

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO USO DE TECNOLOGIA CISCO

WILSON BUSTAMANTE OSPINA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
IBAGUE TOLIMA
2021

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO USO DE TECNOLOGIA CISCO

WILSON BUSTAMANTE OSPINA

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

TUTOR
RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
IBAGUE TOLIMA
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

IBAGUE TOLIMA, 01 de diciembre de 2021

AGRADECIMIENTOS

A Dios y a todas las personas que han hecho posible mi proceso de formación. Agradezco de manera especial a los Tutores que con su dedicación y apoyo han hecho parte de este logro en mi vida personal. Y como profesional espero poder contribuir y retribuir a la sociedad en gran forma y de manera especial, en pro de una mejor sociedad y un mejor futuro de nuestro país.

DEDICATORIA

El presente trabajo lo dedico a Dios por regalarme la vida y el don de aprender, a mi familia por su acompañamiento permanente en las buenas en las malas y en las feas y a mi gloriosa Universidad, que con apoyo incondicional hacen posible la realización de los sueños como profesional y de los Tutores que con su apoyo y ayuda constante hacen posible la realización de los sueños.

TABLA DE CONTENIDO

AGRADECIMIENTOS	4
DEDICATORIA.....	4
CONTENIDO	5
LISTA DE TABLAS.....	7
LISTA DE FIGURAS.....	8
GLOSARIO.....	9
RESUMEN.....	10
ABSTRACT.....	10
INTRODUCCIÓN.....	11
REQUERIMIENTOS ESCENARIO.....	12
ESCENARIO No. 1	12
Parte 1: Construya la Red.....	12
Parte 2: Desarrolle el esquema de direccionamiento.....	13
Parte 3: Configure aspectos básicos	13
ESCENARIO 2.....	20
REQUERIMIENTOS ESCENARIO.....	20
DESARROLLO ESCENARIO 2.....	21
Parte 1: Inicializar dispositivos	21
Parte 2: Configurar los parámetros básicos de los dispositivos.....	22
Parte 3: Seguridad del switch, las VLAN y el routing entre VLAN.....	41
Parte 4: Configurar el protocolo de routing dinámico OSPF.....	50
Parte 5: Implementar DHCP y NAT para ipv4.....	56
Parte 6: Configurar NTP.....	58
Parte 7: Configurar y verificar las listas de control de acceso (ACL).....	59

CONCLUSIONES.....	60
BIBLIOGRAFIA.....	61

LISTA DE TABLAS

Tabla 1- Direccionamiento IP.....	14
Tabla 2. Configuración S1.....	14
Tabla 3. Configuración PC-A.....	17
Tabla 4. Configuración PC-B.....	17
Tabla 5 Configuración de Internet.....	23
Tabla 6. Configuración R1 Paso 2 Parte 2.....	24
Tabla 7 Configuración R2 Paso 3 Parte 2.....	26
Tabla 8. Configuración R3	29
Tabla 9 Configuración S1 Paso 5.....	31
Tabla 10 Configuración S3 Paso 6.....	32
Tabla 11 Verificar Conectividad Paso 7.....	34
Tabla 12. Configuración S1 Paso 1 Parte 3.....	37
Tabla 13 Configuración S3 Paso 2.....	39
Tabla 14 Configuración R1 Paso3 Parte 3.....	41
Tabla 15 Verificación de conectividad S1 y S3. Ping.....	43
Tabla 16. Configuración OSPF en R1.....	45
Tabla 17. Configuración OSPF en R1.....	46
Tabla 18. Configuración OSPF en R2 Paso 2.....	46
Tabla 19. Configuración R3 Paso 3.....	48
Tabla 20. Verificación Información OSPF Paso 4.....	49
Tabla 21 Configurar R1 -servidor de DHCP para las VLAN 21 y 23.....	50
Tabla 22. Restricción de acceso líneas VTY en R2.....	56
Tabla 23. Comando CLI.....	58

LISTA DE FIGURAS

Figura. 1. Topología Asignada Escenario No. 1.....	11
Figura. 2. Topología Creada Escenario No. 1.....	12
Figura. 3. Comando Ipconfig /all PC-B.....	18
Figura. 4 Comando Show IP Router.....	18
Figura. 5 Comando Show IP Router.....	20
Figura. 6 Topología base Escenario 2.....	21
Figura. 7. Configuración de servidor de Internet.....	24
Figura. 8 Configuración R3.....	31
Figura. 9 Configuración S1.....	32
Figura. 10 Configuración S3.....	33
Figura. 11 R2 Ping IP.....	35
Figura. 12 Ping 172.16.2.2.....	36
Figura. 13 Ping 2001:DB8: ACAD: A:1.....	36
Figura. 14 Ping Gateway Predeterminado.....	37
Figura. 15 Configuración S3.....	40
Figura. 16 Configuración Paso 3.....	42
Figura. 17 ping 192.168.99.1 S1 a R1 Vlan 99.....	43
Figura. 18 ping 192.168.21.1 S1 a R1 Vlan 99	44
Figura. 19 ping 192.168.21.1 S1 a R1 Vlan 99	44
Figura. 20. Configuración OSPF en R2 Paso 2.....	47
Figura. 21. Configuración R3 Paso 3.....	48
Figura. 22. verificación Información Ospf Paso 4.....	49
Figura. 23. Paso 2 Configuración Nat estática y dinámica en R2.....	51
Figura. 24. Verificación Protocolo DHCP PC-B.....	55
Figura. 25. Configuración NTP Parte 6.....	56
Figura. 26. Restricción de acceso Líneas VTY ACL en R2.....	57
Figura. 27. Aplicación Comando Show Ip nat Interfaces.....	59

GLOSARIO

Dhcp: (Dynamic Host Configuration Protocol) Es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red

Dirección Ip: Hace referencia a un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red de un dispositivo que utilice el protocolo o, que corresponde al nivel de red del modelo TCP/IP.

Dirección Ipv6: Corresponde a la versión 6 del Protocolo de Internet (Internet Protocol), es decir, es la sexta versión del protocolo que hace posible conectar dispositivos en Internet, identificándolos con una dirección unívoca

Tabla de enrutamiento: Contiene las mejores rutas de trabajo que se utilizarán actualmente para reenviar el tráfico entre dos vecinos.

Tabla de topología: Esta contiene toda la hoja de ruta de la red. Esta hoja de ruta incluye todos los Reuters Open Short Path First disponibles y mantiene datos calculados sobre las mejores rutas alternativas.

Enrutamiento: Proceso que permite que los paquetes IP enviados por el host origen lleguen al host destino de forma adecuada.

Loopback: Hace referencia a una interfaz de red virtual. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí.

Mascara de Subred: Combinación de bits que sirve para delimitar el ámbito de una red de ordenadores. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Vlan: Acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

RESUMEN

En el presente documento identificaremos escenarios propuestos para dar solución a la configuración de redes de datos, donde mediante el uso y la aplicación de software de simulación Packet Tracer, plantearemos el diseño, configuraremos y simularemos diferentes equipos pertenecientes a dos redes.

Los equipos Switch, Routers y Pc, les daremos el direccionamiento, restricciones, segmentación y pruebas respectivas de conectividad, que nos permitir verificar mediante comandos si se logran los objetivos planteados en los escenarios.

Palabras claves: Cisco, Red de datos, protocolo (ipv6-ipv4), conexiones, host.

ABSTRACT

In this document we will identify proposed scenarios to solve data networks, where through the use and application of simulation software packet tracer, we will propose the design, configure and simulate different equipment belonging to two networks. The equipment (sandwiches, Routers and Pc, we will give them the addressing, restrictions, segmentation and respective connectivity tests, which allow us to verify through commands if the objectives set out in the scenarios are achieved. Keywords: Network, protocol (ipv6-ipv4), connections, host, internet, Configuration, addressing.

Keywords: Cisco, Data network, protocol (ipv6-ipv4), connections, host.

INTRODUCCIÓN

En este trabajo final uniremos los dos escenarios propuestos permitiéndonos realizar cálculos de subnetting y los métodos necesarios para configurar una red LAN pequeña, con sus componentes o dispositivos de red. En ello aplicaremos configuraciones mediante comandos de consola, que permiten probar conectividad y seguridad SSH.

El escenario uno presenta una topología de red, conformada por dos PC, un switch y un Reuter, los cuales se configuraron por medio de subnetting a la dirección ip 192.168.6.0 donde los dos penúltimos dígitos corresponden al número de mi documento de identificación, en donde se emplearon LAN extraídas de la dirección de red principal, cada dispositivo se configuro y se probó su conectividad.

De igual manera en el escenario dos, presentamos configuraciones, como direccionamiento, subnetting, seguridad, segmentación mediante vlans, nat, vty, esto permitiendo ver las posibilidades de configuración que presentan las redes de comunicaciones.

REQUERIMIENTOS ESCENARIO

ESCENARIO No. 1

Figura. 1. Topología Asignada Escenario No. 1



Fuente: Prueba de habilidades CISCO CCNAII

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

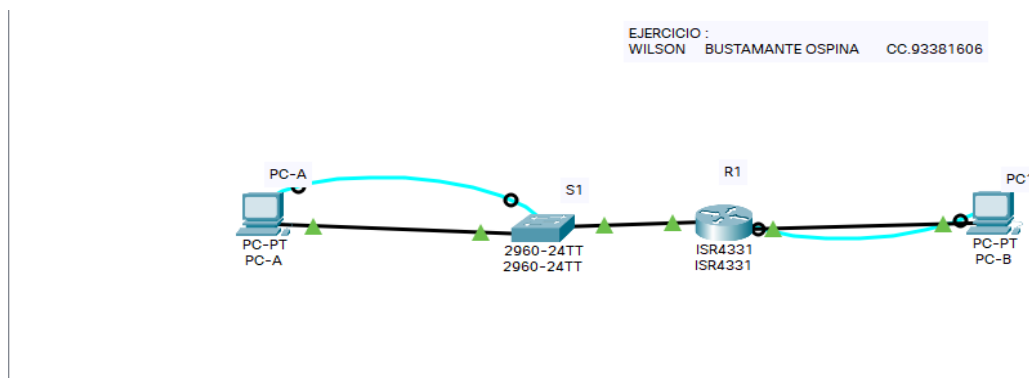
En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el switch S1, y los PC. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

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.

