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

JAIR ALEXANDER OLIVERA RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DECIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRONICA
IBAGUE TOLIMA

2021

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

JAIR ALEXANDER OLIVERA RODRIGUEZ

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

TUTOR:

INGENIERO RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DECIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRONICA
IBAGUE TOLIMA

2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

IBAGUE TOLIMA, 27 de noviembre de 2021

AGRADECIMIENTOS

Quiero agradecer en primer lugar a Dios, por guiarme en el camino y fortalecerme espiritualmente para empezar un camino lleno de éxito.

Así, quiero mostrar mi gratitud a todas aquellas personas que estuvieron presentes en la realización de esta meta, de este sueño que es tan importante para mí, agradecer sus palabras motivadoras, sus conocimientos, sus consejos y su dedicación.

Muestro mis más sinceros agradecimientos a mi tutor de proyecto, quien con su conocimiento y su guía fue una pieza clave para que pudiera desarrollar una clave de hechos que fueron imprescindibles para cada etapa de desarrollo del trabajo.

Por último, quiero agradecer a la base de todo, a mi familia, en especial a mi madre, que quien con sus consejos fueron el motor de arranque y mi constante motivación, muchas gracias por su paciencia y comprensión, y sobre todo por su amor.

¡Muchas gracias por todo!

TABLA DE CONTENIDO

Contenido

LISTA DE TABLAS

LISTA DE IMÁGENES

GLOSARIO

Pv4:

El IPv4 es un sistema direccional de 32 bits usado para identificar un dispositivo en una red. Es el sistema direccional usado en la mayoría de las redes informáticas, incluyendo Internet.

DNS:

Es el acrónimo de Domain Name Server (servidor de nombres de dominio). Un servidor de nombres de dominio es un servidor ubicado en Internet que traduce las URLs (Uniform Resource Locator o localizador uniforme de fuentes) como www.adslayuda.com en direcciones IPs. Muchos ISPs no necesitan que se introduzca esta información en el router. Si está usted utilizando un tipo de conexión de IP estática, entonces puede necesitar introducir una dirección de DNS y una dirección de DNS secundaria específicas para que su conexión funcione adecuadamente. Si su tipo de conexión es dinámica o PPPoE, es muy probable que no necesite introducir una dirección de DNS.

Gateway:

Pasarela, puerta de acceso. Realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Sirve para, por ejemplo, conectar una LAN de ordenadores personales a una red del tipo Internet.

Router:

Enrutador. Originalmente, se identificaba con el término gateway, sobre todo en referencia a la red Internet. En general, debe considerarse como el elemento responsable de discernir cuál es el camino más adecuado para la transmisión de mensajes en una red compleja que está soportando un tráfico intenso de datos.

Swtich:

Dispositivo de red que filtra, envía e inunda de frames en base a la dirección de destino de cada frame. El switch opera en la capa de enlace de datos del modelo OSI. En general se aplica a un dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

IP address:

Dirección IP. Matrícula que identifica a un ordenador de la red. A los ordenadores personales se les asigna una IP address para que naveguen por la red.

OSPF: El protocolo OSPF (Open Shortest Path First) forma parte de una familia de protocolos de enrutamiento IP y es un protocolo de puerta de enlace interior (IGP) para Internet, que se utiliza para distribuir información de enrutamiento IP a través de un único sistema autónomo (AS) en una red IP.

VLAN: Las LAN virtuales, son agrupaciones lógicas de dispositivos en el mismo dominio de transmisión. Las VLAN generalmente se configuran en conmutadores colocando algunas interfaces en un dominio de transmisión y algunas interfaces en otro. Cada VLAN actúa como un subgrupo de puertos de conmutador en una LAN Ethernet.

RESUMEN

Hoy en día la red es un área donde se va actualizando en cada momento, debido al cambio de las necesidades, ya que se han vuelto una herramienta indispensable en el mundo de los negocios como en la vida cotidiana de las personas por su gran utilidad a la hora de compartir información y de relacionarnos.

Este Diplomado de profundización de CISCO con certificación CCNA el cual se basa en el diseño de distintas redes con escenarios distintos para que el estudiante interprete, analice y aborde varias clases de problemas que podría ayudarlo en su vida laboral a un futuro, por medio del programa de diseño Packet Tracer el estudiante puede diseñar, configurar y simular una red electrónica.

Con el certificado CCNA le permite al estudiante implementar, verificar y resolver problemas de redes, como también le da la facultad de trabajar como especialista en enrutamiento y conmutación de diferentes clases de redes avanzadas de seguridad, como también redes de voz, Wireless y de video.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

Nowadays networks is an area where it is updated at all times, due to changing needs, since they have become an indispensable tool in the business world as well as in people's daily lives due to their great utility to when it comes to sharing information and relating.

This CISCO deepening Diploma with CCNA certification which is based on the design of different networks with different scenarios for the student to interpret, analyze and address various kinds of problems that could help them in their working life in the future, through the program In Packet Tracer design the student can design, configure and simulate an electronic network.

With the CCNA certificate it allows the student to implement, verify and solve network problems, as well as the ability to work as a specialist in routing and switching of different classes of advanced security networks, as well as voice, wireless and video networks.

Keywords: CISCO, CCNA, Switching, Routing, Networks, Electronics.

INTRODUCCION

El Diplomado de profundización de CISCO con certificación CCNA es un curso que está basado en especializar al futuro ingeniero en planificar, diseñar y configurar distintas clases de redes locales, como también le da la habilidad de resolver problemas avanzados de seguridad, de voz y Wireless.

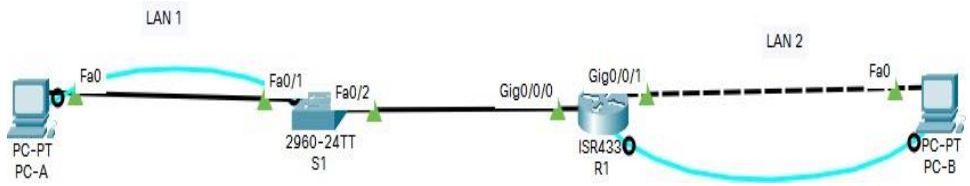
Este trabajo está basado en la realización de dos escenarios propuestos por el tutor del curso, en el cual el primer escenario propone resolver y configurar unos dispositivos de una red pequeña , el cual debe configurar un router, un switch y diseñar el esquema de direccionamiento IPv4 para unas LAN, esto con el propósito de que el estudiante entienda como se diseña una red pequeña en el simulador de redes llamado Packet Tracer, sepa cómo verificar la conectividad entre los equipos e identifique las clases de routers, switches y conexiones que existen dependiendo de las necesidades de la red.

El segundo escenario se debe configurar una red 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 el proceso de conexión y configuración deberá probar, verificar y registrar los resultados que se van generando mediante los comandos comunes de CLI, como por ejemplo el ping, esto con el fin de que el estudiante compruebe de que las configuraciones y conexiones están bien, también entienda su comportamiento y cuál es el propósito de tener una red segura por medio de la creación de cuentas de usuarios y la asignación de contraseñas.

DESARROLLO

Escenario 1
Topología

Figura 1 Topología escenario 1



Fuente. Autor

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

Objetivos

Parte 1: Construir en el simulador la Red

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

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

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

Parte 5: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación

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

Parte 1: Construya la Red

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

Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

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

Solucion:

Direccionamiento: 192.168.95.0/24

Esta dirección es de clase c, lo que significa que los primeros 3 octetos son de red y el ultimo es para host.

Lo que es de 2^8bits para trabajar

Para 100 PC

0 | 0000000

SR 7 host

La nueva mascara para 100 PC es 25 ya que sumando 24 por defecto más 1 que sobra.

