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

ROBERTO CARLOS SIABATTO GARCIA

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

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

ROBERTO CARLOS SIABATTO GARCIA

Diplomado de opción de grado presentado para optar el título

de ingeniero de sistemas

PRESENTADO A:
MAGISTER MARIA ALEJANDRA LOPEZ HURTADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
VILLAVICENCIO - META
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Villavicencio, 26 de noviembre de 2021

AGRADECIMIENTOS

A mi esposa que con esfuerzo me anima a seguir adelante, mis hijos Alejandro y paula Daniela que son mi combustible, mis padres por sus oraciones, amigos que me apoyaron.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

ÍNDICE DE TABLAS

GLOSARIO

ACL Access Control List (en castellano, Una Lista de Control de Accesos) es una serie de instrucciones que controlan que en un router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de los mismos.

BROADCAST: broadcast significa “transmisión o radiodifusión” es un mensaje que se transmite a todos los miembros de una red y que no necesita ninguna acción de retroalimentación. Un equipo conectado a la red envía un paquete de datos al resto de participantes de la red al mismo tiempo. En este proceso, el emisor no especifica ninguna dirección de destino, lo que distingue el broadcast del llamado unicast, en que el paquete solo se envía a un único destino conocido.

CONMUTACIÓN: La conmutación de paquetes trata de combinar las ventajas de las conmutaciones de mensajes y circuitos, minimizando las desventajas de ambas. Es una técnica similar a la de mensajes, con la diferencia de que la longitud de las unidades de información (paquetes) está limitada, en tanto que en la conmutación de mensajes la longitud de estos es mucho mayor**.**

ENLACE TRONCAL: es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. Más adelante en esta sección, aprenderá acerca de 802.1Q.

IEEE 802.1Q: también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking).

LÍNEA VTY: son las líneas de terminal virtual del router, que se utilizan solamente para controlar las conexiones Telnet entrantes. Son virtuales en el sentido que son una función de software; no hay hardware

NAT o Network Address Translation (en castellano, Traducción de Direcciones de Red) se refiere a un proceso específico que implica la reordenación de una única dirección IP en otra dirección IP, a menudo pública, mediante la alteración de la información de red y la información de dirección que se encuentra en la cabecera IP de los paquetes de datos

NETWORKING: relaciona redes de cómputo para vincular dos o más dispositivos informáticos con el propósito de compartir datos. Las redes están construidas con

una mezcla de hardware y software, incluyendo el cableado necesario para conectar los equipos.

OSPF (Open Shortest Path First ó en español, El Camino Más Corto Primero) es un protocolo de enrutamiento dinámico interior (IGP – Internal Gateway Protocol -). Usa un algoritmo de tipo Estado de Enlace. Organiza la información de la tipología de red utilizando lo que se llaman LSA y la base de datos de estado de enlace (LSDB).

SUBNETTING: consiste en dividir una red grande en varias subredes más pequeñas, esto se debe realizar con mucho cuidado y planificación para no desaprovechar direcciones IPv4.

VLAN Acerca de Redes Virtuales de Área Local Las VLAN permiten dividir la red en grupos con una agrupación o estructura jerárquica lógica en lugar de una física. Esto ayuda a liberar al personal de TI de las restricciones del diseño de red y la infraestructura de cableado existente. Las VLAN facilitan el diseño, la implementación y la administración de la red.

VLSM (Máscaras de longitud variable): Se toma una red y se divide en subredes fijas, luego se toma una de esas subredes y se vuelve a dividir en otras subredes tomando más bits del identificador de máquina, ajustándose a la cantidad de equipos requeridos por cada segmento de la red permitiendo tener una organización del espacio de direcciones más acorde con las necesidades reales, sin desaprovechar direcciones IP.

.

RESUMEN

El presente informe tiene como propósito evidenciar la aplicación de conceptos adquiridos en Networking en tecnología, mediante la elaboración paso a paso de dos (2) escenarios. En el primer escenario se busca diseñar y configurar una red pequeña compuesta por un ISR 4331 y un switch 2960-24TT, diseñar el esquema de direccionamiento IPv4, y poner en práctica la distribución de quipos en dos subredes realizando el subnetting con la dirección de red 192.168.33.0 que cumpla con el requerimiento establecidos en la prueba.

En el segundo escenario se busca realizar la configuración de una red que permite la conectividad IPv4 e IPv6, seguridad de switches 3560-24PS, routing 1941, implementado los protocolos DHCP, OSPF, NTP y una lista de control de acceso (ACL).

Cumpliendo con la intención de la guía, la configuración y verificación de cada uno de los dispositivos, se registran de manera detallada tanto el uso de los comandos y el manejo de la herramienta Packet Tracer que demuestren las habilidades adquiridas en los laboratorios.

PALABRAS CLAVES: Direcciones IPv4, subnetting, topología, networking Enrutamiento; Etherchannel; Ipv6; Nat; Ntp; Ospf; Troncal.

ABSTRACT

The purpose of this report is to show the application of concepts acquired in Networking in technology, through the step-by-step development of two (2) scenarios. The first scenario seeks to design and configure a small network made up of a 4331 ISR and a 2960-24TT switch, design the IPv4 addressing scheme, and implement the distribution of equipment in two subnets by subnetting with the network address. 192.168.33.0 that meets the requirement established in the test.

The second scenario seeks to configure a network that allows IPv4 and IPv6 connectivity, 3560-24PS switch security, 1941 routing, implementing the DHCP, OSPF, NTP protocols and an access control lists (ACL).
Complying with the intention of the guide, the configuration and verification of each of the devices, both the use of the commands and the handling of the Packet Tracer tool are recorded in detail, demonstrating the skills acquired in the laboratories.

Complying with the intention of the guide, the configuration and verification of each of the devices, both the use of the commands and the handling of the Packet Tracer tool are recorded in detail, demonstrating the skills acquired in the laboratories.

KEY WORDS: IPv4 addresses, subnetting, topology, networking Routing; Etherchannel; Ipv6; Nat; Ntp; Ospf; Trunk.

INTRODUCCIÓN

Descubrir la magia que ocurre en la red es algo que a muchos nos lleva a pensar que las distancias van desapareciendo en la medida que internet llega a lugares insospechados, todo hacer parte de la evolución que no se detiene. A través de Cisco permite comprender en este primer nivel una visión general, para ir comprendiendo la interconexión las redes de muchos tamaños hasta logran una gran red, en la que los dispositivos, medios y servicios proporcionan toda la funcionalidad en la comunicación que vale la pena aprender.

El presente trabajo se propone contextualizar en la práctica los conocimientos adquiridos en el transcurso desarrollos los distintos escenarios en el Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas LAN WAN. En donde se platea simular el funcionamiento de la red configurando los dispositivos según requerimientos solicitados en la guía del escenario 1.

La construcción de la red acorde a la topología indicada permite aplicar el esquema de direccionamiento IPv4 en las dos sub redes con la cantidad de host especificados aplicando la técnica de subnetting VLSM configuración de mascara de longitud variable permitiendo tener una organización del espacio de direcciones más acorde con las necesidades reales, sin desaprovechar direcciones IP.

En desarrollo del segundo escenario fue importante el análisis de la topología propuesta, en la cual convergen una serie de protocolos que permitieran la conectividad, realizado la simulación en herramienta Packet Tracer determinando cada una de las configuraciones en los equipos intermedios y finales para en al final el objetivo en el funcionamiento exitoso, se manejaron los aspectos importantes en la implementación de la seguridad en los dispositivos que es relevante para garantizar que no sean vulnerados, la asignación de direcciones IP dinámicas y estáticas, entre otras actividades que corresponden a un aplicación normal de producción de redes.

DESARROLLO

Escenario 1

Ilustración 1 Topología Propuesta escenario 1

Figura 1: Topología scenario 1

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.

Aspectos Básicos/Situación

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

1. Se inicia con la selección del equipo de escritorio agregándolo a la topología y se nombra PC-A, y conectado al puerto de red Fa0.
2. Seleccionamos un switch 9260-24TT, los agregamos a la topología y los nombramos S1 respectivamente, se conecta al puerto Fa 0/6, con el PC-A al puerto de red Fa0.
3. Se selecciona una router 4331, se agrega a la topología y lo renombramos como R1, este router soporta direcciones IPv4 e IPv6, además tiene 3 puertos Gigabit Ethernet G0/0/0 a G0/0/2.
4. Por último selecciona otro equipo de escritorio agregándolo a la topología y se nombra PC-B, y conectado al puerto de red Fa0.

Parte1: Construcción la Red

Topología Packet Tracer Escenario 1

Ilustración 2 Topología Packet Tracer

Fuente: Elaboración 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 tabla de direccionamiento.

En el caso del direccionamiento según requerimiento corresponde a 192.168.33.0 por los dos últimos dos dígitos de cédula.

