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

JUAN CARLOS ALVAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

BARRANQUILLA

2021

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

JUAN CARLOS ALVAREZ

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

Tutor

RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

BARRANQUILLA

2021

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

BARRANQUILLA, diciembre 2, 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 en sistemas.

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
Escenario 1....13
Paso 1: configurar los ajustes básicos....14
paso 2. Configurar los equipos....18
Escenario 2....21
Topología....21
Parte 1: Inicializar dispositivos....22
Parte 2: Configurar los parámetros básicos de los dispositivos....29
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN .47
Parte 4: Configurar el protocolo de routing dinámico OSPF....56
Parte 5: Implementar DHCP y NAT para IPv4....61
Parte 6: Configurar NTP....66
Conclusiones....75
Bibliografía....76

Lista de tablas

Tabla 1 item requerimiento 13
Tabla 2 pc-a network configuration 18
Tabla 3 configuración de red de pc-b.....19
Tabla 4 configuracion del servidor 30
Tabla 5 ipv4 subnet.....30
Tabla 6 pv6 subnet 31
Tabla 7 verificar la conectividad de la red.....45
Tabla 8 verificar la conectividad de los dispositivos.....54

Lista de figuras

Figura 1 topología de red escenario 1 13
Figura 2 fastethernet connection pc-a 19
Figura 3 fastethernet connection pc-b 20
Figura 4 topología de red escenario 2 21
Figura 5 configuración ip del servidor 31
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 54
Figura 9 prueba de ping desde s3 a r1, dirección vlan 99. 55
Figura 10 prueba de ping desde s1 a r1, dirección vlan 21 55
Figura 11 prueba de ping desde s3 a r1, dirección vlan 23. 55
Figura 12 show ip protocols 59
Figura 13 sh ip route 60
Figura 14 sh run begin | ospf 61
Figura 15 información de ip del servidor de dhcp en el pc-a. 64
Figura 16 información de ip del servidor de dhcp en el pc-c 65
Figura 17 verificación de ping pc-a a la pc-c 66
Figura 18 prueba de telnet de r1 a r2. 69
Figura 19 r2#show access-list 69
Figura 20 r2#clear access-list 70
Figura 21 r2#show ip interface 70
Figura 22 ver las traducciones nat en el r2 71
Figura 23 prueba de ping al servidor de internet desde la pc-a. 72
Figura 24 prueba de ping al servidor de internet desde la pc-c. 72
Figura 25 prueba de acceso al servidor de web desde pc-a 73
Figura 26 eliminar las traducciones de nat dinámicas. 74
Figura 27 topología de red escenario 2 - cisco packet tracer. 74

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 interfaz de un nodo de la red y usada para identificar (localizar) en forma única el nodo dentro de la Internet. Dos versiones están actualmente implementadas: IPv4 e IPv6.

Dirección IPv4: Una dirección IP con base en el IPv4. Esas direcciones consisten en 32 bits (O 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 O 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.

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 generar más puertos virtuales hasta completar un total de 21 líneas vty.

Resumen

El trabajo se realiza con el propósito de ejecutar de una forma práctica los conocimientos adquiridos a Io 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

Work is done 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

Introducción

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.

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	192.168.46.0
Requerimiento de host Subred LAN1	192.168.46.0 - 192.168.46.127 /25
Requerimiento de host Subred LAN2	192.168.46.128 - 192.168.46.191 /26
R1 G0/0/1	192.168.46.1 /25
R1 G0/0/0	192.168.46.129 /26
S1 SVI	192.168.46.2
PC-A	192.168.46.126
PC-B	192.168.46.190

Fuente: autor

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 Acess is Prohibited#

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

  interface g0/0/0

  description PC-B

  ip address 192.168.46.129 255.255.255.192

  no shutdown

  exit

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

  interface g0/0/1

  description PC-B

  ip address 192.168.46.1 255.255.255.128

  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 Acess 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 192.168.46.2 255.255.255.128

  description Management Interface

  no shutdown

- Configuración del gateway predeterminado.

S1(config)#ip default-gateway 192.168.46.

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	*192.168.46.126*
Máscara de subred	*255.255.255.128*
Gateway predeterminado	*192.168.46.1*

Fuente: autor

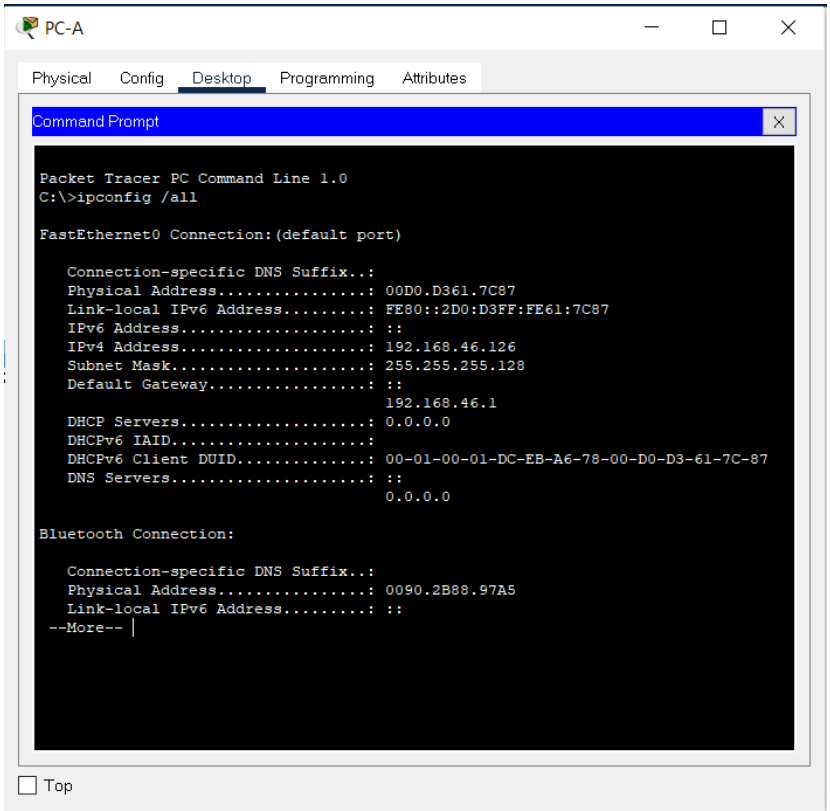
Tabla 3 Configuración de red de PC-B

Configuración de red de PC-B	
Descripción	*PC-B*
Dirección IP	*192.168.46.190*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*192.168.46.129*

