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

RENZO MAURICIO VILLANUEVA BARRAGÁN

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

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

RENZO MAURICIO VILLANUEVA BARRAGÁN

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

DIRECTOR:

MARÍA ALEJANDRA LÓPEZ

MAGISTER

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

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Ibagué, 23 de noviembre de 2021

CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

Cable: es un cordón que se compone de diferentes conductores, los cuales están aislados entre sí. ... Se denomina cable de red o cable de conexión al elemento físico que permite conectar entre sí a diferentes computadoras (ordenadores) y a otros aparatos informáticos.

Computador: es un dispositivo informático que es capaz de recibir, almacenar y procesar información de una forma útil. Una computadora está programada para realizar operaciones lógicas o aritméticas de forma automática.

Configuración: disposición y forma de las partes que componen un todo de los componentes.

DNS: es el acrónimo para “Domain Name System”, es un servicio que habita un enlace entre nombres y direcciones ip con los que están asociados.

IP: dirección de protocolo de internet, conjunto de reglas para la comunicación a través de internet.

Ping: es una utilidad de diagnóstico en red de computadoras que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos remotos de una red que ejecuten IP

Red informática: es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.)

Router: es un dispositivo que ofrece una conexión Wi-Fi, que normalmente está conectado a un módem y que envía información de Internet a tus dispositivos personales, como ordenadores, teléfonos o tables. Los dispositivos que están conectados a Internet en tu casa conforman tu red de área local (LAN).

Switch: es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

RESUMEN

Se presenta trabajo para la sustentación del diplomado de profundización CISCO (LAN/WAN) mediante el uso de herramientas de simulación del software Cisco Packet Tracer en el desarrollo de redes (LAN/WAN) donde se realiza un análisis de comportamiento de diversos protocolos y métricas de enrutamiento para el desarrollo de dos escenarios, compuesto por diferentes dispositivos para lograr una conexión de red satisfactoria.

Se utiliza todo el conocimiento adquirido mediante el desarrollo de diferentes laboratorios, acompañamiento de cipas, y evaluaciones del componente practico obteniendo un resultado positivo, se logra dar solución a cada uno de los escenarios gracias al apoyo incondicional de la tutora y la directora del curso donde se despejaron muchas dudas.

Cada escenario tiene temas de solución como desactivar los DNS de un router, cambio de nombre de los dispositivos, Subneteo de la red, creación de usuario local, creación de contraseñas, encriptación de estas entre otros temas.

A continuación, se sustentará el uso de cada comando en los dispositivos de la red, acompañados por su respectiva imagen, también se mostrara la red de Subneteo a implementar en los diferentes dispositivos evidenciando el proceso realizado obteniendo con un resultado satisfactorio.

Palabras clave : Cable, computador, configuración, dns, internet, ip, ping, red informática, router, switch.

ABSTRACT

Work is presented for the support of the CISCO in-depth diploma (LAN / WAN) through the use of Cisco Packet Tracer software simulation tools in the development of networks (LAN / WAN) where a behavior analysis of various protocols and metrics is performed routing for the development of two scenarios, composed of different devices to achieve a satisfactory network connection.

All the knowledge acquired through the development of different laboratories, monitoring of cipas, and evaluations of the practical component is used, obtaining a positive result, it is possible to solve each of the scenarios thanks to the unconditional support of the tutor and the director of the course where many doubts were cleared.

Each scenario has solution issues such as disabling the DNS of a router, renaming the devices, subnetting the network, creating a local user, creating passwords, encryption of these among other issues.

Next, the use of each command in the network devices will be supported, accompanied by its respective image, the Subneteo network to be implemented in the different devices will also be shown, evidencing the process carried out, obtaining a satisfactory result.

Keywords: Cable, computer, configuration, dns, internet, ip, ping, computer network, router, switch.

INTRODUCCIÓN

Se presentará la documentación del desarrollo y configuración de cada uno de los dispositivos de la topología, información del paso a paso evidenciado por imágenes y programación de los dispositivos, se realizará pruebas de conectividad mediante el comando ping, show ip rout, show running-config con el propósito de demostrar el conocimiento adquirido durante el diplomado de profundización cisco (LAN/WAN).

Su fin es implementar conocimiento mediante el software Cisco Packet Tracer, mediante el uso de diferentes escenarios donde se desarrolla diferentes tipos de topología bajo el uso de las soluciones de Cisco Packet Tracer. Lo primordial es poner a prueba los conocimientos adquiridos para dar soluciones a futuros problemas en nuestro ámbito laboral como ingeniero de sistemas.

OBJETIVOS

OBJETIVO GENERAL

Desarrollar los escenarios de diplomado Evaluación-prueba de habilidades prácticas CCNA como trabajo final, mediante la implementación de los escenarios de diferentes topologías para dar solución para el uso de estas redes.

OBJETIVOS ESPECÍFICOS

- Configurar los dispositivos finales para proporcionar acceso a recursos de la red local.
- Analizar la arquitectura propuesta con el fin de implementar su simulación por medio del software Packet Tracer 8.2.
- Desarrollar y registrar cada uno de los procedimientos realizados para la configuración de los dispositivos.
- Realizar la verificación de la conectividad ende cada uno de ellos.

DESARROLLO

ESCENARIO 1

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.

Figura 1. Topología

Escenario 1

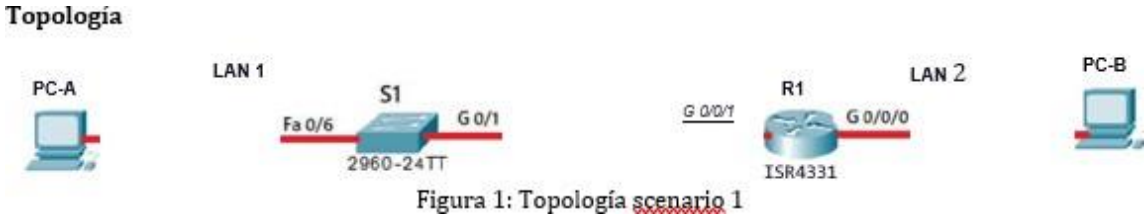


Figura 1: Topología scenario 1

Tomada de prueba de habilidades CCNA

Tabla 1**.** Tabla de direccionamiento

Item	Requerimiento
Dirección de Red	192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1

R1 G0/0/0	Primera dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1
PC-A	Última dirección de host de la subred LAN1
PC-B	Última dirección de host de la subred LAN2

Fuente: Elaboración propia

Tabla 2. Datos de la Subredes

Descripción de la subred	Cantidad de host	Direccionamiento de red	Primera dirección utilizable	Ultima dirección utilizable	Dirección de broascast
Lan 1	100	192.168.41.0/25	192.168.41.1	192.168.41.126	192.168.41.127
Lan 2	50	192.168.41.128/26	192.168.41.129	191.168.41.190	192.168.41.191

Fuente: Elaboración propia

Se realiza el Subneteo de la red con la dirección ip 192.168.41.0 como resultado salen 2 sub redes.

Tabla 3. Direccionamiento de los dispositivos

dispositivo	Interfaz	Dirección	Mascara	Gateway
R 1	G0/0/0/1	192.168.41.1	255.255.255.128	
	G0/0/0/0	192.168.41.129	255.255.255.192	
S1	VLAN1	192.168.41.2	255.255.255.128	192.168.41.1
PC-A	NIC	192.168.41.126	255.255.255.128	192.168.41.1
PC-B	NIC	192.168.41.190	255.255.255.192	192.168.41.129

Fuente: Elaboración propia

Se asigna direcciones a cada uno de los dispositivos de la red.

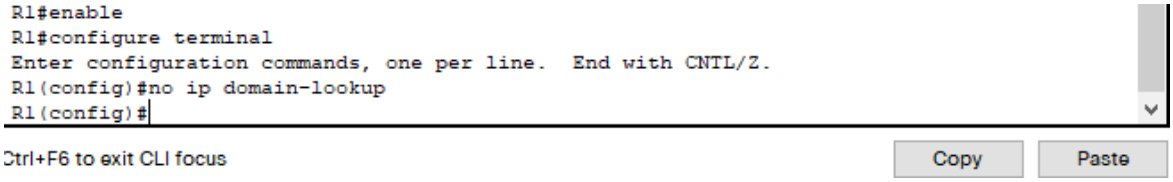
Paso 1: configurar los ajustes básicos

- Desactivar la búsqueda de DNS
- Nombre del router R1
- Nombre de dominio

- Contraseña cifrada para el modo EXEC privilegiado
- Contraseña de acceso a la consola
- Establecer la longitud mínima para las contraseñas
- Crear un usuario administrativo en la base de datos local
- Configurar el inicio de sesión en las líneas VTY para que use las bases de datos local
- Configurar VTY solo aceptando el SSH
- Cifrar las contraseñas de texto no cifrado
- Configure un MOTD banner
- Configurar interfaz G0/0/0
- Configurar interfaz G0/0/1
- Generar una clave de cifrado RSA

```
Router>enable
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
no ip domain-lookup
hostname R1
#interface gigabitEthernet 0/0/1
ip address 192.168.41.1 255.255.255.128
no shut
interface gigabitEthernet 0/0/0
# ip address 192.168.41.129 255.255.255.192
no shut
ip domain-name ccna-lab.com
enable password ciscoenpass
line console 0
Password ciscoconpass
login
security password min-length 10
crypto key generate rsa
ip ssh version 2
line vty 0 15
transport input ssh
login local
username admin secret admin1pass
enable secret admin1pass
banner motd %Se prohibe el acceso no autorizado.%
service password-encryption
do copy running-config startup-config
```

