SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

MAURICIO MEJIA ESTEVEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

BARRANCABERMEJA

2020

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

MAURICIO MEJIA ESTEVEZ

Diplomado de profundización CISCO (Diseño e implementación de soluciones integradas LAN / WAN)

Director /Tutor

Juan Carlos Vesga

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

BARRANCABERMEJA

2020

**NOTA DE ACEPTACIÓN:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firma del presidente del jurado

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firma del jurado

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firma del jurado

Barrancabermeja (mayo 22, 2020)

**DEDICATORIA**

Dios y mi familia.

**AGRADECIMIENTO**

Mi agradecimiento a la Universidad Nacional Abierta y a Distancia – UNAD.

Institucion de educación superior que me brindó la oportunidad a través del programa de Ingenieria de Sistemas de la Escuela de Ciencias Básicas, Tecnología e Ingeniería, ser un profesional competente en la industria.

En general, a todas las institiciones, organismos, archivos, bibliotecas, que de alguna manera contribuyeron a facilitarme acceso a la información requerida para alcanzar los objetivos.

En especial, a Dios y mi familia por el apoyo incodicional.

**CONTENIDO**

[INTRODUCCION 12](#_Toc39678327)

[OBJETIVOS 13](#_Toc39678328)

[General 13](#_Toc39678329)

[Especificos 13](#_Toc39678330)

[ESCENARIO 1 14](#_Toc39678331)

[Parte 1: Inicializar dispositivos 15](#_Toc39678332)

[Paso 1. Inicializar y volver a cargar los routers y los switches. 15](#_Toc39678333)

[Parte 2: Configurar los parámetros básicos de los dispositivos 29](#_Toc39678334)

[Paso 1: Configurar la computadora de Internet. 29](#_Toc39678335)

[Paso 2: Configurar R1. 31](#_Toc39678336)

[Paso 3: Configurar R2. 33](#_Toc39678337)

[Paso 4: Configurar R3. 36](#_Toc39678338)

[Paso 5: Configurar S1. 39](#_Toc39678339)

[Paso 6: Configurar S3. 40](#_Toc39678340)

[Paso 7: Verificar la conectividad de la red. 41](#_Toc39678341)

[Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 43](#_Toc39678342)

[Paso 1: Configurar S1 43](#_Toc39678343)

[Paso 2: Configurar el S3. 46](#_Toc39678344)

[Paso 3: Configurar R1 49](#_Toc39678345)

[Paso 4: Verificar la conectividad de la red 51](#_Toc39678346)

[Parte 4: Configurar el protocolo de routing dinámico RIPv2 53](#_Toc39678347)

[Paso 1: Configurar RIPv2 en el R1. 53](#_Toc39678348)

[Paso 2: Configurar RIPv2 en el R2. 54](#_Toc39678349)

[Paso 3: Configurar RIPv2 en el R2. 55](#_Toc39678350)

[Paso 4: Verificar la información de RIP. 56](#_Toc39678351)

[Parte 5: Implementar DHCP y NAT para Ipv4 56](#_Toc39678352)

[Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23. 56](#_Toc39678353)

[Paso 2: Configurar la NAT estática y dinámica en el R2. 57](#_Toc39678354)

[Paso 3: Verificar el protocolo DHCP y la NAT estática. 59](#_Toc39678355)

[Parte 6: Configurar NTP. 64](#_Toc39678356)

[Parte 7: Configurar y verificar las listas de control de acceso (ACL) 65](#_Toc39678357)

[Paso 1: Restringir el acceso a las líneas VTY en el R2. 65](#_Toc39678358)

[Paso 2: Introducir el comando de CLI . 66](#_Toc39678359)

[ESCENARIO 2 77](#_Toc39678360)

[Parte 1: Configuración del enrutamiento 87](#_Toc39678361)

[Parte 2: Tabla de Enrutamiento 91](#_Toc39678362)

[Parte 3: Deshabilitar la propagación del protocolo OSPF 99](#_Toc39678363)

[Parte 4: Verificación del protocolo OSPF. 100](#_Toc39678364)

[Parte 5: Configurar encapsulamiento y autenticación PPP 108](#_Toc39678365)

[Parte 6: Configuración de PAT 109](#_Toc39678366)

[Parte 7: Configuración del servicio DHCP 112](#_Toc39678367)

[Parte adicional: Guardar los cambios 117](#_Toc39678368)