DESARROLLO ESCENARIO 1

Figura. 2. Topología Creada Escenario No. 1



Fuente: Autoría 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.

Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula. Tabla de direccionamiento. Tabla de direccionamiento CC. 93381606

Para 100 hosts 2 subredes

Dirección: 192.168.6.0/24 mascara 255.255.255.128/25 número de hosts/subredes 128, intervalo de direcciones .192.168.6.1 – 192.168.6.126, dirección de difusión o broadcast. 192.168.6.127

Tablas de direccionamiento ip y subnetting

Subnet ID	Subnet Address	Host Address Range	Broadcast Address
1	192.168.6.0	192.168.6.1 192.168.6.126	192.168.6.127
2	192.168.6.128	192.168.6.129 192.168.6.254	192.168.6.255

Fuente: Autoría Propia

Para 50 hosts 4 subredes: Dirección: 192.168.6.0/24 mascara 255.255.255.192/26 número de hosts/subredes 64, intervalo de direcciones .192.168.6.1 – 192.168.6.62 dirección de difusión o broadcast. 192.168.6.63

Tabla 2 Calculo de Subnetting

Subnet ID	Subnet Address	Host Address Range	Broadcast Address
1	192.168.6.0	192.168.6.1 192.168.6.62	192.168.6.63
2	192.168.6.64	192.168.6.65 192.168.6.126	192.168.6.127
3	192.168.6.128	192.168.6.129 192.168.6.190	192.168.6.191
4	192.168.6.192	192.168.6.193 192.168.6.254	192.168.6.255

Fuente: Autoría Propia

ITEM	REQUERIMIENTO
Dirección de Red	192.168.X.0 Donde se le asigne al octeto donde se encuentra la X los dos últimos dígitos de mi cedula de ciudadanía la cual termina en 47 Quedando así 192.168.6.0 con prefijo 24 por defecto
Requerimiento de Host Subred LAN 1	100
Requerimiento de Host Subred LAN 2	50
R1 G0/0/0	192.168.6.61/26
R1 G0/0/1	192.168.6.1/25
S1 SVI	192.168.6.2/25
PC-A	192.168.6.126/25
PC-B	192.168.6.190/26

Tabla 1- Direccionamiento IP

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 S1

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda de DNS	Se aplica mediante el comando R1(config)#no ip domain-lookup
Nombre del Router	Se le asigno R1 mediante el comando Router(config)#hostname R1
Nombre de dominio	El nombre del dominio se asignó mediante el comando R1(config)#ip domain-name ccna-lab.com

Contraseña cifrada para modo EXEC privilegiado	Se asignó mediante el comando R1(config)#line console 0 R1(config-line) #password ciscoenpass R1(config-line) #login
Contraseña de acceso a la consola	Se digita los comandos R1(config)#line vty 0 12 R1(config-line) #password ciscoenpass R1(config-line) #login R1(config-line) #exit
Establecer la longitud mínima para las contraseñas	Se establece mediante los comandos R1(config)#service password min-length 10
Crear un usuario administrativo en la base de datos local	Se designa mediante los siguientes comandos R1(config)#username admin password admin1pass R1(config)#line console 0 R1(config-line) #login local R1(config-line) #exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se configura con los comandos R1(config)#line vty 0 4 R1(config-line) #login local R1(config-line) #exit
Configurar VTY solo aceptando SSH	Se configura con los comandos R1(config)#line vty 0 4 R1(config-line) #transport input ssh R1(config-line) #login local R1(config-line) #exit
Cifrar las contraseñas de texto no cifrado	R1(config-line) #line console 0 R1(config-line) # service password encryption
Configure un MOTD Banner	R1(config)#banner motd #acceso restringido solo personal autorizado#
Configurar interfaz G0/0/0	R1(config)#interface g0/0/0 R1(config-if) #ip address 192.168.6.129 255.255.255.192 R1(config-if) #description LAN1 R1(config-if) #no sh R1(config-if) #exit
Configurar interfaz G0/0/1	R1(config)#interface g0/0/1 R1(config-if) #ip address 192.168.6.1 255.255.255.128 R1(config-if) #no sh R1(config)#exit
Generar una clave de cifrado RSA	R1(config)#config t R1(config)#crypto key generate rsa general-keys modulus 1024

	R1(config)#login local R1(config)#transport input ssh R1(config)# exit
--	--

Fuente: Autoría Propia

Las tareas de configuración de S1 incluyen lo siguiente:

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda de DNS	Se aplica mediante el comando R1(config)#no ip domain-lookup
Nombre del Router	Se le asigno S1 mediante el comando Router(config)#hostname S1
Nombre de dominio	El nombre del dominio se asignó mediante el comando S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para modo EXEC privilegiado	Se asignó mediante el comando S1(config)#line console 0 S1(config-line) #password ciscoenpass S1(config-line) #login
Contraseña de acceso a la consola	Se digita los comandos S1(config)#line vty 0 12 S1(config-line) #password ciscoenpass S1(config-line) #login S1(config-line) #exit
Crear un usuario administrativo en la base de datos local	Se designa mediante los siguientes comandos S1(config)#username admin password admin1pass S1(config)#line console 0 S1(config-line) #login local S1(config-line) #exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se configura con los comandos S1(config)#line vty 0 4 S1(config-line) #login local S1(config-line) #exit
Configurar VTY solo aceptando SSH	Se configura con los comandos S1(config)#line vty 0 4 S1(config-line) #transport input ssh S1(config-line) #login local S1(config-line) #exit
Cifrar las contraseñas de texto no cifrado	S1(config-line) #line console 0 S1(config-line) # service password encryption
Configure un MOTD Banner	S1(config)#banner motd #este es el switch de la UNAD por favor no entrar aquí#
Configurar la interfaz de administración (SVI)	S1config t S1(config)#interface LAN 1

	(config)#ip address 192.168.6.1 255.255.255.128 S1(config)#no sh S1(config)#end copy running-config startup-config R1(config-if) #exit
Configuración del Gateway predeterminado	S1config t S1(config)#ip default-gateway 192.168.6.1
Generar una clave de cifrado RSA	R1(config)#config t R1(config)#crypto key generate rsa general-keys modulus 1024 R1(config)#line vty 0 4 R1(config)#login local R1(config)#transport input ssh R1(config)#exit

Fuente: Autoría Propia

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 3. Configuración PC-A

Descripción	LAN1
Descripción física	
Dirección IP	192.168.6.126/25
Mascara de subred	255.255.255.128
Gateway Predeterminado	192.168.6.1

Fuente: Autoría Propia

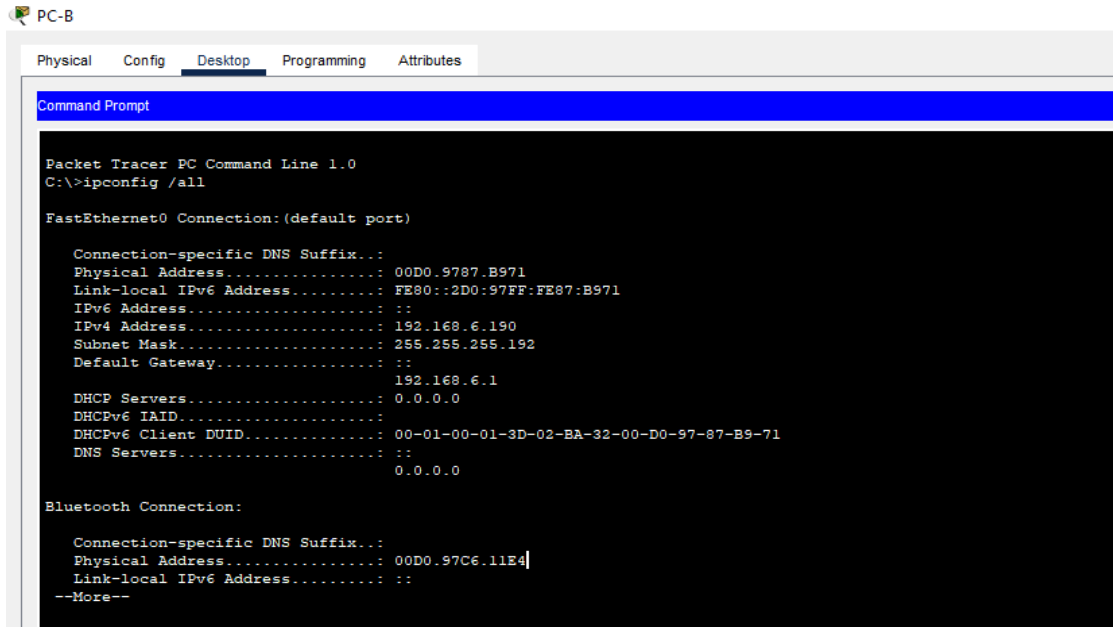
Tabla 4. Configuración PC-B

PC-B Network Configuration	
Descripción	LAN 2
Descripción física	
Dirección IP	192.168.6.190/26
Mascara de subred	255.255.255.192
Gateway Predeterminado	192.168.6.1

Fuente: Autoría Propia

Aplicación Comando ipconfig /all a la PC-A

Figura. 3. Comando Ipconfig /all PC-B



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 00D0.9787.B971
    Link-local IPv6 Address.....: FE80::2D0:97FF:FE87:B971
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.6.190
    Subnet Mask.....: 255.255.255.192
    Default Gateway.....: ::
    192.168.6.1
    DHCP Servers.....: 0.0.0.0
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-3D-02-BA-32-00-D0-97-87-B9-71
    DNS Servers.....: ::
    0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Physical Address.....: 00D0.97C6.11E4
    Link-local IPv6 Address.....: ::
    --More--
```

Fuente: Autoría Propia

Figura. 4 Comando Show IP Route



```
R1
Physical Config CLI Attributes
IOS Command Line Interface

4194304K bytes of physical memory.
3223661K bytes of flash memory at bootflash:.

