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

JOHAN ALEJANDRO PARRA RAMIREZ

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

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

JOHAN ALEJANDRO PARRA RAMIREZ

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

TUTOR:
NANCY AMPARO GUACA

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

NOTA DE ACEPTACIÓN

Director del curso

Firma del Jurado

Firma del Jurado

SOACHA, 30 de noviembre de 2021

AGRADECIMIENTOS

Agradezco a mi familia y allegados que estarán en todos los momentos de mi vida y quien me guían hacia la perseverancia y el éxito, los cuales me han brindado su apoyo y espacio para poder realizar este proceso.

También agradecer en especial a toda la familia Unadista, tutores, directivos, compañeros y todos los que me ayudaron y orientaron en este desarrollo personal y profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CISCO: es una empresa de origen estadunidense, la cual es fabricante de redes locales y externas, también presta servicios de soluciones de red, su objetivo es conectar a todos para mostrar una visión clara del futuro, también tiene un gran reconocimiento en sus certificaciones las cuales son reconocidas a nivel mundial garantizando niveles altos de conocimiento y confiabilidad.

IPV6: el protocolo de internet versión 6 es la versión del protocolo de internet de IP, el cual nos permite trasmitir datos a través de una red a las direcciones IP que son las que nos identifican a los diferentes dispositivos conectados a internet y permitan la comunicación entre ellos, nos dan mejoras significativas a nivel de eficiencia, rendimiento y seguridad.

IPV4**:**es un protocolo de internet que nos entrega los datagramas entre host en una red, ipv4 es la cuarta versión del protocolo de internet que fue adaptado y ahora se utiliza ampliamente en la comunicación de datos a través de diferentes tipos de redes, es el protocolo más básico actualmente por los estándares de internet.

GATEWAY: considerado como un dispositivo en red que actúa como un punto de entrada de una red a otra, se maneja como un enlace que conecta dos ordenadores a internet, como medios de comunicación entre protocolos que les permite compartir datos en los mismos dispositivos informativos o entre diferentes sistemas informativos.

DHCP: un servidor de red el cual permite una asignación automática de direcciones IP, Gateway predeterminadas, con parámetros de red que soliciten sus clientes, también es capaz de enviar automáticamente todos los parámetros para los clientes se comuniquen sin problemas en su red.

RESUMEN

En el proceso de desarrollo y conocimiento del escenario 1 para el diplomado de profundización CCNA para el programa de ingeniería de sistemas de la UNAD, desarrolle diferentes trabajos correspondientes a CISCO, llegando de esta manera a realizar esta práctica mostrando mis conocimientos adquiridos y dar a conocer los pasos a seguir para esta configuración de dispositivos, realizando correctamente los requisitos solicitados y dar la forma de transmitir y salvaguardar la información que se garantice tener un nivel operativo sin fallos, para la integración de los datos y la rapidez que se trasmite de una manera constante en cualquier red con sus respectivas normas y parámetros correspondientes.

palabra claves: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica

ABSTRACT

In the process of development and knowledge of scenario 1 for the CCNA deepening diploma for the systems engineering program of the UNAD, I developed different works corresponding to CISCO, in this way to carry out this practice showing my acquired knowledge and making known the steps to follow for this configuration of devices, correctly carrying out the requested requirements and giving the way to transmit and safeguard the information that is guaranteed to have an operation without failures, for the integration of the data and the speed that it is transmitted in a constant way in any network with their respective standards and corresponding parameters.

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

INTRODUCCIÓN

Actualmente las redes están evolucionadas de manera muy rápida con sus diferentes dispositivos, técnicas y sistemas de comunicación, sus variadas investigaciones y desarrollo tecnológico está guiando la viada actual, la información de voz y de datos que mantienen a sus usuarios en un ámbito cotidiano, ya que las telecomunicaciones representan un gran cambio y éxito para esta sociedad con resultados grandiosos y su buena conexión a internet.

En este informe se encontrará de forma práctica y escrita los conocimientos obtenidos durante este curso del diplomado de profundización CCNA CISCO, desarrollando las varias habilidades y destrezas adquiridas a lo largo de este.

Aplicando uso del simulador para el desarrollo del primer escenario de la práctica de cisco en Packet Tracer, el cual me permitió realizar todas las configuraciones a swithches y routers, con sus respectivos protocolos de ipv4 e ipv6 aplicando redes virtuales VLAN, con esto muestro que este trabajo me permitió demostrar mis conocimientos, habilidades y destrezas en la implementación de redes informáticas.

DESARROLLO ESCENARIO 1

Figura 1: Escenario 1

Fuente: Elaboración propia

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

Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el 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

Figura 2 Simulación de escenario 1

Fuente :Elaboración propia

Parte 3: Configure aspectos básicos

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

-Desactivar la búsqueda DNS:

Router>enable ---> Inicio privilegiado

Router#config t ---> Ingreso configuración

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

Router(config)#no ip domain-lookup ---> Desactivar búsqueda DNS

-Establecer R1 Nombre del router:

Router#config t ---> Ingreso configuración

Router(config)#hostname R1 ---> nombrando Dispositivo

-Nombre de dominio ccna-lab.com:

R1(config)#ip domain-name ccna-lab.com ---> Nombre de Dominio

-Contraseña cifrada para el modo EXEC privilegiado cisco pass:

R1(config)#enable secret ciscoenpass --->Establecer Contraseña privilegiado

-Contraseña de acceso a la consola cisco conpass:

R1(config)#line console 0 ---> configuración línea de consola 0 como primera

R1(config-line)#password ciscoconpass---> Se establece la contraseña de inicio de consola

R1(config-line) #login ---> activar dispositivo

-Establecer la longitud mínima para las contraseñas 10 caracteres

R1(config)#security password min-length 10 ---> contraseña con mínimo de caracteres

-Crear un usuario administrativo en la base de datos local Usuario admin y password admin1pass

R1(config)#username admin password admin 1 pass ---> crear usuario con contraseña única

-Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

R1(config)#line console 0 ---> configuración línea de consola 0 como primera

R1(config-line)#login local ---> usuario creado para iniciar el dispositivo

R1(config)#line vty 0 4 ---> Ingreso a config line vty 0 4 para acceso telnet R1(config-line)#login local---> usuario creado para iniciar en telnet