Fuente: autor

Ipconfig PC-A

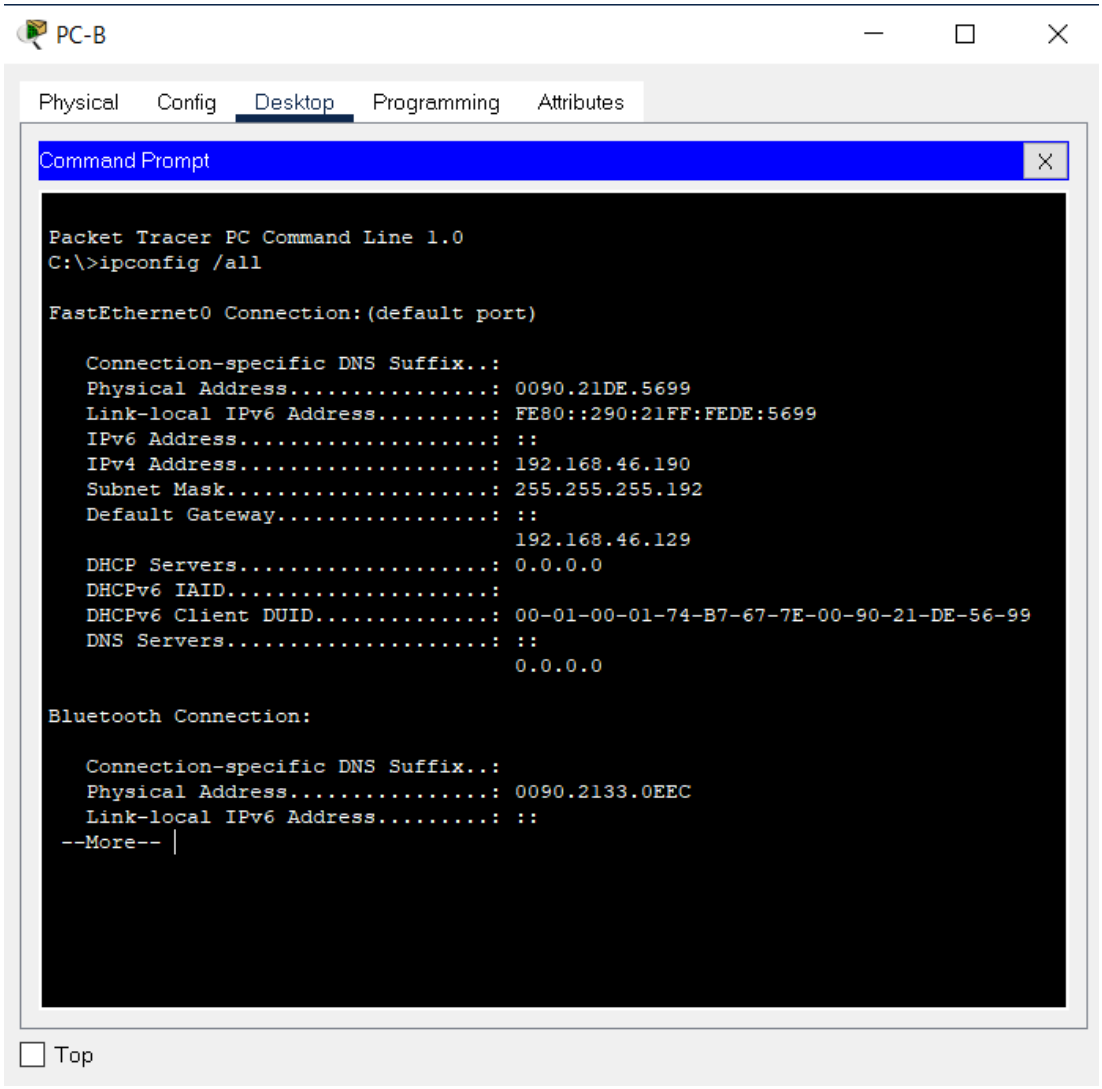
Figura 2 Fast Ethernet connection PC-A



Fuente: autor

Ipconfig PC-B

Figura 3 Fast Ethernet connection PC-B



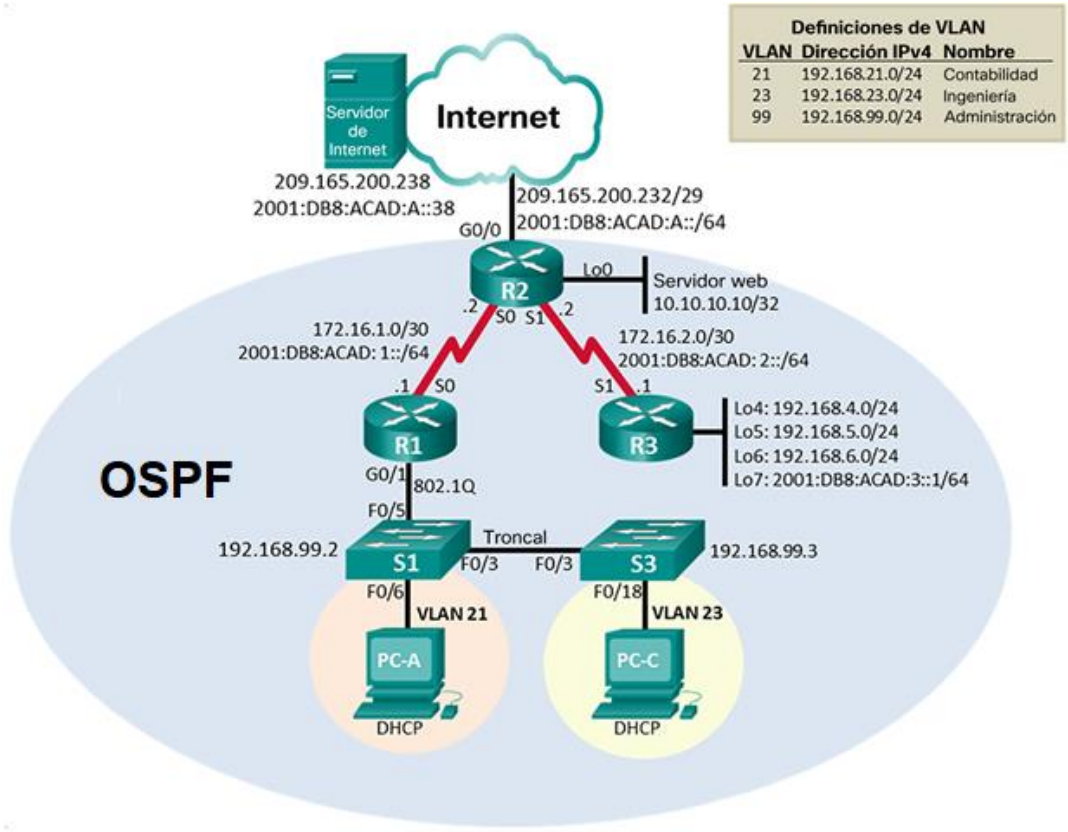
Fuente: autor

Escenario 2

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

Topología

Figura 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 lpv4	209.165.200.238
Máscaras de subred para lpv4:	255.255.255.248
Gateway predeterminado:	209.165.200.233
Dirección lpv6/subred:	201:db8:acad:a::38/64
Gateway prederminado lpv6:	201:db8:acad:a::1

Fuente: autor

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

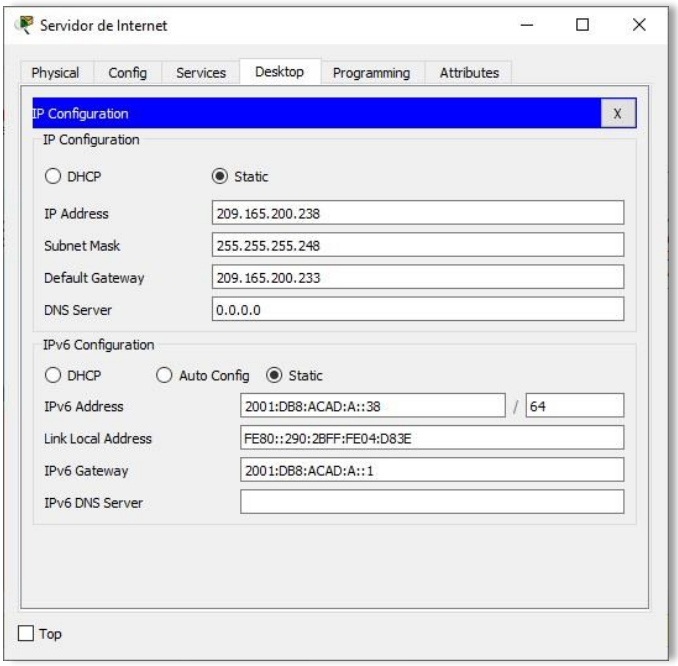
Fuente: autor

Tabla 6 pV6 Subnet

Ip Addres:	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: autor

Figura 5 Configuración IP del servidor



Fuente: autor

Paso 2. Configurar R1

Nombre del router

Router(config)#hostname R1 en modo global asignamos nombre al R

Desactivar la búsqueda DNS

R1(config)#no ip domain-lookup desactivo búsquedas DNS

Contraseña de exec privilegiado cifrada

R1(config)#enable secret class habilito contraseña en modo privilegiado

Contraseña de acceso a la consola

R1(config-line)#line console 0 accedo a la consola
principalR1(config-line)#password cisco asigno contraseña
R1(config-line)#login confirmo contraseña

Contraseña de acceso Telnet

R1(config-line)#line vty 0 4 accedo a la consola telnet
R1(config-line)#password cisco asigno contraseña
R1(config-line)#login confirmo la contraseña

Cifrar las contraseñas de texto no cifrado

R1(config)#service password-encryption encripto contraseñas sin encriptar

Mensaje MOTD

R1(config)#banner motd # se prohibe el acceso no autorizado# asigo un banner

Interfaz S0/2/0

Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección dis ponible en la subred.

R1(config)#interf s0/2/0 accedo a la interfaz

R1(config-if)#ip address 172.16.1.1 255.255.255.252 asigno una ip

R1(config-if)#no shutdown subo la interfaz

Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz

R1(config)#ipv6 unicast-routing en modo global, habilito usar ipv6R1(config)#interfac s0/2/0 accedo a la interfaz

R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 asigno una ip

R1(config-if)#clock rate 128000 asigno frecuencia de reloj

R1(config-if)#no shutdown subo la interfaz

R1(config-if)#

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

R1(config)#ip route 0.0.0.0 0.0.0.0 S0/2/0 asigno ruta pred. En ipv4

%Default route without gateway, if not a point-to-point interface, may impactperformance

R1(config)#

R1(config)#ipv6 route ::/0 S0/2/0 asigno ruta pred.en ipv6

Configurar R2

Desactivar la búsqueda DNS

Router(config)#no ip domain-lookup en modo global se deactiva búsqueda DNS

Nombre del router

Router(config)#hostname R2 se da nombre al R

Contraseña de exec privilegiado cifrada

R2(config)#enable secret class se da contraseña en modo privilegiado

Contraseña de consola principal

CR2(config)#line console 0 se accede a la consola principal

R2(config-line)#password cisco se asigna contraseña

R2(config-line)#logi se confirma contraseña

Contraseña de acceso Telnet

R2(config-line)#line vty 0 4 se accede a la consola telnet

R2(config-line)#password cisco se asigna contraseña

R2(config-line)#login se confirma contraseña

R2(config-line)#exit se sale

Cifrar las contraseñas de texto no cifrado

R2(config)#service password-encryption se encriptan contraseñas no cifradas

HR2(config)#ip http server comando invalido en el IOS

% Invalid input detected at '^'
marker. R2(config)#ip
http secure-server

% Invalid input detected at '^'
marker.habilitar el
servidor HTTP

Este comando no es soportado en packet-tracer

Mensaje MOTD

R2(config)#banner motd $se prohibe el acceso no autorizado$ se pone un banner

Interfaz S0/2/0

Establezca la descripción

Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.

R2(config)#ipv6 unicast-routing se activa protocolo ipv6

R2(config)#interfac s0/2/0 se accede a la interfaz

R2(config-if)#ip address 172.16.1.2 255.255.255.252 se asigna una ip

R2(config-if)#description esta interfaz va hacia el R1 se da una descripcion

Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz

R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 se asigna una ipv6
R2(config-if)#no shutdown se sube la interfaz

R2(config-if)#

%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed stateto up

Interfaz S0/2/1

Establecer la descripción

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

R2(config)#interfac s0/2/1 se accede a la interfaz

R2(config-if)#description esta interfaz va hacia el R3 se da una descripcion

R2(config-if)#ip address 172.16.2.1 255.255.255.252 se asigna una ip

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)#ipv6 add 2001:DB8:ACAD:2::2/64 se asigna una ipv6

R2(config-if)#clock rate 128000 se asigna una frecuencia de reloj

R2(config-if)#no shutdown se sube la interfaz

%LINK-5-CHANGED: Interface Serial0/2/1, changed state to down

Interfaz G0/0/0 (simulación de Internet)Establecer la descripción.