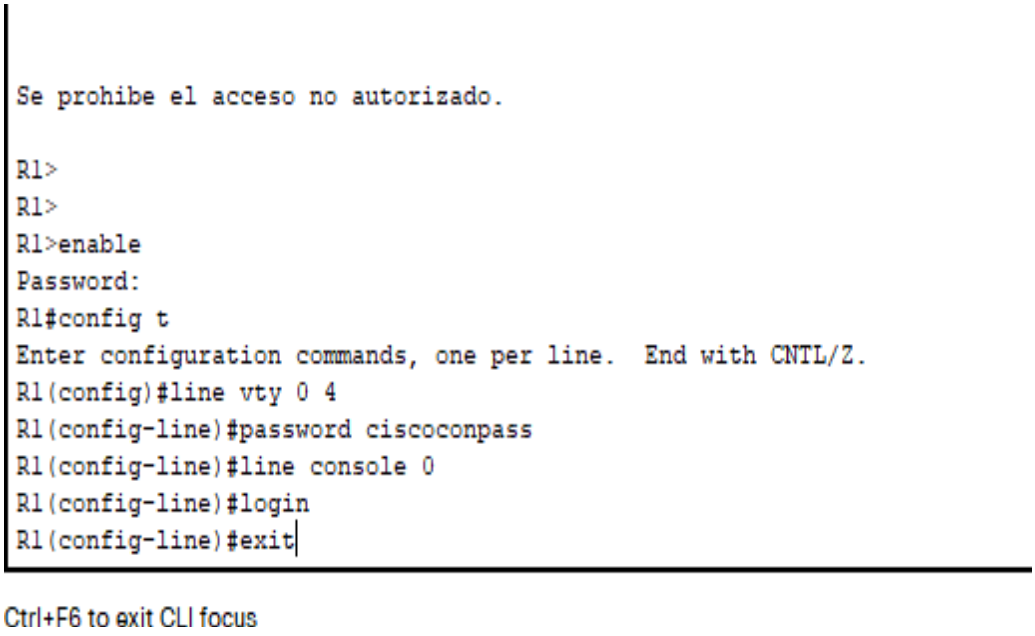
Figura 2. Desactivar búsqueda de DNS



Fuente: Elaboración propia

Mediante el código no ip domain-lookup se desactiva la búsqueda de los DNS

Figura 3. Configuración password



Fuente: Elaboración propia

Mediante el comando line vty 0, password ciscoconpas, line console 0, login

Figura 4. Configuración de ip R1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gi
Router(config)#interface gigabitEthernet 0/0/1
Router(config-if)# ip address 192.168.41.1 255.255.255.128
Router(config-if)#no shut
Router(config-if)#
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)# ip address 192.168.41.129 255.255.255.192
Router(config-if)#no shut
Router(config-if)#
Router#
```

Fuente: Elaboración propia

Mediante el comando de interface gigabitEthernet 0/0/0 y interface gigabitEthernet 0/0/1, ip address 192.168.41.1 255.255.255.128 y ip address 192.168.41.129 255.255.255.192 y no shut se activan las interfaces.

Figura 5. Configuración Dominio R1

```
R1(config)#ip domain-name ccna-lab.com
```

Fuente: Elaboración propia

Se utiliza el comando ip domain-name ccna-lab.com

Figura 6. Configuración de mínimo 10 caracteres R1

```
R1(config)#security password min-length 10
R1(config)#
```

Fuente: Elaboración propia

Se utiliza el comando security password min-length 10

Figura 7. Configuración SSh R1

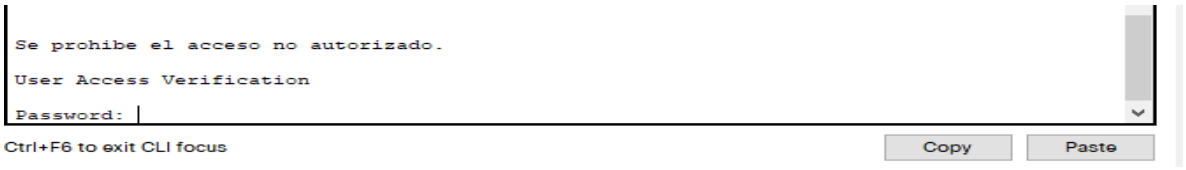
```
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

Fuente: Elaboración propia

Se utiliza crypto key generate rsa

Figura 8. Configuración banner R1



Fuente: Elaboración propia

Se utiliza el comando banner

Configuración S1

- Desactivar la búsqueda DNS
- Nombre del switch
- Nombre de dominio
- Contraseña cifrada para el modo EXEC privilegiado
- Contraseña de acceso a la consola
- Crear un usuario administrativo en la base de datos local
- 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
- Configurar la interfaz de administración (SVI)
- Configuración del Gateway predeterminado

S1

```
enable
config terminal
no ip domain-lookup
hostname S1
ip domain-name ccna-lab.com
enable password ciscoenpass
line console 0
```

Password ciscoconpass
login
username admin secret admin1pass
enable secret admin1pass
service password-encryption

crypto key generate rsa
ip ssh version 2
line vty 0 15
transport input ssh
banner motd %Se prohibe el acceso no autorizado.%
exit
interface VLAN1
address 192.168.41.2 255.255.255.128
no shutdown
exit
ip default-gateway 192.168.41.1
copy running-config startup-config
Figura 9. Configuración S1

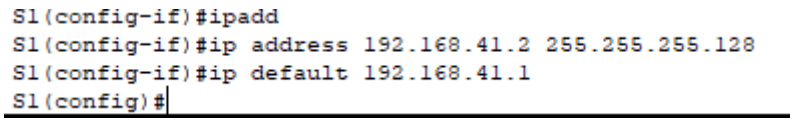
```
S1>enable
Password:
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#no ip domain-lookup
S1(config)#hostname S1
S1(config)#
S1(config)#
S1(config)#
S1(config)#enable password ciscoenpass
S1(config)#line console 0
S1(config-line)#Password ciscoconpass
S1(config-line)#login
S1(config-line)#username admin secret admin1pass
S1(config)#enable secret admin1pass
S1(config)#service password-encryption
S1(config)#
S1(config)#crypto key generate rsa
% Please define a domain-name first.
S1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#banner motd %Se prohibe el acceso no autorizado.%
S1(config)#do copy runnin startup-config
Destination filename [startup-config]?
Building configuration...
```

Fuente: Elaboración propia

Se utilizaron los siguientes

enable
config terminal
no ip domain-lookup
hostname S1
ip domain-name ccna-lab.com
enable password ciscoenpass
line console 0
Password ciscoconpass
login
username admin secret admin1pass
enable secret admin1pass
service password-encryption
crypto key generate rsa
ip ssh version 2
line vty 0 15