Para 100 computadores:

192.168.95.0/25

Mascara: 255.255.255.128

Para la siguiente subred se toma el valor máximo de octeto que es 256 posiciones y se resta la máscara menos significativa que es 128, lo que nos da 128.

Para 50 PC: 192.168.95.128

00 | 000000

SR 6 host

Para la nueva mascara se tomaría 24 por defecto, más los dos que sobraron, lo que daría 26.

Para 50 PC: 192.168.95.128/26

La máscara seria **255.255.255.192**, ya que sumando 128 con 64 daría 192

Para las IP disponibles:

Para 100 PC:

Primera disponible: 192.168.95.1

Ultima seria: 192.168.95.126

Para Broddcast: 192.168.95.127

Para futuro crecimiento de redes: 192.168.95.128

Para 50 PC:

Primera disponible: 192.168.95.129

Ultima seria: 192.168.95.190

Para Broddcast: 192.168.95.191

Para futuro crecimiento de redes: 192.168.95.192

Tabla 1 Direccionamiento

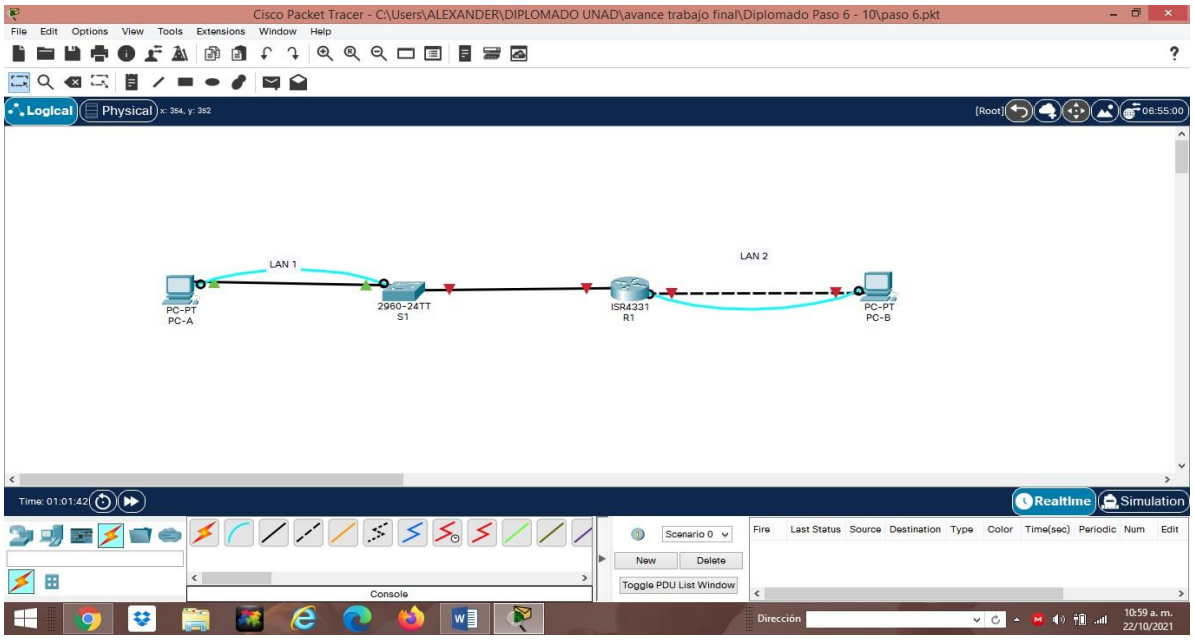
Item	**Requerimiento**
Dirección de Red	192.168.95.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.95.1
R1 G0/0/0	192.168.95.129
S1 SVI	192.168.95.2
PC-A	192.168.95.126
PC-B	192.168.95.190

Fuente. Autor:

Parte 3: Configure aspectos básicos

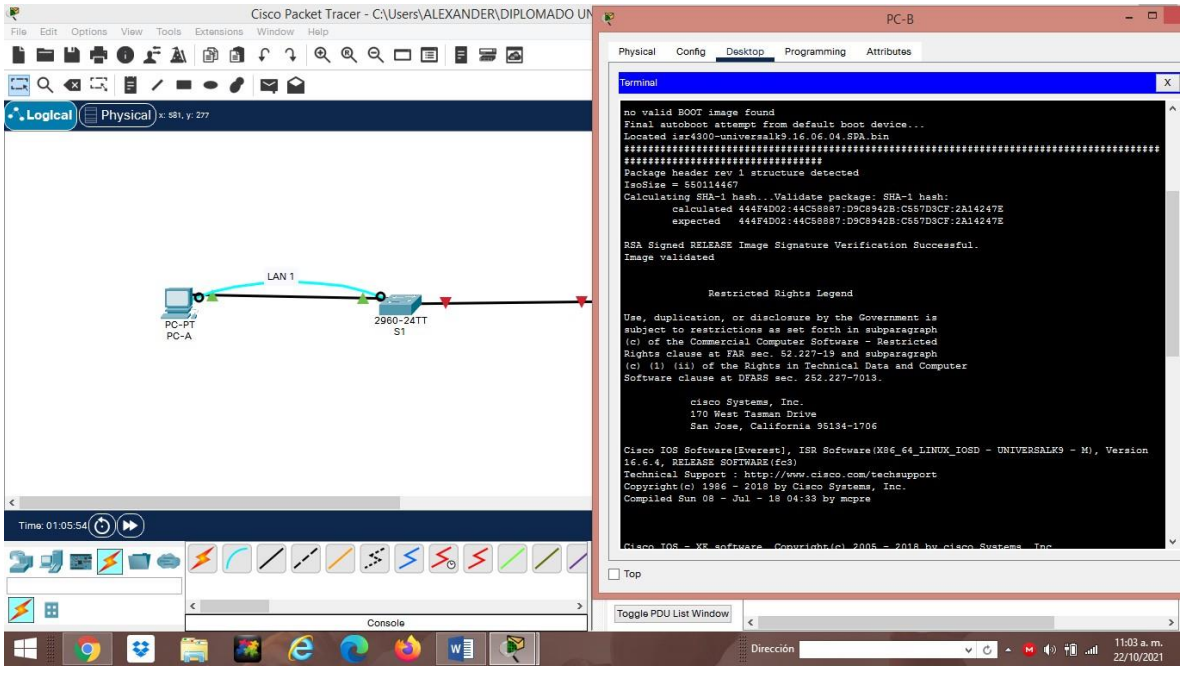
Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Figura 2 Topología de la red escenario 1.



Fuente. Autor:

Figura 3 Configuración PC-B



Fuente. Autor

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2 Configuración para R1

Tarea	**Especificación**
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente. Autor:

Código:

Router>enable (ingreso a modo privilegiado)
Router#config t (ingreso a modo configuración)
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup (Desactiva la búsqueda DNS)
Router(config)#ho R1 (Asigna el nombre al router)
R1(config)#ip domain-name ccna-lab.com (Dominio del router)
R1(config)#enable secret ciscoenpass (Para encriptar la contraseña de modo privilegiado)
R1(config)#line console 0 (contraseña acceso consola)
R1(config-line)#password ciscoconpass (contraseña)
R1(config-line)#login (Para habilitar la contraseña)
R1(config-line)#exit (salir)
R1(config)#security password min-length 10 (longitud mínima para la contraseña. 10 caracteres)

