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

JAIME JESUS OSPINO DELGADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
SANTA ANA
2021

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

JAIME JESUS OSPINO DELGADO

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

DIRECTOR:
RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
SANTA ANA
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del jurado

_____

Firma del jurado

SANTA ANA, 28 de noviembre de 2021

AGRADECIMIENTOS

Quiero expresar mis más sinceros agradecimientos a Dios, a mi familia que hicieron posible lograr alcanzar este sueño que ha venido acompañado de mucho esfuerzo y dedicación

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

La simulación y documentación de dos escenarios propuestos cada uno con un tipo de configuración especiales fueron necesarias en el funcionamiento y requerimiento para la problemática planteada en un entorno virtual, pero que puede ser extrapolado a nivel comercial, industrial entre otros campos, para lograrlo se empleó la tecnología dispuesta por CISCO. Así pues, para el primere escenario se configuraron los equipos mostrados en la topología ser realizó un direccionamiento IPv4 para las LAN propuestas.

Seguidamente, en el segundo escenario el cual está compuesto por una pequeña red se configuraron los equipos para poder recibir una conectividad IPv4 e IPv6 bajo los lineamientos de los protocolos de configuración OSPF, DHCP y NTP principalmente.

El trabajo se realiza con el objetivo de dar una visión preliminar de dos escenarios propuestos de lo que como producto final se obtuvo un aporte a la solución del primer escenario para el cual se adquieren destrezas en cuanto a la configuración de los equipos presentados en la tipología y las respectivas direcciones solicitadas.

Palabras Clave: cisco, ccna, dhcp, ntp, ospf.

ABSTRACT

The simulation and documentation of two scenarios proposed each with a special type of configuration were necessary in the operation and requirement for the problem posed in a virtual environment, but that can be extrapolated to commercial, industrial level among other fields, to achieve this the technology provided by CISCO was used. Thus, for the first scenario, the computers shown in the topology were configured to be made an IPv4 address for the proposed LANs.

Then, in the second scenario, which is composed of a small network, the computers were configured to receive IPv4 and IPv6 connectivity under the guidelines of the OSPF, DHCP and NTP configuration protocols mainly.

The work is carried out with the aim of giving a preliminary vision of two proposed scenarios of what as a final product was obtained a contribution to the solution of the first scenario for which skills are acquired in terms of the configuration of the equipment presented in the typology and the respective addresses requested.

Keywords: cisco, ccna, dhcp, ntp, ospf.

INTRODUCCIÓN

En la actualidad el procesamiento de datos, así como también la administración de estos han generado a la industria la búsqueda de la capacitación de personal apto para poder ser más competitivos en el mercado.

Por otro lado, las certificaciones CISCO facilitan las herramientas para lograr capacitarse en el diseño y soporte de redes logrando dar las habilidades necesarias para desempeñarse en este campo

El siguiente documento presenta la información que se ha obtenido primeramente mediante el desarrollo del primer ejercicio práctico, así como también se realizan las observaciones técnicas, las limitaciones y al final del documento se presentan las conclusiones obtenidas y las referencias bibliográficas que sirvieron de consulta

DESARROLLO

1. ESCENARIO 1

1.1. Parte 1. Construya la Red

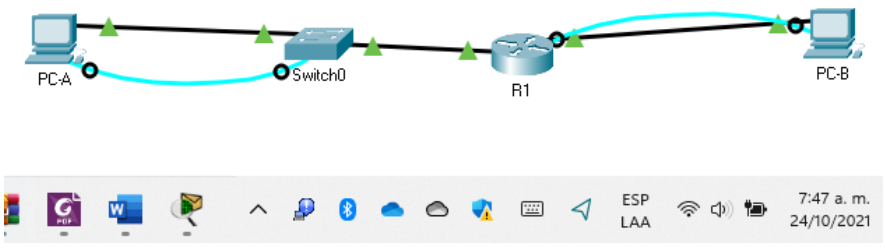
En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Figura 1. Topología escenario 1

Fuente propia

En la figura 2 se muestra la implementación que se realizó en el software packet tracer v8.0.0.0212

Figura 2. Implementación del escenario 1 en el software packet tracer



Fuente propia

1.2. 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.

De acuerdo con la información suministrada el direccionamiento será igual a 192.168.17.0 y la tabla de direccionamiento se muestra en la tabla 1.

Tabla 1. Tabla de direccionamiento

Ítem	Requerimiento
Dirección de Red	192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1
R1 G0/0/0	Primera dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1
PC-A	Última dirección de host de la subred LAN1
PC-B	Última dirección de host de la subred LAN2

Fuente propia

Por tanto, realizando los respectivos cálculos para obtener un host Subred LAN1 de 100 y host Subred LAN2 de 50 se procede de la siguiente manera:

$$2^7 - 2 = 126$$

$$2^6 - 2 = 62$$

Se obtiene que las direcciones son las que se presentan en la tabla 2.

Tabla 2. direccionamiento

	Dirección de red	Mascara	Primer IP	Broadcast
LAN1	192.168.17.128	255.255.255.128	192.168.17.1	192.168.17.127
LAN2	192.168.17.192	255.255,255,192	192.168.17.129	192.168.17.191

Fuente propia

Entonces, una vez obtenidos los datos mostrados en la tabla 2 se procede a realizar el llenado de la tabla 1 y se obtiene la tabla 3.