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to
ACCESO RESTRINGIDO.

User Access Verification
Username: admin
Password:

R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.47.0/24 is variably subnetted, 4 subnets, 3 masks
   C       192.168.47.0/25 is directly connected, GigabitEthernet0/0/1
   L       192.168.47.1/32 is directly connected, GigabitEthernet0/0/1
   C       192.168.47.128/26 is directly connected, GigabitEthernet0/0/0
   L       192.168.47.129/32 is directly connected, GigabitEthernet0/0/0

R1>
```

Fuente: Autoría Propia

Comando Ping y prueba conectividad. Pc A y B

PC-A

```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.6.190

Pinging 192.168.6.190 with 32 bytes of data:

Request timed out.
Reply from 192.168.6.190: bytes=32 time<lms TTL=127
Reply from 192.168.6.190: bytes=32 time<lms TTL=127
Reply from 192.168.6.190: bytes=32 time<lms TTL=127

Ping statistics for 192.168.6.190:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

PC-B

```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.6.126

Pinging 192.168.6.126 with 32 bytes of data:

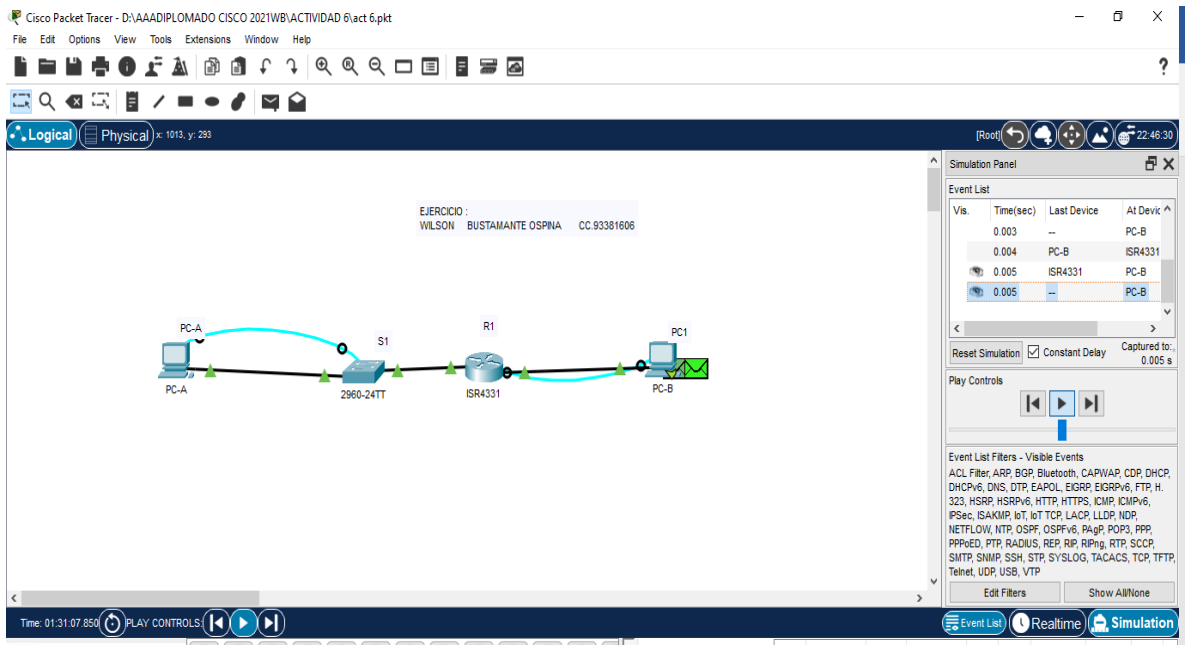
Reply from 192.168.6.126: bytes=32 time<lms TTL=127
Reply from 192.168.6.126: bytes=32 time<lms TTL=127
Reply from 192.168.6.126: bytes=32 time<lms TTL=127
Reply from 192.168.6.126: bytes=32 time<lms TTL=127

Ping statistics for 192.168.6.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autoría Propia

Figura. 5 Comando Show IP Route



Fuente: Autoría Propia

Análisis.

Después de realizar el presente taller identificamos, clase de red, configuración de equipos, y pruebas de conectividad. Identificamos el número de hosts y subredes según la petición, después de esto se realizaron los cálculos de direccionamiento, y con base en esa solicitud se configuraron el Router el switch y los pc, permitiéndonos mediante comandos de consola configurar y probar las conexiones según requerimientos solicitadas en la guía.

ESCENARIO 2

REQUERIMIENTOS ESCENARIO

Escenario:

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switch, router 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

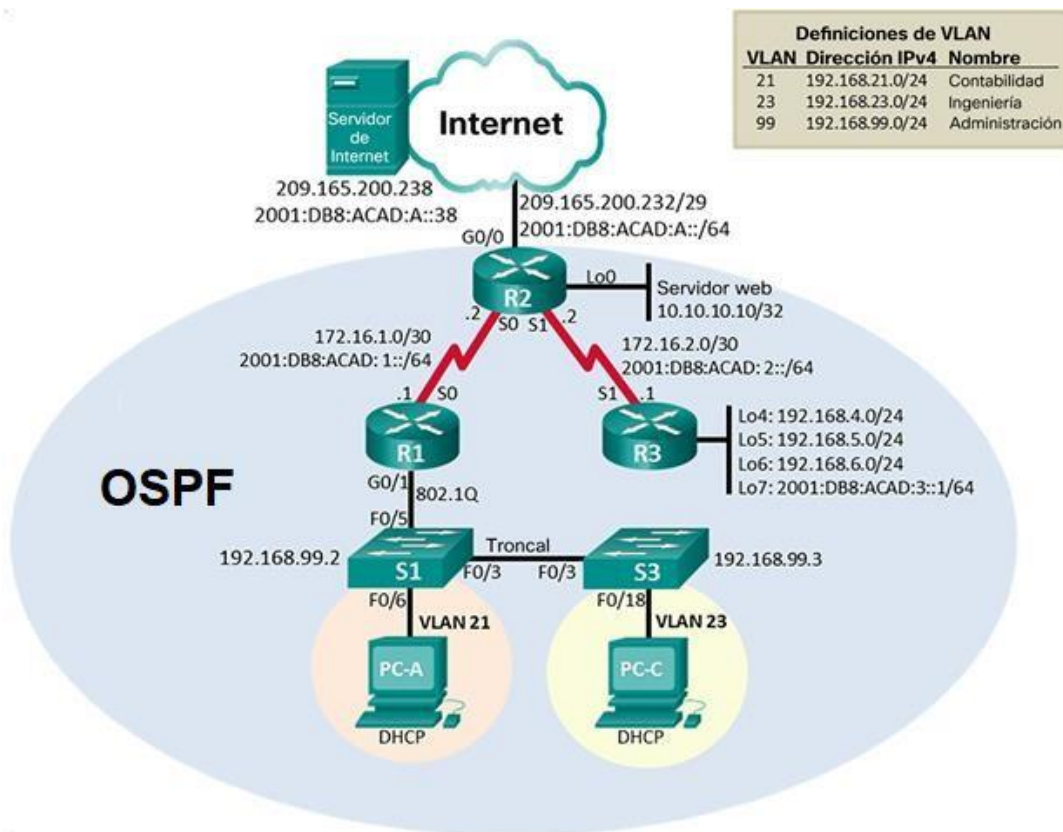
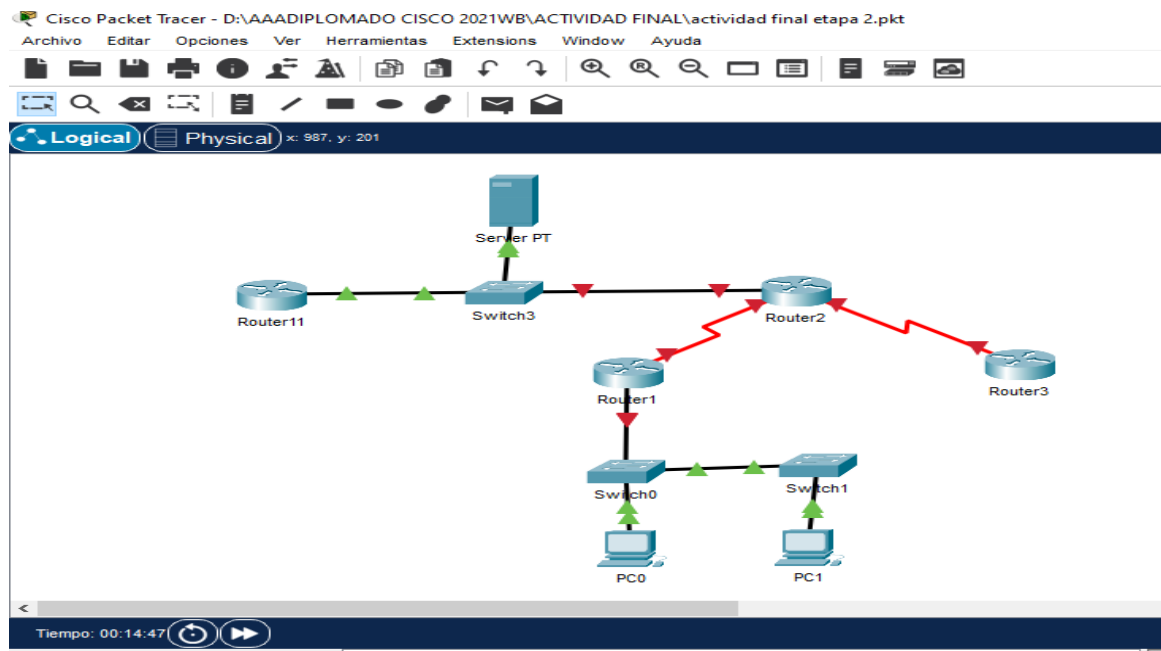


Figura. 6 Topología base Escenario 2

DESARROLLO ESCENARIO 2

Parte 1: Inicializar dispositivos

Figura 1: Diagrama inicial de dispositivos.



Fuente: Autoría Propia

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Para realizar la configuración es necesario que los dispositivos estén limpios y que se borren las configuraciones anteriores para que más adelante no se presenten errores. Por lo anterior se ejecuta el comando `erase configuración inicial` para la eliminación de la configuración de inicio para deshacer los últimos cambios realizados. En los switch se eliminan las bases de datos de la Vlan anterior y con el comando `Show flash` se hace la verificación.

Tabla 1 Comandos iniciales

TAREA	COMANDO DE IOS
Eliminar el archivo startup-config de todos los routers	En cada Router se dan los comandos Router>enable Router#erase startup-config
Volver a cargar todos los routers	Router#reload Se da inicialización Hardware de nuevo a los routers
Eliminar el archivo startup-config de todos los switch y eliminar la base de datos de VLAN anterior	En cada Switch se ejecutan los comandos Switch>enable Swich#erase startup-config Swich#delete vlan.dat
Volver a cargar ambos switch	Swich#reload Se da inicialización Hardware de nuevo a los Switch
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switch	Swich#enable Swich#show flash

Fuente: Autoría Propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

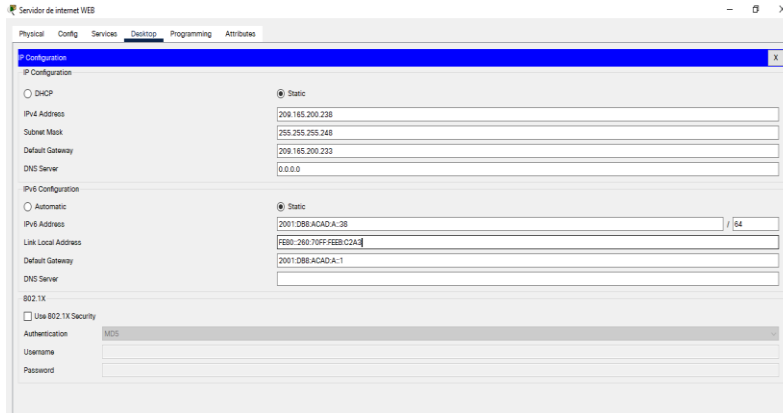
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología): IP, consulte la topología):

Tabla 5 Configuración de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238/29
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	Gateway: 209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64 es la ipv6
Gateway predeterminado IPv6	Gateway: 2001:DB8:ACAD:A::1/64

Fuente : Aatoria Propia

Figura. 7. Configuración de servidor de Internet.



Fuente: Autoría Propia

Paso 2: Configurar R1

Se requiere la configuración del router que proporcione conectividad a nivel de red con el fin de encaminar paquete de datos de una red a otra, la configuración será básica y se inicia con la desactivación del servicio DNS para que más adelante no cause retrasos, luego colocamos el nombre del router y el de dominio, protección por contraseña para proteger el acceso a EXEC privilegiado y así proporcionar seguridad, se realiza la configuración de las interfaces del dispositivo.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 6. Configuración R1 Paso 2 Parte 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config T Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#
Nombre del Router	Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	Se aplica el comando R1(config)#enable secret class
Contraseña de acceso a la consola	Se aplican los comandos

	<pre>R1(config)#line console 0 R1(config-line) #password cisco R1(config-line) # login R1(config-line) #</pre>
Contraseña de Acceso Telnet	<pre>Se aplican los comandos R1(config-line) #line vty 4 R1(config-line) #password cisco R1(config-line) #login R1(config-line) #</pre>
Cifrar las contraseñas de texto no cifrado	<pre>Se aplican los comandos R1(config)#line console 0 R1(config-line) #service password-encryption</pre>
Mensaje MOTD	<pre>Se ejecuta el comando R1(config)#banner motd "Se prohíbe el acceso no autorizado"</pre>
Interfaz S0/2/0	<pre>Se ejecutan los comandos R1(config)#int s0/2/0 R1(config-if) #description interface hacia el router R2 R1(config-if) #exit R1(config)#ipv6 unicast-routing R1(config)#int s0/2/0 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 sh %LINK-5-CHANGED: Interface Serial0/2/0, changed state to down R1(config-if) #exit R1(config)#</pre>
Rutas Predeterminadas	<pre>Se ejecutan los comandos R1(config)#ip route 0.0.0.0 0.0.0.0 S0/2/0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 S0/2/0 R1(config)#</pre>

Fuente: Autoría Propia

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 7 Configuración R2 Paso 3 Parte 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ejecutan los comandos Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain -lookup Router(config)#
Nombre del Router	Se ejecutan los comandos Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	Se ejecutan los comandos R2(config)#enable secret class
Contraseña de acceso a la consola	Se ejecutan los comandos R2(config)#line console 0 R2(config-line) #password cisco R2(config-line) #login
Contraseña de Acceso Telnet	Se ejecutan los comandos 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	Se ejecutan los comandos R2(config)#service password-encryption
Habilitar el servidor HTTP	El comando http no sirve en ninguna versión de los routers
Mensaje MOTD	Se ejecutan los comandos R2(config)#banner motd #se prohíbe el acceso no autorizado# R2(config)#
Interfaz S0/0/0	Se ejecutan los comandos R2(config)#ipv6 unicast -routing R2(config)#int s0/2/0

	<pre> 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 sh R2(config-if) # %LINK-5-CHANGED: Interface Serial0/2/0, changed state to up R2(config-if) # %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up R2(config-if) # </pre>
Interfaz S0/0/1	<pre> Se ejecutan los comandos R2(config)#int s0/2/1 R2(config-if) #ip address 172.16.2.1 255.255.255.252 R2(config-if) #ipv6 add 2001:DB8:ACAD:2::2/64 R2(config-if) #clock rate 128000 R2(config-if) #no sh %LINK-5-CHANGED: Interface Serial0/2/1, changed state to down R2(config-if) # R2(config-if) # </pre>
Interfaz G0/0 (Simulación de Internet)	<pre> Se ejecuta los comandos R2(config-if) #int g0/0/0 R2(config-if) #description interface hacia internet R2(config-if) #exit R2(config)#ipv6 unicast -routing R2(config)#int G0/0/0 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 sh R2(config-if) # </pre>

	<pre>%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up R2(config-if) #</pre>
Interfaz Loopback 0 (Servidor web simulado)	<pre>Se ejecutan 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 description servidor WEB R2(config-if) #ip address 10.10.10.10 255.255.255.255</pre>
Ruta predeterminada	<pre>Se ejecutan R2(config-if) #ip route 0.0.0.0 0.0.0.0 G0/0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 G0/0/0 R2(config)#</pre>

Fuente: Autoría Propia

Paso 4: Configurar R3

Cisco Packet Tracer - D:\AAADIPLOMADO CISCO 2021WB\ACTIVIDAD FINAL\ESCENARIO 2 DIPLOMADO CISCO 1 okwd.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 879, y: 209

Autoría: Fuente propia

La configuración del R3 incluye las siguientes tareas:

Tabla 8. Configuración R3

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

	R3(config)#
Interfaz S0/0/1	Se ejecutan los comandos int s0/2/1 ipv6 unicast-routing int s0/2/1 ip address 172.16.2.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::1/64 no sh
Interfaz loopback 4	Se ejecutan los comandos R3(config-if) #int loopback 4 R3(config-if) #ip address 192.168.4.1 255.255.255.0 R3(config-if) #exit %LINK-5-CHANGED: Interface Loopback4, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up R3(config)#
Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if) #ip address 192.168.5.1 255.255.255.0 R3(config-if) #exit %LINK-5-CHANGED: Interface Loopback5, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up R3(config)#
Interfaz loopback 6	Se ejecutan los comandos R3(config)#int loopback 6 R3(config-if) #ip address 192.168.6.1 255.255.255.0 R3(config-if) #exit %LINK-5-CHANGED: Interface Loopback6, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

	R3(config)#
Interfaz loopback 7	Se ejecutan los comandos interface loopback 7 ipv6 address 2001:DB8: ACAD:3::1/64 exit
Rutas predeterminadas	Se ejecutan los comandos R3(config)#ip route 0.0.0.0 0.0.0.0 S0/2/1 %Default route without gateway, if not a point-to-point interface, may impact performance R3(config)#ipv6 route: :/0 S0/2/1 R3(config)#

Fuente: Autoría Propia

Figura. 8 Configuración R3