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

R2(config)#interfac g0/0/0 se accede a la interfaz

R2(config-if)#description interface hacia internet se da una descripción

R2(config-if)#exit se sale

R2(config)#ipv6 unicast-routing se activa protocolo ipv6

R2(config)#interfac g0/0/0 se accede a la interfaz

R2(config-if)#ip address 209.165.200.233 255.255.255.248 se asigna una ip

Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.

Activar la interfaz

R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64 se asigna una ipv6

R2(config-if)#no shutdown se sube la interfaz

R2(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

Interfaz loopback 0 (servidor web simulado)

Establecer la descripción. Establezca la dirección IPv4.

R2(config)#interfac loopback 0 se asigna una interfaz loopback

R2(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

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

R2(config-if)#description servidor web se da una descripcion

R2(config-if)#ip address 10.10.10.10 255.255.255.255 se asigna una ip

R2(config-if)#

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 G0/0/0 se da una ruta pred. ipv4

%Default route without gateway, if not a point-to-point interface, may impact performance

R2(config)#ipv6 route ::/0 G0/0/0 se asigna ruta pred.ipv6

R2(config)#

Configurar R3

Desactivar la búsqueda DNS

Router>en se accede al modo privilegiado

Router#config termi se accede al modo de configuración global

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#no ip domain-lookup se desactivan búsquedas DNS

Nombre del router

Router(config)#hostname R3 se asigna un nombre al R

Contraseña de exec privilegiado cifrada

R3(config)#enable secret class se da contraseña al modo privilegiado

Contraseña de acceso a la consola

R3(config)#line console 0 se accede a la consola principal

R3(config-line)#password cisco se asigna contraseña

R3(config-line)#login se confirma contraseña

Contraseña de acceso Telnet

R3(config-line)#line vty 0 4 se accede a la consola de telnet

R3(config-line)#password cisco se asigna contraseña

R3(config-line)#login se confirma contraseña

Cifrar las contraseñas de texto no cifrado

R3(config-line)#exit se sale

R3(config)#service password-encryption se encripta contraseñas sin encriptar

Mensaje MOTD

R3(config)#banner motd $Se Prohibe El Acceso No Autorizado$ se da un banner
R3(config)#

Interfaz S0/2/1 Establecer la descripción

R3(config-if)#description esta es la interfaz hacia el R2 se da una descripcion

Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.

R3(config)#ipv6 unicast-routing se activa el protocolo ipv6

R3(config)#interfac s0/2/1 se accede a la interfaz

R3(config-if)#ip address 172.16.2.2 255.255.255.252 se da una ip

Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz

R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 se da una ipv6

R3(config-if)#no shutdown se sube la interfaz

R3(config-if)#

%LINK-5-CHANGED: Interface Serial0/2/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to up

Interfaz loopback 4

R3(config)#interfac loopback 4 se crea la loopback

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback4, changed state to up

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

R3(config-if)#ip add 192.168.4.1 255.255.255.0 se da una ip

R3(config-if)#exit se sale

Interfaz loopback 5

R3(config)#interfa loopback 5 se crea la interfazR3(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 se le da una ip

R3(config-if)#exit se sale In

R3(config)#interfac loopback 6 se crea la interfaz

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 se le da una ip

R3(config-if)#exit se sale

Interfaz loopback 7

R3(config)#interfac loopback 7 se crea la interfaz

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)#

Rutas predeterminadas

R3(config-if)#ip route 0.0.0.0 0.0.0.0 S0/2/1 se crea ruta pred.ipv4

%Default route without gateway, if not a point-to-point interface, may impactperformance

R3(config)#ipv6 route ::/0 S0/2/1 se crea ruta pred. Ipv6

R3(config)#

Configurar S1

Desactivar la búsqueda DNS

Switch(config)#no ip domain-lookup se desactivan búsquedas DNS

Nombre del switch

Switch(config)#hostname S1 se da un nombre al R

Contraseña de exec privilegiado cifrada

S1(config)#enable secret class se asigna contraseña en modo privilegiado

Contraseña de acceso a la consola

S1(config)#line console 0 se accede a la consola 0

S1(config-line)#password cisco se asigna una contraseña

S1(config-line)#login se confirma contraseña

Contraseña de acceso Telnet

S1(config-line)#line vty 0 15 se accede a la consola telnet

S1(config-line)#password cisco se asigna contraseña

S1(config-line)#login se confirma contraseña

S1(config-line)#exit se sale

Cifrar las contraseñas de texto no cifrado

S1(config)#service password-encryption se cifran contraseñas sin cifrar

Mensaje MOTD

S1(config)#banner motd Se Prohibe El Acceso No Autorizado se da un banner
S1(config)#

Configurar el S3

Desactivar la búsqueda DNS

Switch(config)#no ip domain-lookup se dasactivan búsquedas DNS

Nombre del switch

Switch(config)#hostname S3 se da un nombre al Switch

Contraseña de exec privilegiado cifrada

S3(config)#enable secret class se da contraseña al modo privilegiado

Contraseña de acceso a la consola

S3(config)#line console 0 se accede a la consola 0

S3(config-line)#password cisco se asigna contraseña

S3(config-line)#login se confirma contraseña

Contraseña de acceso Telnet

S3(config)#line vty 0 15 se accede a la consola telnet

S3(config-line)#password cisco se asigna contraseña

S3(config-line)#login se confirma contraseña

Cifrar las contraseñas de texto no cifrado

S3(config)#service password-encryption se cifran contraseñas sin cifrar
S3(config)#

Mensaje MOTD

S3(config-line)#banner motd Se prohibe El Acceso No Autirizado se da un banner

S3(config)#exit

Paso 7. Verificar la conectividad de la red

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

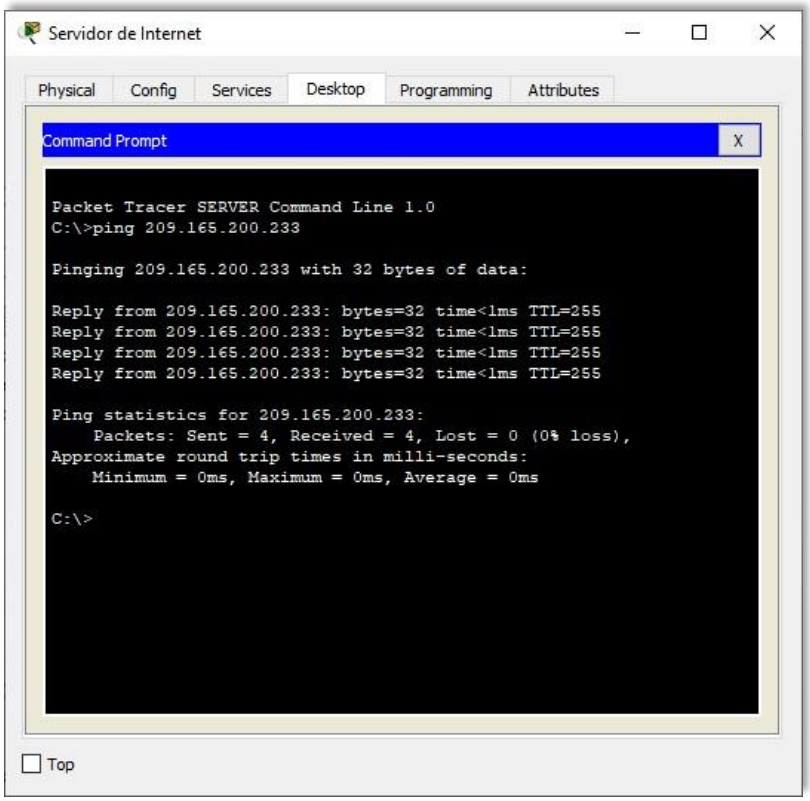
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla.

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

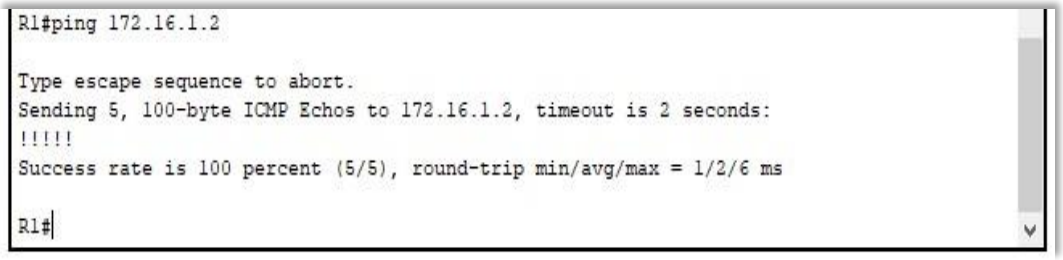
Fuente: autor

Figura 6 Prueba de Ping desde R1 a R2



Fuente: autor

Figura 7 Prueba de ping desde Servidor de Internet a Gateway predeterminado



Fuente: autor

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

S1(config)#vlan 21 se crea la interfaz

S1(config-vlan)#name contabilidad Se asigna un nombre

S1(config-vlan)#vlan 23 se crea la interfaz

S1(config-vlan)#name ingeniería se asigna un nombre

S1(config-vlan)#vlan 99 se crea la interfaz

S1(config-vlan)#name administración se asigna un nombreAsignar la dirección IP de administración.