Tabla 1 Direccionamiento

Ítem	Requerimiento
Dirección de Red	192.168.33.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.33.1
R1 G0/0/0	192.168.33.129
S1 SVI	192.168.33.2
PC-A	192.168.33.126
PC-B	192.168.33.190

Ilustración 3 Configuración de mascara variable

VLSM Configuración de mascara variable						
LAN 1 = 100	192,168,33,0	/25= 255,255,255,128	126	192,168,33,1	192,168,33,126	192,168,33,127
LAN 2 = 50	192,168,33,128	/26 = 255,255,255,192	62	192,168,33,129	192,168,33,190	192,168,33,191
direccion de red: 192,168,33,0		11111111	11111111	00100001	00000000	
		11111111	11111111	11111111	10000000	
		255	255	255	128	/25
direccion de red: 192,168,33,0		11111111	11111111	00100001	00000000	
		11111111	11111111	11111111	11000000	
		255	255	255	192	/26

Fuente: Elaboración 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 2 Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	R1Router(config)#hostname R1 R1(config)# R1#
Nombre de dominio	R1#config t R1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1#config t R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login

Establecer la longitud mínima para las	R1(config)#security password min-length 10
Crear un usuario administrativo en la base de	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#ip ssh version 2 *Mar 1 0:40:4.656: %SSH-5-ENABLED: SSH 1.99 has been enabled R1(config)#line vty 0 4 R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]
Configure un MOTD Banner	R1#config t R1(config)#banner motd "Authorized personal only"
Configurar interfaz G0/0/0	R1(config-if)#interface gigabitEthernet 0/0/0 R1(config-if)#ip address 192.168.33.129 255.255.255.192 R1(config-if)#no shutdown

Configurar interfaz G0/0/1	R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#ip address 192.168.33.1 255.255.255.128
Generar una clave de cifrado RSA	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]

Las Tareas De Configuración De S1 Incluyen Lo Siguiente:

Tabla 3 Configuración S1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch	Switch#config t Switch(config)#hostname S1 S1(config)#
Nombre de dominio	S1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secretciscoenpass

Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#crypto key generate rsa The name for the keys will be: S1.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] S1(config)#ip ssh version 2 *Mar 1 4:34:36.334: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config)#line vty 0 4 S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1#copy run star Destination filename [startup-config]? Building configuration... [OK]
Configurar un MOTD Banner	S1(config)#banner motd "Authorized personal only"

Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa The name for the keys will be: S1.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]
Configurar la interfaz de administración (SVI)	S1#configure terminal S1(config)#interface FastEthernet0/24 S1(config-if)#exit S1(config)#interface vlan 1 S1(config-if)#ip address 192.168.33.2 255.255.255.128
Configuración del gateway predeterminado	S1(config-if)#ip default-gateway 192.168.30.0 S1(config)#exit

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.

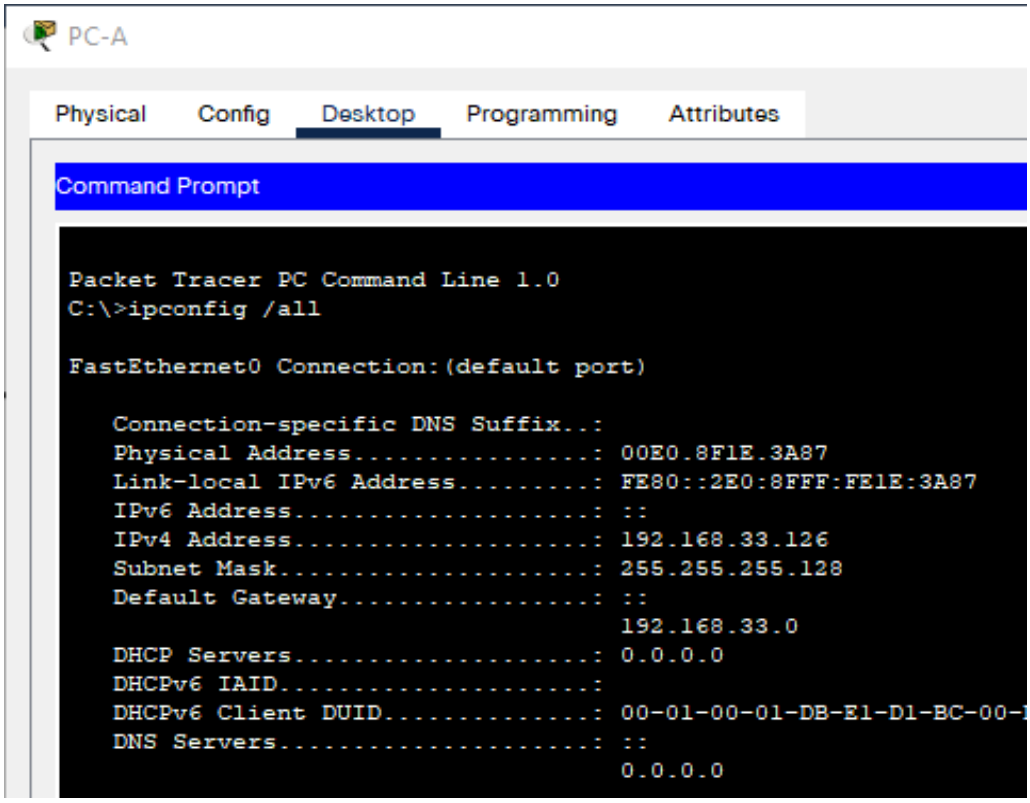
Tabla 4 Configuración PC-A

PC-A Network Configuración	
Descripción	Dirección IPv4
Dirección física	00E0.8F1E.3A87
Dirección IP	192.168.33.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.33.0

Tabla 5 Configuración PC-B

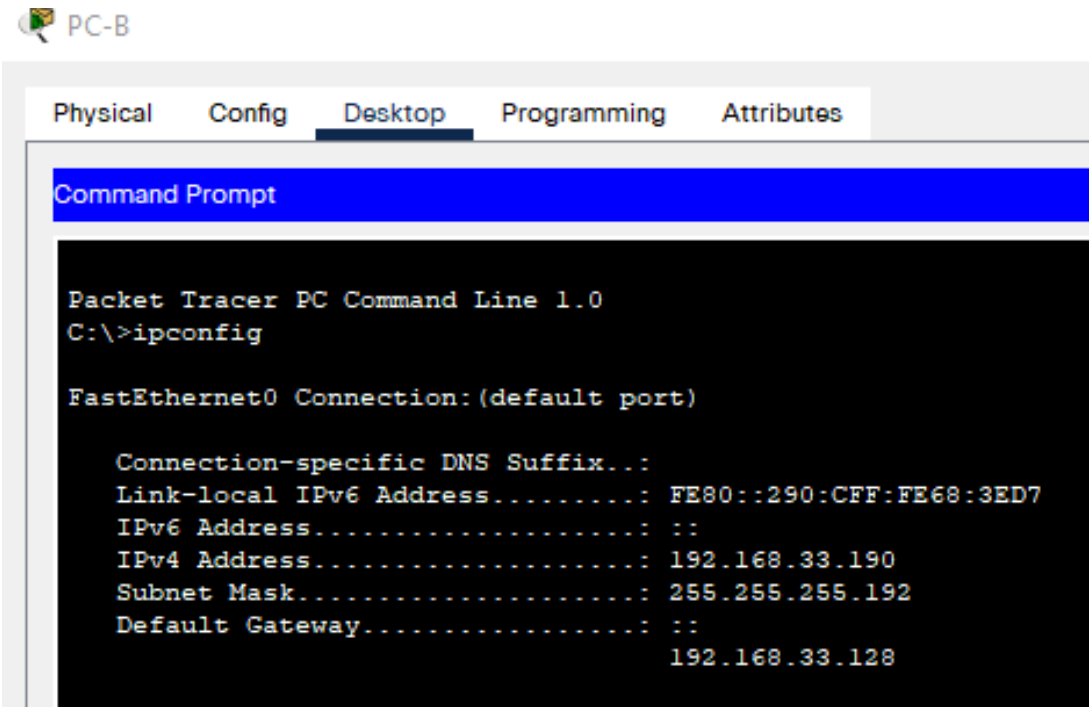
PC-B Network Configuración	
Descripción	Dirección IPv4
Dirección física	0090.0C68.3ED7
Dirección IP	192.168.33.190
Máscara de subred	192.168.33.192
Gateway predeterminado	192.168.33.0