[CONCLUSIONES 120](#_Toc39678369)

[BIBLIOGRAFÍA 121](#_Toc39678370)

**LISTA DE FIGURAS**

[Fígura 1. Topología de red escenario 1. 14](#_Toc40888423)

[Fígura 2. Configuración IP del servidor de Internet. 31](#_Toc40888424)

[Fígura 3. Prueba de ping desde R1 a R2 41](#_Toc40888425)

[Fígura 4. Prueba de ping desde R2 a R3 42](#_Toc40888426)

[Fígura 5. Prueba de ping desde Servidor de Internet a Gateway predeterminado 42](#_Toc40888427)

[Fígura 6. Prueba de ping desde S1 a R1, dirección VLAN 99 51](#_Toc40888428)

[Fígura 7. Prueba de ping desde S3 a R1, dirección VLAN 99. 52](#_Toc40888429)

[Fígura 8. Prueba de ping desde S1 a R1, dirección VLAN 21 52](#_Toc40888430)

[Fígura 9. Prueba de ping desde S3 a R1, dirección VLAN 23 52](#_Toc40888431)

[Fígura 10. Ver las redes conectadas directamente en R1 54](#_Toc40888432)

[Fígura 11. Ver las redes conectadas directamente en R2 55](#_Toc40888433)

[Fígura 12. Ver las redes conectadas directamente en R3 56](#_Toc40888434)

[Fígura 13. Información de IP del servidor de DHCP en el PC-A 60](#_Toc40888435)

[Fígura 14. Información de IP del servidor de DHCP en el PC-C 61](#_Toc40888436)

[Fígura 15. Verificación de ping PC-A a la PC-C 62](#_Toc40888437)

[Fígura 16. Acceso Servidor Web desde el Servidor de Internet 63](#_Toc40888438)

[Fígura 17. Prueba de Telnet de R1 a R2 66](#_Toc40888439)

[Fígura 18. Prueba de Telnet de R3 a R2 66](#_Toc40888440)

[Fígura 19. Ver las las traducciones NAT en el R3 71](#_Toc40888441)

[Fígura 20. Prueba de ping al Servidor de Internet desde la PC-A 71](#_Toc40888442)

[Fígura 21. Prueba de ping al Servidor de Internet desde la PC-C 72](#_Toc40888443)

[Fígura 22. Prueba de acceso al Servidor de Web desde PC-A 73](#_Toc40888444)

[Fígura 23. Prueba de acceso al Servidor de Web desde PC-C 74](#_Toc40888445)

[Fígura 24. Eliminar las traducciones de NAT dinámicas 75](#_Toc40888446)

[Fígura 25. Topología de red del escenario – Cisco Packet Tracer 76](#_Toc40888447)

[Fígura 26. Topología de red escenario 2 77](#_Toc40888448)

[Fígura 27. Show ip route en Router Medellin1. 92](#_Toc40888449)

[Fígura 28. Show ip route en Router Medellin2 93](#_Toc40888450)

[Fígura 29. Show ip route en Router Medellin3 94](#_Toc40888451)

[Fígura 30. Show ip route en Router Bogota1 95](#_Toc40888452)

[Fígura 31. Show ip route en Router Bogota2 96](#_Toc40888453)

[Fígura 32. Show ip route en Router Bogota3 97](#_Toc40888454)

[Fígura 33. Show ip route en Router ISP 98](#_Toc40888455)

[Fígura 34. Show ip route protocols en Router Medellin1 101](#_Toc40888456)

[Fígura 35. Show ip route protocols en Router Medellin2 102](#_Toc40888457)

[Fígura 36. Show ip route protocols en Router Medellin3. 103](#_Toc40888458)

[Fígura 37. Show ip route protocols en Router Bogota1 104](#_Toc40888459)

[Fígura 38. Show ip route protocols en Router Bogota2 105](#_Toc40888460)

[Fígura 39. Show ip route protocols en Router Bogota3 106](#_Toc40888461)

[Fígura 40. Show ip route protocols en Router ISP 107](#_Toc40888462)

[Fígura 41. Prueba de ping de Medellin1 a Medellin2 y Medellin3 111](#_Toc40888463)

[Fígura 42 Prueba de ping de Bogota1 a Bogota2 y Bogota3 111](#_Toc40888464)

[Fígura 43. Configuración IP PC1\_Med 113](#_Toc40888465)