-Configurar VTY solo aceptando SSH

R1(config-line)#transport input ssh ---> conexión ssh dentro de las líneas

-Cifrar las contraseñas de texto no cifrado

R1(config)#Service password-encryption---> contraseñas cifradas

-Configure un MOTD Banner

R1(config)#banner motd # El acceso no autorizado está prohibido!# --->mensaje de alerta

-Configurar interfaz G0/0/0 establecer la dirección IPv4 y activar la interfaz

R1(config)#interface g0/0/0 --->Ingreso a la interface

R1(config-if)#ip address 192.168.82.129 255.255.255.192 ---> Configuracion de direccionamiento

R1(config-if)#no shutdown ---> Activar interfaz

-Configurar interfaz G0/0/1 establecer la dirección IPv4 y activar la interfaz

R1(config-if)#interface g0/0/1 ---> Ingreso a la interface

R1(config-if)#ip address 192.168.82.1 255.255.255.128 ---> Configuracion de direccionamiento

R1(config-if)#no shutdown ---> Activar interfaz

-Generar una clave de cifrado RSA Módulo de 1024 bits

R1(config)#ip domain-name ccna-lab.com --->Establecer Nombre de Dominio R1(config)#crypto key generate rsa ---> clave de encryption

Paso 2: configurar los ajustes básicos en el S1

-Desactivar la búsqueda DNS

Switch>enable ---> Inicio privilegiado

Switch#config t ---> Ingreso configuración

Switch(config)#no ip domain-lookup ---> Desactivar DNS

-Establecer S1 Nombre del Switch

Switch(config)#hostname S1 ---> nombrando dispositivo

-Nombre de dominio ccna-lab.com

S1(config)#ip domain-name ccna-lab.com ---> Nombre de Dominio S1

-Contraseña cifrada para el modo EXEC privilegiado cisco en pass

S1(config)#enable secret ciscoenpass ---> Contraseña cifrada

-Contraseña de acceso a la consola ciscoconpass Se habilita la contraseña enable y se establece como se indica

S1(config)#line console 0 ---> configuracion línea de consola 0 como primera

S1 (config-line)#password ciscoconpass ---> contraseña de inicio de consola

S1(config-line)# Login---> activar dispositivo

-Crear un usuario administrativo en la base de datos local Usuario admin y password admin1pass

S1(config)#username admin password admin1pass ---> usuario con contraseña para ingresar

-Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

S1(config)#line console 0 ---> configuracion línea de consola 0 como primera

S1(config-line)#login--->usuario creado para iniciar el dispositivo

S1(config-line)#exit ---> salir de consola 0

S1(config)#line vty 0 4 ---> Ingreso a config line vty 0 4

S1(config-line)#login local ---> usuario creado para iniciar el dispositivo

-Configurar VTY solo aceptando SSH

S1(config) line vty 0 4---> Ingreso a config line vty 0 4

S1(config-line)#transport input ssh ---> acepten conexión SSH para las líneas vty

-Cifrar las contraseñas de texto no cifrado

S1(config)#service password-encryption ---> contraseñas cifradas

-Configure un MOTD Banne

S1(config)#banner motd #El acceso no autorizado está prohibido!# ---> mensaje de alerta

-Generar una clave de cifrado RSA Módulo de 1024 bits

How many bits in the modulus [512]: 1024 ---> modulo en 1024 bits

% Generating 1024 bit RSA keys, keys will be nonexportable...[OK]

-Configurar interfaz VLAN 1 establecer la dirección IPv4 y activar la interfaz

S1(config)#interface vlan 1---> Ingresar al modo de configuración Vlan 1

*Mar 1 0:54:40.329: %SSH-5-ENABLED: SSH 1.99 has been enabled

S1(config-if)#ip address 192.168.82.2 255.255.255.128 ---> Configuracion de vlan

-Configuración del Gateway predeterminado

S1(config)#ip default-gateway 192.168.82.1 ---> se agrega un gateway

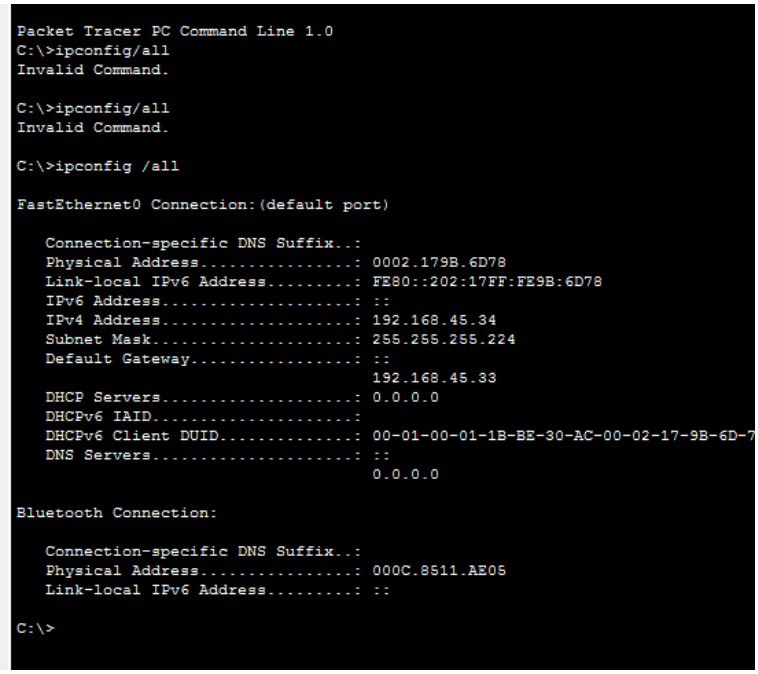
Paso 3: Configurar los equipos

Tabla 1 Direccionamiento 1

	fastEthernet0
Dirección física	0002.179B.6D78
Dirección ip	192.168.45.128
Máscara	255.255.255.128
Gateway	192.168.45.33