Ilustración 4 Comando ipconfig /all host PC-A y PC-B



Fuente: Elaboración propia

Ilustración 5 ipconfig PC-B



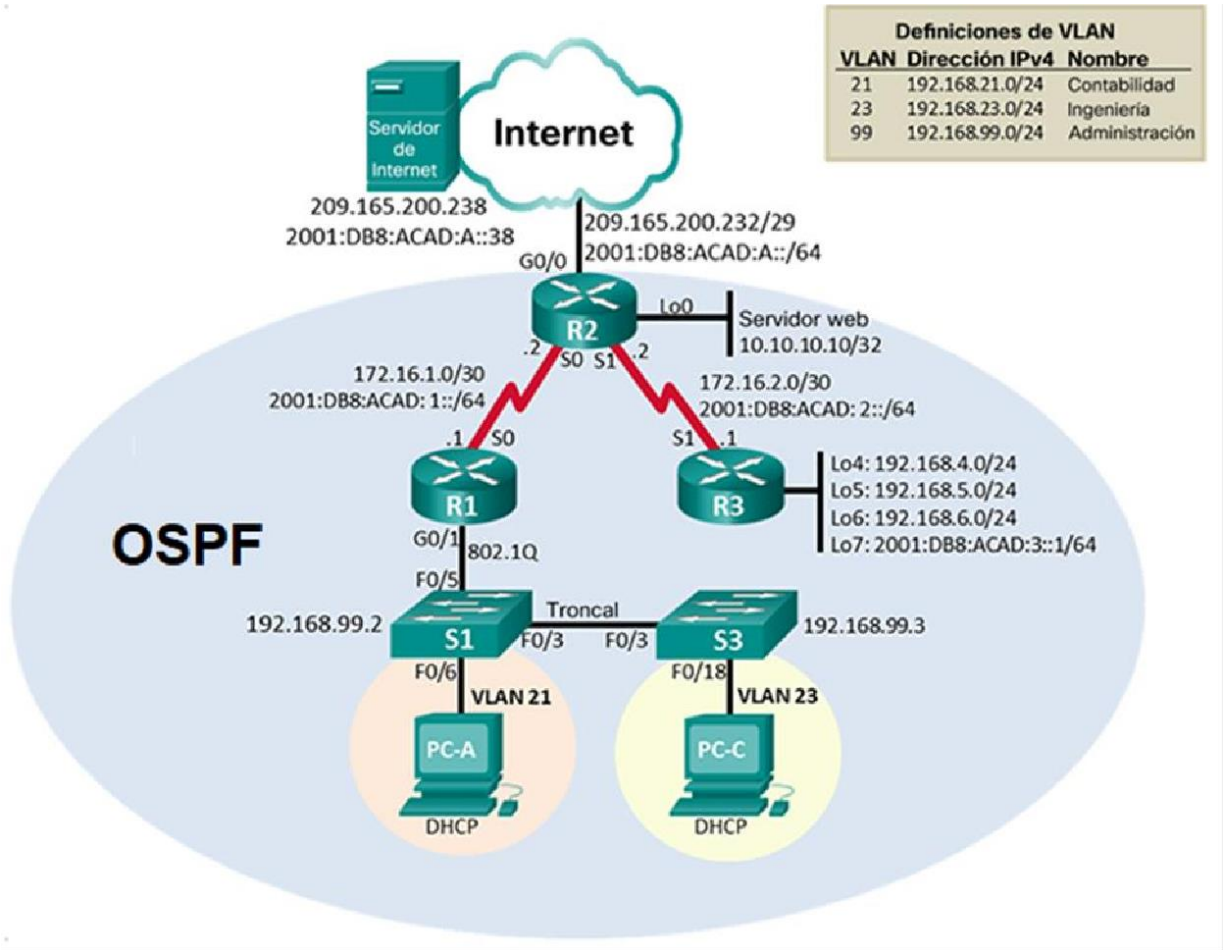
Fuente: Elaboración propia

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.

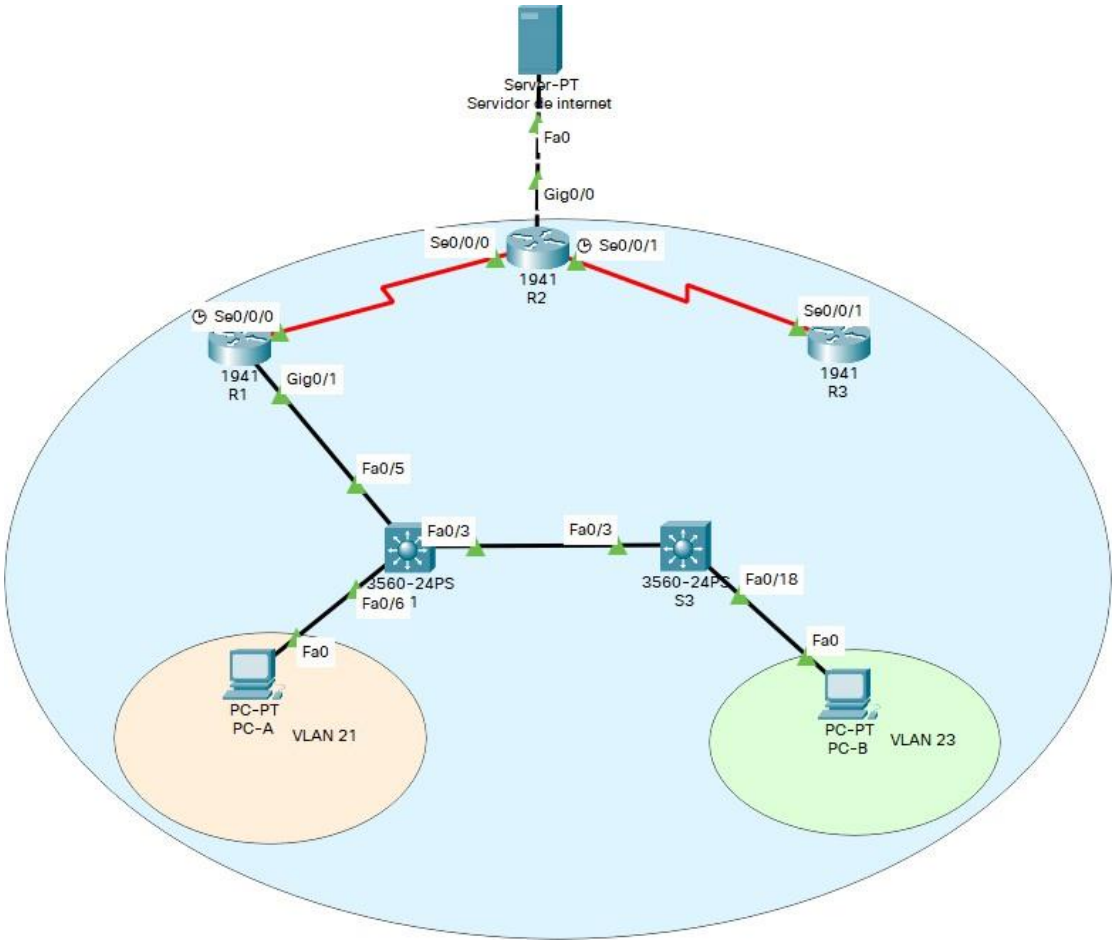
Topología

Ilustración 6 Topología Propuesta escenario 2



Topología Packet Tracer Escenario 2

Ilustración 7 Topología Packet Tracer Escenario 2



Fuente: Elaboración 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 6 Inicializar Router y Switch

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config /Se realiza esta operación en los tres Router/
Volver a cargar todos los routers	Router#reload /Se realiza esta operación en los tres Router/
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#del vlan.dat /Se realiza esta operación en los dos Switch/
Volver a cargar ambos switches	Switch#reload /Se realiza esta operación en los dos Switch/
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash /Vemos la información guardada en la memoria flash/

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 Servidor de internet

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

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8 Configurar R1 básico

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd "Se prohibe el acceso no autorizado”

Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description CONEXION2 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 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	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#copy run start Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9 Configurar R2 básico

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class

Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server /Este commando no funciona en PT por lo tanto no se usará/
Mensaje MOTD	R2(config)#banner motd "Se prohibe el acceso no autorizado”
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description CONEXION1 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 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	R2(config)#interface serial 0/0/1 R2(config-if)#description CONEXION3 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 R2(config-if)#no shutdown 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)	R2(config)#interface g0/0 R2(config-if)#description 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 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)	R2(config)#interface loopback 0 R2(config-if)#description SERVIDORWEB R2(config-if)#ip address 10.10.10.10 255.255.255.255 Establecer la descripción. Establezca la dirección IPv4.

Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 R2(config)#copy run start Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10 Configurar R3 básico

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd "Se prohibe el acceso no autorizado”

Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description CONEXION2 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 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	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#end R3#copy run start Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11 Configuración S1 básico

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd "Se prohibe el acceso no autorizado”

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12: configuración S3 básico

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class

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

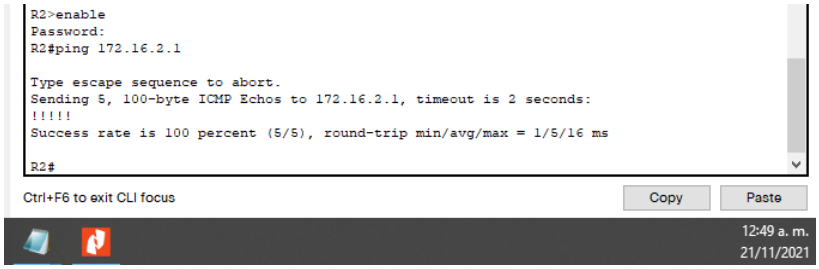
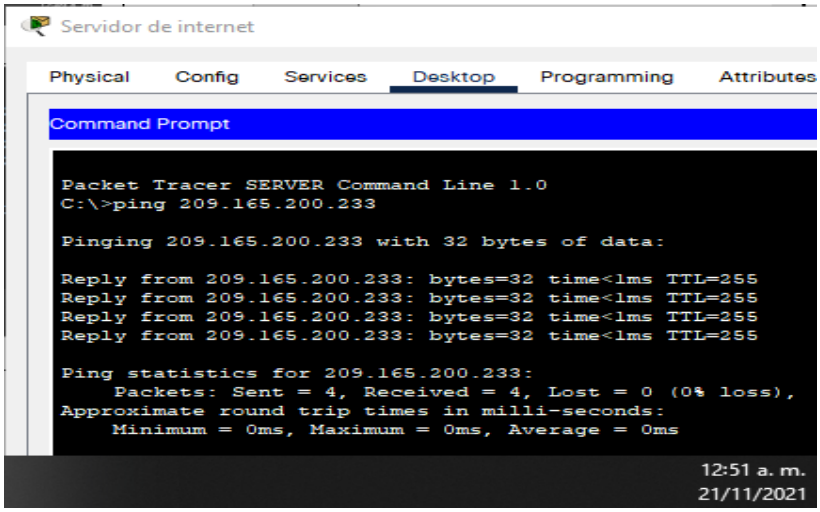
Paso 7: Verificar la conectividad de la red

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 Verificación de conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	*Ilustración 8 Ping de R1 a 172.16.1.2*  *Fuente: Elaboración propia*

R2	R3, S0/0/1	172.16.2.1	*Ilustración 9 Ping de R2 a 172.16.2.1*  *Fuente: Elaboración propia*
PC de Internet	Gateway predeterminado	200.165.200.233	*Ilustración 10 Ping servidor de internet a 200.165.200.233*  *Fuente: Elaboración propia*

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Ilustración 11 configuración de seguridad del switch y las VLAN S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-if)#name CONTABILIDAD S1(config-if)#exit S1(config)#vlan 23 S1(config-if)#name INGENIERIA S1(config-if)#exit S1(config)#vlan 99 S1(config-if)#name ADMINISTRACION S1(config-if)#exit 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.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 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	S1(config-if)#ip default-gateway 192.168.99.1 Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport trunk encapsulation dot1Q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown Utilizar la red VLAN 1 como VLAN nativa

Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1Q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range f0/1-2, f0/4, f0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#no shutdown
Apagar todos los puertos sin usar	S1(config)#interface range f0/1-2, f0/4, f0/7-24 S1(config-if-range)#shutdown S1(config-if-range)#end S1#copy run start

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Ilustración 12 configuración de seguridad del switch y las VLAN S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-if)#name CONTABILIDAD S3(config-if)#exit S3(config)#vlan 23 S3(config-if)#name INGENIERIA S3(config-if)#exit S3(config)#vlan 99 S3(config-if)#name ADMINISTRACION S3(config-if)#exit 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	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 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.	S3(config-if)#ip default-gateway 192.168.99.1 Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport trunk encapsulation dot1Q S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#no shutdown Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range f0/1-2, f0/4-24 S3(config-if-range)#switchport mode access S3(config-if-range)#exit Utilizar el comando interface range
Asignar F0/18 a la VLAN 23	S3(config)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#no shutdown
Apagar todos los puertos sin usar	S3(config)#interface range f0/1-2, f0/4-17, f0/19-24 S3(config-if-range)#shutdown S3(config-if-range)#end S3#copy run start

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

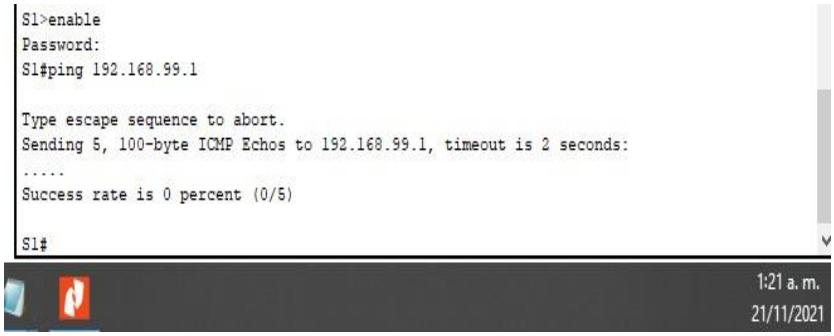
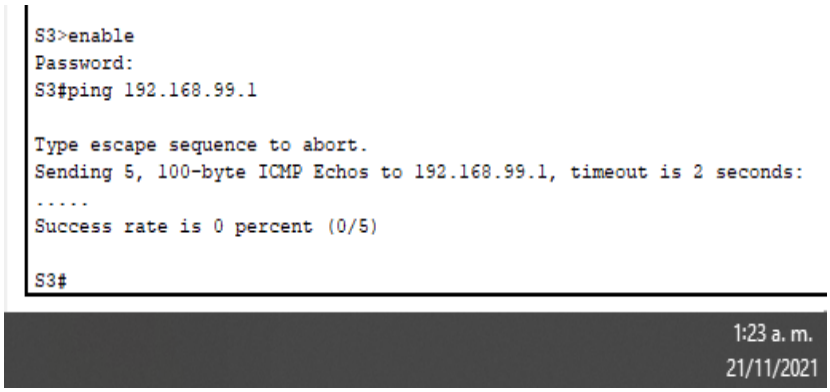
Ilustración 13 configuración de seguridad R1 entre VLAN

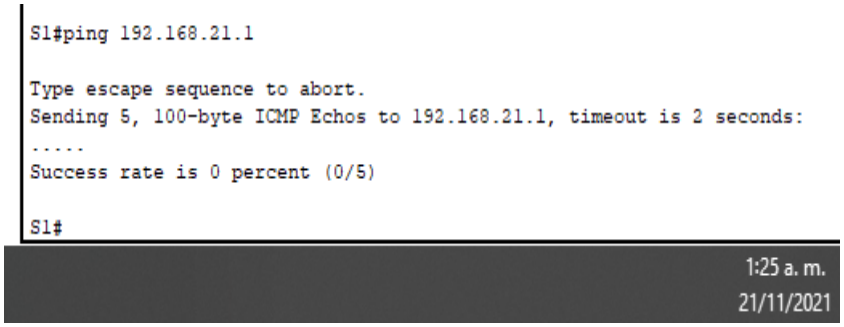
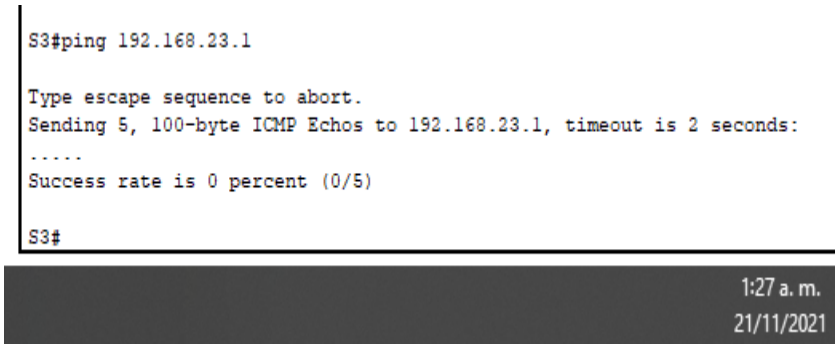
lemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit 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	R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit 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	R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#description LAN de Administración R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown R1(config-if)#end R1#copy run start

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 14 verificación de conectividad

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	*Ilustración 14 Ping de S1 a 192.168.99.1*  *Fuente: Elaboración propia*
S3	R1, dirección VLAN 99	192.168.99.1	*Ilustración 15 Ping de S3 a 192.168.99.1*  *Fuente: Elaboración propia*

S1	R1, dirección VLAN 21	192.168.21.1	*Ilustración 16 Ping de S1 a 192.168.21.1*  *Fuente: Elaboración propia*
S3	R1, dirección VLAN 23	192.168.23.1	*Ilustración 17 Ping de S3 a 192.168.23.1*  *Fuente: Elaboración 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 15 configuración OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1

Anunciar las redes conectadas directamente	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)#network 172.16.1.0 0.0.0.3 area 0 Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface gigabitEthernet 0/1
Desactive la sumarización automática	R1(config-router)#no auto-summary <Debido a que OSPF no sumariza automáticamente, no necesita el comando “no auto-summary”>

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 16 configuración OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 **Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary <Debido a que OSPF no sumariza automáticamente, no necesita el comando “no auto-summary”>

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 17 configuración OSPFv3 en R3

Elemento o tarea de configuración	Especificación
Configurar OSPFv3 área 0	R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 1 R3(config-rtr)#router-id 33.33.33.33 R3(config-rtr)#passive-interface default R3(config-rtr)#no passive-interface s0/0/1 R3(config-rtr)#exit R3(config)#interface s0/0/1 R3(config-if)#ipv6 ospf 1 area 0 R3(config)#interface loopback 7 R3(config-if)#ipv6 ospf 1 area 0 R3(config-if)#exit
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary <Dado que OSPF no sumariza automáticamente, no necesita el comando “no auto-summary>