S1(config-vlan)#interfac vlan 99 se crea la interfaz

S1(config-if)#ip address 192.168.99.2 255.255.255.0

S1(config-if)#no shutdown se sube la interfaz

S1(config-if)#exit se sale

S1(config)#

Asignar el gateway predeterminado

S1(config)#ip default-gateway 192.168.99.1 se asigna un Gateway pred.

S1(config)#

Forzar el enlace troncal en la interfaz F0/3

S1(config)#interfac f0/3 se accede ala interfaz

S1(config-if)#switchport mode trunk se asigna modo troncal en el

SS1(config-if)#switchport trunk native vlan 1 se asigna vlan nativa en troncal

Forzar el enlace troncal en la interfaz F0/5

S1(config)#interface f0/5 se accede ala interfaz

S1(config-if)#switchport trunk native vlan 1 se asigna vlan nativa en troncal

S1(config-if)#switchport mode trunk se asigna modo troncal en el S

S1(config-if)#

Configurar el resto de los puertos como puertos de acceso

S1(config)#interf range f0/1-f0/2 se accede ala interfaz

S1(config-if-range)#switchport mode access se asigna mode de acceso en S

S1(config-if-range)#interfa f0/4 se accede ala interfaz

S1(config-if)#switchport mode Access se asigna modo de acceso en S

S1(config-if)#interf range f0/7-f0/24 se asigna un rango en la interfaz

S1(config-if-range)#switchport mode access se asignan modo de acceso

Asignar F0/6 a la VLAN 21

S1(config-if-range)#interface f0/6 se accede ala interfaz

S1(config-if)#switchport mode Access se asigna modo de acceso al S

S1(config-if)#switchport access vlan 21 se da modo de acceso a la vlan

S1(config-if)#

Apagar todos los puertos sin usar

S1(config-if)#interfa range f0/7-f0/24 se asigna un rango en la interfaz

S1(config-if-range)#shutdown se desactivan las interfaces

%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

Configurar el S3

Crear la base de datos de VLAN

S3(config)#vlan 21 se crea la interfaz

S3(config-vlan)#name contabilidad se asigna un nombre

S3(config-vlan)#vlan 23 se crea la interfaz

S3(config-vlan)#name ingeniería se asigna un nombre

S3(config-vlan)#vlan 99 se crea la interfaz

S3(config-vlan)#name administración se asigna un nombre

Asignar la dirección IP de administración

S3(config-vlan)#interfac vlan 99 se crea la interfaz

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 se da una ip

S3(config-if)#no shutdown se sube la interfaz

S3(config-if)#exit se sale

Asignar el gateway predeterminado.

ip default-gateway 192.168.99.1 se asigna un Gateway pred.

Forzar el enlace troncal en la interfaz F0/3

S3(config)#interfac f0/3 se accede a la interfaz

S3(config-if)#switchport mode trunk se configura modo troncal

S3(config-if)#switchport trunk native vlan 1 se asigna vlan1 nativa en troncal

S3(config-if)#

Configurar el resto de los puertos como puertos de acceso

S3(config)#interfac range f0/1-f0/2 se asigna un rango en la interface

S3(config-if-range)#switchport mode access se asigna mode de acceso

S3(config-if-range)#interf range f0/4-f0/24 se asigna un rango en la interface

S3(config-if-range)#switchport mode Access se asigna modo de acceso

S3(config-if-range)#exit se sale

Asignar F0/18 a la VLAN 21

S3(config)#interf f0/18 se accede a la interfaz

S3(config-if)#switchport access vlan 21 se configura modo de acceso a la vlan

S3(config-if)#exit se sale

Apagar todos los puertos sin usar

S3(config)#interface range f0/4-f0/17 se configura un rango en elinterface

S3(config-if-range)#shutdown se desactivan las interfaces

%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

Configurar R1

R1(config)#interface g 0/0/1 se accede a la interfaz

R1(config-if)#no shutdown se sube la interfaz

Configurar la subinterfaz 802.1Q .21 en G0/0/1

R1(config)#interface g 0/0/1.21 se accede a la interfaz vlan

R1(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface

GigabitEthernet0/0/1.21,changed state to up

R1(config-subif)#description LAN de Contabilidad se describe la interfaz

R1(config-subif)#encapsulation dot1q 21 se da un comando de encapsulación

R1(config-subif)#ip address 192.168.21.1 255.255.255.0 se asigna una ip

R1(config-subif)#exit se sale

Configurar la subinterfaz 802.1Q .23 en G0/0/1

R1(config)#interface g 0/0/1.23 se crea la subinterfaz

R1(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1.23,changed state to up

R1(config-subif)#description Lan de Ingeniería se da descripción de la interfaz

R1(config-subif)#encapsulation dot1q 23 se asigna modo de encapsulación

R1(config-subif)#ip address 192.168.23.1 255.255.255.0 se da una ip

R1(config-subif)#exit

Configurar la subinterfaz 802.1Q .99 en G0/0/1

R1(config)#interface g 0/0/1.99 se crea la subinterfaz

R1(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.99, changed state to up

R1(config-subif)#description LAN de Administración se da una descripcion

R1(config-subif)#encapsulation dot1q 99 se da modo de encapsulación

R1(config-subif)#ip add 192.168.99.1 255.255.255.0 se da una ip

R1(config-subif)#exit

Activar la interfaz G0/0/1

R1(config)#interface g 0/0/1 se accede a la interfaz

R1(config-if)#no shutdown se sube la interfaz

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.

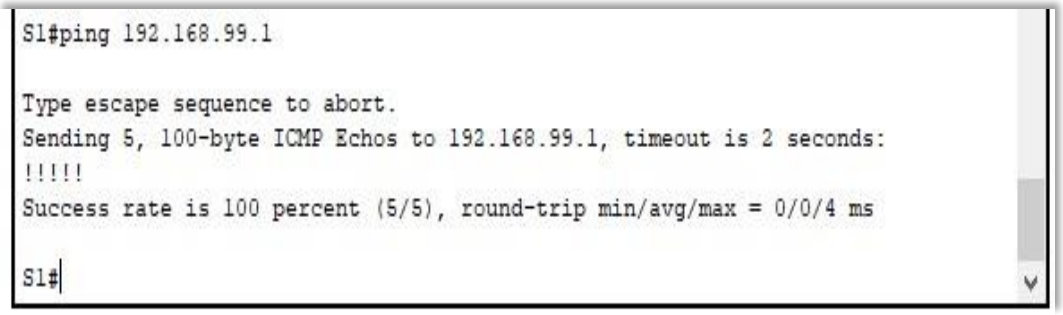
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

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

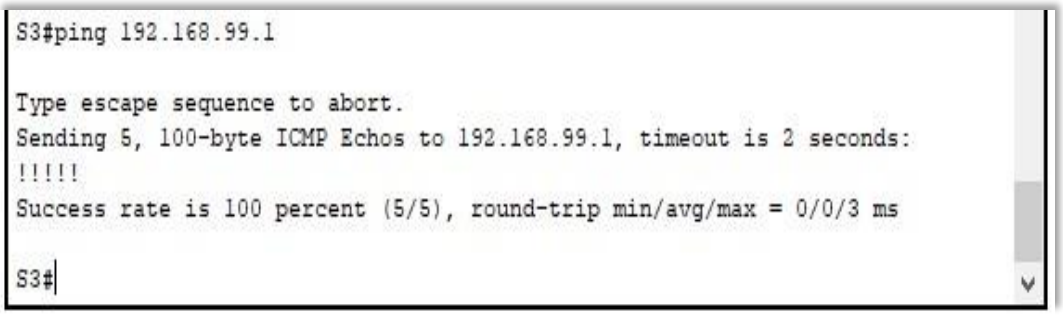
Fuente: autor

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



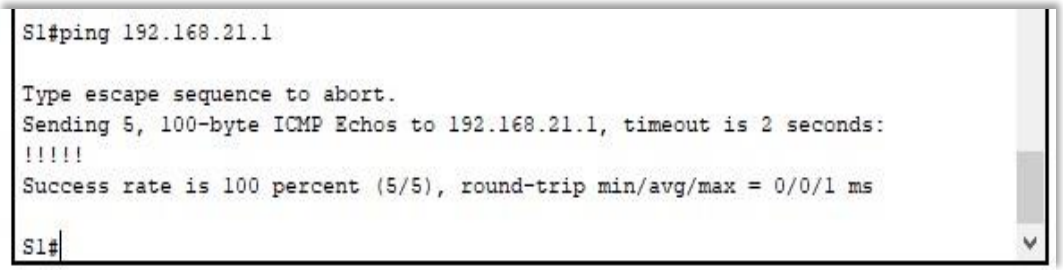
Fuente: autor

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



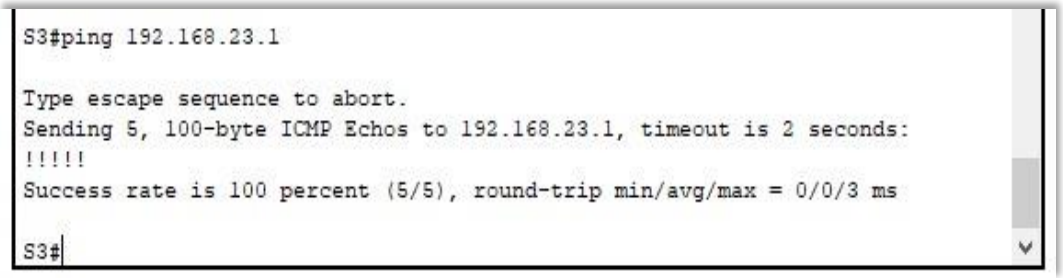
Fuente: autor

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



Fuente: autor

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



Fuente: autor

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1. Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Configurar OSPF área 0

Anunciar las redes conectadas directamente

R1(config)#router ospf 58 se configura el router al protocolo ospf

R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 se declaran la red

R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 se declaran la red

R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 se declaran la red

R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 se declaran la red

Establecer todas las interfaces LAN como pasivas

R1(config-router)#passive-interface g0/0/1 se declara la interfaz pasiva

R1(config-router)#passive-interface g0/0/1.21 se declara la interfaz pasiva

R1(config-router)#passive-interface g0/0/1.23 se declara la interfaz pasiva

R1(config-router)#passive-interface g0/0/1.99 se declara la interfaz pasiva

Desactive la sumarización automática

OSPF no realiza la sumarización automática

Configurar OSPF en el R2Configurar OSPF área 0

Anunciar las redes conectadas directamente

Nota: Omitir la red G0/0.

