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

YEFFERSON BERMUDEZ PALACIOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD) ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIAS (ECBTI)
INGENIERIA DE SISTEMAS
BUENAVENTURA
2021

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

YEFFERSON BERMUDEZ PALACIOS

Diplomado de opción de grado presentado para optar por el título de Ingeniero de Sistemas

Asesora:
Magister MARIA ALEJANDRA LOPEZ HURTADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIAS
INGENIERIA DE SISTEMAS
BUENAVENTURA
2021

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del director

_____

Firma del Tutor

_____

Firma del Jurado

Santiago de Cali, Valle 28/11/2021

AGRADECIMIENTOS

El presente trabajo es dedicado a Dios que ha sido fiel conmigo y me ha sustentado en gran manera en mi carrera profesional y a mi familia, especialmente a mi Madre Yolanda Palacios por estar conmigo, por apoyarme y guiarme, por enseñarme a ser una persona de bien, gracias a los consejos dado por mi madre soy lo que soy y base a eso me han llevado hasta donde estoy ahora.

También quiero agradecer a la Universidad Nacional Abierta y a Distancia (UNAD) y a todos mis tutores y directores en los cursos que pude aprobar en el transcurso de mi carrera profesional, a mis compañeros que fueron clave y me tendieron su mano inmensamente agradecido con ellos.
Por último, agradecido con la tutora y directora del curso del diplomado de profundización de cisco por ese último empujón hacia la culminación de mi etapa formativa como profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Ethernet: La capa física de interconexión de sistemas abiertos (OSI) proporciona el medio para transportar los bits que componen una trama de capa de enlace de datos a través de los medios de red.

Gateway predeterminado: El gateway predeterminado es el dispositivo de red que puede enrutar el tráfico a otras redes. Es el router el que puede enrutar el tráfico fuera de la red local. Si se piensa en una red como si fuera una habitación, el gateway predeterminado es como la puerta. Si desea ingresar a otra habitación o red, debe encontrar la puerta.

Direcciones IPv4: El sistema binario es un sistema numérico que consiste en los números 0 y 1, denominados bits. En comparación, el sistema numérico decimal consiste en 10 dígitos, que incluyen los números 0 a 9.

Terminales: Los dispositivos de red con los que la gente está más familiarizada se denominan terminales. Un terminal es el origen o el destino de un mensaje transmitido a través de la red, como se muestra en la animación de la figura. Para distinguir un terminal de otro, cada terminal en la red se identifica por una dirección. Cuando un terminal inicia una comunicación, utiliza la dirección del terminal de destino para especificar adónde se debe enviar el mensaje.

Mascara subred: es la dirección que te asigna tu IPS empresa que da el acceso a internet como telefonía, y sirve para identificarte dentro de internet cuando te conectas, pero la IP por si sola tampoco sirve para identificarte en la red. A esta dirección la vas a tener que acompañar siempre de la máscara9 de subred. A efectos prácticos se trata de otra IP, pero cuya numeración casi siempre va a estar compuesta por ceros y 255.

Switch: es un dispositivo de interconexión utilizado para conectar equipos de red formando lo que se conoce como una red de área local (LAN) cuyas especificaciones técnicas siguen el estándar conocido como ethernet. Es importante tener claro que un switch NO proporciona por si solo conectividad con otras redes, y obviamente tan poca conectividad con internet.

RESUMEN

En el tiempo del proceso de aprendizaje que he tenido en el diplomado de profundización CISCO (diseños e implementaciones de soluciones integradas LAN/WAN) (OPCI - (203092A_954, se desarrolló cada uno los módulos del curso correspondientes CCNA, donde se adquirió habilidades de poder configurar dispositivos PC, Router, Switch entre otros de las simulaciones de los escenarios propuesto.

En este primer escenario 1 se configura los dispositivos de una red pequeña donde se debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN1 LAN2.

En el segundo escenario 2 es una topología más grande en este escenario se plantean aspectos como: 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.

palabras claves: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In the time of the learning process that I have had in the CISCO deepening diploma (designs and implementations of integrated solutions LAN / WAN) (OPCI - (203092A_954), each one of the corresponding CCNA course modules was developed, where power skills were acquired configure PC devices, Router, Switch among others of the simulations of the proposed scenarios.

In this first scenario 1, the devices of a small network are configured where a router, a switch and equipment must be configured, and the IPv4 addressing scheme for the LAN1 LAN2 must be designed.

In the second scenario 2 is a larger topology in this scenario, aspects such as: a small network must be configured to support IPv4 and IPv6 connectivity, switch security, routing between VLANs, the dynamic routing protocol OSPF, the protocol of dynamic host configuration (DHCP), static and dynamic network address translation (NAT), access control lists (ACL), and server / client Network Time Protocol (NTP). During the evaluation, you will test and register your network using common CLI commands.

keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

INTRODUCCIÓN

La simulación de las redes ha venido evolucionando, en cuanto a sus versiones del simulador de packet trecer donde por medio de este programa podemos crear topología de red, enviar paquetes de información de un dispositivo a otro, y luego ver en modo simulación la transmisión de datos. Estas tecnologías deben ir adaptándose y evolucionando para cumplir con las necesidades comunicativas de las personas en distintos ámbitos sociales.

En este documentos veremos la configuración de 2 escenarios dados, donde relacionan los temas que hemos vistos al paso de diplomado cisco, las actividades y ejercicios como configuración: router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas, 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 y entre otros.

Por último, el simulador de packet tracer es indispensable estarcapacitado para con esta aplicación para comprender su lógica, su funcionamiento y poder solucionar problemáticas relacionadas con redes de distintos tipos.

DESARROLLO ESCENARIO 1

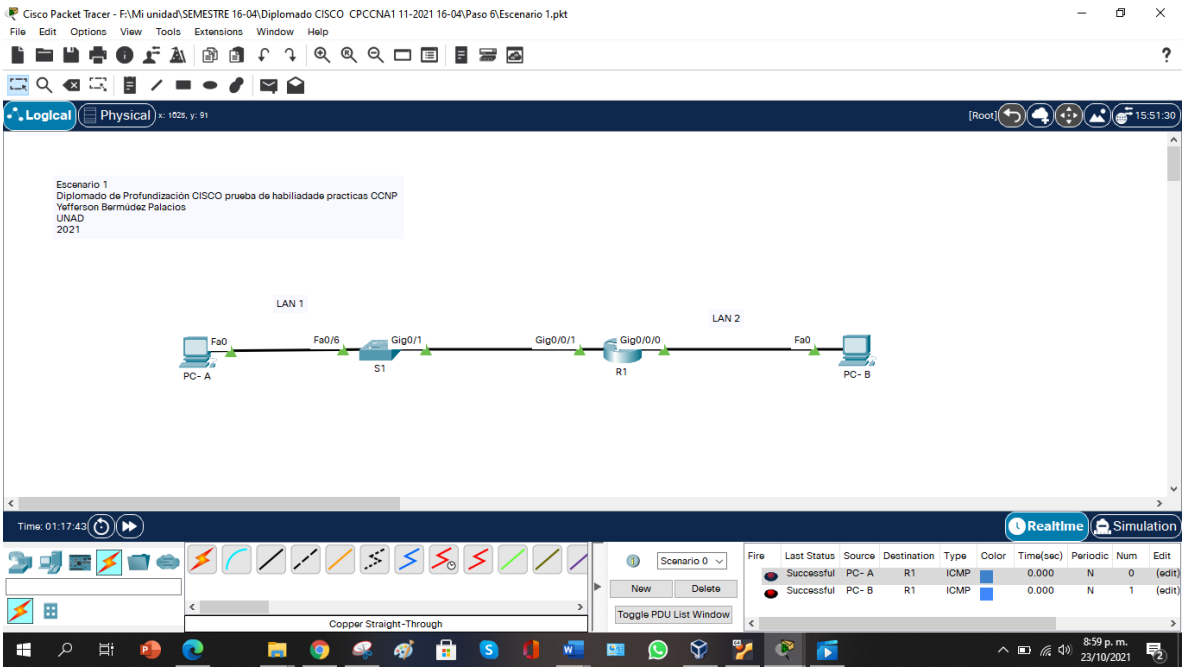
Figura 1 Topología escenario 1.

Fuente: Elaboración propia

Como trabajo inicial se debe realizar lo siguiente:

- Realizar una construcción de red de acuerdo con la topología lógica que se plantea en la figura 1.
- Realizar el direccionamiento de las subredes LAN 1 y LAN 2 y desarrollar las configuraciones básicas de router y switch.
- Realizar la conexión física de los equipos con base en la topología de red.

Figura 2: Escenario propuesto



Fuente: Elaboración propia 1

Tabla 1 direccionamiento del escenario 1

Item	Requerimiento
Dirección de Red	192.168.89.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.89.1
R1 G0/0/0	192.168.89.129
S1 SVI	192.168.89.2
PC-A	192.168.89.126
PC-B	192.168.89.190

Fuente: Elaboración propia

Paso 1: Configuración y ajuste básico del Router - R1

Tabla 2 Configuración de R1

Tarea	**Especificaciones**
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com R1(config)#
Contraseña cifrada para el modo EXEC privilegiado	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
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line) #login local R1(config-line) #exit R1(config)#
Configurar VTY solo aceptando SSH	R1(config)#hostname R1 R1(config)#ip domain-name ccna-lab.com

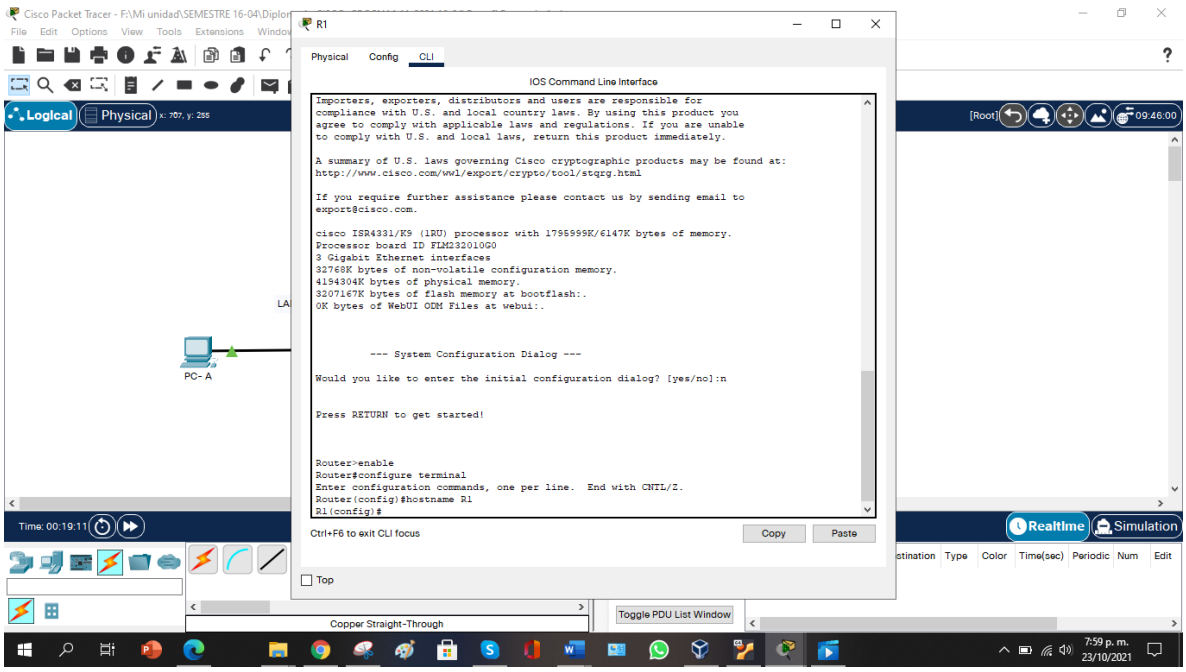
	R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024? % Generating 1024 bit RSA keys, keys will be non-exportable..[OK] R1(config)#ip ssh version 2 *Mar 1 0:38:50.383: %SSH-5-ENABLED: SSH 1.99 has been enabled R1(config)#ip ssh authentication-retries 2 R1(config)#line vty 0 15 R1(config-line) #login local R1(config-line) #exit R1(config)#username admin password admin1pass R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd $ESTUDIANTES CISCOSUNAD$
Configurar interfaz G0/0/0	R1(config)#interface gi0/0/0 R1(config-if) #ip add 192.168.89.129 255.255.255.128 R1(config-if) #no shut R1(config-if) # %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

	R1# %SYS-5-CONFIG_I: Configured from console by console
Configurar interfaz G0/0/1	R1(config)#interface gi0/0/1 R1(config-if)#ip add 192.168.89.1 255.255.255.128 R1(config-if) #no shut R1(config-if) # %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa % You already have RSA keys defined named R1.ccna-lab.com. % Do you really want to replace them? [yes/no]: y 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]

Fuente: Elaboración propia

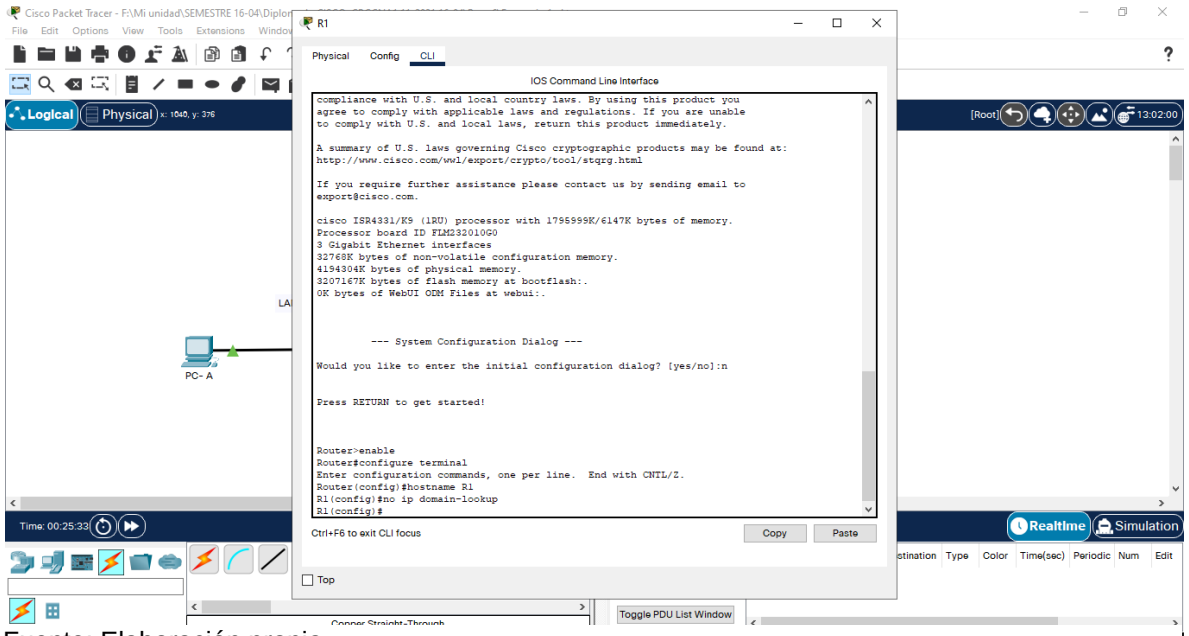
*Nota se precede con la ilustración de cada punto de la configuración del R1