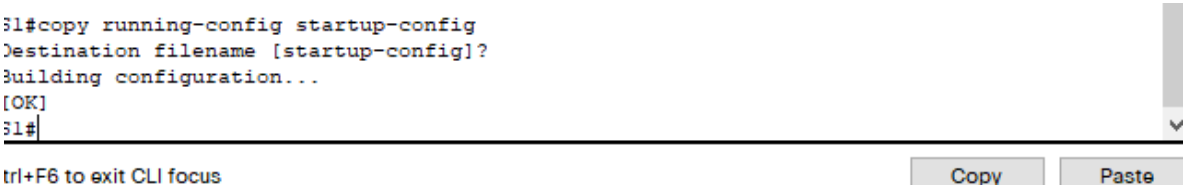
Figura 10. Configuración ip S1



Fuente: Elaboración propia

Se utiliza el comando ip addres 192.168.41.2 255.255.255.128

Figura 11. Guardado de configuración



Fuente: Elaboración propia

Se utiliza el comando copy running-config startup-config

Paso 2 configurar los equipos

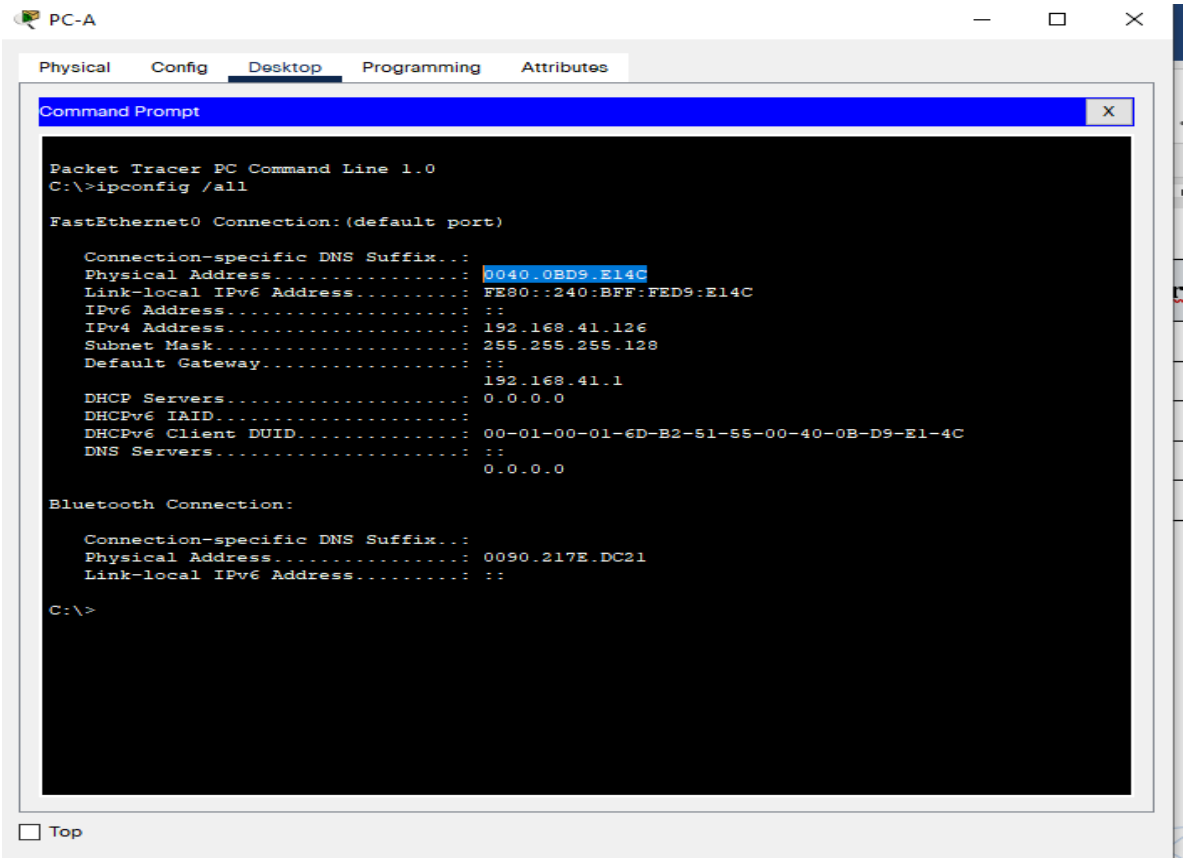
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 4. Configuración PC-A

PC-A Network Configuration	
Descripción	
Dirección física	0040.0BD9.E14C
Dirección IP	192.168.41.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.41.1

Fuente: Elaboración propia

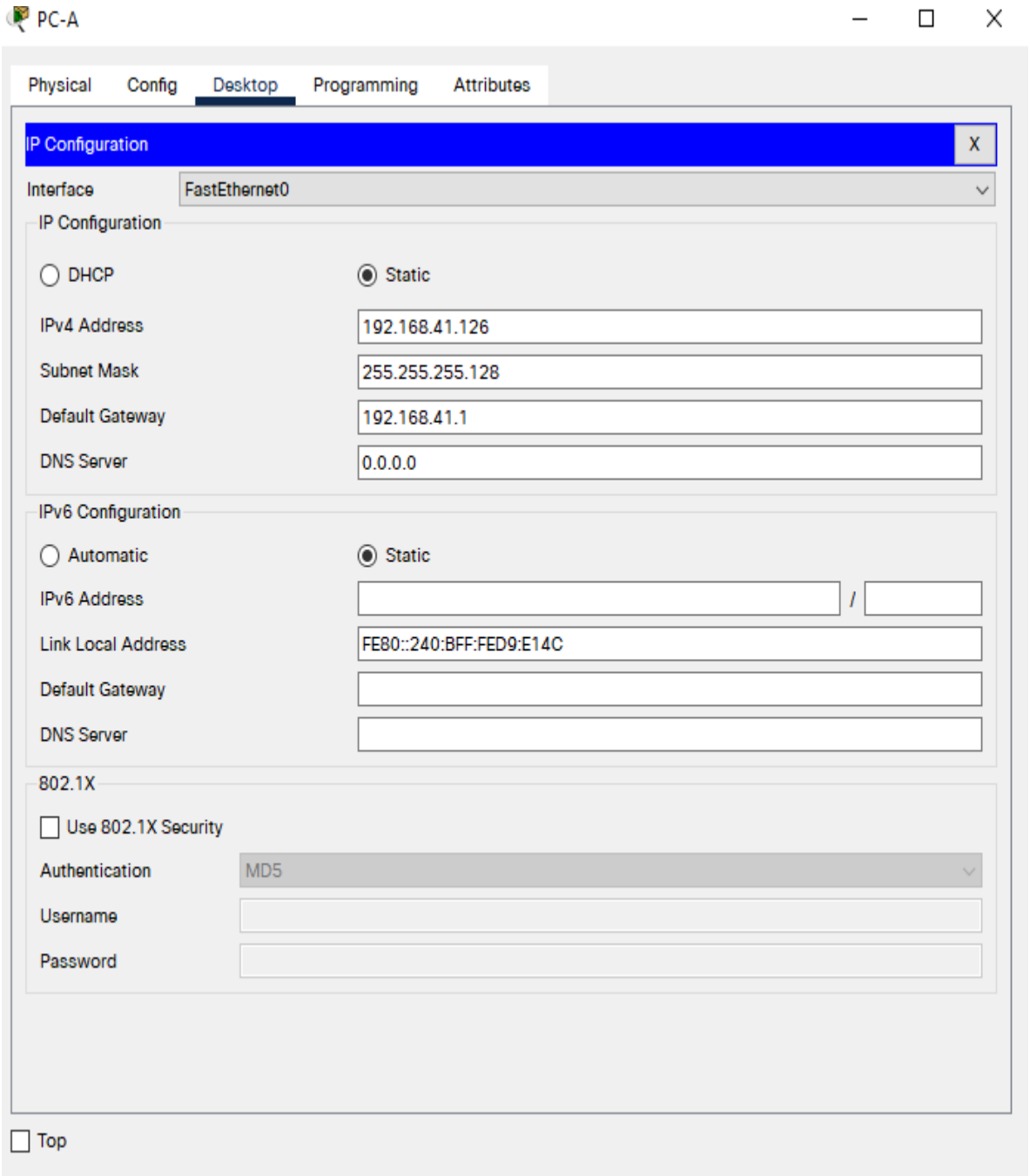
Figura 12. Información ip



Fuente: Elaboración propia

Se utiliza el comando ipconfig /all

Figura 13. Configuración del PC-A



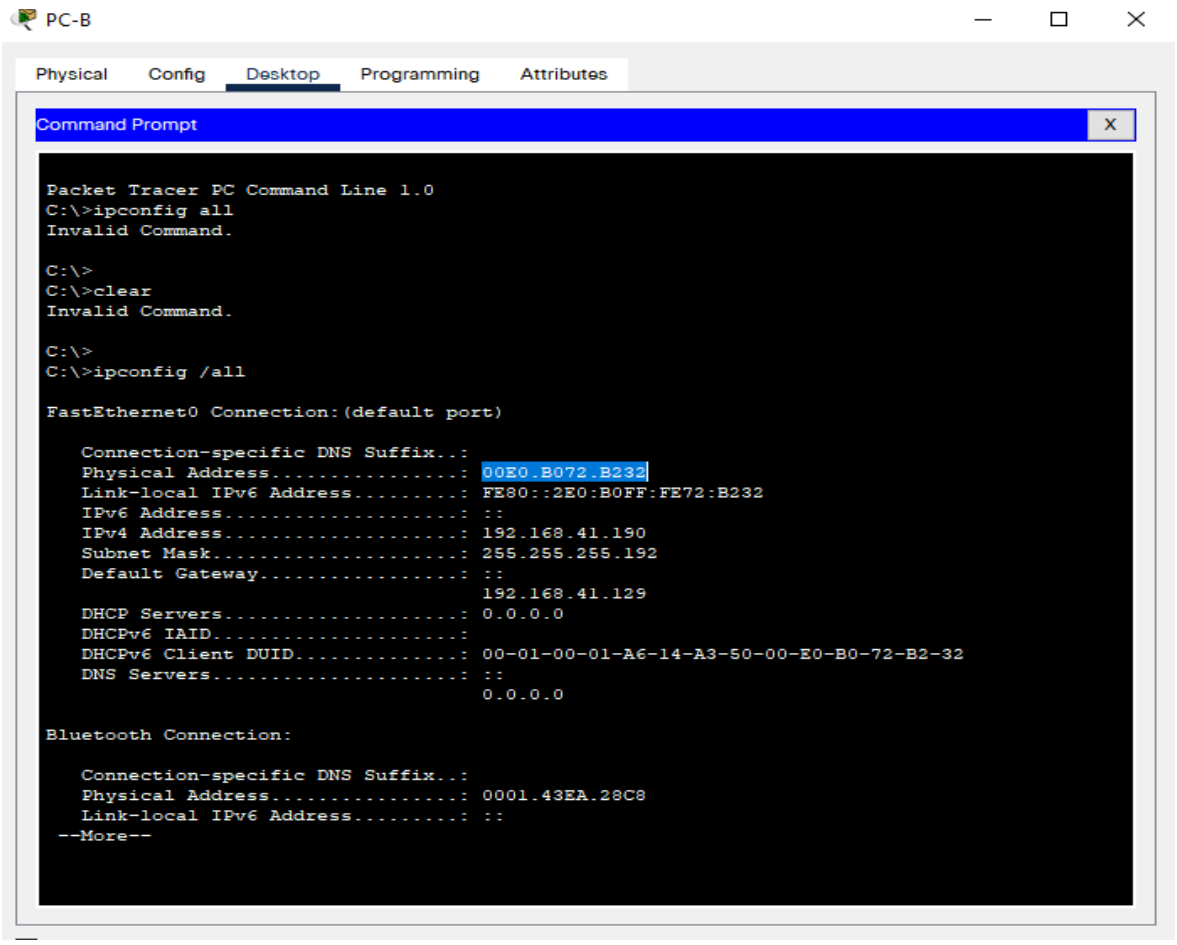
Fuente: Elaboración propia

Tabla 5. Configuración PC-B

PC-B Network Configuration	
Descripción	
Dirección física	00E0.B072.B232
Dirección IP	192.168.41.190
Máscara de subred	255.255.255.192