R2(config)#router ospf 58 se declara protocolo ospf

R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 se declara la red

R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 se declara la red

R2(config-router)#

11:19:47: %OSPF-5-ADJCHG: Process 58, Nbr 192.168.99.1 on Serial0/2/0 from LOADING to FULL, Loading Done

R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 se declara la red

Establecer la interfaz LAN (loopback) como pasiva

R2(config-router)#passive-interface loopback 0 se declara pasiva esta interfaz

R2(config-router)#exit se sale

Desactive la sumarización automática

OSPF no realiza la sumarización automática

Configurar OSPFv3 en el R2

Configurar OSPF área 0

R2(config)#interface s 0/2/0 se accede a la interfaz

R2(config-if)#ipv6 ospf 59 area 0 se activa protocolo ospf ipv6

R2(config-if)#exit se sale

R2(config)#interfece s 0/2/1 se accede ala interfaz

R2(config-if)#ipv6 ospf 59 area 0 se activa protocolo ospf ipv6

R2(config-if)#exit se sale

R2(config)#interface g 0/0/0 se accede a la interfaz

R2(config-if)#ipv6 ospf 59 area 0 se activa protocolo ospf ipv6

R2(config-if)#exit se sale

Anunciar redes IPv4 conectadas directamente

El protocolo OSPF V3. No maneja redes IPV4

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas

la loopback no tiene direcciones bajo IPV6.

en este protocolo eso no se hace para eso se coloca la wildcard y en IPV6 no se hace.

Desactive la sumarización automática.

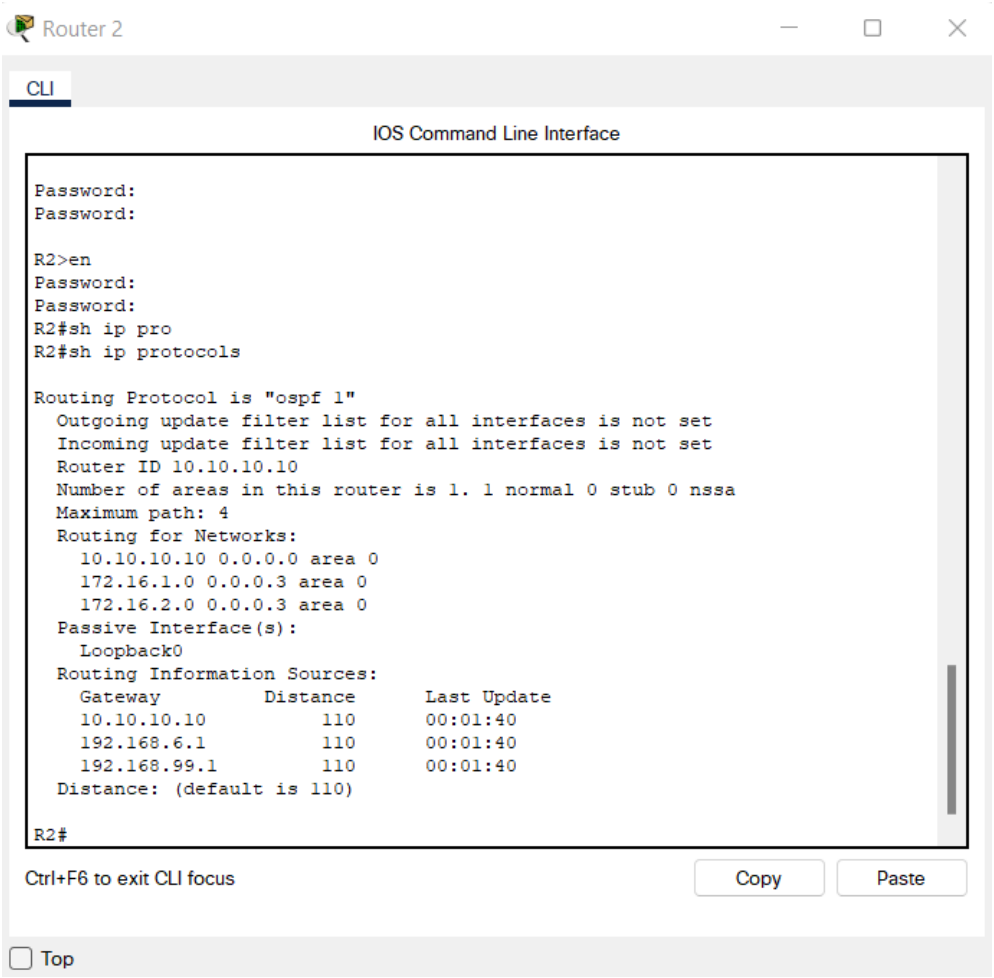
OSPF no realiza la sumarización automática

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?

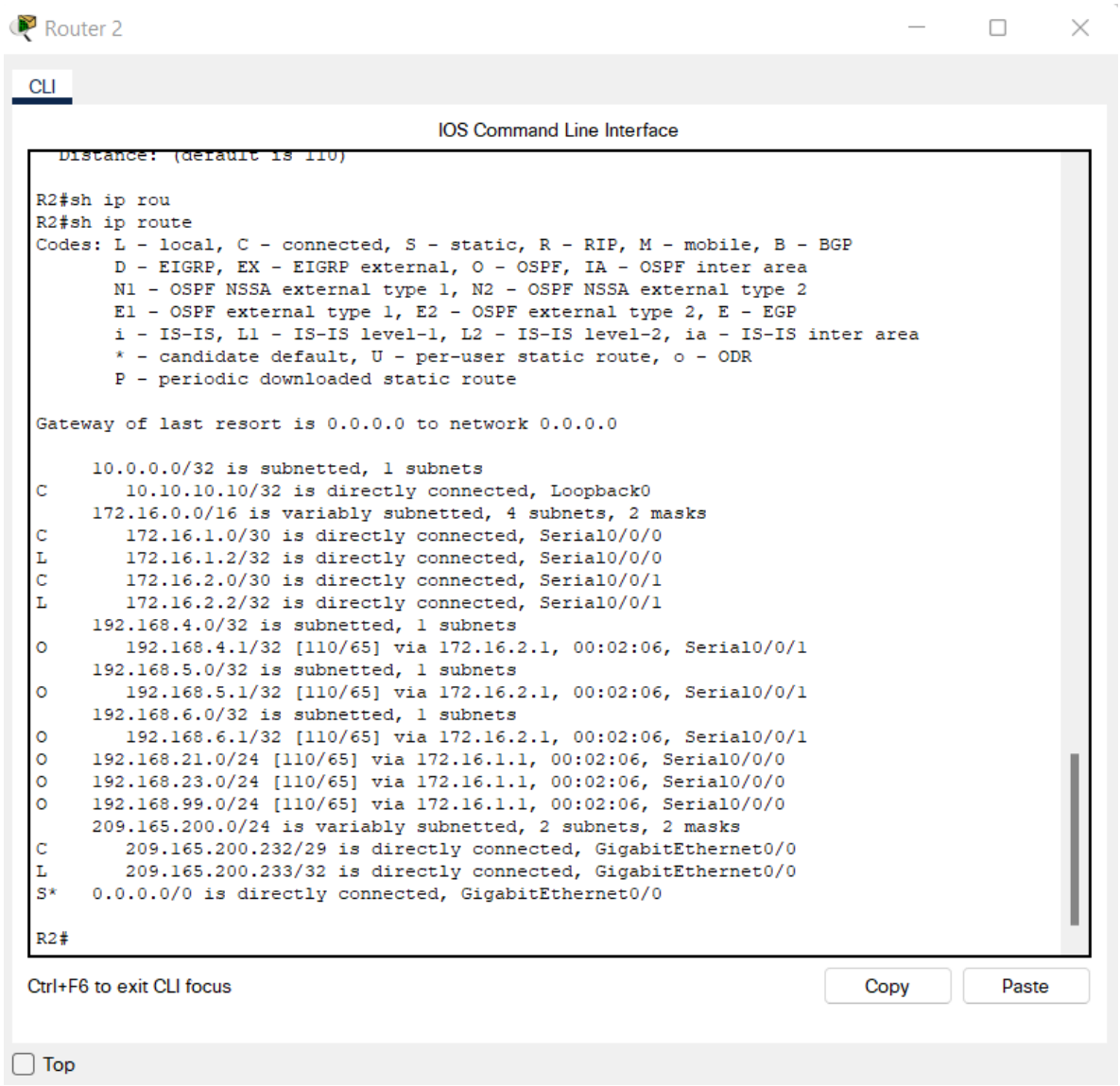
Figura 12 Show ip protocols



Fuente: autor

¿Qué comando muestra solo las rutas OSPF?

