

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

JAIME ANDRÉS VERU LISCANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA

PITALITO

2021

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

JAIME ANDRÉS VERU LISCANO

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO
DE INGENIERÍA ELECTRÓNICA

TUTORA

MG. MARIA ALEJANDRA LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA ELECTRÓNICA

PITALITO

2021

NOTA DE ACEPTACIÓN:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

PITALITO, (noviembre 28, 2021)

DEDICATORIA

A Dios primeramente y a mi familia que desde el inicio de mis estudios han sido un baluarte incondicional en los momentos buenos y complicados en mi sueño y objetivo de ser ingeniero en sistemas.

AGRADECIMIENTO

Agradecimiento en especial a mi familia que me ha brindado todo el apoyo incondicional en este proceso de formación profesional como ingeniero electrónico. De igual modo, agradezco a todos mis compañeros y tutores por el compromiso y acompañamiento oportuno.

Finalmente, mi agradecimiento a la Universidad Nacional Abierta a Distancia (UNAD) y a su extenso equipo de trabajo, sin este método de formación, muchas personas no podrían optar por una educación superior. Agradezco sinceramente todo el apoyo y espacio de formación, espero seguir perteneciendo a esta gran familia y ser parte de su futuro.

CONTENIDO

LISTA DE TABLAS	7
LISTA DE FIGURAS	8
GLOSARIO	9
RESUMEN	11
ABSTRACT	11
INTRODUCCIÓN	12
OBJETIVOS	13
ESCENARIO 1	14
PASO 1: CONFIGURAR LOS AJUSTES BÁSICOS	15
PASO 2. CONFIGURAR LOS EQUIPOS	19
ESCENARIO 2	22
Topología	22
Parte 1: Inicializar dispositivos	23
Parte 2: Configurar los parámetros básicos de los dispositivos	30
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN	47
Parte 4: Configurar el protocolo de routing dinámico OSPF	59
Parte 5: Implementar DHCP y NAT para IPv4	62
Parte 6: Configurar NTP	69
Parte 7: Configurar y verificar las listas de control de acceso (ACL)	70
CONCLUSIONES	82
BIBLIOGRAFÍA	83

LISTA DE TABLAS

Tabla 1 ITEM REQUERIMIENTO	14
Tabla 2 PC-A NETWORK CONFIGURATION	19
Tabla 3 CONFIGURACIÓN DE RED DE PC-B	20
Tabla 4 CONFIGURACION DEL SERVIDOR	31
Tabla 5 IPV4 SUBNET	31
Tabla 6 PV6 SUBNET	32
Tabla 7 VERIFICAR LA CONECTIVIDAD DE LA RED	45
Tabla 8 VERIFICAR LA CONECTIVIDAD DE LOS DISPOSITIVOS	57

LISTA DE FIGURAS

Figura 1 TOPOLOGÍA DE RED ESCENARIO 1	14
Figura 2 FASTETHERNET CONNECTION PC-A	20
Figura 3 FASTETHERNET CONNECTION PC-B	21
Figura 4 TOPOLOGÍA DE RED ESCENARIO 2	22
Figura 5 CONFIGURACIÓN IP DEL SERVIDOR	32
Figura 6 PRUEBA DE PING DESDE R1 A R2	46
Figura 7 PRUEBA DE PING DESDE SERVIDOR DE INTERNET A GATEWAY PREDETERMINADO	46
Figura 8 PRUEBA DE PING DESDE S1 A R1, DIRECCIÓN VLAN 99	58
Figura 9 PRUEBA DE PING DESDE S3 A R1, DIRECCIÓN VLAN 99.	58
Figura 10 PRUEBA DE PING DESDE S1 A R1, DIRECCIÓN VLAN 21	58
Figura 11 PRUEBA DE PING DESDE S3 A R1, DIRECCIÓN VLAN 23.	59
Figura 12 INFORMACIÓN DE IP DEL SERVIDOR DE DHCP EN EL PC-A.	66
Figura 13 INFORMACIÓN DE IP DEL SERVIDOR DE DHCP EN EL PC-C	67
Figura 14 VERIFICACIÓN DE PING PC-A A LA PC-C	68
Figura 15 ACCESO SERVIDOR WEB DESDE EL SERVIDOR DE INTERNET	69
Figura 16 PRUEBA DE TELNET DE R1 A R2.	72
Figura 17 VER LAS TRADUCCIONES NAT EN EL R3	78
Figura 18 PRUEBA DE PING AL SERVIDOR DE INTERNET DESDE LA PC-A.	79
Figura 19 PRUEBA DE PING AL SERVIDOR DE INTERNET DESDE LA PC-C.	79
Figura 20 PRUEBA DE ACCESO AL SERVIDOR DE WEB DESDE PC-A	80
Figura 21 ELIMINAR LAS TRADUCCIONES DE NAT DINÁMICAS.	81
Figura 22 TOPOLOGÍA DE RED ESCENARIO 2 - CISCO PACKET TRACER.	81

GLOSARIO

DNS: Sistema de nombres de dominio". Este sistema es básicamente la agenda telefónica de la Web que organiza e identifica dominios.

Dirección IP: Una dirección en la red asignada a una in-terfaz de un nodo de la red y usada para identificar (localizar) en forma única el nodo dentro de la Internet. Dos versiones estan actualmente implementadas: IPv4 e IPv6.

Dirección IPv4: Una dirección IP con base en el IPv4. Esas direcciones consisten en 32 bits (0 al 31) particionados en cuatro grupos de ocho bits cada uno (llamados octetos) y organizados en cinco clases (A a la E) con base en los valores de bits 0 al 3.

Dirección IPv6: Una dirección IP con base en IPv6. Una dirección IPv6 consiste en 128 bits y tiene 4000 millones X 4000 millones de veces el tamaño del espacio de dirección IPv4 (2¹²⁸ vs. 2³²). A diferencia de las direcciones IPv4, las direcciones IPv6 usan dos puntos como delimitador (en vez de una notación "punto"), y ellas son escritas como ocho enteros de 16 bits expresados en forma hexadecimal.

Dominio: es el nombre exclusivo y único que se le da a un sitio web para que cualquier internauta pueda visitarlo e identificarlo.

Exec privilegiado: El modo EXEC privilegiado permite el acceso a todos los comandos del enrutador. Este modo se puede configurar para requerir que el usuario proporcione una contraseña antes de otorgar acceso. Para mayor protección, también se puede configurar para solicitar una identificación de usuario. Esto solo permite que los usuarios autorizados inicien sesión en el enrutador. Los comandos de configuración y administración requieren que el administrador de la red esté en el nivel EXEC privilegiado.

LAN (del inglés Local Area Network, Red de Área Local): Una red local es la interconexión de varios computadores y periféricos. Su extensión está limitada

físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación más extendida es la interconexión de computadores personales y estaciones de trabajo en oficinas, fábricas, etc;

SSH: SSH es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada

VTY: Se trata de un conjunto de puertos virtuales utilizados para la conexión vía telnet, SSH, http o https al dispositivo para realizar administración in band. La mayoría de los dispositivos tienen al menos 5 puertos virtuales identificados como vty 0 a 4. Sin embargo, en la medida en que resulte necesario, se pueden general más puertos virtuales hasta completar un total de 21 líneas vty.

RESUMEN

En trabajo se realiza con el propósito de ejecutar de una forma práctica los conocimientos adquiridos a lo largo del Diplomado De Profundización CISCO (Diseño e Implementación de soluciones integradas LAN/WAN), aportando al estudiante las habilidades necesarias en el manejo de redes, enfrentándolo a dos escenarios, en donde para cada uno de ellos debe construir su topología.