Fuente: Elaboración propia

Figura 3PC-A



Fuente :Elaboración propia

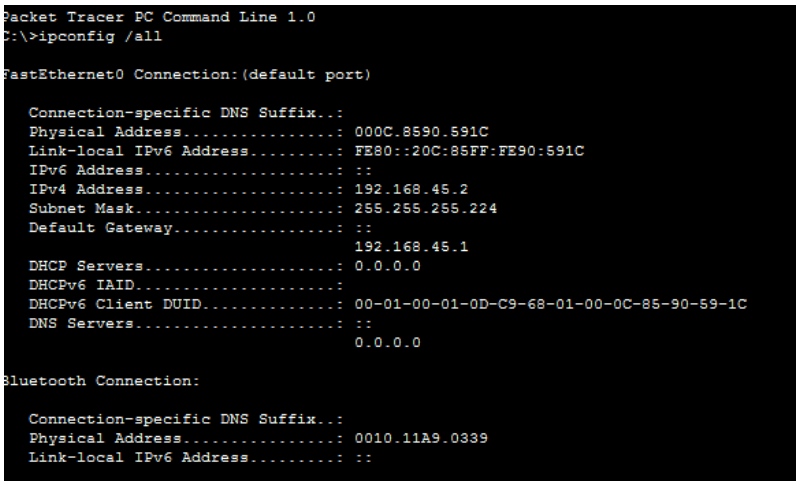
PC-C

Tabla 2 Direccionamiento 2

	fastEthernet0
Dirección física	000c.8590.591c
Dirección ip	192.168.45.2
Máscara	255.255.255.224
Gateway	192.168.45.1

Fuente: Elaboración propia

Figura 4 PC-B



Fuente :Elaboración propia

Figura 5 conexión exitosa

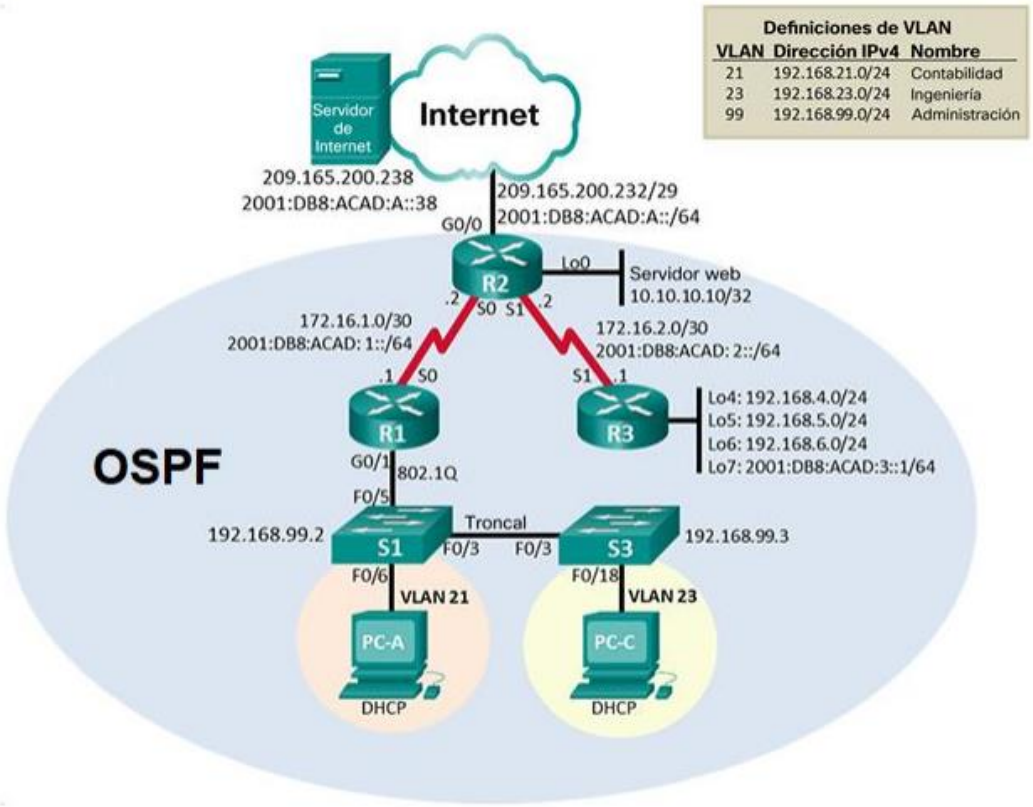
Fuente :Elaboración propia

Desarrollo escenario 2

Escenario 2 Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Figura 6 topología

Topología



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

-Eliminar el archivo startup-config de todos los routers

Router>ena--->inicio

Router#erase startup-config --->configuración de inicio para router

Erasing the nvram filesystem will remove all configuration files! Continue? [Confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

-Volver a cargar todos los routers

Router#reload--->cargar las configuraciones nuevamente

Proceed with reload? [Confirm]

System Bootstrap, Version 15.1 (4) M4, RELEASE SOFTWARE (fc1)

-Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior

Switch>ena

Switch#erase startup-config--->borrar contenido nvram

Erasing the nvram file system will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

-Volver a cargar ambos switches

Switch#reload--->se cargan las configuraciones

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

-Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

Figura 7 Vlan Swtich

```
Switch>ena
Switch#show flash
Directory of flash:/

    1  -rw-     4670455          <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch#
```

Fuente :Elaboración 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):

Tabla3 Direccionamiento computadora 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:DB8:200:238
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente :Elaboración propia

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes

-Desactivar la búsqueda DNS

Router>ena--->inicio

Router#conf t--->ingreso a configuración

Router (config) #no ip domain-lookup---> desactivar DNS

-Nombre del router

Router (config) #hostname R1---> nombrando r1

-Contraseña de exec privilegiado cifrada

R1(config)#enable secret class--->contraseña privilegiada

-Contraseña de acceso Telnet

R1(config)#line vty 0 4--->configuración de línea consola
R1(config-line)#password cisco--->contraseña de inicio
R1(config-line)#login--->activar al iniciar

-Cifrar las contraseñas de texto no cifrado

R1(config)#service password-encryption---> contraseña cifrada

-Mensaje MOTD

R1(config)#banner motd #Se prohíbe el acceso no autorizado#--->mensaje de alerta

-Interfaz S0/0/0

R1(config)#inter s0/0/0--->ingreso a la interfaz

R1(config-if)#description Conexión hacia el R2--->descripción
R1(config-if)#ip address 172.16.1.1 255.255.255.252--->configuracion de direccionamiento ipv4
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64---> configuración de direccionamiento ipv6
R1(config-if)#clock rate 128000--->activación 128000
This command applies only to DCE interfaces
R1(config-if)#no shut--->activar interfaz

-Rutas predeterminadas

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0--->ruta predeterminada ipv4
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 s0/0/0--->ruta predeterminada ipv6

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

-Desactivar la búsqueda DNS

Router>ena--->inicio
Router#conf t--->ingreso a configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup--->desactivar DNS
-Nombre del router