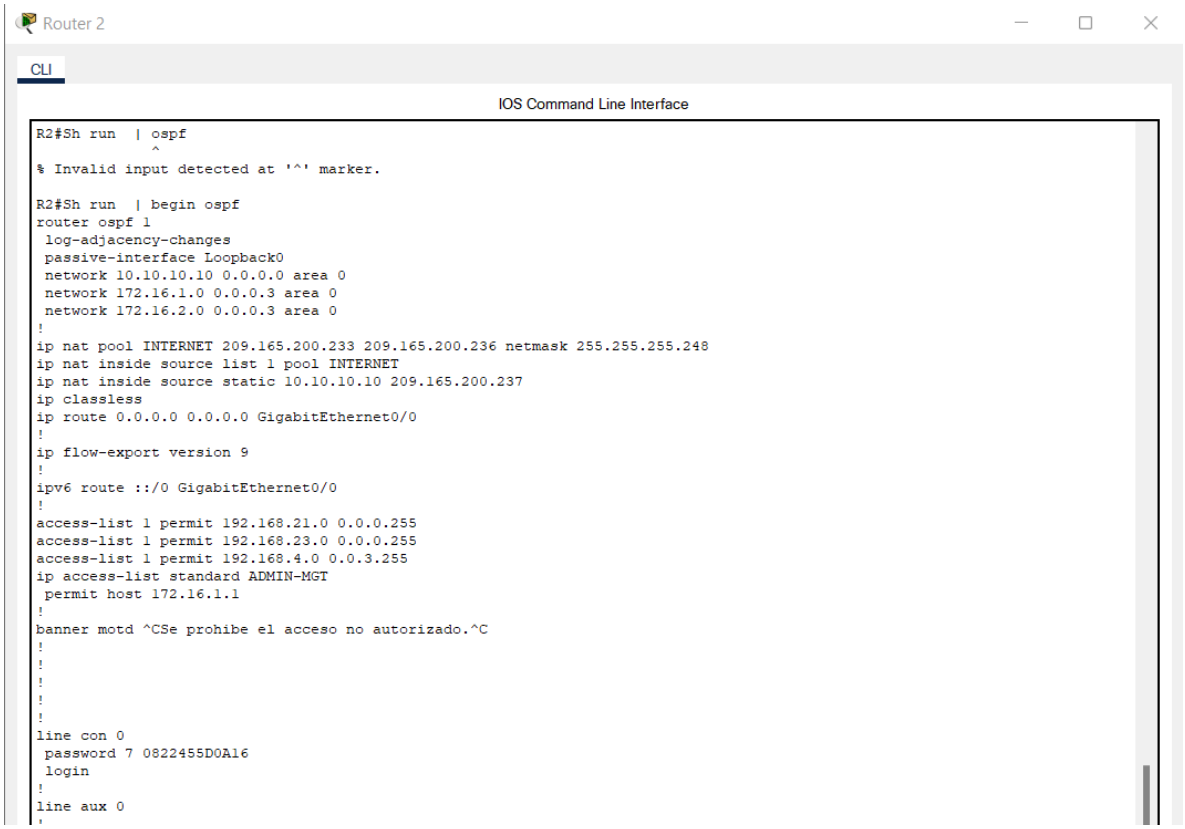
Figura 13 Show ip router



Fuente: autor

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

Figura 14 Show run begin | ospf



Fuente: autor

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

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

ip dhcp excluded-address 192.168.21.1 192.168.21.20 se excluyen estas redes

ip dhcp excluded-address 192.168.23.1 192.168.23.20 se excluyen estas redes

Crear un pool de DHCP para la VLAN 21.

R1(config)#ip dhcp pool ACCT se crea el nombre del pool de direcciones
R1(dhcp-config)#network 192.168.21.0 255.255.255.0 se declara la red

R1(dhcp-config)#domain-name ccna-sa.com se crea al dominio

R1(dhcp-config)#dns-server 10.10.10.10 se declara servidor de DNS
R1(dhcp-config)#default-router 192.168.21.1 se declara el gateway

Crear un pool de DHCP para la VLAN 23

R1(config)#ip dhcp pool ENGNR se crea el nombre del pool de direcciones
R1(dhcp-config)#network 192.168.23.0 255.255.255.0 se declara la red

R1(dhcp-config)#dns-server 10.10.10.10 se declara el servidor DNS

R1(dhcp-config)#domain-name ccna-sa.com se accede al dominio

R1(dhcp-config)#default-router 192.168.23.1 se declara el gateway

R1(dhcp-config)#

Configurar la NAT estática y dinámica en el R2

Crear una base de datos local con una cuenta de usuario

R2(config)#username webuser privilege 15 password cisco12345 se asigna usuario y clave

HR2(config)#ip http server

comando no funciona en el IOS

% Invalid input detected at '^' marker. habilitar el servicio del servidor HTTP packet tracer no recibe este comando

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación

R2(config)#ip http authentication local comando no funciona en el IOS

% Invalid input detected at '^' marker. packet tracer no recibe este comando

Crear una NAT estática al servidor web.

ip nat inside source static 10.10.10.10 209.165.200.233 se crea ip NAT estática

Asignar la interfaz interna y externa para la NAT estática

R2(config)#interface g0/0/0 se accede a la interfaz

R2(config-if)#ip nat outside se declara interfaz de salida

R2(config-if)#interface S0/2/0 se accede a la interfaz

R2(config-if)#ip nat inside se declara interfaz de entrada

R2(config-if)#interface S0/2/1 se accede a la interfaz

R2(config-if)#ip nat inside se declara interfaz de entrada

R2(config-if)#interface loopback 0 se accede a la interfaz

R2(config-if)#ip nat inside se declara de entrada R2(config-if)#

Configurar la NAT dinámica dentro de una ACL privada

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 red q se traduce

R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 red q se traduce

R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255 red q se traduce

R2(config)#

Defina el pool de direcciones IP públicas utilizables.

R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask255.255.255.248 pool de direcciones q se van a usar

R2(config)# ip nat inside source list 1 pool INTERNET se declaran como entrada

Definir la traducción de NAT dinámica

NAT (Network Address Traslation), permite acceder a internet traduciendo las direccones privadas en direcciones ip públicas.

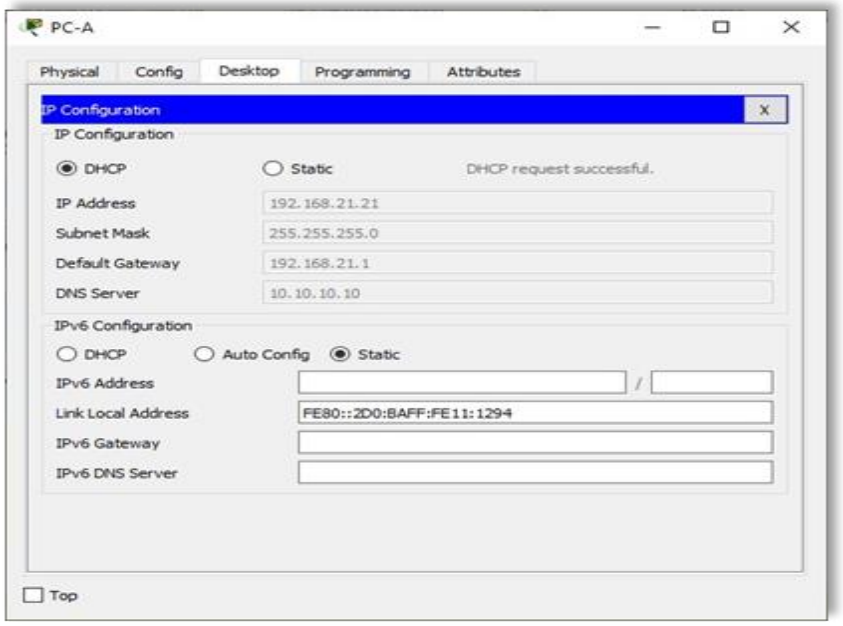
Incrementando la seguridad y la privacidad de la red local al traducir el direccionamiento interno a uno externo.

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.

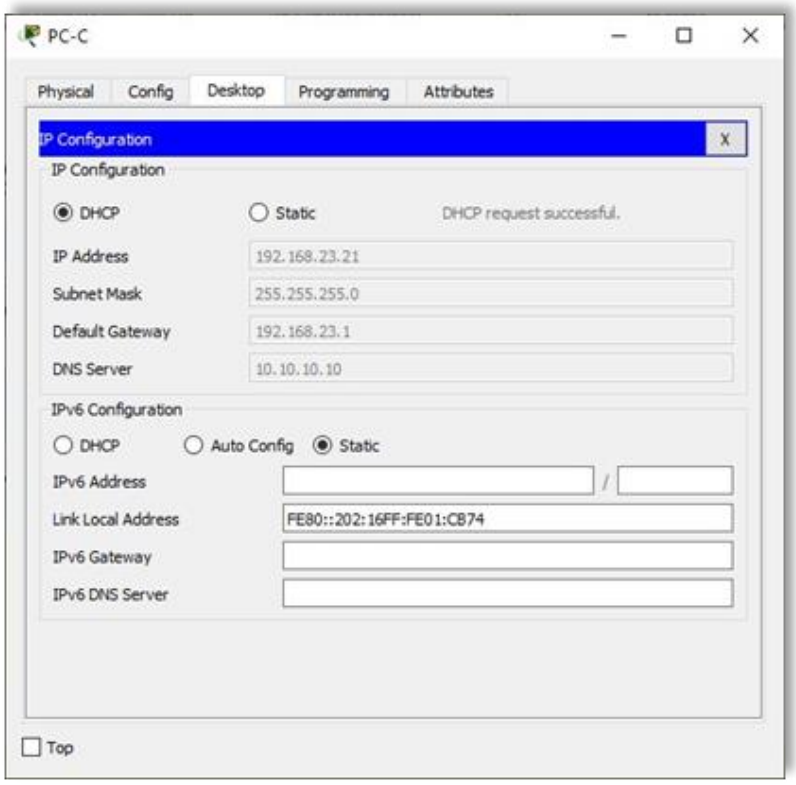
- Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

Figura 15 Información de IP del servidor de DHCP en el PC-A.