Tabla 3. direccionamiento para el escenario 1

Ítem	Requerimiento
R1 G0/0/1	192.168.17.1
R1 G0/0/0	192.168.17.129
S1 SVI	192.168.17.2
PC-A	192.168.17.126
PC-B	192.168.17.190

Fuente propia

1.3. Parte 3: Configure aspectos básicos

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

1.3.1. Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4. tareas realizadas en el PC-B

Tarea	Especificación
Desactivar la búsqueda DNS	para realizar la desactivación de la búsqueda se hace uso de los siguientes comandos: Router(config)#no ip Router(config)#no ip domain
Nombre del router	La asignación del nombre R1 se emplea: Router(config)#ho R1
Nombre de dominio	El nombre del dominio es asignado empleado: R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Para accede al modo privilegiado se sigue: R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit R1(config)#security pass

Establecer la longitud mínima para las contraseñas	Para declarar una longitud mínima de 10 caracteres se emplea el comando security passwords min-length, por tanto: R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos locales	Para la creación del usuario con contraseña de datos local se usan los comandos username admin pass. R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Para configura la sesión VTY se usa line VTY 0 4 R1(config)#line VTY 0 4 R1(config-line)#password admin1pass R1(config-line)#login local
Configurar VTY solo aceptando SSH	Seguidamente para configura que solo sea aceptado SSH se usa transport input R1(config-line)#transport input SSH
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseña se usa service password-encryption R1(config)#service password-encryption
Configure un MOTD Banner	En la configuración del banner se usa banner motd, se debe tener en cuenta que el banner debe ir entre #--# R1(config)#banner motd #Este es el banner de Jaime#
Configurar interfaz G0/0/0	Para establecer la descripción, la dirección IPv4 y activar la interfaz, se emplean los siguientes comandos R1(config)#int g0/0/0 R1(config-if)#ip address 192.168.17.129 255.255.255.192

	R1(config-if)#description #interfaz de LAN2# R1(config-if)#no shutdown R1(config-if)#exit Las direcciones IP son las que se muestran en la tabla 3
Configurar interfaz G0/0/1	El igual que como se procedió en la anterior sección se realiza para la interfaz G0/0/1 R1(config)#interface g0/0/1 R1(config-if)#description #Interfaz de LAN1# R1(config-if)#ip address 192.168.17.1 255.255.255.128 R1(config-if)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA	Finalmente, para generar la clave de cifrado RSA se sigue: R1(config)#ip domain name ccna-lab.com R1(config)#crypto key generate RSA The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] R1(config)#exit *Mar 1 0:14:12.875: %SSH-5-ENABLED: SSH 1.99 has been enabled

	R1# %SYS-5-CONFIG_I: Configured from console by console wr Building configuration... [OK] R1#

Fuente propia

Tabla 5. Configuración el PC-A

Tarea	Especificación
Desactivar la búsqueda DNS.	S1(config)#ip default-gateway 192.168.17.1
Nombre del switch	Switch(config)#ho S1
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config-line)#exit S1(config)#username admin password dmin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line VTY 0 15 S1(config-line)#password admin1pass S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input SSH S1(config-line)#exit

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #Este es el S de Jaime#
Generar una clave de cifrado RSA	S1(config)#crypto key generate Rsa The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configurar la interfaz de administración (SVI)	S1(config)#int vlan1 *Mar 1 0:7:20.32: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if)#ip address 192.168.17.2 255.255.255.128 S1(config-if)#no shutdown %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Configuración del gateway predeterminado	S1(config)#ip de S1(config)#ip default-gateway 192.168.17.1 S1(config)#exit

Fuente propia

1.3.2. Paso 2. Configurar los equipos

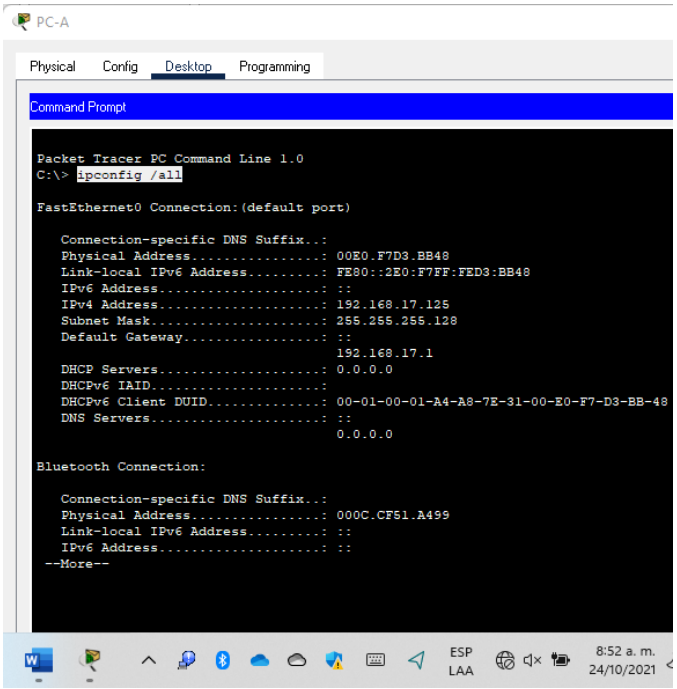
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 6. PC-A Network Configuration

Descripción	Como se puede observar en la figura 1 o 2 el PC-A se encuentra conectado al R1
Dirección física	00E0.F7D3.BB48
Dirección IP	192.168.17.125
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.17.1