Paso 4: Verificar la información de OSPF

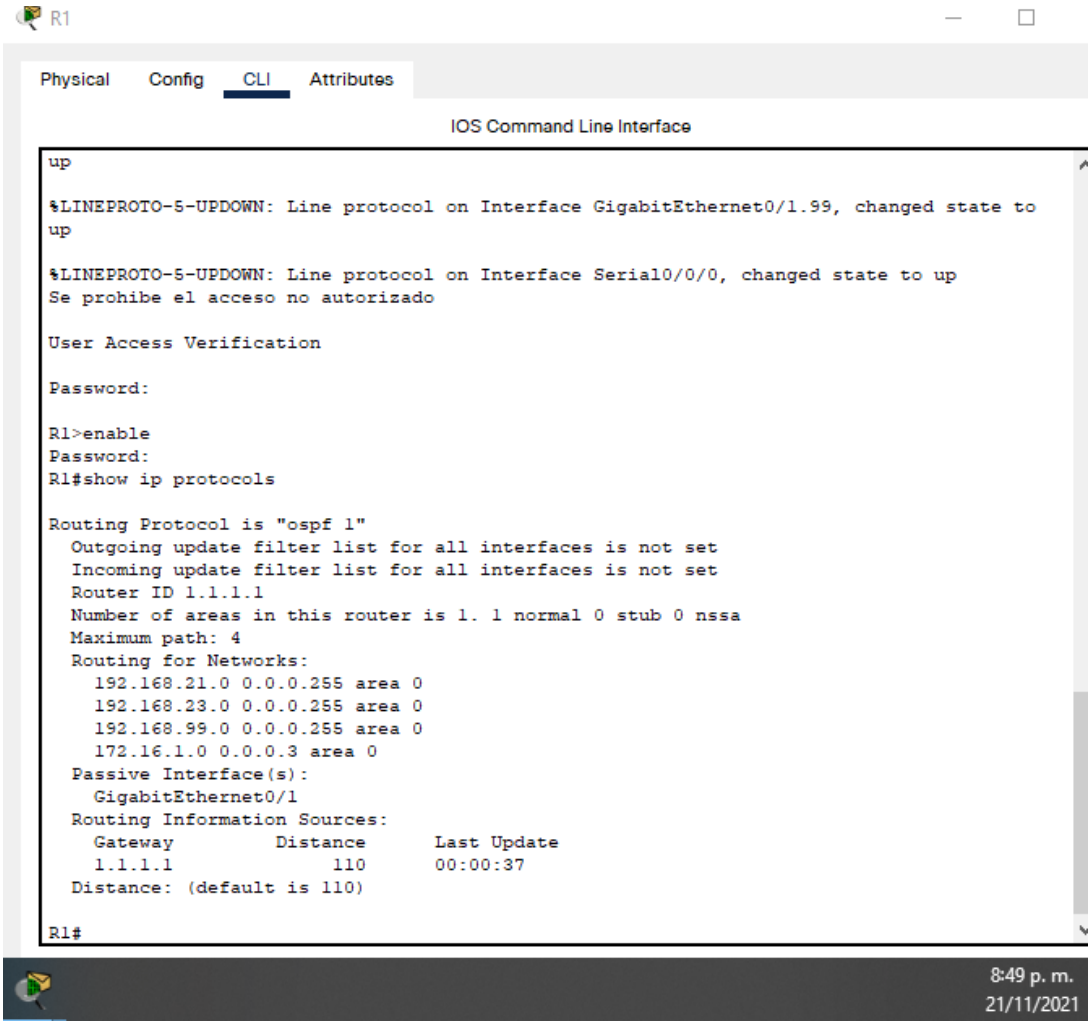
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 18 Verificar de información comandos 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?	show ip protocols show ip ospf interface <Las capturas de imagen de los resultados en la ejecución

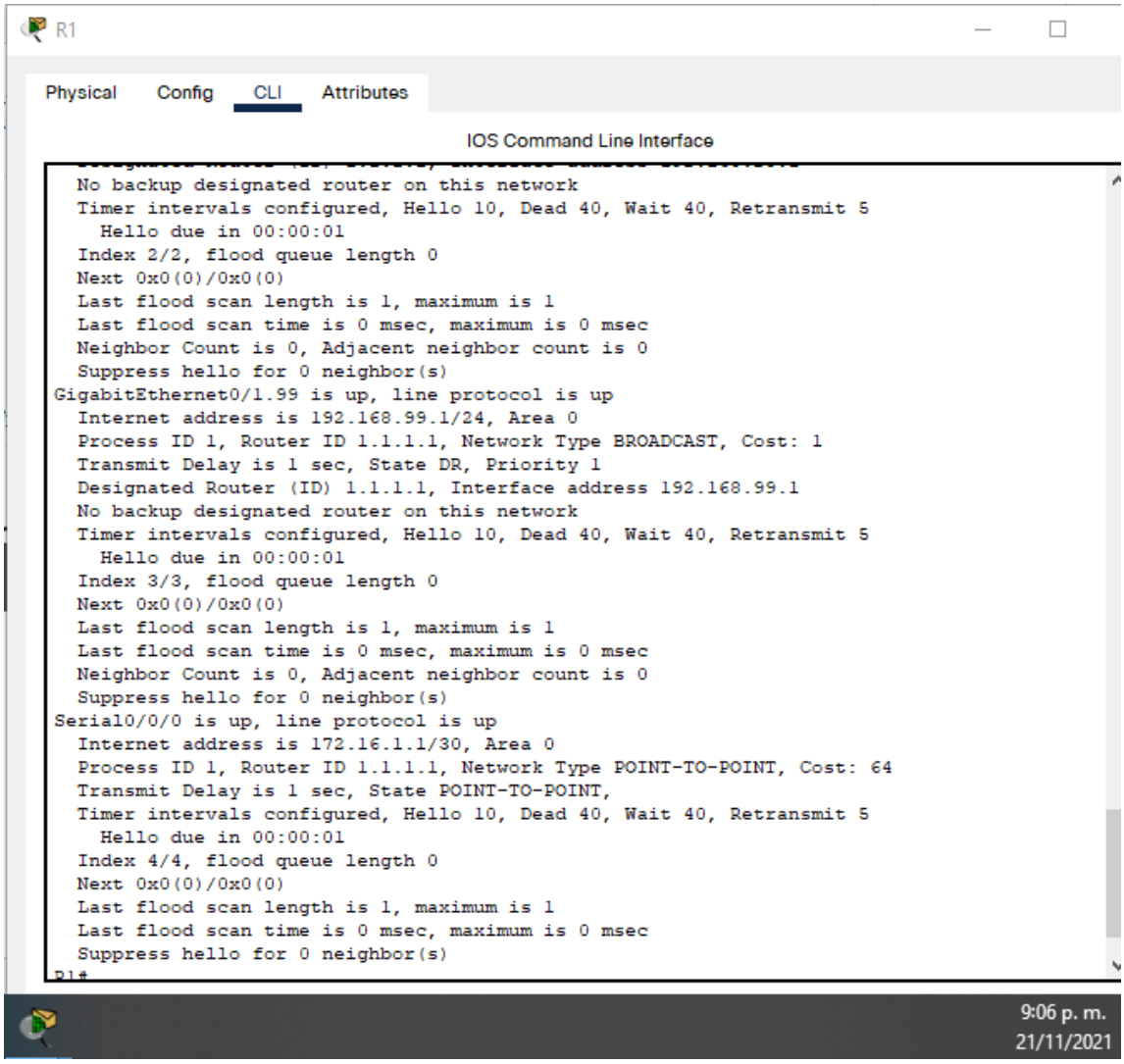
	de los comandos show se encuentran en la ilustración 18 y 19 >
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show run | section ospf <La captura de imagen del resultados en la ejecución de los comandos show se encuentran en la ilustración 20>

Ilustración 18 resultado comando show ip protocols



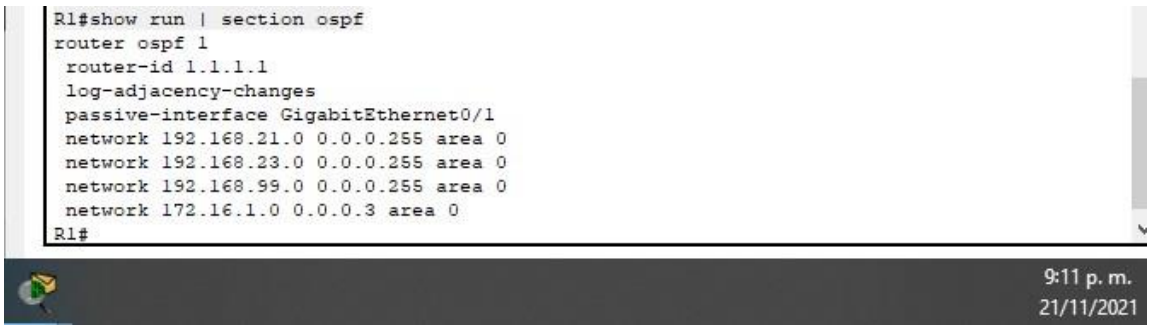
Fuente: Elaboración propia

Ilustración 19 resultado comando show ip ospf interface



Fuente: Elaboración propia

Ilustración 20 show run | section ospf



fuente: Elaboración 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 19 configuración servidor de DHCP para las VLAN 21 y 23 R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(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(config)#domain-name ccna-sa.com 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	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(config)#domain-name ccna-sa.com Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