```

IOS Command Line Interface
Enter configuration commands, one per line. End with CTRL/Z.
R3(config)#int s0/2/1
R3(config-if)#ipv6 unicast-routing
R3(config)#int s0/2/1
R3(config-if)#ip address 172.16.2.2 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#no sh

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/1, changed state to up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to up

R3(config-if)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#exit
%LINK-5-CHANGED: Interface Loopback4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up

R3(config)#int loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#exit
%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up

R3(config)#int loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
%LINK-5-CHANGED: Interface Loopback6, changed state to up

```

Fuente: Autoría Propia

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9 Configuración S1 Paso 5

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ejecuta el comando switch(config)#no ip domain-lookup Switch(config)#
Nombre del Switch	Se ejecuta el comando Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	Se ejecuta el comando S1(config)#enable secret class S1(config)#
Contraseña de acceso a la consola	Se ejecuta el comando S1(config)#line console 0 S1(config-line) #password cisco S1(config-line) #login
Contraseña de acceso Telnet	Se ejecuta el comando S1(config-line) #line vty 0 15 S1(config-line) #password cisco S1(config-line) #login S1(config-line) #
Cifrar las contraseñas de texto no cifrado	Se ejecuta el comando S1(config-line) #service password-encryption
Mensaje MOTD	Se ejecuta el comando S1(config)#banner motd #se prohíbe el acceso no autorizado#

Fuente: Autoría Propia

Figura. 9 Configuración S1