Figura 3 Nombre del router



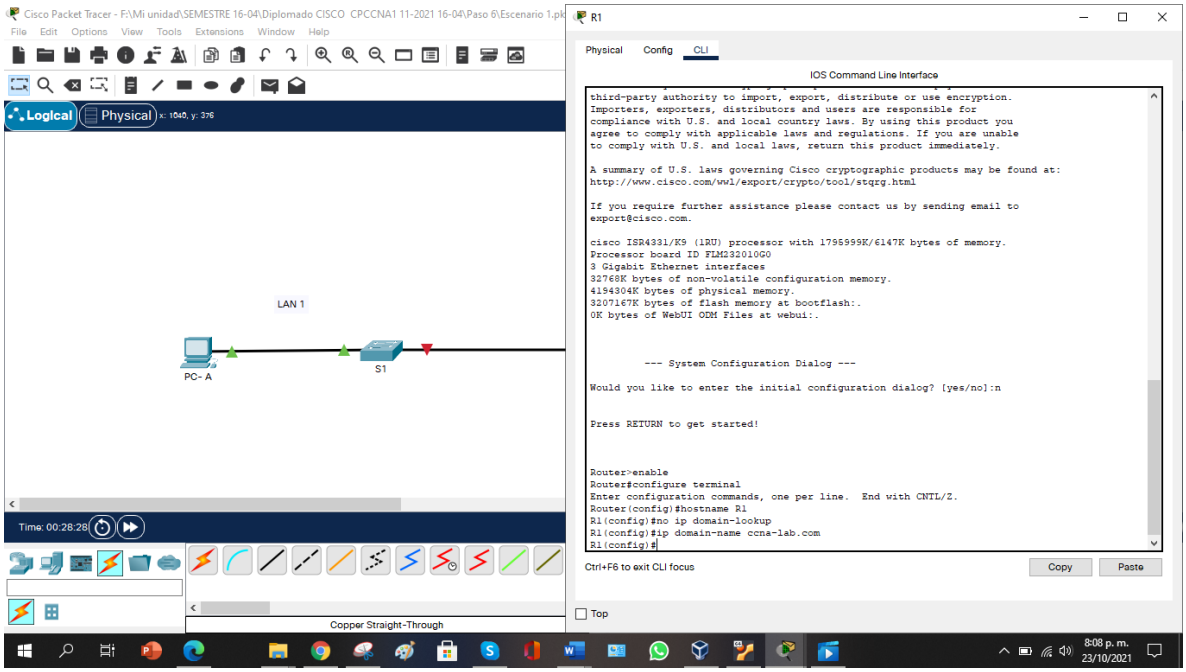
Fuente: Elaboración propia

Figura 4 Desactivar la búsqueda DNS



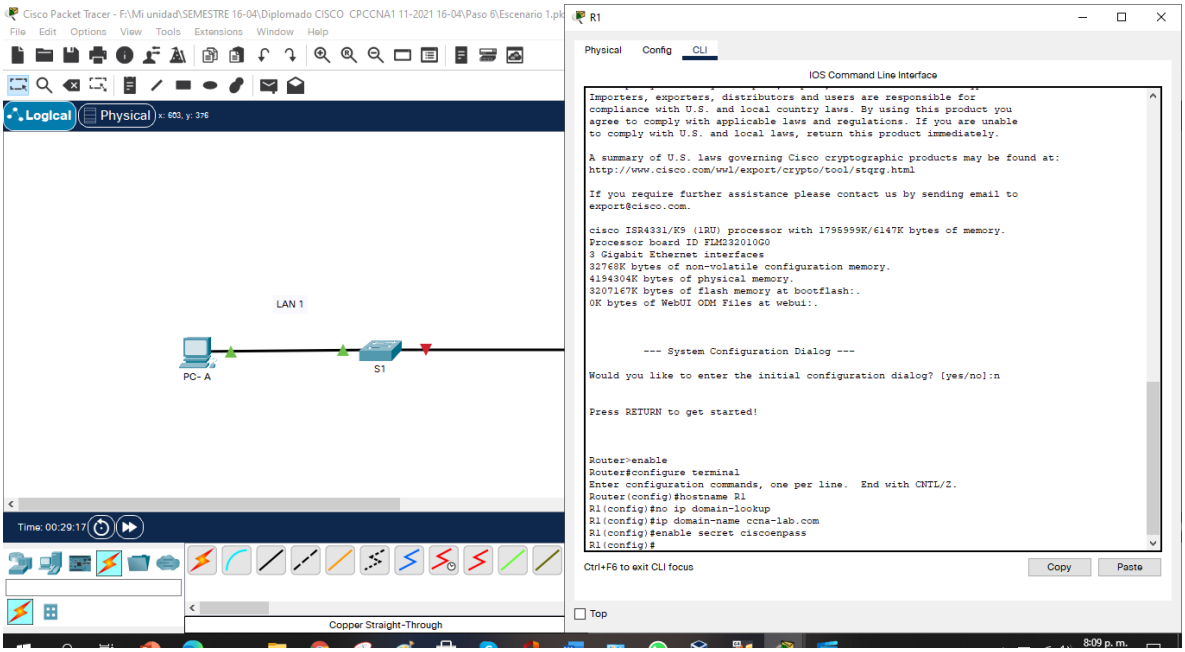
Fuente: Elaboración propia

Figura 5 Nombre de dominio



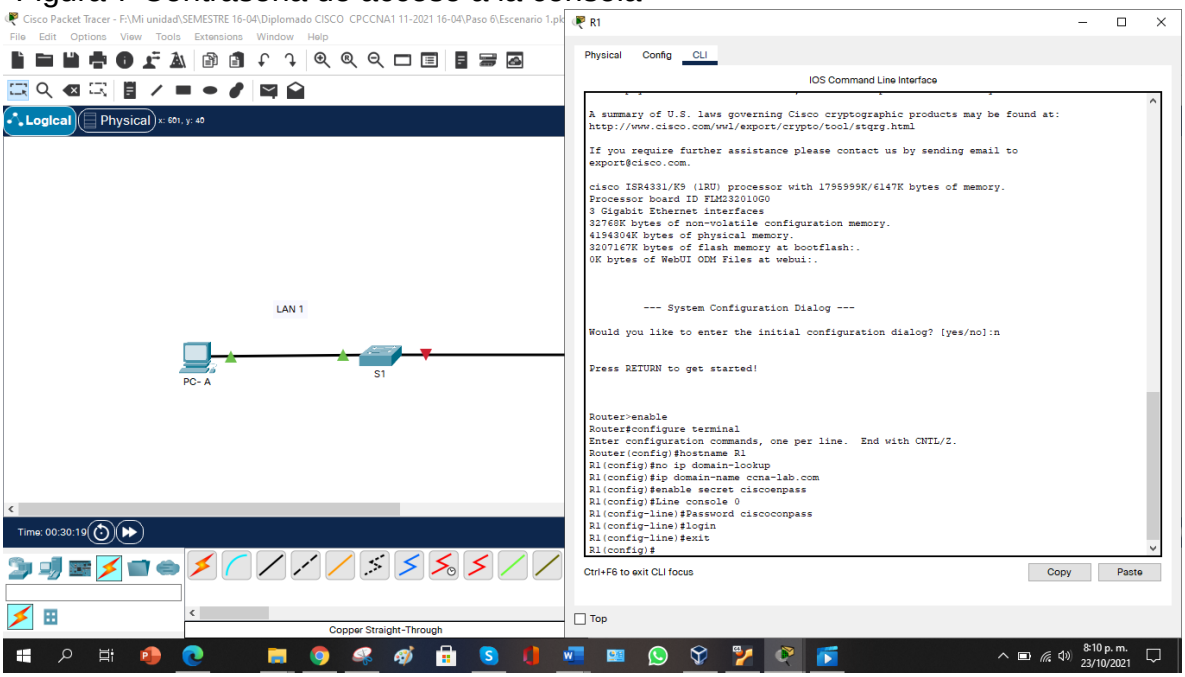
Fuente: Elaboración propia

Figura 6 Contraseña cifrada para el modo EXEC Privilegiado



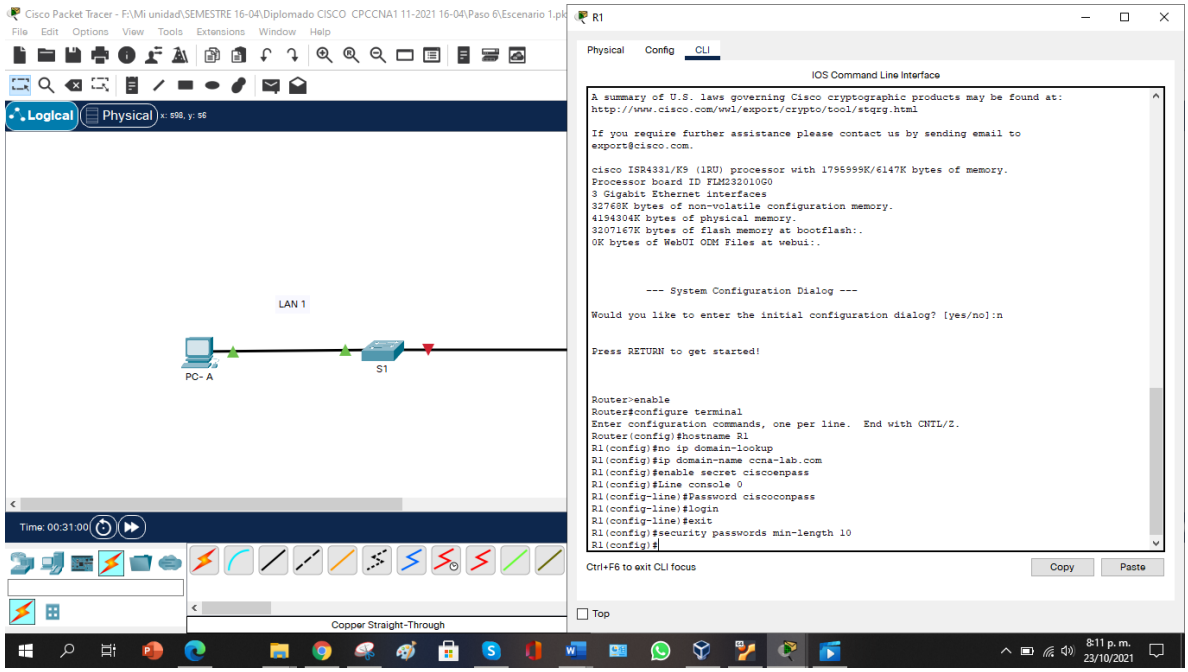
Fuente: Elaboración propia 2

Figura 7 Contraseña de acceso a la consola



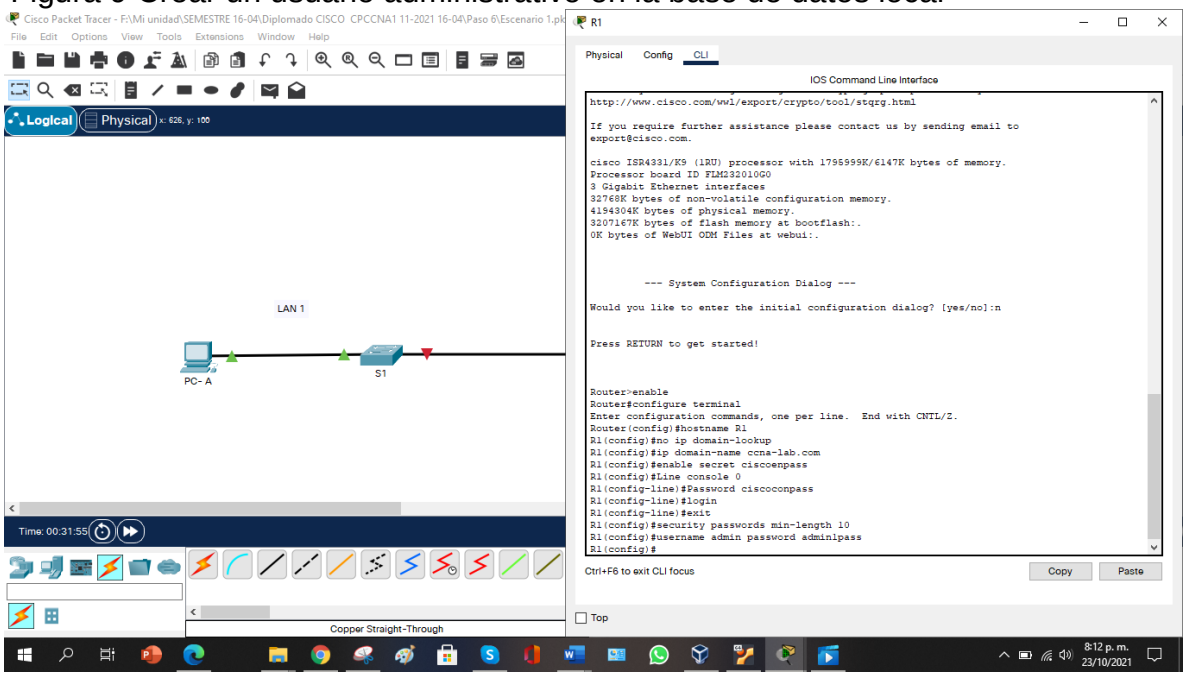
Fuente: Elaboración propia

Figura 8 Establecer la longitud mínima para las Contraseñas



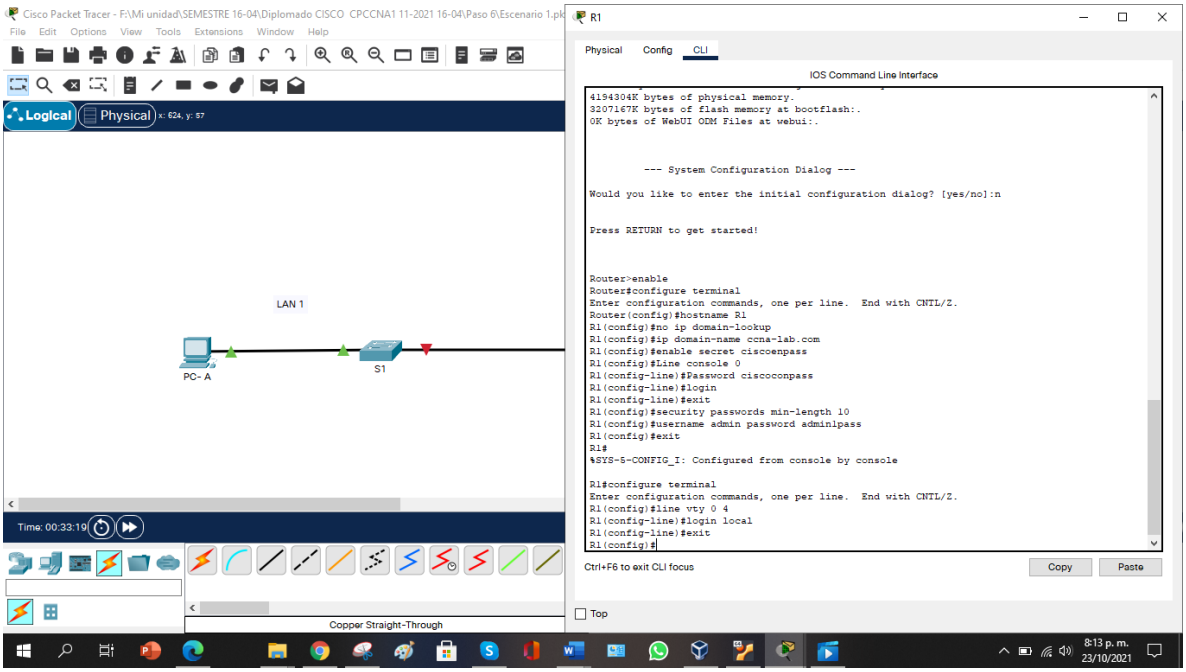
Fuente: Elaboración propia

Figura 9 Crear un usuario administrativo en la base de datos local



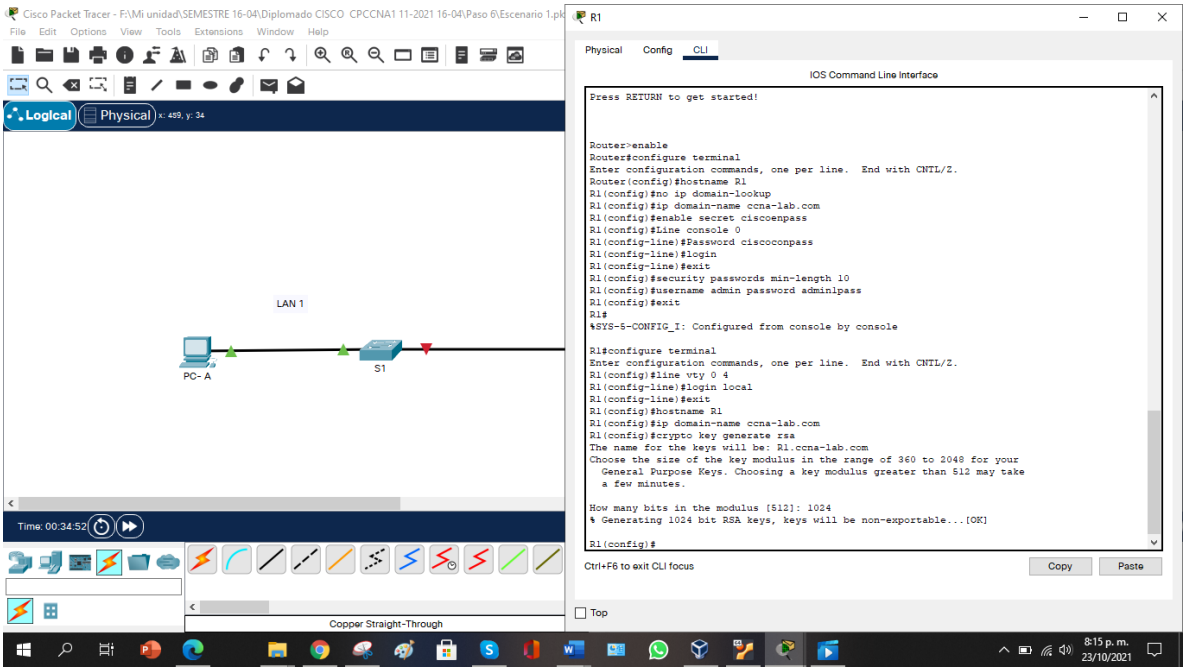
Fuente: Elaboración propia

Figura 10 Configurar el inicio de sesión en las líneas VTY para que use la base de datos local



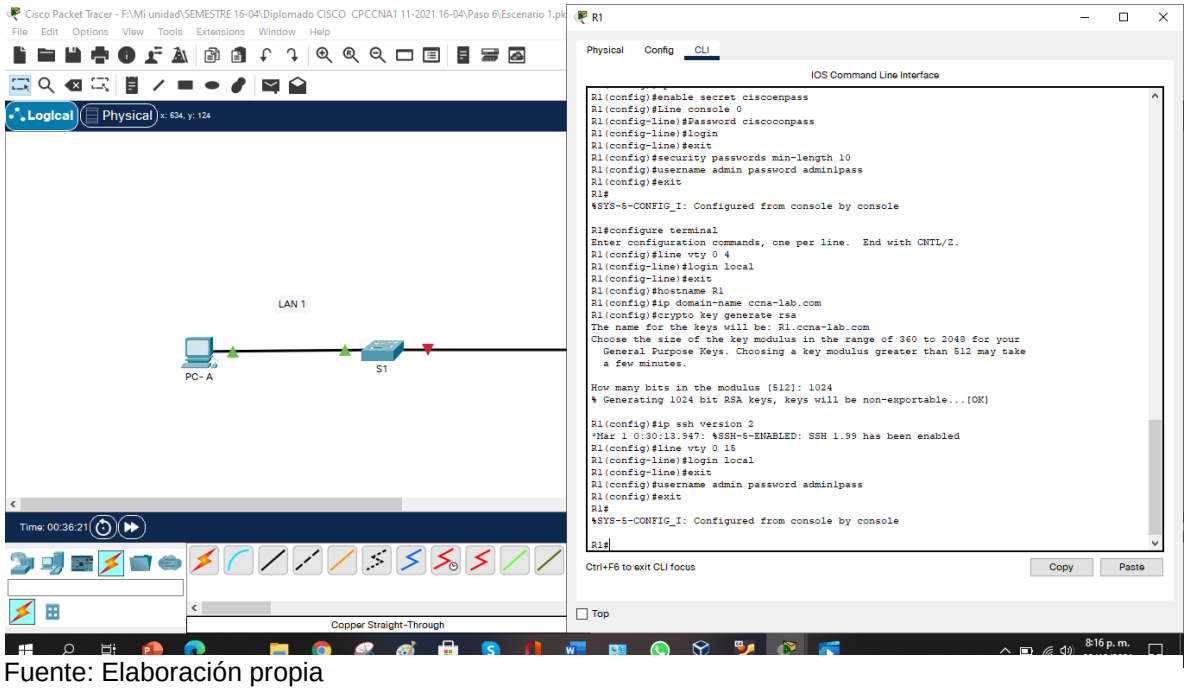
Fuente: Elaboración propia 1

Figura 11 Configurar VTY solo aceptando SSH



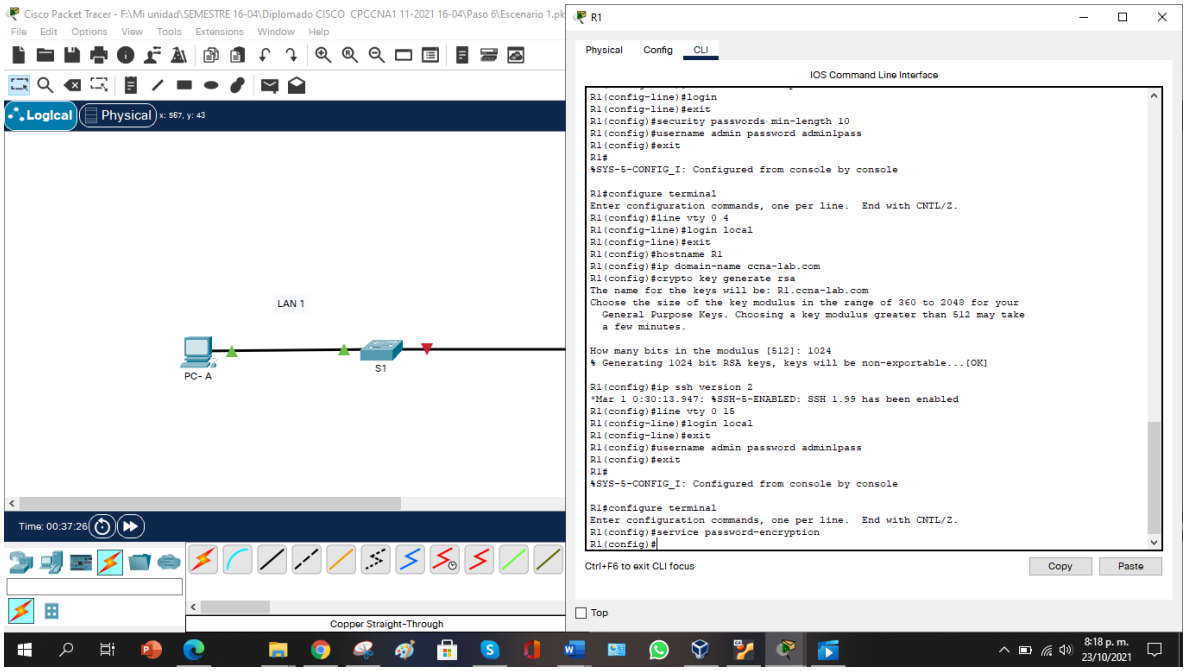
Fuente: Elaboración propia

Figura 12 Configurar VTY solo aceptando SSH



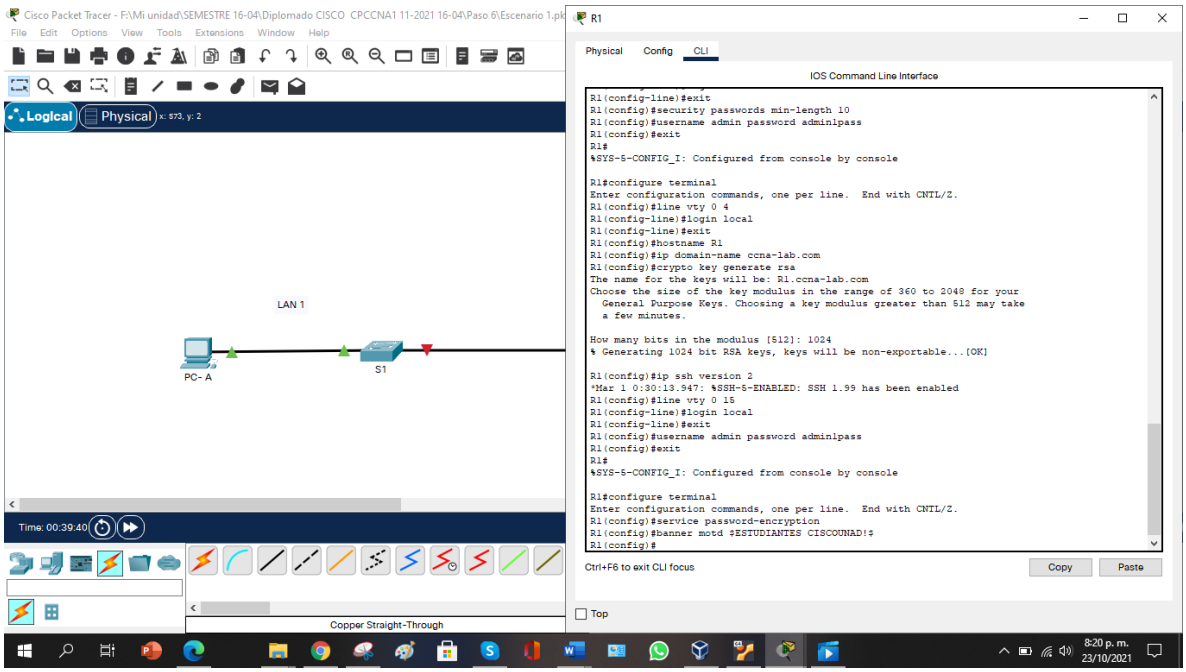
Fuente: Elaboración propia

Figura 13 Cifrar las contraseñas de texto no cifrado



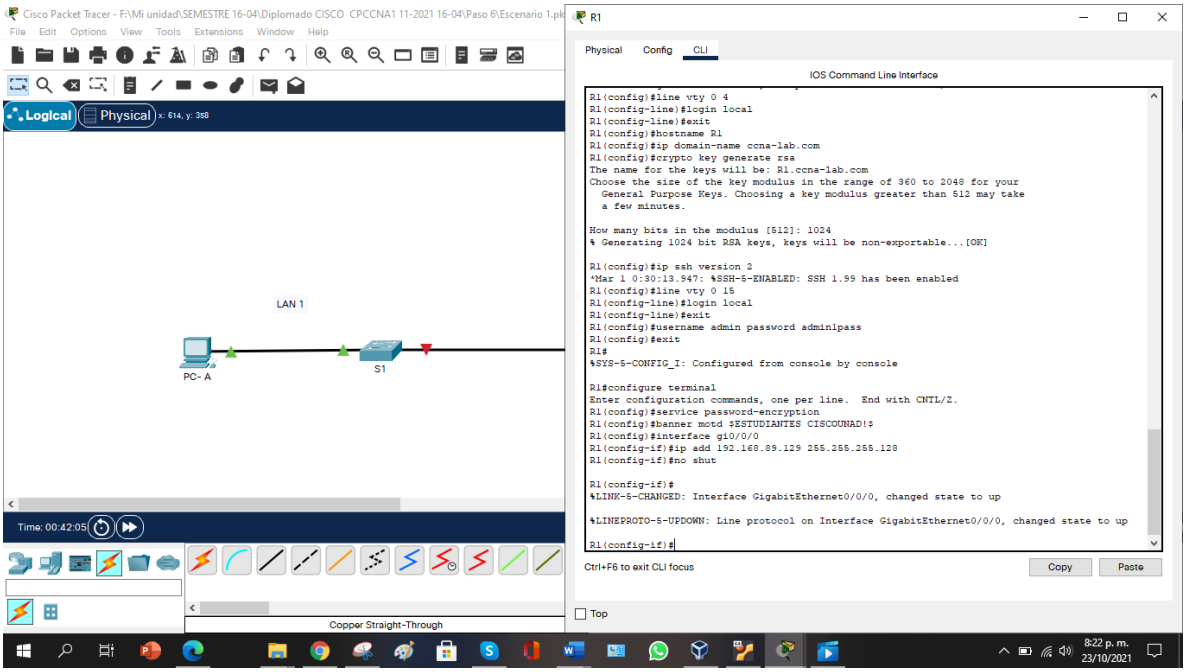
Fuente: Elaboración propia

Figura 14 Configure un MOTD Banner



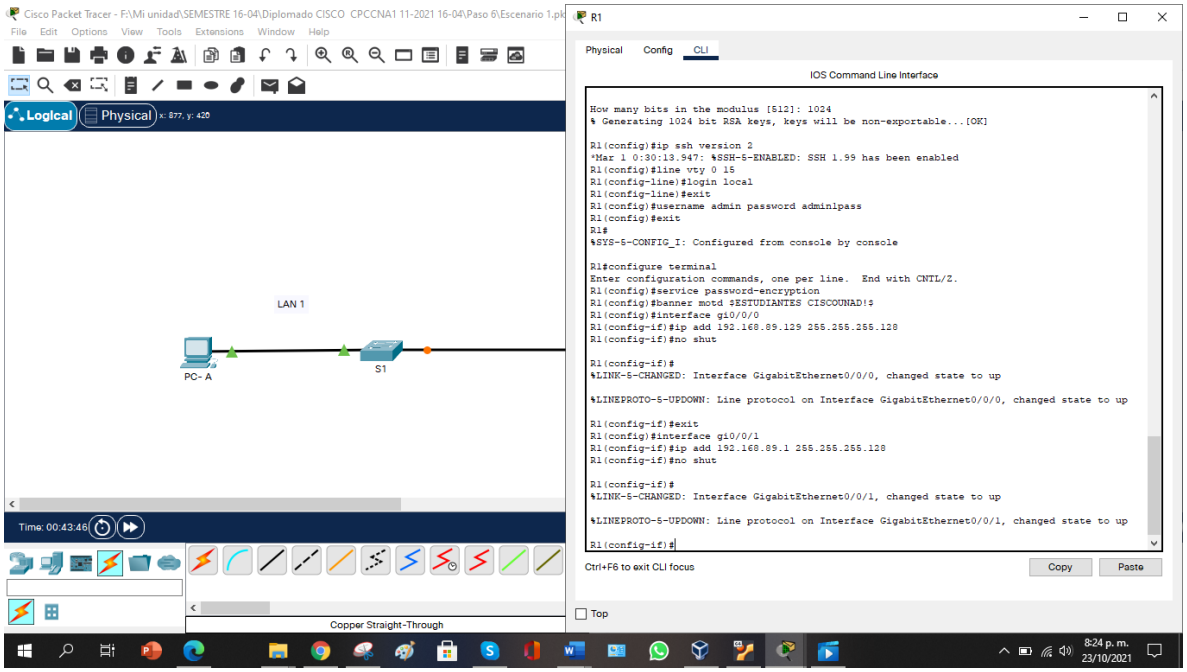
Fuente: Elaboración propia

Figura 15 Configurar interfaz G0/0/0



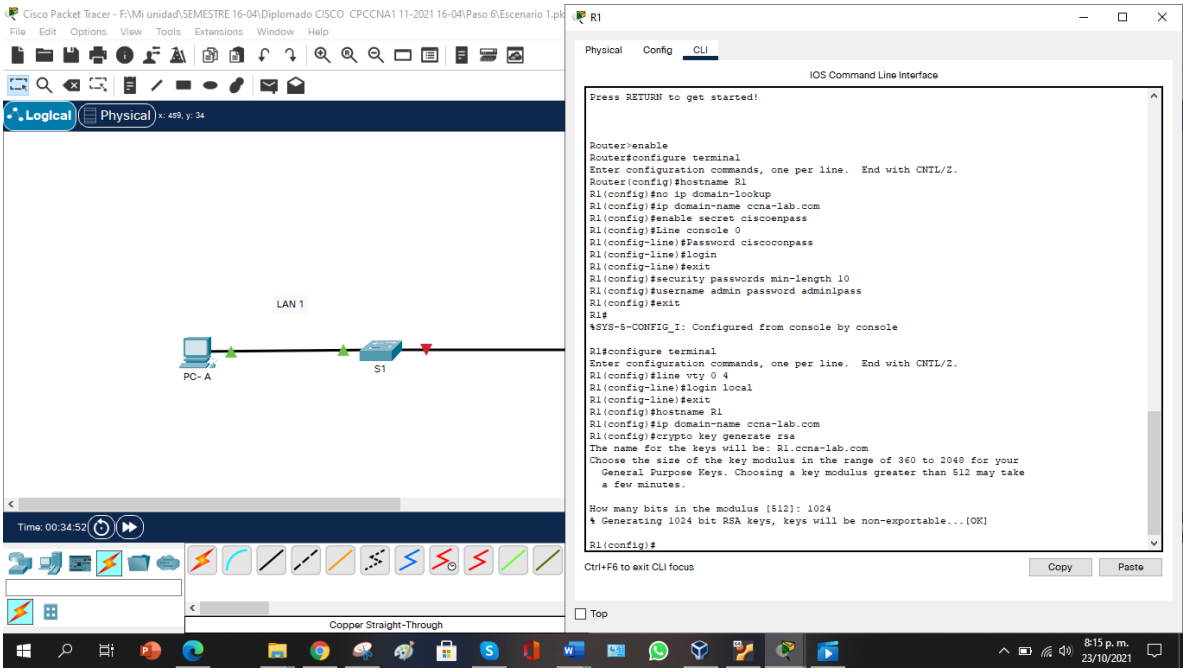
Fuente: Elaboración propia

Figura 16 Configurar interfaz G0/0/1



Fuente: Elaboración propia

Figura 17 Generar una clave de cifrado RSA



Fuente: Elaboración propia

Paso 2: Configuración inicial S1

Tabla 3 Configuración de S1

Tarea	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname 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) #login S1(config-line) #exit
Establecer la longitud mínima para las Contraseñas	S1(config)#security passwords min-length 10
Crear un usuario	S1(config)#username admin password

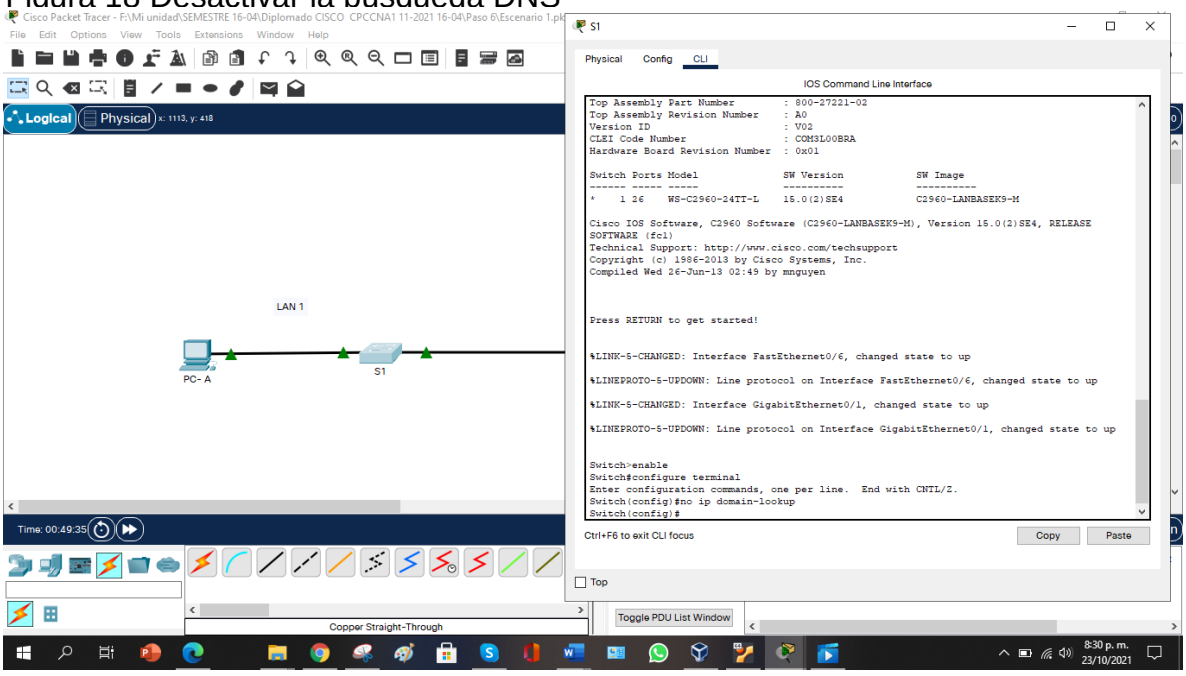
administrativo en la base de datos local	admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line) #login local S1(config-line) #exit
Configurar VTY solo aceptando SSH	S1(config)#hostname S1 S1(config)#ip domain-name ccna-lab.com S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]:1024 % Generating 1024-bit RSA keys, keys will be non-exportable... [OK] S1(config)#ip ssh version 2 *Mar 1 4:7:0.42: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config)#line vty 0 15 S1(config-line) #login local S1(config-line) #exit S1(config)#username admin password admin1pass S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configure un MOTD Banner	S1(config)#banner motd $ESTUDIANTES CISCOUNAD$
Configurar la interfaz de administración (SVI)	S1(config)#int vlan 1 S1(config-if) #ip add 192.168.89.2 255.255.255.0 S1(config-if) #no shut S1(config-if) # %LINK-5-CHANGED: Interface Vlan1, changed state to up