Fuente propia

Figura 3. configuración de red para el PC-A



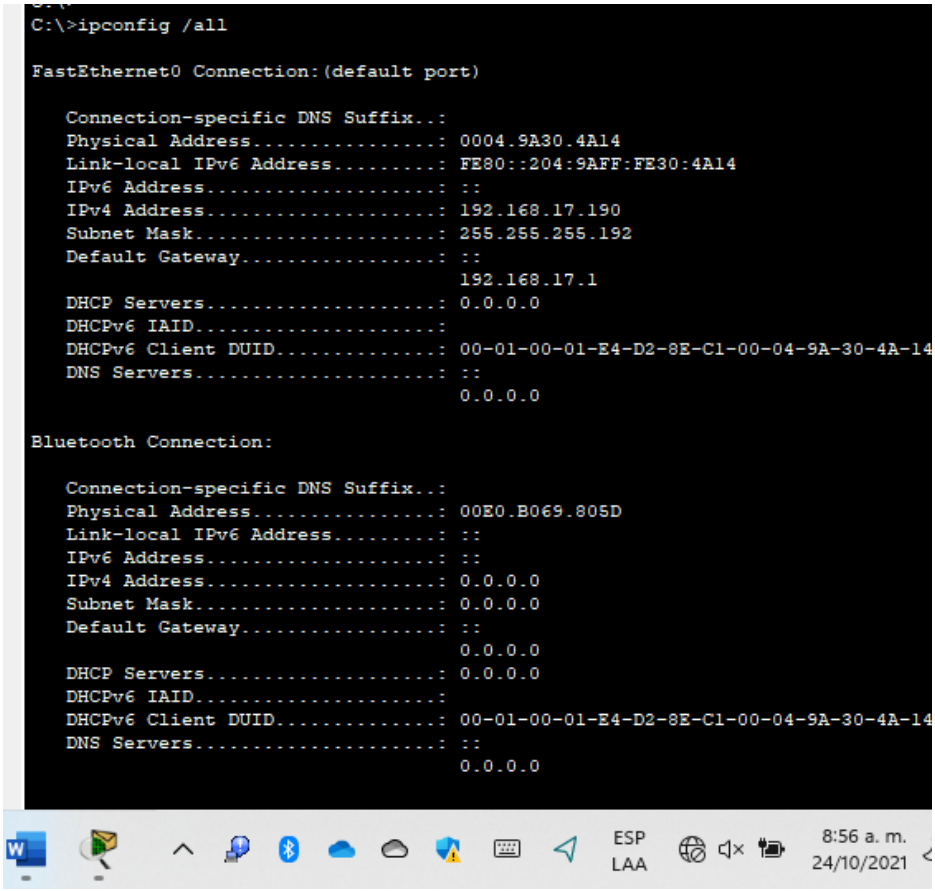
Fuente propia

Tabla 7. PC-B Network Configuration

Descripción	Como se puede observar en la figura 1 o 2 el PC-B se encuentra conectado a S1
Dirección física	0004.9A30.4A14
Dirección IP	192.168.17.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.17.1

Fuente propia

Figura 4. PC-B Network Configuration



Fuente propia

2. ESCENARIO 2

2.1. Parte 1: Inicializar dispositivos

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

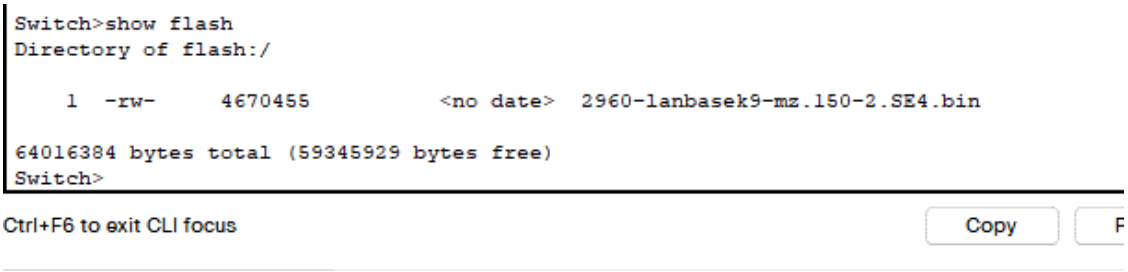
Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 8. Inicialización cargue de los routers switches

Tarea Comando de IOS	Tarea Comando de IOS
Eliminar el archivo startup-config de todos los routers	Para cada uno de los routers se aplica la siguiente línea de código una vez se haya habilitado el dispositivo Router#erase startup-config
Volver a cargar todos los routers	Para volver a cargar cada uno de los routers se realizar la siguiente línea Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	De igual manera que como se procedió con la configuración de los routers se procede de la misma manera para cada uno de los switches Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash

Fuente propia

Figura 5. Verificación de la base de datos de VLAN



Fuente propia

2.2. Parte 2: Configurar los parámetros básicos de los dispositivos

2.2.1. Paso 1: Configurar la computadora de Internet

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

Tabla 9. Configuración de la computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente propia

2.2.2. Paso 2: Configurar R1

Tabla 10. Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#ho R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class R1(config)#line console 0
Contraseña de acceso a la consola	R1(config-line)#password cisco R1(config-line)#login R1(config-line)#line vty 0 4
Contraseña de acceso Telnet	R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #se prohibe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#ipv6 unicast-routing R1(config)#int s0/0/0 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
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 S0/0/0 R1(config)#ipv6 route ::/0 S0/0/0

Fuente propia

2.2.3. Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 11. configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Para asignar el nombre de R1 se usa la siguiente línea de código de forma derivada Router(config)#ho R2
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class R1(config)#line console 0
Contraseña de acceso a la consola	R1(config-line)#password cisco R1(config-line)#login R1(config-line)#line vty 0 4
Contraseña de acceso Telnet	R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	R1(config)#banner motd #se prohibe el acceso no autorizado#
Interfaz S0/0/0	R2(config)#ipv6 unicast-routing R2(config)#int s0/0/0 R2(config-if)#ip add

	R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 add R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#description conexión entre R3 - R1 R2(config-if)#no sh
Interfaz S0/0/1	R2(config)#int s0/0/1 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
Interfaz G0/0 (simulación de Internet)	R2(config)#ipv6 unicast-routing R2(config)#int G0/0 R2(config-if)#ip add R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 add R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64 R2(config-if)#no sh
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#description servidor WEB R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0 R2(config)#ipv6 route ::/0 G0/0

Fuente propia

2.2.4. Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas

Tabla 12. configuración en R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Para asignar el nombre de R1 se usa la siguiente línea de código de forma derivada Router(config)#ho R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class R3(config)#line console 0
Contraseña de acceso a la consola	R3(config-line)#password cisco R3(config-line)#login R3(config-line)#line vty 0 4
Contraseña de acceso Telnet	R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #acceso restringido#
Interfaz S0/0/1	R3(config)#int s0/0/1 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
Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#ip add 192.168.4.1 255.255.255.0