```

S1>enable
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#
S1(config)#banner motd #se prohíbe el acceso no autorizado#
S1(config)#
    
```

Fuente: Autoría Propia

Paso 6: Configurar S3

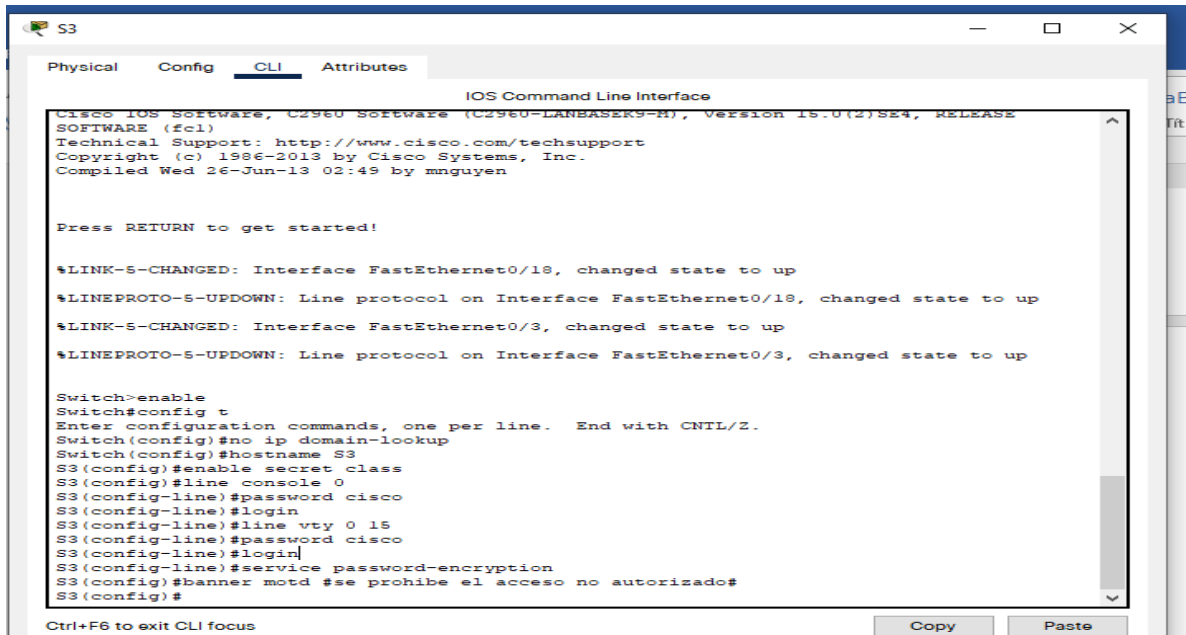
La configuración del S3 incluye las siguientes tareas:

Tabla 10 Configuración S3 Paso 6

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ejecuta el comando Switch(config)#no ip domain-lookup
Nombre del Switch	Se ejecuta el comando Switch(config)#hostname S3 S3(config)#
Contraseña de exec privilegiado cifrada	Se ejecuta el comando S3(config)#enable secret class
Contraseña de acceso a la consola	Se ejecuta el comando S3(config)#line console 0 S3(config-line) #password cisco S3(config-line) #login S3(config-line) #
Contraseña de acceso Telnet	Se ejecuta el comando S3(config-line) #line vty 0 15 S3(config-line) #password cisco S3(config-line) #login S3(config-line) #
Cifrar las contraseñas de texto no cifrado	Se ejecuta el comando S3(config-line) #service password-encryption
Mensaje MOTD	Se ejecuta el comando S3(config)#banner motd #se prohíbe el acceso no autorizado# S3(config)#

Fuente: Autoría Propia

Figura. 10 Configuración S3



Fuente: Autoría Propia

Paso 7: Verificar la conectividad de la red

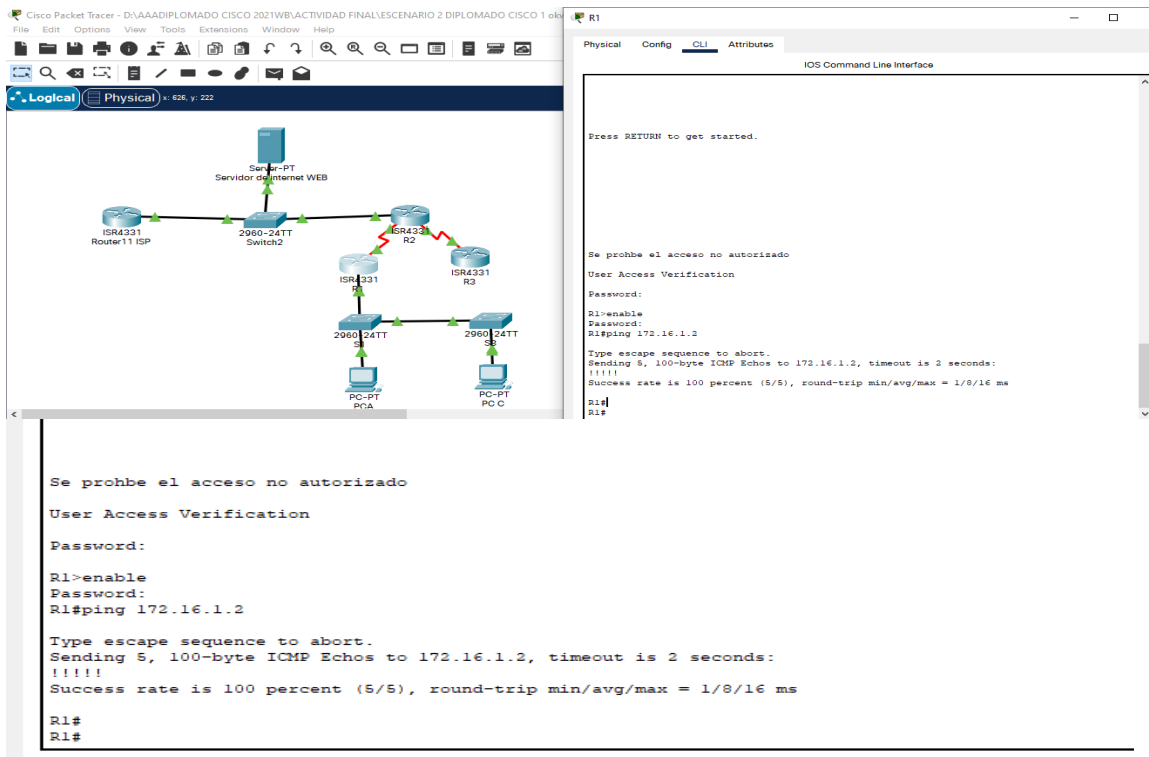
Utilice el comando ping para probar la conectividad entre los dispositivos de red.

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:

Desde	A	Dirección IP	Resultados de ping
R1	2 S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.2	Exitoso
PC de Internet	Gateway Predeterminado	209.165.200.233	Exitoso

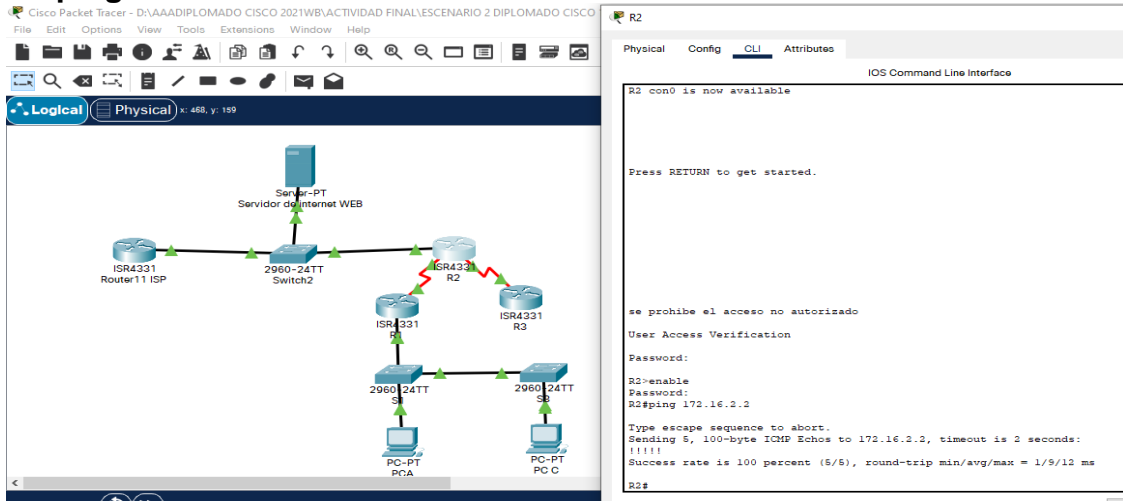
Tabla 11 Verificar Conectividad Paso 7

R1 Ping Exitoso



Fuente: Autoría Propia

R2 ping Exitoso



Fuente: Autoría propia

Figura. 11 R2 Ping IP

```
Password:
R2>enable
Password:
R2#ping 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/12 ms

R2#
R2#
R2#ping 2001:db8:acad:a::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:a::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/12 ms

R2#
```

Fuente: Autoría propia

Ping desde el Servidor de Internet IPv4

Desde el pc de internet se hace ping con la ip 172.16.2.2 arrojando como resultado la conectividad entre los dos dispositivos.

Figura. 12 Ping 172.16.2.2

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.2.2

Pinging 172.16.2.2 with 32 bytes of data:

Reply from 172.16.2.2: bytes=32 time=14ms TTL=253
Reply from 172.16.2.2: bytes=32 time=2ms TTL=253
Reply from 172.16.2.2: bytes=32 time=2ms TTL=253
Reply from 172.16.2.2: bytes=32 time=2ms TTL=253

Ping statistics for 172.16.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 5ms

C:\>
```

Fuente: Autoría Propia

Ping con IPV6

Desde la pc de internet se hace ping con la ipv6 2001:DB8:ACAD:A::1: arrojando como resultado la conectividad entre los dos dispositivos.