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

La configuración del R2 incluye las siguientes tareas:

Tabla 20 configuración NAT estática y dinámica R2

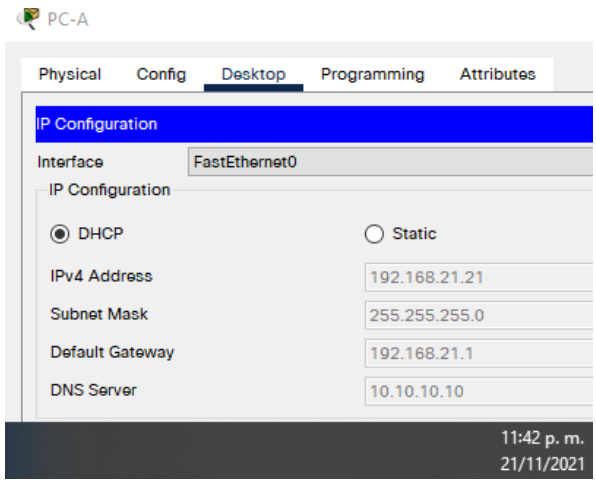
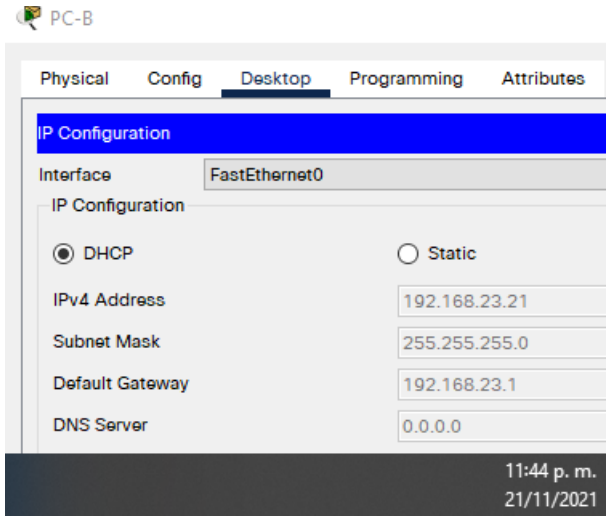
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 password cisco12345 Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	R2(config)#ip http server <la ejecución de este comando presenta fallas en Packet Tracer>
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http secure-server R2(config)#ip http authentication login local <Estos dos comandos presentaron error no funcionan en Packet Tracer>
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface loopback 0 R2(config-if)#ip nat inside R2(config-if)#exit

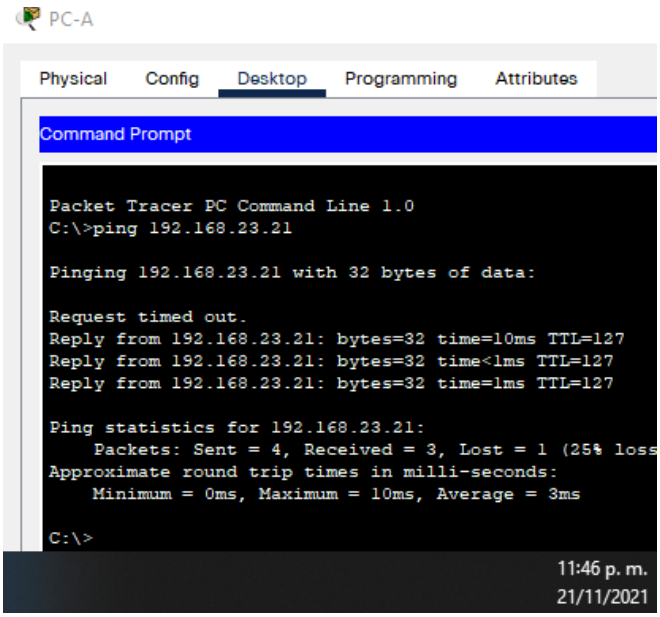
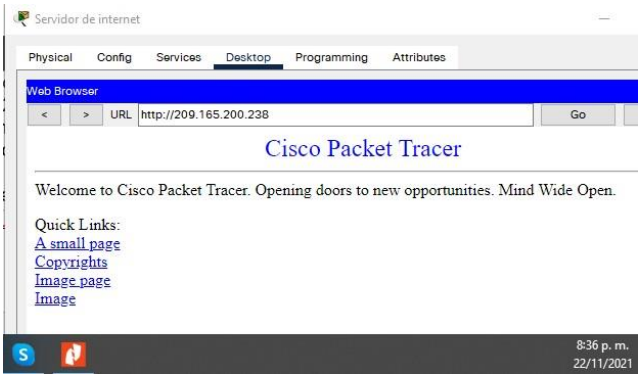
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255 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.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 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 R2(config)#exit R2#copy run start

Paso3. 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 21 verificación protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	*Ilustración 21 dhcp en PC-A*  *Fuente: Elaboración propia*
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	*Ilustración 22 dhcp en PC-B*  *Fuente: Elaboración propia*

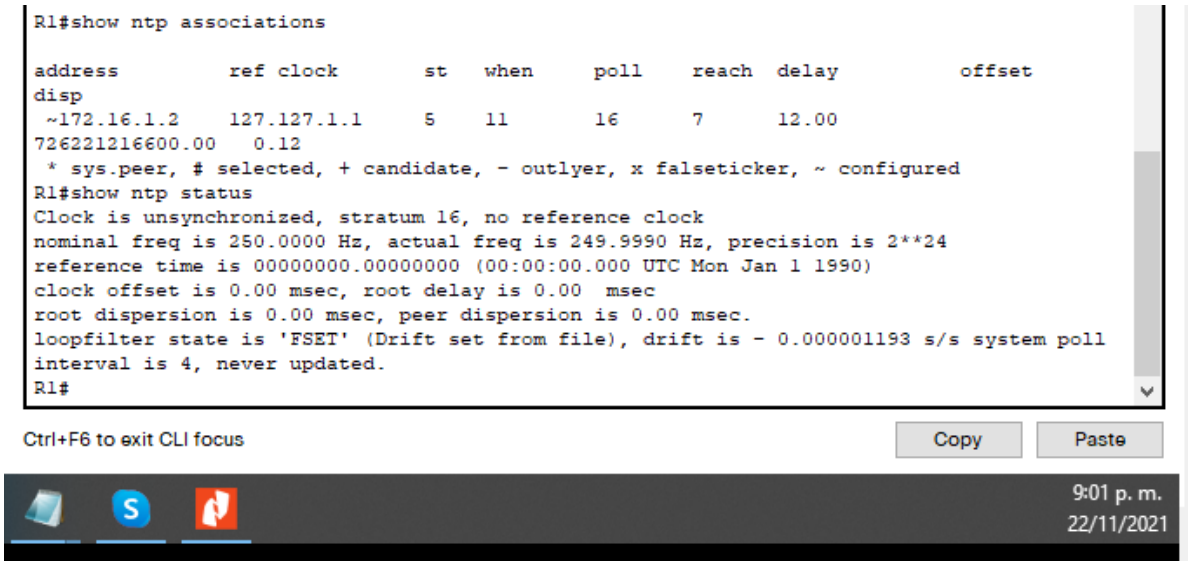
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	*Ilustración 23 Ping de PC-A a PC-B*  *Fuente: Elaboración propia*
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	*Ilustración 24 navegador web desde 209.165.200.238*  *Fuente: Elaboración propia*

Parte 6: Configurar NTP

Tabla 22 Configuración NTP en R2 y R1

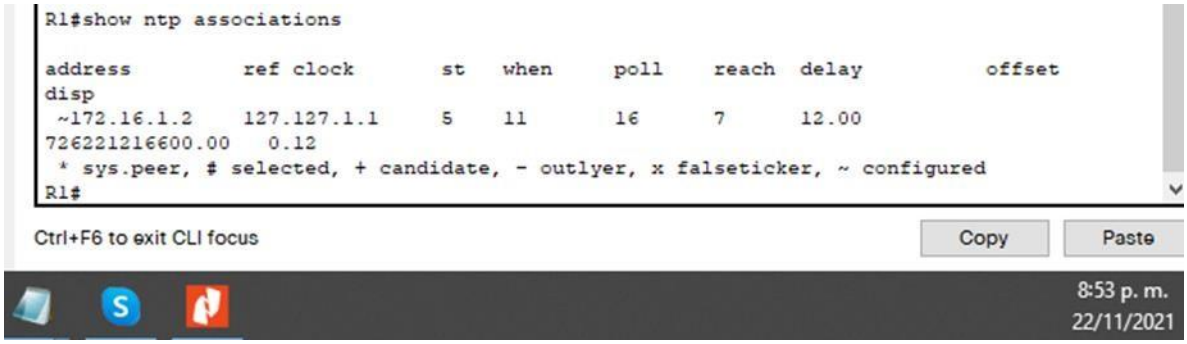
Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 mar 2016 **5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	R2(config)#ntp master 5 Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2 Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations R1#show ntp status <Las captura de imagen de los resultados en la ejecución de los comandos show se encuentran en las ilustraciónes 25 y 26>

