos requisitos, pero que usa la misma infraestructura de red.

DSL:

Tecnología que le ofrece al usuario conexión a Internet con ancho de banda de alta velocidad a través de una línea telefónica.

Intranet:

Una interconexión privada de redes LAN y WAN dentro de una organización a la que solo pueden acceder los miembros de la organización o las personas que no sean miembro, pero tengan autorización.

Extranet:

Una red que proporciona acceso seguro a los datos de una organización a las personas autorizadas que trabajan fuera de la organización.

Internet:

El conjunto de redes con interconexión global.

Shell:

Parte del sistema operativo que interactúa con las aplicaciones y el usuario.

Kernel:

Parte del sistema operativo que se comunica directamente con el hardware de la computadora.

Consola:

Un puerto físico de un dispositivo Cisco que proporciona acceso al dispositivo a través de un canal de administración exclusivo, también conocido como acceso fuera de banda.

Configuración de inicio:

Archivo que se almacena en la memoria de acceso aleatorio no volátil (NVRAM) y contiene la configuración guardada en un dispositivo que se utilizará en el inicio o en el reinicio.

SSH:

Un protocolo para establecer una conexión de Interfaz de línea de comandos (CLI) remota y segura a través de la red.

Ping:

Comando para verificar la conectividad entre el origen (el dispositivo en el que se emitió el comando) y el destino (la dirección IP que se utilizó como argumento).

Traceroute:

Comando para verificar la ruta por la que se traslada un paquete para llegar al destino.

Ipconfig:

Comando de Windows que muestra los parámetros de configuración IP en una PC.

Encapsulamiento:

Proceso mediante el cual se inserta un mensaje con formato dentro de otro mensaje con formato.

Unidifusión:

Una forma de entrega de mensajes en la que el mensaje se entrega a un solo puerto de destino.

Multidifusión:

Una forma de transmisión en la que el mensaje se entrega a un grupo de hosts.

PDU:

La forma que adopta una porción de datos asociada con cada capa de protocolo.

Topología física:

Los diseños y las conexiones reales de los dispositivos de una red.

RESUMEN

En el siguiente informe se documenta el desarrollo elegido para el diplomado de profundización en CCNA CISCO, buscando las destrezas, habilidades y conocimiento en entornos de trabajo propuestos en Networking. La prueba plantea la solución a dos escenarios correspondientes a la implementación de entornos reales basados en los diferentes lineamientos de direccionamiento IPv4, el registro de configuración de dispositivos, la digitalización del código del paso a paso de cada etapa trabajada, el registro de cada uno de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros utilizando la herramienta CISCO Packet Tracer en la versión 8.0.1.

Palabras Clave: CISCO, CCNA, Networking, Configuración, Conectividad, Packet Tracer, Comandos.

ABSTRACT

The following report documents the development chosen for the deepening diploma at CCNA CISCO, seeking the skills, abilities and knowledge in work environments proposed in Networking. The test proposes the solution to two scenarios corresponding to the implementation of real environments based on the different IPv4 addressing guidelines, the device configuration register, the digitization of the step-by-step code of each stage worked, the registration of each one of the connectivity verification processes through the use of ping, traceroute, show ip route commands, among others using the CISCO Packet Tracer tool in version 8.0.1.

Keywords: CISCO, CCNA, Networking, Configuration, Connectivity, Packet Tracer, Commands.

INTRODUCCIÓN

Como parte del desarrollo personal y profesional, decidí realizar el diplomado de profundización cisco enfocado en el diseño e implementación de soluciones integradas LAN / WAN, ya que la academia CISCO es líder en el mundo de las redes de datos y TI, CISCO ofrece gran cantidad de componentes y equipos necesarios en las comunicaciones y las redes, gran parte del mundo trabaja con este tipo de elementos, es en este planteamiento donde cobra fuerza la idea de adquirir conocimiento, practica y habilidades necesarios para el manejo de estos equipos ya que además cuenta con plataformas para el desarrollo de prácticas en entornos cotidianos. CISCO ofrece la certificación de los cursos aprobados.

Para el primer escenario se plantea la configuración de una red doméstica pequeña con un router, un switch y dos pc. Podemos encontrar la documentación de las tareas propuestas soportado por un archivo pkz en el cual se desarrolla el diseño del esquema de direccionamiento IPV4. Tambien encontramos el desarrollo del subneteo de acuerdo a la dirección de red No. 192.168.58.0.

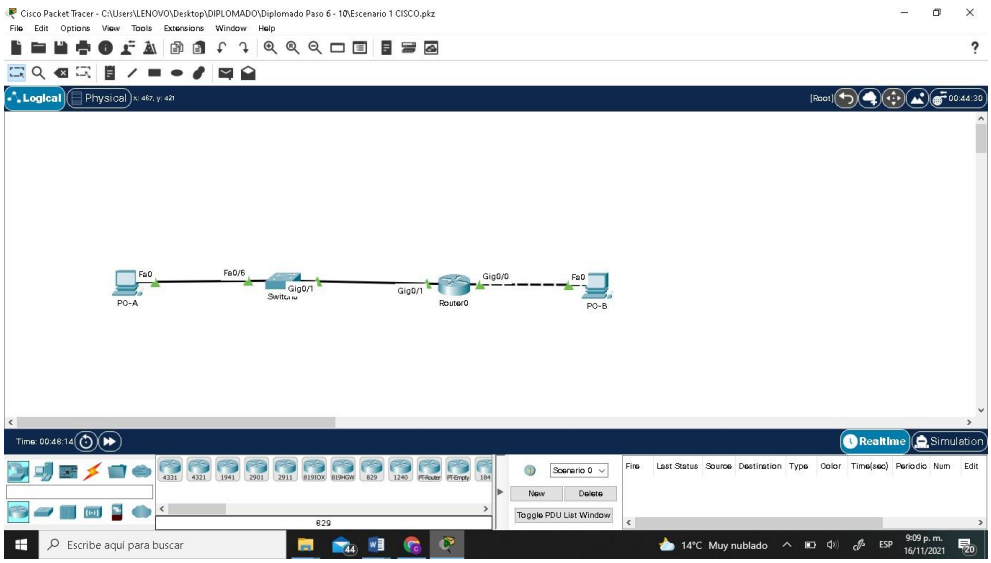
Para el segundo escenario la prueba de habilidades nos solicita crear una red pequeña con conectividad IPv4 e IPv6, parámetros de seguridad en los switches y routers, VLAN, configuración con protocolos OSPF, DHCP, NTP, listas de control ACL y comandos CLI. De esta forma logramos la interpretación, diseño y configuración de ambientes reales de RED sus conexiones y jugar con los protocolos según la necesidad del cliente.

DESARROLLO

ESCENARIO 1:

Topología:

Figura 1. Topología de simulación escenario 1



Fuente: Autor

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 5: 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).

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.

El swicht maneja tramas de internet, tiene una dirección IP para la administración de red, y para la etapa de enrutamiento lo realizará el router.

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.