R1(config)#username admin password admin1pass (crear un usuario administrativo)
R1(config)#line vty 0 4 (configurar el inicio de sesión en las lineas VTY)
R1(config-line)#password ciscocisco (se asigna contraseña)
R1(config-line)#login local (en el local)
R1(config-line)#transport input SSH (para que solo acepte SSH)
S1(config-line)#exit (salir)
R1(config)#service password-encryption (para cifrar las contraseñas de texto no sifrado)
R1(config)#banner motd #Este es el router de la UNAD, cualquier intrusión tendrá efectos judiciales# (Configuracion del MOTD banner)
R1(config)#int g0/0/0 (configur la interfaz)
R1(config-if)#ip address 192.168.95.129 255.255.255.192 (dirección ip y la mascara)
R1(config-if)#description esta es la interfaz de la Lan 2
R1(config-if)# no sh
R1(config-if)#exit (salir)
R1(config)# int g0/0/1 (configurar la otra interfaz)
R1(config-if)#description esta es la interfaz de la Lan 1
R1(config-if)# ip address 192.168.95.1 255.255.255.128 (dirección ip y la mascara)
R1(config-if)# no sh
R1(config-if)#exit (salir)
R1(config)#ip domain name ccna-lab.com (generar el cifrado RSA)
R1(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 (asignar 1024 bits)
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#exit (salir)
R1#wr

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3 Configuración S1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	
Nombre del switch	S1
Nombre de dominio	ccna-lab.com

Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass

Fuente. Autor

Tabla 4 Asignación de usuario y contraseña para S1

Tarea	**Especificación**
Contraseña de acceso a la consola	ciscoconpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.

Fuente. Autor

Código:

Switch>enable (ingreso a modo privilegiado)
Switch#config t ingreso a modo configuración)
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup (Desactiva la búsqueda DNS)
Switch(config)#ho S1 (Asigna el nombre al switch)
S1(config)#ip domain-name ccna-lab.com (Dominio del switch)
S1(config)#enable secret ciscoenpass (Para encriptar la contraseña de modo privilegiado)
S1(config)#line console 0 (contraseña acceso consola)
S1(config-line)#password ciscoconpass (contraseña)
S1(config-line)#login (Para habilitar la contraseña)
S1(config-line)#exit (salir)
S1(config)#user name admin password admin1pass (crear un usuario administrativo)
^
% Invalid input detected at '^' marker.

S1(config)#username admin password admin1pass (crear un usuario administrativo)
S1(config)#line vty 0 15 (configurar el inicio de sesión en las lineas VTY)
S1(config-line)#password ciscocisco (contraseña)
S1(config-line)#login local (área local)
S1(config-line)#transport input SSH (para que solo acepte SSH)
S1(config-line)#exit (salir)
S1(config)#service password-encryption (para cifrar las contraseñas de texto no sifrado)
S1(config)#banner motd #Este es el switch de la UNAD por favor no ingresar aqui# (Configuracion del MOTD banner)
S1(config)#ip domain name ccna.lab.com (asignar el nombre ip dominio)
S1(config)#crypto key generate rsa (generar el cifrado 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 (asignar 1024 bits)
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#int vlan 1
*Mar 1 1:12:34.849: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-if)#ip address 192.168.95.2 255.255.255.128 (se asigna la segunda dirección ip y la mascara)
S1(config-if)#no sh

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit (salir)
S1(config)#ip default-gateway 192.168.95.1 (asignar Gateway por defecto)
S1(config)# exit (salir)
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#wr
Building configuration...
[OK]

Paso 2. Configurar los equipos

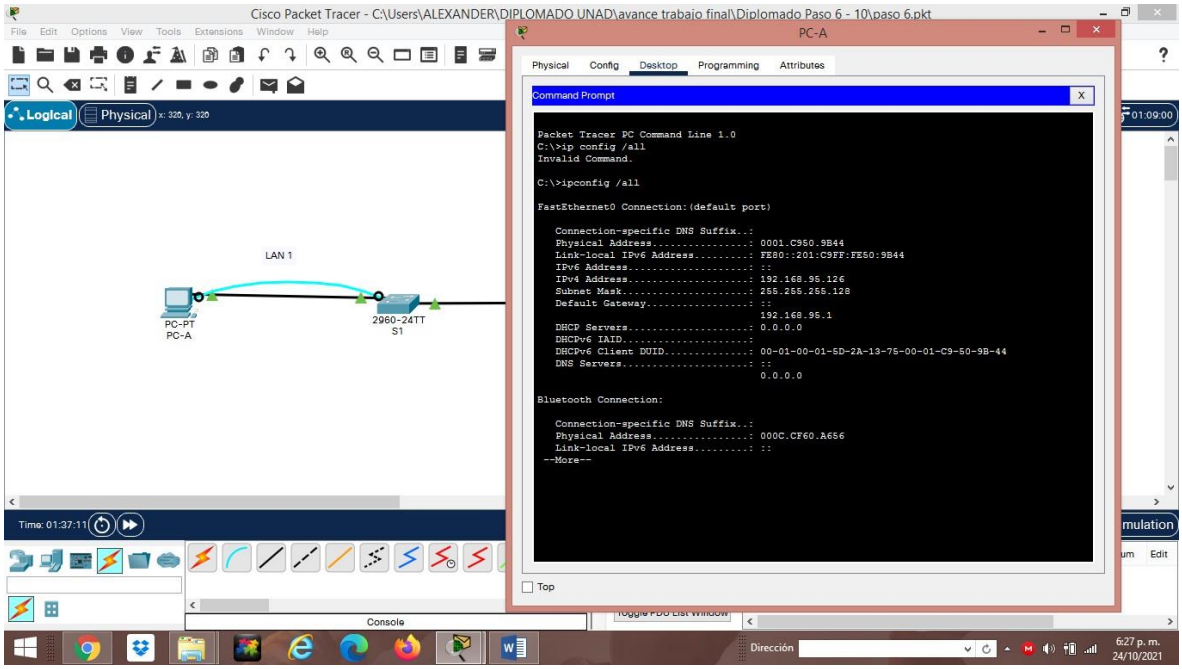
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all.**

Tabla 5 Configuración PC-A

PC-A Network Configuration	
Descripción	Este es el PC-A
Dirección física	0001.C950.9B44
Dirección IP	192.168.95.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.95.1

Fuente. Autor

Figura 4 Configuración Network PC-A



Fuente. Autor

Resultado con el comando ipconfig /all

C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address. .....0001.C950.9B44 (Dirección fisica)
Link-local IPv6 Address.....: FE80::201:C9FF:FE50:9B44
IPv6 Address..... : ::
IPv4 Address.....: 192.168.95.126 (Dirección IP del PC-A)

Subnet Mask.....255.255.255.128 (La mascara de la PC-A)
Default Gateway .....: ::
192.168.95.1 (Gateway por defecto)
DHCP Servers. .....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-5D-2A-13-75-00-01-C9-50-9B-44
DNS Servers. .....: ::
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix..:
Physical Address.....: 000C.CF60.A656
Link-local IPv6 Address.....: ::
--More—

Tabla 6 Configuración Network PC-B

PC-B Network Configuration	
Descripción	Este es el PC-B
Dirección física	00D0.BADD.05DC
Dirección IP	192.168.95.190
Máscara de subred	255.255.255.192