	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up exit S1(config)#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa % You already have RSA keys defined named S1.ccna-lab.com. % Do you really want to replace them? [yes/no]: y 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]
Configuración del gateway predeterminado	S1(config)#ip default-gateway 192.168.89.1

Fuente: Elaboración propia 2

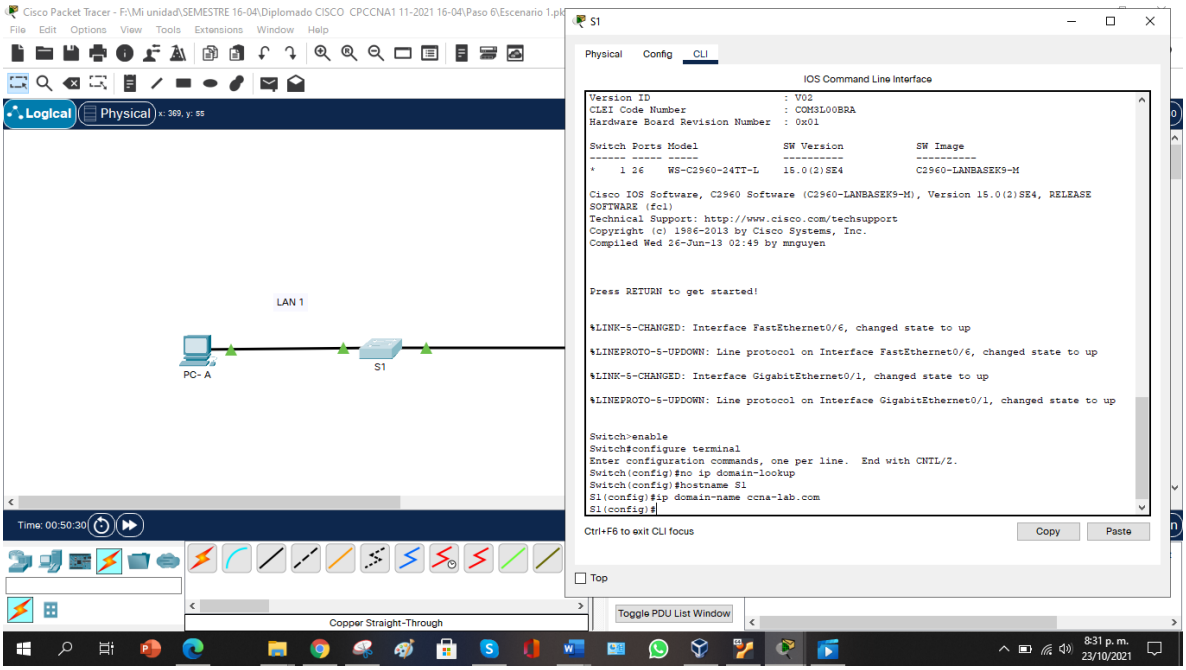
*Nota se precede con la ilustración de cada punto de la configuración del S1

Figura 18 Desactivar la búsqueda DNS



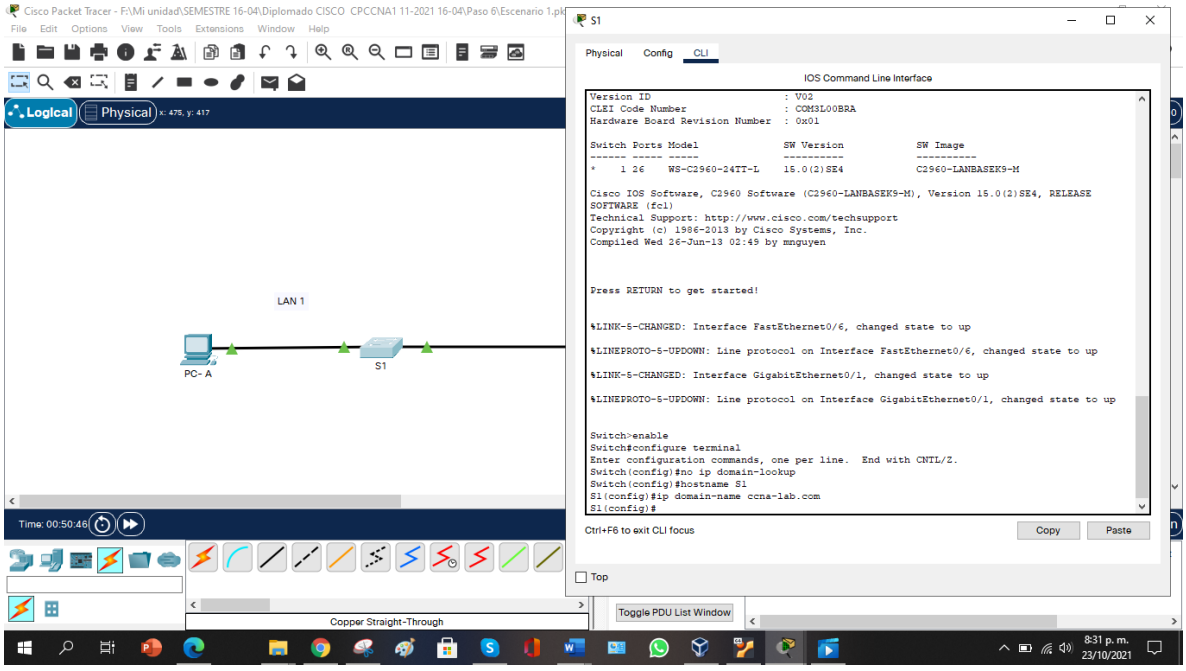
Fuente: Elaboración propia

Figura 19 Nombre del switch



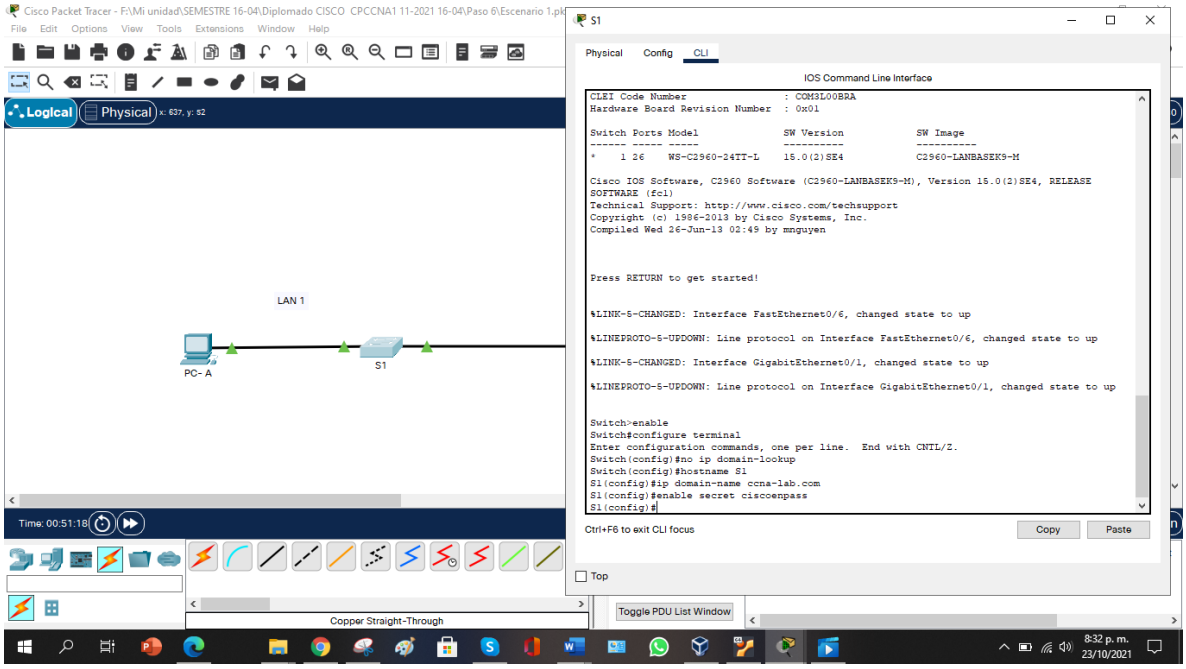
Fuente: Elaboración propia

Figura 20 Nombre de dominio



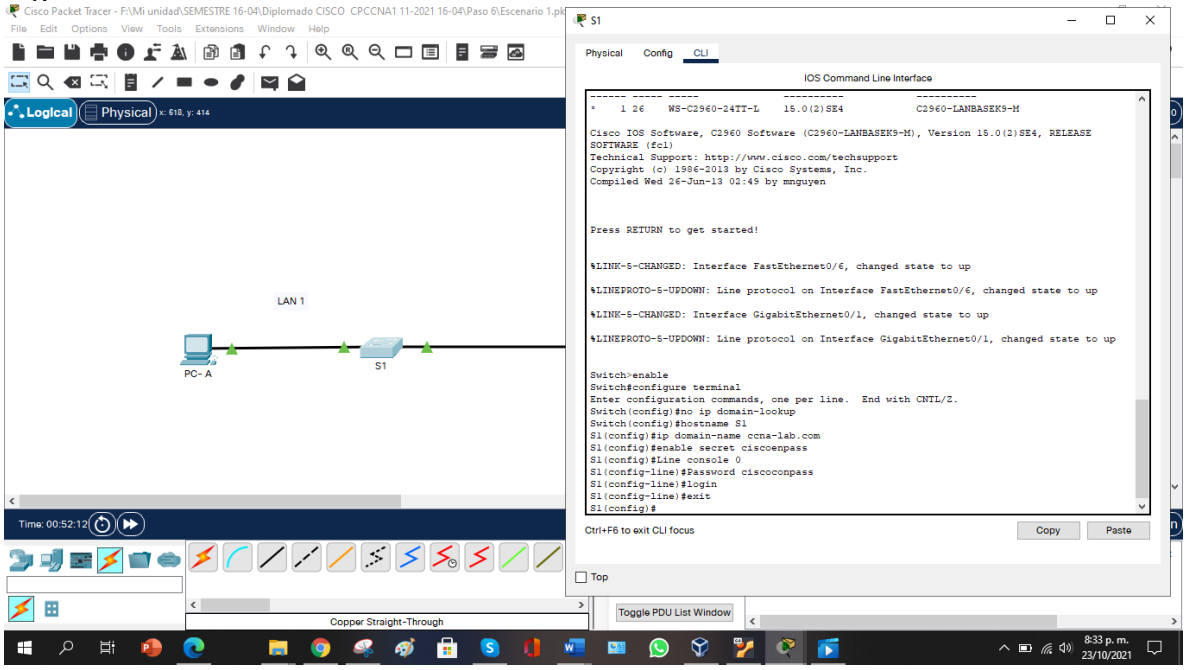
Fuente: Elaboración propia

Figura 21 Contraseña cifrada para el modo EXEC Privilegiado



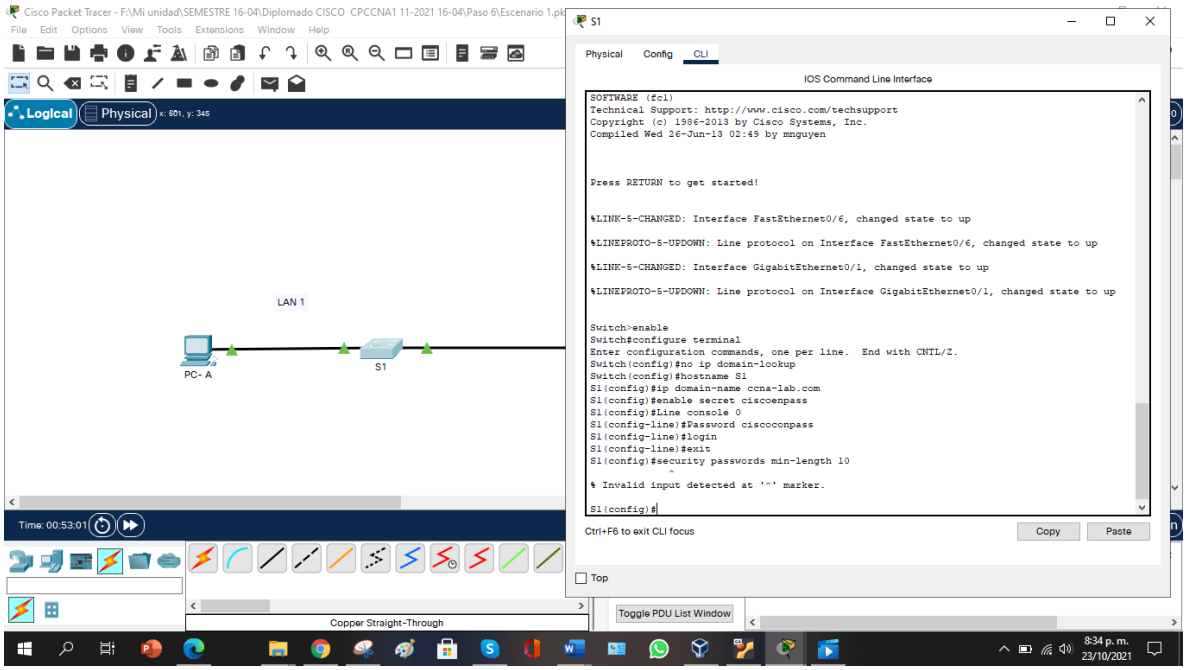
Fuente: Elaboración propia

Figura 22 Contraseña de acceso a la consola



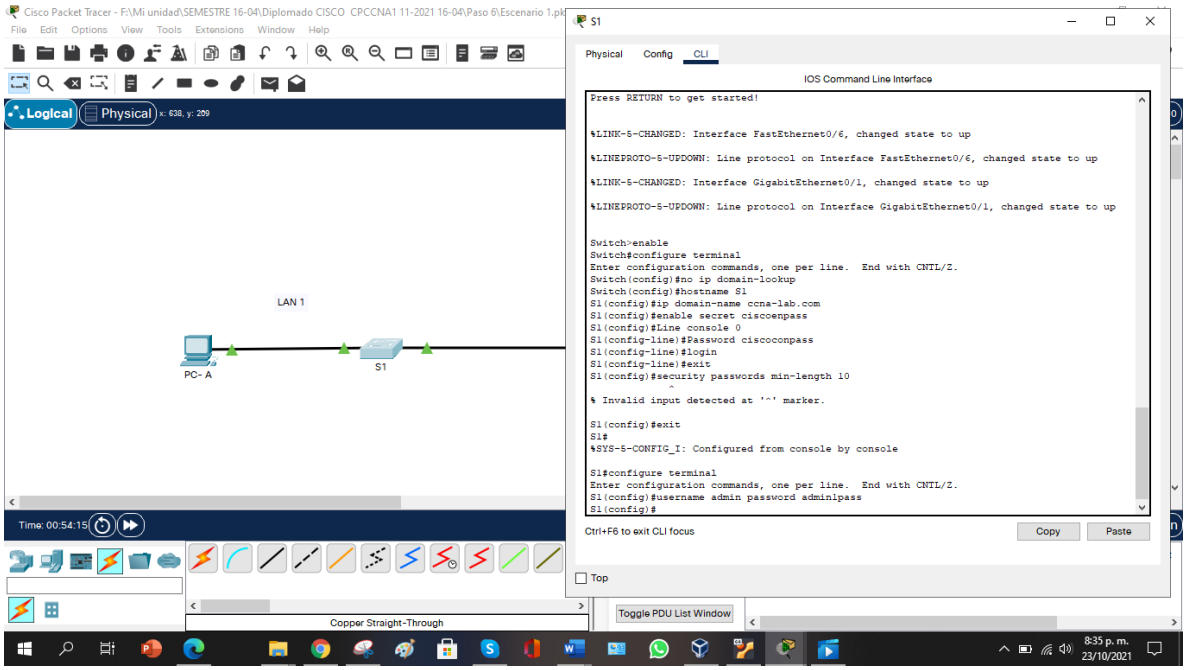
Fuente: Elaboración propia

Figura 23 Establecer la longitud mínima para las Contraseñas



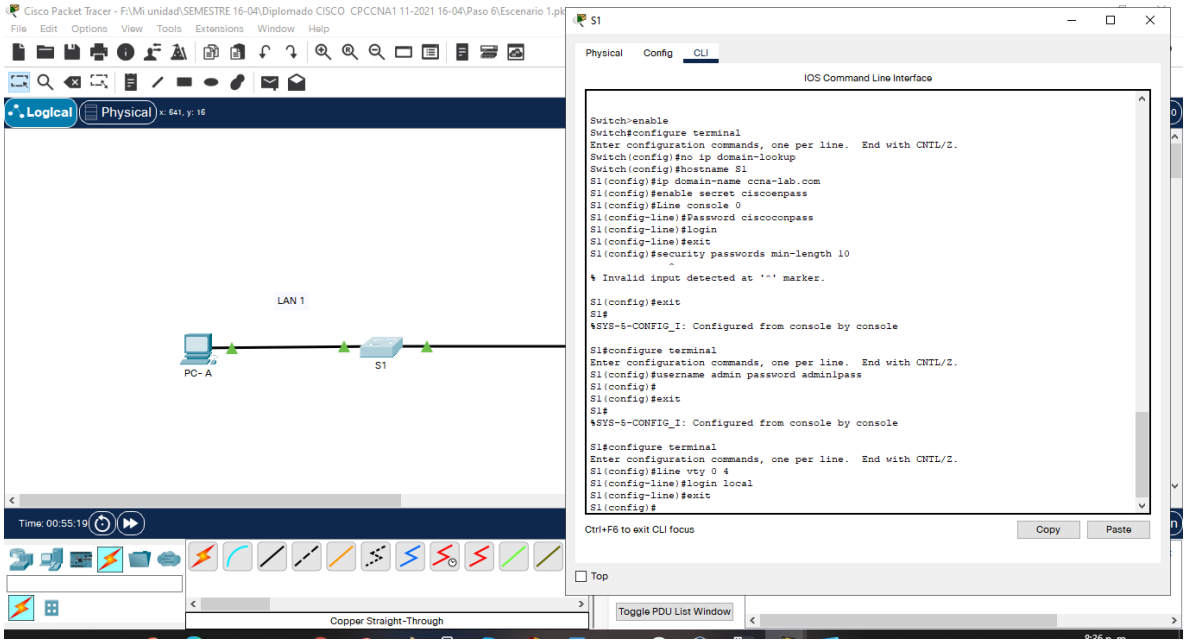
Fuente: Elaboración propia

Figura 24 Crear un usuario administrativo en la base de datos local



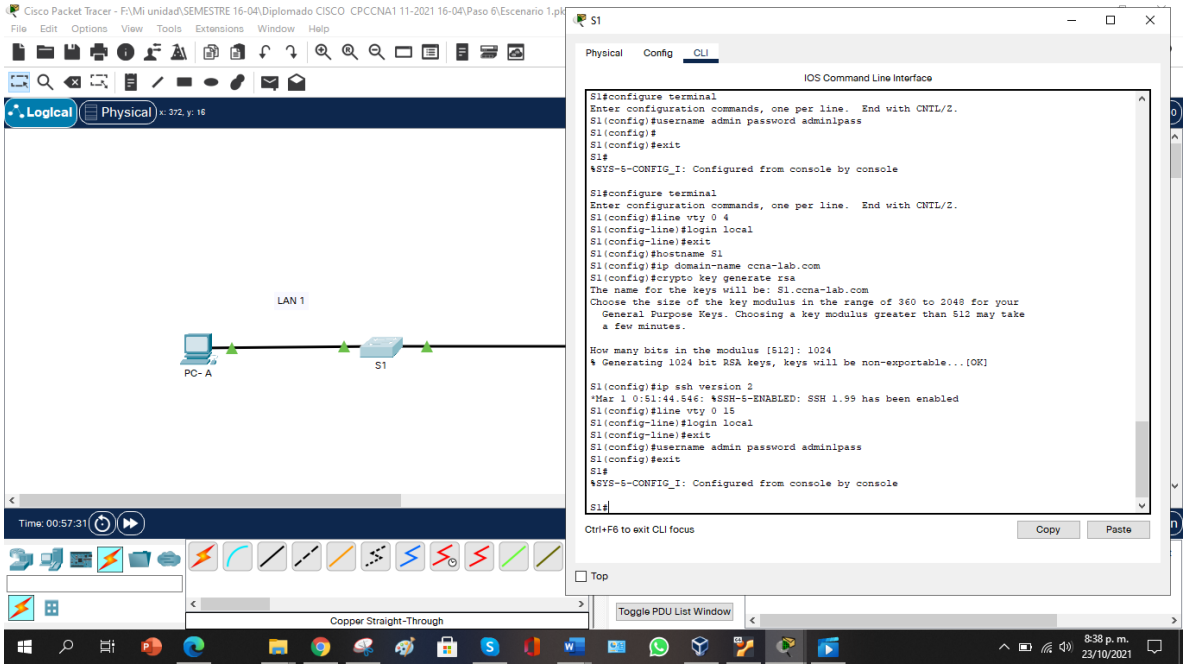
Fuente: Elaboración propia

Figura 25 Configurar el inicio de sesión en las líneas VTY para que use la base de datos local