	R3(config-if)#exit
Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if)#ip add 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 S0/0/1 R3(config)#ipv6 route ::/0 S0/0/1

Fuente propia

2.2.5. Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas

Tabla 13. configuración del switch S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Para asignar el nombre de S1 se usa la siguiente línea de código de forma derivada Switch(config)#ho S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class S1(config)#line console 0
Contraseña de acceso a la consola	S1(config-line)#password cisco S1(config-line)#login

	S1(config-line)#line vty 0 15
Contraseña de acceso Telnet	S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #acceso restringido#

Fuente propia

2.2.6. Paso 6: Configurar el S3

Figura 6. configuración del switch S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Para asignar el nombre de S3 se usa la siguiente línea de código de forma derivada Switch(config)#ho S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class S3(config)#line console 0
Contraseña de acceso a la consola	S3(config-line)#password cisco S3(config-line)#login S3(config-line)#line vty 0 15
Contraseña de acceso Telnet	S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #acceso restringido#

Fuente propia

2.2.7. Paso 7: Verificar la conectividad de la red

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

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 14. Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	R1#ping 172.16.1.2	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/13 ms
R2	R3, S0/0/1	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 = 1/2/8 ms

PC de Internet	Gateway predeterminado	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<1ms 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 = 1ms, Average = 0ms

Fuente propia

Figura 7. Verificación de la conectividad de la red desde R2 hasta R3

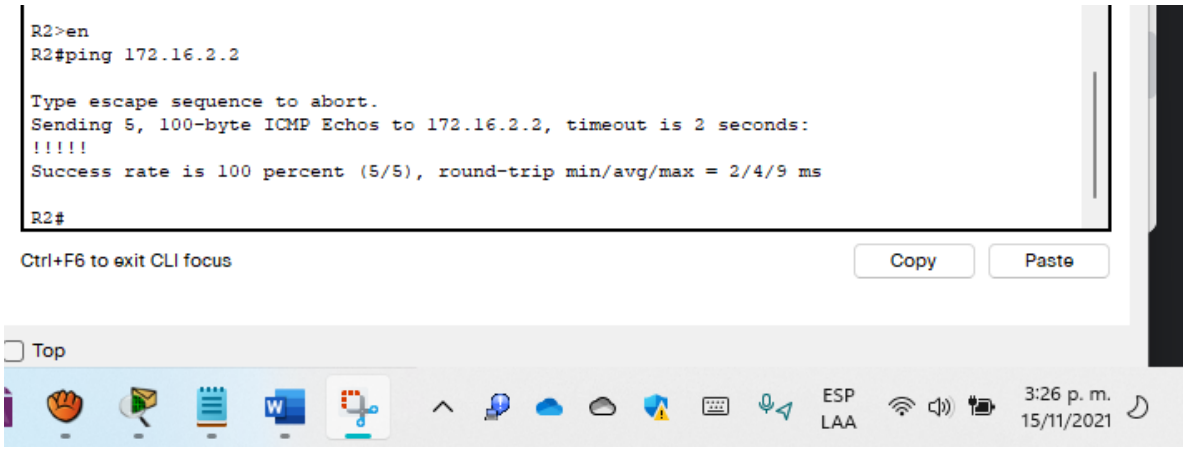
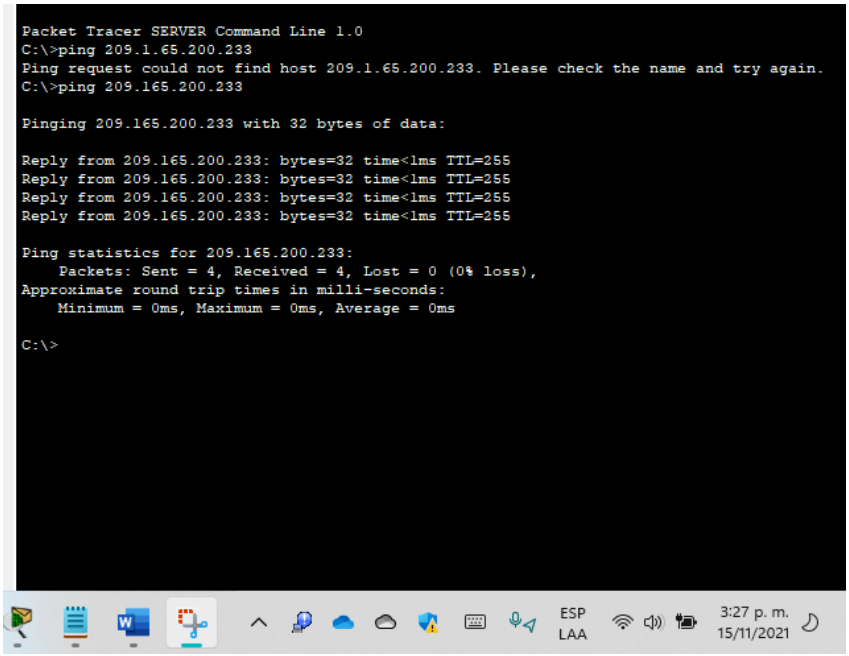


Figura 8. ping hacia default gateway



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

2.3.1. Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas

Tabla 15. Configuración de la seguridad del switch, las VLAN y el routing entre VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Switch(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name administracion
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip add 192.16.99.2 255.255.255.0 S1(config-if)#no sh S1(config-if)#exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#sw mode trunk
Forzar el enlace troncal en la interfaz F0/5	S1(config)#int f0/5 S1(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	S1(config)#int range f0/1- f0/2 S1(config-if-range)#sw mode access S1(config-if-range)#int range f0/7- f0/24 S1(config-if-range)#sw mode access
Asignar F0/6 a la VLAN 21	S1(config-if)#int f0/6 S1(config-if)#sw mode access S1(config-if)#sw access vlan 21
Apagar todos los puertos sin usar	S1(config)#int range f0/7 - f0/24 S1(config-if-range)#sh