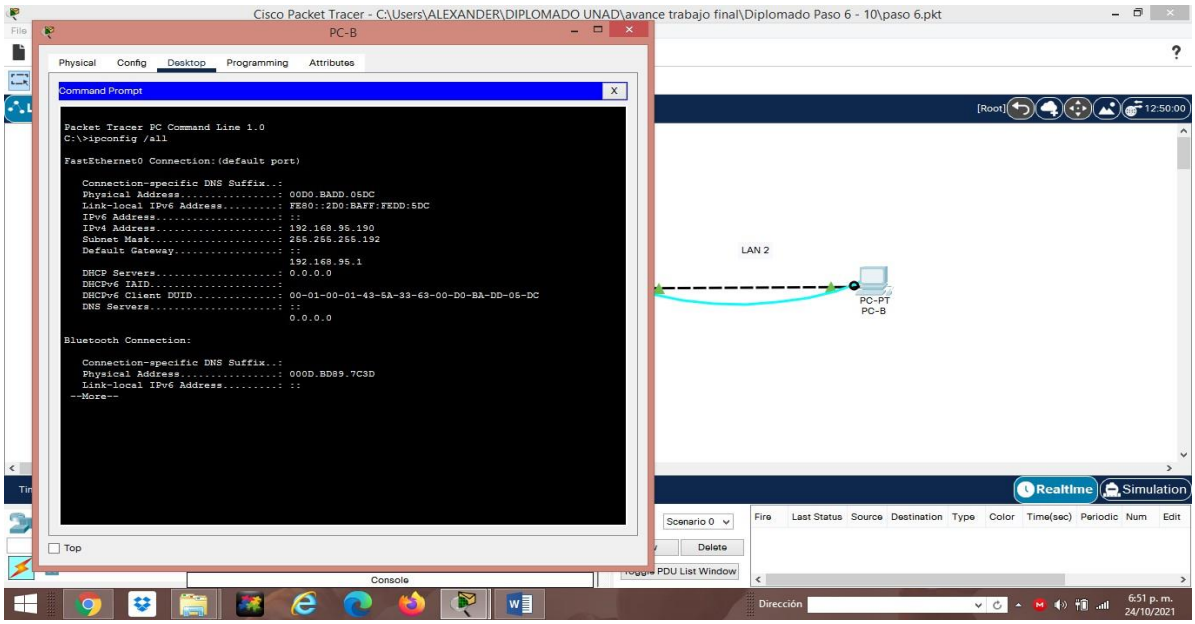
Fuente. Autor

Tabla 7 Gateway predeterminado para PC-B

PC-B Network Configuration	
Gateway predeterminado	192.168.95.1

Fuente. Autor

Figura 5 Configuración PC-B



Fuente. Autor

Resultado con el comando ipconfig /all

C:\>ipconfig /all

FastEthernet0 Connection:(default port)

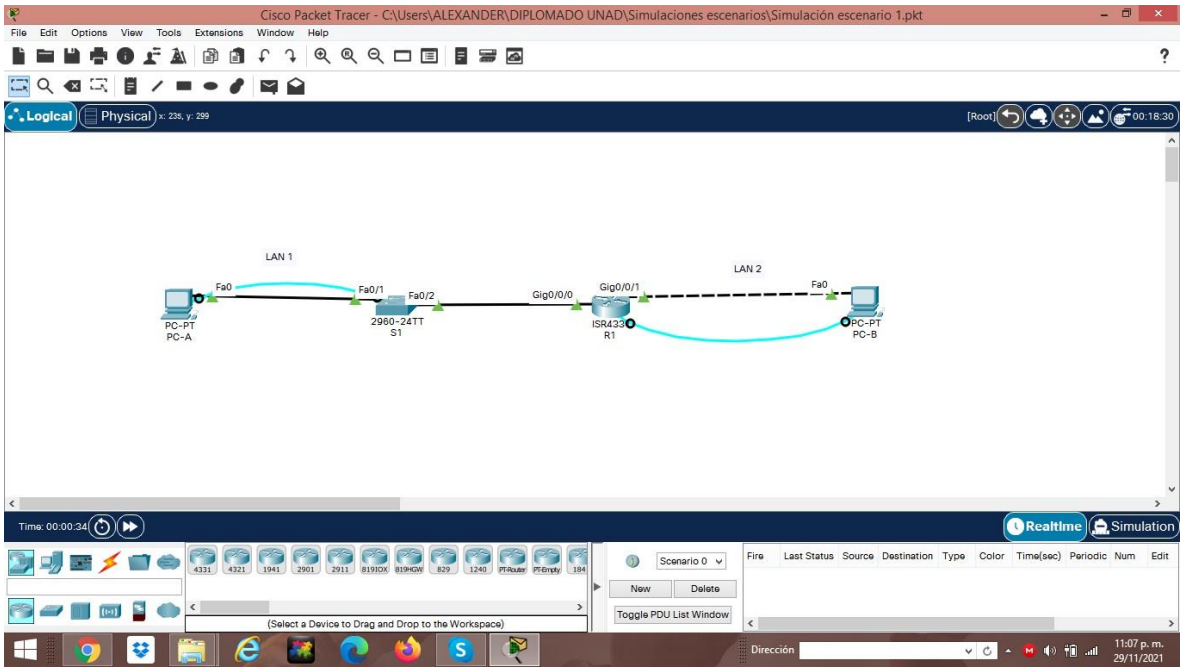
Connection-specific DNS Suffix..:
Physical Address. .....00D0.BADD.05DC (Dirección fisica)
Link-local IPv6 Address.....: FE80::2D0:BAFF:FEDD:5DC
IPv6 Address..... : ::
IPv4 Address.....: 192.168.95.190 (Dirección ip PC-B)
Subnet Mask.....: 255.255.255.192 (Mascara de la PC-B)
Default Gateway .....: ::
192.168.95.1 (Gateway por defecto)
DHCP Servers. .....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-43-5A-33-63-00-D0-BA-DD-05-DC
DNS Servers. .....: ::
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix..:
Physical Address. 000D.BD89.7C3D

Link-local IPv6 Address.....: ::
--More—

Figura 6 Resultado simulación



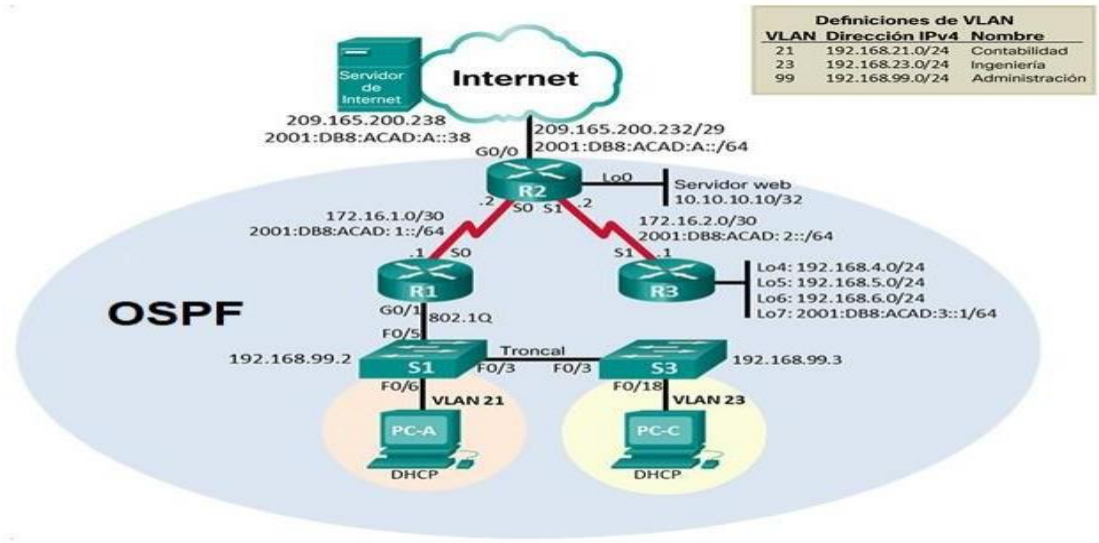
Fuente. Autor

Escenario 2

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

Topología

Figura 7 Topología escenario 2.