Router(config)#hostname R2--->nombrando a R2

-Contraseña de exec privilegiado cifrada

R2(config)#enable secret class--->contraseña privilegiada

-Contraseña de acceso a la consola

R2(config)#line console 0--->configuracion línea de consola
R2(config-line)#password cisco--->contraseña de inicio
R2(config-line)#login--->activar dispositivo

-Contraseña de acceso Telnet

R2(config)#line vty 0 4--->configuración line vty
R2(config-line)#password cisco--->contraseña de consola
R2(config-line)#login--->activar dispositivo

-Cifrar las contraseñas de texto no cifrado

R2(config)#service password-encryption--->contraseña cifrada

-Habilitar el servidor HTTP

El comando no fue soportado por el simulador
-Mensaje MOTD

R2(config)#banner motd #Se prohíbe el acceso no autorizado#--->mensaje alerta

-Interfaz S0/0/0

R2(config)#inter s0/0/0--->ingreso a la interfaz
R2(config-if)#description Conexión hacia el R1--->descripción
R2(config-if)#ip address 172.16.1.2 255.255.255.252--->configuracion de direccionamiento ipv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64---> configuración de direccionamiento ipv6
R2(config-if)#no shutdown--->activar

-Interfaz S0/0/1

R2(config)#interface s0/0/1---> ingreso a la interfaz
R2(config-if)#description Conexión Hacia R3---> descripción
R2(config-if)#ip address 172.16.2.2 255.255.255.252---> configuracion de direccionamiento ipv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64---> configuración de direccionamiento ipv6
R2(config-if)#clock rate 128000--->active sincronización
R2(config-if)#no shutdown--->activar interfaz
-Interfaz G0/0 (simulación de Internet)

R2(config)#interface g0/0---> ingreso a la interfaz
R2(config-if)#description Conexión A Servidor Internet---> descripción
R2(config-if)#ip address 209.165.200.233 255.255.255.248---> configuracion de direccionamiento ipv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64---> configuración de direccionamiento ipv6
R2(config-if)#no shutdown--->activar interface

-Interfaz loopback 0 (servidor web simulado)

R2(config)#interface loopback 0--->ingreso a loopback
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 10.10.10.10 255.255.255.255--->direccionamiento a la interface
R2(config-if)#description Simulación de servidor WEB--->descripción

-Ruta predeterminada

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0--->ruta ipv4
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 g0/0--->ruta ipv6

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

-Desactivar la búsqueda DNS

Router(config)#no ip domain-lookup--->desactivar DNS

-Nombre del router

Router(config)#hostname R3--->nombrando R3

-Contraseña de exec privilegiado cifrada

R3(config)#enable secret class--->contraseña cifrada

-Contraseña de acceso a la consola

R3(config)#line console 0--->configuración línea consola

R3(config-line)#password cisco--->contraseña de consola

R3(config-line)#login --->activar dispositivo

-Contraseña de acceso Telnet

R3(config)#line vty 0 4--->configuración vty

R3(config-line)#password cisco--->contraseña de inicio

R3(config-line)#login--->activar dispositivo

-Cifrar las contraseñas de texto no cifrado

R3(config)#service password-encryption--->contraseña cifrada

-Mensaje MOTD

R3(config)#banner motd #Se prohíbe el acceso no autorizado#--->mensaje de alerta

-Interfaz loopback 4

R3(config)#interface loopback 4--->ingreso a interface loopback 4

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback4, changed state to up

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

R3(config-if)#ip address 192.168.4.1 255.255.255.0--->direccionamiento sobre interface

-Interface loopback 5

R3(config)#interface loopback 5---> ingreso a interface loopback 5

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback5, changed state to up

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

R3(config-if)#ip address 192.168.5.1 255.255.255.0--->direccionamiento sobre interface

-Interface loopback 6

R3(config)#interface loopback 6---> ingreso a interface loopback 6

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

R3(config-if)#ip address 192.168.6.1 255.255.255.0---> direccionamiento sobre interface

-Interface loopback 7

R3(config)#interface loopback 7---> ingreso a interface loopback 7

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64---> direccionamiento sobre interface

-Rutas Predeterminadas

R3(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/1--->ruta predeterminada ipv4

%Default route without gateway, if not a point-to-point interface, may impact performance

R3(config)#ipv6 route ::/0 serial0/0/1--->ruta predeterminada ipv6

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

-Desactivar la búsqueda DNS

Switch(config)#no ip domain-lookup--->desactivar DNS

-Nombre del Switch

Switch(config)#hostname S1--->nombrando S1

-Contraseña de exec privilegiado cifrada

S1(config)#enable secret class--->contraseña cifrada

-Contraseña de acceso a la consola

S1(config)#line console 0--->configuración línea de consola

S1(config-line)#password cisco--->contraseña de inicio

S1(config-line)#login--->activar dispositivo

-Contraseña de acceso Telnet

S1(config)#line vty 0 4--->configuración vty

S1(config-line)#password cisco--->contraseña de inicio

S1(config-line)#login--->activar dispositivo

-Cifrar las contraseñas de texto no cifrado

S1(config)#service password-encryption--->contraseña cifrada

-Mensaje MOTD

S1(config)#banner motd #Se prohíbe el acceso no autorizado#--->mensaje de alerta

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

-Desactivar la búsqueda DNS

Switch(config)#no ip domain-lookup--->desactivar DNS

-Nombre del Switch

Switch(config)#hostname S3--->nombrando S3

-Contraseña de exec privilegiado cifrada

S3(config)#enable secret class--->contraseña cifrada

-Contraseña de acceso a la consola

S3(config)#line console 0--->configuración línea de consola

S3(config-line)#password cisco--->contraseña de inicio

S3(config-line)#login--->activar dispositivo

-Contraseña de acceso Telnet

S3(config)#line vty 0 4--->configuración vty

S3(config-line)#password cisco--->contraseña de inicio

S3(config-line)#login--->activar dispositivo

-Cifrar las contraseñas de texto no cifrado

S3(config)#service password-encryption--->contraseña cifrada

-mensaje motd

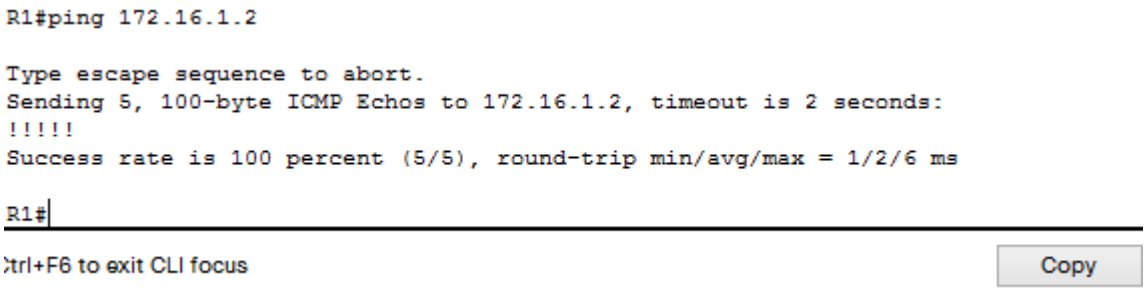
S3(config)#banner motd #Se prohíbe el acceso no autorizado#--->mensaje alerta