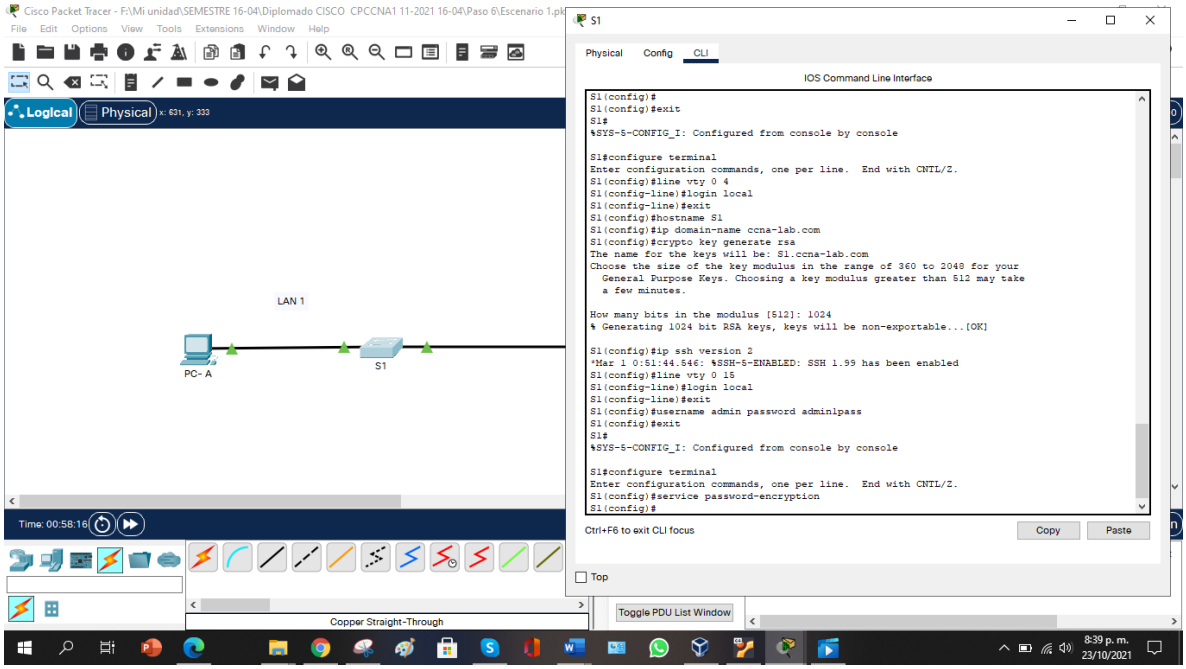
Fuente: Elaboración propia

Figura 26 Configurar VTY solo aceptando SSH



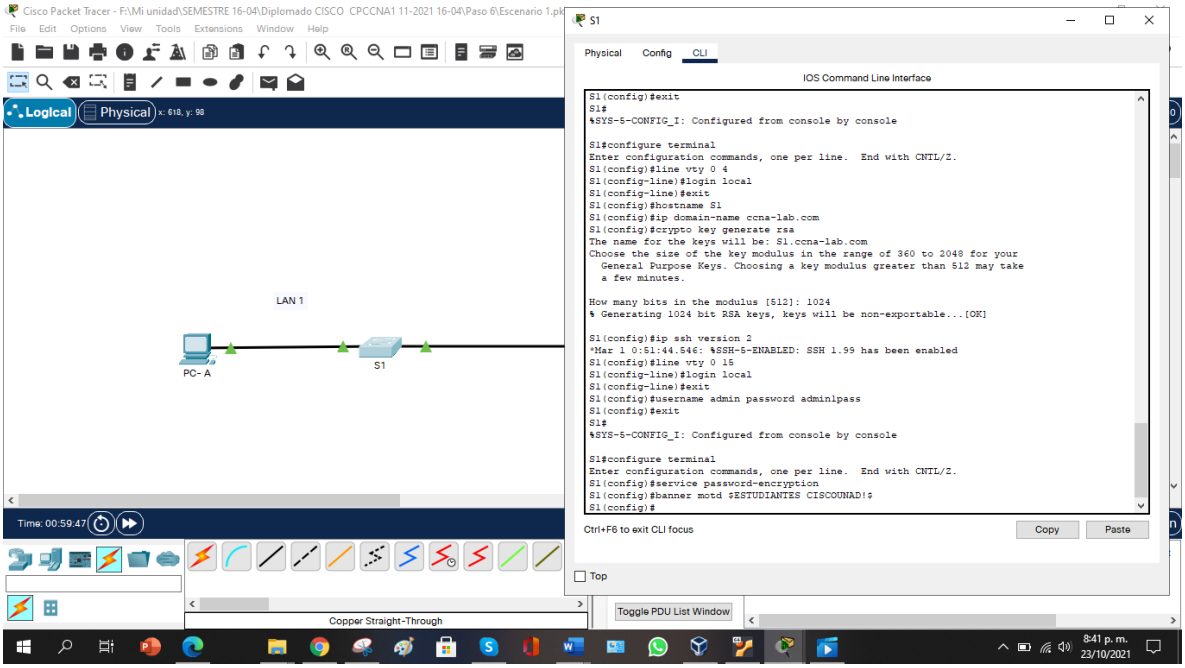
Fuente: Elaboración propia

Figura 27 Cifrar las contraseñas de texto no cifrado



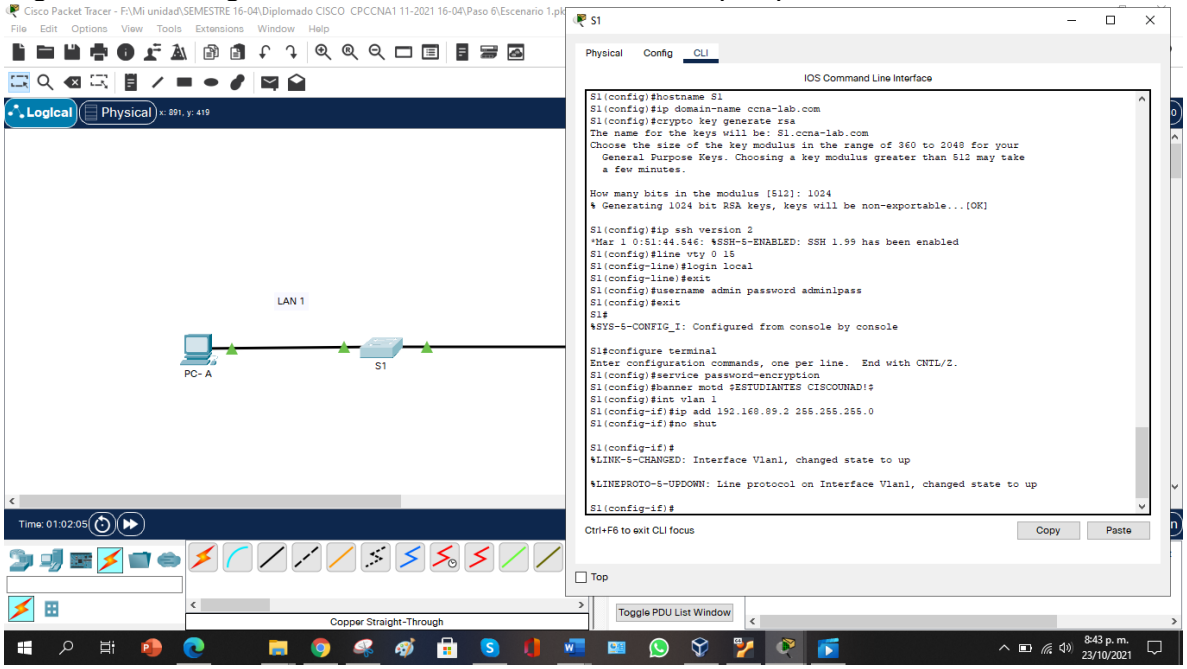
Fuente: Elaboración propia

Figura 28 Configure un MOTD Banner



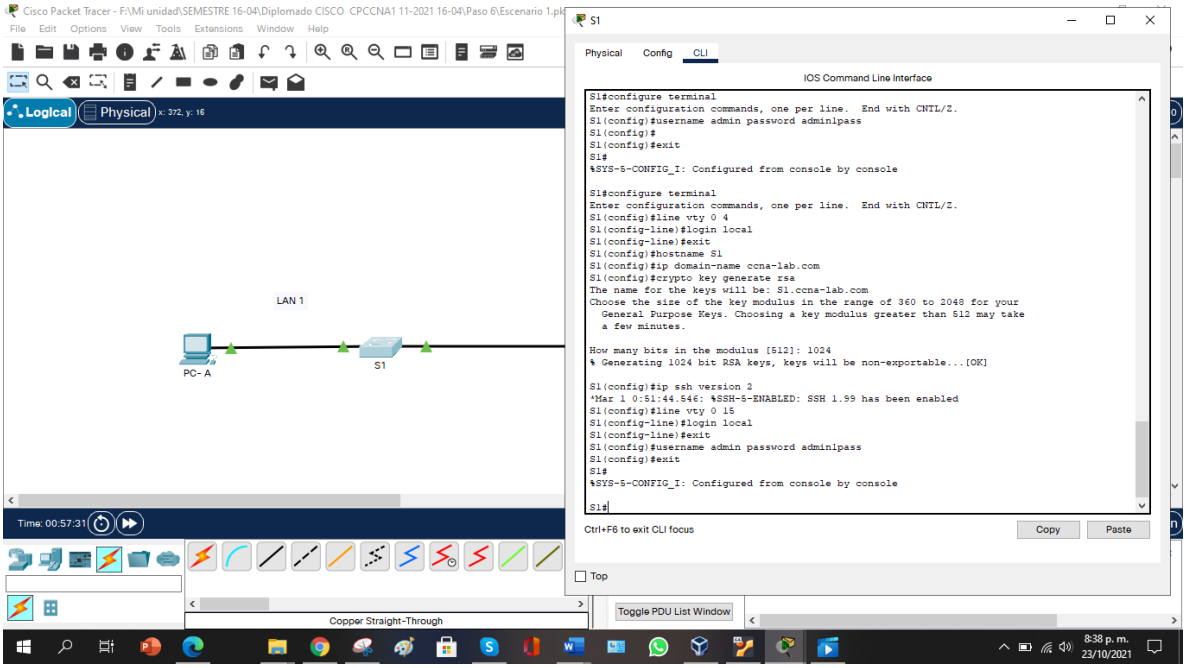
Fuente: Elaboración propia

Figura 29 Configurar la interfaz de administración (SVI)



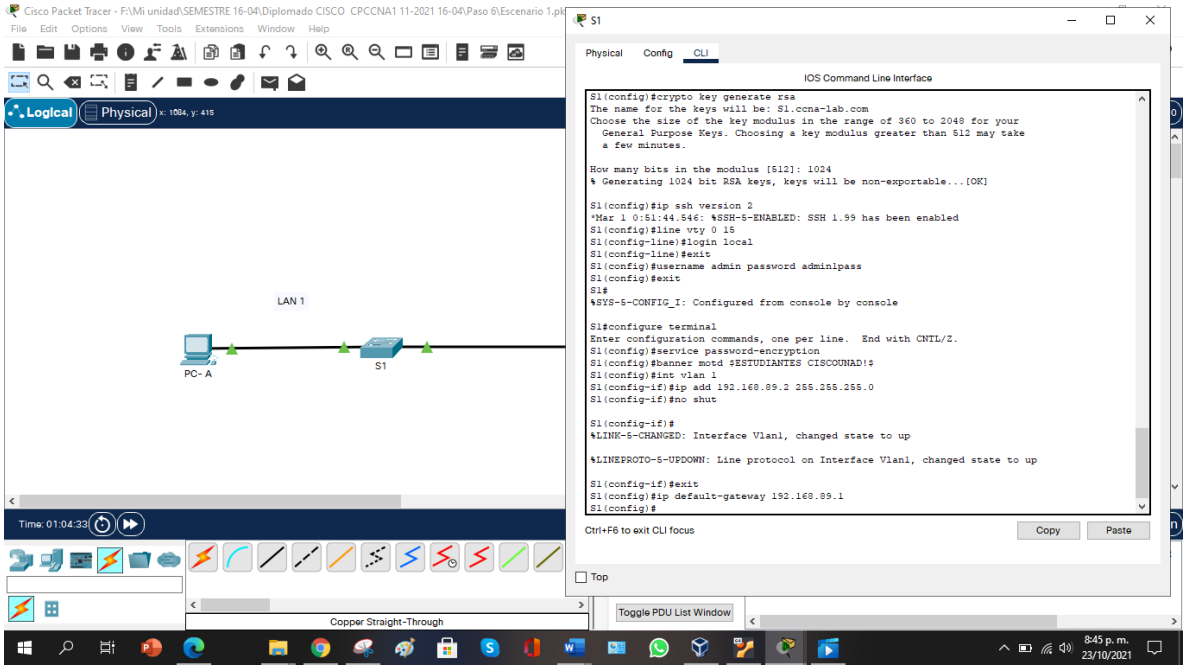
Fuente: Elaboración propia

Figura 30 Generar una clave de cifrado RSA



Fuente: Elaboración propia

Figura 31 Configuración del gateway predeterminado



Fuente: Elaboración propia

*Nota: se procede con la configuración inicial de los dispositivos expuestos en la topología de red que es PC-A:

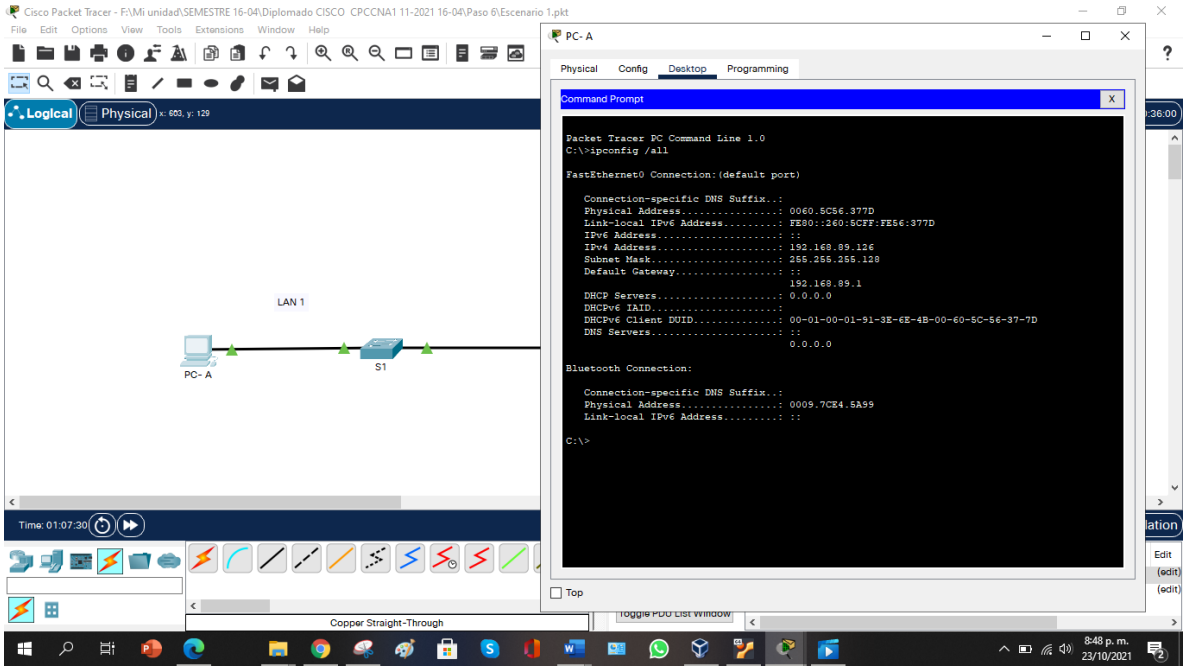
Paso 3. Configuración computador PC-A

Tabla 4 descripción PC-A

PC-A Configuración de la red	
Descripción	PC-A este dispositivo está conectado a la LAN 1 que cuenta con 126 Host utilizables y su dirección IP es la última utilizable, conectado al R1 por medio de la interfaz g0/0/1.
Dirección física	0060.5C56.377D
Dirección IP	192.168.89.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.89.1

Fuente: Elaboración propia

Figura 32 Descripción del PC-A



Fuente: Elaboración propia

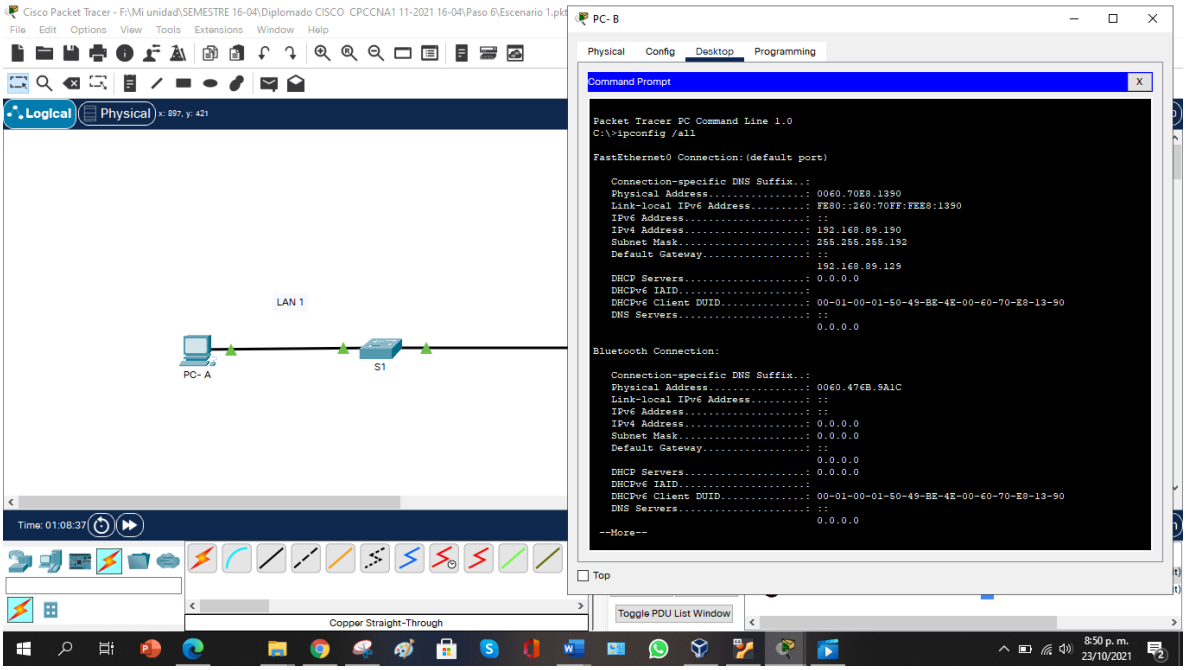
Paso 3.1: Configuración PC-B

Tabla 5 Descripción PC-B

Configuración de la red PC-B	
Descripción	PC-A este dispositivo está conectado a la LAN 2 que cuenta con 62 Host utilizables y su dirección IP es la última utilizable, conectado al S1 por medio de la interfaz g0/0/0.
Dirección física	0060.70E8.1390
Dirección IP	192.168.89.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.89.129

Fuente: Elaboración propia

Figura 33 Descripción del PC-B

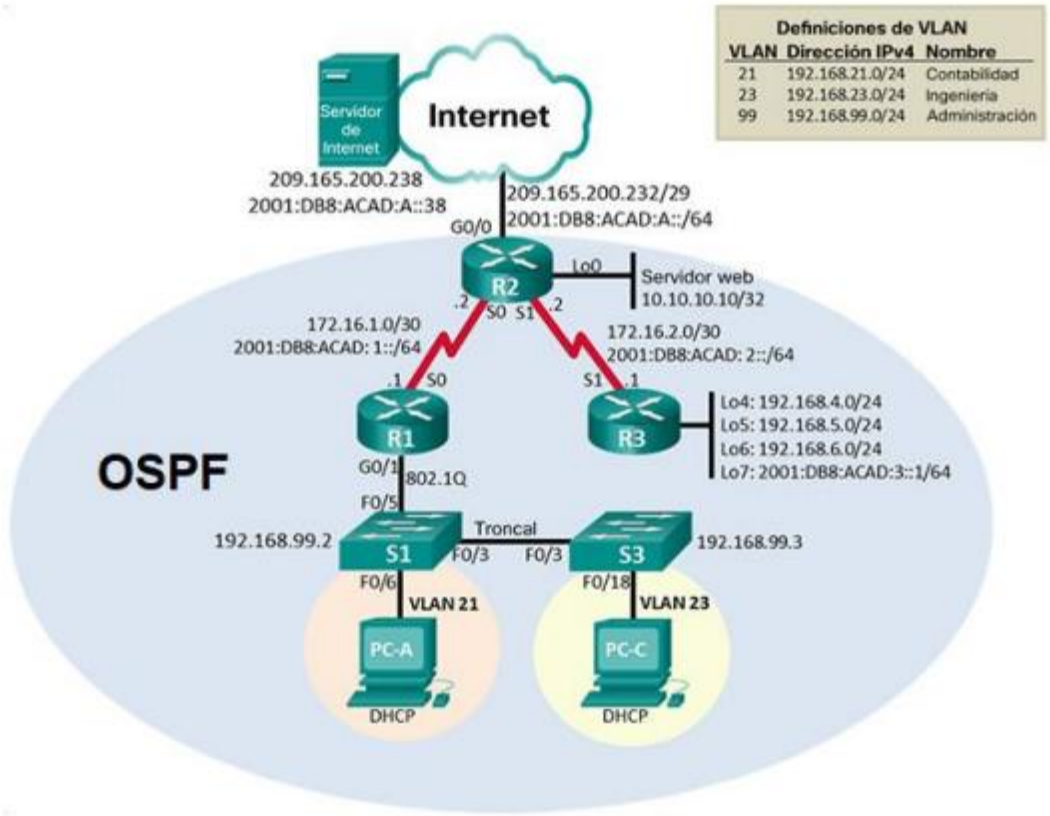


Fuente: Elaboración propia

DESARROLLO 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 RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Figura 34 Topología escenario 2



Fuente: Elaboración propia

PARTE 1: INICIALIZAR DISPOSITIVOS

Paso 1: inicializar y volver a cargar los routers y los switchs

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

Tabla 6 – inicialización dispositivos

Tarea	Comandos de IOS
Eliminar el archivo startup-config de todos los routers	erase startup-config
Volver a cargar todos los routers	reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete flash: 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>enable Switch#show flash

Fuente: Elaboración propia

Eliminar el archivo startup-config de todos los routers

R1:
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#

R2:
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#

R3:

Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#

Volver a cargar todos los routers

Nota: Se cargan todos los Routers de la topología

Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2901/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC disabled
Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340
IOS Image Load Test

_____
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x3bcd3d8
Self decompressing the image:
##
############### [OK]
Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
HWIC Slot 0 0x00200000 Onboard devices &
buffer pools 0x0228F000

TOTAL: 0x02A8F000
Rounded IOMEM up to: 44Mb.
Using 6 percent iomem. [44Mb/512Mb]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M5, RELEASE SOFTWARE (fc2)Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product, you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco CISCO2901/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: n

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

Nota. Se eliminan el archivo startup-config de los dos Switches

```
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete flash: vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)
```

Volver a cargar ambos switches: S1 y S3

```
Switch#
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0002.16BD.EE92
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs [0]: 0 orphaned files, 0 orphaned directories
flashfs [0]: Total bytes: 64016384
flashfs [0]: Bytes used: 4670455
flashfs [0]: Bytes available: 59345929
flashfs [0]: flashfs fsck took 1 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"...
################################################################################ [OK]
Smart Init is enabled
smart init is sizing iomem
                TYPE      MEMORY_REQ
```

TOTAL: 0x00000000
Rounded IOMEM up to: 0Mb.
Using 6 percent iomem. [0Mb/512Mb]
Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen
Initializing flashfs...
fsck: Disable shadow buffering due to heap fragmentation.
Flashfs [2]: 2 files, 1 directories
Flashfs [2]: 0 orphaned files, 0 orphaned directories
Flashfs [2]: Total bytes: 32514048
Flashfs [2]: Bytes used: 11952128
Flashfs 2]: Bytes available: 20561920
flashfs[2]: flashfs fsck took 2 seconds.
flashfs[2]: Initialization complete.... done Initializing flashfs.
Checking for Bootloader upgrade..
Boot Loader upgrade not required (Stage 2)
POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed
POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed
POST: CPU MIC interface Loopback Tests : Begin
POST: CPU MIC interface Loopback Tests : End, Status Passed
POST: PortASIC RingLoopback Tests : Begin
POST: PortASIC RingLoopback Tests : End, Status Passed
POST: PortASIC CAM Subsystem Tests : Begin
POST: PortASIC CAM Subsystem Tests : End, Status Passed
POST: PortASIC Port Loopback Tests : Begin
POST: PortASIC Port Loopback Tests : End, Status Passed
Waiting for Port download...Complete
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found
at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 65536K
bytes of memory.
Processor board ID FOC1010X104
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:17:59:A7:51:80
Motherboard assembly number : 73-10390-03
Power supply part number : 341-0097-02
Motherboard serial number : FOC10093R12
Power supply serial number : AZS1007032H
Model revision number : B0
Motherboard revision number : B0
Model number : WS-C2960-24TT-L
System serial number : FOC1010X104
Top Assembly Part Number : 800-27221-02
Top Assembly Revision Number : A0
Version ID : V02
CLEI Code Number : COM3L00BRA
Hardware Board Revision Number : 0x01

Switch	Ports	Model	SW Version	SW Image
* 1	26	WS-C2960-24TT-L	15.0(2)SE4	C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version
15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

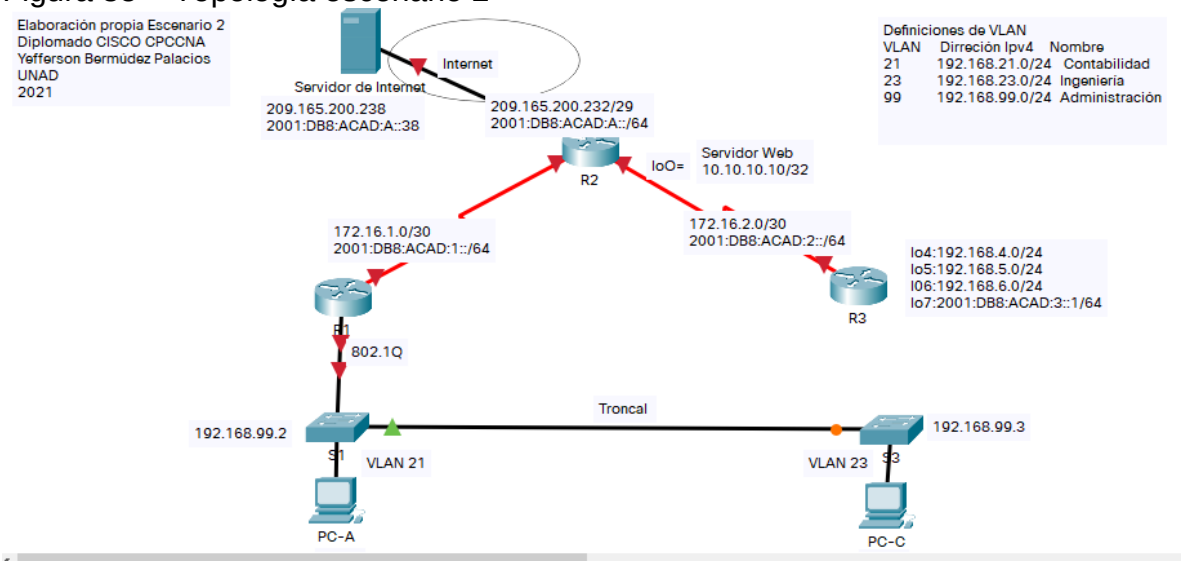
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos Switches

S1 y S3
Switch>enable
Switch#show flash
Directory of flash:/

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

64016384 bytes total (59345929 bytes free)

Figura 35 – Topología escenario 2



Fuente: Elaboración propia

PARTE 2: CONFIGURAR LOS PÁRÁMETROS BÁSICOS DE LOS DISPOSITIVOS

Paso 1: configurar la computadora de internet

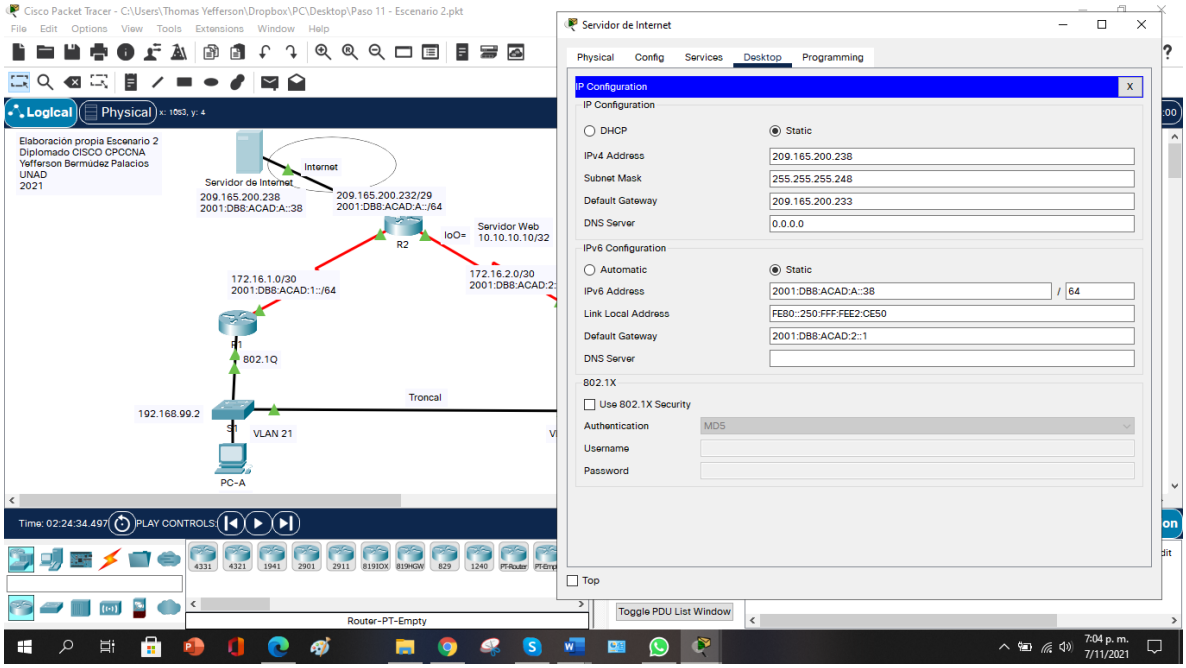
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 7- Configurar 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::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: Elaboración propia

Figura 36 – Servidor de Internet



Fuente: Elaboración propia

Paso 2: configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Desactivar la búsqueda DNS

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup

Nombre del router

- R1
  Router(config)#hostname R1

Contraseña de exec privilegiado cifrada

- class
  R1(config)#enable secret class

Contraseña de acceso a la consola y Contraseña de acceso Telnet

- cisco
  R1(config)#line console 0
  R1(config-line)#password cisco
  R1(config-line)#login
  R1(config-line)#line vty 0 15
  R1(config-line)#password cisco
  R1(config-line)#login
  R1(config-line)#

Cifrar las contraseñas de texto no cifrado

R1(config-line)#service password-encryption

Mensaje MOTD

- Se prohíbe el acceso no autorizado
  R1(config)#banner motd $SE PROHIBE EL ACCESO NO AUTORIZADO$

Interfaz S0/0/0

- Establezca la descripción
- Establecer la dirección IPv4 Consultar el diagrama de
- topología para conocer la información de direcciones
- Establecer la dirección IPv6 Consultar el diagrama de
- topología para conocer la información de direcciones
- Establecer la frecuencia de reloj en 128000
- Activar la interfaz
  R1(config)#int s0/0/0

R1(config-if)#description connection to R2
R1(config-if)#ip add 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 add 2001:DB8:ACAD:1::1/64
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit

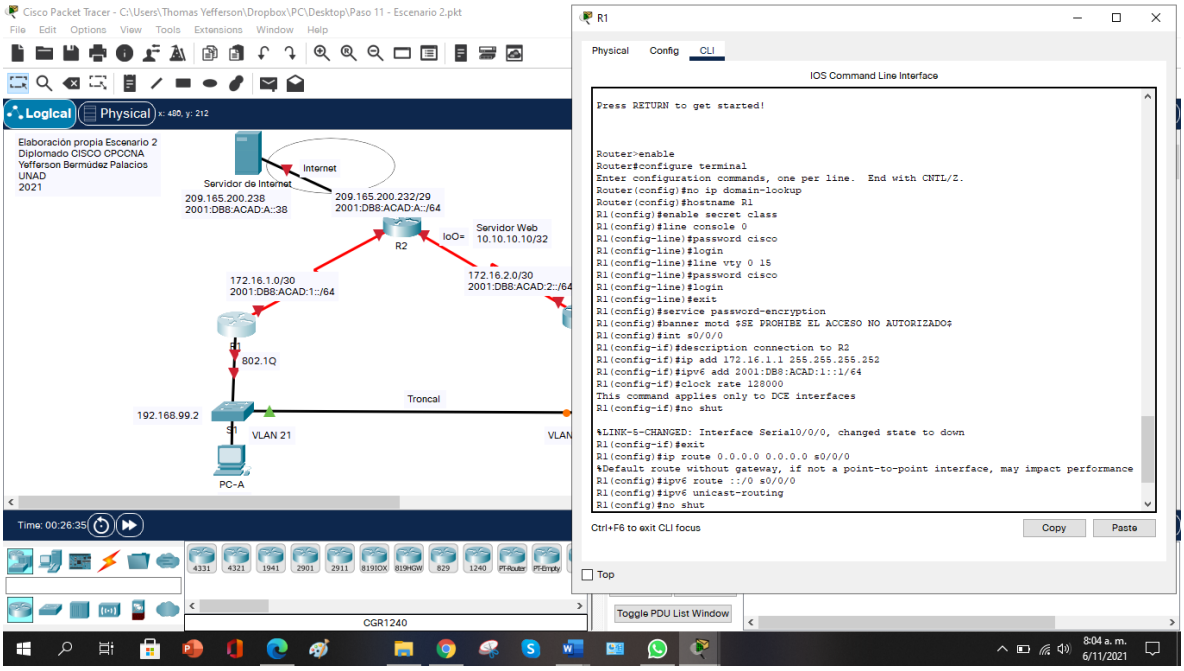
Rutas predeterminadas

- Configurar una ruta IPv4 predeterminada de S0/0/0
- Configurar una ruta IPv6 predeterminada de S0/0/0

R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#ipv6 route ::/0 s0/0/0
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

Nota: Todavía no configure G0/1.