Referencia: *(UNAD, Prueba de Habilidades CCNA, 2021)*

Parte 1: Inicializar dispositivos

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

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

Tabla 8 Iniciar y cargar routers y switches

Tarea	Comandos de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config

Volver a cargar todos los routers	Router# reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch# erase startup-config
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. Autor

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

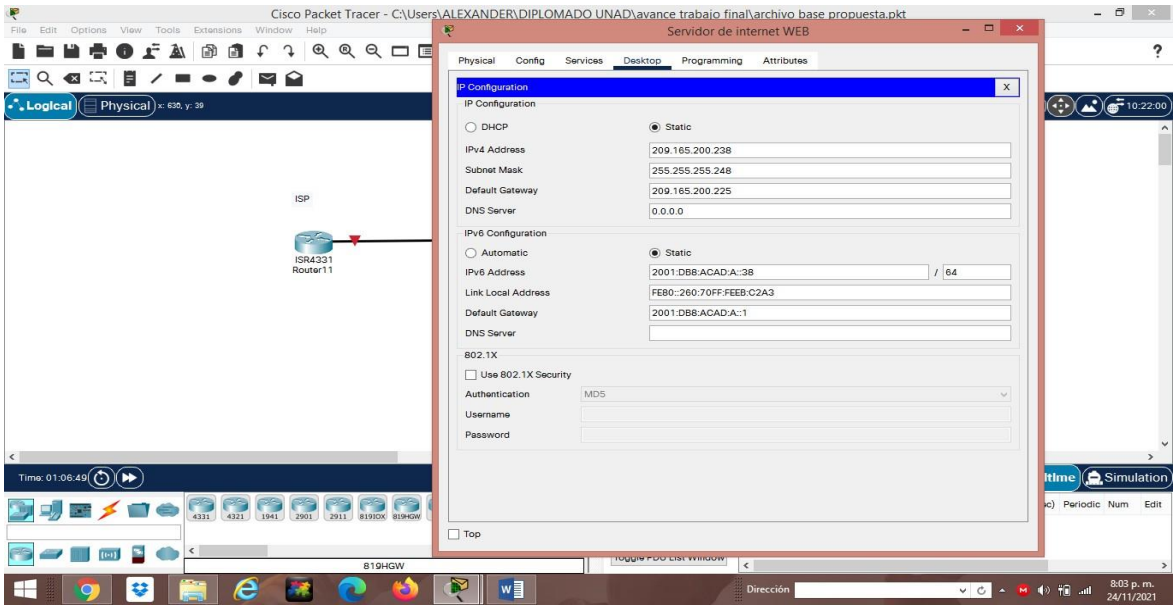
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 9 Configurar la 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:acad:a::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:**A**::1

Fuente. Autor

Figura 8 Configuración computadora internet



Fuente. Autor

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 10 Código para configurar R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login

Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd # Se prohibe el acceso no autorizado.#
Interfaz S0/2/0	R1(config)#int s0/2/0 R1(config-if)#description Connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 addres 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0 R1(config)#ipv6 route ::/0 s0/2/0

Fuente. Autor

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 11 Código configuración R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login

Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server ^ % Invalid input detected at '^' marker.
Mensaje MOTD	R2(config)#banner motd # Se prohibe el acceso no autorizado.#
Interfaz S0/2/0	R2(config)#int s0/2/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/2/1	R2(config-if)#int s0/2/1 R2(config-if)#description Connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0/0 (simulación de Internet)	R2(config-if)#int g0/0 /0 R2(config-if)#description Connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulated Web Server R2(config-if)#exit

Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Fuente. Autor

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 12 Configurar R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>en Router#conf t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd # Se prohibe el acceso no autorizado.#
Interfaz S0/2/1	R3(config)#int s0/2/1 R3(config-if)#description Connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0.

Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int 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 s0/2/1 R3(config)#ipv6 route ::/0 s0/2/1

Fuente. Autor

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 13 Código configuración S1

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

Fuente. Autor

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 14 Configuración S3

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

Fuente. Autor

Paso 7: Verificar la conectividad de la red

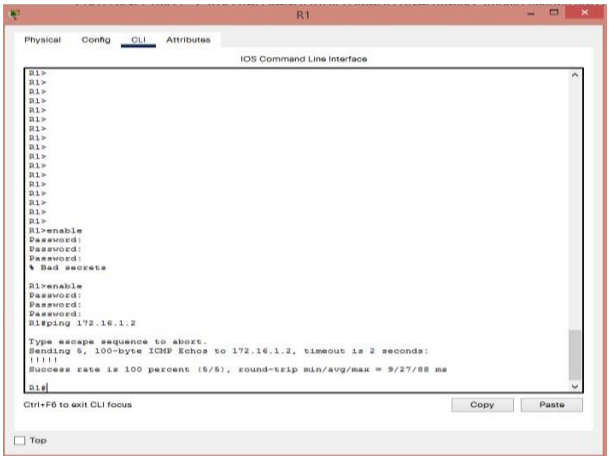
Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

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

Verificar la conectividad de la red

Desde R1 a R2, S0/2/0, Dirección IP 172.16.1.2, resultado de ping.

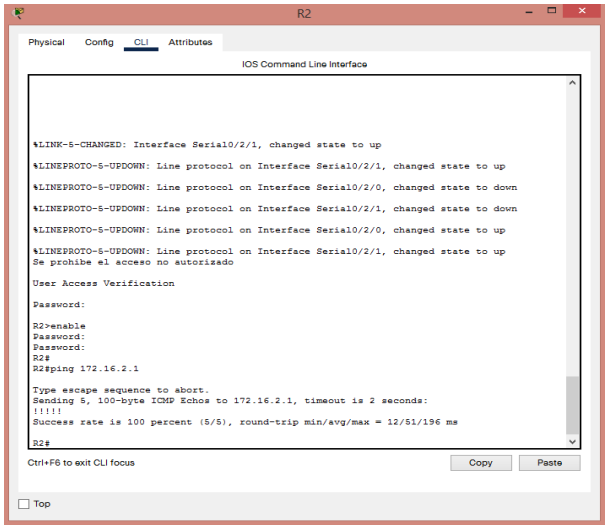
Figura 9 R1 ping 172.16.1.2



Fuente. Autor

Desde R2 a R3, S0/2/1, Dirección IP 172.16.2.1, resultado de ping.

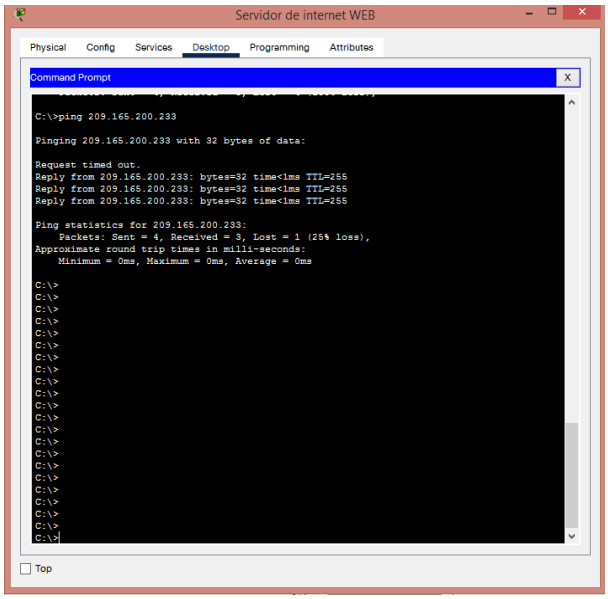
Figura 10 R2 ping 172.16.2.1



Fuente. Autor

Desde PC de Internet a Gateway predeterminado, Dirección IP 209.165.200.233, resultado de ping.