Paso 7: Verificar la conectividad de la red

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

-Ping desde R1 a R2 , S0/0/0 dirección 172.16.1.2

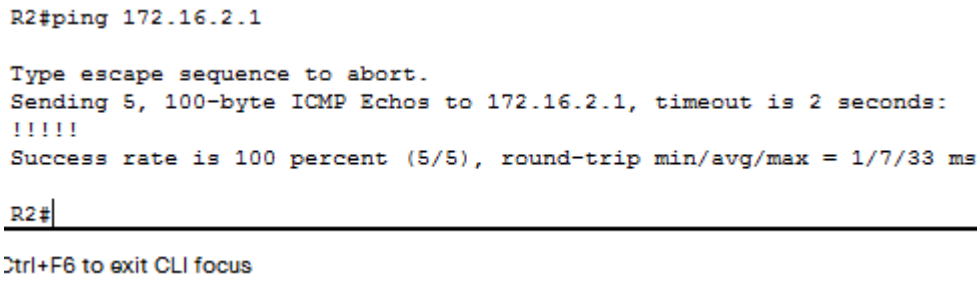
Figura 8 ping R1 a R2



Fuente :Elaboración propia

-Ping desde R2 a R3 , S0/0/1 dirección 172.16.2.1

Figura 9 ping R2 a R3



Fuente :Elaboración propia

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

Paso 1: Configurar S1

-Crear la base de datos de VLAN

S1(config)#vlan 21--->configuración vlan 21

S1(config-vlan)#name Contabilidad--->nombre de vlan

S1(config-vlan)#vlan 23--->configuración vlan 23

S1(config-vlan)#name Ingeniería--->nombre de vlan

S1(config-vlan)#vlan 99--->configuración vlan 99

S1(config-vlan)#name administración--->nombre vlan

-Asignar la dirección IP de administración.

S1(config)#interface vlan 99--->configuración vlan 99

S1(config-if)#

%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0--->direccionamiento vlan

S1(config-if)#no shut--->activar interface

-Asignar el gateway predeterminado

S1(config)#ip default-gateway 192.168.99.1--->gateway predeterminado

-Forzar el enlace troncal en la interfaz F0/3

S1(config)#interface f0/3--->ingreso a interface

S1(config-if)#switchport mode trunk--->interface troncal

S1(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

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

-Forzar el enlace troncal en la interfaz F0/5

S1(config)#interface f0/5--->ingreso interface

S1(config-if)#switchport mode trunk--->interface troncal

S1(config-if)#switchport trunk native vlan 1--->vlan nativa para enlaces

-Configurar el resto de los puertos de acceso

S1(config)#interface range f0/1-2,f0/4,f0/6-24,g0/1-2--->interfaces a la vez de rango

S1(config-if-range)#switchport mode Access--->acceso interfaces seleccionadas

-Asignar F0/6 a la VLAN 21

S1(config-if)#interface f0/6--->ingreso a interface

S1(config-if)#switchport access vlan 21--->interface de vlan

-Apagar todos los puertos sin usar

S1(config)#interface range f0/1-2,f0/4,f0/7-24,g0/1-2---> interfaces a la vez de rango

S1(config-if-range)#shutdown--->apagan las interfaces

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

-Crear la base de datos de VLAN

S3(config)#vlan 21--->configuración vlan 21

S3(config-vlan)#name Contabilidad--->nombre de vlan

S3(config-vlan)#vlan 23--->configuración vlan 23

S3(config-vlan)#name Ingeniería--->nombre de vlan

S3(config-vlan)#vlan 99--->configuración vlan 99

S3(config-vlan)#name Administración--->nombre de vlan

-Asignar la dirección IP de administración

S3(config)#interface vlan 99--->configuración vlan

S3(config-if)#

%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0--->direccionamiento sobre vlan

-Asignar el gateway predeterminado.

S3(config)#ip default-gateway 192.168.99.1--->gateway predeterminado

-Forzar el enlace troncal en la interfaz F0/3

S3(config)#interface f0/3--->ingreso interface

S3(config-if)#switchport mode trunk--->interface troncal

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

-Configurar el resto de los puertos de acceso

S3(config-if)#interface range f0/1-2,f0/4-24,g0/1-2--->interfaces de rango

S3(config-if-range)#switchport mode access--->acceso a las interfaces

-Asignar F0/18 a la VLAN 21

S3(config)#interface f0/18--->ingresó a interface

S3(config-if)#switchport access vlan 21--->interface vlan

-Apagar todos los puertos sin usar

S3(config)#interface range f0/1-2,f0/4-17,f0/19-24,g0/1-2--->selección de interfaces

S3(config-if-range)#shutdown--->apagar interfaces

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

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

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

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

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

-Configurar la subinterfaz 802.1Q .21 en G0/1

R1(config)#interface g0/1.21--->configuración interface virtual

R1(config-subif)#description LAN Contabilidad--->descripción

R1(config-subif)#encapsulation dot1q 21--->vlan especifica

R1(config-subif)#ip address 192.168.21.1 255.255.255.0--->direccionamiento interface

-Configurar la subinterfaz 802.1Q .23 en G0/1

R1(config)#interface g0/1.23--->configuración interface virtual

R1(config-subif)#description LAN Ingeniería--->descripción

R1(config-subif)#encapsulation dot1q 23--->vlan especifica

R1(config-subif)#ip address 192.168.23.1 255.255.255.0--->direccionamiento de interface