En el escenario 1 se desarrolla los conocimientos en cuanto a la configuración de los equipos descritos en una topología y en una tabla la cual contiene el direccionamiento de cada uno de ellos.

En cuanto al escenario 2, se evalúa las competencias en la implementación del enrutamiento por OSPFv2, habilitar y deshabilitar DNS, al igual que NAT y VLAN

Palabras clave: Dirección IP, Dirección IPv4, Dirección IPv6, LAN, Network

ABSTRACT

This work is carried out with the purpose of executing in a practical way the knowledge acquired throughout the CISCO In-depth Course (Design and Implementation of integrated LAN/WAN solutions), providing the student with the necessary skills in the management of networks, facing two scenarios, where for each one of them he/she must build his/her topology.

In scenario 1, knowledge is developed regarding the configuration of the equipment described in a topology and in a table containing the addressing of each one of them.

As for scenario 2, the competences in the implementation of OSPFv2 routing, enabling and disabling DNS, as well as NAT and VLAN are evaluated.

Keywords: Dirección IP, Dirección IPv4, Dirección IPv6, LAN, Network

INTRODUCCION

La red ahora juega un papel importante al facilitar la comunicación, la colaboración y la interacción de nuevas formas en todo el mundo, proporcionando una plataforma para brindar servicios que apoyan la conectividad. A medida que la red global continúa expandiéndose, también deben hacerlo las plataformas que la conectan y la respaldan.

Su finalidad es buscar que como futuro profesional en la rama se obtengan conocimientos y experiencias aplicando soluciones de estudios de caso bajo el uso de tecnología Cisco usando el software de simulación Cisco Packet Tracer. Lo principal es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de networking.

A través de esta prueba de habilidad, se discutirán métodos importantes relacionados con la planificación e implementación de varias redes. Ejecute el laboratorio a través del software Packet Tracer. Aquí aprenderás la configuración básica y de seguridad en switches y routers, verás los tipos de conexión y los tipos de cables requeridos, veremos el funcionamiento de las herramientas de protocolo, las herramientas que permiten y niegan el acceso de los usuarios, y experimentarás Conexión remota con enrutadores e interruptores.

OBJETIVOS

OBJETIVO GENERAL

Dominar conceptos y tecnologías de redes básicas, desarrollar planes e implementar las habilidades necesarias para redes pequeñas con diversas aplicaciones.

Objetivos Específicos

- Desarrollar la actividad propuesta con el uso de la herramienta Cisco Packet Tracer.
- Configurar el direccionamiento IP para cada dispositivo en el esquema de acuerdo con la topología de la red.
- Verificar la conectividad de los dispositivos de red.

ESCENARIO 1

Figura 1 Topología de red escenario 1



Fuente: Prueba de habilidades CCNA 2021, Cisco Academy.

Tabla 1 Item Requerimiento

Item Requerimiento	Item Requerimiento
Dirección de Red	192.168.19.0
Requerimiento de host Subred LAN1	192.168.19.0 - 192.168.19.127 /25
Requerimiento de host Subred LAN2	192.168.19.128 - 192.168.19.191 /26
R1 G0/0/1	192.168.19.1 /25
R1 G0/0/0	192.168.19.129 /26
S1 SVI	192.168.19.2
PC-A	192.168.19.126
PC-B	192.168.19.190

Fuente: Elaboración propia

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

- Desactivar la búsqueda DNS
Router(config)#no ip domain lookup
- Nombre del router R1
Router(config)#hostname R1
- Nombre de dominio ccna-lab.com
R1(config)#ip domain name ccna-lab.com
- Contraseña cifrada para el modo EXEC privilegiado ciscoenpass
R1(config)#enable secret ciscoenpass
- Contraseña de acceso a la consola ciscoconpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
- Establecer la longitud mínima para las contraseñas 10 caracteres
R1(config)#security passwords min-length 10
- Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass
R1(config)#username admin secret admin1pass

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

```
R1(config)#line vty 0 15
```

```
R1(config-line)#login local
```

- Configurar VTY solo aceptando SSH

```
R1(config-line)#transport input ssh
```

- Cifrar las contraseñas de texto no cifrado

```
R1(config)#service password-encryption
```

- Configure un MOTD Banner

```
R1(config)#banner motd #Unauthorized Access is Prohibited#
```

- Configurar interfaz G0/0/0 Establezca la descripción Establece la dirección IPv4.

```
interface g0/0/0
```

```
description PC-B
```

```
ip address 192.168.19.129 255.255.255.192
```

```
no shutdown
```

```
exit
```

- Configurar interfaz G0/0/1 Establezca la descripción Establece la dirección IPv4.

```
interface g0/0/1
```

```
description PC-B
```

```
ip address 192.168.19.1 255.255.255.128
```

```
no shutdown
```

```
exit
```

- Generar una clave de cifrado RSA Módulo de 1024 bits

```
crypto key generate rsa 1024
```

Las tareas de configuración de S1 incluyen lo siguiente:

- Desactivar la búsqueda DNS

```
Router(config)#no ip domain lookup
```

- Nombre del switch S1

```
Router(config)#hostname R1
```

- Nombre de dominio ccna-lab.com

```
S1(config)#ip domain name ccna-lab.com
```

- Contraseña cifrada para el modo EXEC privilegiado ciscoenpass

```
S1(config)#enable secret ciscoenpass
```

- Contraseña de acceso a la consola ciscoconpass
 S1(config)#line console 0
 S1(config-line)#password ciscoconpass
 S1(config-line)#login
- Establecer la longitud mínima para las contraseñas 10 caracteres
 S1(config)#security passwords min-length 10
- Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass
 S1(config)#username admin secret admin1pass
- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local
 S1(config)#line vty 0 15
 S1(config-line)#login local
- Configurar VTY solo aceptando SSH
 S1(config-line)#transport input ssh
- Cifrar las contraseñas de texto no cifrado
 S1(config)#service password-encryption

- Configure un MOTD Banner

S1(config)#banner motd #Unauthorized Access is Prohibited#

- Generar una clave de cifrado RSA Módulo de 1024 bits

crypto key generate rsa 1024

- Configurar la interfaz de administración (SVI)

ip address 192.168.19.2 255.255.255.128

description Management Interface

no shutdown

- Configuración del gateway predeterminado.

S1(config)#ip default-gateway 192.168.19.3

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 2 PC-A Network Configuration

PC-A Network Configuration	
Descripción	PC-A
Dirección IP	192.168.19.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.19.1