[Fígura 44. Configuración IP PC2\_Med 114](#_Toc40888466)

[Fígura 45. Configuración IP PC1\_Bog 116](#_Toc40888467)

[Fígura 46. Configuración IP PC2\_Bog 117](#_Toc40888468)

[Fígura 47. Topologia de red escenario 2 - Cisco Packet Tracer 119](#_Toc40888469)

**LISTA DE TABLAS**

[Tabla 1. Direccionamiento IP Servidor de Internet 29](#_Toc40888470)

[Tabla 2 .Ipv4 Subnet 29](#_Toc40888471)

[Tabla 3. Ipv6 Subnet 30](#_Toc40888472)

[Tabla 4 .Verificar la conectividad de la red 41](#_Toc40888473)

[Tabla 5. Verificar la conectividad de los dispositivos 51](#_Toc40888474)

[Tabla 6 . Especificaciones de la topologia de red 81](#_Toc40888475)

[Tabla 7. Interfaces de los Router 99](#_Toc40888476)

**RESUMEN**

La Universidad Nacional Abierta y a Distancia, durante el proceso de aprendizaje del diplomado de profundización CISCO (diseño e implementación de soluciones integradas LAN / WAN) utilizando el software de simulación Cisco Packet Tracer, el cual es un programa que nos permite realizar la simulación de las redes, se busca experimentar los diferentes parámetros de configuración de una topología de red.

En el desarrollo de los módulos CCNA1 (CCNA R&S: Introduction to Networks) y CCNA2 (CCNA R&S: Routing and Switching Essentials), se obtiene las bases teóricas y practicas de laboratorio para el aprendizaje de la tecnología. Con los conocimientos obtenidos y puestos en práctica se busca obtener el desarrollo de la actividad final como prueba de habilidades, donde mediante los escenarios propuestos se coloca en habilidad los conocimientos previamente aprendidos realizando configuraciones como: IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2 y 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, encapsulamiento PPP y su autenticación.

Durante la realización de las configuraciones, se probará y registrará la red mediante el uso de comandos en la Interfaz de línea de comandos (CLI) y algunos ajustes usando la interfaz grafica de los dispositivos.

# INTRODUCCIÓN

La necesidad de tener personal capacitado, competitivo, idóneo en el campo laboral ha sido una de los objetivos más importantes hoy en día para el mercado laboral, porque deben a su vez contar con las competencias necesarias para desarrollar actividades relacionas con las tecnologías de la información y la comunicación. Es ahí donde la certificación CCNA permite dar a conocer las habilidades necesarias para trabajar y emplear soluciones de red en el mundo real.

Durante el desarrollo del diplomado de profundización Cisco (diseño e implementación de soluciones integradas LAN/WAN), se busca que como futuro profesional en la rama obtener conocimientos y experiencias aplicando soluciones de estudios de caso bajo el uso de tecnología Cisco usando el software de simualción Cisco Packet Tracer.

# OBJETIVOS

## General

Fomentar en el estudiante la capacidad de configurar y administrar dispositivos de Networking orientados al diseño de redes escalables y de conmutación usando tecnologia Cisco.