Figura. 13 Ping 2001:DB8:ACAD:A::1

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autoría Propia

Ping Gateway Predeterminado

Desde Pc de internet se hace ping al Gateway predeterminado, ip 209.165.200.233 arrojando como resultado la conectividad entre los dos dispositivos.

Figura. 14 Ping Gateway Predeterminado

```

>kwd.pkt
Servidor de internet WEB

Physical  Config  Services  Desktop  Programming  Attributes

Command Prompt

C:\>
C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time=8ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms
C:\>

```

Fuente: Autoría Propia

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12. Configuración S1 Paso 1 Parte 3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Se ejecutan los comandos S1(config)#enable S1(config)#config t 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 Administration S1(config-vlan) #exit S1(config)#
Asignar la dirección IP de Administración	Se ejecutan los comandos S1(config)#int vlan 99 S1(config-if) #ip address 192.168.99.2 255.255.255.0 S1(config-if) #no sh S1(config-if) #exit

	S1(config)#
Asignar el Gateway Predeterminado	Se ejecuta el comando S1(config)#ip default -Gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Se ejecutan los comandos S1(config)#int f0/3 S1(config-if) # switchport mode trunk S1(config-if) # switchport trunk native vlan 1 S1(config-if) #
Forzar el enlace troncal en la interfaz F0/5	Se ejecutan los comandos S1(config)#int f0/5 S1(config-if) #switchport mode trunk S1(config-if) #switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Se ejecutan los comandos S1#enable S1#config t S1(config)#int range f0/1- f0/2 S1(config-if-range) # switchport mode acces S1(config-if- range) #exit S1(config-if- range) #int range f0/4 S1(config-if- range) #switchport mode acces S1(config-if- range) #exit S1(config-if- range) #exit S1(config)#int range f0/6-24 S1(config-if- range) #switchport mode acces S1(config-if- range) #exit
Asignar F0/6 a la VLAN 21	Se ejecutan los comandos S3(config)#int f0/6 S3(config-if) #switchport access vlan 21
Apagar todos los puertos sin usar	Se ejecutan los comandos S1(config-if) #int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if- range) #shutdown S1(config-if- range) #exit S1(config)#exit S1#

Fuente: Autoría Propia

Configuración S1 Paso 1 Parte 3

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

S1#enable
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int range f0/1- f0/2
S1(config-if-range)#switchport mode acces
S1(config-if-range)#exit
S1(config)#int range f0/4
S1(config-if-range)#switchport mode acces
S1(config-if-range)#exit
S1(config)#int range f0/6-24
S1(config-if-range)#switchport mode acce^Z
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#enable
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int range f0/6-24
S1(config-if-range)#switchport mode acces
S1(config-if-range)#exit
S1(config)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#exit
S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#sh

```

Fuente: Autoría Propia

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13 Configuración S3 Paso 2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Se ejecutan los comandos S3#enable S3#config t 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 administration S3(config-vlan) #exit S3(config)#
Asignar la dirección IP de Administración	Se ejecutan los comandos S3(config)#int vlan 99 S3(config-if) #

	<pre>S3(config-if) #ip address 192.168.99.3 255.255.255.0 S3(config-if) #no sh S3(config-if) #exit</pre>
Asignar el Gateway Predeterminado	<pre>Se ejecuta el comando S3(config)#ip default -Gateway 192.168.99.1</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>Se ejecutan los comandos S3(config)#int f0/3 S3(config-if) #switchport mode trunk S3(config-if) #switchport trunk native vlan 1</pre>
Configurar el resto de los puertos como puertos de acceso	<pre>Se ejecutan los comandos S3(config)#int range f0/1 - f0/2 S3(config-if- range) #switchport mode acc S3(config-if- range) #exit S3(config)#int ran f0/7 - f0/24 S3(config-if- range) #switchport mode access S3(config-if- range) #exit</pre>
Asignar F0/18 a la VLAN 21	<pre>Se ejecutan los comandos S3(config)#int f0/18 S3(config-if) #switchport acc vlan 21 S3(config-if) # exit</pre>
Apagar todos los puertos sin usar	<pre>Se ejecutan los comandos S3(config)#int range f0/7 - f0/17 S3(config-if- range) #sh S3(config-if- range) #int range f0/19 - f0/24 S3(config-if- range) #sh S3(config-if- range) #exit S3(config)#exit S3#</pre>

Fuente: Autoría Propia

Figura. 15 Configuración S3

```

S3#enable
S3#config t
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-S-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-S-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no sh
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit
S3(config)#int range f0/1 - f0/2
S3(config-if-range)#switchport mode acc
S3(config-if-range)#exit
S3(config)#int ran f0/7 - f0/24
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
S3(config)#int f0/18
S3(config-if)#switchport acc vlan 21
S3(config-if)#exit
S3(config)#int range f0/7 - f0/17
S3(config-if-range)#sh
    
```

Fuente: Autoría Propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14 Configuración R1 Paso3 Parte 3

Elemento o tarea de configuración	Especificación
Configurar la sub interfaz 802.1Q .21 en G0/1	Se ejecutan los siguientes comandos R1#enable R1#config t R1(config)#int g0/0/1 R1(config-if) #no sh R1(config-if) #int g0/0/1.21 R1(config-subif) # R1(config-subif) #description Lan contabilidad R1(config-subif) #encapsulation dot1q 21 R1(config-subif) #ip address 192.168.21.1 255.255.255.0 R1(config-subif) #
Configurar la subinterfaz 802.1Q .23 en G0/1	Se ejecutan los siguientes comandos R1(config-subif) #int g0/0/1.23

	<pre>R1(config-subif) # R1(config-subif) #description Lan Ingenieria R1(config-subif) #encapsulation dot1q 23 R1(config-subif) #ip add 192.168.23.1 255.255.255.0 R1(config-subif) #exit</pre>
Configurar la subinterfaz 802.1Q .99 en G0/1	<pre>Se ejecutan los siguientes comandos R1(config)#int g0/0/1.99 R1(config-subif) # R1(config-subif) #description Lan administración R1(config-subif) #en dot1q 99 R1(config-subif) #encapsulación dot1q 99 R1(config-subif) #ip add 192.168.99.1 255.255.255.0 R1(config-subif) #exit R1(config)#</pre>
Activar la interfaz G0/1	<pre>Se ejecutan los siguientes comandos R1(config)#int g0/0/1 R1(config-if) #no sh</pre>

Fuente: Autoría Propia

Figura. 16 Configuración Paso 3

```
IOS Command Line Interface
%LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.21, changed state to
up
R1(config-subif)#description Lan contabilidad
R1(config-subif)#enc dot1q 21
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/0/1.23
R1(config-subif)#
%LINK-S-CHANGED: Interface GigabitEthernet0/0/1.23, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.23, changed state to
up
R1(config-subif)#description Lan ingenieira
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip add 192.168.23.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0/1.99
R1(config-subif)#
%LINK-S-CHANGED: Interface GigabitEthernet0/0/1.99, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.99, changed state to
up
R1(config-subif)#description LAN administracion
R1(config-subif)#en dot1q 99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#exit
R1#
%SYS-S-CONFIG_I: Configured from console by console
```

Fuente: Autoría Propia

Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switch 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 15 Verificación de conectividad S1 y S3. Ping

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: Autoría Propia

Figura. 17 ping 192.168.99.1 S1 a R1 Vlan 99

```

Password:

S1>enable
Password:
S1#enable
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 = 0/7/29 ms
```

Fuente: Autoría Propia

Figura. 18 ping 192.168.21.1 S1 a R1 Vlan 99

```
se prohíbe el acceso no autorizado
User Access Verification
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 100 percent (5/5), 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#
```

Ctrl+F6 to exit CLI focus

Fuente: Autoría Propia

Figura. 19 ping 192.168.21.1 S1 a R1 Vlan 99

The figure consists of two parts. On the left is a network diagram showing a topology with several devices: a Server-PT (Servidor de Internet WEB) connected to a 2960-24TT Switch2, which is connected to Router11 ISP (ISR4331). Router11 ISP is also connected to Router R2 (ISR4331). Router R2 is connected to Router R3 (ISR4331). Router R3 is connected to another 2960-24TT switch, which is connected to S1 (2960-24TT). On the right is a screenshot of the CLI for S3, showing the following commands and output:

```
S3>enable
Password:
S3#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 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms
S3#ping 192.168.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3#
S3#
S3#
```

Fuente: Autoría Propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Se configura la OSPF en al área 0 lo que hace que el router dentro de un área mantiene la información completa de la topología del área. Se anuncian las redes conectadas directamente y las interfaces LAN se establecen como pasivas

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configuración OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Se ejecutan los comandos R1>enable Password: R1#enable R1#config t R1(config)#router ospf 6 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
Anunciar las redes conectadas directamente	Se ejecutan los comandos 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)#net 172.16.1.0 0.0.0.3 area 0 R1(config-router)#
Establecer todas las interfaces LAN como pasivas	Se ejecutan los comandos R1(config-router)#passive-interface g0/0/1 R1(config-router)#passive-interface g0/0/1.21 R1(config-router)#passive-interface g0/0/1.23 R1(config-router)#passive-interface g0/0/1.99 R1(config-router)#exit R1(config)#exit
Desactive la sumarización automática	En ospf no se puede hacer de acuerdo a la web conferencia de fecha 15 de noviembre de 2021

Fuente: Autoría propia

Tabla 17. Configuración OSPF en R1

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.23, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up
Se prohbe el acceso no autorizado

User Access Verification

Password:

R1>enable
Password:
R1#enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 47
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)#net 172.16.1.0 0.0.0.3 area 0
R1(config-router)#passive-interface g0/0/1
R1(config-router)#passive-interface g0/0/1.21
R1(config-router)#passive-interface g0/0/1.23
R1(config-router)#passive-interface g0/0/1.99
R1(config-router)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
  