Figura 37 – Configuración de R1



Fuente: Elaboración propia

Paso 3: configurar R2

Desactivar la búsqueda DNS

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup

Nombre del router

- R2
  Router(config)#hostname R2

Contraseña de exec privilegiado cifrada

- Class
  R2(config)#enable secret class

Contraseña de acceso a la consola y Contraseña de acceso Telnet

- Cisco
  R2(config)#enable secret class
  R2(config)#line console 0
  R2(config-line)#password cisco
  R2(config-line)#login
  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

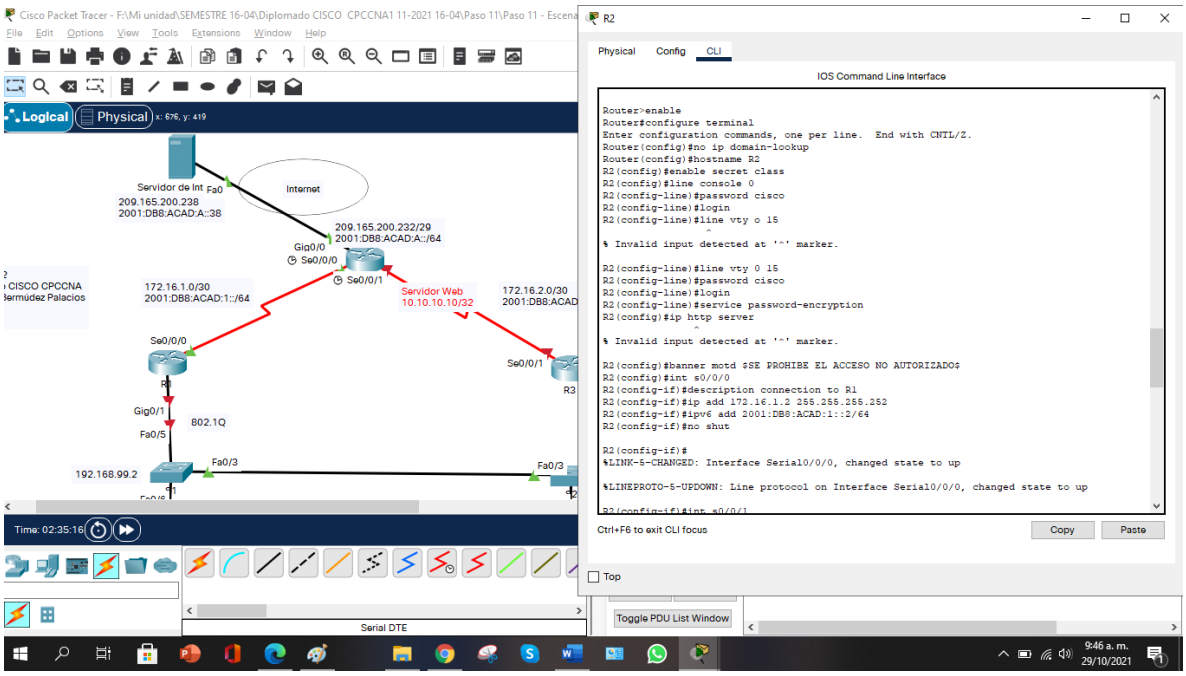
Nota: Este comando (ip http server) no es compatible con Packet Tracer.
Mensaje MOTD

Se prohíbe el acceso no autorizado.
R2(config)#banner motd $SE PROHIBE EL ACCESO NO AUTORIZADO$

Interfaz S0/0/0

- Establezca la descripción
- Establezca la dirección IPv4. Utilizar la siguiente
- dirección disponible en la subred.
- Establezca la dirección IPv6. Consulte el diagrama de
- topología para conocer la información de direcciones.
- Activar la interfaz
  R2(config)#int s0/0/0
  R2(config-if)#description connection to R1
  R2(config-if)#ip add 172.16.1.2 255.255.255.252
  R2(config-if)#ipv6 add 2001:DB8:ACAD:1::2/64
  R2(config-if)#no shut
  R2(config-if)#%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Figura 38 – Configuración R2 Interfaz s0/0/0



Fuente: Elaboración propia

Interfaz S0/0/1

- Establecer la descripción
- Establezca la dirección IPv4. Utilizar la primera
- dirección disponible en la subred.
- Establezca la dirección IPv6. Consulte el diagrama de
- topología para conocer la información de direcciones.
- Establecer la frecuencia de reloj en 128000.
- Activar la interfaz
  R2(config-if)#int s0/0/1
  R2(config-if) #description connection to R3
  R2(config-if) #ip add 172.16.2.2 255.255.255.252
  R2(config-if) #ipv6 add 2001:DB8:ACAD:2::2/64
  R2(config-if) #clock rate 128000
  R2(config-if) #no shut
  %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

Interfaz G0/0 (simulación de Internet)

- Establecer la descripción.
- Establezca la dirección IPv4. Utilizar la primera
- dirección disponible en la subred.
- Establezca la dirección IPv6. Utilizar la primera
- dirección disponible en la subred.
- Activar la interfaz
  R2(config-if) #description connection to Internet
  R2(config-if) #ip add 209.165.200.233 255.255.255.248
  R2(config-if) #ipv6 add 2001:DB8:ACAD:A::1/64
  R2(config-if) #no shut
  R2(config-if) #%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Interfaz loopback 0 (servidor web simulado)

- Establecer la descripción.
- Establezca la dirección IPv4
  R2(config-if)#int loopback 0
  R2(config-if)#

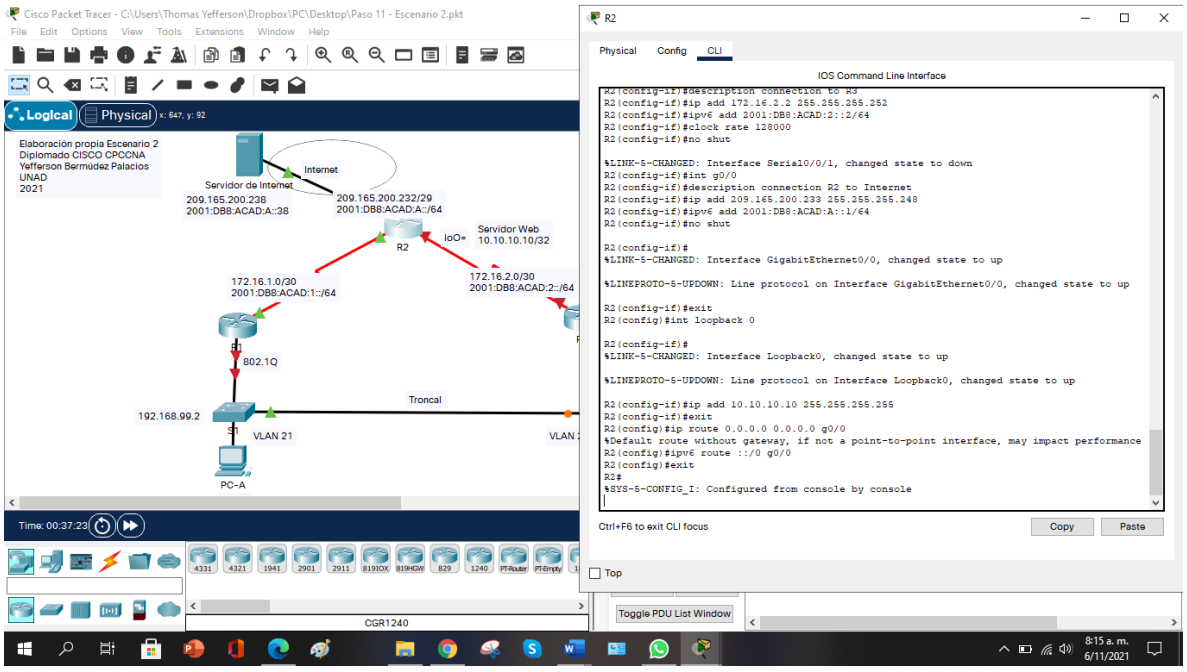
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#ip add 10.10.10.10 255.255.255.255
R2(config-if)#exit

Ruta predeterminada

- Configure una ruta IPv4 predeterminada de G0/0.
- Configure una ruta IPv6 predeterminada de G0/0.

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 g0/0
R2(config)#exit
R2#%SYS-5-CONFIG_I: Configured from console by console
Exit

Figura 39 – Configuración total R2



Fuente: Elaboración propia

Paso 4: configurar R3

La configuración del R3 incluye las siguientes tareas:

Desactivar la búsqueda DNS
R3#enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#no ip domain-lookup

Nombre del router

- R3
  Router(config)#hostname R3

Contraseña de exec privilegiado cifrada

- Class
  R3(config)#enable secret class

Contraseña de acceso a la consola y Contraseña de acceso Telnet

- Cisco
  R3(config)#line console 0
  R3(config-line) #password cisco
  R3(config-line) #login
  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

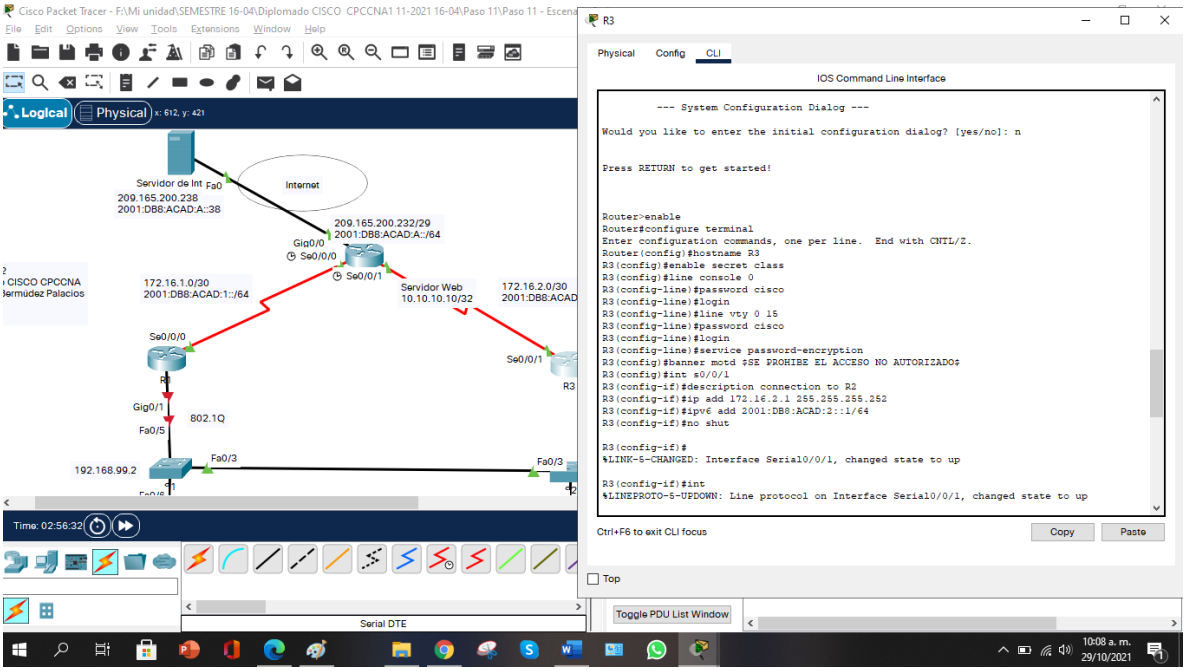
Mensaje MOTD
Se prohíbe el acceso no autorizado.
R3(config)#banner motd $SE PROHIBE EL ACCESO NO AUTORIZADO$

Interfaz S0/0/1

- Establecer la descripción
- Establezca la dirección IPv4. Utilizar la siguiente dirección
- disponible en la subred.
- Establezca la dirección IPv6. Consulte el diagrama de
- topología para conocer la información de direcciones.
- Activar la interfaz
  R3(config)#int s0/0/1

R3(config-if)#description connection to R2
R3(config-if)#ip add 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 add 2001:DB8:ACAD:2::1/64
R3(config-if)#no shut
R3(config-if)#%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
R3(config-if)#int
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

Figura 40- Configuración R3



Fuente: Elaboración propia

Interfaz loopback 4

- Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
  R3(config-if) #int loopback 4
  R3(config-if) #
  %LINK-5-CHANGED: Interface Loopback4, changed state to up
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
  R3(config-if) #ip add 192.168.4.1 255.255.255.0

Interfaz loopback 5

- Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
  R3(config-if) #int loopback 5
  R3(config-if) #
  %LINK-5-CHANGED: Interface Loopback5, changed state to up
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
  R3(config-if)#ip add 192.168.5.1 255.255.255.0

Interfaz loopback 6

- Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
  R3(config-if)#int loopback 6
  R3(config-if)#
  %LINK-5-CHANGED: Interface Loopback6, changed state to up
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
  R3(config-if)#ip add 192.168.6.1 255.255.255.0

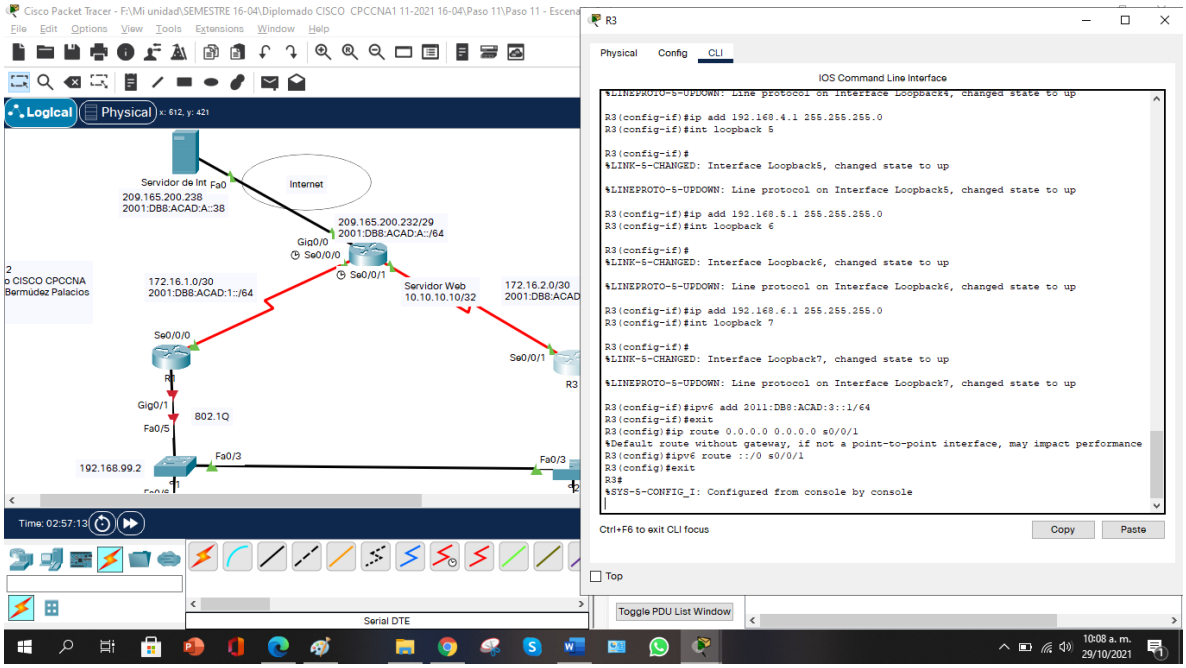
Interfaz loopback 7

- Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
  R3(config)#int loopback 7
  R3(config-if)#
  %LINK-5-CHANGED: Interface Loopback7, changed state to up
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
  R3(config-if)#ipv6 add 2011:DB8:ACAD:3::1/64
  R3(config-if)#exit
  R3(config)#ipv6 unicast-routing
  R3(config)#

Rutas predeterminadas

R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

Figura 41 rutas predeterminadas del R3



Fuente: Elaboración propia

Paso 5: configurar S1

La configuración del S1 incluye las siguientes tareas:

Desactivar la búsqueda DNS
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup

Nombre del switch

- S1
  Switch(config)#hostname S1

Contraseña de exec privilegiado cifrada

- class
  S1(config)#enable secret class

Contraseña de acceso a la consola y Contraseña de acceso Telnet cisco

- cisco

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
```

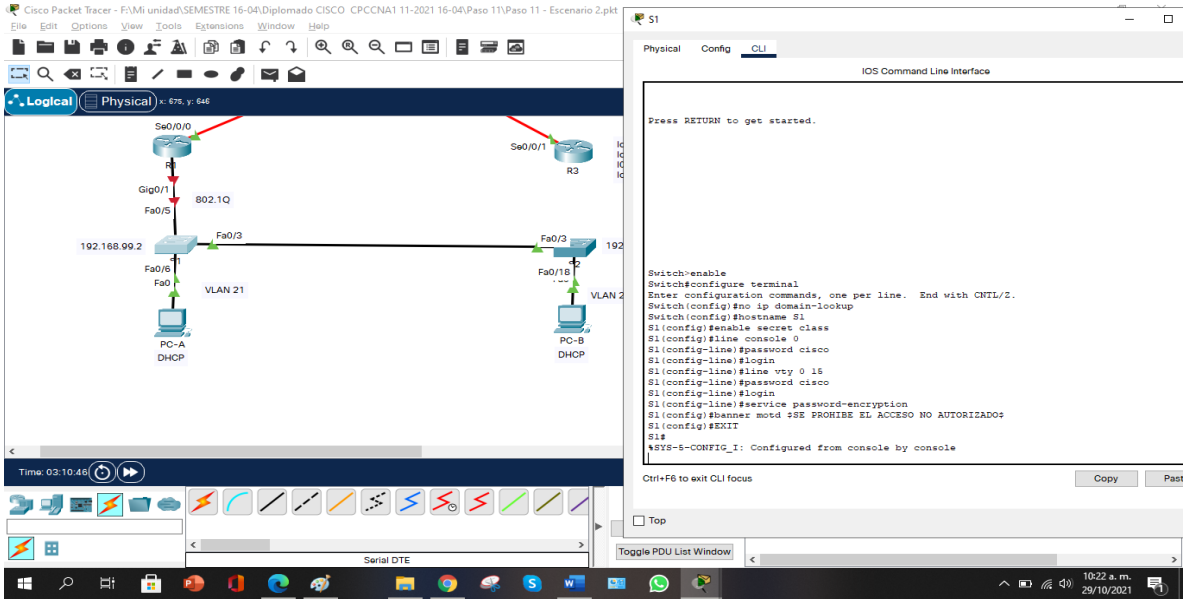
Cifrar las contraseñas de texto no cifrado

S1(config-line)#service password-encryption

Mensaje MOTD

- Se prohíbe el acceso no autorizado.
  S1(config)#banner motd $SE PROHIBE EL ACCESO NO AUTORIZADO$

Figura 42 – Configuración S1



Fuente: Elaboración propia

Paso 6: configurar S3
La configuración del S3 incluye las siguientes tareas:

Desactivar la búsqueda DNS
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup

Nombre del switch

- S3
  Switch(config)#hostname S3

Contraseña de exec privilegiado cifrada

- class
  S3(config)#enable secret class

Contraseña de acceso a la consola y Contraseña de acceso Telnet

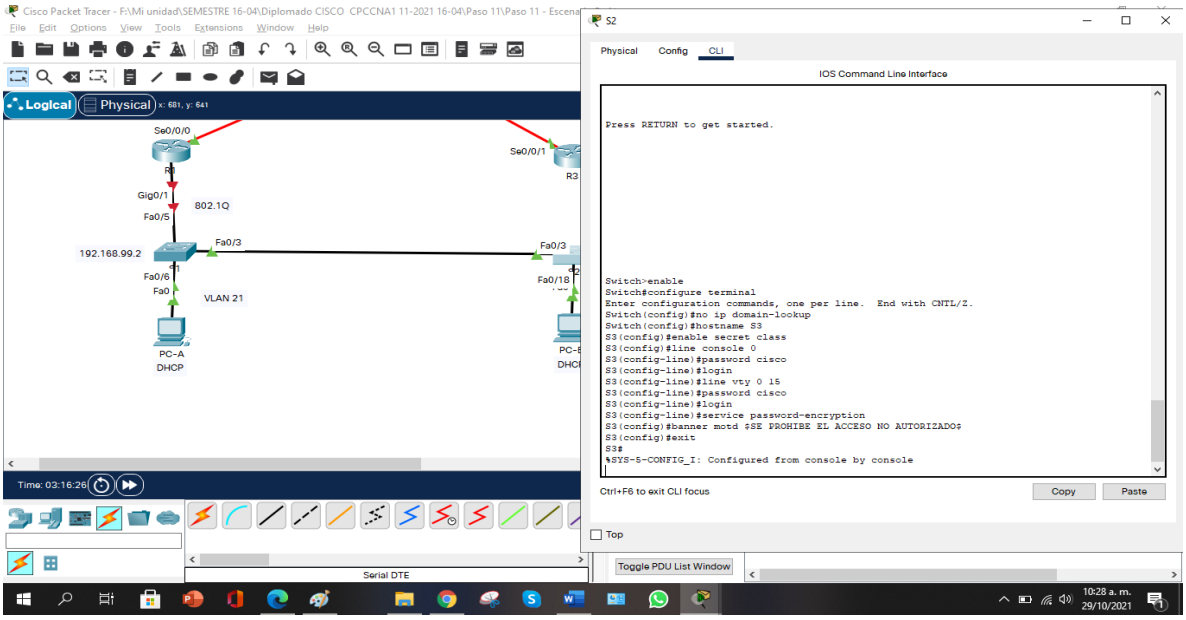
- cisco
  S3(config)#line console 0
  S3(config-line)#password cisco
  S3(config-line)#login
  S3(config-line)#line vty 0 15
  S3(config-line)#password cisco
  S3(config-line)#login

Cifrar las contraseñas de texto no cifrado
S3(config-line)#service password-encryption

Mensaje MOTD

- Se prohíbe el acceso no autorizado
  S3(config)#banner motd $SE PROHIBE EL ACCESO NO AUTORIZADO$

Figura 43 – Configuración S3



Fuente: Elaboración propia

Paso 7: verificar la conectividad de la red

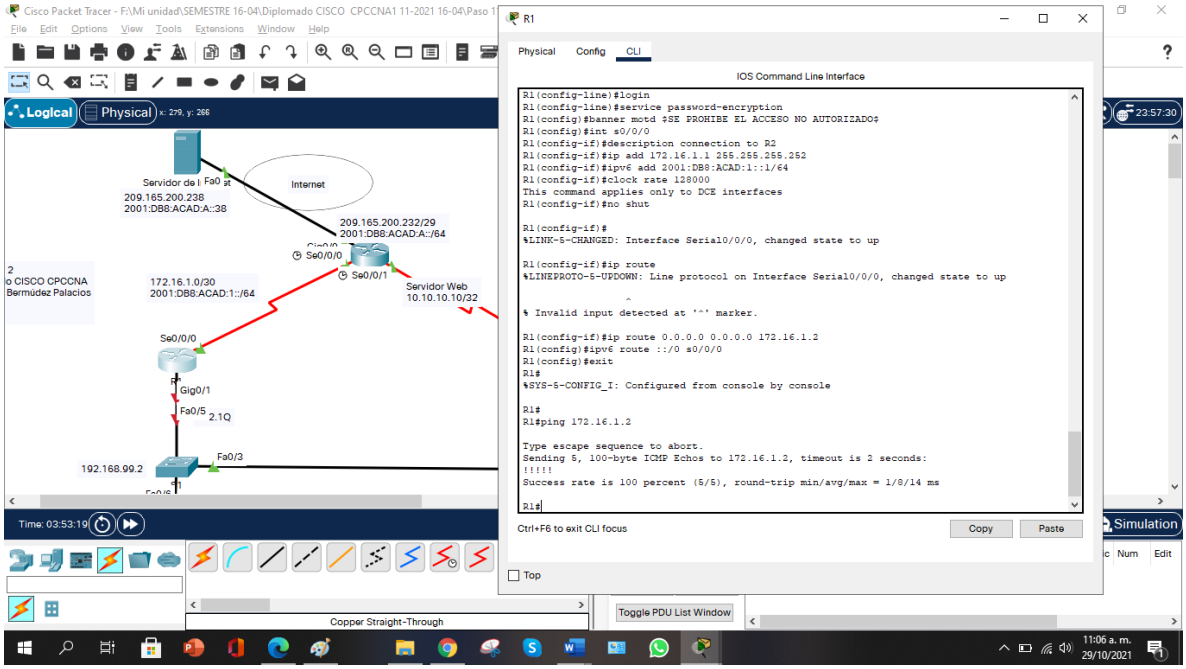
Utilice el comando ping para probar la conectividad entre los dispositivos de red.
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 8- Verificar la conexión de la red

Desde	A	Dirección IP	Resultado de ping
R1	R2, S0/0/0	172.16.1.2	exitoso
R2	R3, S0/0/1	172.16.2.1	exitoso
PC de Internet	Gateway predeterminado	209.165.200.232	exitoso

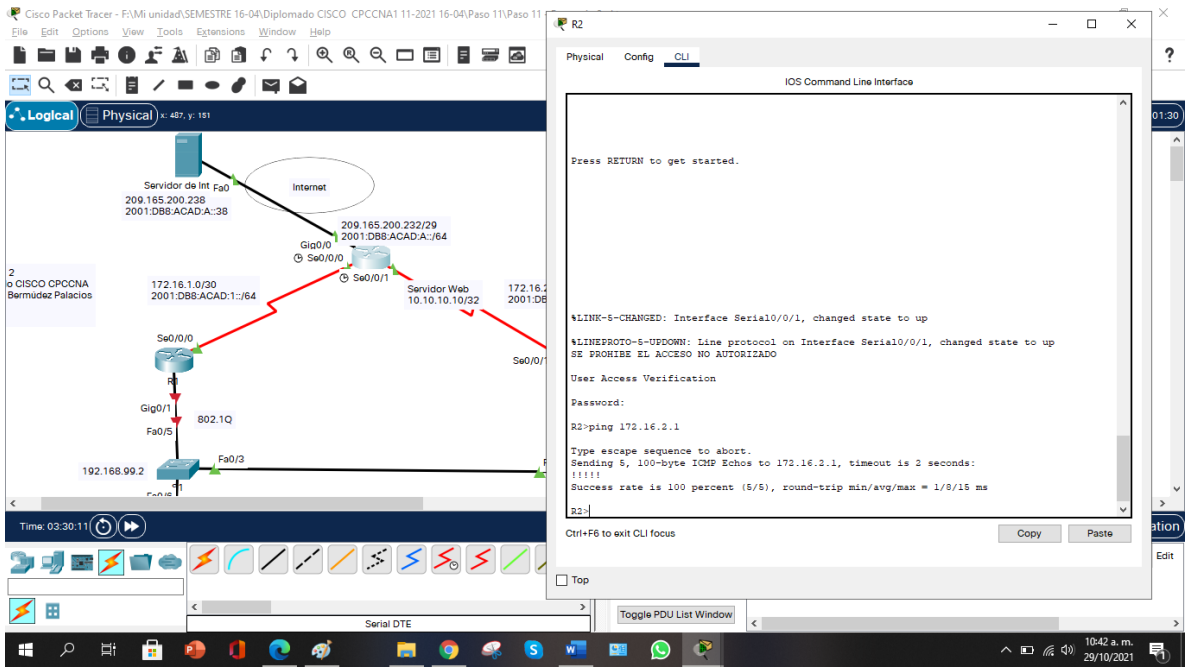
Fuente: Elaboración propia

Figura 44 – Verificación ping de R1 a R2 s0/0/0



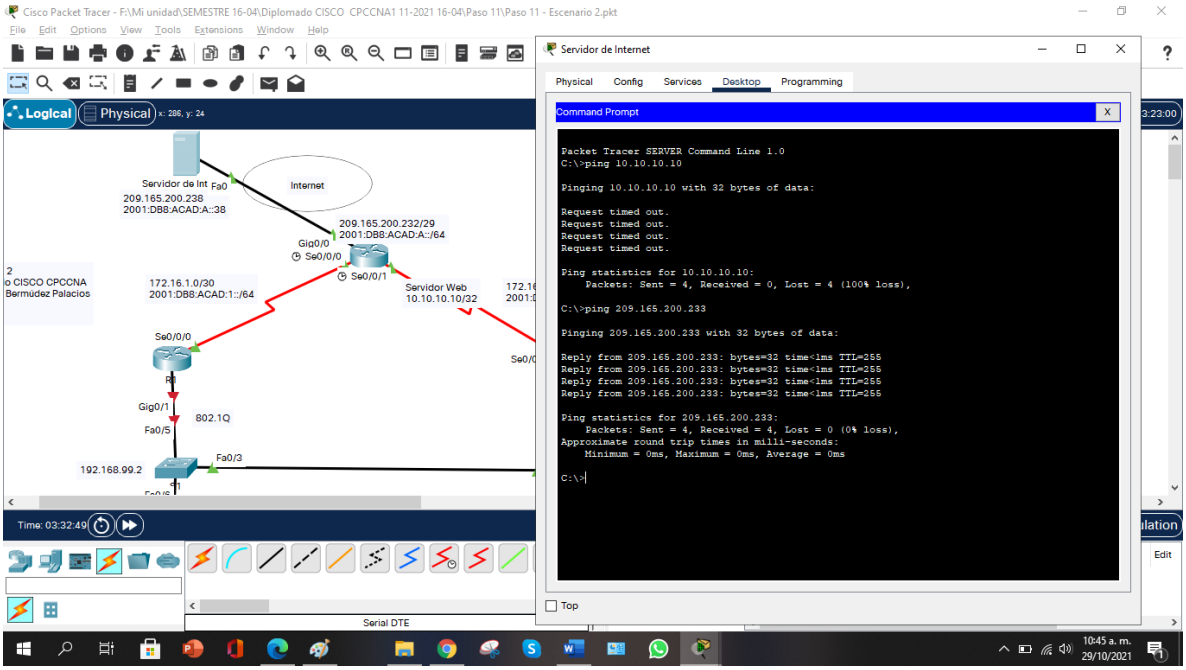
Fuente: Elaboración propia

Figura 45 – Verificación ping de R2 a R3 s0/0/1



Fuente: Elaboración propia

Figura 46 – Verificación de PC de internet a Gateway predeterminado



Fuente: Elaboración propia

PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas

Crear la base de datos de VLAN

- Utilizar la tabla de equivalencias de VLAN para topología
- para crear y nombrar cada una de las VLAN que se indican