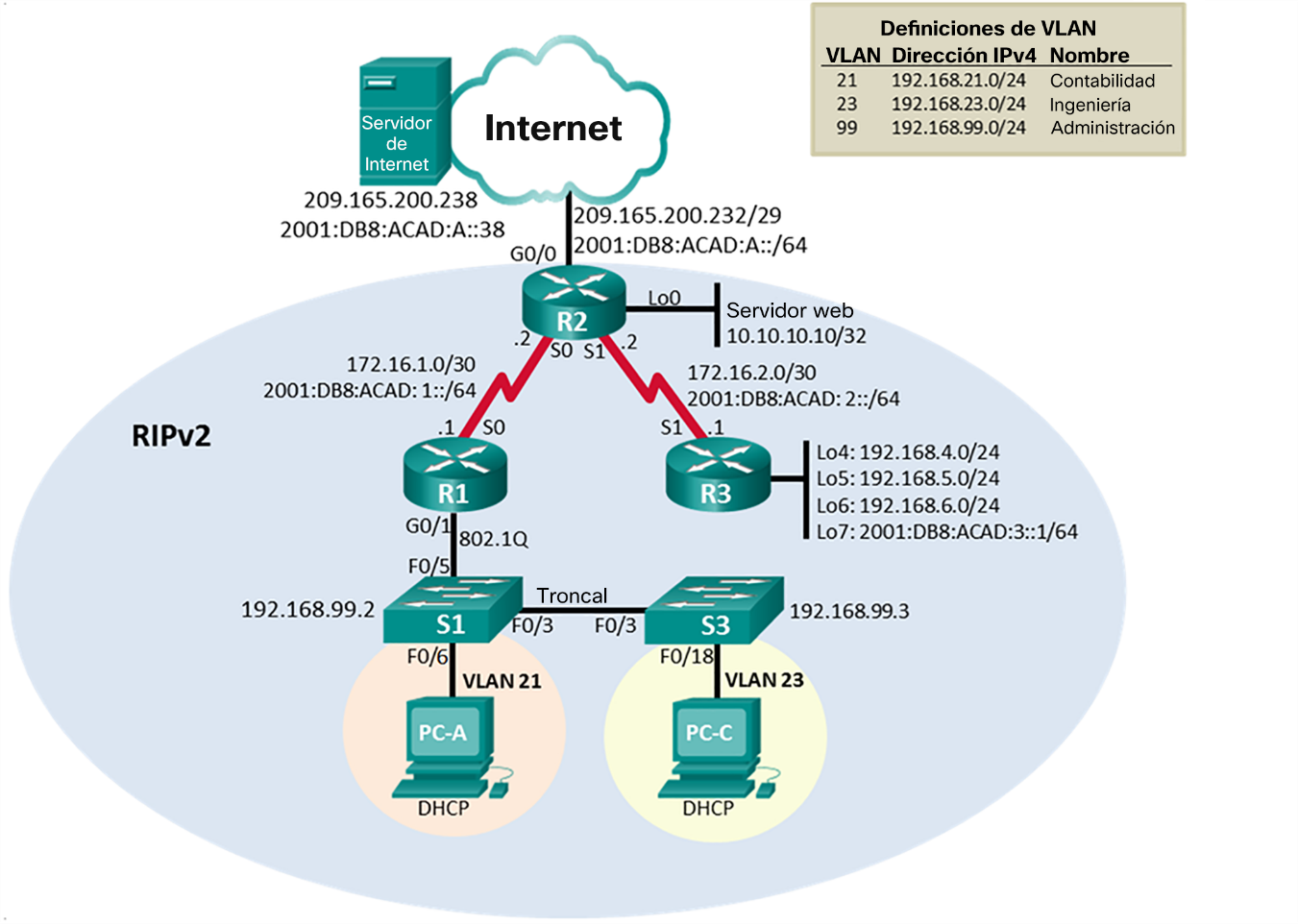
## Especificos

* Emplear comandos de configuración en dispositovos de red mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.
* Utilizar herramientas de simulación y laboratorios con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.
* Configurar esquemas de conmutación soportadas en Switches, mediante el uso de protocolos basados en STP y VLANs en escenarios corporativos.

# ESCENARIO 1

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e Ipv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Fígura 1. Topología de red escenario 1.



Fuente: Prueba de habilidades CCNA 2020, 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

Press RETURN to get started!

Router>

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

Press RETURN to get started!

Router>

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

Press RETURN to get started!

Router>

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#

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

Switch>

Switch#reload

Proceed with reload? [confirm]

C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.

2960-24TT starting...

Base ethernet MAC Address: 00E0.F949.C97D

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 : 00E0.F949.C97D

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 FastEthernet0/18, changed state to up

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

Switch>

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 1. Direccionamiento IP Servidor de Internet

|  |  |
| --- | --- |
| Elemento o tarea de configuración | Especificación |
| Dirección Ipv4 | 209.165.200.238 |
| Máscara de subred para Ipv4 | 255.255.255.248 |
| Gateway predeterminado | 209.165.200.233 |
| Dirección Ipv6/subred | 2001:db8:acad:a::38/64 |
| Gateway predeterminado Ipv6 | 2001:db8:acad:a::1 |

Fuente: Autor.