Fuente: Elaboración propia

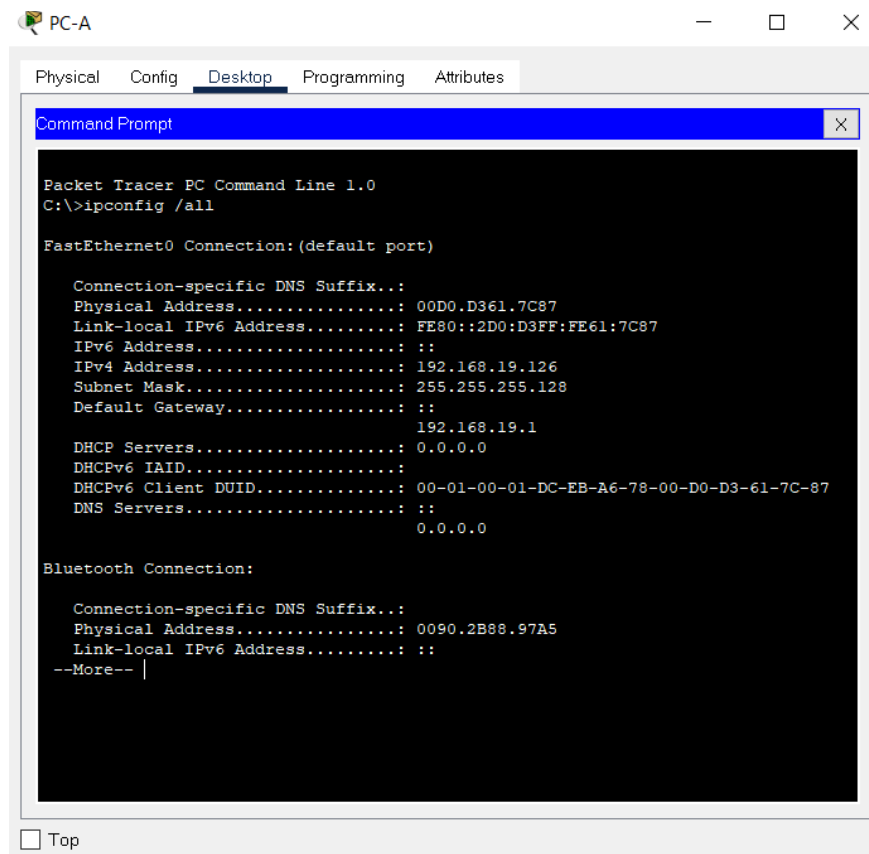
Tabla 3 Configuración de red de PC-B

Configuración de red de PC-B	
Descripción	<i>PC-B</i>
Dirección IP	192.168.19.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.19.129

Fuente: Elaboración propia

Ipconfig PC-A

Figura 2 Fastethernet connection PC-A



Fuente: Elaboración propia

Ipconfig PC-B

Figura 3 Fastethernet connection PC-B

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix.:
Physical Address.: 0090.21DE.5699
Link-local IPv6 Address.: FE80::290:21FF:FEDE:5699
IPv6 Address.: ::
IPv4 Address.: 192.168.19.190
Subnet Mask.: 255.255.255.192
Default Gateway.: ::
DHCP Servers.: 192.168.19.129
DHCPv6 IAID.: 0.0.0.0
DHCPv6 Client DUID.: 00-01-00-01-74-B7-67-7E-00-90-21-DE-56-99
DNS Servers.: ::
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix.:
Physical Address.: 0090.2133.0EEC
Link-local IPv6 Address.: ::
--More-- |
```

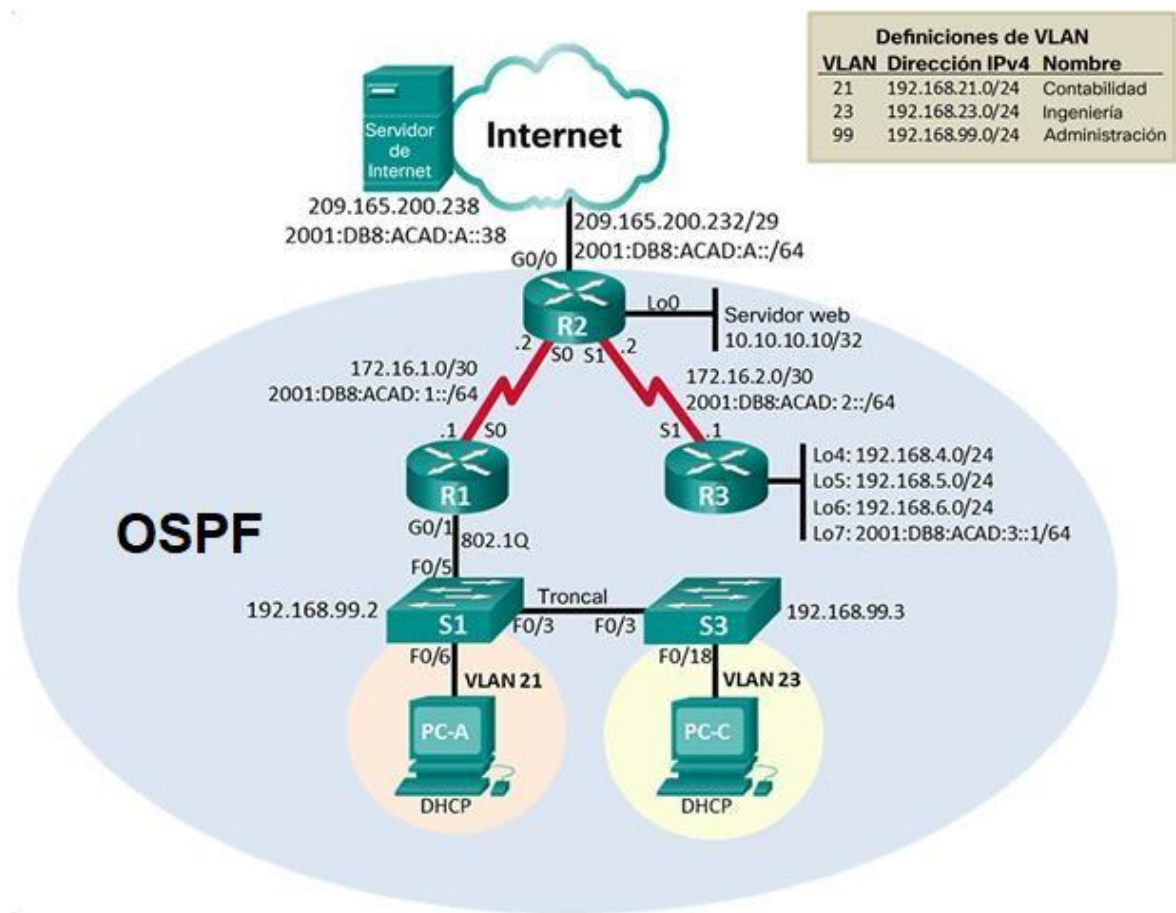
Fuente: Elaboración propia

ESCENARIO 2

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

Topología

Figura 4 Topología de red escenario 2



Fuente: Prueba de habilidades CCNA 2021, Cisco Academy.

Parte 1: Inicializar dispositivos

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

- Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
- Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.
- Eliminar el archivo startup-config de todos los routers

```
Router>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#
```

```
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#
```

```
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

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 0 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 ---

Would you like to enter the initial configuration dialog? [yes/no]: no

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

```
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 vlan.dat

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]

%Error deleting flash:/vlan.dat (No such file or directory)

Switch#

Volver a cargar ambos switches

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: 0001.C997.6CC1

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: 4414921 flashfs[0]:

Bytes available: 59601463 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:/c2960-lanbase-mz.122-25.FX.bin"...

#####

[OK] 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-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Image text-base: 0x80008098, data-base: 0x814129C4

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address : 0001.C997.6CC1

Motherboard assembly number : 73-9832-06

Power supply part number : 341-0097-02

Motherboard serial number :

FOC103248MJ Power supply serial

number : DCA102133JA Model revision

number : B0

Motherboard revision number : C0

Model number : WS-C2960-24TT

System serial number : FOC1033Z1EY

Top Assembly Part Number : 800-26671-02

Top Assembly Revision Number : B0

Version ID : V02

CLEI Code Number : COM3K00BRA

Hardware Board Revision Number : 0x01

Switch Ports Model SW Version SW Image

* 1 26 WS-C2960-24TT 12.2 C2960-LANBASE-M

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version

12.2(25)FX, RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2005 by Cisco Systems, Inc.

Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!

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

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

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

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

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