```

Fuente: Autoría Propia

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configuración OSPF en R2 Paso 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Se ejecutan los comandos R2>enable Password: R2#enable R2#config t R2(config)#router ospf 6 R2(config-router)#net 10.10.10.10 0.0.0.0 area 0
Anunciar las redes conectadas directamente	Se ejecutan los comandos R2(config-router)#net 10.10.10.10 0.0.0.0 area 0

	<pre>R2(config-router)#net 172.16.1.0 0.0.0.3 area 0 R2(config-router)#net 172.16.2.0 0.0.0.3 area 0</pre>
<p>Establecer todas las interfaces LAN (loopback) como pasivas</p>	<pre>Se ejecutan los comandos R2(config-router)#passive-interface lo R2(config-router)#passive-interface loopback 0 R2(config-router)#exit R2(config)#int s0/2/0 R2(config-if) #ipv6 ospf 6 area 0 R2(config-if) #exit R2(config)#int s0/2/1 R2(config-if) #ipv6 ospf 6 area R2(config-if) #int g0/0/0 R2(config-if) #ipv6 ospf 6 area 0 R2(config-if) #exit R2(config)#exit R2#</pre>
<p>Desactive la sumarización automática</p>	<p>NO se puede hacer en este sistema de enrutamiento, solo se hace en rip y en EIGRP la sumarización automática</p>

Fuente: Autoría Propia

Figura. 20. Configuración OSPF en R2 Paso 2

```
R2
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/2/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up
se prohíbe el acceso no autorizado

User Access Verification
Password:
R2>enable
Password:
R2#enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 47
R2(config-router)#net 10.10.10.10 0.0.0.0 area 0
R2(config-router)#net 172.16.1.0 0.0.0.3 area 0
R2(config-router)#net 172.16.2.0 0.0.0.3 area 0
R2(config-router)#
00:58:53: %OSPF-5-ADJCHG: Process 47, Nbr 192.168.99.1 on Serial0/2/0 from LOADING to
FULL, Loading Done

R2(config-router)#passive-interface lo
% Incomplete command.
R2(config-router)#passive-interface loopback 0
R2(config-router)#exit
R2(config)#
```

Fuente: Autoría Propia

Paso 3: Configurar OSPFv3 en el R3

en el paso 3 Configurar ospfv3 en R2 no se hace anunciar redes ipv4 sino ipv6 de acuerdo a las indicaciones dadas en la web conferencia ya que existe error en la guía, error esto debe ser para las redes bajo IPV6.

La configuración del R3 incluye las siguientes tareas:

Tabla 19. Configuración R3 Paso 3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Se ejecutan los comandos R3(config)#ipv6 router ospf 48 R3(config-rtr)#router-id 2.2.2.2
Anunciar las redes IPV4 conectadas directamente	Se ejecutan los comandos network 172.16.2.0 0.0.0.3 area 0 network 192.168.4.0 0.0.3.255 area 0
Establecer todas las interfaces LAN IPV4 (loopback) como pasivas	Se ejecutan los comandos R3(config)#int s0/2/1 R3(config-if) #ipv6 ospf 48 area 0 R3(config-if) #exit R3(config)#ipv6 router ospf 48 R3(config-rtr)#passive-interface lo 4 R3(config-rtr)#passive-interface lo 5 R3(config-rtr)#passive-interface lo 6 R3(config-rtr)#
Desactive la sumarización automática	NO se puede hacer en este sistema de enrutamiento, solo se hace en rip y en EIGRP la sumarización automática

Fuente: Autoría Propia

Figura. 21. Configuración R3 Paso 3

```

R3(config-if)#ipv6 ospf 48 area 0
OSPFv3: No IPV6 enabled on this interface
R3(config-if)#exit
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, ch
R3(config)#no ipv6 router ospf 2
R3(config)#no router-id 2.2.2.2
^
% Invalid input detected at '^' marker.
R3(config)#ipv6 router ospf 2
R3(config-rtr)#router-id 2.2.2.2
OSPF: router-id 2.2.2.2 in use by ospf process 48
R3(config-rtr)#exit
R3(config)#int loopback 7
R3(config-if)#ipv6 ospf 48 area 0
OSPFv3: No IPV6 enabled on this interface
R3(config-if)#exit
R3(config)#passive-interface loopback 4
^

```

Fuente: Autoría Propia

Paso 4: Verificar la información de OSPF

En el R2 se ejecuta el comando show ip protocols donde muestra la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router

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

Tabla 20. Verificación Información OSPF Paso 4

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

Fuente: Autoría Propia

Figura. 22. verificación Información Ospf Paso 4.

```
R2
Physical Config CLI Attributes
IOS Command Line Interface

R2(config-if)#show ip protocols
% Invalid input detected at '^' marker.
R2(config-if)#exit
R2(config)#exit
10:23:41: %OSPF-5-ADJCHG: Process 6, Nbr 192.168.99.1 on Serial0/2/0 from LOADING to FULL, Loading Done

R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip protocols

Routing Protocol is "ospf 6"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.10.10 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10         110          00:02:21
    192.168.99.1        110          00:02:22
  Distance: (default is 110)

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.165.200.233
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  --More--
```

Fuente: Autoría 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 21 Configurar R1 -servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Se ejecuta el comando 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	Se ejecuta el comando R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Se ejecutan los comandos R1#enable R1#config t R1(config)#ip dhcp pool ACCT R1(dhcp-config) #network 192.168.21.0 255.255.255.0 R1(dhcp-config) #domain-name ccna-sa.com R1(dhcp-config) #dns-server 10.10.10.10 R1(dhcp-config) #default-router 192.168.21.1 R1(dhcp-config)#
Crear un pool de DHCP para la VLAN 23	Se ejecutan los comandos R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config) #dns-server 10.10.10.10 R1(dhcp-config) #domain-name ccna-sa.com R1(dhcp-config) #default-router 192.168.23.1 R1(dhcp-config)#

Fuente: Autoría Propia

Figura.24 Configurar R1 Servidor de DHCP para las Vlan 21 y 23

```

R1
Physical  Config  CLI  Attributes
IOS Command Line Interface

Se prohbe el acceso no autorizado
User Access Verification
Password:
R1>enable
Password:
R1#config t
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)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#R1(dhcp-config)#default-router 192.168.21.1
^
% Invalid input detected at '^' marker.
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#

```

Fuente: Autoría Propia

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

La configuración del R2 incluye las siguientes tareas:

Figura. 23. Paso 2 Configuración Nat estática y dinámica en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Se ejecutan los comandos R2>enable Password: R2#config t R2(config)#username web user privilege 15 password cisco12345
Habilitar el servicio del servidor HTTP	eso es un error de comando ip http server comando no sirve ip http server R2(config)#ip http server ^ % Invalid input detected at '^' marker.

	R2(config)#
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2#config t Enter configuration commands, one per line. End with CNTL/Z. ip http authentication local ^ % Invalid input detected at '^' marker. R2(config)#
Crear una NAT estática al servidor web.	Se ejecuta el comando R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233
Asignar la interfaz interna y externa para la NAT estática	Se ejecutan los comandos R2(config)#interface g0/0/0 R2(config-if) #ip nat out R2(config-if) #ip nat outside R2(config-if) #int S0/2/0 R2(config-if) #ip nat in R2(config-if) #ip nat inside R2(config-if) #int s0/2/1 R2(config-if) #ip nat insi R2(config-if) #ip nat inside R2(config-if) #int lo ^ % Invalid input detected at '^' marker. R2(config-if) #int lo 0 R2(config-if) #ip nat ins R2(config-if) #ip nat inside R2(config-if) #exit R2(config)#
Configurar la NAT dinámica dentro de una ACL privada	Se ejecutan los comandos R2(config)#access-lists 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 192.168.0.0 0.0.7.255 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 192.168.0.0 0.0.7.255

	<pre>R2(config)#no access-list 1 permit 192.168.0.0 0.0.7.255 R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255 R2(config)#</pre>
Defina el pool de direcciones IP públicas utilizables.	<pre>Se ejecuta el comando R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248</pre>
Definir la traducción de NAT dinámica	<pre>Se ejecuta el comando R2(config)#ip nat inside source list 1 pool INTERNET</pre>

Fuente: Autoría Propia

```

R2
Physical Config CLI Attributes
IOS Command Line Interface

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233
R2(config)#interface g0/0/0
R2(config-if)#ip nat out
R2(config-if)#ip nat outside
R2(config-if)#int s0/2/0
R2(config-if)#ip nat in
R2(config-if)#ip nat inside
R2(config-if)#int s0/2/1
R2(config-if)#ip nat insi
R2(config-if)#ip nat inside
R2(config-if)#int lo
R2(config-if)#int lo 0
R2(config-if)#ip nat ins
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 192.168.0.0 0.0.7.255
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 192.168.0.0 0.0.7.255
R2(config)#no access-list 1 permit 192.168.0.0 0.0.7.255
R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
R2(config)#
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.