```
S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administración
S1(config-vlan)#exit
```

Asignar la dirección IP de administración.

- Asigne la dirección IPv4 a la VLAN de administración.
- Utilizar la dirección IP asignada al S1 en el diagrama de topología
  S1(config)#int vlan 99
- S1(config-if)#
- %LINK-5-CHANGED: Interface Vlan99, changed state to up
- S1(config-if) #ip add 192.168.99.2 255.255.255.0
- S1(config-if)#no shut

Asignar el gateway predeterminado

- Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
  S1(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3

- **Utilizar la red VLAN 1 como VLAN nativa**
  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

- Utilizar la red VLAN 1 como VLAN nativa
  S1(config-if) #int f0/5
  S1(config-if) #switchport mode trunk
  S1(config-if) #switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso

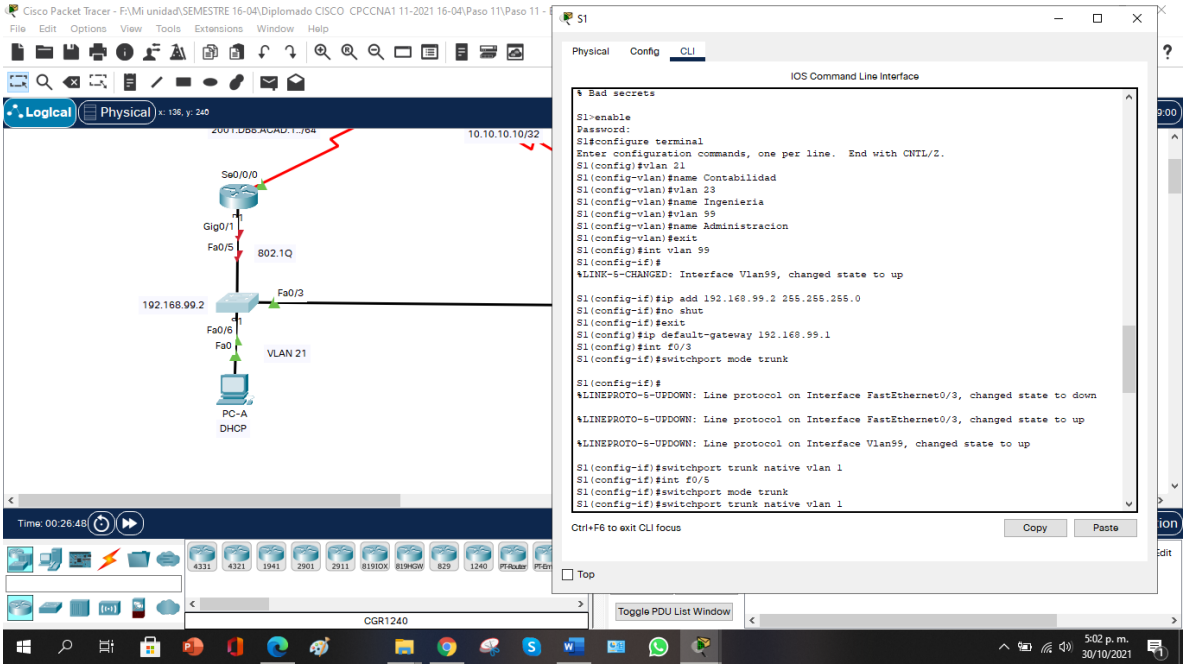
- Utilizar el comando interface range
  S1(config-if) #int range f0/1-2, f0/4, f0/6-24
  S1(config-if-range) #switchport mode access

Asignar F0/6 a la VLAN 21

S1(config-if-range) #int f0/6
S1(config-if) #switchport access vlan 21

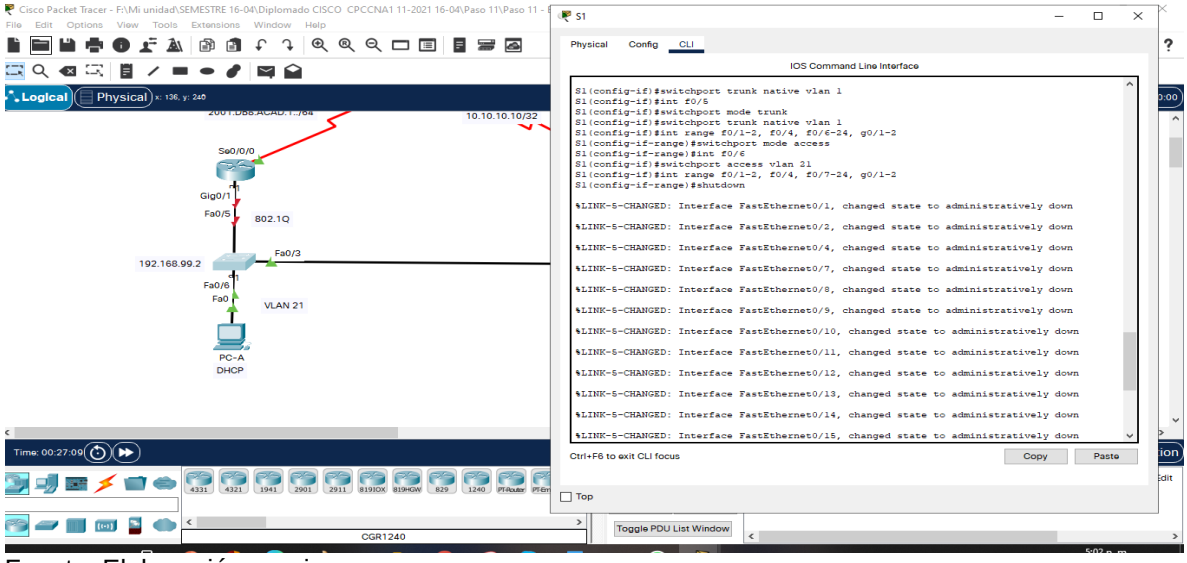
Apagar todos los puertos sin usar
S1(config-if) #int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range) #shutdown

Figura 47 – Configuración S1 con VLAN, asignación IP de administración



Fuente: Elaboración propia

Figura 48 – Configuración S1 con troncal de interfaz



Fuente: Elaboración propia

Paso 2: Configurar S3
La configuración del S3 incluye las siguientes tareas:

Crear la base de datos de VLAN

- Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
  S3>enable
  Password:
  Password:
  Password:
  S3#configure terminal
  Enter configuration commands, one per line. End with CNTL/Z.
  S3(config)#vlan 21
  S3(config-vlan) #name Contabilidad
  S3(config-vlan) #vlan 23
  S3(config-vlan) #name Ingenieria
  S3(config-vlan) #vlan 99
  S3(config-vlan) #name Administracion
  S3(config-vlan) #exit

Asignar la dirección IP de administración

- Asigne la dirección IPv4 a la VLAN de administración.
- Utilizar la dirección IP asignada al S3 en el diagrama de topología
  S3(config)#int vlan 99
  S3(config-if) #ip add 192.168.99.3 255.255.255.0
  S3(config-if) #no shut
  S3(config-if) #exit

Asignar el gateway predeterminado.

- Asignar la primera dirección IP en la subred como gateway predeterminado.
  S3(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3

- Utilizar la red VLAN 1 como VLAN nativa
  S3(config) #int f0/3
  S3(config-if) #switch mode trunk
  S3(config-if) #switch trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso

- Utilizar el comando interface range
  S3(config-if) #int range f0/1-2, f0/4-24, g0/1-2
  S3(config-if-range) #switchport mode access

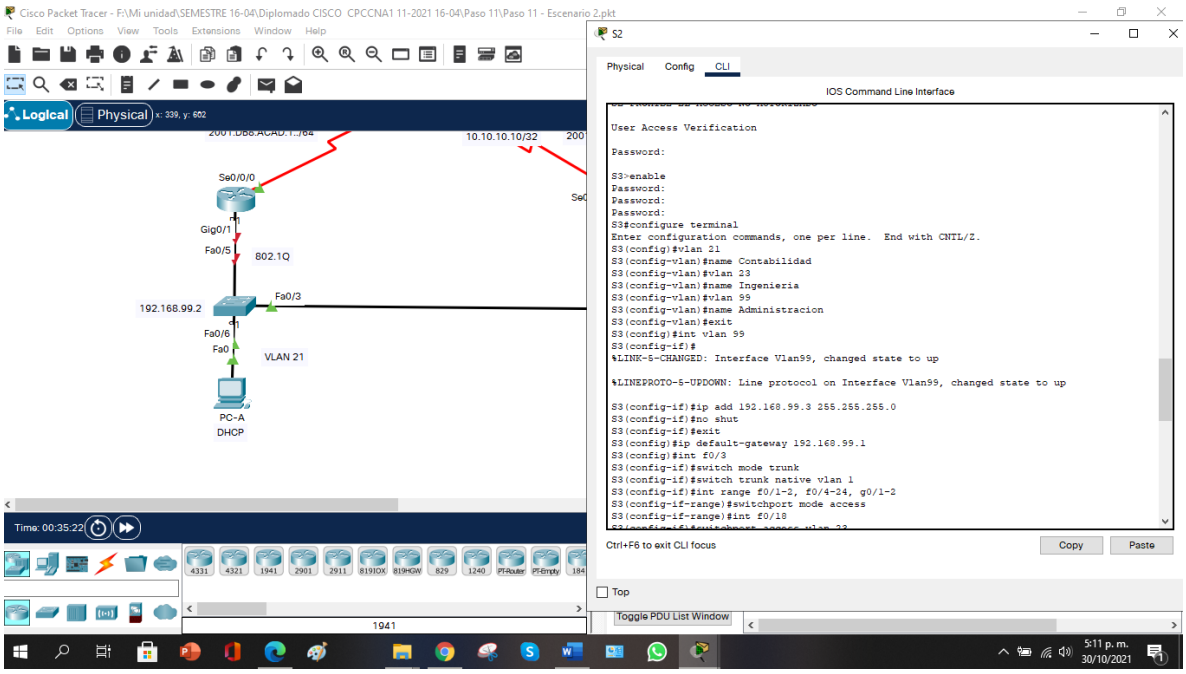
Asignar F0/18 a la VLAN 21

S3(config-if-range) #int f0/18
S3(config-if) #switchport access vlan 21

Apagar todos los puertos sin usar

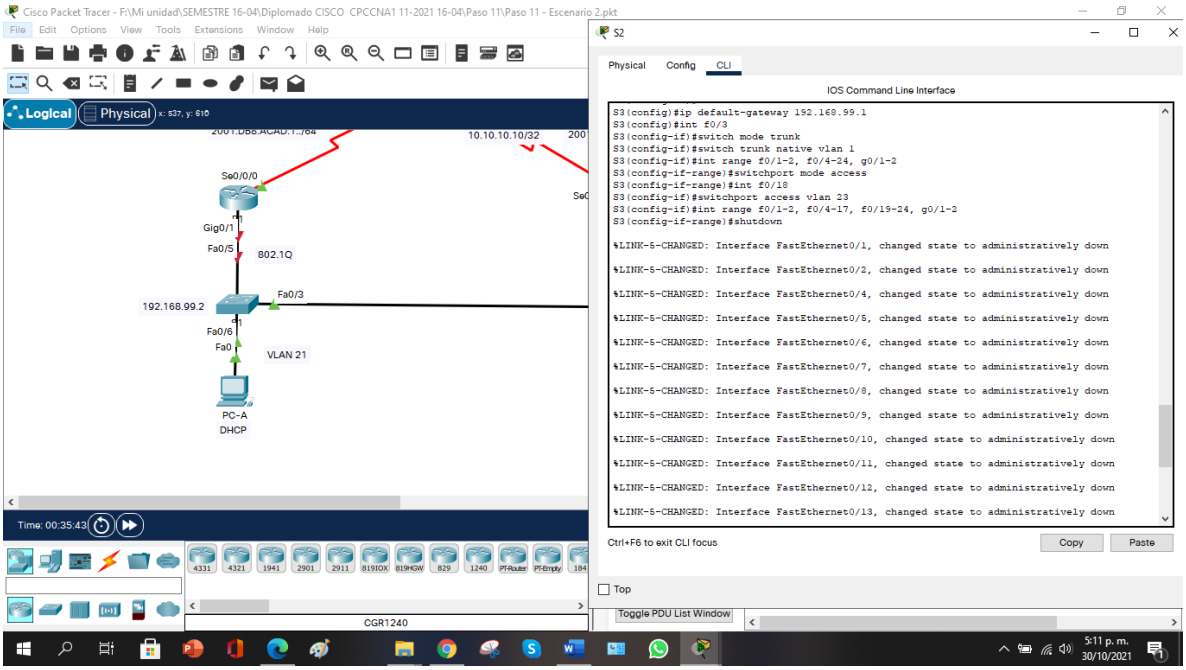
S3(config-if) #int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range) #shutdown

Figura 49 – Configuración S3 con VLAN, asignación IP de administración



Fuente: Elaboración propia

Figura 50 - Configuración S3 con troncal de interfaz



Fuente: Elaboración propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Configurar la subinterfaz 802.1Q .21 en G0/1

- Descripción: LAN de Contabilidad
- Asignar la VLAN 21
- Asignar la primera dirección disponible a esta interfaz
  R1>enable
  Password:
  R1#configure terminal
  Enter configuration commands, one per line. End with CNTL/Z.
  R1(config)#int g0/1.21
  R1(config-subif) #description LAN de Contabilidad
  R1(config-subif) #encapsulation dot1q 21
  R1(config-subif) #ip add 192.168.21.1 255.255.255.0

Configurar la subinterfaz 802.1Q .23 en G0/1

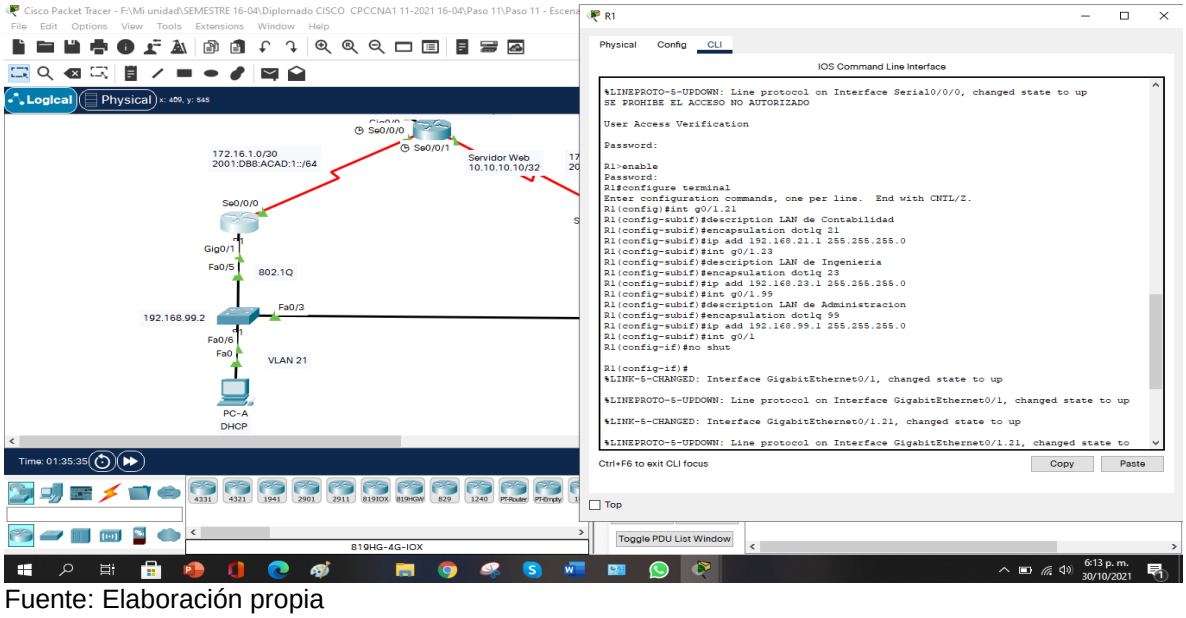
- Descripción: LAN de Ingeniería
- Asignar la VLAN 23
- Asignar la primera dirección disponible a esta interfaz
  R1(config-subif) #int g0/1.23
  R1(config-subif) #description LAN de Ingenieria
  R1(config-subif) #encapsulation dot1q 23
  R1(config-subif) #ip add 192.168.23.1 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1

- Descripción: LAN de Administración
- Asignar la VLAN 99
- Asignar la primera dirección disponible a esta interfaz
  R1(config-subif) #int g0/1.99
  R1(config-subif) #description LAN de Administracion
  R1(config-subif) #encapsulation dot1q 99
  R1(config-subif) #ip add 192.168.99.1 255.255.255.0

Activar la interfaz G0/1
R1(config-subif) #int g0/1
R1(config-if) #no shut

Figura 51- Configuración de subinterfaz (Q.21, Q.23, Q.99)



Fuente: Elaboración propia

Paso 4: Verificar la conectividad de la red

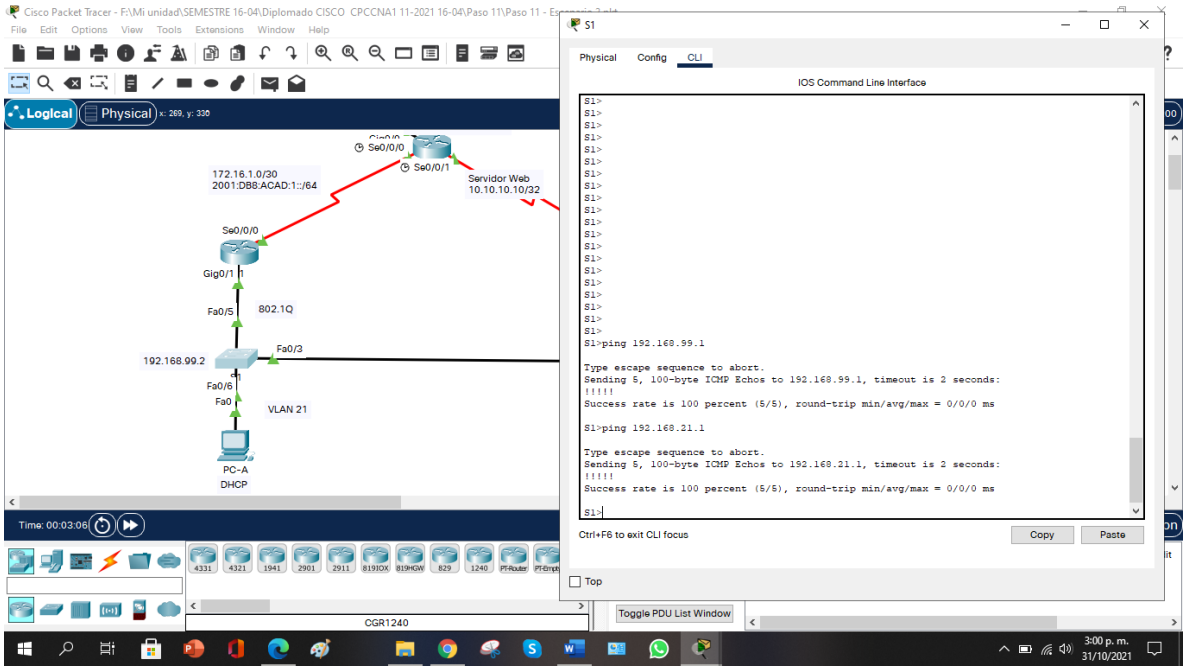
Utilice el comando ping para probar la conectividad entre los switches y el R1.
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 9- Verificar la conectividad de la red

Desde	A	Dirección IP	Resultado de ping
S1	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S3	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S1	R1, dirección VLAN 21	192.168.21.1	Satisfactorio
S3	R1, dirección VLAN 23	192.168.23.1	Satisfactorio

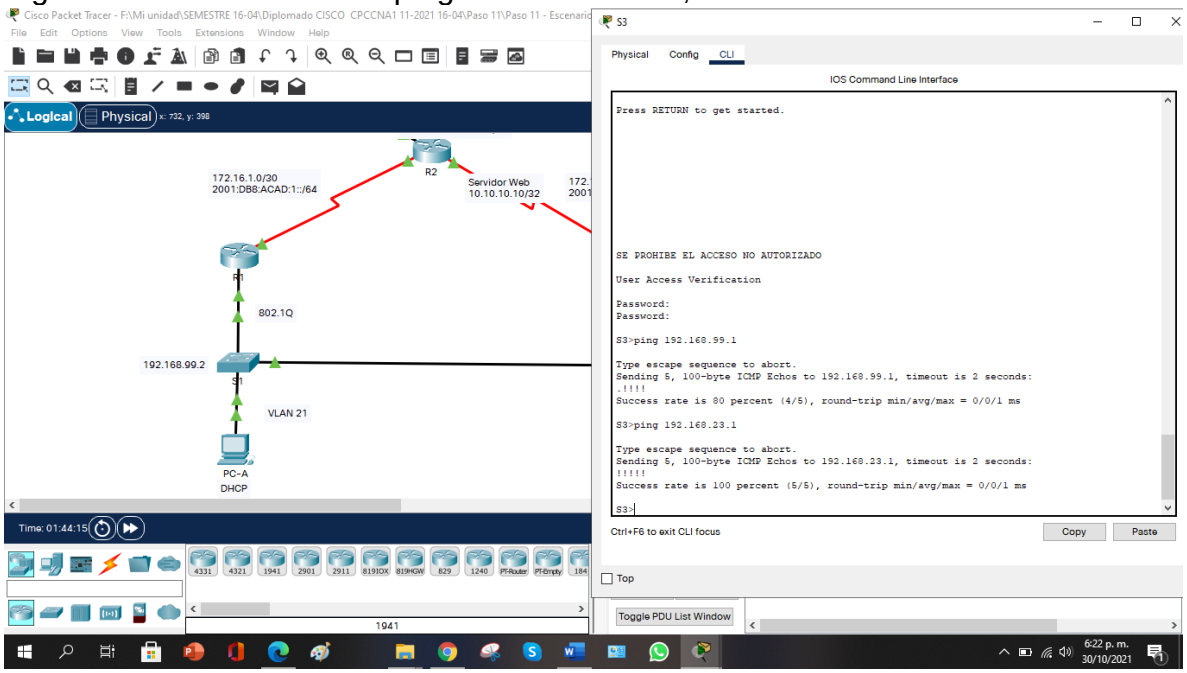
Fuente: Elaboración propia

Figura 52 – Verificación de ping entre S1 a R1 vlan99, R1 vlan 21.



Fuente: Elaboración propia

Figura 53 – Verificación de ping S3 a R1 vlan99, R1 vlan 23.



Fuente: Elaboración propia

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

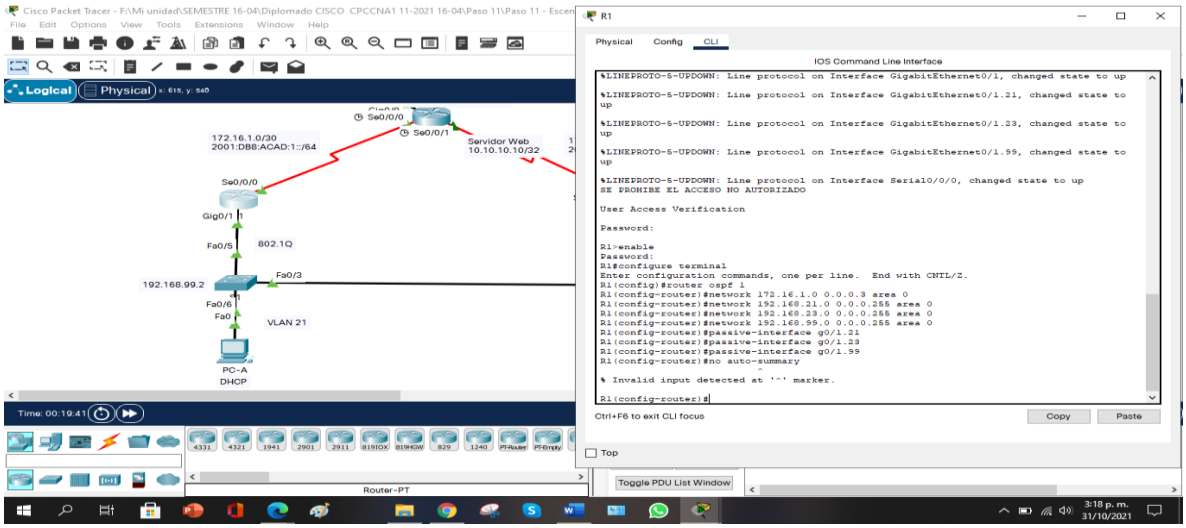
Tabla 10 - Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Fuente: Elaboración propia

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
R1(config-router) #passive-interface g0/1.21
R1(config-router) #passive-interface g0/1.23
R1(config-router) #passive-interface g0/1.99
R1(config-router) #no auto-summary

Figura 54 - Configurar OSPF en el R1



Fuente: Elaboración propia

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

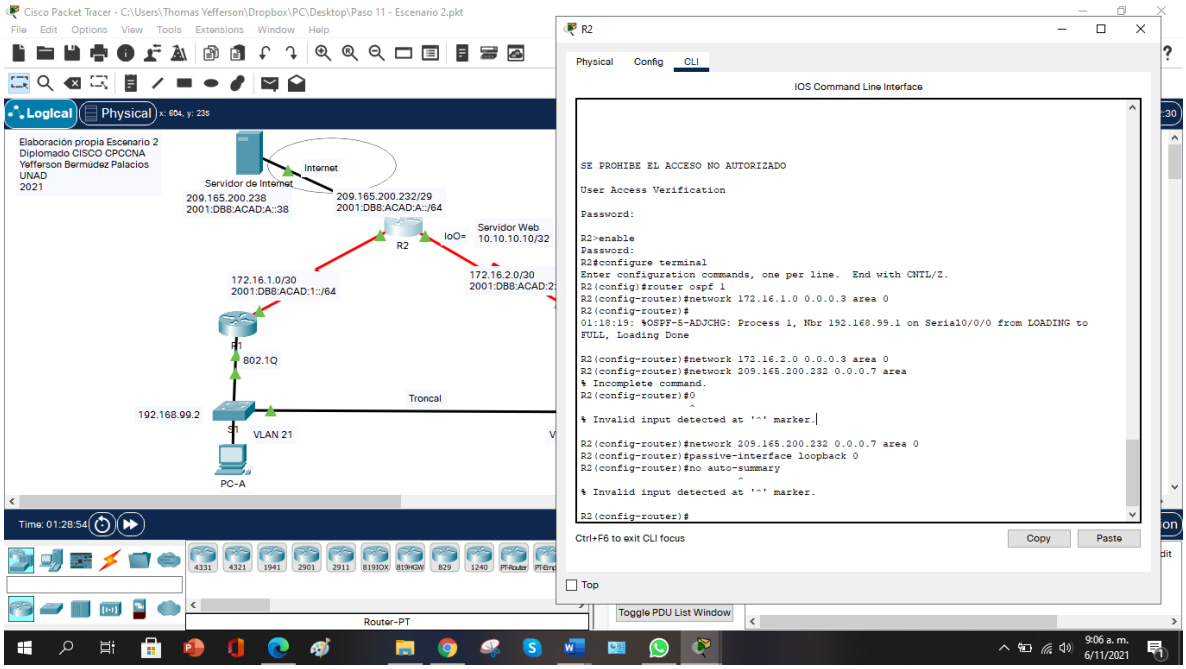
Tabla 11 - Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Fuente: Elaboración propia