2.3.2. Paso 2: Configurar el S3

Tabla 16. configuración de S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	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
Asignar la dirección IP de administración	S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config-if)#no sh
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#sw mode trunk S3(config-if)#sw trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S3(config)#int range f0/1 - f0/2 S3(config-if-range)#sw mode access S3(config-if-range)#int ran f0/7 - f0/24 S3(config-if-range)#sw MODE ACCess S3(config-if-range)#exit
Asignar F0/18 a la VLAN 21	S3(config)#int f0/18 S3(config-if)#sw acc vlan 21
Apagar todos los puertos sin usar	S3(config-if)#int range f0/7 - f0/17 S3(config-if-range)#sh

Fuente propia

2.3.3. Paso 3: Configurar R1

Tabla 17. configuración de R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/1.21 R1(config-subif)#description Lan contabilidad R1(config-subif)#enc dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#int g0/1.23 R1(config-subif)#desc Lan ingenieira R1(config-subif)#en dot1q 23 R1(config-subif)#ip add 192.168.23.1 255.255.255.0

	R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#int g0/1.99 R1(config-subif)#description LAn administracion R1(config-subif)#en dot1q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no sh

Fuente propia

2.3.4. Paso 4: Verificar la conectividad de la red

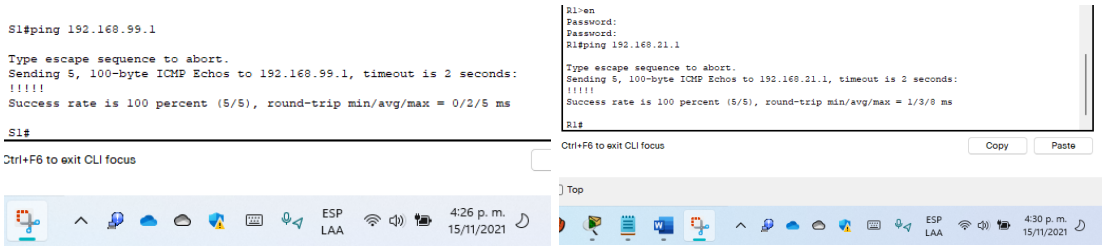
Tabla 18. Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	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 = 3/8/13 ms
S3	R1, dirección VLAN 99	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 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1	R1, dirección VLAN 21	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 = 0/2/4 ms
S3	R1, dirección VLAN 23	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 = 0/1/5 ms

Fuente propia

Figura 9. Verificación de la conectividad de la red



Fuente propia

2.4. Parte 4: Configurar el protocolo de routing dinámico OSPF

2.4.1. Paso 1: Configurar OSPF en el R1

Tabla 19. Configuración de OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 9
Anunciar las redes conectadas directamente	R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)#net 172.16.1.0 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1 R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	no se puede hacer en ospf

Fuente propia

2.4.2. Paso 2: Configurar OSPF en el R2

Tabla 20. Configuración de OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 9
Anunciar las redes conectadas directamente	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 Nota: se omitió la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	No se puede hacer en este sistema de enrutamiento

Fuente propia

2.4.3. Paso 3: Configurar OSPFv3 en el R2

Tabla 21. Configuración de OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#int s0/2/0 R2(config-if)#ipv6 ospf 8 area 0 R2(config-if)#exit R2(config)#int s0/0/1 R2(config-if)#ipv6 ospf 8 area 0 R2(config-if)#exit R2(config)#int g0/0

	R2(config-if)#ipv6 ospf 8 area 0
Anunciar redes IPv4 conectadas directamente	No es posible realizar redes IPv4 conectadas directamente para esta red
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	No se puede realizar para la red ipv6, la loopback no tiene direcciones bajo IPV6.
Desactive la sumarización automática.	En este protocolo eso no se hace para eso se coloca la wildcard y en IPV6 no se hace.

Fuente propia

2.4.4. Paso 4: Verificar la información de OSPF

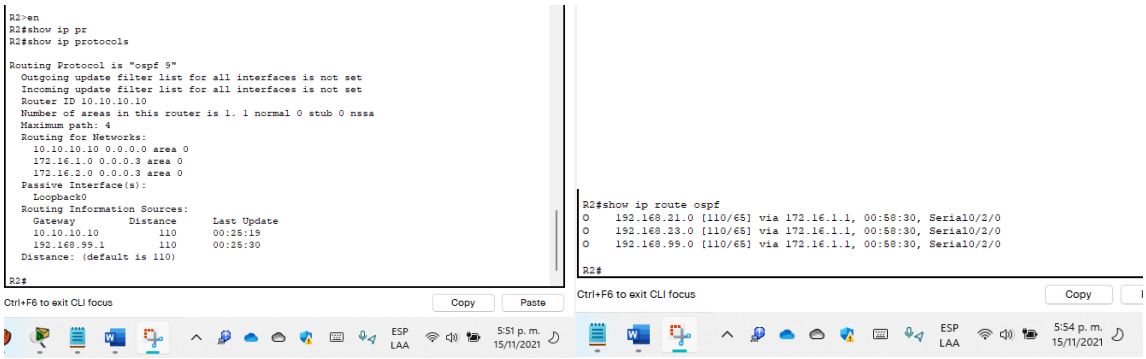
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información

Tabla 22. información de OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R2#show ip protocols R2#show ip route ospf R2#show running-config
¿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 | sección

Fuente propia

Figura 10. información de OSPF



Fuente propia

2.5. Parte 5: Implementar DHCP y NAT para IPv4

2.5.1. Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Tabla 23. Configuración del R1 como 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	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0

	R1(dhcp-config)#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)#exit
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1

Fuente propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Configuración de NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 password cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No es posible realizar esta acción, ver imagen adjunta

Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#int S0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#int lo 0 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.0.0 0.0.7.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente propia

2.5.3. 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.