Tabla 1 de direccionamiento

Item	Requerimiento	
Dirección de Red 192.168.**X**.0 donde X corresponde a los últimos dos dígitos de su cédula.	192.168.58.0 / 24	
Requerimiento de host Subred LAN1 100	Dirección de red:	192.168.58.0
	Masc:	/25
	Cantidad de direcciones:	128
	Cantidad de direcciones útiles:	126
	Primera dirección valida:	192.168.58.1
	Ultima dirección valida:	192.168.58.126
	Broadcast:	192.168.58.127
	Mascara decimal	255.255.255.128
Requerimiento de host Subred LAN2 50	Dirección de red:	192.168.58.128
	Masc:	/26
	Cantidad de direcciones:	64
	Cantidad de direcciones útiles:	62
	Primera dirección valida:	192.168.58.129
	Ultima dirección valida:	192.168.58.190
	Broadcast:	192.168.58.191
	Mascara decimal	255.255.255.192
R1 G0/0/1 Primera dirección de host de la subred LAN1	192.168.58.1 /26	
R1 G0/0/0 Primera dirección de host de la subred LAN2	192.168.58.129 /25	
S1 SVI Segunda dirección de host de la subred LAN1	192.168.58.1	
PC-A Última dirección de host de la subred LAN1	192.168.58.129 /26	
PC_A Última dirección de host de la subred LAN2	192.168.58.99 /25	

Nota: Se desarrolla la tabla de direccionamiento de acuerdo a los requerimientos de la actividad.
Fuente: Autor

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 2 Configuración y direccionamiento del router

Tarea	Especificación
Desactivar la búsqueda DNS	Deshabilite la búsqueda DNS Si se desactiva la búsqueda DNS un router no podría resolver los nombres, lo cual provocaría posibles problemas cuando el router necesite una dirección IP para enviar un paquete (se desactiva cuando se hacen pruebas para que el Router no intente buscas una entrada DNS para un nombre que en realidad es un error de escritura). Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#exit Router# %SYS-5-CONFIG_I: Configured from console by console Router#
Nombre del router R1	Asigne el nombre de dispositivo al Router (R1). Se utiliza el comando hostname con el fin de que establezca el nombre de Router a R1. Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R1 R1(config)#exit
Nombre de dominio	Asigne el nombre del dominio en el router para el usuario ingrese a la dirección que es ccna-lab.com R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip domain-name ccna-lab.com R1(config)#exit R1#

Contraseña cifrada para el modo EXEC privilegiado	El usuario ingrese con la contraseña que es ciscoenpass. R1# R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#enable secret ciscoenpass R1(config)#exit R1#
Contraseña de acceso a la consola	Asigne ciscoconpass como la contraseña de consola 0 y habilite el inicio de la sesión. Y pueda ingresar a la consola con la contraseña que aparece y el login es para deshabilitar la autenticación. R1# %SYS-5-CONFIG_I: Configured from console by console R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit R1(config)#exit R1#
Establecer la longitud mínima para las contraseñas en 10 caracteres.	Se utiliza el comando security passwords min-length longitud en el modo de configuración global. En el ejemplo, cualquier contraseña nueva configurada debería tener una longitud mínima de ocho caracteres. Password: Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#security password min-length 10 R1(config)#exit R1#

Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#username admin secret admin1pass R1(config)#exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)# R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)# R1(config)#service password-encryption R1(config)#exit R1#
Configure un MOTD Banner	R1#configure terminal R1(config)#banner motd $Prohibido el acceso no autorizado$ R1(config)#exit R1#
Configurar interfaz G0/0/0 Establezca la descripción Establece la dirección IPv4. Activar la interfaz.	R1>enable Password: Password: R1#configure terminal R1(config)#interfa R1(config)#interface gi R1(config)#interface gigabitEthernet 0/0 R1(config-if)#ip address 192.168.58.129 255.255.255.192 R1(config-if)#no shut R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

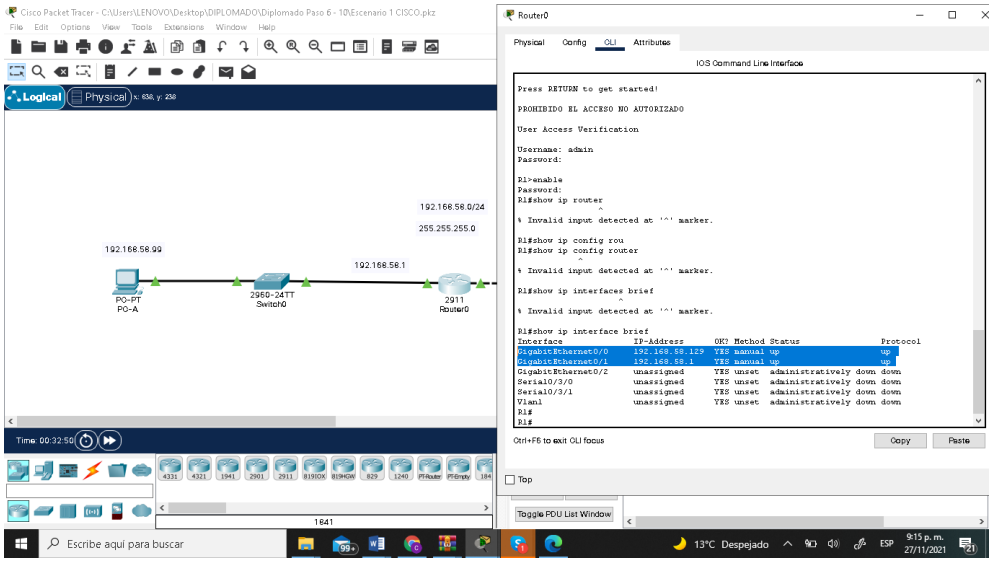
	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up R1(config-if)#
Configurar interfaz G0/0/1 Establezca la descripción Establece la dirección IPv4. Activar la interfaz.	R1>enable Password: Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#inter R1(config)#interface gig R1(config)#interface gigabitEthernet 0/1 R1(config-if)#ip address 192.168.58.1 255.255.255.128 R1(config-if)#no sh R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Generar una clave de cifrado RSA	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#no ip domain-lookup R1(config)#crypto key generate rsa % Please define a domain-name first. R1(config)#ip domain-name ccna-lab.com R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Mar 6 23:57:6.933: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#

Nota: El desarrollo de la tabla está enfocada a la configuración del ruoter y al direccionamiento del mismo según las especificaciones de la guía.
Fuente: Autor

Figura 2. Comando show ip interface brief



Fuente: Autor

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3 Configuración del switch

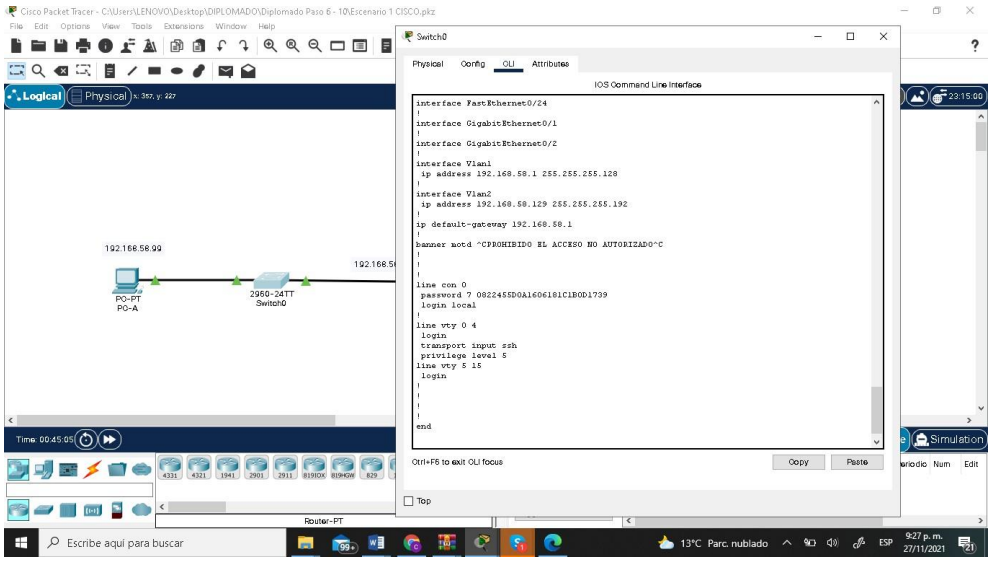
Tarea	Especificación
Desactivar la búsqueda DNS.	Enter configuration commands, one per line. End with CNTL/Z. S1(config)#no ip domain-lookup S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console S1#
Nombre del switch	S1 Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname S1 S1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console S1#
Nombre de dominio	S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#ip domain-name ccna-lab.com S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console S1#
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass S1(config)#enable secret ciscoenpass S1(config)#line console 0
Contraseña de acceso a la consola	ciscoconpass S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass S1(config)#username admin password admin1pass