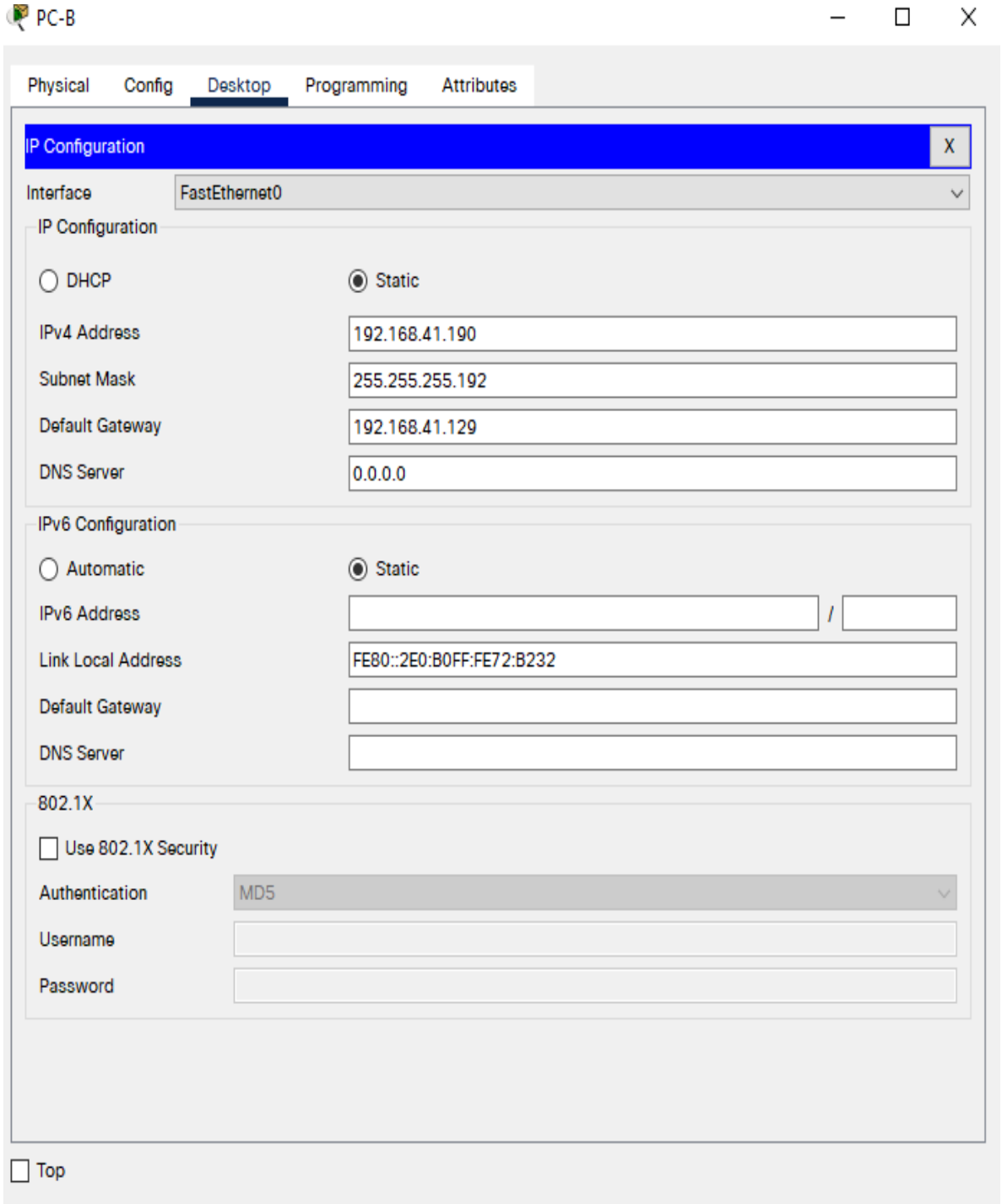
Fuente: Elaboración propia

Figura 14. Información ip



Fuente: Elaboración propia

Figura 15. Configuración PC-B



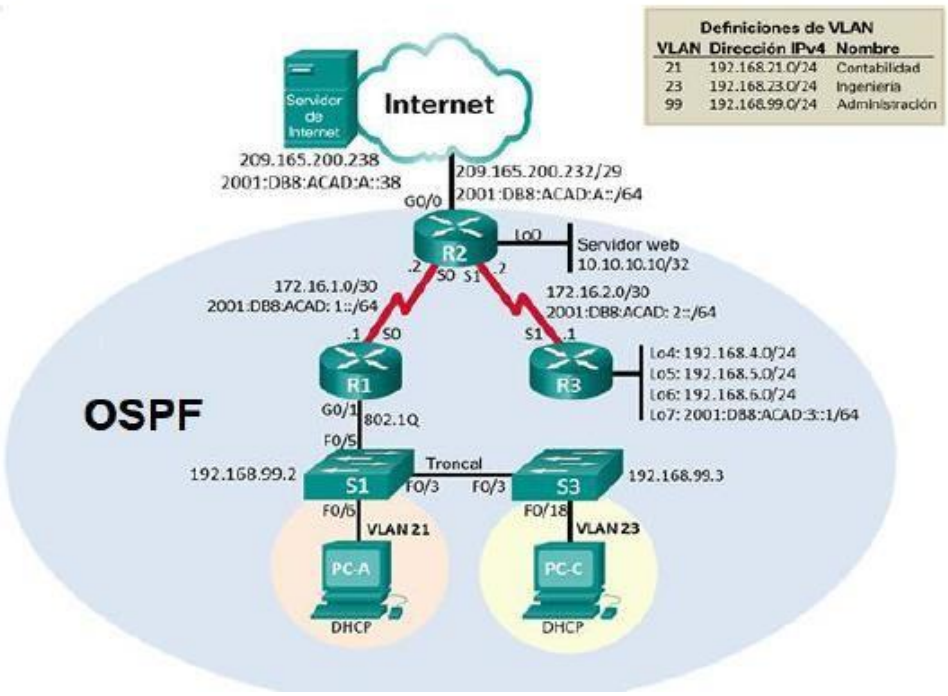
Fuente: Elaboración propia

Escenario 2

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

Figura 16. Topología Escenario 2

Topología



Tomada de prueba de habilidades CCNA

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 6. Eliminación de configuración Router y switches

Tarea	Comando IOS
Eliminar el archivo startup-config de todos los routers	Erase startuo-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	Erase startuo-config
Volver a cargar ambos switches	reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	

Fuente: Elaboración propia

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>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>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#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
CISCO1941/K9 platform with 524288 Kbytes of main memory

Main memory is configured to 64/-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: 0x2bb1c58
Self decompressing the image :
##
######## [OK]
Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
HWIC Slot 1 0x00200000 Onboard devices &
buffer pools 0x01E8F000
- -
TOTAL: 0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/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, C1900 Software (C1900-UNIVERSALK9-M), Version
15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 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 CISCO1941/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 ---