-Configurar la subinterfaz 802.1Q .99 en G0/1

R1(config-subif)#interface g0/1.99--->configuración interface virtual

R1(config-subif)#description LAN Administración--->descripción

R1(config-subif)#encapsulation dot1q 99--->vlan especifica

R1(config-subif)#ip address 192.168.99.1 255.255.255.0--->direccionamiento de interface

-Activar la interfaz G0/1

R1(config-subif)#interface g0/1--->configuración de interface

R1(config-if)#no shutdown--->activar interface

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

Paso 4: Verificar la conectividad de la red

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

-Ping desde S1 a R1, dirección VLAN 99 , IP 192.168.99.1

figura 10 ping S1 a R1

```
S1>ena
Password:
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms

S1#
```

Fuente :Elaboración propia

-Ping desde S3 a R1, dirección VLAN 99 , IP 192.168.99.1

Figura 11 S3 a R1

```
S3>ena
Password:
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/7/12 ms

S3#
```

Fuente :Elaboración propia

-Ping desde S1 a R1, dirección VLAN 21 , IP 192.168.21.**1**

figura 12 S1 a R1

```
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 = 0/0/1 ms

S1#
```

Fuente :Elaboración propia

-Ping desde S3 a R1, dirección VLAN 23 , IP 192.168.23.1

figura 13 S3 a R1

```
S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

S3#
```

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:

Configurar OSPF área 0 b. Anunciar las redes conectadas directamente
Establecer todas las interfaces LAN como pasivas
Desactive la sumarización automática

R1(config)#router ospf 1--->enrutamiento OSPF

R1(config-router)#network 172.16.1.0 0.0.0.3 area 0---> habilitar OSPF

R1(config-router)#network 192.168.21.0 0.0.0.255 area 0---> habilitar OSPF

R1(config-router)#network 192.168.23.0 0.0.0.255 area 0---> habilitar OSPF

R1(config-router)#network 192.168.24.0 0.0.0.255 area 0---> habilitar OSPF

R1(config-router)#passive-interface g0/1.21--->mensajes de routing a la interface

R1(config-router)#passive-interface g0/1.23---> mensajes de routing a la interface

R1(config-router)#passive-interface g0/1.99---> mensajes de routing a la interface

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Configurar OSPF área 0 b. Anunciar las redes conectadas directamente

Establecer todas las interfaces LAN (loopback) como pasivas

Desactive la sumarización automática

R2(config)#router ospf 1---> enrutamiento OSPF

R2(config-router)#network 172.16.1.0 0.0.0.3 area 0---> habilitar OSPF

R2(config-router)#

02:26:37: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0 from LOADING to FULL, Loading Done

R2(config-router)#network 172.16.1.0 0.0.0.3 area 0---> habilitar OSPF

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

R2(config-router)#network 10.10.10.10 0.0.0.0 area 0---> habilitar OSPF

R2(config-router)#passive-interface loopback 0--->Evita los mensajes de routing a través de interface

Paso 3: Configurar OSPF en el R3

La configuración del R3 incluye las siguientes tareas:

Configurar OSPF área 0 b. Anunciar las redes IPv4 conectadas directamente

Establecer todas las interfaces LAN IPv4 (loopback) como pasivas

Desactive la sumarización automática

R3(config)#router ospf 1---> enrutamiento OSPF

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

R3(config-router)#

01:34:51: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/1 from LOADING to FULL, Loading Done

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

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

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

R3(config-router)#passive-interface loopback 4--->Evita los mensajes de routing a través de interface

R3(config-router)#passive-interface loopback 5---> Evita los mensajes de routing a través de interface

R3(config-router)#passive-interface loopback 6---> Evita los mensajes de routing a través de interface

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:

¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?

R1#show ip protocols

Figura 14 show protocols

```
R1#show ip protocols

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 192.168.99.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.24.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10           110      00:02:25
    192.168.6.1           110      00:02:06
    192.168.99.1          110      00:06:27
  Distance: (default is 110)
 --More--
```

Fuente :Elaboración propia

-¿Qué comando muestra solo las rutas OSPF?

R1#show ip route ospf

Figura 15 ip route ospf

```
R1#show ip route ospf
      10.0.0.0/32 is subnetted, 1 subnets
O        10.10.10.10 [110/65] via 172.16.1.2, 00:06:44, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O        172.16.2.0 [110/128] via 172.16.1.2, 00:07:00, Serial0/0/0
      192.168.4.0/32 is subnetted, 1 subnets
O        192.168.4.1 [110/129] via 172.16.1.2, 00:03:24, Serial0/0/0
      192.168.5.0/32 is subnetted, 1 subnets
O        192.168.5.1 [110/129] via 172.16.1.2, 00:03:14, Serial0/0/0
      192.168.6.0/32 is subnetted, 1 subnets
O        192.168.6.1 [110/129] via 172.16.1.2, 00:03:14, Serial0/0/0

R1#
```

Fuente :Elaboración propia

-¿Qué comando muestra la sección de OSPF de la configuración en ejecución?

R1#show run | section ospf router ospf 1

Figura 16 show run

```
R1#show run | section ospf
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet0/1.21
 passive-interface GigabitEthernet0/1.23
 passive-interface GigabitEthernet0/1.99
 network 172.16.1.0 0.0.0.3 area 0
 network 192.168.21.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
 network 192.168.24.0 0.0.0.255 area 0
```

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:

-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--->dirección para reservarlas a futuro

-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---> dirección para reservarlas a futuro

-Crear un pool de DHCP para la VLAN 21.