	S1(config)# S1(config)#^Z S1# %SYS-5-CONFIG_I: Configured from console by console S1#exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Switch 1 S1(config)#line vty 0 4
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#privilege level 5 S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd $PROHIBIDO EL ACCESO NO AUTORIZADO$
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa general-keys modulus 1024 % You already have RSA keys defined named S1.ccna-lab.com % They will be replaced. % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *Mar 1 0:23:55.506: %SSH-5-ENABLED: SSH 1.99 has been enabled
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento S1(config)#interface vlan1 S1(config-if)#ip address 192.168.58.1 255.255.255.128 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

	%IP-4-DUPADDR: Duplicate address 192.168.58.1 on Vlan1, sourced by 0003.E4C5.E202 S1(config-if)#exit S1(config)#exit S1# %SYS S1(config)# S1(config)#interface vlan2 S1(config-if)#ip address 192.168.58.128 255.255.255.192 Bad mask /26 for address 192.168.58.128 S1(config-if)#no shutdown S1(config-if)#
Configuración del Gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento. S1(config-if)# S1(config-if)#ip default-gateway 192.168.58.1 S1(config)#exit S1#

Nota: El desarrollo de la tabla es enfocado en la configuración del switch de acuerdo a los parámetros solicitados en la guía.
Fuente: Autor

Figura 3. Comando show runing-config



Fuente: Autor

Paso 2. Configurar los equipos

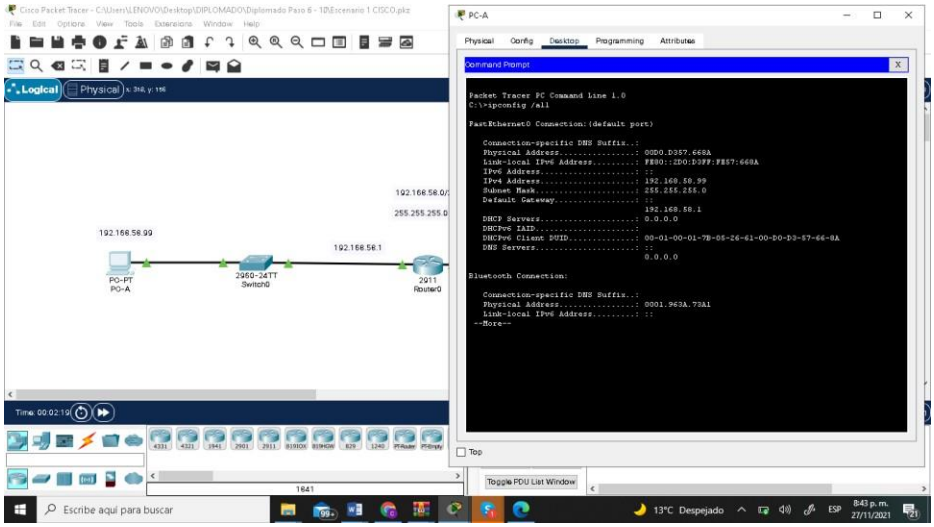
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 4 Configuración computador A

	PC-A Network Configuration
Descripción	*PC-A*
Dirección física	*en blanco*
Dirección IP	*192.168.59.99*
Máscara de subred	*255.255.255.0*
Gateway predeterminado	*192.168.58.1*

Nota: El desarrollo de la tabla está enfocado a la configuración del computador A de acuerdo a los parámetros solicitados en la guía
Fuente: Autor.

Figura 4. Comando ipconfig /all PC-A



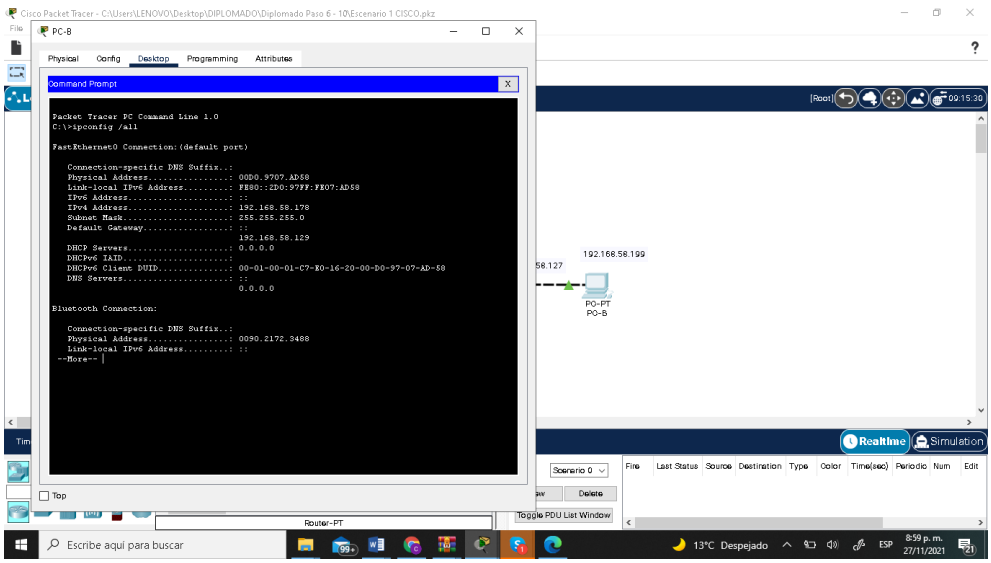
Fuente: Autor

Tabla 5 Configuración computador B.