Fuente: autor

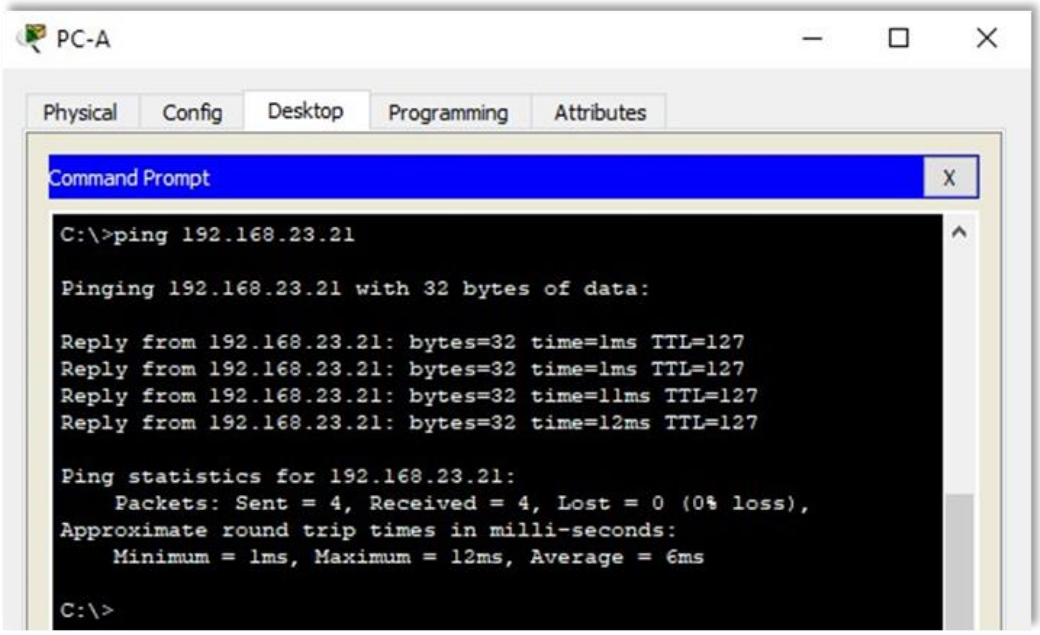
Figura 16 Información de IP del servidor de DHCP en el PC-C



Fuente: autor

- 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 17 Verificación de ping PC-A a la PC-C



Fuente: autor

- 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**

Parte 6: Configurar NTP

- Ajuste la fecha y hora en R2.

R2#clock set 09:00:00 05 march 2016 se configura el set clock

R2#show clock se muestra el set clock 9:6:11.735 UTC Sat Mar 5 2016

Configure R2 como un maestro NTP.

R2#confi termi se accede al modo global Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#ntp master 5 se configura R2 como maestro

Configurar R1 como un cliente NTP.

R1#show clock se muestra el set clock

*6:11:32.929 UTC Mon Mar 1 1993

R1#config termi se accede al modo global Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ntp server 172.16.1.2 se configura R1 como cliente

Configure R1 para actualizaciones de calendario periódicas con hora NTP.

R1(config)#ntp update-calendar se actualiza el calendario

R1(config)#exit se sale

Verifique la configuración de NTP en R1.

R1#show clock muestra el set clock9:22:20.404 UTC Sat Mar 5 2016

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

R2(config)#ip access-list standard ADMIN-MGT crea una lista de acceso standar

R2(config-std-nacl)#permit host 172.16.1.1 se permite esta red

R2(config-std-nacl)#deny any se deniega el resto

R2(config-std-nacl)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed stateto down

10:19:05: %OSPF-5-ADJCHG: Process 58, Nbr 192.168.99.1 on Serial0/2/0 from FULL to DOWN, Neighbor Down: Interface down or detached

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed stateto down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed stateto up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up

10:19:15: %OSPF-5-ADJCHG: Process 58, Nbr 192.168.99.1 on Serial0/2/0 from LOADING to FULL, Loading Done

Aplicar la ACL con nombre a las líneas VTY

R2(config-std-nacl)#exit se sale

R2(config)#line vty 0 4 se accede ala consola de telnet

R2(config-line)#ip access-class ADMIN-MGT in permite que esta red acceda a vty

Permitir acceso por Telnet a las líneas de VTY

transport input telnet accede mediante protocolo telnet

Verificar que la ACL funcione como se espera

R1#telnet 172.16.1.2 telnet a esa ip

Trying 172.16.1.2 ...Opense prohibe el acceso no autorizado User Access Verification

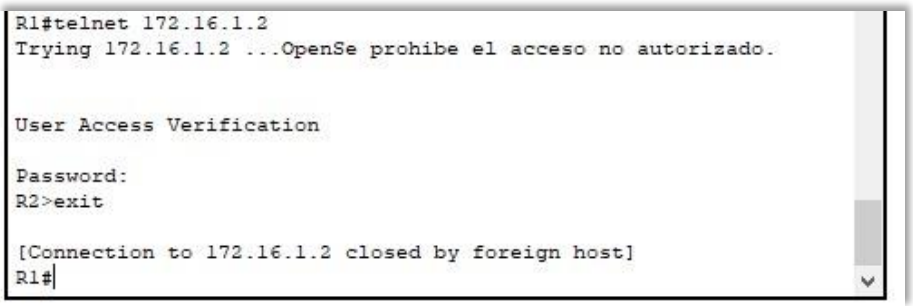
Password:

R2>en

Password:

Password:

Figura 18 Prueba de Telnet de R1 a R2.

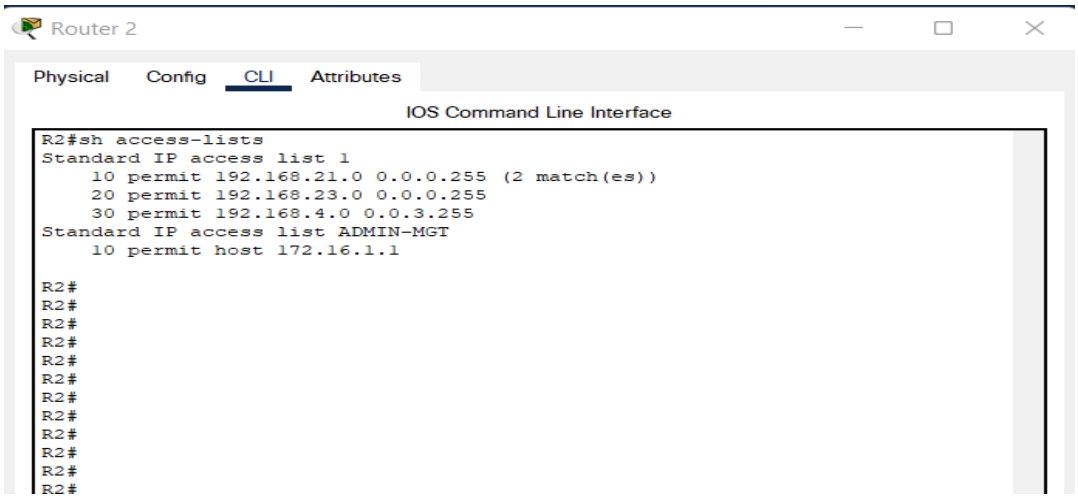


Fuente: autor

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

Figura 19 R2#show access-list



Fuente: autor

- Restablecer los contadores de una lista de acceso

clear access-list counters

R2#clear access-list

countersR2#show access-

list

Figura 20 R2#clear access-list

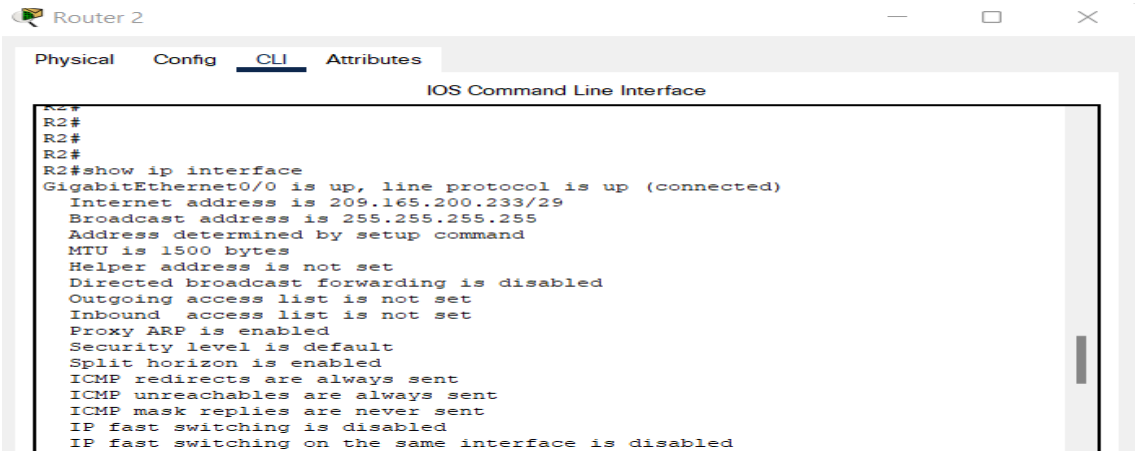
```
R2#clear  access-list counters
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.0.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
    20 deny any
```