Figura 11 Ping Gateway predeterminado



Fuente. Autor

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 15 Configurar la seguridad del S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1#conf t S1(config)#vlan 21 S1(config-vlan)#name tesoreria S1(config-vlan)#vlan 23 S1(config-vlan)#name tecnologia S1(config-vlan)#vlan 99 S1(config-vlan)#name administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0

	S1(config-if)#no shutdown S1(config-if)#exit
Asignar el gateway predeterminado	1(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)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if-range)#switchport mode access
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-2, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Fuente. Autor

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16 Configurar la seguridad de S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S3>en S3#conf t S3(config)#vlan 21 S3(config-vlan)#name tesoreria S3(config-vlan)#vlan 23 S3(config-vlan)#name tecnologia S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#int vlan 99

	S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
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)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#int range f0/1-2, f0/4-17, f0/19- 24, g0/1-2
Apagar todos los puertos sin usar	S3(config-if-range)#shutdown

Fuente. Autor

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17 Configurar la seguridad de R1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1>en R1(config)#int g0/0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#int g0/0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/0/1 R1(config-if)#no shutdown

Fuente. Autor

Paso 4: Verificar la conectividad de la red

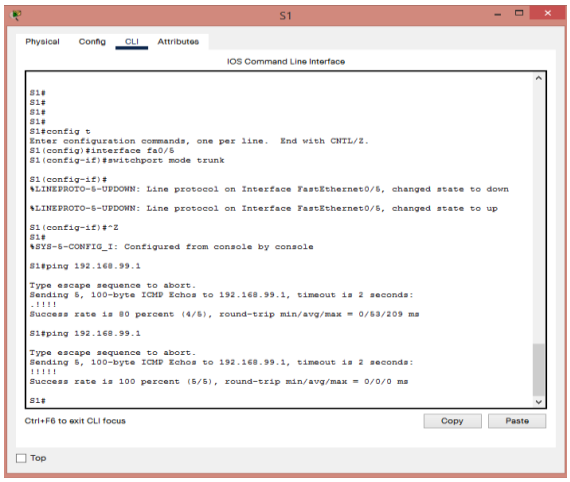
Utilice el comando ping para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Resultados de ping:

Desde S1 a R1, dirección VLAN 99, dirección IP, 192.168.99.1 resultado de ping.

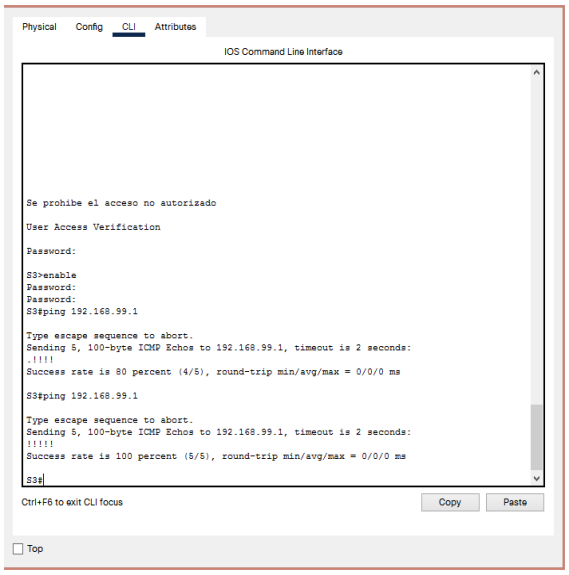
Figura 12 Desde S1 ping R1



Fuente. Autor

Desde S3 a R1, dirección VLAN 99, dirección IP, 192.168.99.1 resultado de ping.

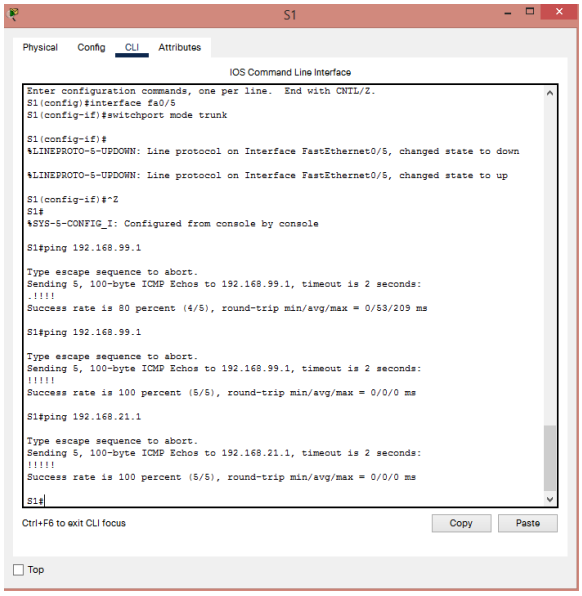
Figura 13 Desde S3 ping R1



Fuente. Autor

Desde S3 a R1, dirección VLAN 21, dirección IP, 192.168.21.1 resultado de ping.

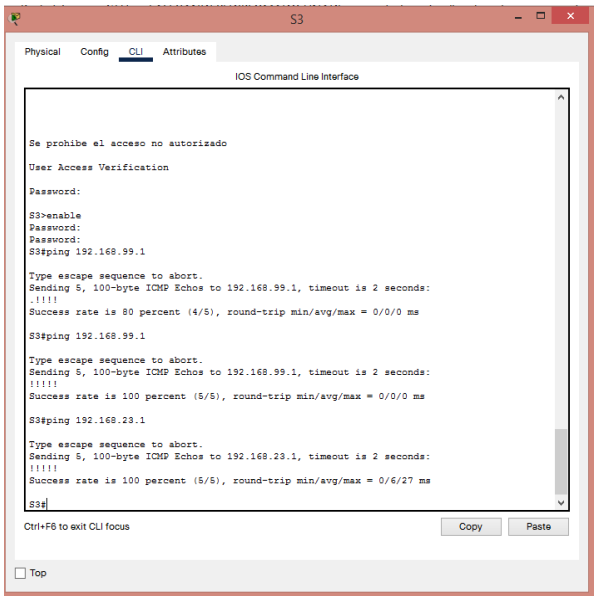
Figura 14 Desde S1 ping 192.168.21.1



Fuente. Autor

Desde S3 a R1, dirección VLAN 23, dirección IP, 192.168.23.1 resultado de ping.

Figura 15 Desde S3 ping 192.168.23.1



Fuente. Autor

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18 Configurar OSPF en R1

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	R1(config-router)#do show ip route connected R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/0/1.21 R1(config-router)#passive-interface g0/0/1.23 R1(config-router)#passive-interface g0/0/1.99

Desactive la sumarización automática	R1(config-router)#no auto-summary

Fuente. Autor

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19 Configurar OSPF en R2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0. R2(config-router)#do show ip route connected R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary (no funciona)

Fuente. Autor

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 20 Configurar OSPFv3 en R3

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#do show ip route connected R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4

	R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Fuente. Autor

Paso 4: Verificar la información de OSPF

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

Tabla 21 Pregunta y respuesta sobre OSPF

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

Fuente. Autor

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22 Configuración de R1 como servidor DHCP

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1>en R1#conf t 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)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#network 192.168.21.0 255.255.255.0

	R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcpconfig)#dns-server 10.10.10.10 R1(dhcpconfig)#domain-name ccna-sa.com R1(dhcpconfig)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1

Fuente. Autor

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23 Configuración de la NAT estática y dinámica en R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)#username webuser secret cisco12345 privilege 15
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	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/2/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/2/1 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 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.225 netmask 255.255.255.228

Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente. Autor

Paso 3: Verificar el protocolo DHCP y la NAT estática

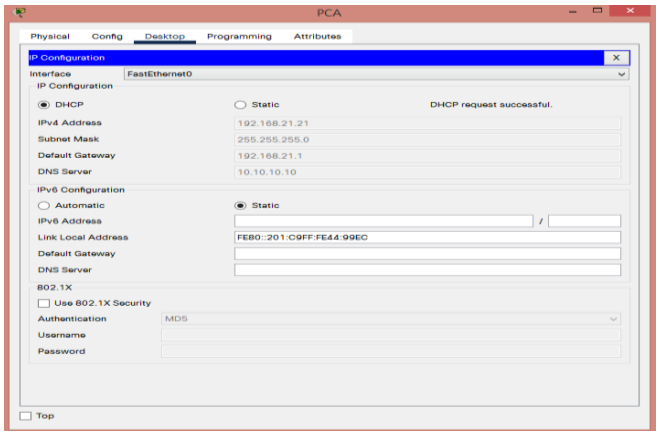
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Prueba del protocolo DHCP y la NAT estática.