```
Switch>enable
```

```
Switch#show flash
```

```
Directory of flash:/
```

```
1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin
```

```
64016384 bytes total (59601463 bytes  
free) Switch#
```

```
Switch>enable
```

```
Switch#show flash
```

```
Directory of flash:/
```

```
1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin
```

```
64016384 bytes total (59601463 bytes  
free) Switch#
```

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1. Configurar la computadora de Internet

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

Tabla 4 configuración del servidor

Elemento o tarea de configuración	Especificación
Dirección Ipv4	209.165.200.238
Máscaras de subred para Ipv4:	255.255.255.248
Gateway predeterminado:	209.165.200.233
Dirección Ipv6/subred:	201:db8:acad:a::38/64
Gateway prederminado Ipv6:	201:db8:acad:a::1

Fuente Elaboración propia

Tabla 5 IpV4 Subnet

Id address:	209.165.200.232
Network Address:	209.165.200.232
Usable Host Ip Range:	209.165.200.233-209.165.200.238
Broadcast Address:	209.165.200.239
Total Number of Hosts:	8
Number of Usable:	6
Subnet mask:	255.255.255.248
Wildcard Mask:	0.0.0.7
Binary subnet Mask:	11111111.11111111.11111111.111110
Ip Type:	PUBLICIP-CLASS C

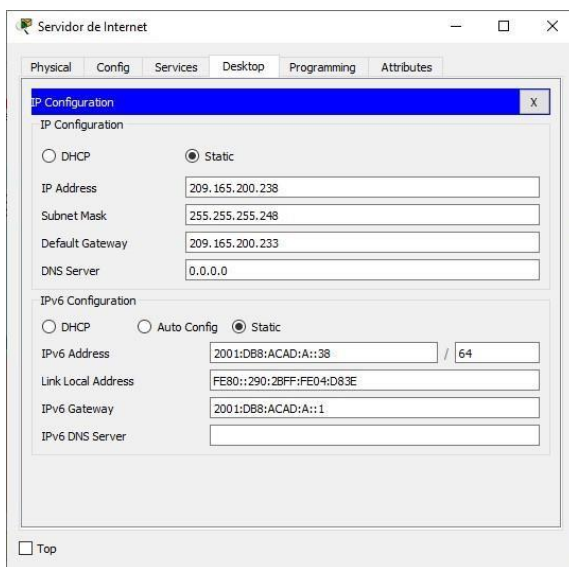
Fuente: Elaboración propia

Tabla 6 pV6 Subnet

Ip Adres:	2001.db8:a cad:a::38/64
Full Ip Address:	2001:0db8:acad:000a:0000:0000:0000:0038
Total Ip Addresses:	18.446.744.073.709.551.616
Network:	2001:0db8:acad:000a:: /64 2001:0db8:acad:000a:0000:0000:0000:0000/
Ip Range	2001:db8:acad:a::1 2001:0db8:acad:000a:0000:0000:0000:0001 2001:db8:acad:a:ffff:ffff:ffff:ffff 2001:0db8:acad:000a:ffff:ffff:ffff:ffff
Ip Type:	GLOBAL UNICAST

Fuente: Elaboración propia

Figura 5 Configuración IP del servidor



Fuente Elaboración propia

Paso 2. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

- Desactivar la búsqueda DNS
- Nombre del router R1
- Contraseña de exec privilegiado cifrada class
- Contraseña de acceso a la consola cisco
- Contraseña de acceso Telnet cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD
- Se prohíbe 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
- Rutas predeterminadas
- Configurar una ruta IPv4 predeterminada de S0/0/0
- Configurar una ruta IPv6 predeterminada de S0/0/0

```
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 prohíbe el acceso no  
autorizado.% R1(config)#int s0/0/0
```

```
R1(config-if)#description Connection to R2
```

```
R1(config-if)#ip address 172.16.1.1 255.255.255.252
```

```
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
```

```
R1(config-if)#clock rate 128000
```

```
R1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
```

```
R1(config-if)#exit
```

```
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)#
```

Nota: Todavía no configure G0/1.

Paso 3. Configurar R2

La configuración del R2 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del router R2
- Contraseña de exec privilegiado cifrada class
- Contraseña de acceso a la consola cisco
- Contraseña de acceso Telnet cisco
- Cifrar las contraseñas de texto no cifrado
- Habilitar el servidor HTTP
- Mensaje MOTD Se prohíbe el acceso no autorizado.

```
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)#banner 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

```
R2(config)#int s0/0/0
```

```
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 Serial0/0/0, changed state to up
```

```
R2(config-if)#
```

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

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 address 172.16.2.2 255.255.255.252
```

```
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
```

```
R2(config-if)#clock rate 128000
```

```
R2(config-if)#no shutdown
```

```
%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)#int g0/0
R2(config-if)#description Connection to Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64
R2(config-if)#no shutdown
```

```
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 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)#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
```

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

Paso 4. Configurar R3

- La configuración del R3 incluye las siguientes tareas:
- Desactivar la búsqueda DNS
- Nombre del router R3
- Contraseña de exec privilegiado cifrada class
- Contraseña de acceso a la consola cisco
- Contraseña de acceso Telnet cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD Se prohíbe el acceso no autorizado.

```
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 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

```
R3(config)#int s0/0/1
R3(config-if)#description Connection to R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:db8:acad:2::1/64
R3(config-if)#no shutdown
```

```
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
```

```
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
```

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 address 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 address 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 address 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-if)#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 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
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 performance
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#
```

Paso 5. Configurar S1

La configuración del S1 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del switch S1
- Contraseña de exec privilegiado cifrada class

- Contraseña de acceso a la consola cisco
- Contraseña de acceso Telnet cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD Se prohíbe el acceso no autorizado.

```

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
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
S1(config-line)#service password-encryption
S1(config)#banner motd %Se Se prohíbe el acceso no autorizado.%
S1(config)#

```

Paso 6. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del switch S1
- Contraseña de exec privilegiado cifrada class
- Contraseña de acceso a la consola cisco
- Contraseña de acceso Telnet cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD Se prohíbe el acceso no autorizado.