Ilustración 25 show ntp associations



Fuente: Elaboración propia

Ilustración 26 show ntp status



Fuente: Elaboración propia

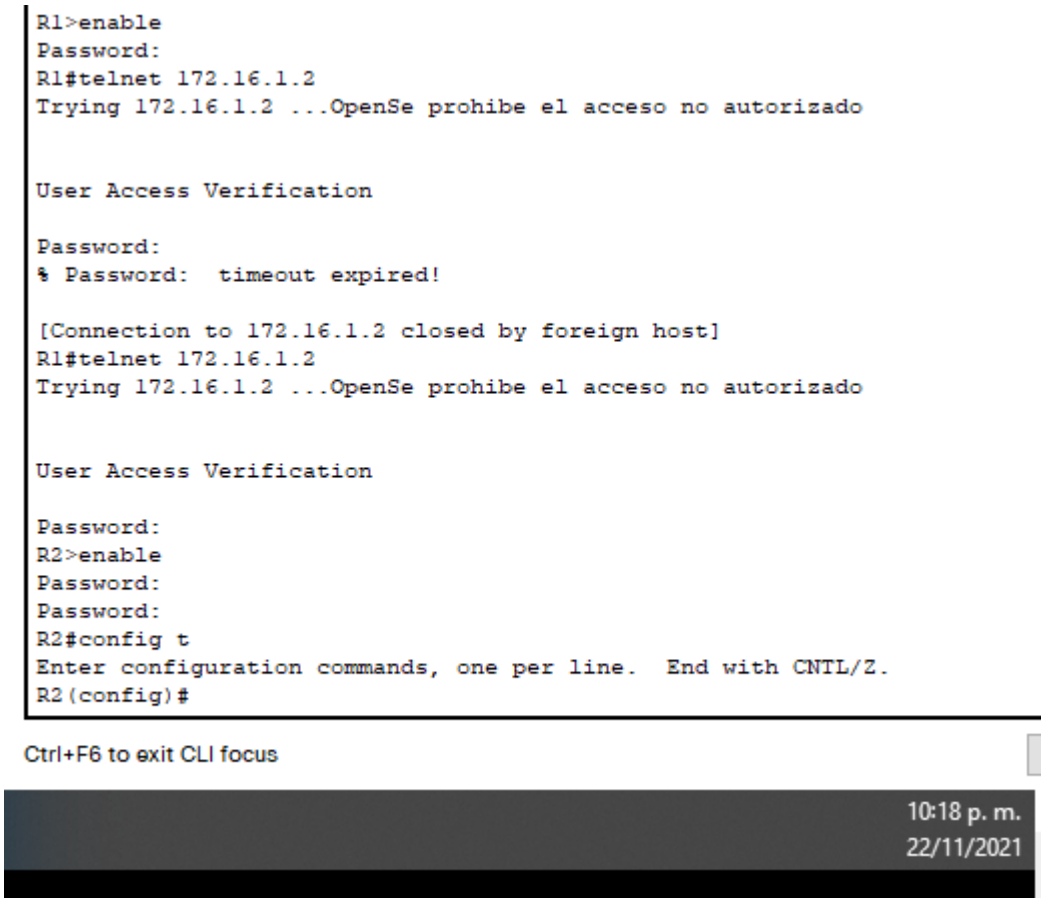
Parte 7: Configurar y verificar las listas de control de acceso (ACL)

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

Tabla 23 Restricción de acceso VTY en R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 Nombre de la ACL: **ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 <La captura de imagen del resultado telnet se encuentran en la ilustración 27>

Ilustración 27 telnet desde R1 A R2



Fuente: Elaboración propia

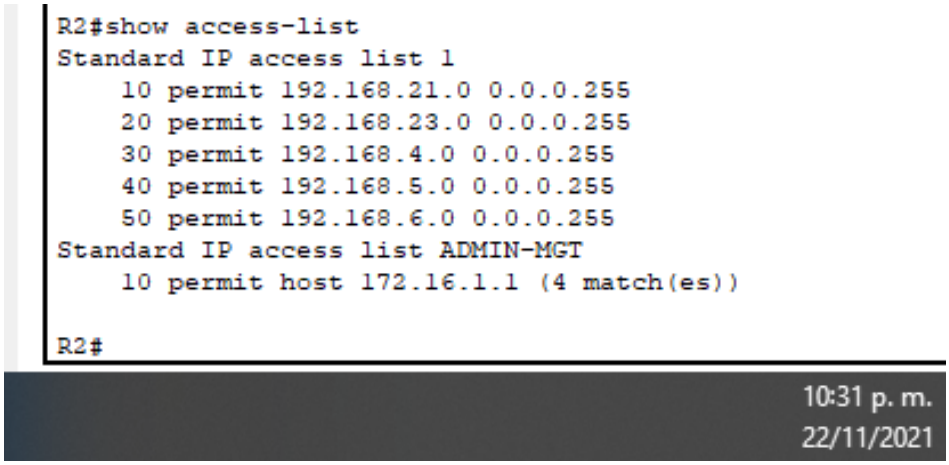
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

Tabla 24 ejecución de comando de CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-list <La captura de imagen del resultado del comando show access-list se encuentran en la ilustración 28>
Restablecer los contadores de una lista de acceso	clear access-list counters <La captura de imagen del resultado del comando clear access-list counters se encuentran en la ilustración 29>

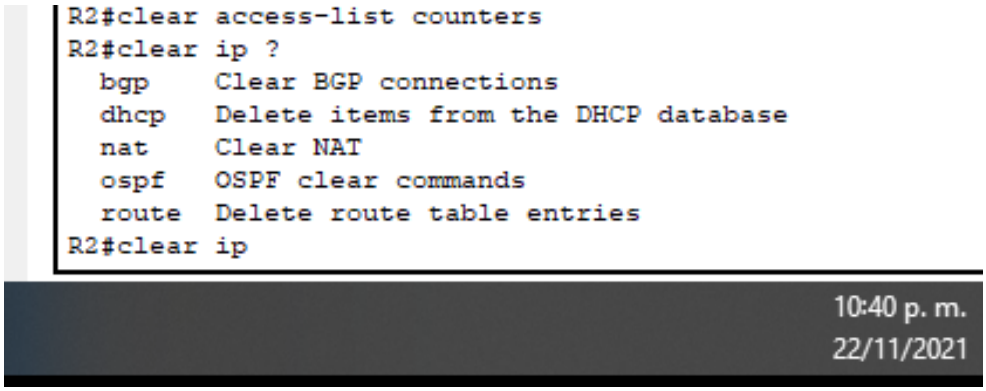
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface <La captura de imagen del resultado del comando show ip interface se encuentran en la ilustración 30>
¿Con qué comando se muestran las traducciones NAT?	show ip nat translations <La captura de imagen del resultado del comando show ip nat translations se encuentran en la ilustración 31> **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?	clear ip nat translation* <La captura de imagen del resultado del comando show ip nat translations* se encuentran en la ilustración 32>