	PC-B Network Configuration
Descripción	*PC-B*
Dirección física	*en blanco*
Dirección IP	*192.168.59.178*
Máscara de subred	*255.255.255.0*
Gateway predeterminado	*192.168.58.129*

Nota: El desarrollo de la tabla está enfocado a la configuración del computador B de acuerdo a los parámetros solicitados en la guía.
Fuente: Autor

Figura 5. Comando ipconfig /all PC-B



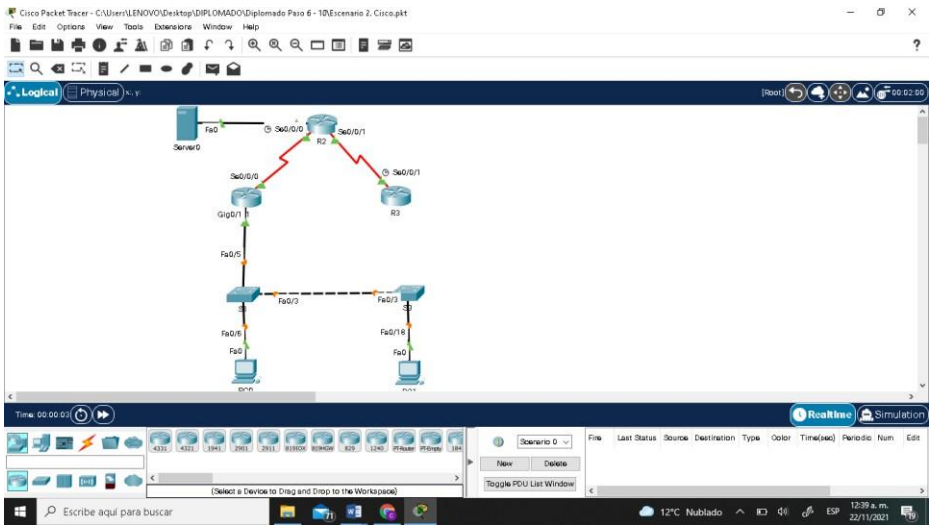
Fuente: Autor

ESCENARIO 2:

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

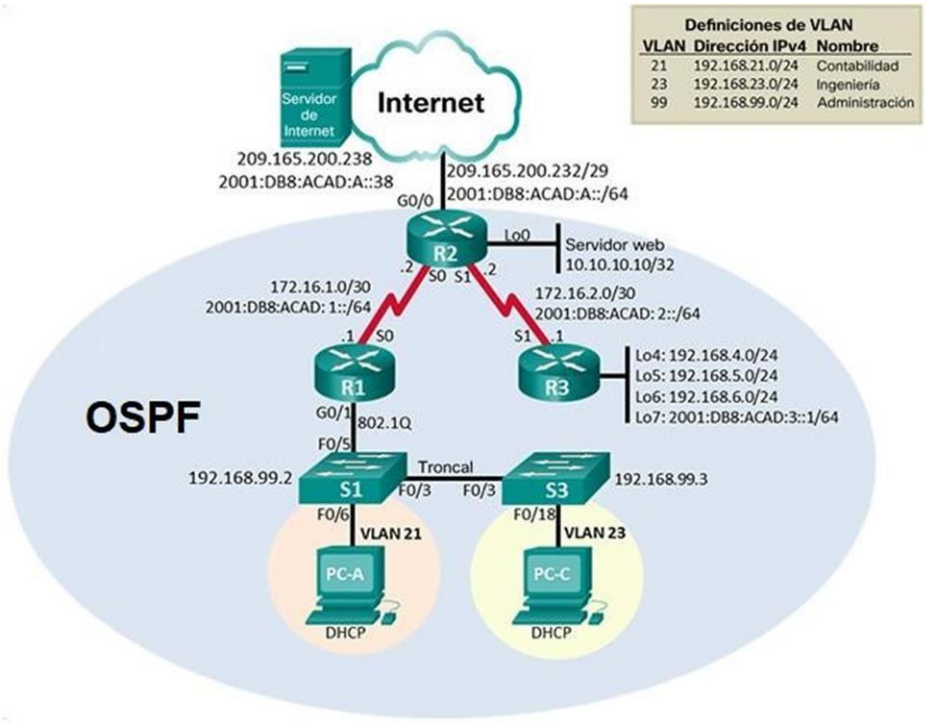
Topología:

Figura 6. Topología de simulación escenario 2.



Fuente: Autor

Figura 7. Escenario 2



Fuente: Evaluación: Prueba de habilidades prácticas CCNA

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 6 Configuración de routers y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Would you like to enter the initial configuration dialog? [yes/no]: no Press RETURN to get started! 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#
Eliminar el archivo startup-config de todos los routers	Would you like to enter the initial configuration dialog? [yes/no]: no Press RETURN to get started! 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# Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete

	%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch# Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory) Switch#
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté 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#

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

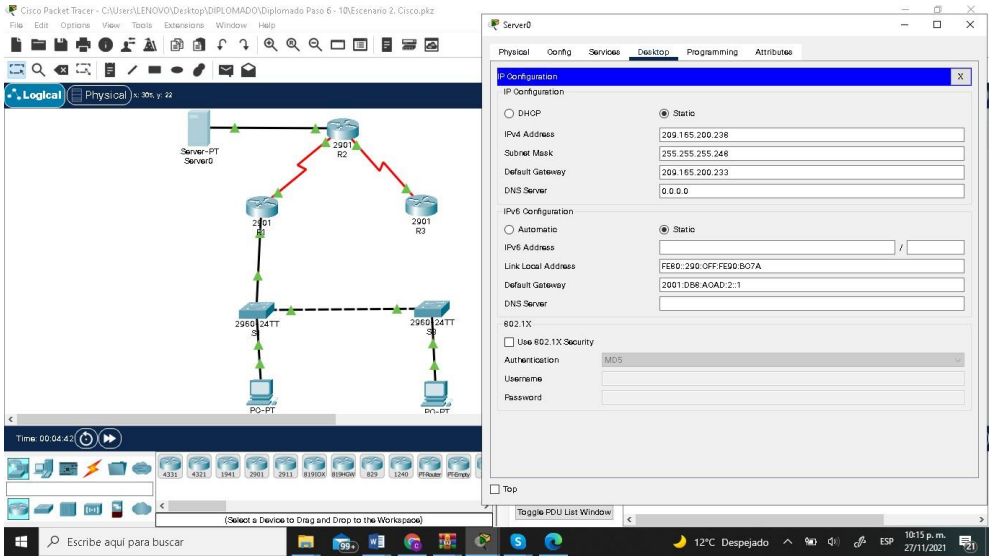
(para obtener información de las direcciones IP, consulte la topología):

Tabla 7 Configuración de la computadora de internet.

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	
Máscara de subred para IPv4	
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: Autor

Figura 8. Configuracion computadora de Internet



Fuente: Autor

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

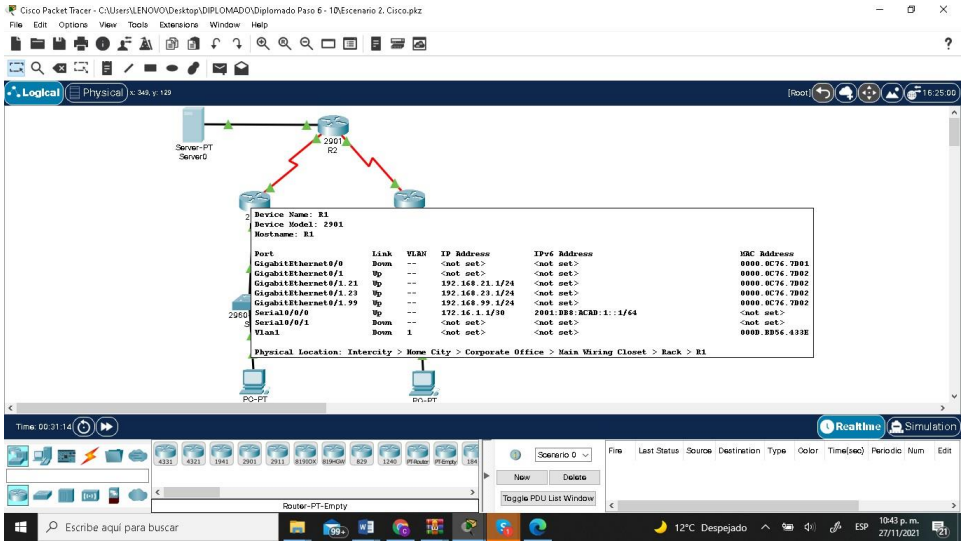
Tabla 8 Configuración R1

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
Nombre del router R1	Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada class	R1(config)# R1(config)#enable secret class
Contraseña de acceso a la consola cisco	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet cisco	R1(config-line)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exi

Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#
Mensaje MOTD Se prohíbe el acceso no autorizado.	R1(config)#banner motd $SE PROHIBE EL ACCESO NO AUTORIZADO$ R1(config)#exit R1#
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	R1>enable Password: Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int R1(config)#interface se R1(config)#interface serial 0/0/0 R1(config-if)#description Connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down R1(config-if)#ipv6 unicast-routing R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1(config)#ipv6 route ::/0 s0/0/0 %Invalid interface type and number R1(config)#

Nota: Todabiía no se a configurado G0/1
Fuente: Autor

Figura 9. Configuración direccionamiento R1



Fuente: Autor

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

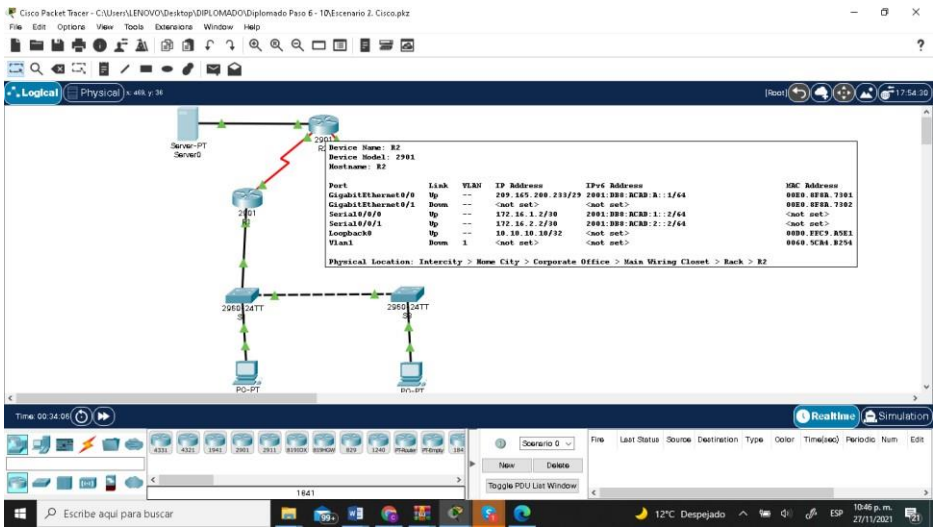
Tabla 9 Configuración R2

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
Nombre del router R2	Router(config)#hostname R2 R2(config)#
Contraseña de exec privilegiado cifrada class	R2(config)# R2(config)#enable secret class
Contraseña de acceso a la consola cisco	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet cisco	R2(config-line)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
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 R2(config)#int R2(config)#interface ser R2(config)#interface serial 0/0/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
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 R2(config-if)#interface serial 0/0/1 R2(config-if)#description Connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 This command applies only to DCE interfaces R2(config-if)#no shutdown
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 R2(config-if)#interface g0/0

	R2(config-if)#description Connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown 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
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. R2(config-if)#int 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)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulated Web Server R2(config-if)#exit R2(config)#
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Figura 10. Configuracción direccionamiento R2



Fuente: Autor

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10 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
Nombre del router R3	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada class	R3(config)#enable secret class
Contraseña de acceso a la consola cisco	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet cisco	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption

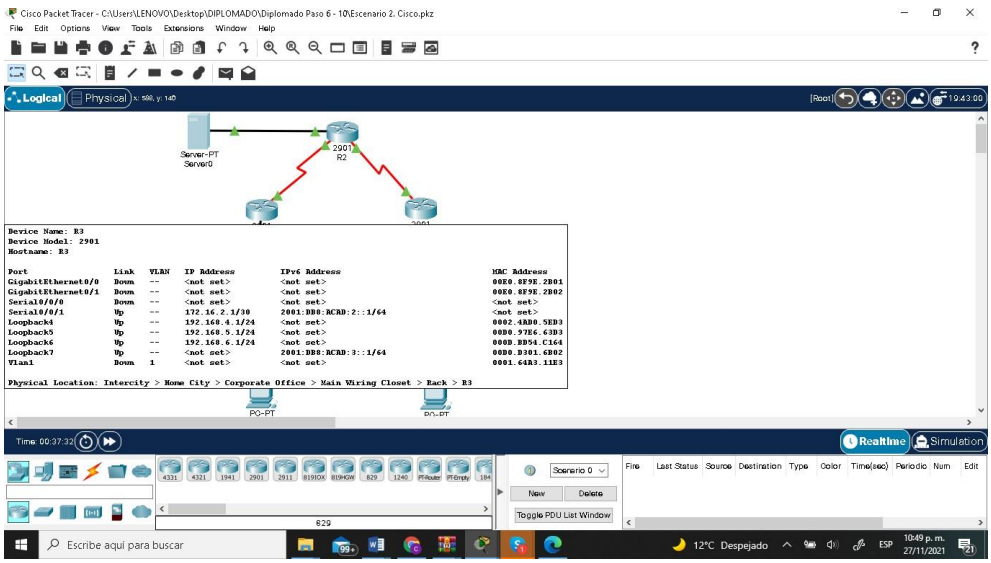
Mensaje MOTD	R3(config)#banner motd %Se prohibe el acceso no autorizado% R3(config)#
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R3(config)#int s0/0/1 R3(config-if)#description Connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown R3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up R3(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up R3(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up R3(config-if)#int 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
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)# R3(config-if)#int 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
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)# R3(config-if)#int 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
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)# R3(config-if)#int 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)#exit R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)# R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 %Default route without gateway, if not a point-to-point interface, may impact performance R3(config)#ipv6 route ::/0 s0/0/1 R3(config)#

Fuente: Autor

Figura 11. Configuración direccionamiento R3



Fuente: Autor

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11 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
Nombre del switch S1	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada class	S1(config)#enable secret class
Contraseña de acceso a la consola cisco	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet cisco	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	S1(config)#banner motd %Se prohibe el acceso no autorizado%

Fuente: Autor

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12 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
Nombre del switch S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada class	S3(config)#enable secret class

Contraseña de acceso a la consola cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet cisco	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	S3(config)#banner motd %Se prohibe el acceso no autorizado% S3(config)#

Fuente: Autor

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 13 Conectividad de Red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

Fuente: Autor

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 14 Configuración del switch, routing y VLAN

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 el gateway 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	
Apagar todos los puertos sin usar	

Fuente: Autor

Desarrollo:

S1>enable

Password:

S1#configure terminal

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)#interface 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)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

S1(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

S1(config-if)#

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#int f0/5

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2

S1(config-if-range)#switchport mode access

S1(config-if-range)#int f0/6

S1(config-if)#switchport access vlan 21

S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2

S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

S1(config-if-range)#

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15 Configuración 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 nombre a 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 de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	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	
Apagar todos los puertos sin usar	

Fuente: Autor

Desarrollo:

S3>enable

Password:

S3#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

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)#int 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 addrress 192.168.99.3 255.255.255.0

^

% Invalid input detected at '^' marker.