```

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
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
S3(config-line)#service password-encryption
S3(config)#banner motd %Se Se prohíbe el acceso no autorizado.%
S3(config)#

```

Paso 7. Verificar la conectividad de la red

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

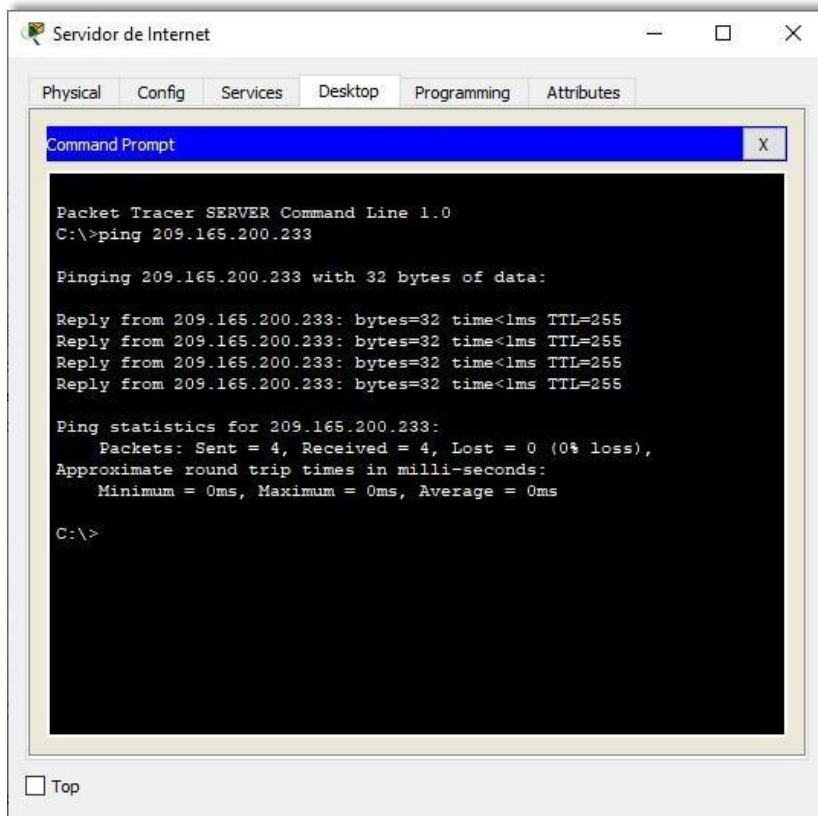
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla.

Tabla 7 Verificar la conectividad de la red

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
Servidor de internet	Gateway predetermi	209.165.200.233	Success

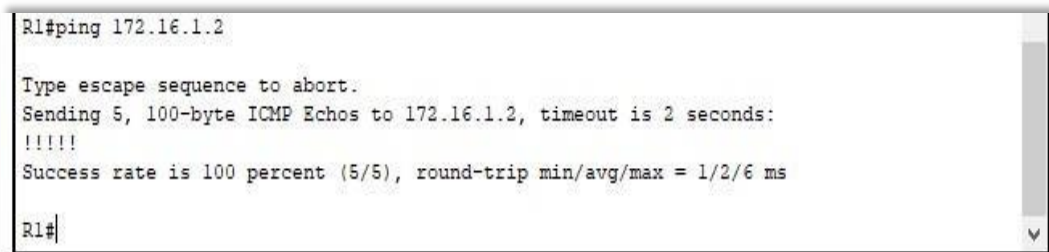
Fuente: Elaboración propia

Figura 6 Prueba de Ping desde R1 a R2



Fuente: Elaboración propia

Figura 7 Prueba de ping desde Servidor 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 1

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

```
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 Administracion
S1(config-vlan)#exit
S1(config)#interface vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state
to up

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
```

S1(config-if-range)#shutdown

%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

Paso 2. Configurar el 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.

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
- Apagar todos los puertos sin usar

```
S3(config-vlan)#name Contabilidad
```

```
S3(config-vlan)#vlan 23
```

```
S3(config-vlan)#name Ingenieria
```

```
S3(config-vlan)#vlan 99
```

```
S3(config-vlan)#name Administracion
```

```
S3(config-vlan)#exit
```

```
S3(config)#int vlan 99
```

```
S3(config-if)#
```

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

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

```
S3(config-if)#ip address 192.168.99.3 255.255.255.0
```

```
S3(config-if)#no shutdown
```

```
S3(config-if)#exit
```

```
S3(config)#ip default-gateway 192.168.99.1
```

```
S3(config)#int f0/3
```

```
S3(config-if)#switchport mode trunk
```

```
S3(config-if)#switchport trunk native vlan 1
```

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

```
S3(config-if-range)#switchport mode Access
```

```
S3(config-if-range)#int f0/18
```

```
S3(config-if)#switchport access vlan 23
```

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

```
S3(config-if-range)#shutdown
```

%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

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

```
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
S3(config-if-range)#
```

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(config)#int g0/1.21
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
```

Configurar la subinterfaz 802.1Q .23 en G0/1

- 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 address 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
- Activar la interfaz G0/1

```
R1(config-subif)#int g0/1.99
```

```
R1(config-subif)#description LAN de 45suario45o n45ón
```

```
R1(config-subif)#encapsulation dot1q 99
```

```
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
```

```
R1(config-subif)#int g0/1
```

```
R1(config-if)#no shutdown
```

```
R1(config-if)#
```

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

```
%LINEPROTO-5-UPDOWN: Line 45suario45o n Interface  
GigabitEthernet0/1, changed state to up
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line 45suario45o n Interface  
GigabitEthernet0/1.21, changed state to up
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line 45suario45o n Interface  
GigabitEthernet0/1.23, changed state to up
```

%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line 45suario45o n Interface
GigabitEthernet0/1.99, changed state to up

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 8 Verificar la conectividad de los dispositivos

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	Success

Fuente: Elaboración propia

Figura 8 Prueba de ping desde S1 a R1, dirección VLAN 99

```
S1#ping 192.168.99.1

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

S1#
```

Fuente: Elaboración propia

Figura 9 Prueba de ping desde S3 a R1, dirección VLAN 99.

```
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms

S3#
```

Fuente: Elaboración propia

Figura 10 Prueba de ping desde S1 a R1, dirección VLAN 21

```
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S1#
```

Fuente: Elaboración propia

Figura 11 Prueba de ping desde S3 a R1, dirección VLAN 23.

```
S3#ping 192.168.23.1

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

S3#
```

Fuente: Elaboración propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1. Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

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

```
R1(config)#router ospf 1
```

```
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)#
```

Paso 2. Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

- Configurar OSPF área 0
- Anunciar las redes conectadas directamente
- Establecer la interfaz LAN (loopback) como pasiva
- Desactive la sumarización automática.

```
R2(config)#router ospf 1
```

```
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
```

```
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
```

```
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
```

```
R2(config-router)#passive-interface loopback 0
```

```
R2(config-router)#
```

Paso 3. Configurar OSPFv3 en el R3

La configuración del R2 incluye las siguientes tareas:

- Configurar OSPF área 0

- Anunciar las redes conectadas directamente
- Establecer la interfaz LAN (loopback) como pasiva
- Desactive la sumarización automática.

```
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
```

Paso 4. Verificar la información de OSPF

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

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

```
Sh ip protocols
```

¿Qué comando muestra solo las rutas OSPF?

```
Sh ip route
```

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

```
Sh run begin | ospf
```

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

- Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas
- Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas

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 excluded-address 192.168.21.1 192.168.21.20
```

```
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
```

```
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
```

```
R1(config)#ip dhcp pool ENGR
```

Crear un pool de DHCP para la VLAN 23

- Nombre: ENGR
- Servidor DNS: 10.10.10.10

- Nombre de dominio: ccna-sa.com
- Establecer el gateway predeterminado

```
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
```

```
R1(config)#
```

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

```
R2(config)#username webuser privilege 15 secret cisco12345
```

```
R2(config)#ip http server
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
R2(config)#ip http authentication local
```

% Invalid input detected at '^' marker.

```
R2(config)#ip http secure-server
```

^

% Invalid input detected at '^' marker.

Crear una NAT estática al servidor web.

- Dirección global interna: **209.165.200.229**
- Asignar la interfaz interna y externa para la NAT estática
- 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

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
```

```
R2(config)#intg0/0
```

```
R2(config-if)#ip natoutside
```

```
R2(config-if)#ints0/0/0
```

```
R2(config-if)#ipnat inside
```

```
R2(config-if)#ints0/0/1
```

```
R2(config-if)#ipnat inside
```

```
R2(configif)#exit
```

```
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
```

```
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236
netmask
255.255.255.2
8
R2(config)#ip nat inside source list 1 pool
INTERNET
R2(config
#
```

Nota: Los siguientes comandos no son compatibles con Packet Tracer.