```
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router) #network 172.16.1.0 0.0.0.3 area 0
R2(config-router) #network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#network 209.165.200.232 0.0.0.7 area 0
R2(config-router) #passive-interface loopback 0
R2(config-router) #no auto-summary
```

Figura 55 - Configurar OSPF en el R2



Fuente: Elaboración propia

Paso 3: Configurar OSPFv3 en R2

La configuración del R3 incluye las siguientes tareas:

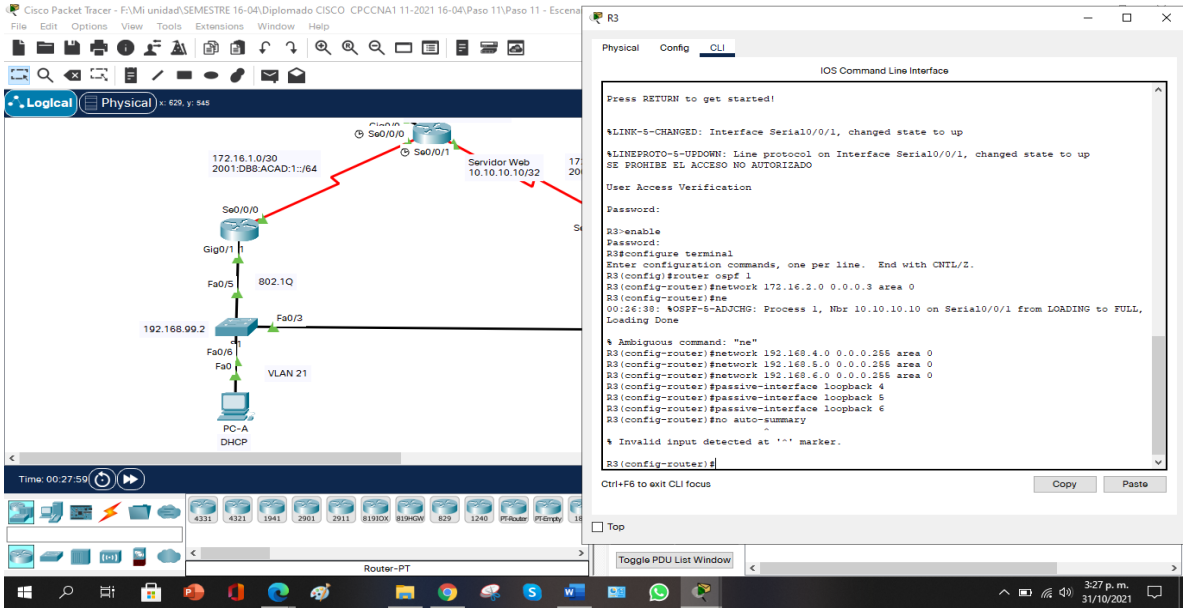
Tabla 12 - Configurar OSPFv3 en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática	

Fuente: Elaboración propia

```
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
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
R3(config-router) #passive-interface loopback 4
R3(config-router) #passive-interface loopback 5
R3(config-router) #passive-interface loopback 6
R3(config-router) #no auto-summary
```

Figura 56 - Configurar OSPFv3 en R2



Fuente: Elaboración propia

Paso 4: Verificar la información OSPF

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

Tabla 13 - Verificar la información 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 ip ospf database

Fuente: Elaboración propia

Figura 57 – R1 Verificar la información de OSPF

```
R1>show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.99.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10           110      00:02:39
    192.168.6.1           110      00:02:10
    192.168.99.1          110      00:06:26
  Distance: (default is 110)

R1>show ip route ospf
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O        172.16.2.0 [110/128] via 172.16.1.2, 00:06:33, Serial0/0/0
      192.168.4.0/32 is subnetted, 1 subnets
O        192.168.4.1 [110/129] via 172.16.1.2, 00:02:58, Serial0/0/0
      192.168.5.0/32 is subnetted, 1 subnets
O        192.168.5.1 [110/129] via 172.16.1.2, 00:02:40, Serial0/0/0
      192.168.6.0/32 is subnetted, 1 subnets
O        192.168.6.1 [110/129] via 172.16.1.2, 00:02:30, Serial0/0/0
      209.165.200.0/29 is subnetted, 1 subnets
O        209.165.200.232 [110/65] via 172.16.1.2, 00:06:04, Serial0/0/0

R1>Show ip ospf database
            OSPF Router with ID (192.168.99.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.99.1    192.168.99.1    434         0x80000005 0x00b2d3 5
10.10.10.10     10.10.10.10     207         0x80000005 0x001f4c 5
192.168.6.1     192.168.6.1     178         0x80000005 0x00c5f6 5
```

Fuente: Elaboración propia

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

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

Las tareas de configuración para R1 incluyen las siguientes:

Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas.

```
R1>enable
Password:
R1#configure terminal
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.

- Nombre: ACCT
- Servidor DNS: 10.10.10.10
- Nombre de dominio: ccna-sa.com
- Establecer el gateway predeterminado

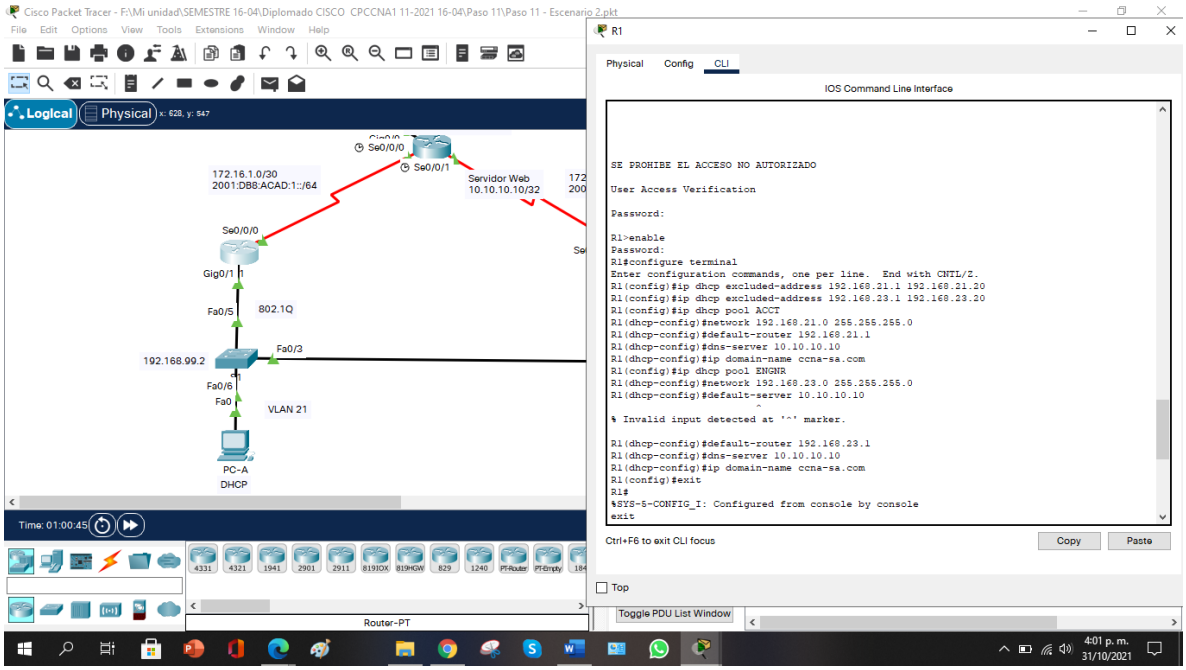
```
R1(config)#ip dhcp pool ACCT
R1(dhcp-config) #network 192.168.21.0 255.255.255.0
R1(dhcp-config) #default-router 192.168.21.1
R1(dhcp-config) #dns-server 10.10.10.10
R1(dhcp-config) #ip domain-name ccna-sa.com
```

Crear un pool de DHCP para la VLAN 23

- Nombre: ENGNR
- Servidor DNS: 10.10.10.10
- Nombre de dominio: ccna-sa.com
- Establecer el gateway predeterminado

```
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config) #network 192.168.23.0 255.255.255.0
R1(dhcp-config) #default-router 192.168.23.1
R1(dhcp-config) #dns-server 10.10.10.10
R1(dhcp-config) #ip domain-name ccna-sa.com
```

Figura 58 - Configurar R1 como servidor DHCP para las VLAN 21 y 23



Fuente: Elaboración propia

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

La configuración del R2 incluye las siguientes tareas:

Crear una base de datos local con una cuenta de usuario

- Nombre de usuario: webuser
- Contraseña: cisco12345
- Nivel de privilegio: 15
  Password:
  R2>enable
  Password:
  R2#configure terminal
  R2(config)#username webuser privilege 15 secret cisco12345

Habilitar el servicio del servidor HTTP
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación.

Nota: Al tratar de habilitar el servicio del servidor HTTP, al igual que para configurarlo para utilizar la base de datos local para la autenticación; packet tracer no admite los comandos:
ip http server, ip http authentication local, ip http secure-server

Crear una NAT estática al servidor web.

- Dirección global interna: 209.165.200.229
  R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238

Asignar la interfaz interna y externa para la NAT estática
R2(config)#int g0/0
R2(config-if)#ip nat inside

Configurar la NAT dinámica dentro de una ACL privada

- Lista de acceso: 1
- Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1
- Permitir la traducción de un resumen de las redes LAN (loopback) en el R3

R2(config-if)#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

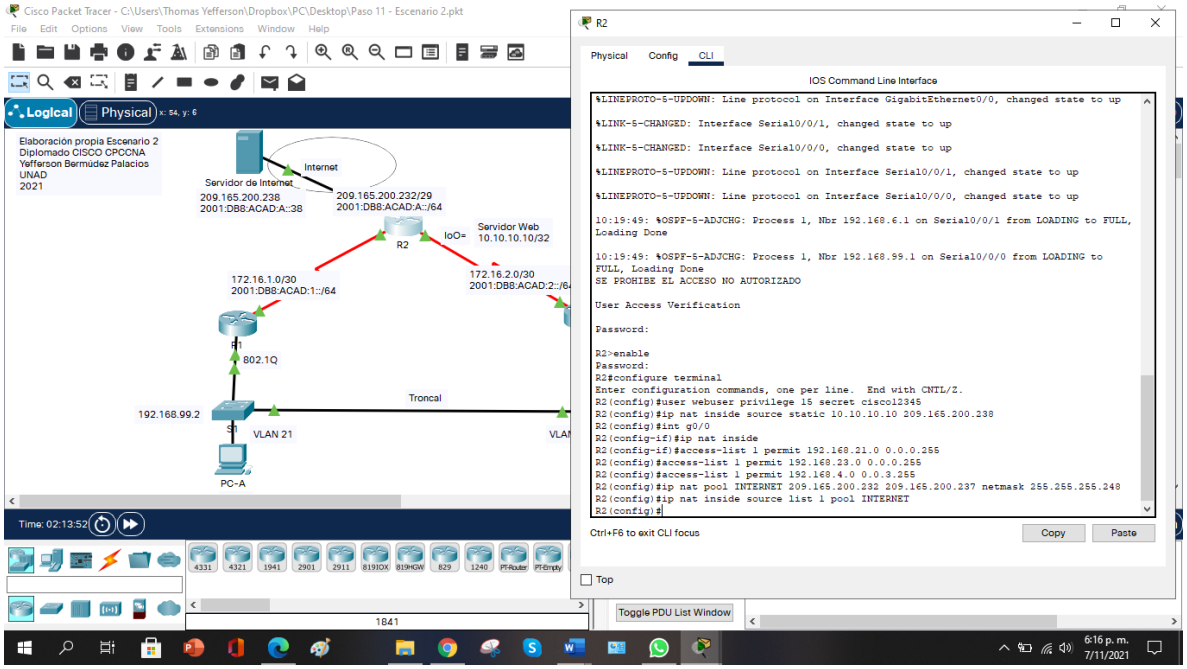
Defina el pool de direcciones IP públicas utilizables.

- Nombre del conjunto: INTERNET
- El conjunto de direcciones incluye:209.165.200.225 – 209.165.200.228

R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248

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

Figura 59 - Configurar la NAT estática y dinámica en el R2



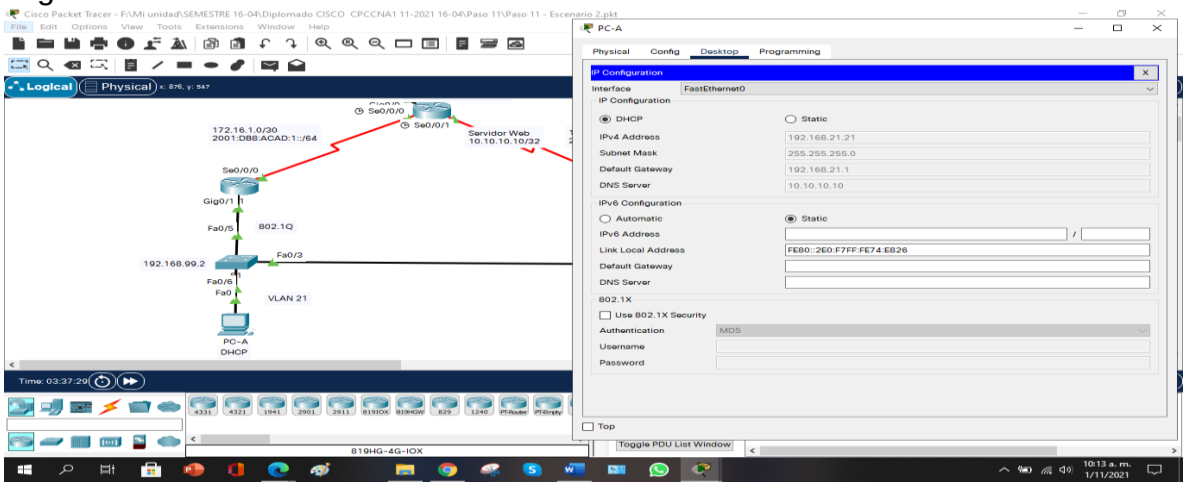
Fuente: Elaboración propia

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

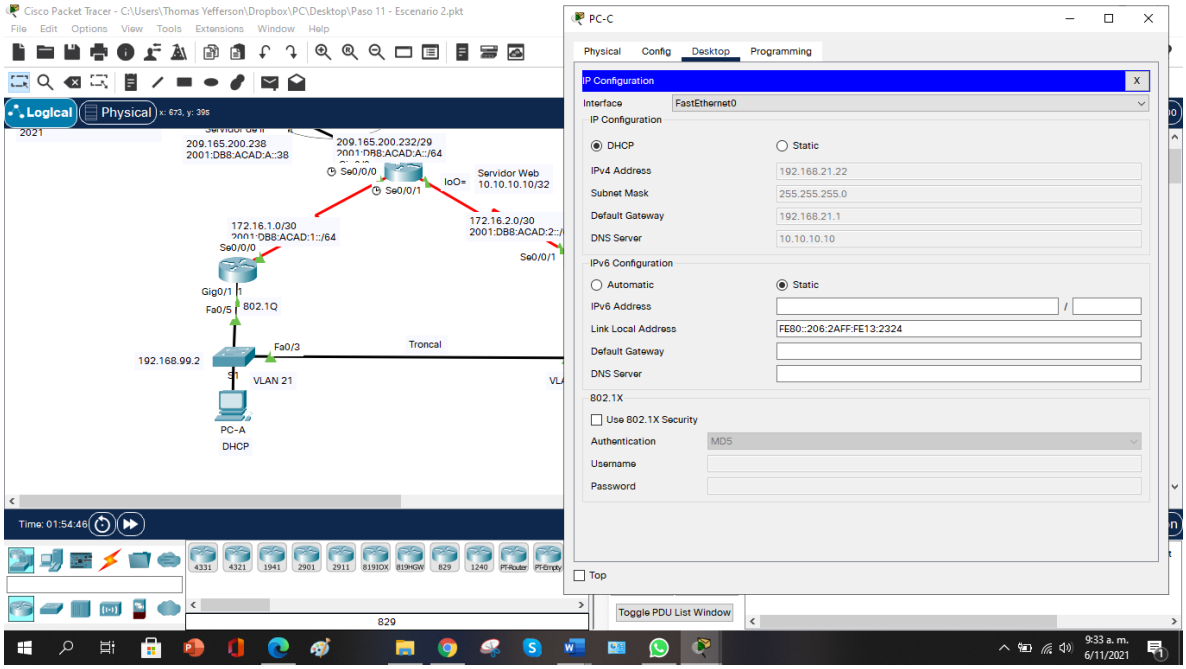
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

Figura 60 – DHCP de PC-A



Fuente: Elaboración propia

Figura 61 - DHCP de PC-C

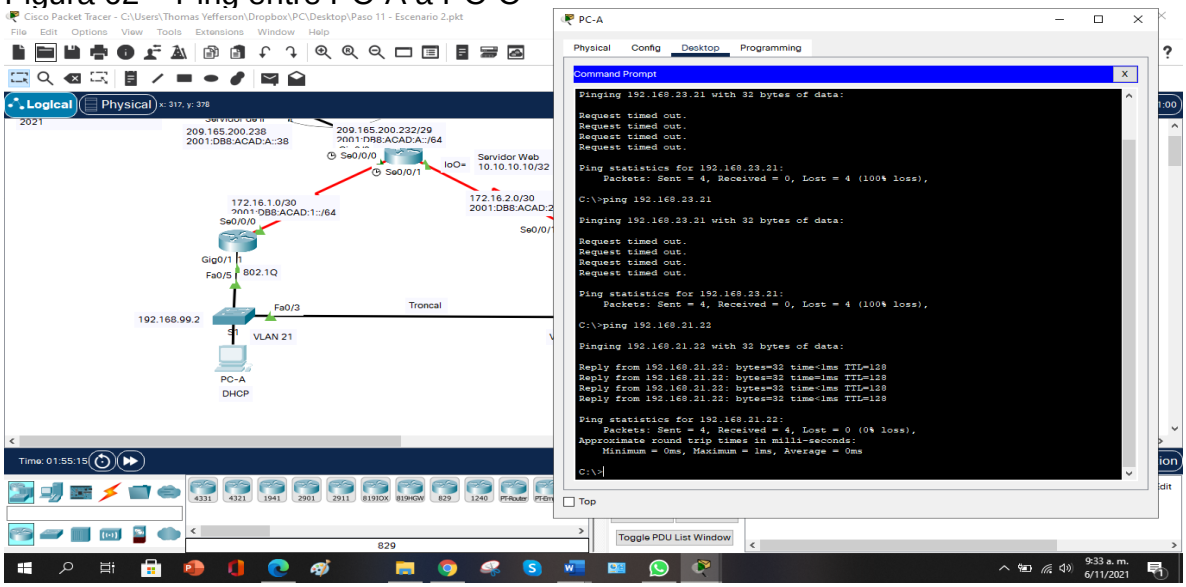


Fuente: Elaboración propia

Verificar que la PC-A pueda hacer ping a la PC-C

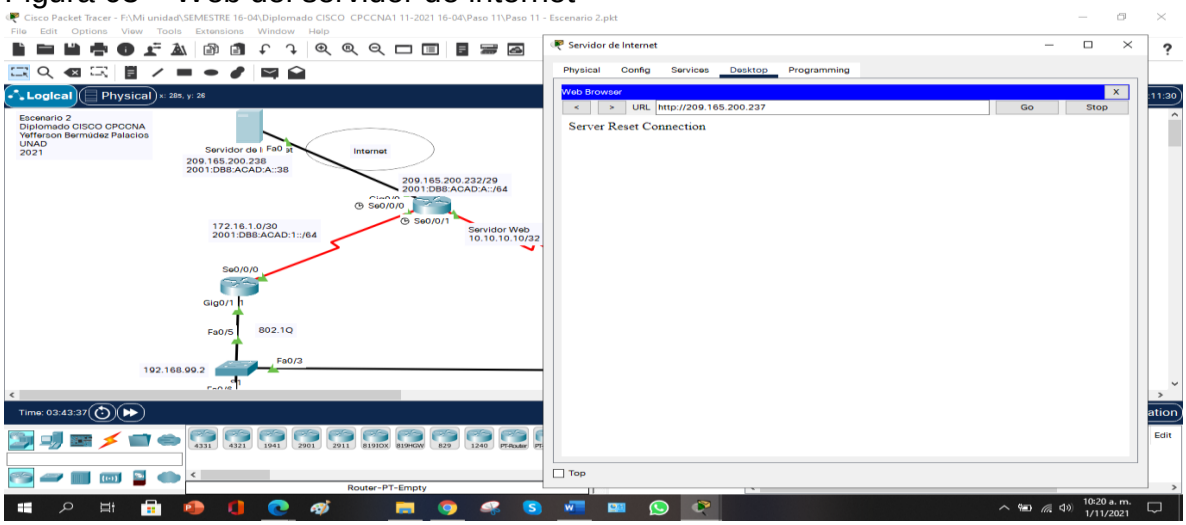
- Nota: Quizá sea necesario deshabilitar el firewall de la PC.