S3(config-if)#ip address 192.168.99.3 255.255.255.0

S3(config-if)#no shutdown

S3(config-if)#exit

S3(config)#ip default-gateway 192.168.99.1

S3(config)#int f0/3

S3(config-if)#S1(config-if)#switchport trunk native vlan 1

S3(config-if)#switchport mode trunk

S3(config-if)#switchport trunk native vlan 1

S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2

S3(config-if-range)#switchport mode Access

S3(config-if-range)#int f0/18

S3(config-if)#switchport access vlan 23

S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2

S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

S3(config-if-range)#

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16 Configuración 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: Autor

Desarrollo:

Se prohibe el acceso no autorizado

User Access Verification

Password:

R1>enable

Password:

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

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)#int 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)#int g0/1.99

R1(config-subif)#description LAN de 45suario45o n45on

R1(config-subif)#encapsulation dot1q 99

R1(config-subif)#ip address 192.168.99.1 255.255.255.0

R1(config-subif)#int g0/1

R1(config-if)#no shutdown

R1(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.21, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.23, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.99, changed state to up

R1(config-if)#

Paso 4: Verificar la conectividad de la red

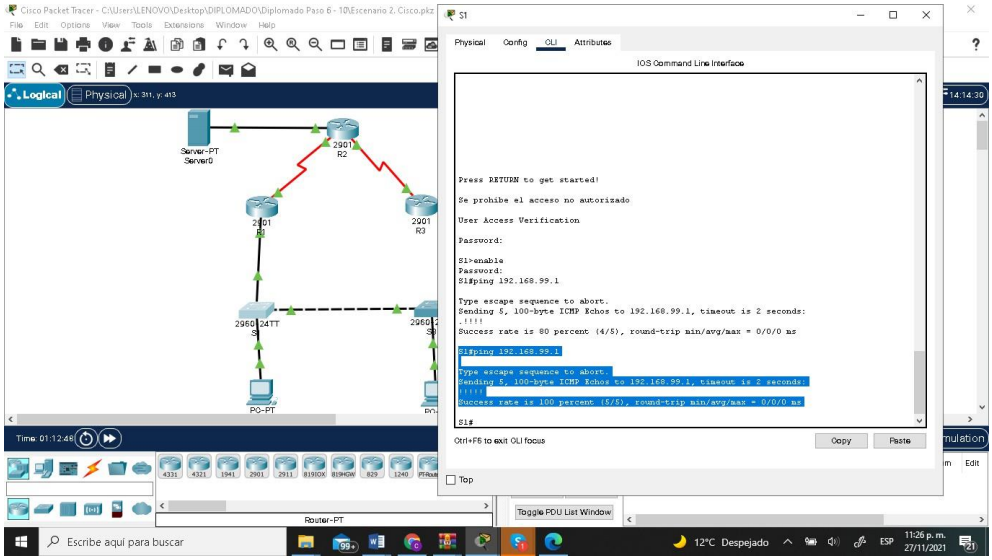
Utilice el comando ping para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17 Verificación de conectividad de la Red