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

Tabla 2 .Ipv4 Subnet

|  |  |
| --- | --- |
| IP 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 Hosts: | 6 |
| Subnet Mask: | 255.255.255.248 |
| Wildcard Mask: | 0.0.0.7 |
| Binary Subnet Mask: | 11111111.11111111.11111111.11111000 |
| IP Type: | PUBLIC IP – CLASS C |

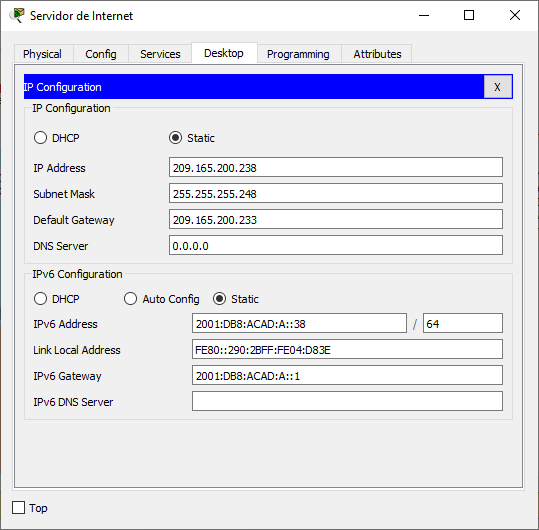
Fuente: Autor.

Tabla 3. Ipv6 Subnet

|  |  |
| --- | --- |
| IP Address: | 2001:db8:acad: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 / 64 |
| 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.

Fígura 2. Configuración IP del servidor de Internet.



Fuente: Autor.

## 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 prohibe 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 prohibe el acceso no autorizado.)

Interfaz S0/0/0

* Establezca la descripción
* Establezca la dirección Ipv4. Utilizar la siguiente dirección disponible en la subred.
* Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones.
* Activar la interfaz

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

Interfaz G0/0 (simulación de Internet)

* Establecer la descripción.
* Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.
* Establezca la dirección Ipv6. Utilizar la primera dirección disponible en la subred.
* Activar la interfaz

Interfaz loopback 0 (servidor web simulado)

* Establecer la descripción.
* Establezca la dirección Ipv4.

Ruta predeterminada

* Configure una ruta Ipv4 predeterminada de G0/0.
* Configure una ruta Ipv6 predeterminada de G0/0.

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

^

% Invalid input detected at ‘^’ marker.

R2(config)#banner motd %Se prohibe el acceso no autorizado.%

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 suarioo n Interface Serial0/0/0, changed state to up

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

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 suarioo n Interface GigabitEthernet0/0, changed state to up

R2(config-if)#int loopback 0

R2(config-if)#

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

%LINEPROTO-5-UPDOWN: Line suarioo n 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

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0

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

R2(config)#ipv6 route ::/0 g0/0

R2(config)#

**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 suario el acceso no autorizado.)

Interfaz S0/0/1

* Establecer la descripción.
* Establezca la dirección Ipv4. Utilizar la siguiente dirección disponible en la subred.
* Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones.
* Activar la interfaz.

Interfaz loopback 4

* Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.

Interfaz loopback 5

* Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.

Interfaz loopback 6

* Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.

Interfaz loopback 7

* Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones.

Rutas predeterminadas

* Configure una ruta Ipv4 predeterminada S0/0/1.
* Configure una ruta Ipv6 predeterminada S0/0/1.

Router>enable

Router#configure terminal

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

Router(config)#no ip domain-lookup

Router(config)#hostname R3

R3(config)#enable secret class

R3(config)#line console 0

R3(config-line)#password cisco

R3(config-line)#login

R3(config-line)#line vty 0 15

R3(config-line)#password cisco

R3(config-line)#login

R3(config-line)#service password-encryption

R3(config)#banner motd %Se prohibe el acceso no autorizado.%

R3(config)#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 suarioo n Interface Serial0/0/1, changed state to up

R3(config-if)#int loopback 4

R3(config-if)#

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

%LINEPROTO-5-UPDOWN: Line suarioo n Interface Loopback4, changed state to up

R3(config-if)#ip address 192.168.4.1 255.255.255.0

R3(config-if)#int loopback 5

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line suarioo n Interface Loopback5, changed state to up

R3(config-if)#ip address 192.168.5.1 255.255.255.0

R3(config-if)#int loopback 6

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line suarioo n Interface Loopback6, changed state to up

R3(config-if)#ip address 192.168.6.1 255.255.255.0

R3(config-if)#int loopback 7

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback7, changed state to up

%LINEPROTO-5-UPDOWN: Line suarioo n 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 suario, if not a point-to-point interface, may impact 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 prohibe 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 prohibe el acceso no autorizado.%