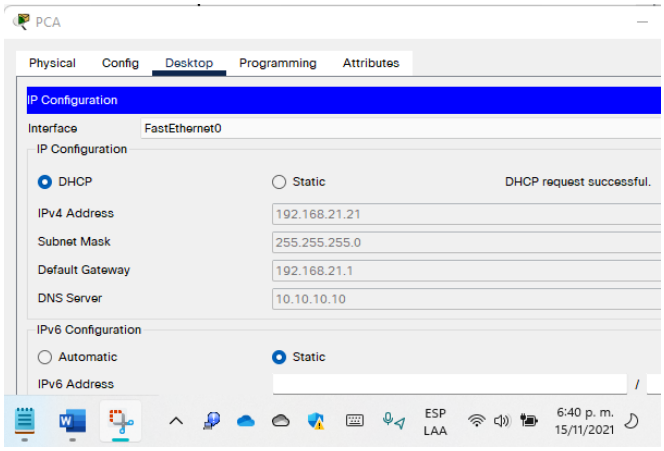
Tabla 25. Verificación del protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	C:\>ping 192.168.21.22 Pinging 192.168.21.22 with 32 bytes of data: Reply from 192.168.21.22: bytes=32 time<1ms TTL=128 Reply from 192.168.21.22: bytes=32 time<1ms TTL=128 Reply from 192.168.21.22: bytes=32 time<1ms TTL=128 Reply from 192.168.21.22: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.21.22: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Para verificar esta información por favor ver las figuras 27 y 28
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Packet Tracer PC Command Line 1.0 C:\>ping 192.168.21.21 Pinging 192.168.21.21 with 32 bytes of data: Reply from 192.168.21.21: bytes=32 time<1ms TTL=128 Reply from 192.168.21.21: bytes=32 time<1ms TTL=128

	Reply from 192.168.21.21: bytes=32 time<1ms TTL=128 Reply from 192.168.21.21: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.21.21: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
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	Solo es posible realizar acceso al navegador con la siguiente dirección IP http://209.165.200.238