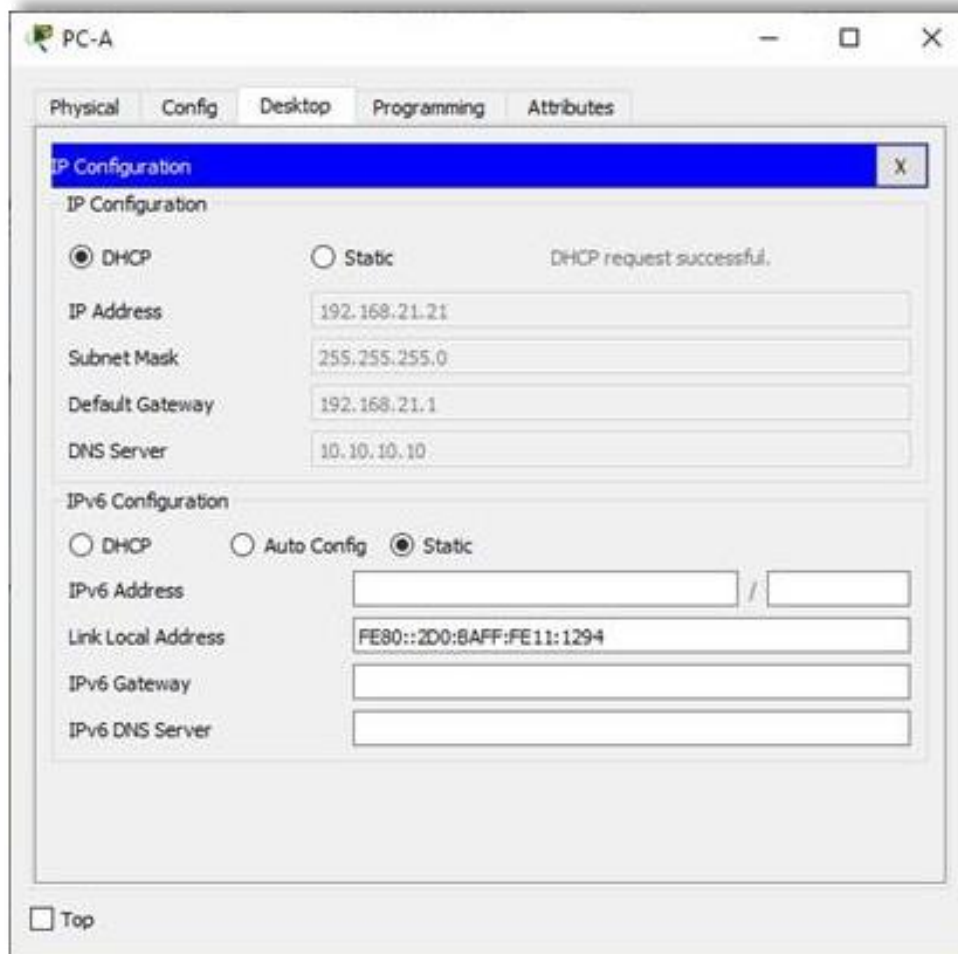
- ip http server
- ip http authentication local
- ip http secure-server

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.

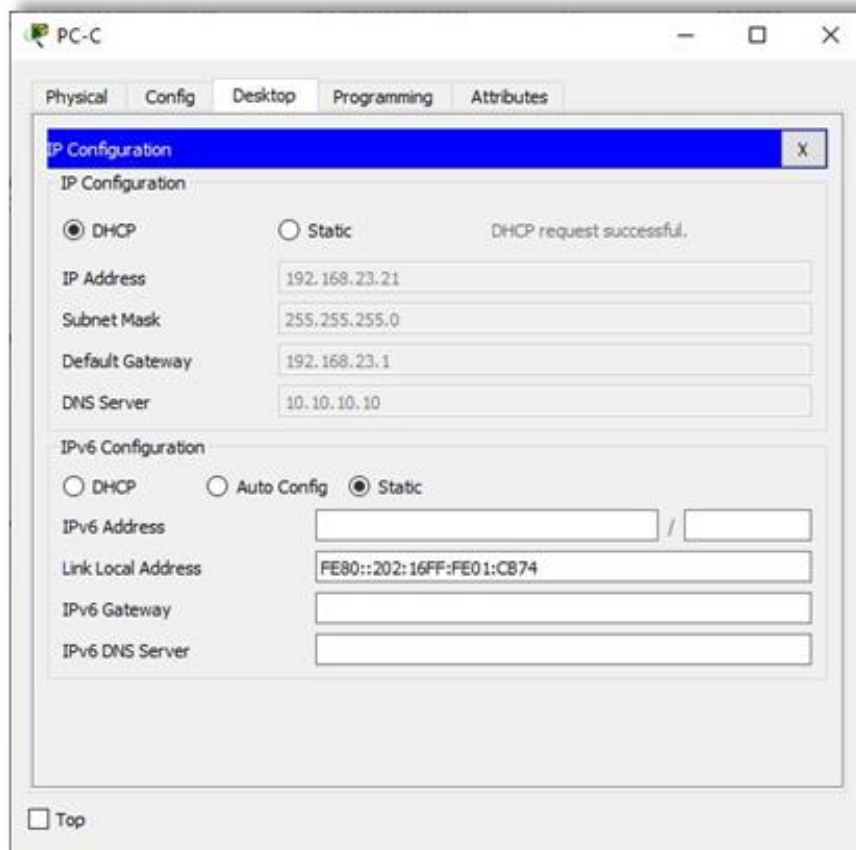
- Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

Figura 12 Información de IP del servidor de DHCP en el PC-A.



Fuente: Elaboración propia

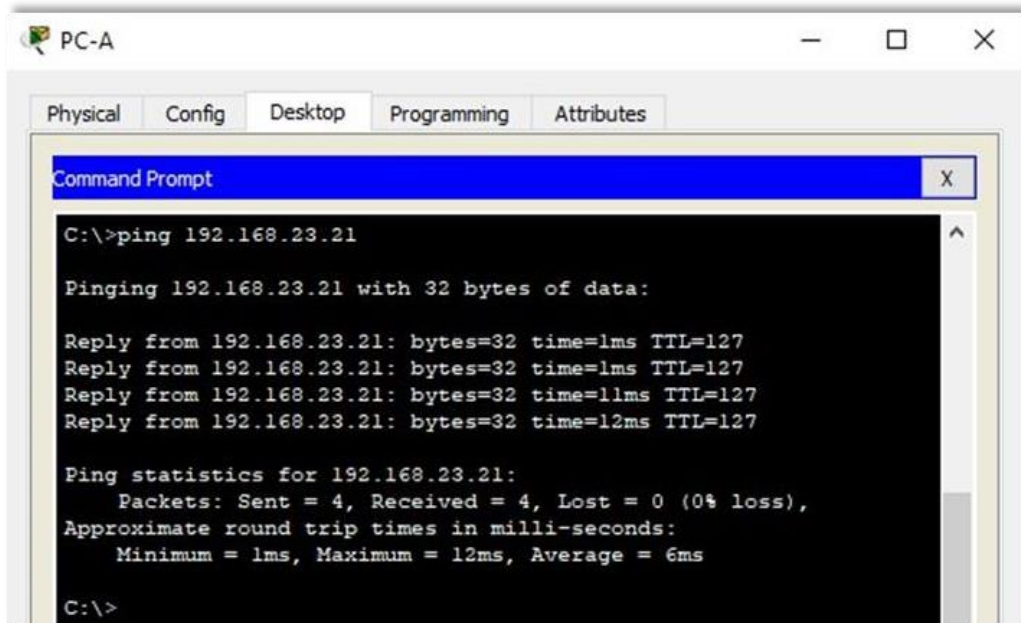
Figura 13 Información de IP del servidor de DHCP en el PC-C



Fuente: Elaboración propia

- Verificar que la PC-C haya adquirido información de IP del servidor de DHCP
- Verificar que la PC-A pueda hacer ping a la PC-C

Figura 14 Verificación de ping PC-A a la PC-C



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.23.21

Pinging 192.168.23.21 with 32 bytes of data:

Reply from 192.168.23.21: bytes=32 time=1ms TTL=127
Reply from 192.168.23.21: bytes=32 time=1ms TTL=127
Reply from 192.168.23.21: bytes=32 time=11ms TTL=127
Reply from 192.168.23.21: bytes=32 time=12ms TTL=127

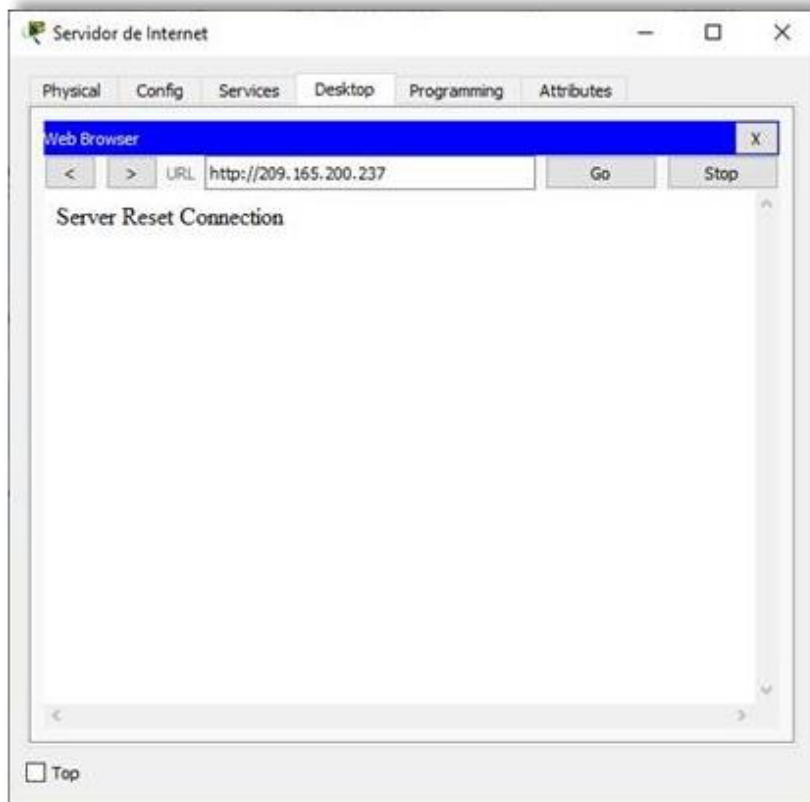
Ping statistics for 192.168.23.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 6ms

C:\>
```

Fuente: Elaboración propia

- Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**

Figura 15 Acceso Servidor Web desde el Servidor de Internet



Fuente: Elaboración propia

Parte 6: Configurar NTP

- Ajuste la fecha y hora en R2.

```
R2#clock set 00:40:00 30 April 2020
```

- Configure R2 como un maestro NTP.

```
R2(config)#ntp master 5
```

```
^% Invalid input detected at '^' marker. R2(config)#
```

Nota: Packet tracer no soporta este comando.

- Configurar R1 como un cliente NTP. Servidor: R2

```
R1(config)#ntp server 172.16.1.2  
R1(config)#
```

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

```
R1(config)#ntp update-calendar  
R1(config)#
```

- Verifique la configuración de NTP en R1.

```
R1#show ntp associations  
% This command is not supported by Packet  
Tracer. R1#
```

Nota: Este comando no es compatible con Packet Tracer.

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**
- Aplicar la ACL con nombre a las líneas VTY

- Permitir acceso por Telnet a las líneas de VTY
- Verificar que la ACL funcione como se espera

```
R2(config)#ip access-list standard ADMIN-MGT
```

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

```
R2(config-std-nacl)#exit
```

```
R2(config)#line vty 0 15
```

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

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

```
R1#telnet 172.16.1.2
```

```
Trying 172.16.1.2 ...OpenSe prohíbe el acceso no Elaboración propiaizado.
```

```
User Access Verification
```

```
Password:
```

```
R2>exit
```

```
[Connection to 172.16.1.2 closed by foreign host]
```

```
R1#
```

```
R3#telnet 172.16.1.2
```

```
Trying 172.16.1.2 ...
```

```
% Connection refused by remote host
```

```
R3#
```

Figura 16 Prueba de Telnet de R1 a R2.

```
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohíbe el acceso no autorizado.

User Access Verification

Password:
R2>exit

[Connection to 172.16.1.2 closed by foreign host]
R1#
```

Fuente: Elaboración propia

Paso 2: Introducir el comando de 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#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#
```

- Restablecer los contadores de una lista de acceso

```
R2#clear ip access-list counters
R2#clear ip
bgp Clear BGP connections
dhcp Delete items from the DHCP database
```

nat Clear NAT
ospf OSPF clear commands
route Delete route table entries

R2#

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

```
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 209.165.200.233/29
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always
sent ICMP mask replies are
never sent IP fast switching is
disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
```

IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
GigabitEthernet0/1 is administratively down, line protocol is down (disabled)
Internet protocol processing disabled
Serial0/0/0 is up, line protocol is up (connected)
Internet address is 172.16.1.2/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
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
ICMP unreachable are always sent
ICMP mask replies are never sent IP
fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled RTP/IP
header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Serial0/0/1 is up, line protocol is up (connected) Internet
address is 172.16.2.2/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
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 ICMP
unreachables are always sent ICMP
mask replies are never sent IP fast
switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled

BGP Policy Mapping is disabled
Loopback0 is up, line protocol is up (connected)
Internet address is 10.10.10.10/32
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1514bytes
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
ICMP unreachable are always
sent ICMP mask replies are
never sent IP fast switching is
disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is
disabled RTP/IP header compression
is disabled Probe proxy name replies
are disabled Policy routing is
disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is
disabled WCCP Redirect inbound
is disabled WCCP Redirect
exclude is disabled

Vlan1 is administratively down, line protocol is down
Internet protocol processing disabled

R2#

- ¿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

--- 209.165.200.237 10.10.10.10 --- ---

Tcp 209.165.200.237:80 10.10.10.10:80

209.165.200.238:1033209.165.200.238:1033

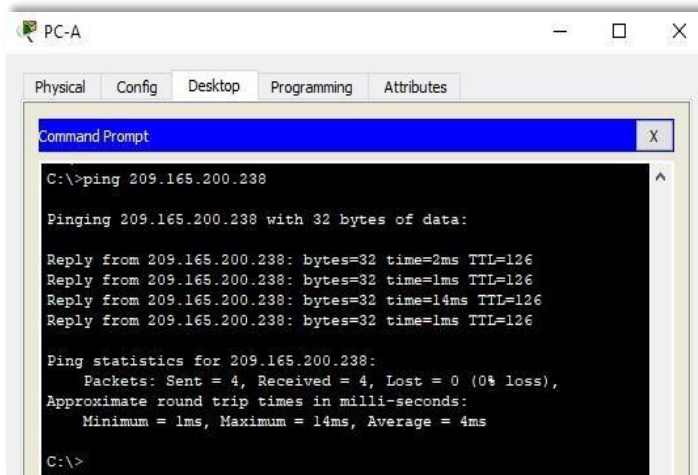
R2#

Figura 17 Ver las traducciones NAT en el R3

```
R2# show ip nat translations
Pro  Inside global    Inside local    Outside local    Outside global
---  209.165.200.237   10.10.10.10    ---              ---
tcp  209.165.200.237:80 10.10.10.10:80  209.165.200.238:1033 209.165.200.238:1033
R2#
```

Fuente: Elaboración propia

Figura 18 Prueba de ping al Servidor de Internet desde la PC-A.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 209.165.200.238