Prueba: Verificar que la PC-A haya adquirido información de IP del servidor de DHCP.

Resultado:

Figura 16 Verificación PC-A

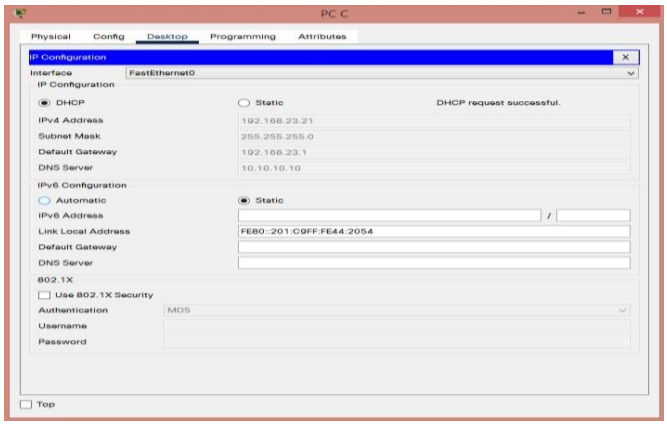


Fuente. Autor

Prueba: Verificar que la PC-C haya adquirido información de IP del servidor de DHCP.

Resultados:

Figura 17 Verificación PC-C

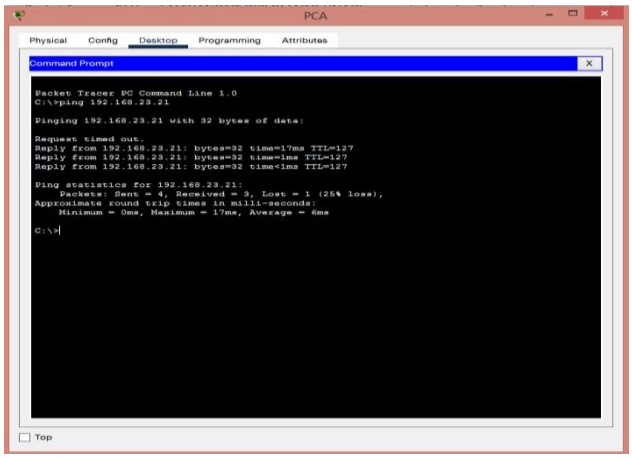


Fuente. Autor

Prueba: Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.

Resultados:

Figura 18 Desde PC-A ping PC-C

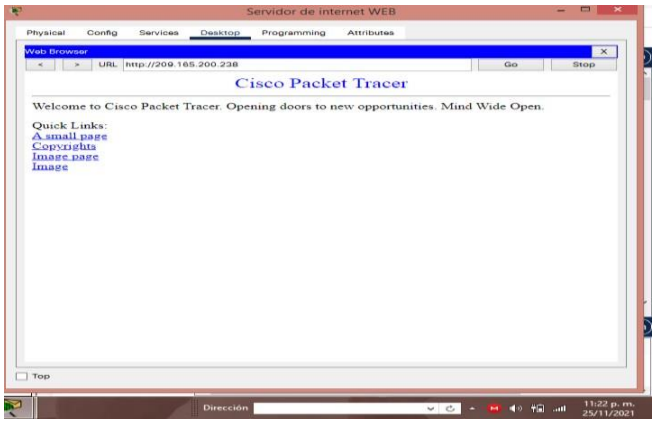


Fuente. Autor

Prueba: 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.

Resultados:

Figura 19 Verificación del navegador web desde Internet.



Fuente. Autor

Parte 6: Configurar NTP

Tabla 24 Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 12:23:00 25 nov 2021
Configure R2 como un maestro NTP.	Nivel de estrato: 5 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
Verifique la configuración de NTP en R1.	R1#show ntp associations

Fuente. Autor

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

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

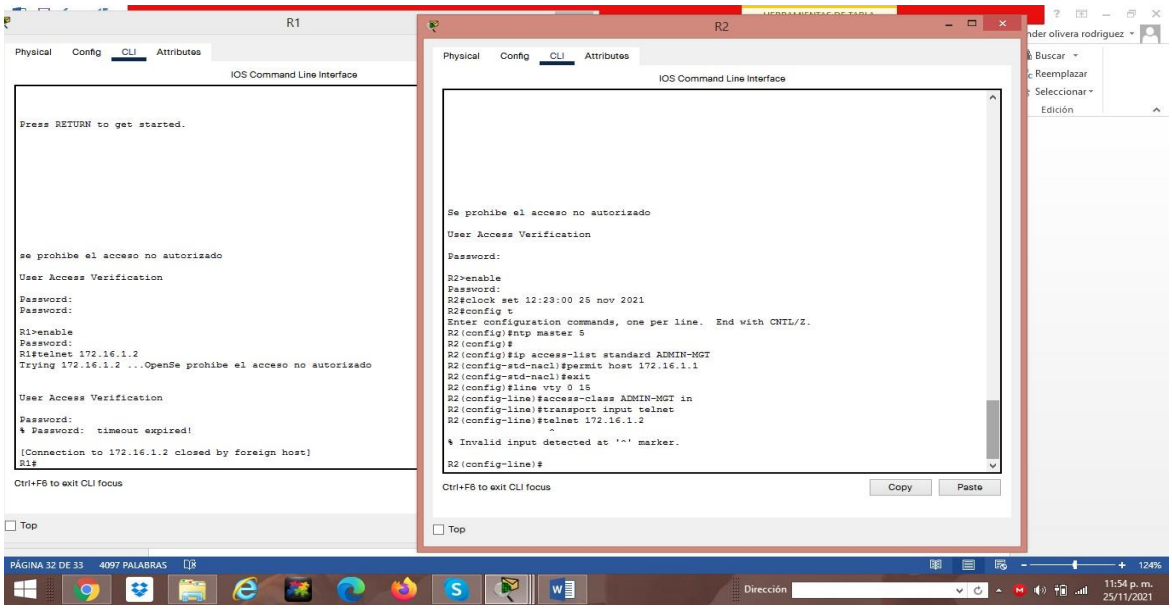
Tabla 25 Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet

Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Fuente. Autor

Figura 20 Configurar el acceso a las líneas VTY en el R2



Fuente. Autor

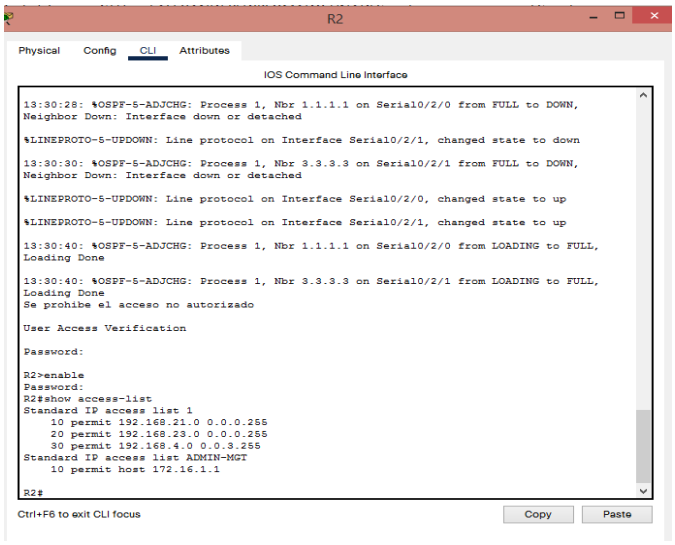
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Preguntas y respuestas sobre el comando CLI

Descripción del comando: Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció.