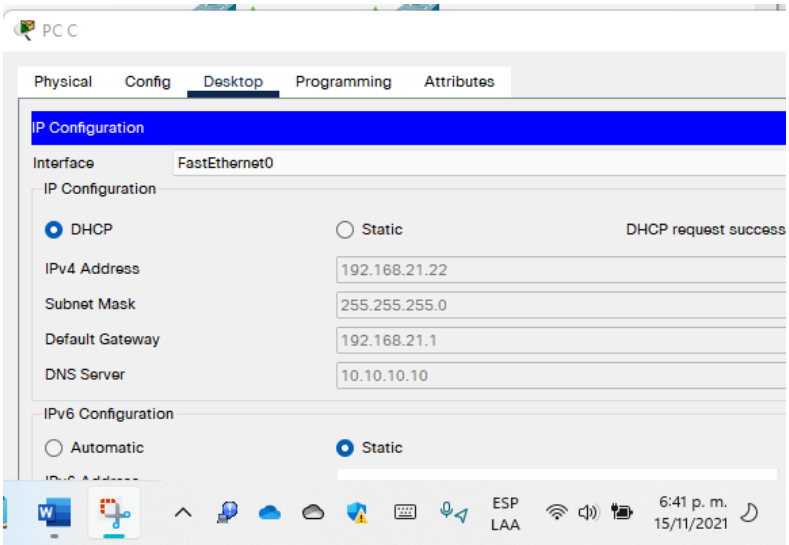
Fuente propia

Figura 11. DHCP para el PCA



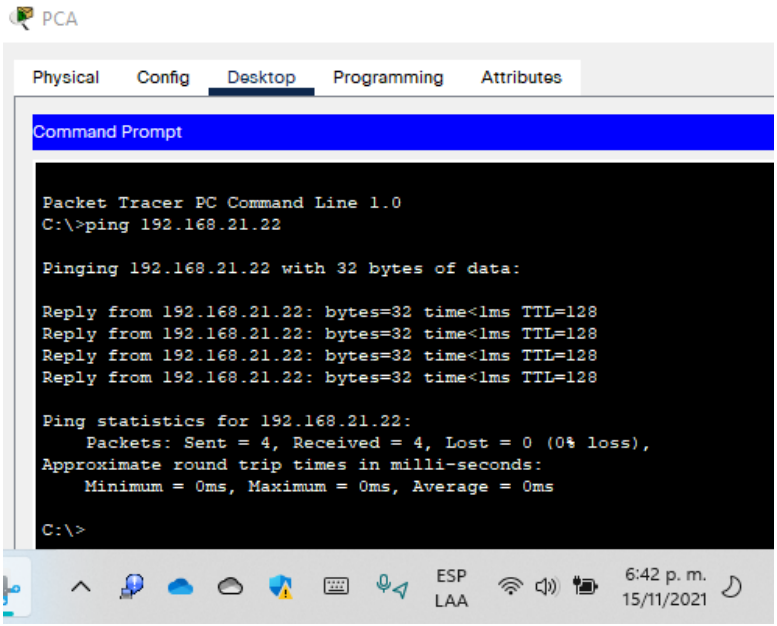
Fuente Propia

Figura 12. DHCP para el PCC



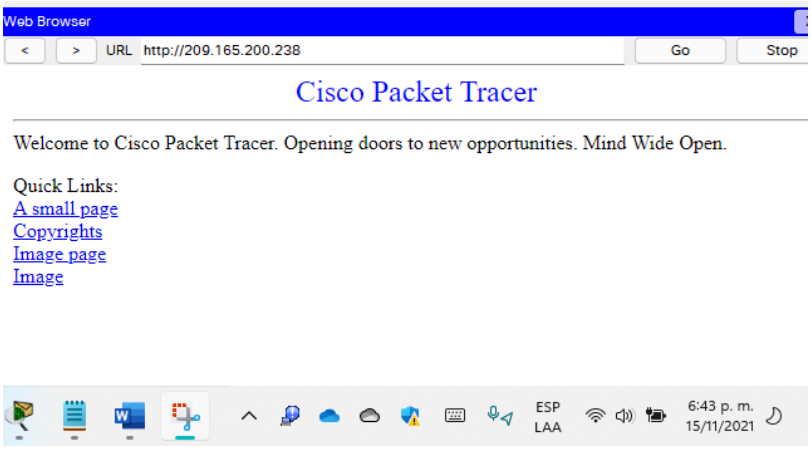
Fuente propia

Figura 13. ping entre PCA y PCC



Fuente Propia

Figura 14. comunicación con el servidor WEB



Fuente Propia

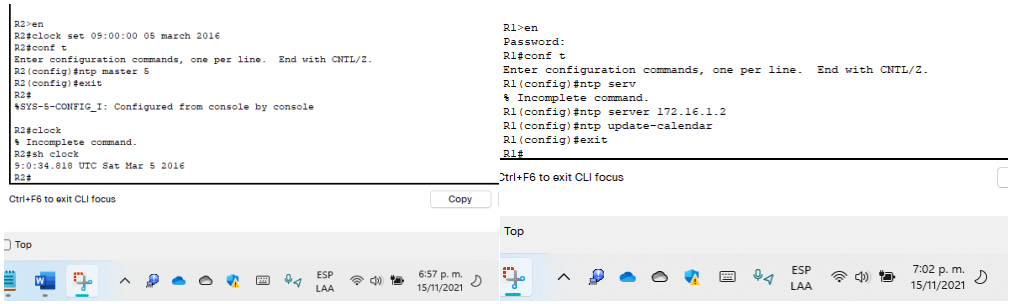
2.6. Parte 6: Configurar NTP

Tabla 26. Configuración de NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar R1(config)#exit
Verifique la configuración de NTP en R1.	R1#sh clock Los resultados se muestran en las siguientes figuras

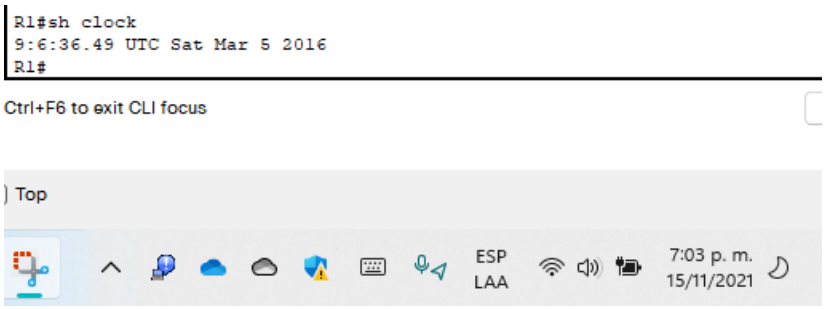
Fuente propia

Figura 15. configuración de NTP en R2 y R1



Fuente propia

Figura 16. verificación de asignación de la fecha requerida



Fuente propia

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

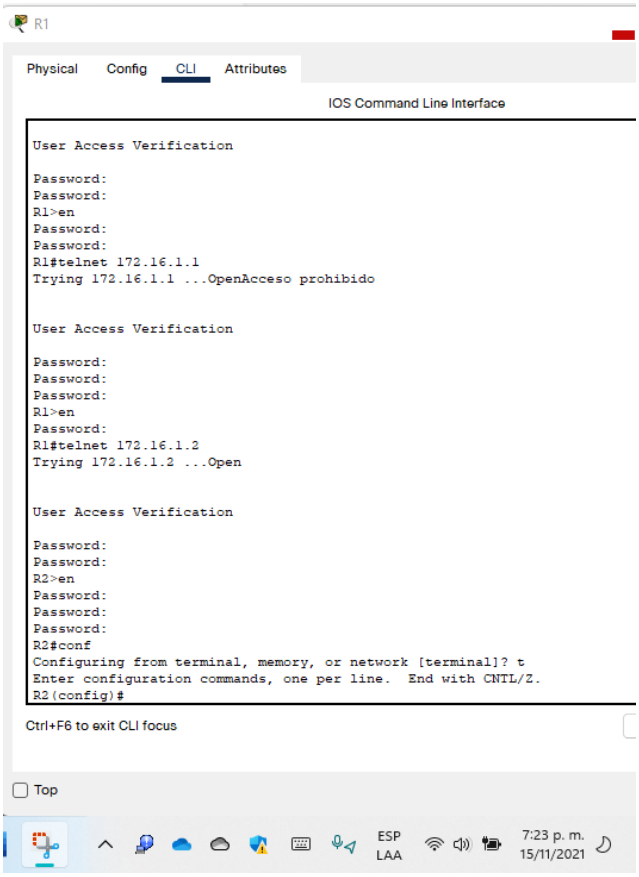
2.7.1. Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 27. Restricción del acceso a las líneas VTY en el 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	R1(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#deny any R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#ip access-class ADMIN-MGT in R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Fuente propia

Figura 17. acceso desde R1 a R2



Fuente propia

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

Tabla 28. comandos para obtener información

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde	R2#sh access-lists Standard IP access list 1 10 permit 192.168.0.0 0.0.3.255 20 permit 192.168.21.0 0.0.0.255 (18 match(es))

la última vez que se restableció	30 permit 192.168.23.0 0.0.0.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 20 deny any
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show run
¿Con qué comando se muestran las traducciones NAT?	R2#show Access-lists
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip access-list counters