Fuente: autor

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

Show ip interface

Figura 21 R2#show ip interface



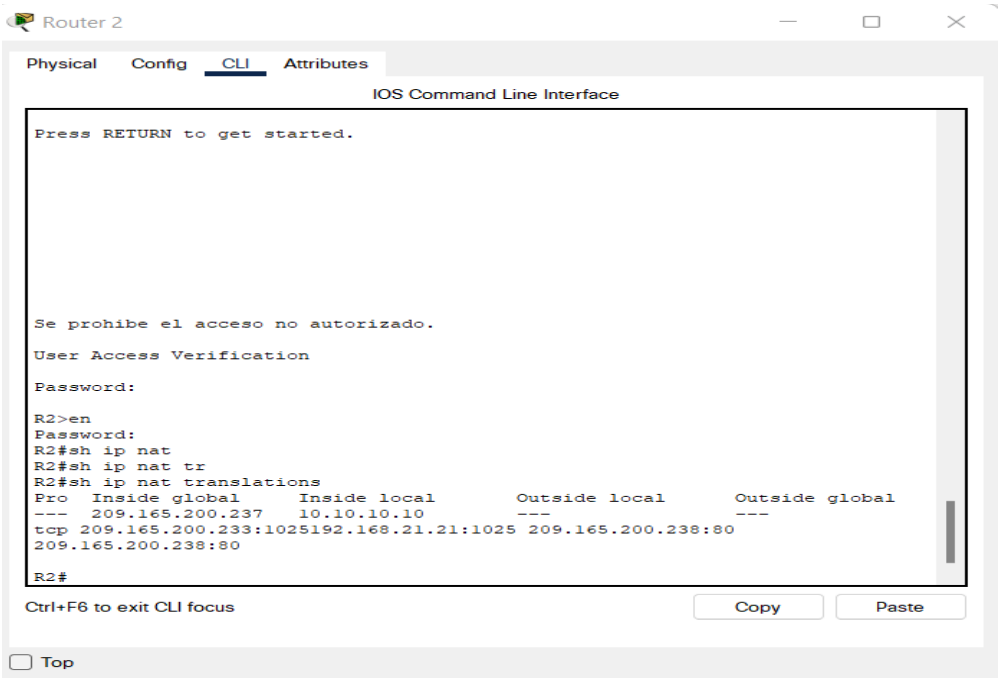
Fuente: Autor

- ¿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.

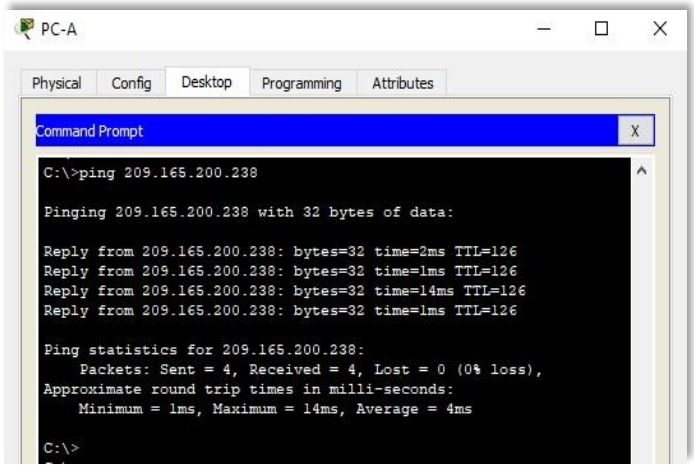
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
Tcp 209.165.200.237:80 10.10.10.10:80
209.165.200.238:1033209.165.200.238:1033

Figura 22 Ver las traducciones NAT en el R2



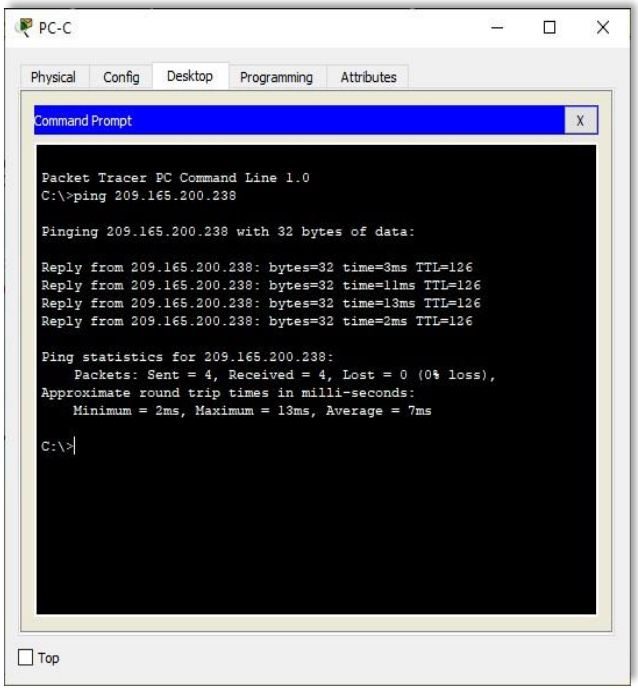
Fuente: autor

Figura 23 Prueba de ping al Servidor de Internet desde la PC-A.



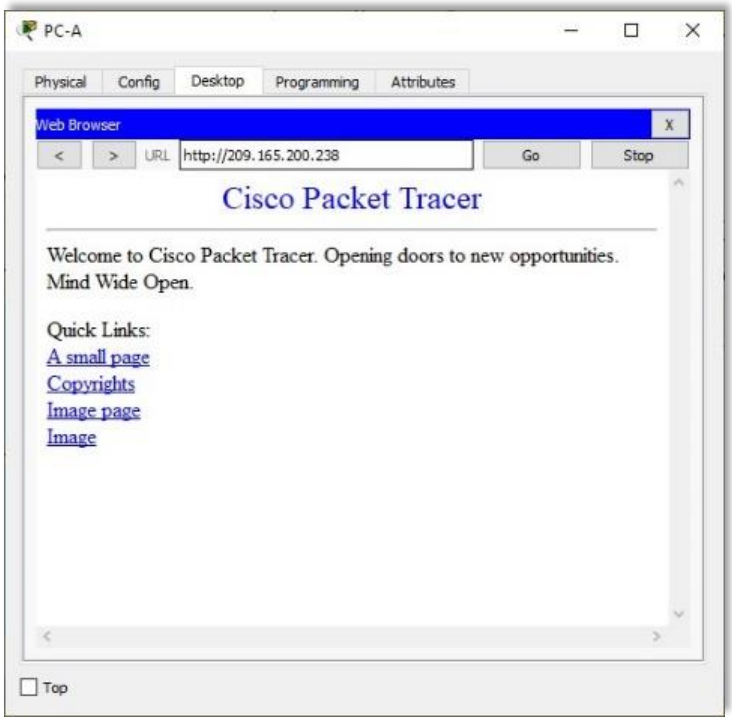
Fuente: autor

Figura 24 Prueba de ping al Servidor de Internet desde la PC-C.



Fuente: autor

Figura 25 Prueba de acceso al Servidor de Web desde PC-A



Fuente: autor

¿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 26 Eliminar las traducciones de NAT dinámicas.

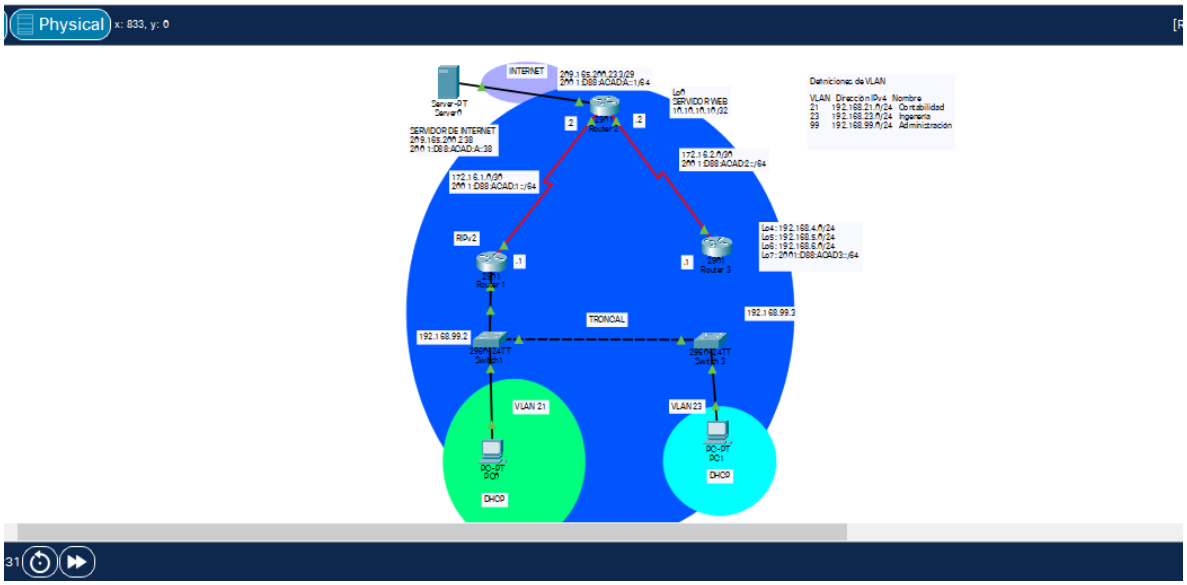
```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.237   10.10.10.10        ---                ---
tcp 209.165.200.233:1025192.168.23.21:1025 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.234:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
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#
```

Fuente: autor

Figura 27 Topología de red escenario 2 - Cisco Packet Tracer.



Fuente: autor

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

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

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

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

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

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

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. Inge Cuc, 12(1), 86-93.

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.