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
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-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: 0x2bb1c58
Self decompressing the image :

```
#############################################################################
######## [OK]
Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
HWIC Slot 1 0x00200000 Onboard devices &
buffer pools 0x01E8F000
- - - - - - - - - - - - - - - - - - - - - - - - -
TOTAL: 0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/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, C1900 Software (C1900-UNIVERSALK9-M), Version
15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 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 CISCO1941/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 ---

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
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-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: 0x2bb1c58
Self decompressing the image :
[OK]
Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
HWIC Slot 1 0x00200000 Onboard devices &
buffer pools 0x01E8F000
- -
TOTAL: 0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/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, C1900 Software (C1900-UNIVERSALK9-M), Version
15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 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 CISCO1941/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 ---

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>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#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: 00E0.F9E0.BE12
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

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Switch#reload
Proceed with reload? [confirm]
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

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: 0002.1747.5E84
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

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Parte 2: configurar los parámetros básicos de los dispositivos.

Paso 1: configurar la computadora del internet

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

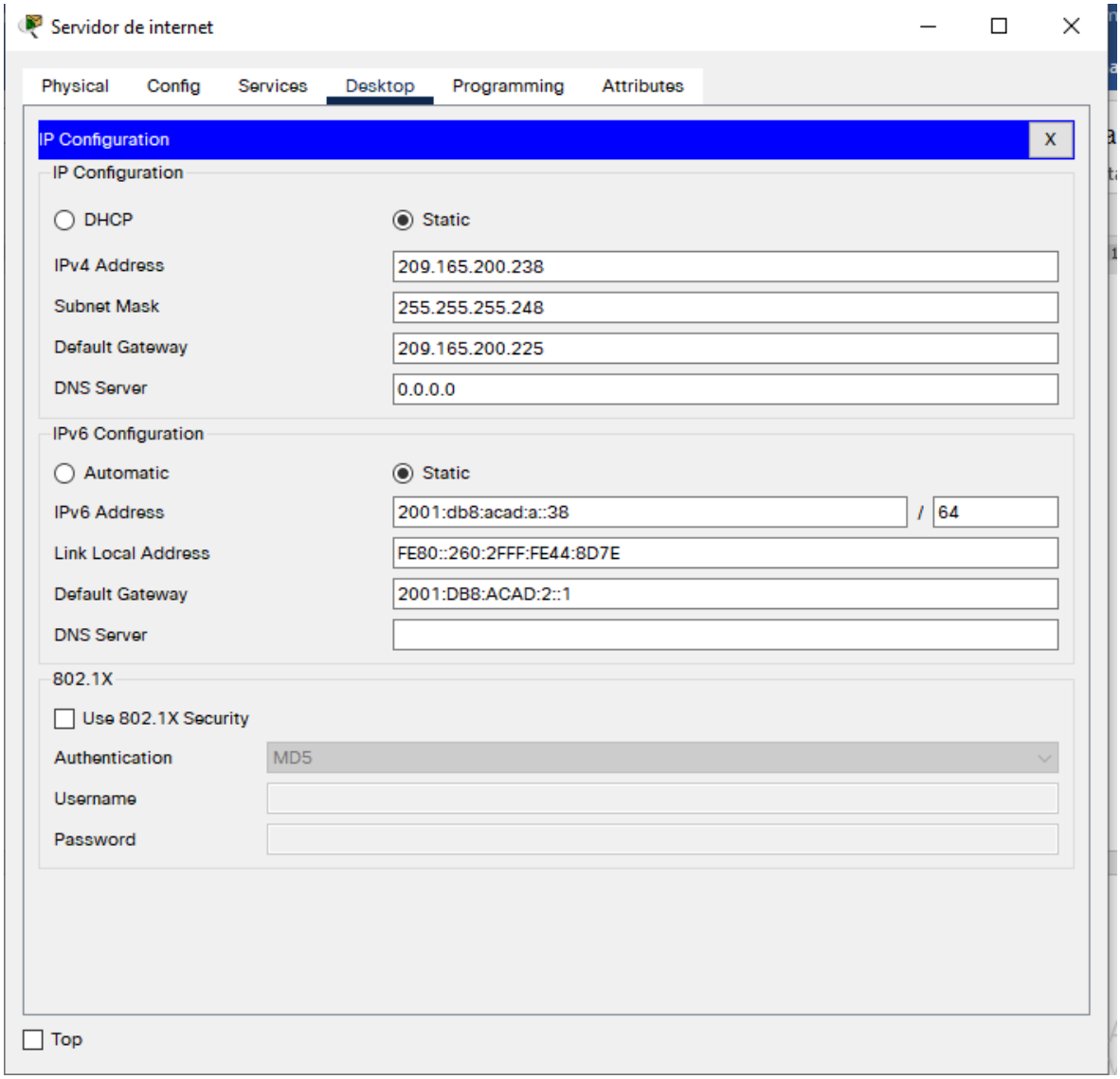
Tabla 7. Datos de configuración del servidor

Elemento o tarea de configuración	Especificación
Direccionamiento IPv4	209.165.200.238
Mascara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:db8:acad:a::38/64

Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: Elaboración propia

Figura 17. Configuración ip servidor



Fuente: Elaboración propia

Paso 2: configurar R1

Tabla 10. Datos de configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Contraseña de exec privilegiado	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no	
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe 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
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

Fuente: Elaboración propia

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
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)#service password-encryption
R1(config)#banner motd %Se prohibe el acceso no autorizado.%
R1(config)#ipv6 unicast-routing
R1(config)#int s0/0/0
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R1(config)#ipv6 route ::/0 s0/0/0
R1(config)#
```

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 11. Datos de configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no	service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe 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
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.
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
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Fuente: Elaboración propia

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
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
R2(config-line)#service password-encryption

R2(config)#ip http server


R2(config)#int s0/1/0
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

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state
to up

R2(config-if)#int s0/1/1
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
This command applies only to DCE interfaces
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down


int g0/0

description Connection to Internet

ip address 209.165.200.238 255.255.255.248
```

ipv6 address 2001:db8:acad:a::1/64

no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description Simulated Web Server
R2(config-if)#
R2#
%SYS-5-CONFIG_I: Configured from console by console

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

Observación: el comando (ip http server) no es compatible con Packet Tracer.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 12. Datos de configuración R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado	class
Contraseña de acceso a la	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no	
Mensaje MOTD	Se prohíbe 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
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7 Router>	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la

Fuente: Elaboración propia

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
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
R3(config-line)#service password-encryption
R3(config)#banner motd %Se prohibe el acceso no autorizado.%
R3(config)#
R3(config)#ipv6 unicast-routing
R3(config)#int s0/0/1
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:AC
% Incomplete command.
R3(config-if)#
R3(config-if)#interface loopback 4

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

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

R3(config-if)#int loopback 5

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

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

R3(config-if)#
R3(config-if)#interface loopback 6

R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#
R3(config-if)#interface loopback 7

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

Paso 5: configurar S1

Tabla 13. Datos de configuracion S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado	Class
Contraseña de acceso a la consola	Cisco

Contraseña de acceso Telnet	Cisco
Cifrar las contraseñas de texto no	Enable secret
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Elaboración propia

enable

configure terminal

no ip domain-lookup

hostname S1

enable secret class

line console 0

password cisco

login

exit

line vty 0 15

password cisco

login

exit

service password-encryption

banner motd %Se Se prohíbe el acceso no autorizado.%

Paso 6: configurar S3

Tabla 14. Datos de configuración S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco
Cifrar las contraseñas de texto no	Enable secret

Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Elaboración propia

enable

configure terminal

no ip domain-lookup

hostname S3

enable secret class

line console 0

password cisco

login

line vty 0 15

password cisco

login

exit

service password-encryption

banner motd %Se Se prohíbe el acceso no autorizado.%

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.

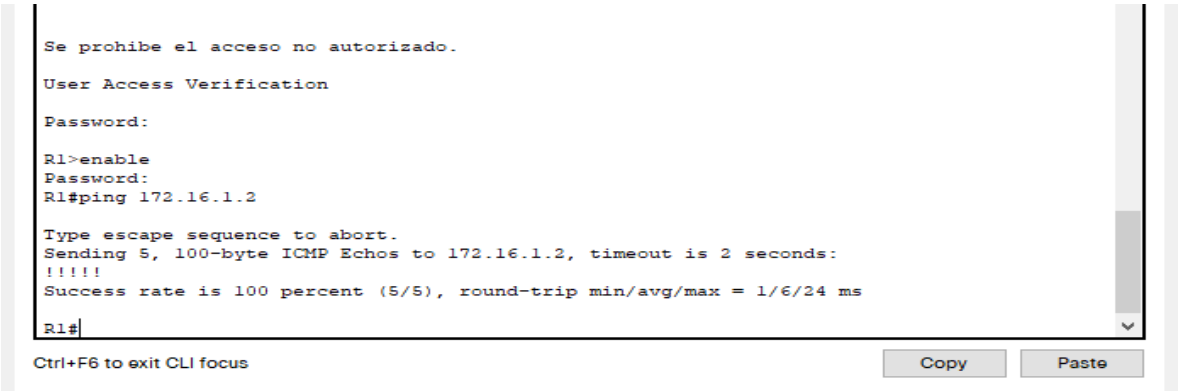
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 15. Datos para realizar ping

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	success
R2	R3, S0/0/1	172.16.2.1	Success
PC de Internet	Gateway	209.165.200.238	Succes

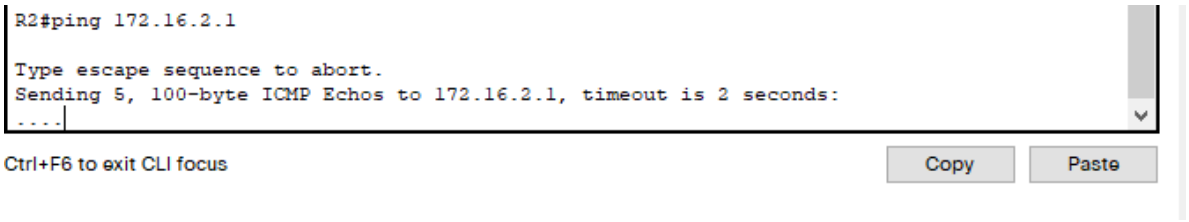
Fuente: Elaboración propia

Figura 18. Ping 172.16.1.2



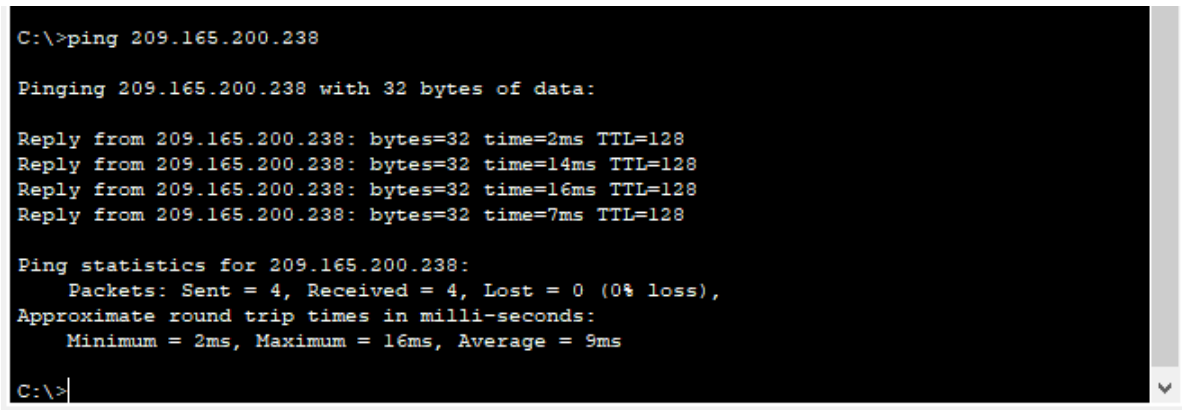
Fuente: Elaboración propia

Figura 19. Ping 172.16.2.1



Fuente: Elaboración propia

Figura 20. Ping 209.165.200.223



Fuente: Elaboración propia

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

Tabla 16. Seguridad del switchs

Elemento o tarea de configuración	Especificación
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
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
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

Fuente: Elaboración propia