Pinging 209.165.200.238 with 32 bytes of data:

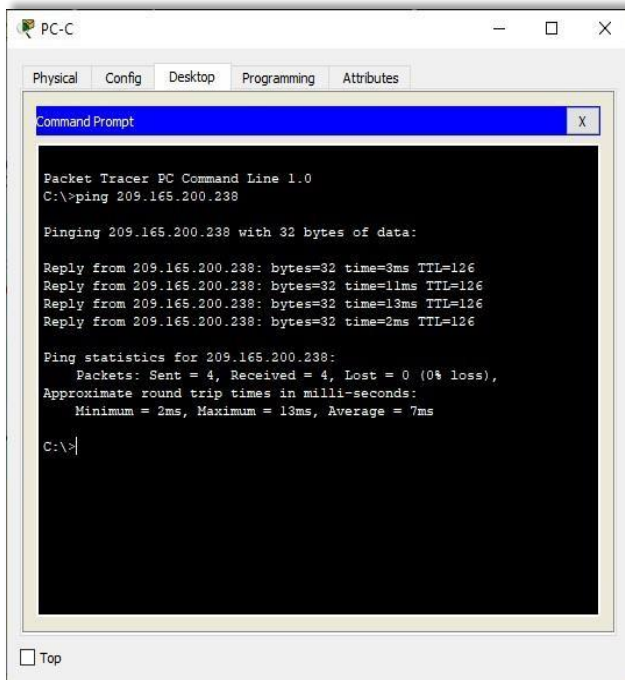
Reply from 209.165.200.238: bytes=32 time=2ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=14ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.200.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 4ms

C:\>
```

Fuente: Elaboración propia

Figura 19 Prueba de ping al Servidor de Internet desde la PC-C.



```
PC-C
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.238

Pinging 209.165.200.238 with 32 bytes of data:

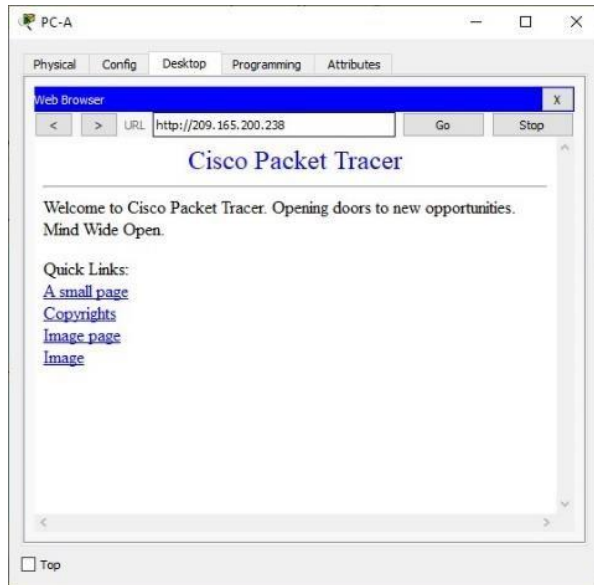
Reply from 209.165.200.238: bytes=32 time=3ms TTL=126
Reply from 209.165.200.238: bytes=32 time=11ms TTL=126
Reply from 209.165.200.238: bytes=32 time=13ms TTL=126
Reply from 209.165.200.238: bytes=32 time=2ms TTL=126

Ping statistics for 209.165.200.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 13ms, Average = 7ms

C:\>
```

Fuente: Elaboración propia

Figura 20 Prueba de acceso al Servidor de Web desde PC-A



Fuente: Elaboración propia

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas

```
R2#show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global
```

```
--- 209.165.200.237 10.10.10.10 --- ---
```

```
tcp 209.165.200.233:1025192.168.23.21:1025 209.165.200.238:80  
209.165.200.238:80
```

```
tcp 209.165.200.234:1025192.168.21.21:1025 209.165.200.238:80  
209.165.200.238:80 tcp 209.165.200.237:80 10.10.10.10:80  
209.165.200.238:1033209.165.200.238:1033
```

```
R2#clear ip nat translation * R2#show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global
```

```
--- 209.165.200.237 10.10.10.10 -----R2#
```

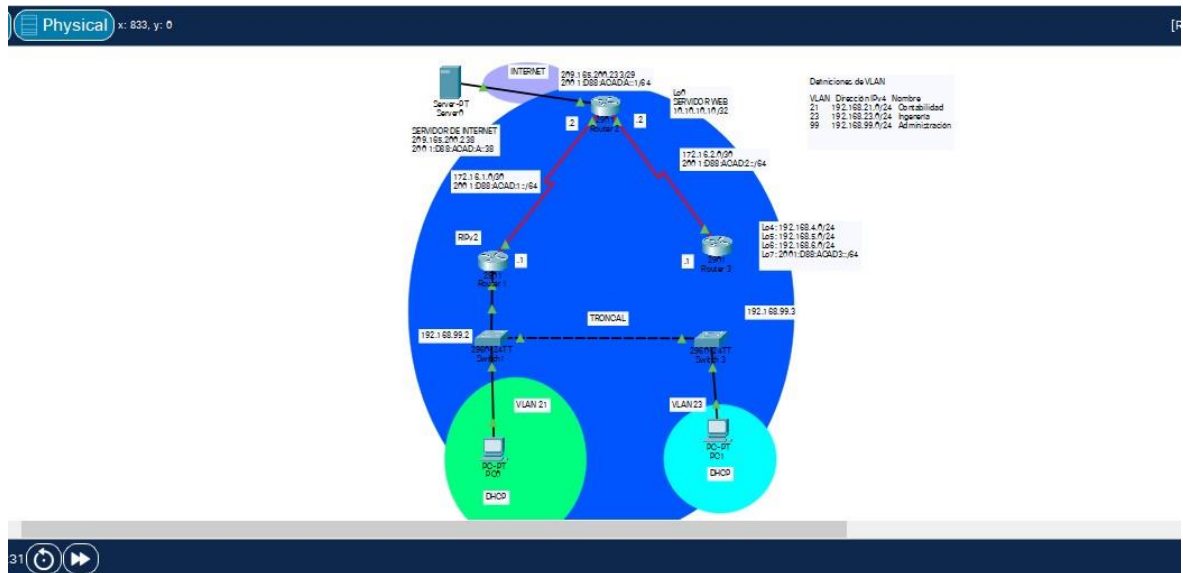
Figura 21 Eliminar las traducciones de NAT dinámicas.

```
R2#show ip nat translations
Pro Inside global   Inside local       Outside local       Outside global
--- 209.165.200.237  10.10.10.10       ---                ---
tcp 209.165.200.233:1025 192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.234:1025 192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.237:80  10.10.10.10:80    209.165.200.238:1033 209.165.200.238:1033

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

Fuente: Elaboración propia

Figura 22 Topología de red escenario 2 - Cisco Packet Tracer.



Fuente: Elaboración propia

CONCLUSIONES

El diseño e implementación de escenarios en Cisco Packet Tracer Student ofrece visualización, creación, evaluación y capacidades de colaboración, y facilita a los estudiantes la comprensión de conceptos tecnológicos complejos

La implementación de los elementos abordados proporciona un mejor rendimiento de la red pues los mismos garantizan seguridad, fácil administración, redundancia incremento del ancho de banda, entre otras ventajas.

La verificación de las configuraciones desarrolladas y la realización de pruebas de conectividad entre los dispositivos, se torna una necesidad para el administrador, pues en caso de fallos en la red es importante descubrir el origen del problema para su solución inmediata.

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). Capa de red. Fundamentos de Networking. Recuperado de

<https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1>

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado

de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos

de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1>

CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de

Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>