R1(config)#ip dhcp pool ACCT--->pool dhcp

R1(dhcp-config)#network 192.168.21.0 255.255.255.0--->red de vlan 21

R1(dhcp-config)#default-router 192.168.21.1--->gateway predeterminado pool

R1(dhcp-config)#dns-server 10.10.10.10--->dns pool

R1(dhcp-config)#ip domain-name ccna-sa.com---> nombre del dominio

-Crear un pool de DHCP para la VLAN 23

R1(config)#ip dhcp pool ENGNR--->crear pool dhcp

R1(dhcp-config)#network 192.168.23.0 255.255.255.0--->red de la vlan 23

R1(dhcp-config)#default-router 192.168.23.1---> gateway predeterminado a pool

R1(dhcp-config)#dns-server 10.10.10.10--->dns a pool

R1(dhcp-config)#ip domain-name ccna-sa.com--->nombre de dominio

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

La configuración del R2 incluye las siguientes tareas

-Crear una base de datos local con una cuenta de usuario

R2(config)#username web user privilege 15 secret cisco 12345--->usuario con privilegio y clave encriptada

-Crear una NAT estática al servidor web**.**

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237--->dirección local interna y global

-Asignar la interfaz interna y externa para la NAT estática

R2(config)#interface g0/0--->ingreso a interface

R2(config-if)#ip nat outside--->interface externa

R2(config-if)#interface s0/0/0--->ingreso a interface

R2(config-if)#ip nat inside--->interface como interna

R2(config-if)#interface s0/0/1--->interface

-Configurar la NAT dinámica dentro de una ACL privada Lista de acceso: **1**

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255--->interface entrante y saliente

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

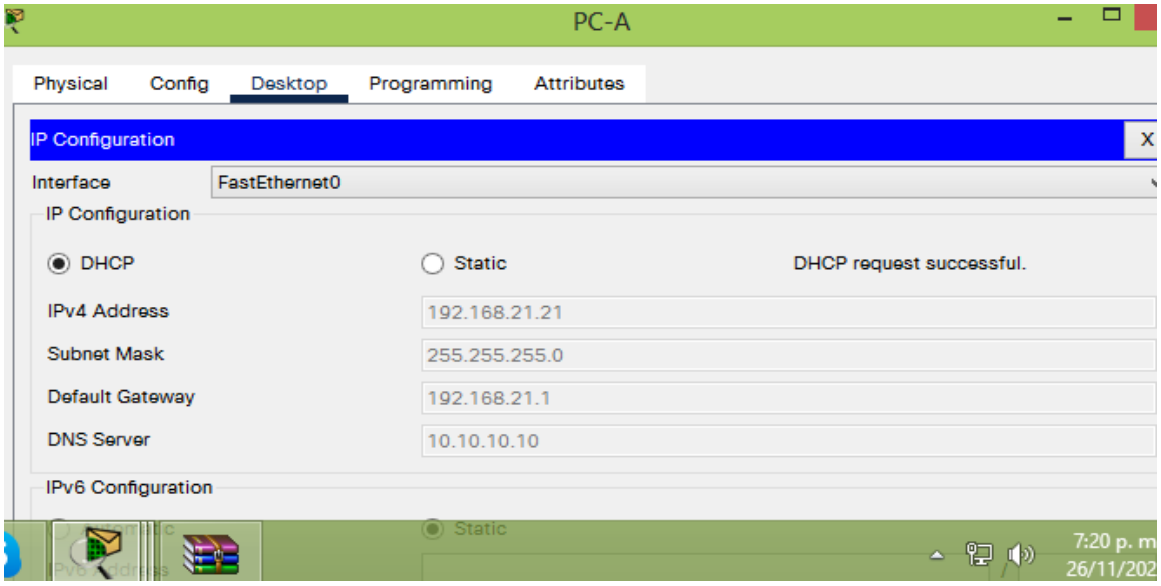
-Defina el pool de direcciones IP públicas utilizables.

R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248

Paso 3: Verificar el protocolo DHCP y la NAT estática

-Verificar que la PC-A haya adquirido información de IP del servidor de DHCP asignado con éxito

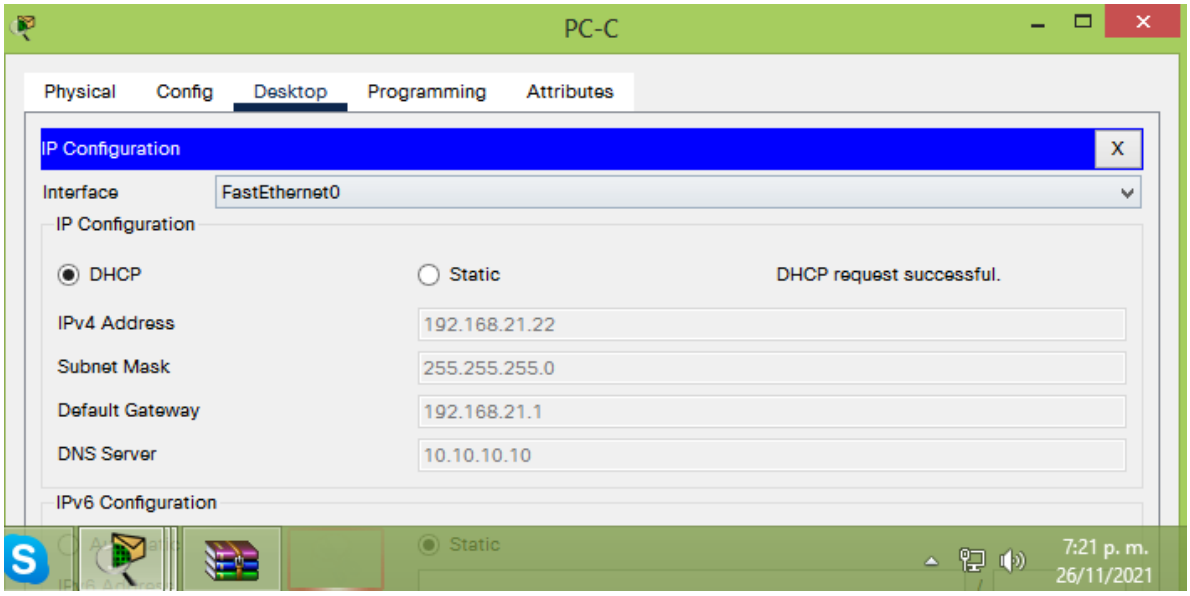
Figura 17 PC-A DHCP



Fuente :Elaboración propia

-Verificar que la PC-C haya adquirido información de IP del servidor de DHCP asignado con éxito

Figura 18 PC-C DHCP



Fuente :Elaboración propia

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco 12345

Parte 6: Configurar NTP

-Ajuste la fecha y hora en R2.

R2#clock set 9:00:00 5 march 2016---> fecha y hora establecida

-Configure R2 como un maestro NTP.

R2(config)#ntp master 5--->protocolo de tiempo

-Configurar R1 como un cliente NTP. Servidor R2

R1(config)#ntp server 172.16.1.2--->servidor r2 a r1

-Configure R1 para actualizaciones de calendario periódicas con hora NTP.

R1(config)#ntp update-calendar--->actualización de calendario

-Verifique la configuración de NTP en R1.