```
S1>enable
Password:
S1#enable
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)#exit
S1(config)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#exit
S1(config)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
S1(config)#
interface vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
%LINK-5-CHANGED: Interface Vlan99, changed state to up
```

```
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#
S1(config)#interface f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to down

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

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

S1(config-if)#
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
```

--More—

```
S1#enable
S1#
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#no shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
show interface f0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

S1#enable
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
S1(config)#interface range g0/1-2, f0/1-2, f0/4, f0/6-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#
S1(config-if-range)#exit
S1(config)#interface f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#exit
S1(config)#interface range g0/1-2, f0/1-2, f0/4, f0/7-24
S1(config-if-range)#shutdown

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

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down

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

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

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

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to
administratively down
```

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#

Paso 2: configurar el S3

Tabla 17. Configuración S3

Elemento o tarea de configuración	**Especificación**

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.
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
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	interface f0/18
Apagar todos los puertos sin usar	switchport access vlan 21

Fuente: Elaboración propia

```
S3>enable
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)#exit
S3(config)#vlan 23
S3(config-vlan)#name ingenieria
S3(config-vlan)#exit
S3(config)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
S3(config)#
S3(config)#interface vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
%LINK-5-CHANGED: Interface Vlan99, changed state to up

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

S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#
S3(config)#interface f0/3
S3(config-if)#switchport mode trunk
```

S3(config-if)#switchport trunk native vlan 1
S3(config-if)#no shutdown

S3#show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

S3(config-if-range)#interface range g0/1-2, f0/1-2, f0/4-24
S3(config-if-range)#switchport mode access
S3(config-if-range)# S3(config)#interface f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#

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

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

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

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

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

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

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

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

Paso 3: configurar R1

Tabla 18. Configuración R1

Elemento o tarea de configuración	Especificación
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
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
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
Activar la interfaz G0/1	No shutdown

Fuente: Elaboración propia

R1#enable

```
R1#interface g
R1#interface gi
R1#configure y
R1#configure t
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

R1(config-if)#do copyrunnig-config startup-config
copyrunnig-config startup-config
^
% Invalid input detected at '^' marker.
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-co
R1#copy running-config st
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#



R1 con0 is now available


Press RETURN to get started.
```

Se prohibe el acceso no autorizado.

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/1.21
R1(config-subif)#R1(config-subif)#description LAN de Contabilidad
^
% Invalid input detected at '^' marker.
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.21, changed state to up

R1(config-subif)#exit
R1(config)#
R1(config)#interface g0/1.23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.23, changed state to up

R1(config-subif)#exit
R1(config)#interface g0/1.99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.99, changed state to up

R1(config-subif)#exit
R1(config)#interface g0/1
R1(config-if)#no shutdown
R1(config-if)#

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.

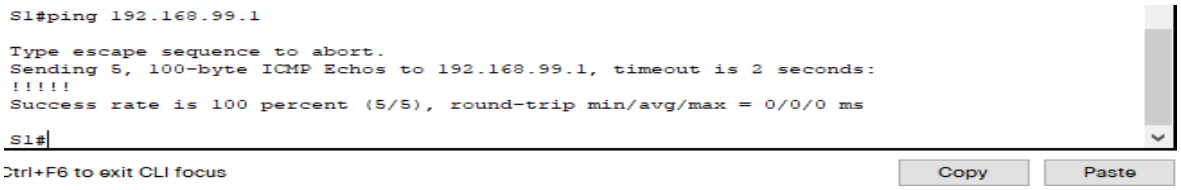
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 19 verificación de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	success
S3	R1, dirección VLAN 99	192.168.99.1	success
S1	R1, dirección VLAN 21	192.168.21.1	success
S3	R1, dirección VLAN 23	192.168.23.1	error

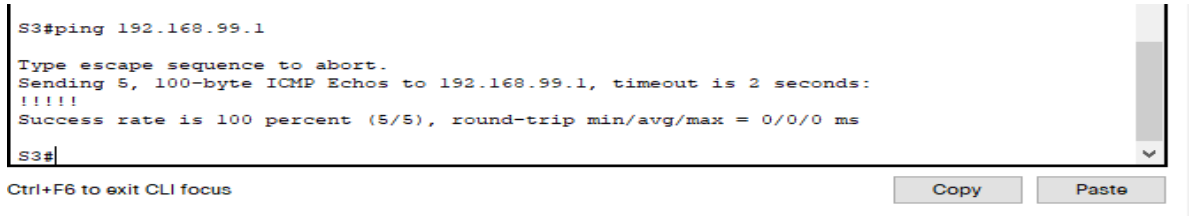
Fuente: Elaboración propia

Figura 21. Ping S1



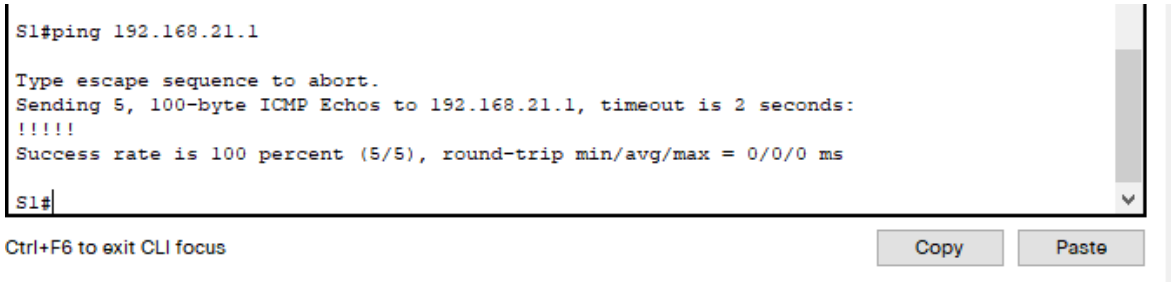
Fuente: Elaboración propia

Figura 22. Ping S3



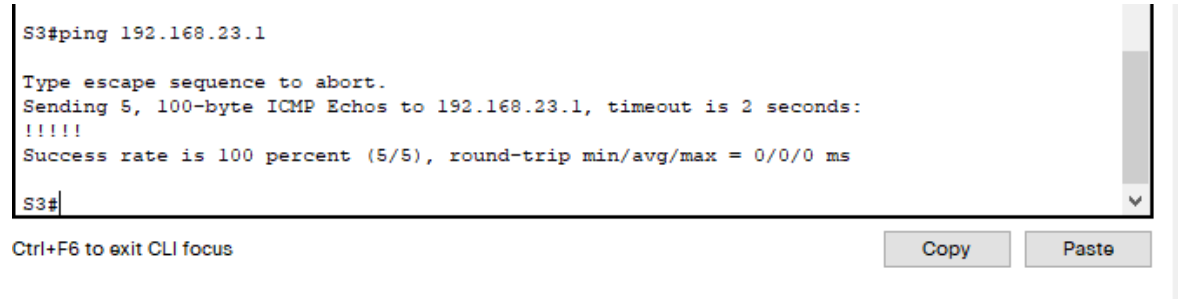
Fuente: Elaboración propia

Figura 23. Ping S1



Fuente: Elaboración propia

Figura 24. Ping S3



Fuente: Elaboración propia

Parte 4: Configurar el protocolo de Routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Tabla 20. Protocolo de Routing dinámico OSPF

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#enable

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 10
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.168.99.1 0.0.0.0 area 0
R1(config-router)#network 192.168.23.1 0.0.0.0 area 0
R1(config-router)#network 192.168.21.1 0.0.0.0 area 0
R1(config-router)#network 172.16.1.1 0.0.0.3 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)#exit
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 10
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#interface s0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#ipv6 ospf 10 area 0
R1(config-if)#
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 2: Configurar OSPF en el R2

Tabla 21. Configuración OSPF 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(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
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 10.10.10.10 0.0.0.0 area 0
```

```
R2(config-router)#
00:42:58: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done

R2(config-router)#passive-interface loopback 0
R2(config-router)#exit
R2(config)#
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#enable
R2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#interface g0/0
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#exit

R2(config)#interface s0/0/0
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#exit

R2(config)#interface s0/0/1
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#exit

R2(config)#ipv6 router ospf 10
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#exit

R2(config)#interface g0/0
R2(config-if)#ipv6 ospf 10 area 0
R2(config-if)#exit

R2(config)#interface s0/0/0
R2(config-if)#ipv6 ospf 10 area 0
R2(config-if)#exit
R2(config)#
00:49:08: %OSPFv3-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done


R2(config)#interface s0/0/1
R2(config-if)#ipv6 ospf 10 area 0
R2(config-if)#exit
R2(config)#exit
```