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

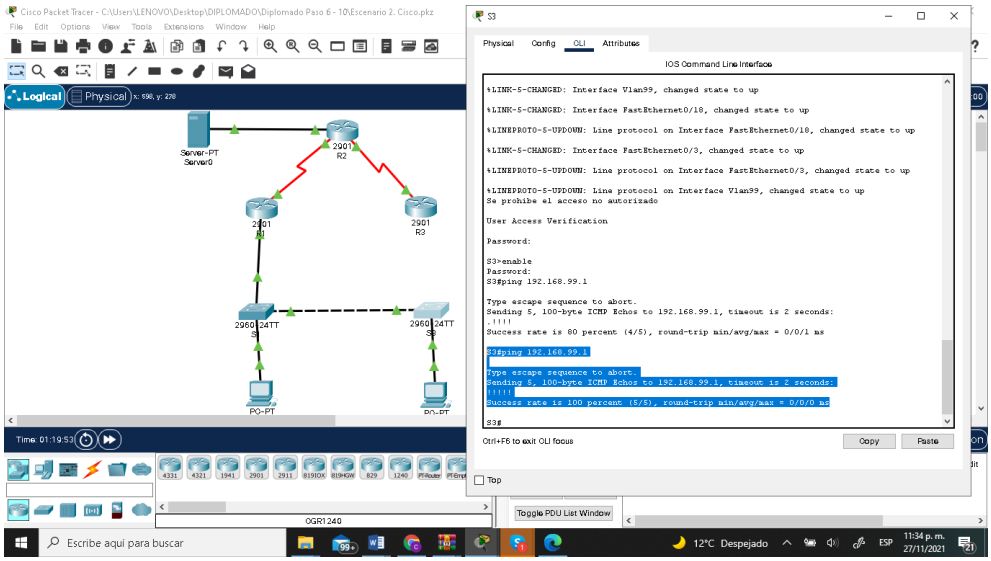
Fuente: Autor

Figura 12. ping de S1 a dirección VLAN 99 IP 192.168.99.1



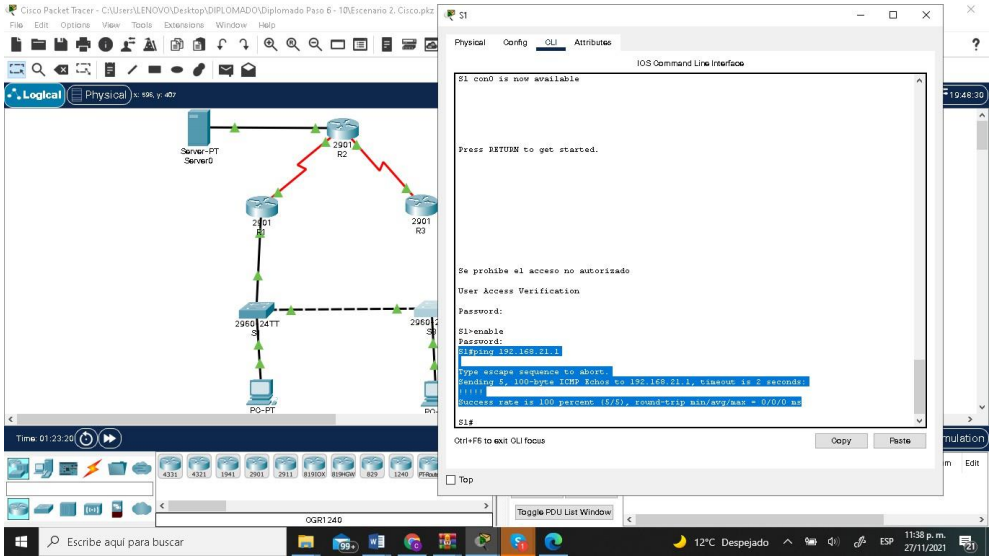
Fuente: Autor

Figura 13. ping de S3 a dirección VLAN 99 IP 192.168.99.1



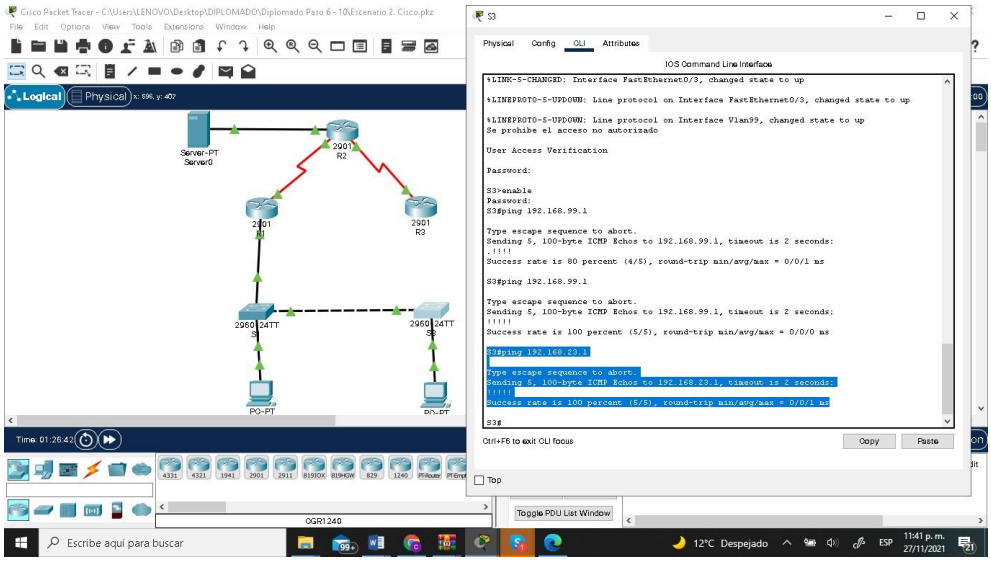
Fuente: Autor

Figura 14. ping de S1 a VLAN 21 IP 192.168.21.1



Fuente: Autor

Figura 15. ping de S3 a VLAN 23 IP 192.168.23.1



Fuente: Autor

Desarrollo:

Password:

S1>enable
Password:
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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S1#

Password:

S3>enable

Password:

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 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms

S3#

Password:

S1>enable

Password:

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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

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

S1#

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 = 0/1/5 ms

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 = 0/0/1 ms

S3#

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 18 Configuración prodocolo routing dinamico OSPF

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: Autor

Desarrollo:

Se prohibe el acceso no autorizado

User Access Verification

Password:

R1>enable

Password:

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#router ospf 1

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

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)#

03:33:39: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/0 from LOADING to FULL, Loading Done

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19 Configuración de OSPF en 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: Autor

Desarrollo:

Se prohibe el acceso no autorizado

User Access Verification

Password:

R2>enable

Password:

R2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#router ospf 1

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)#network 172

03:33:39: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0 from LOADING to FULL, Loading Done

^

% Invalid input detected at '^' marker.

R2(config-router)#network 172.16.2.0 0.0.0.3 area 0

R2(config-router)#passive-interface loopback 0

R2(config-router)#

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 20 Configuración de OSPFv3 en R3

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: Autor

Desarrollo:

Se prohibe el acceso no autorizado

User Access Verification

Password:

R3>enable

Password:

R3#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#router ospf 1

R3(config-router)#network 172.16.2.0 0.0.0.3 area 0

R3(config-router)#

03:39:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/1 from LOADING to FULL, Loading Done

R3(config-router)#network 192.168.4.0 0.0.0.255 area 0

R3(config-router)#network 192.168.5.0 0.0.0.255 area 0

R3(config-router)#network 192.168.6.0 0.0.0.255 area 0

R3(config-router)#passive-interface loopback 4

R3(config-router)#passive-interface loopback 5

R3(config-router)#passive-interface loopback 6

R3(config-router)#

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 del protocolo OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Sh ip protocols
¿Qué comando muestra solo las rutas OSPF?	Sh ip route
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Sh run begin | ospf

Fuente: Autor

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 Implementación DHCP y NAT para IPv4

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
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: Autor

Desarrollo:

Se prohibe el acceso no autorizado

User Access Verification

Password:

R1>enable

Password:

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

R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

R1(config)#ip dhcp pool ACCT

R1(dhcp-config)#network 192.168.21.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.21.1

R1(dhcp-config)#dns-server 10.10.10.10

R1(dhcp-config)#ip domain-name ccna-sa.com

R1(config)#ip dhcp pool ENGNR

R1(dhcp-config)#network 192.168.23.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.23.1

R1(dhcp-config)#dns-server 10.10.10.10

R1(dhcp-config)#ip domain-name ccna-sa.com

R1(config)#

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23 Configuración de NAR estatica 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	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	

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	

Fuente: Autor

Desarrollo:

User Access Verification

Password:

R2>enable

Password:

R2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#username webuser privilege 15 secret cisco12345

R2(config)#ip http server

^

% Invalid input detected at '^' marker.

R2(config)#ip http authentication local

^

% Invalid input detected at '^' marker.

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237

R2(config)#int g0/0

R2(config-if)#ip natoutside

^

% Invalid input detected at '^' marker.

R2(config-if)#int s0/0/0

R2(config-if)#ipnat inside

^

% Invalid input detected at '^' marker.

R2(config-if)#ip nat inside

R2(config-if)#int s0/0/1

R2(config-if)#ip nat inside

R2(config-if)#exit

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255

R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255

R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 net mask 255.255.255.28

^

% Invalid input detected at '^' marker.

R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.28

%Pool INTERNET mask 255.255.255.28 too small; should be at least 255.255.255.252

%Start and end addresses on different subnets

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 pings se realicen correctamente.

Tabla 24 Protocolo DHCP Y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	

Fuente: Autor

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.
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 hora NTP.	

Verifique la configuración de NTP en R1.

Fuente: Autor

Desarrollo:

User Access Verification

Password:

R2>enable

Password:

R2#clock set 00:40:

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

04:27:32: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

04:27:32: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.6.1 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

% Incomplete command.

R2#

04:27:42: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.6.1 on Serial0/0/1 from LOADING to FULL, Loading Done

04:27:42: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0 from LOADING to FULL, Loading Done

R2#clock set 12:00:00 22 November 2021

R2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#ntp master 5

R2(config)#

Password:

R1>enable

Password:

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)#exit

R1#

%SYS-5-CONFIG_I: Configured from console by console

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 77 2.00 906535876070.00 0.12

** sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured*

R1#

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

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

Tabla 26 Configuración (ACL)

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	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Fuente: Autor

Desarrollo:

R2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#ntp master 5

R2(config)#

R2(config)#ip access-list standard ADMIN-MGT

R2(config-std-nacl)#permit host 172.16.1.1

R2(config-std-nacl)#exit

R2(config)#line vty 0 15

R2(config-line)#access-class ADMIN-MGT in

R2(config-line)#transport input telnet

R2(config-line)#

R2(config-line)#exit

R2(config)#exit

R2#

%SYS-5-CONFIG_I: Configured from console by console

R1#

R1#telnet 172.16.1.2

Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado

User Access Verification

Password:

% Password: timeout expired!