Ilustración 28 resultado comando show access-list



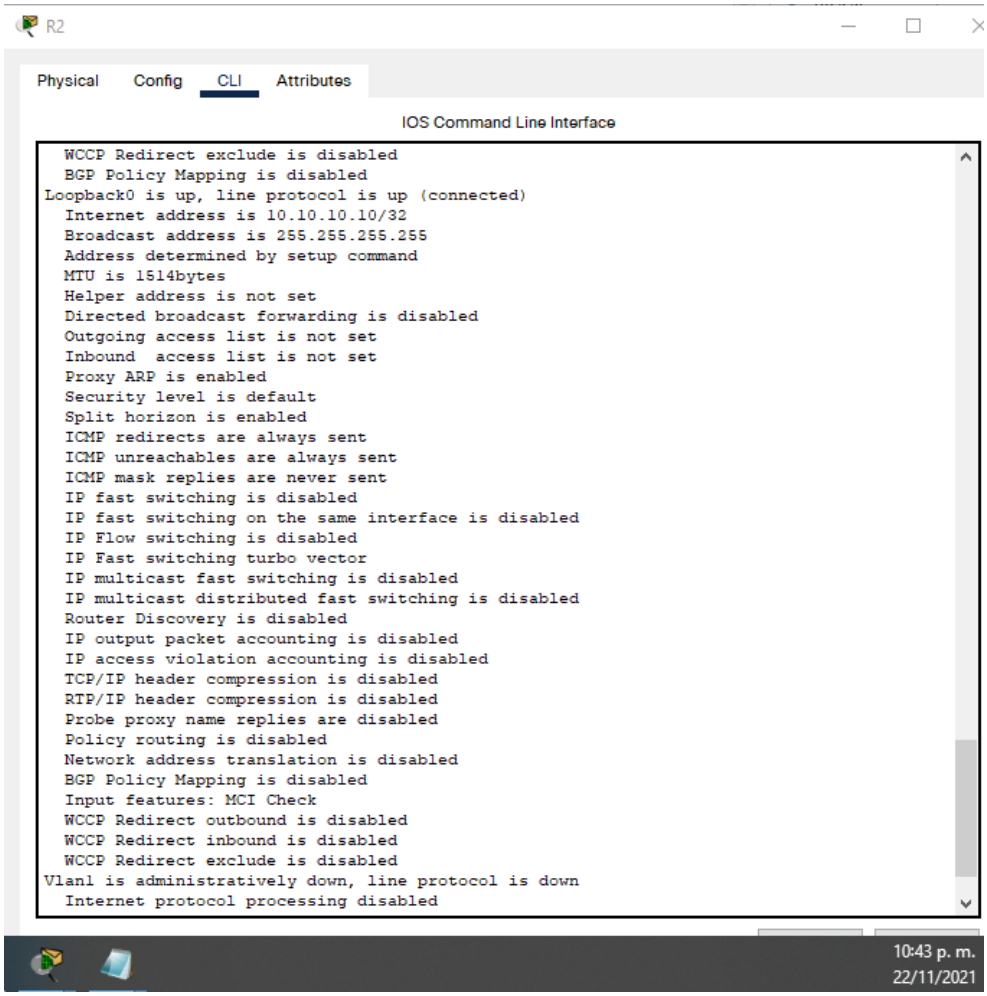
Fuente: Elaboración propia

Ilustración 29 resultado comando clear access-list counters



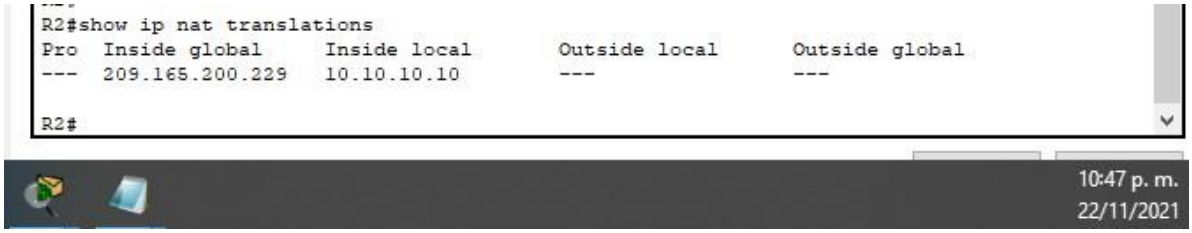
Fuente: Elaboración propia

Ilustración 30 resultado ejecución comando show ip interface



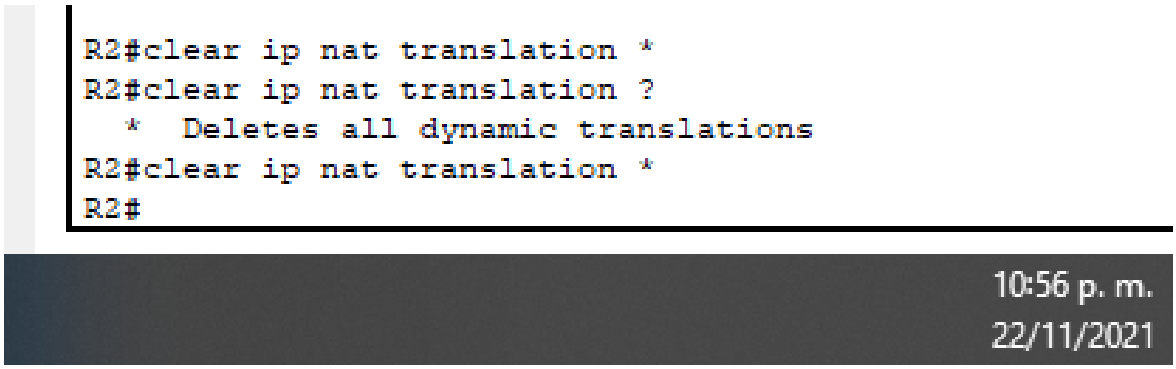
Fuente: Elaboración propia

Ilustración 31 resultado ejecución comando show ip nat translations



Fuente: Elaboración propia

Ilustración 32 ejecución Comando clear ip nat translation ?



Fuente: Elaboración propia

CONCLUSIONES

En este primer escenario se resalta la importancia en el diseño, configuración e implementación de una red, con las especificaciones que permitan tener en cuenta parámetros en las cantidades específicas de equipos optimizando el uso de las direcciones IP, gracias al subnetting; proceso que permitió dividir una red en dos sub redes, generando ventaja evitando que el tráfico en la red consuma una ancho de banda y resta recursos a los equipos intermedios, permite una mayor organización y la implementación de la seguridad en la misma red.

Con la puesta en funcionamiento de la red se logró óptimo desempeño, configurando los parámetros en los equipos intermedios el Reuter ISR 4331 y un switch 2960-24TT, usando los medios acordes a la topología y los host finales, que garantizan el buen desempeño en el funcionamiento de la red.

Desde la implementación de la red se intervinieron todos los equipos propuestos en la topología, configurando los parámetros básicos y específicos que admitiera la conectividad del protocolo IPv4 e IPv6, así como la traducción de direcciones de red dinámicas y estáticas como lo requería el laboratorio.

Se obtuvo con el desarrollo de los dos escenarios la comprensión de conceptos complejos en la interpretación literal como los protocolos DHCP, OSPF, NTP y una listas de control de acceso (ACL), pero que en la medida que fueron aplicados de manera practica en cada uno de los pasos permitieron ganar confianza en el momento que fueron ejecutados, arrojando en algunos casos acierto y en otro errores comunes en este ejercicio que en la medida que se practica se gana confianza y seguridad pensando en un escenario real donde sean aplicados a cabalidad.

BIBLIOGRAFÍA

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. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

CISCO.COM. N.D. Configuración de DNS en los routers de Cisco [online] Recuperado de: https://www.cisco.com/c/es_mx/support/docs/ip/domain-name-system-dns/24182-reversedns.pdf

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

Cortes Robles, D., 2015. Configurar DHCP Por VLAN En Equipos CISCO, Packet Tracer. [online] Seguridadyfirewall.cl. Recuperado de: https://www.seguridadyfirewall.cl/2015/08/configurar-dhcp-por-vlan-en-equipos.html

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 redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

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

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

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

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

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

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

FERNÁNDEZ, R., 2016. ⋆ Enrutamiento Dinámico OSPF Con Packet Tracer. [online] Raulprietofernandez.net. Recuperado de: https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ospf-con-packet-tracer

MARIONTECHACADEMY, 2013. CS071 21.02 OSPF - Configuracion OSPF En Packet Tracer. [online] www.youtube.com. Recuperado de: https://www.youtube.com/watch?v=lw-IekHi9eY

MOISA, J., 2018. *Asignación De IP A VLAN Administrativa*. [online] Community.cisco.com. Recuperado de: https://community.cisco.com/t5/discusiones-routing-y-switching/asignaci%C3%B3n-de-ip-a-vlan-administrativa/td-p/3357709

MOISA, J., 2018. Configurar La Hora Y Fecha Correcta. [online] Community.cisco.com. Recuperado de: https://community.cisco.com/t5/discusiones-general/configurar-la-hora-y-fecha-correcta/td-p/3735472

MOODLECF.SAPALOMERA.CAT. n.d. *3.2.1.2 Configuración De Interfaces*. [online] Recuperado de: http://moodlecf.sapalomera.cat/RS/3/course/module3/3.2.1.2/3.2.1.2.html

NETACAD.COM, n.d. 2.2.4.8 Protocolo De Hora De Red (NTP). [online] Static-course-assets.s3.amazonaws.com. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/2.2.4.8/2.2.4.8.html

NET CLOUD ENGINEERING. 2019. *Configuración De Una VLAN En Cisco Switch | Netcloud Engineering*. [online] Recuperado de: https://netcloudengineering.com/configuracion-vlan-cisco-switch/

PEREZ, J., 2018. Cómo Habilitar El Soporte De Ipv6 En Un Switch Cisco Catalisys 3560. [online] red10education.com. Recuperado de: https://red10education.com/blog/como-habilitar-el-soporte-de-ipv6-en-un-switch-cisco-catalisys-3560/

ROSALES, D., 2014. *Autenticación, Utilizando La Base De Datos Local*. [online] Seguridad y Redes. Recuperado de: https://delfirosales.blogspot.com/2014/04/autenticacion-utilizando-la-base-de.html