Paso 3: Configurar ospfv3 en el R2

Tabla 22. Configuración OSPKv3 en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 10
Anunciar redes IPv4 conectadas directamente	172.16.2.0 0.0.0.3 area 0 172.16.2.0 0.0.0.4 area 0 172.16.2.0 0.0.0.5 area 0 172.16.2.0 0.0.0.6 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.	network summarization is not in

Fuente: Elaboración propia

```
R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#network 172.16.2.0 0.0.0.4 area 0
OSPF: Invalid address/mask combination (discontiguous mask)
R3(config-router)#network 172.16.2.0 0.0.0.5 area 0
OSPF: Invalid address/mask combination (discontiguous mask)
R3(config-router)#network 172.16.2.0 0.0.0.6 area 0
OSPF: Invalid address/mask combination (discontiguous mask)
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#exit

R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router ospf 10
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#interface s0/0/1
R3(config-if)#ipv6 ospf 10 area 0
R3(config-if)#
```

01:13:04: %OSPFv3-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#interface loopback 7
R3(config-if)#ipv6 address FE80::3 link-local
01:13:21: %OSPFv3-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done

R3(config-if)#ipv6 ospf 10 area 0
R3(config-if)#exit
R3(config)#

Paso 4: Verificar la información de OSPF

Verifique que OSPF este funcionando como se espera. Introduzca el comando de Cli adecuado para obtener la siguiente información:
Tabla 22. Verificación de 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

Fuente: Elaboración propia

Comprobacion de configuracion ip protocold R1

R1#show ip protocols
R1#show ip protocols

Routing Protocol is "ospf 10"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
192.168.99.1 0.0.0.0 area 0

192.168.23.1 0.0.0.0 area 0
192.168.21.1 0.0.0.0 area 0
172.16.1.0 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/1.21
GigabitEthernet0/1.23
GigabitEthernet0/1.99
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:02:17
2.2.2.2 110 00:07:06
3.3.3.3 110 00:07:06
Distance: (default is 110)

Comprobacion de configuracion protocols R2

R2>enable
Password:
R2#show ip protocols

Routing Protocol is "ospf 10"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 2.2.2.2
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
172.16.2.0 0.0.0.3 area 0
10.10.10.10 0.0.0.0 area 0
Passive Interface(s):
Loopback0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:03:03
2.2.2.2 110 00:07:52
3.3.3.3 110 00:07:52
Distance: (default is 110)

Comprobación ip protocols R3

R3>enable
Password:
R3#show ip protocols

Routing Protocol is "ospf 10"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 3.3.3.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.16.2.0 0.0.0.3 area 0
Passive Interface(s):
Loopback4
Loopback5
Loopback6
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:03:58
2.2.2.2 110 00:08:46
3.3.3.3 110 00:08:46
Distance: (default is 110)

R1#show ip route ospf
10.0.0.0/32 is subnetted, 1 subnets
O 10.10.10.10 [110/65] via 172.16.1.2, 00:37:18, Serial0/0/0
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O 172.16.2.0 [110/128] via 172.16.1.2, 00:37:18, Serial0/0/0

Parte 5: Implementar DHCP y NAT para IPv4

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

Tabla 23. Configuración DHCP para R1 VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para	192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para	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
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

Fuente: Elaboración propia

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#
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)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

Tabla 24. Configuración la NAT estática y dinámica en el 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**
Habilitar el servicio del servidor HTTP	add service <name> <IP> <serviceType> <port> -cacheType <cacheType> - show service [<name>]
Configurar el servidor HTTP para utilizar la base de datos local para	username webuser privilege 15 secret cisco12345
Crear una NAT estática al servidor	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	Ip nat outside
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
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**
Definir la traducción de NAT dinámica	es el tipo de **NAT** que se utiliza con más frecuencia. Cambia la dirección IP de origen de una conexión saliente a la dirección IP

Fuente: Elaboración propia

R2#enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

Paso 3: Verificar el protocolo DHCP y la NAT estática

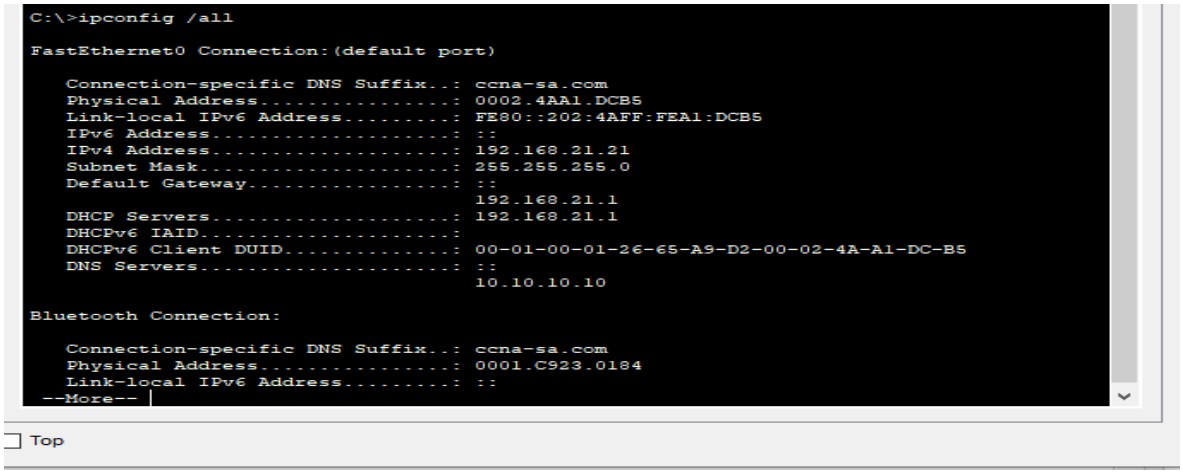
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 25. Verificación de protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del	Correcto ver figura 23
Verificar que la PC-C haya adquirido información de IP del	Correcto ver figura 23
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Correcto ver figura 23
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	Correcto ver figura 23