[Connection to 172.16.1.2 closed by foreign host]

R1#

User Access Verification

Password:

R3>enable
Password:
R3#172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#

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

Tabla 27 Comando CLI

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

Fuente: Autor

Desarrollo:

R2#show access-list

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 (2 match(es))

R2#

R2#show ip interface

GigabitEthernet0/0 is up, line protocol is up (connected)

Internet address is 209.165.200.233/29

Broadcast address is 255.255.255.255

Address determined by setup command

MTU is 1500 bytes

Helper address is not set

Directed broadcast forwarding is disabled

Outgoing access list is not set

Inbound access list is not set

Proxy ARP is enabled

Security level is default

Split horizon is enabled

ICMP redirects are always sent

ICMP unreachables are always sent

ICMP mask replies are never sent

IP fast switching is disabled

IP fast switching on the same interface is disabled

IP Flow switching is disabled

IP Fast switching turbo vector

IP multicast fast switching is disabled

IP multicast distributed fast switching is disabled

Router Discovery is disabled

IP output packet accounting is disabled

IP access violation accounting is disabled

TCP/IP header compression is disabled

RTP/IP header compression is disabled

Probe proxy name replies are disabled

Policy routing is disabled

Network address translation is disabled

BGP Policy Mapping is disabled

Input features: MCI Check

WCCP Redirect outbound is disabled

WCCP Redirect inbound is disabled

WCCP Redirect exclude is disabled

GigabitEthernet0/1 is administratively down, line protocol is down (disabled)

Internet protocol processing disabled

Serial0/0/0 is up, line protocol is up (connected)

Internet address is 172.16.1.2/30

Broadcast address is 255.255.255.255

Address determined by setup command

MTU is 1500

Helper address is not set

Directed broadcast forwarding is disabled

Outgoing access list is not set

Inbound access list is not set

Proxy ARP is enabled

Security level is default

Split horizon is enabled

ICMP redirects are always sent

ICMP unreachables are always sent

ICMP mask replies are never sent

IP fast switching is disabled

IP fast switching on the same interface is disabled

IP Flow switching is disabled

IP Fast switching turbo vector

IP multicast fast switching is disabled

IP multicast distributed fast switching is disabled

Router Discovery is disabled

IP output packet accounting is disabled

IP access violation accounting is disabled

TCP/IP header compression is disabled

RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Serial0/0/1 is up, line protocol is up (connected)
Internet address is 172.16.2.2/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled

IP access violation accounting is disabled

TCP/IP header compression is disabled

RTP/IP header compression is disabled

Probe proxy name replies are disabled

Policy routing is disabled

Network address translation is disabled

WCCP Redirect outbound is disabled

WCCP Redirect exclude is disabled

BGP Policy Mapping is disabled

Loopback0 is up, line protocol is up (connected)

Internet address is 10.10.10.10/32

Broadcast address is 255.255.255.255

Address determined by setup command

MTU is 1514bytes

Helper address is not set

Directed broadcast forwarding is disabled

Outgoing access list is not set

Inbound access list is not set

Proxy ARP is enabled

Security level is default

Split horizon is enabled

ICMP redirects are always sent

ICMP unreachables are always sent

ICMP mask replies are never sent

IP fast switching is disabled

IP fast switching on the same interface is disabled

IP Flow switching is disabled

IP Fast switching turbo vector

IP multicast fast switching is disabled

IP multicast distributed fast switching is disabled

Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
Vlan1 is administratively down, line protocol is down
Internet protocol processing disabled

R2#

CONCLUSIONES

Se logra concluir que la herramienta CCNA – Cisco, nos proporciona una adecuada forma de trabajo virtual para el desarrollo de habilidades y adquisición de destreza para dar soluciones a los problemas cotidianos reales.

Se adquieren habilidades con el desarrollo del primer escenario que consiste en la configuración de una red doméstica pequeña con un router, un switch y dos pc, realizando las configuraciones y las tareas solicitadas abordando temas de protocolo, mecanismos de acceso al medio y características de la capa de red, capa de transporte, asignación de direcciones IP.

Con la culminanación de la actividad del segundo escenario se logra identificar fallas de conexión en la configuración y su respectivo arreglo, asi como el manejo de protocolos necesarios para el trabajo en un ambiente de redes y soluciones integralesde los requerimientos del cliente.

Gran satisfacción de haber logrado realizar el desarrollo de la actividad con muchos obstáculos y situaciones pero que a lo largo he podido dar solución.

BIBLIOGRÁFIA

Bareño Gutierrez, R. (2021, 10 noviembre). web u8-10 diplomado. Web U8-10 Diplomado de profundización. https://drive.google.com/drive/u/0/my-drive

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

C. (2019). *Principios de Enrutamiento y Conmutación.* NAT para IPv4. https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

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

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

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

CISCO. (2019). Capa de aplicación. Fundamentos de Networking.

Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

CISCO, (2020). Networking Academy. “Packet Tracer: Configuración de los parámetros iniciales del switch”. Recuperado de: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2.2.3.3).

CISCO, (2020). Networking Academy. “Packet Tracer: Situación de división en subredes 1”. Recuperado de: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.1.4.6).

CISCO, (2020). Networking Academy. “Packet Tracer: Situación de división en subredes 2”. Recuperado de: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.1.4.7).

CISCO, (2020). Networking Academy. “Práctica de laboratorio: configuración de redes VLAN y enlaces troncales”. Recuperado de: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3.2.2.5).

CISCO, (2020). Networking Academy. “Práctica de laboratorio: implementación de seguridad de VLAN”. Recuperado de: (https://static-course- assets.s3.amazonaws.com/ITN6/es/index.html#3.3.2.2).

CISCO, (2020). Networking Academy. “Práctica de laboratorio: configuración deNAT dinámica y estática”. Recuperado de: (https://static-course- assets.s3.amazonaws.com/ITN6/es/index.html#11.2.2.6).

CISCO, (2020) Networking Academy. “Práctica de laboratorio: configuración de unconjunto de NAT con sobrecarga y PAT”. Recuperado de: (https://static-

courseassets.s3.amazonaws.com/ITN6/es/index.html#11.2.3.7).

CISCO, (2020) Networking Academy. “Packet Tracer: Configure IP ACLs toMitigate

Attacks”. Recuperado de: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4.4.1.2).

CISCO, (2020). Networking Academy. “Packet Tracer: Configuring Standard ACLs”. Recuperado de: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.2.1.10).

CISCO, (2020). Networking Academy. “Packet Tracer: Configuring Named Standard ACLs”. Recuperado de: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.2.1.11).

CISCO, (2020). Networking Academy. “Packet Tracer: Configuring an ACL on VTY Lines”. Recuperado de: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.2.3.3).

Guaca, N. A. (2021). *CIPA unidad 1 (2021–09-10 at 16:00 GMT-7)*. Google Drive.https://drive.google.com/file/d/11OLunv509ocZjQNrzWDuqcRch_TmMdCr/view?usp=sharing

Guaca, N. A. (2021). *CIPAS Subneting_DIPLOMADO (2021–10-06 at 18:02 GMT-7)*. Google Drive. https://drive.google.com/file/d/1CmNJEoygio-FsfLe7AG55MbMCFRR27ip/view?usp=sharing

Guaca, N. A. (2021). *Web U1-2 Diplomado (2021–09-16 at 16:00 GMT-7)*. Google Drive. https://drive.google.com/file/d/129yYqLK46kY-2odBcd3tBbbxpri_pdfV/view?usp=sharing

Guaca, N. A. (2021). *Web U3-5 Diplomado (2021–10-05 at 16:01 GMT-7)*. Google Drive. https://drive.google.com/file/d/1rXEGtp-L_8sOTORuQ9aLrSK7w5zcpEGe/view?usp=sharing