Figura 62 – Ping entre PC-A a PC-C



Fuente: Elaboración propia

Figura 63 – Web del servidor de internet



Fuente: Elaboración propia

Nota: observamos que no es satisfactorio, recordemos que al tratar de habilitar el servidor HTTP, packet tracer no aceptó los comandos.

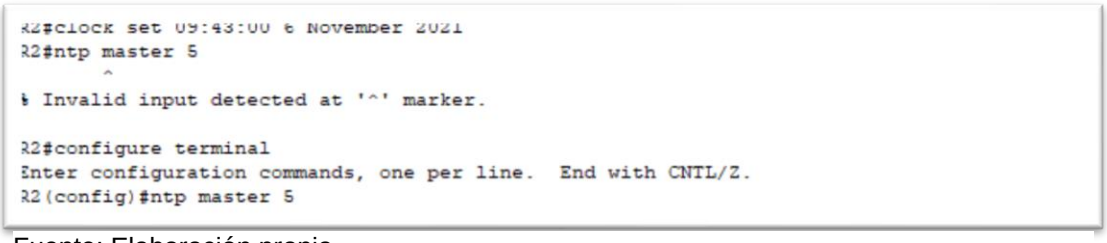
PARTE 6: CONFIGURAR NTP

Ajuste la fecha y hora en R2. 5 de marzo de 2016, 9 a. m.
SE PROHIBE EL ACCESO NO AUTORIZADO
User Access Verification
Password:
R2>enable
Password:
R2#clock set 10:26:00 01 November 2021

Configure R2 como un maestro NTP.

- Nivel de estrato: 5
  R2(config)#ntp master 5

Figura 64 – R2 maestro NTP

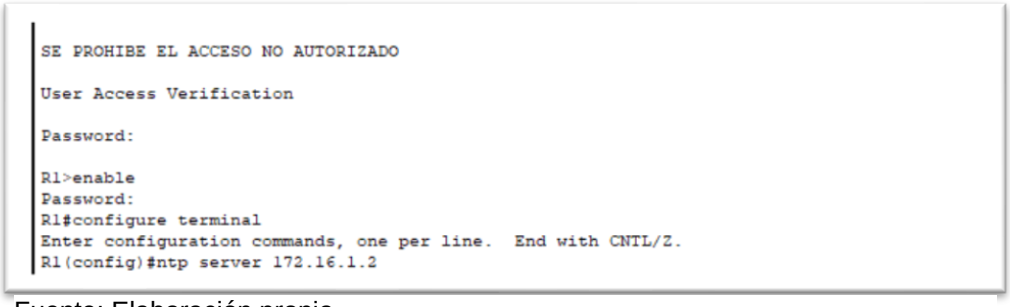


Fuente: Elaboración propia

Configurar R1 como un cliente NTP.

- Servidor: R2
  R1>enable
  Password:
  R1#configure terminal
  Enter configuration commands, one per line. End with CNTL/Z.
  R1(config)#ntp server 172.16.1.2

Figura 65 – Configuración R1 como un cliente NTP



Fuente: Elaboración propia

Configure R1 para actualizaciones de calendario periódicas con hora NTP.

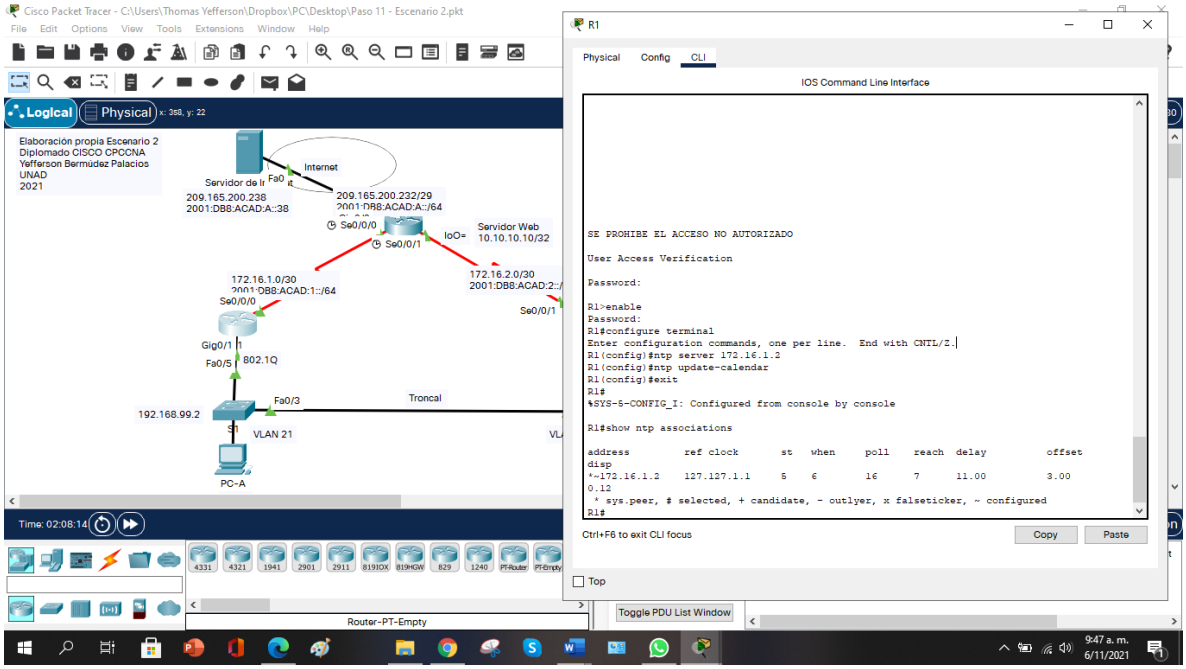
R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1

R1#show ntp associations

address ref clock st when poll reach delay offset disp
*~172.16.1.2 127.127.1.1 5 6 16 7 11.00 3.00 0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#

Figura 65 – Verificación de R1 con NTP



Fuente: Elaboración propia

PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO(ACL)

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

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

Aplicar la ACL con nombre a las líneas VTY

R2(config-std-nacl) #permit host 172.16.1.1
R2(config-std-nacl)#exit

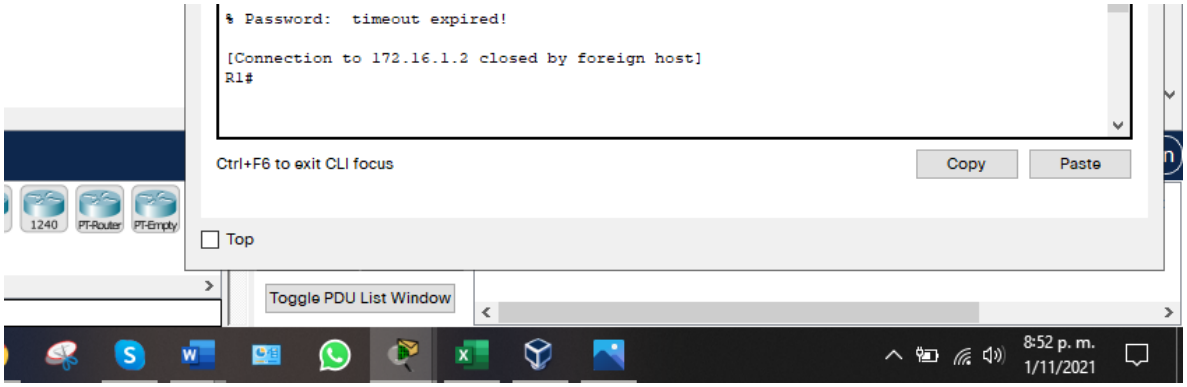
Permitir acceso por Telnet a las líneas de VTY

R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#exit

Verificar que la ACL funcione como se espera

R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSE PROHIBE EL ACCESO NO AUTORIZADO

Figura 66- verificación en el R1 que funciona



Fuente: Elaboración propia

R3>enable
Password:
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#

Figura 67- verificación en el R3 que funciona

Fuente: Elaboración propia

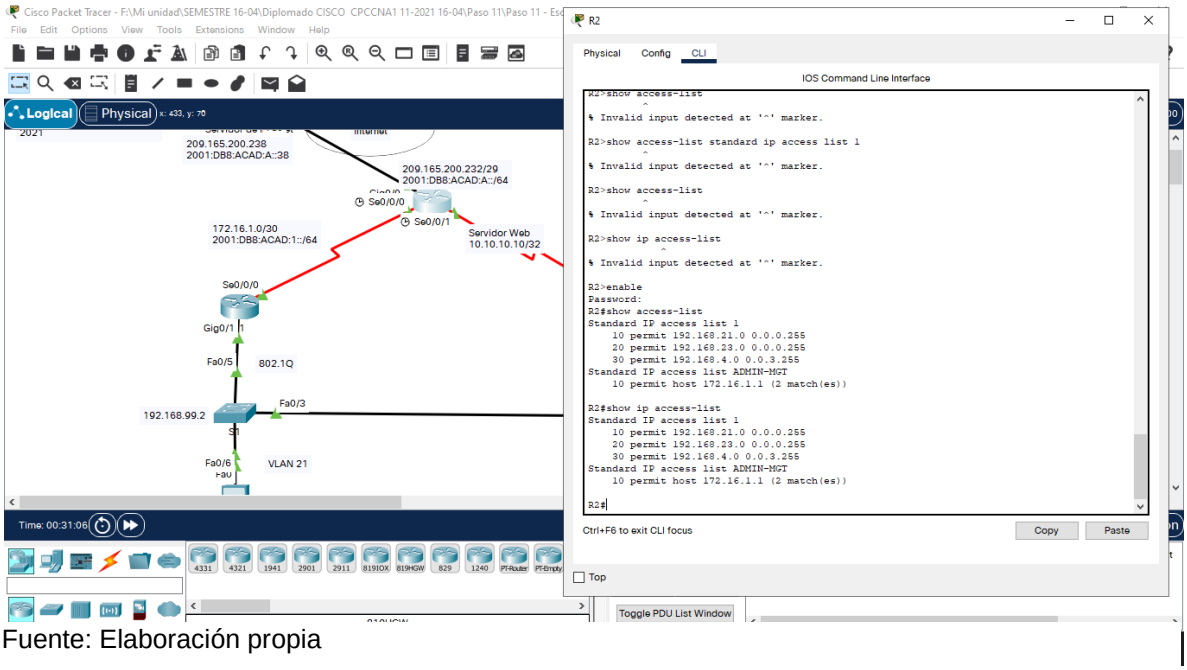
Paso 2: Introducir el comando CLI adecuado que se necesita para mostrar lo siguiente

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

R2>enable
Password:
R2#show access-list
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1 (2 match(es))

R2#show ip access-list
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1 (2 match(es))

Figura 68- Verificación coincidencias recibidas por una lista de acceso desde la última vez que se restableció.



Fuente: Elaboración propia

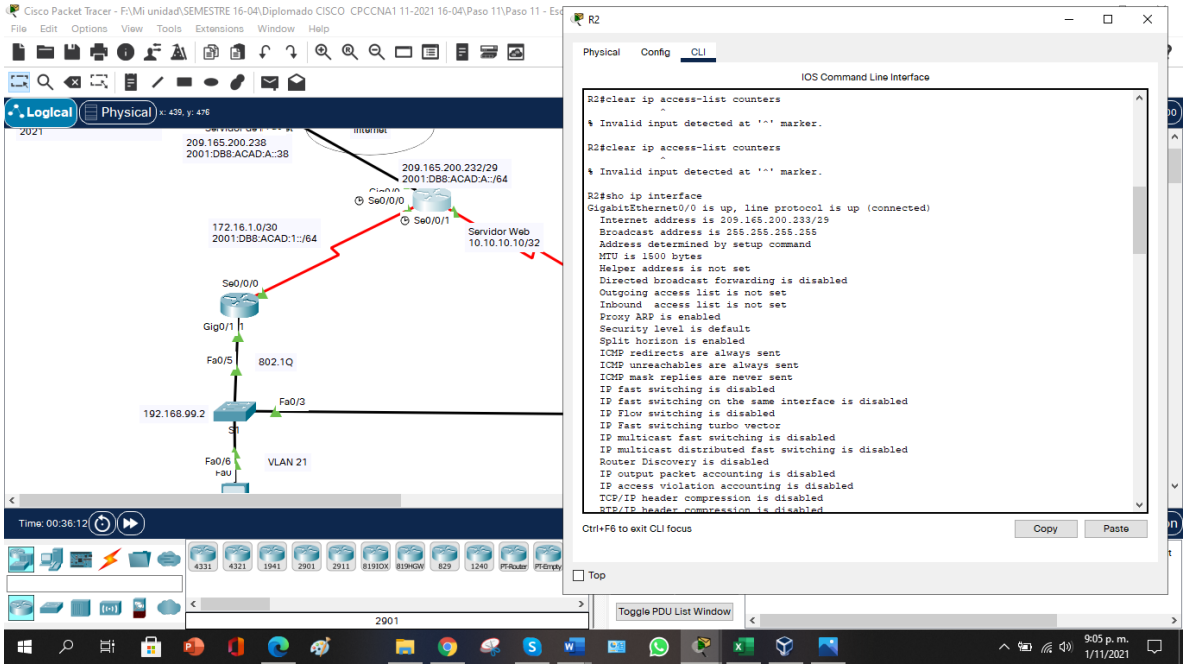
Restablecer los contadores de una lista de acceso

R2#clear access-list counters

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

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

Figura 69 - show ip interface



Fuente: Elaboración propia

¿Con qué comando se muestran las traducciones NAT?

- Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.

R2#show ip nat translations

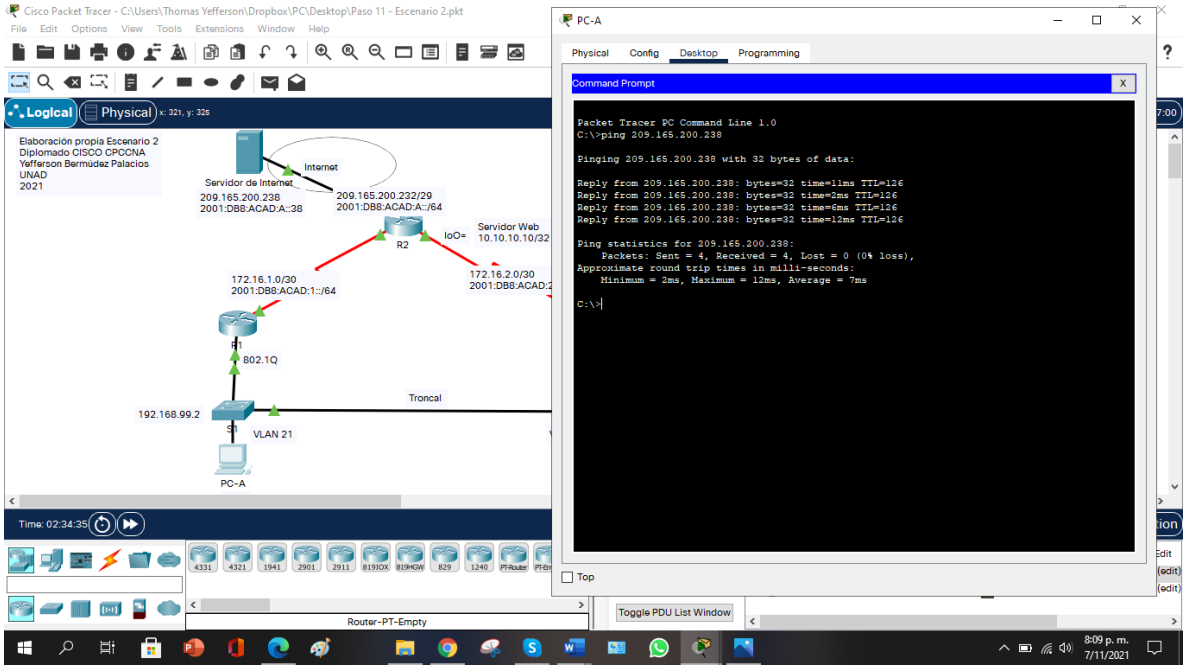
Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.238	10.10.10.10	---	---

Figura 70 – show ip nat translations en R2.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.238   10.10.10.10        ---                ---
```

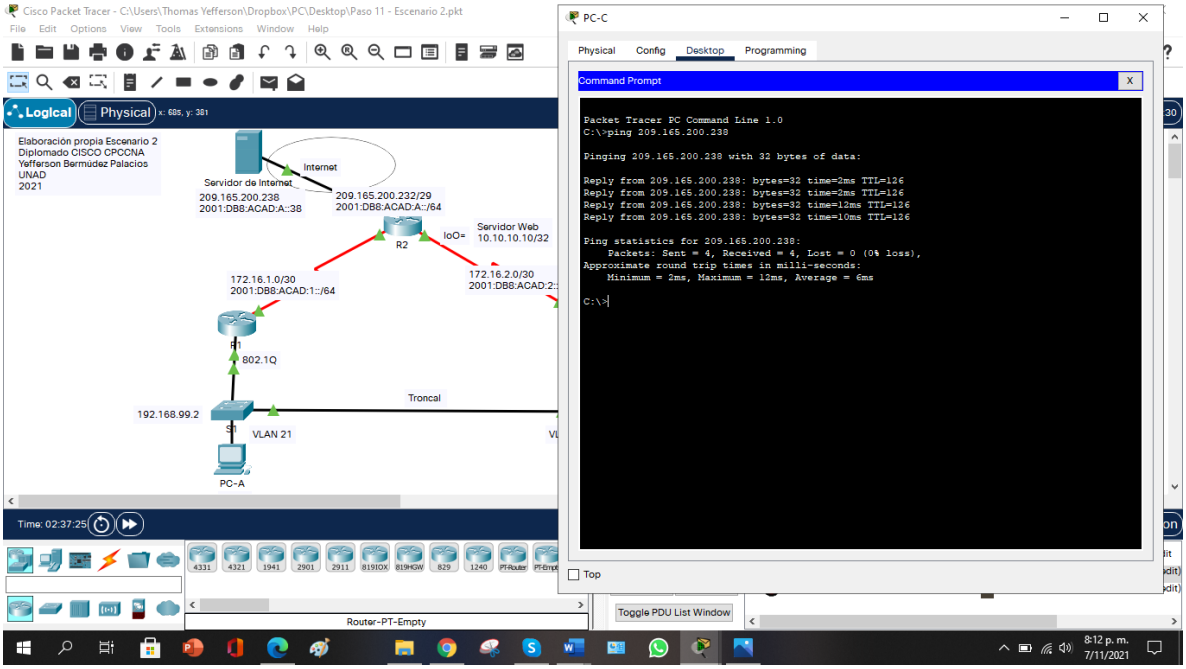
Fuente: Elaboración propia

Figura 71 - Ping del PC-A al servidor de Internet



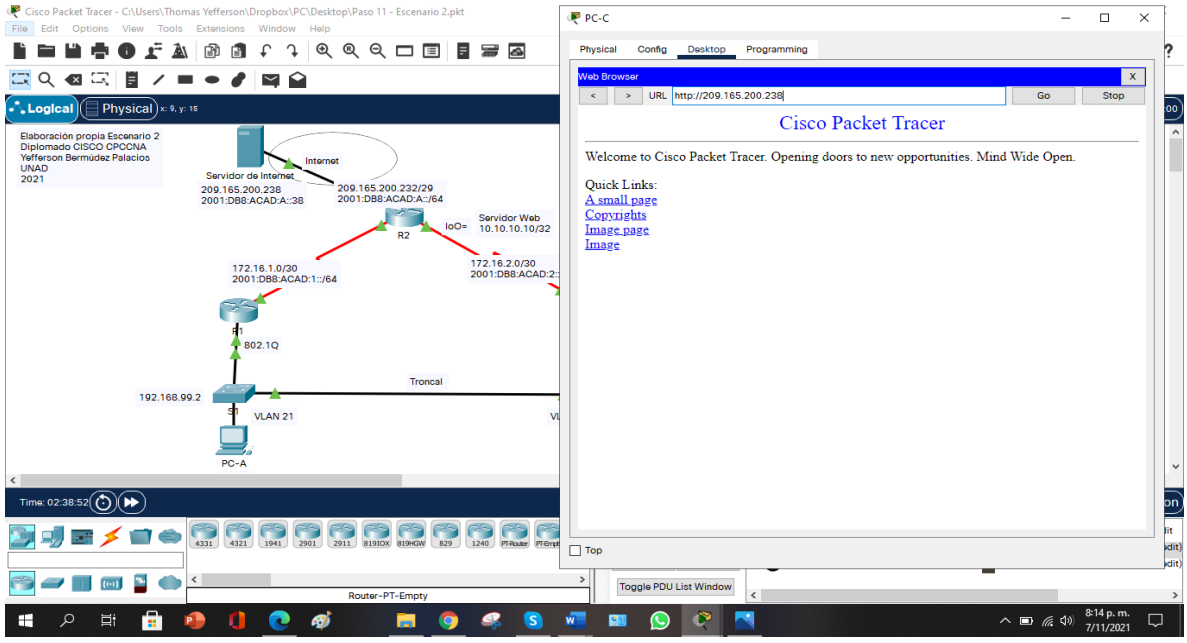
Fuente: Elaboración propia

Figura 72 - Ping del PC-C al servidor de internet



Fuente: Elaboración propia

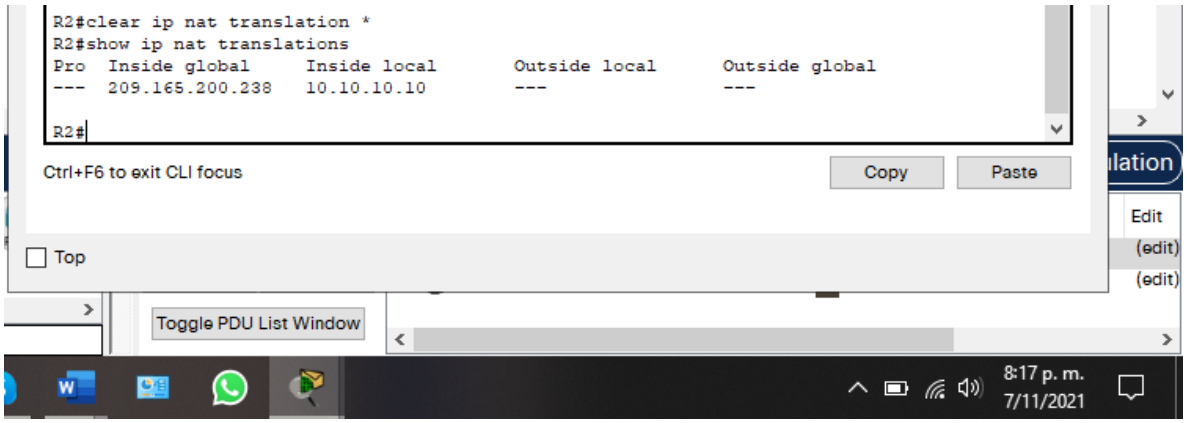
Figura 73 – Acceso del PC-C a servidor web.



Fuente: Elaboración propia

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?
R2#clear ip nat translation *

Figura 74 – clear ip nat translation *



Fuente: Elaboración propia

CONCLUSIONES

De acuerdo con los contenidos analizado por los dos escenarios, podemos conceptualizar con claridad el termino de red, que no es más que un conjunto de equipos conectador por cables señales, ondas o cualquier otro método de transportes de datos, que comparte información, (archivos) y servicios como lo es acceso a internet, se pudo comprender todos los beneficios y mecanismos que se implementan en una red y comandos al configurarla y tener la mejor optimización de la misma.

Se aprendieron mediante simulaciones distintas tareas básicas para configurar, conexión y administración de redes. Además, se cumplió con la totalidad de los puntos propuestos en la guía de actividades del curso de diseño e implementación de soluciones integradas LAN, correspondientes al diplomado de profundización prueba de habilidades practicas CCNP.

BIBLIOGRÁFIAS

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4.

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10.

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6.

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.

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

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2.

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

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7.

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8.

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5.

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1.

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3.

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

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

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

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC.

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm.

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9.

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3.

Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167.