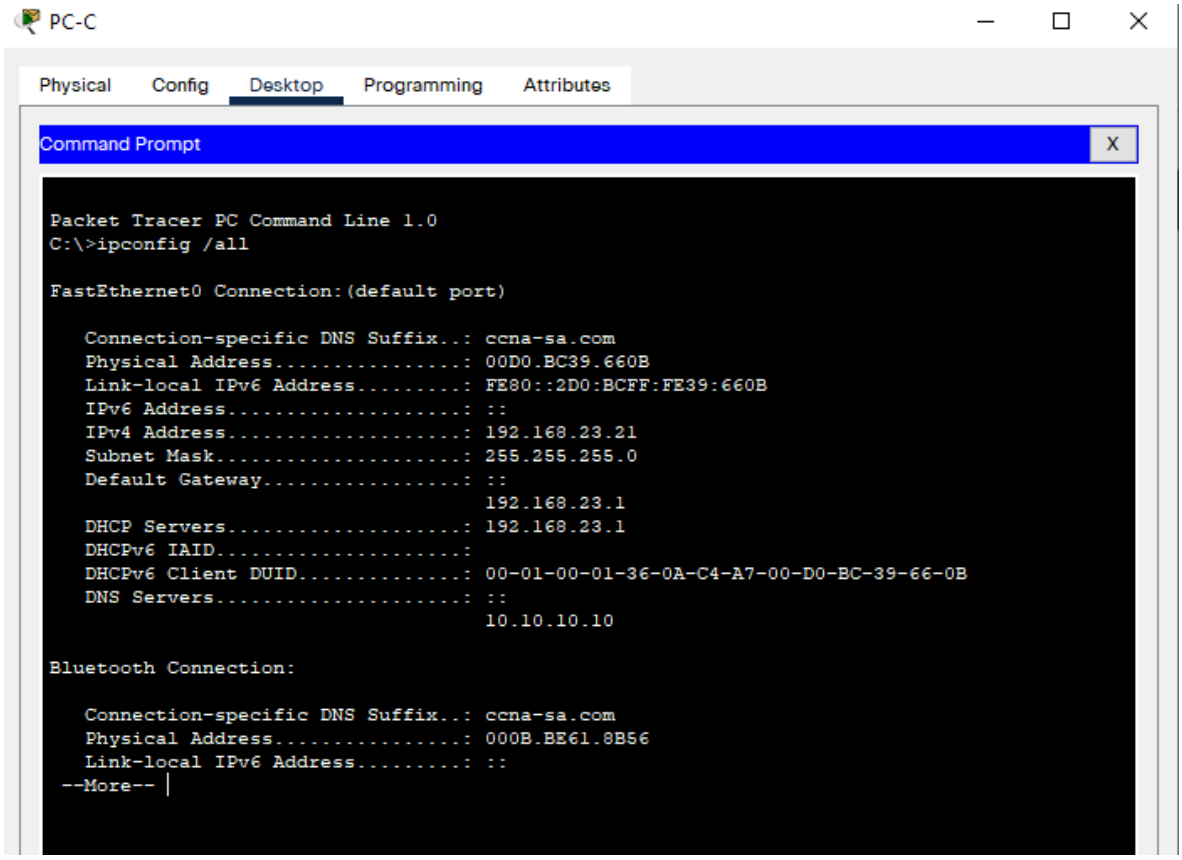
Fuente: Elaboración propia

Figura 23 ping PC-A



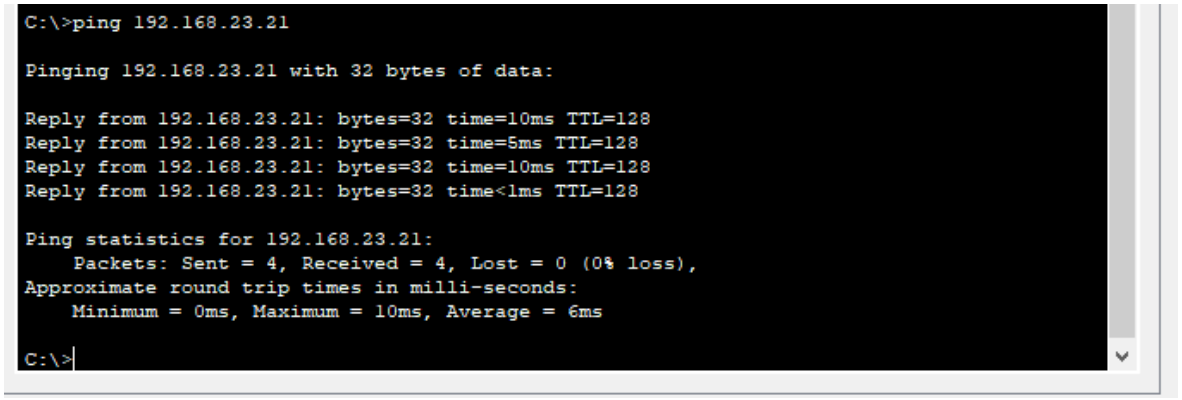
Fuente: Elaboración propia

Figura 24 ping PC-C



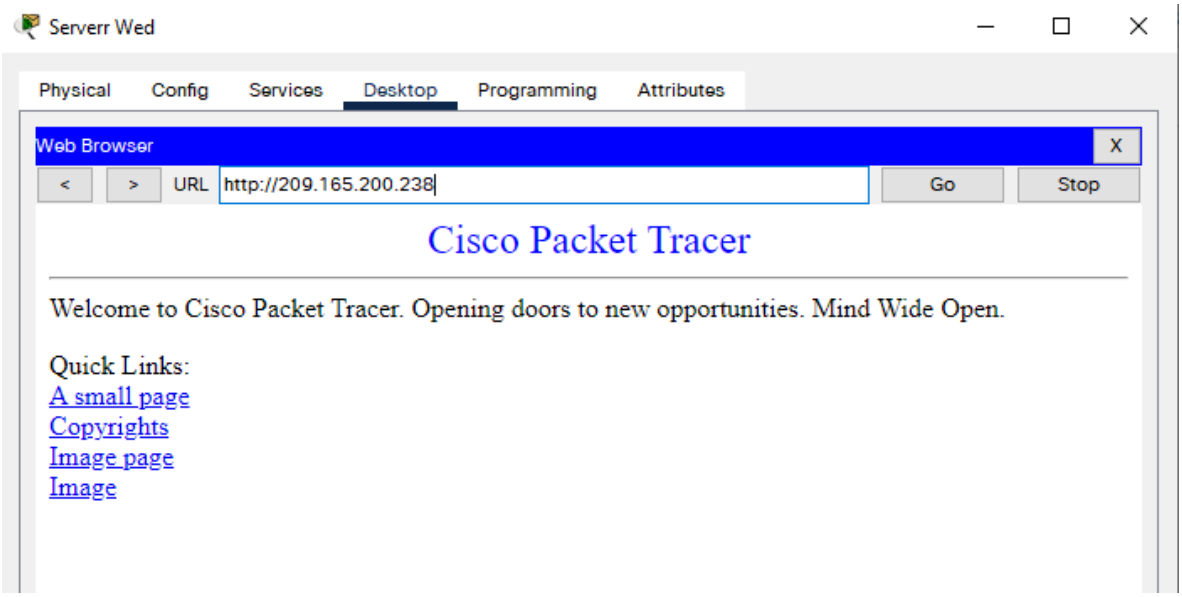
Fuente: Elaboración propia

Figura 25 ping PC-A a PC-C



Fuente: Elaboración propia

Figura 26. Acceso al sitio desde el servidor



Fuente: Elaboración propia

Parte 6: Configurar NTP

Tabla 26. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

Fuente: Elaboración propia

```
R2>enable
Password:
R2#clock set 9:00:00 05 march 2016
R2#
R2#ntp master 5
^
% Invalid input detected at '^' marker.
R2#configure t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5
R2(config)#
```

```
R1>enable
Password:
R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 172.16.1.2
R1(config)#
R1(config)#nyp update-calendar
^
% Invalid input detected at '^' marker.
R1(config)#ntp update-calendar
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ntp associations

address ref clock st when poll reach delay offset disp
~172.16.1.2 127.127.1.1 5 4 16 37 9.00 726216275142.00 0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
R1#
```

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 27. Restricción de acceso a líneas VTY en R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	Line vty 015
Permitir acceso por Telnet a las líneas de VTY	Acces-class ADMIN MGT
Verificar que la ACL funcione como se espera	Correcto

Fuente: Elaboración propia

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#end

Figura 27. Conexión del Telnet con R2

```
Password:
R2#enable
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente: Elaboración propia

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#

Figura 28. Aplicar la ACL con nombres a las líneas VTY

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#
```

Fuente: Elaboración propia

Figura 29. Permitir Acceso por Telnet a las lieas VTY

```
R2(config-line)#
R2(config-line)#transport input telnet
R2(config-line)#
```

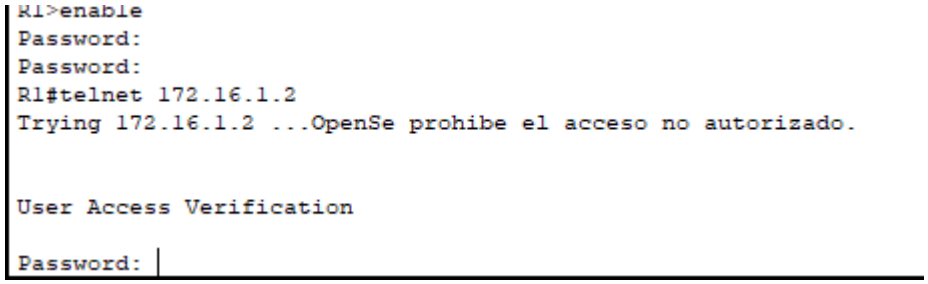
Fuente: Elaboración propia

R2(config-line)#transport input telnet

R2(config-line)#

R1>enable
Password:
R1#enable
R1#tel
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado.

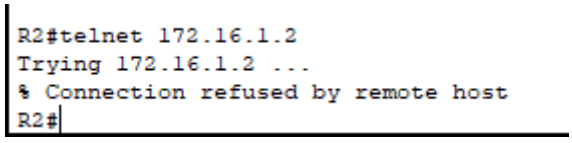
Figura 30. Verificar que el ACL funcione



Fuente: Elaboración propia

R2#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R2#

Figura 31. Verificar que el ACL Funcione



Fuente: Elaboración propia

Paso 2: introducir el comando de clic que se necesita para mostrar los siguientes

Tabla 27. Comandos para mostrar información

Descripción del comando	Entrada del estudiante (comando)

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se	Show access list
Restablecer los contadores de una lista de acceso	Clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se	Show ip interface
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translations **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
¿Qué comando se utiliza para eliminar las traducciones de NAT	Clear ip nat translation

Fuente: Elaboración propia

R2#show interface s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 172.16.1.2/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 471 bits/sec, 2 packets/sec
5 minute output rate 428 bits/sec, 2 packets/sec
2818 packets input, 206559 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
2554 packets output, 193292 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets

0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.229 10.10.10.10 --- ---

R2#

CONCLUSIONES

Se utilizó el software de Cisco Packet Tracer, y se utilizaron sus herramientas gracias a esta tecnología se puede dar soluciones a problemas de redes en la vida laboral, donde se puede determinar cuántas subredes son utilizables en una empresa u organización dependiendo la necesidad.

Se documento el desarrollo de dos escenarios paso a paso acompañado con su respectiva evidencia del proceso realizado en cada uno de los dispositivos de la red, realizando pruebas de conectividad donde el resultado fue satisfactorio.

Con el desarrollo del segundo escenario se aplicaron comandos ya utilizados en el primer escenario, en este escenario se hizo configuración en el servidor y configuraciones para acceso a este.

Como resultado final se aplicó todo el conocimiento adquirido durante el diplomado del curso logrando dar solución a los dos escenarios planteados como trabajo final.

BIBLIOGRAFÍA

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. “DHCP Principios de Enrutamiento y Conmutación”. {En línea}. (2019). {27 Noviembre de 2020}. Disponible en:https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. “NAT para IPv4. Principios de Enrutamiento y Conmutación”. {En línea}. (2019). {27 Noviembre de 2020}.Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9