Fuente propia

Figura 18. comando sh access-lists

```
R2#show acc
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255 (12 match(es))
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.4.0 0.0.0.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1 (2 match(es))
    20 deny any

R2#
```

Ctrl+F6 to exit CLI focus Copy

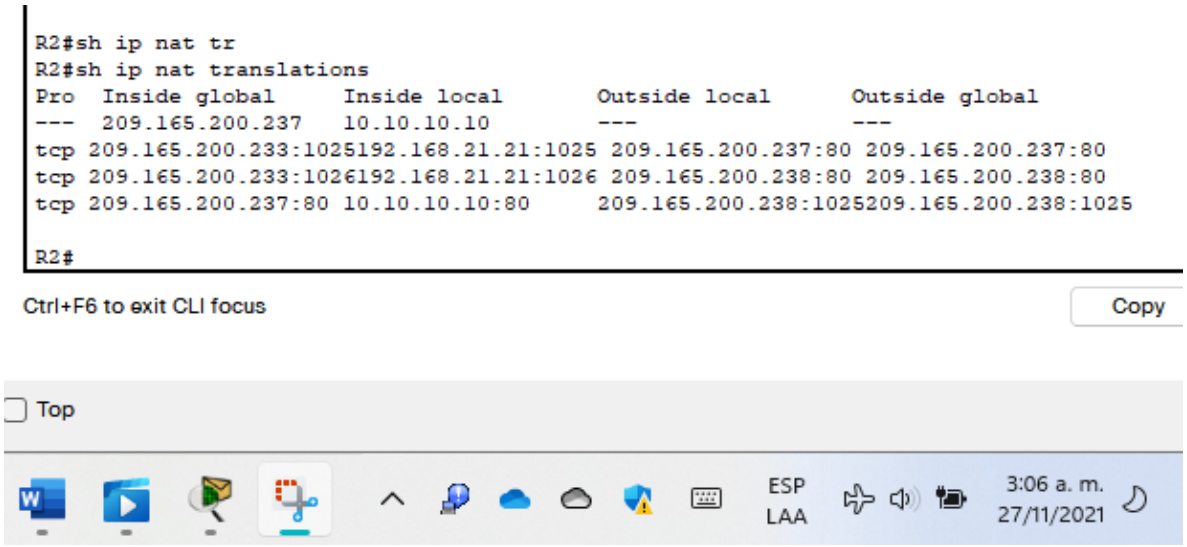
Fuente propia

Figura 19. comando show run

```
interface Loopback0
 description servidor web
 ip address 10.10.10.10 255.255.255.255
 ip nat inside
!
interface GigabitEthernet0/0
 description Web server
 ip address 209.165.200.233 255.255.255.248
 ip nat outside
 duplex auto
 speed auto
 ipv6 address 2001:DB8:ACAD:A::1/64
 ipv6 ospf 8 area 0
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 description coneccion a R1
 ip address 172.16.1.2 255.255.255.252
 ip nat inside
 ipv6 address 2001:DB8:ACAD:1::2/64
 ipv6 ospf 8 area 0
!
interface Serial0/0/1
 description coneccion a R3
 ip address 172.16.2.2 255.255.255.252
 ip nat inside
 ipv6 address 2001:DB8:ACAD:2::2/64
 ipv6 ospf 8 area 0
 clock rate 128000
!
 --More--
```

Fuente propia

Figura 20. comando sh ip nat translations



Fuente propia

CONCLUSIONES

Con todos los contenidos aquí estudiados es válido afirmar con certeza que las configuraciones de las redes que hoy en día se emplean continuamente son un campo que requiere profundizar todos los temas que tienen que ver con la configuración DHCP, IPv4, IPv6, NAT, entre otros. Todos estos conceptos hacen posible que los equipos de cómputo se puedan comunicar entre sí y poder compartir información de interés, así pues, el protocolo DHCP es un protocolo que pretende ahorrar tiempo en la gestión de direcciones IP. A lo largo de todo el documento se pudo evidenciar que junto con los demás protocolos ya mencionados hacen posible la transferencia de información, pero para lograrlo es necesario realizar un estudio profundo de su correcto uso y no desfallecer en el intento tras la implementación de una red sin importar el tamaño.

BIBLIOGRAFÍA

Al-Ani, D. R., & Al-Ani, A. R. (2018). The Performance of IPv4 and IPv6 in Terms of Routing Protocols using GNS 3 Simulator. Procedia Computer Science, 130, 1051–1056. doi:10.1016/j.procs.2018.04.147

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

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

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

BAREÑO Raúl, G., & Sevillano, A. M. L. (2017). 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.

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.

Manzoor, A., Hussain, M., & Mehrban, S. (2020). Performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols. Computer Standards & Interfaces, 68, 103391. doi:10.1016/j.csi.2019.103391

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.

Riley, C., Flannagan, M. E., Fuller, R., Khan, U., Lawson, W. A., O'Brien, K., & Walshaw, M. (2003). Cisco Technologies, Routers, and Switches. The Best Damn Cisco Internetworking Book Period, 1–89. doi:10.1016/b978-193183691-3/50018-3

Sarala, S., & Krishnamoorthi, K. (2020). Enhanced packet routing queuing model in optical burst switching network using queue-based dynamic optical route scheduling. Microprocessors and Microsystems, 79, 103296. doi:10.1016/j.micpro.2020.103296

Tse, E. S. H. (2005). Switch fabric design for high performance IP routers: A survey. Journal of Systems Architecture, 51(10-11), 571–601. doi:10.1016/j.sysarc.2004.12.005

Žarković, S. D., Shayesteh, E., & Hilber, P. (2021). Integrated reliability centered distribution system planning — Cable routing and switch placement. Energy Reports, 7, 3099–3115. doi:10.1016/j.egyr.2021.05.045