```

Fuente: Autoría Propia

Paso 3: Verificar el protocolo DHCP y la NAT estática

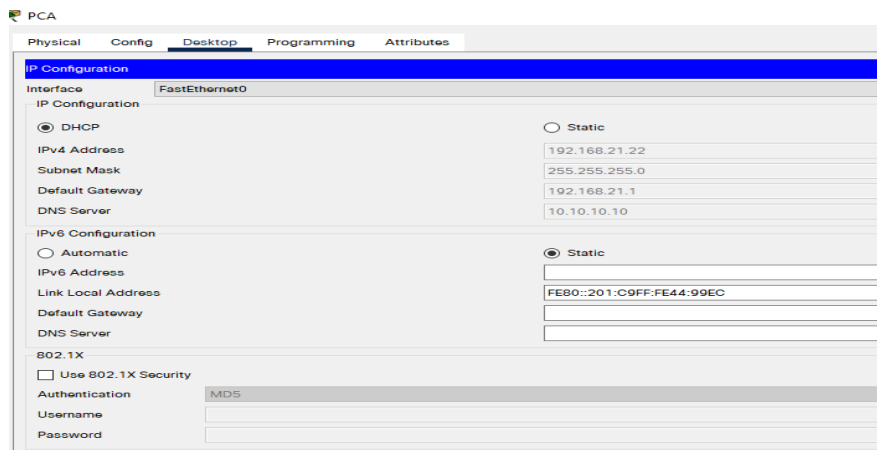
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 26. Paso 3 Verificar Protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	192.168.21.22 255.255.255. 0
Verificar que la PC-B haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-B Nota: Quizá sea necesario deshabilitar el firewall de la PC	ping 192.168.21.21
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	Falló (ip http server” no funciona en Packet Tracer)

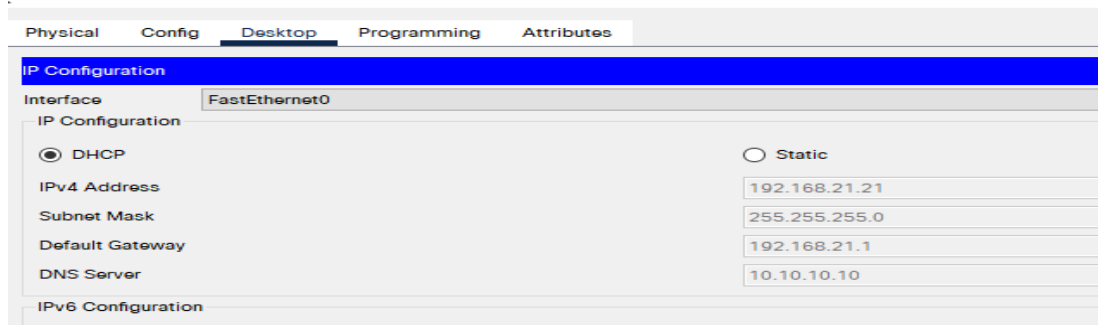
Fuente: Autoría Propia

Figura. 27. Verificación Protocolo DHCP PC-A



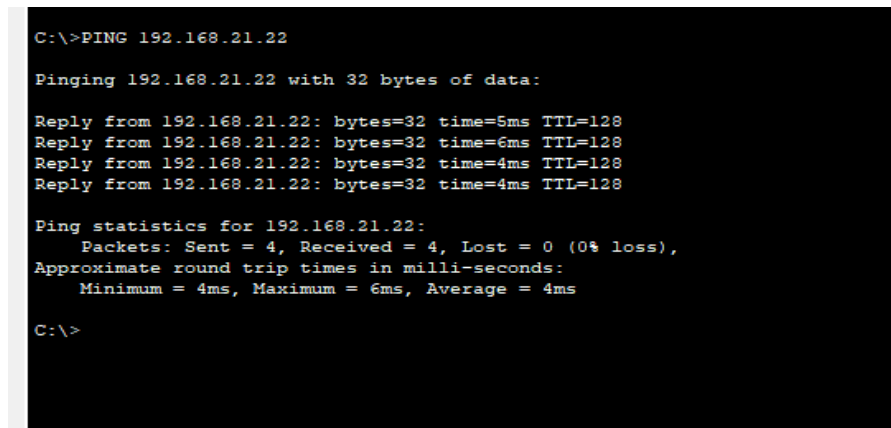
Fuente: Autoría Propia

Figura. 24. Verificación Protocolo DHCP PC-B



Fuente; Autoría propia

Figura. 34. PC-A ping PC_B 192.168.21.22



Fuente: Autoría Propia

Parte 6: Configurar NTP

Tabla 27. Configuración NTP Parte 6

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2	Se ejecuta el comando R2#clock set 09:00 05 march 2016
Configure R2 como un maestro NTP.	Se ejecutan los comandos R2#enable R2#config t R2(config)#ntp master 5 R2(config)#exit
Configurar R1 como un cliente NTP.	Se ejecutan los comandos R1>enable Password:

	Password: R1#config t R1(config)#ntp server 172.16.1.2 R1(config)#
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Se ejecuta el comando R1(config)#ntp update-calendar R1(config)#exit
Verifique la configuración de NTP en R1	Se ejecuta el comando R1#show ntp associations

Fuente: Autoría Propia

Figura. 25. Configuración NTP Parte 6

```

R1
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

Password:
R1>enable
Password:
R1#config t
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-S-CONFIG_I: Configured from console by console

R1#enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#show ntp associations
-
% Invalid input detected at '^' marker.

R1(config)#exit
R1#
%SYS-S-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   13    16    337   12.00
726216241191.00  0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1#
R1#
R1#

```

Fuente: Autoría 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 22. Restricción de acceso líneas 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	Se ejecutan los comandos R2(config)#ip Access -list standard ADMIN-MGT R2(config-std-)#permit host 172.16.1.1

	R2(config-std-nacl)#deny an R2(config-std-nacl)#deny any R2(config-std-nacl)#
Aplicar la ACL con nombre a las líneas VTY	Se ejecutan los comandos R2(config)#line vty 0 4 R2(config-line) #ip access-class ADMIN-MGT in R2(config-line) #
<Permitir acceso por Telnet a las líneas de VTY	Se ejecutan los comandos R2(config)#line vty 0 4 R2(config-line) #transport input telnet R2(config-line) #
Verificar que la ACL funcione como se espera	Se ejecutan los comandos R2#telnet 172.16.1.2 Trying 172.16.1.2 ...Open "se prohíbe el acceso no autorizado" User Access Verification

Fuente : Autoría propia

Figura. 26. Restricción de acceso Líneas VTY ACL en R2

The screenshot displays the Cisco Packet Tracer interface. On the left, a network topology is shown with the following components and connections:

- Router11 ISP** (ISR4331) connected to **Switch2** (2960-24TT) via Fa0/0/1 and Fa0/3.
- Switch2** connected to **R2** (ISR4331) via Fa0/1 and Fa0/3.
- R2** connected to **R3** (ISR4331) via Se0/2/0 and Se0/2/1.
- R2** connected to **PC A** (PC-PT) via Gig0/0/1 and Fa0/6.
- R3** connected to **PC B** (PC-PT) via Gig0/0/0 and Fa0/18.

On the right, the CLI window for R2 shows the following configuration and output:

```

R2
Physical Config CLI Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list satndart ADMIN-MGT
% Invalid input detected at '^' marker.
R2(config)#ip access-list standart ADMIN-MGT
% Invalid input detected at '^' marker.
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
% Incomplete command.
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show access-list
Standard IP access list 1
 10 permit 192.168.0.0 0.0.3.255
 20 permit 192.168.23.0 0.0.0.255
 30 permit 192.168.21.0 0.0.0.255
 40 permit 192.168.6.0 0.0.0.255
Standard IP access list ADMIN-MGT
 10 permit host 172.16.1.1 (4 match(es))
 20 deny any (16 match(es))
Standard IP access list ADMIN-MGTS
 10 permit host 172.16.1.1
R2#

```

Fuente: Autoría Propia

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

Tabla 23. 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	Se ejecutan los comandos R2#show access-lists Standard IP access list 1 10 permit 192.168.0.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 20 deny any R2#
Restablecer los contadores de una lista de acceso	Se aplica el comando R2#clear ip access-list counters. ^ % Invalid input detected at '^' marker. R2# Pero no lo soporta Packet Tracer
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Se ejecuta el comando R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Se aplican los comandos R2#show ip nat translations

Fuente: Autoría Propia

Figura. 27. Aplicación Comando Show Ip nat Interfaces

```

R2#
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345
ERROR: Can not have both a user password and a user secret.
Please choose one or the other.
R2(config)#
R2(config)#exit
R2#
$SYS-5-CONFIG I: Configured from console by console
show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  209.165.200.233    10.10.10.10      ---                ---
---  209.165.200.237    10.10.10.10      ---                ---

R2#show ip interface
GigabitEthernet0/0/0 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 unreachable 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
--More--
Ctrl+F6 to exit CLI focus
  
```

Fuente; Autoría propia

Fig 38: se muestran las traducciones NAT

```

R2#
R2#
R2#
R2#
R2#
R2#
R2#show ip nat translations
Pro  Inside global      Inside local      Outside local      Out
---  209.165.200.233    10.10.10.10      ---                ---
---  209.165.200.237    10.10.10.10      ---                ---

R2#
Ctrl+F6 to exit CLI focus
  
```

Fuente; Autoría propia

CONCLUSIONES

En el presente trabajo realizamos aprendizaje basado prácticas donde se integran equipos, direccionamiento, protocolos y configuraciones que nos permiten demostrar la conectividad de las redes planteadas en los dos escenarios propuestos.

Profundizamos en temas de direccionamiento, segmentación y seguridad, tomamos en estos escenarios las configuraciones dadas, realizamos las respectivas simulaciones de conectividad, dándonos la oportunidad de aprender sobre la práctica. En estos dos ambientes trabajamos configuraciones básicas desde reinicio de equipos, configuración de nombres, seguridad, encriptación de las claves, creación de subredes basado en vlan, creación de nat (estáticas, o dinámicas), salida a internet con interacción con servidor web, (como en la vida real), creación de vty y ospf o protocolo de encaminamiento jerárquico, todo esto se analizó después de habernos dado unos datos iniciales y cuyos cálculos serian parte de un escenario real de la vida de un ingeniero en telecomunicaciones.

Afianzamos varios temas la vida cotidiana para un ingeniero, obtuvimos familiaridad en procesos y comandos encontrando lineamientos poco comunes hasta ahora de mi conocimiento.

Es de anotar y agradecer inmensamente a nuestra Universidad, a nuestros Tutores por su compromiso y dedicación en la orientación de los nuevos ingenieros que seremos la base de nuevas generaciones.

BIBLIOGRAFIA

- CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3>
- CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4>
- 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). Ethernet. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5>
- CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6>
- GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. *Inge Cuc*, 12(1), 86-93.
- GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. *Revista de Tecnología*, 14(1), 127-138.
- MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In 2019 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONITI) (pp. 1-6). IEEE.
- Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgTCtKY-7F5KIRC3>
- BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations* (pp. 331-344). Springer, Cham.