Figura 19 show ntp associations

```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offse
disp
 ~172.16.1.2    127.127.1.1     5    2        16      17     10.00
726213705407.00   0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
```

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 a. 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--->nombre ACL

R2(config-std-nacl)#permit host 172.16.1.1--->dirección R1 permite conexión

-Aplicar la ACL con nombre a las líneas VTY

R2(config)#line vty 0 15--->interface vty

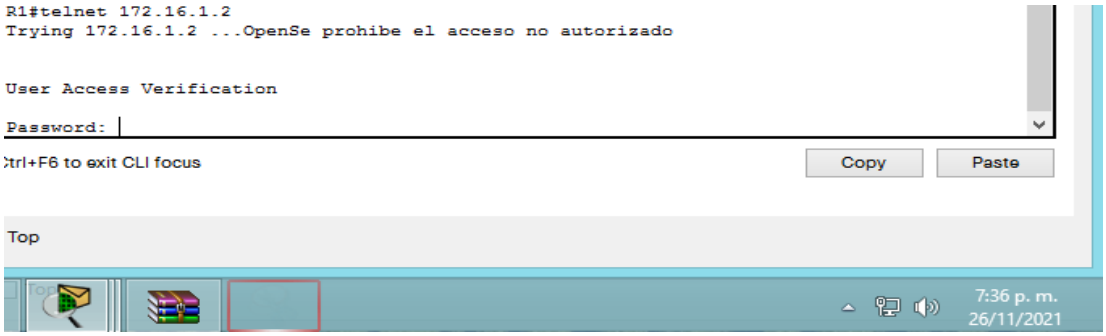
R2(config-line)#access-class ADMIN-MGT in

-Permitir acceso por Telnet a las líneas de VTY

R2(config-line)#transport input telnet--->conexiones a líneas vty

-Verificar que la ACL funcione como se espera

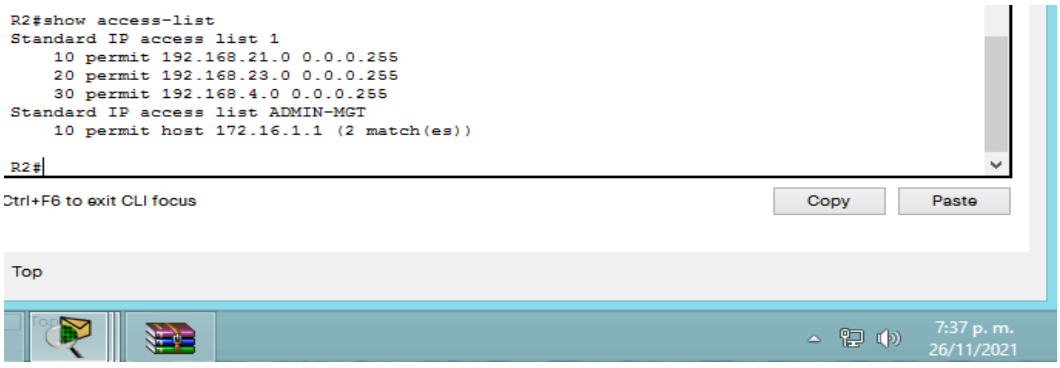
Figura 20 telnet 172.16.1.2



Fuente :Elaboración propia

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente a. Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

Figura 21 access list



Fuente :Elaboración propia

-Restablecer los contadores de una lista de acceso

el comando no funciona

-¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?

Figura 22 ip interface

```
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 209.165.200.233/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
```

Fuente :Elaboración propia

-¿Con qué comando se muestran las traducciones NAT?

Figura 1.23ip nat traslation

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

Fuente :Elaboración propia

CONCLUSIONES

En el desarrollo de este escenario, con diferentes entornos en este documento aprendí que esta actividad se puede demostrar mis habilidades y conocimientos en CISCO con la realización de una configuración básica a routers, Switch etc. aplicando la herramienta de Packet Tracer con un problema propuesto y darle la solución, con sus diferentes protocolos y topologías.

Entender los beneficios y ayuda que me da la implementación de red al configurar, los diferentes dispositivos manejados, para tener una mejor optimización del uso de estas ,lo cual me ayudo a ser más analítico con los comandos, las redes, las direcciones, equipos, cableado y muchas más cosas que muestran lo aprendido en este curso.

Fue importante poder realizar análisis en cada topología y diseño de la red, los cuales me llevaron a escoger los dispositivos correctos que se adecuarán a el escenario y su respectiva configuración dando a cada uno de ellos una solución correcta y adecuada.

Los conocimientos que adopte estos meses para el diplomado me a echo identificar la importancia de la red , con sus diferentes protocolos, enrutamientos ,direccionamientos, vlan, ospf, etc. desarrollar todo mi potencial y ejerciendo mis habilidades como ingeniero.

BIBLIOGRAFÍA

[*interface Range Specification. (n.d.). Recuperado el 17 de Julio, 2021, from Cisco.com*

Administración de vlan.dat en switches Cisco Catalyst que ejecutan el software Cisco IOS. (n.d.). recuperado el 17 de julio, 2021, desde Cisco.com

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

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

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

BAREÑO, Gutiérrez, R., 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.

CISCO, Networking Academy. "Packet Tracer: Configuración de los parámetros iniciales del switch". {En línea}. {8 mayo de 2020} disponible en: (https://staticcourse-assets.s3.amazonaws.com/ITN6/es/index.html#2.2.3.3).

CISCO, Networking Academy. "Packet Tracer: Situación de división en subredes 1". {En línea. {8 mayo de 2020} disponible en: (https://static-courseassets.s3.amazonaws.com/ITN6/es/index.html#9.1.4.6).

CISCO, Networking Academy. "Práctica de laboratorio: configuración de redes VLAN y enlaces troncales". {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3.2.2.5).

Configuración de EtherChannel y Trunking 802.1Q entre Switches de Configuración Fija Catalyst L2 y un Router (Ruteo InterVLAN). (s/f). Recuperado el 10 de junio de 2021, de Cisco.com

del Castillo, A. (s/f). Calculadora IP - Subneteo Online - Redes - Hosts - classful / cidr / vlsm. Recuperado el 10 de junio de 2021, de Calculadora-redes.com

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.

IP Addressing and Subnetting for New Users. (s/f). Recuperado el 6 de junio de 2021, de Cisco.com

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In *2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI)* (pp. 1-6). IEEE.