Entrada del estudiante (comando): R2#show access-list

Figura 21 Resultado comando Show access-list

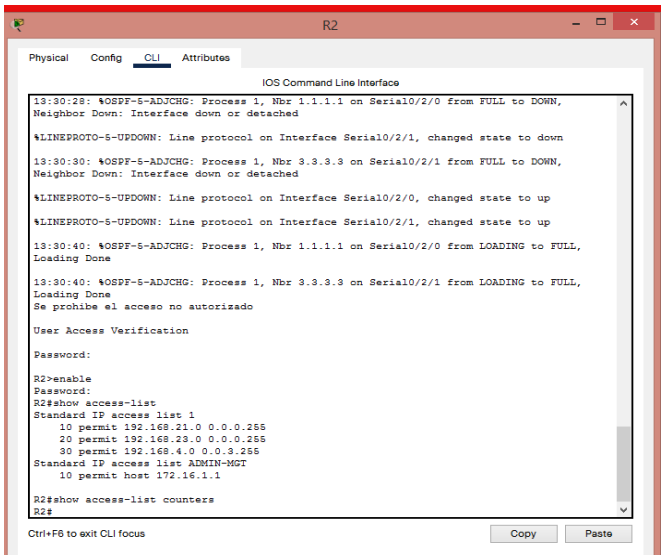


Fuente. Autor

Descripción del comando: Restablecer los contadores de una lista de acceso.

Entrada del estudiante (comando): R2#show access-list counters

Figura 22 Resultado comando Show access-list counters

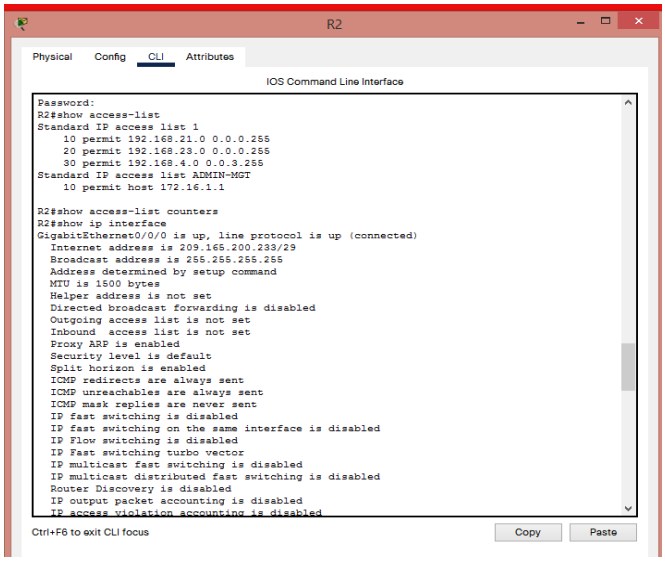


Fuente. Autor

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

Entrada del estudiante (comando): R2#show ip interface

Figura 23 Resultado comando Show ip interface

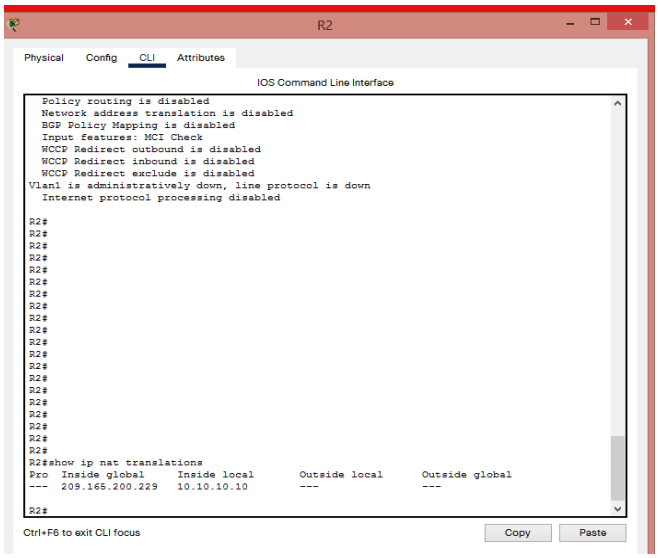


Fuente. Autor

Descripción del comando: ¿Con qué comando se muestran las traducciones NAT?

Entrada del estudiante (comando): R2# show ip nat translations

Figura 24 Resultado comando Show ip nat translations

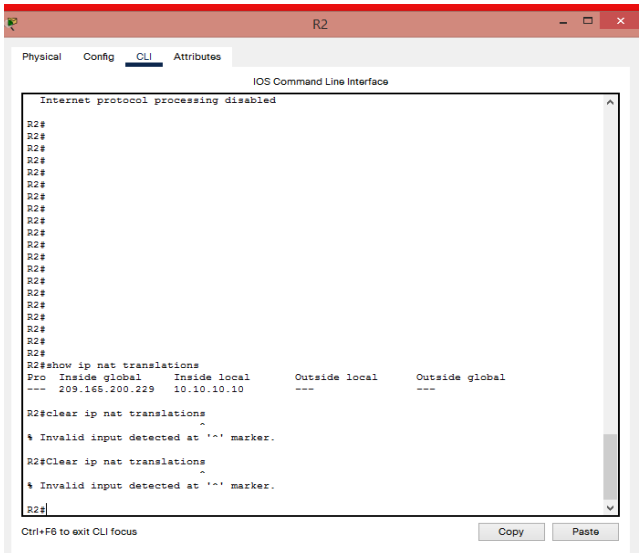


Fuente. Autor

Descripción del comando: ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

Entrada del estudiante (comando): R2# Clear ip nat translations (comando no funciono en el simulador)

Figura 25 Resultado comando Clear ip nat translations



Fuente. Autor

CONCLUSIONES

El estudiante aprendió a diseñar y configurar una red básica por medio de comandos en el programa Packet Tracer, como también se aprendió a validar la interacción de los dispositivos por medio del comando ping.

Se entendió como configurar una red que admita la conectividad IPv4 e IPv6 por comandos en la red.

Se aprendió a configurar y comprender es el propósito de tener una red segura por medio de la creación de cuentas de usuarios y la asignación de contraseñas para los router, switches y otros dispositivos por medio de comandos.

Se aprendió a realizar la traducción de direcciones de red dinámicas y estáticas (NAT) por medio de comandos en una red.

Se implementó el código necesario para configurar las VLAN en los switchs para luego configurar un router como servidor DHCP para que los dispositivos tomen una dirección ip disponible automáticamente.

BIBLIOGRÁFIA

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

Alex Alvarez. (2009). Comandos Basicos de un Router Cisco. mayo 17 de 2009, de Wordpress Sitio web: https://alexalvarez0310.wordpress.com/category/comandos-basicos-de-un-routercisco/

Cisco. (2006). NAT: Definiciones locales y globales. Agosto 24 del 2006, de Cisco Sitio web: https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/4606-8.html

Cisco. (2020). Configurar ACL de IP de uso general. Abril 29 del 2020, de Cisco Sitio web: https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html

Cisco. (2005). Guía de diseño de OSPF. Agosto 10 del 2005, de Cisco Sitio web: https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Cisco. (2005). Configuración dinámica de las opciones del servidor DHCP. Octubre 12 del 2005, de cisco Sitio web: https://www.cisco.com/c/es_mx/support/docs/ip/dynamic-addressallocation-resolution/22920-dhcp-ser.html

CISCO SYSTEMS, CISCO. Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. [sitio web]. Bogotá; [Consultado; 10 de mayo 2020]. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de: http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/CiscoICND2.pdf