S1(config)#

## Paso 6: Configurar S3.

La configuración del S3 incluye las siguientes tareas:

Desactivar la búsqueda DNS

Nombre del switch (S3)

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 prohibe 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 prohibe 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:

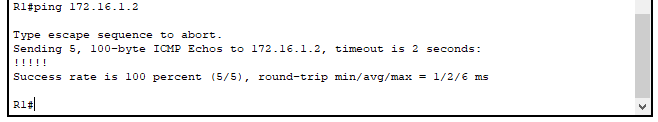
Tabla 4 .Verificar la conectividad de la red

|  |  |  |  |
| --- | --- | --- | --- |
| 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 predeterminado | 209.165.200.233 | Success |

Fuente: Autor.

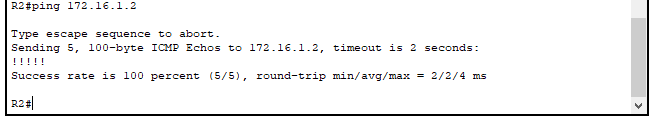
**Nota:** Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Fígura 3. Prueba de ping desde R1 a R2



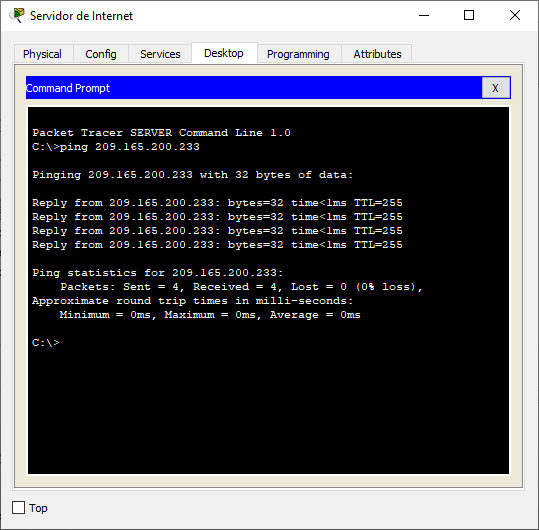
Fuente: Autor.

Fígura 4. Prueba de ping desde R2 a R3



Fuente: Autor.

Fígura 5. 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

* 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

%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

S1(config-if-range)#

## 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 21

S3(config-vlan)#name Contabilidad

S3(config-vlan)#vlan 23

S3(config-vlan)#name Ingenieria

S3(config-vlan)#vlan 99

S3(config-vlan)#name Administracion

S3(config-vlan)#exit

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.

Configurar la subinterfaz 802.1Q .23 en G0/1

* Descripción: LAN de Ingeniería.
* Asignar la VLAN 23.
* Asignar la primera dirección disponible a esta interfaz.

Configurar la subinterfaz 802.1Q .99 en G0/1

* Descripción: LAN de Administración
* Asignar la VLAN 99
* Asignar la primera dirección disponible a esta interfaz

Activar la interfaz G0/1

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

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

R1(config-subif)#int g0/1.99

R1(config-subif)#description LAN de Administracion

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 protocol on Interface GigabitEthernet0/1, changed state to up

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

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

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

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

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

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

R1(config-if)#

## Paso 4: Verificar la conectividad de la red

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

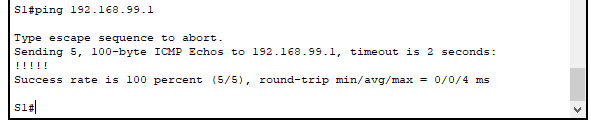
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 5. 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 |

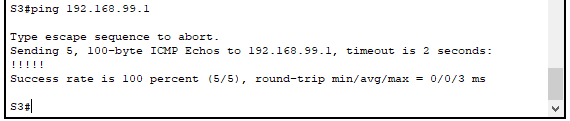
Fuente: Autor

Fígura 6. Prueba de ping desde S1 a R1, dirección VLAN 99



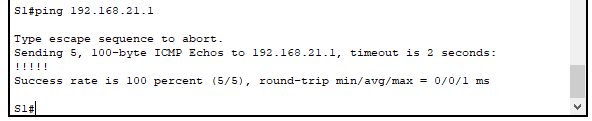
Fuente: Autor

Fígura 7. Prueba de ping desde S3 a R1, dirección VLAN 99.



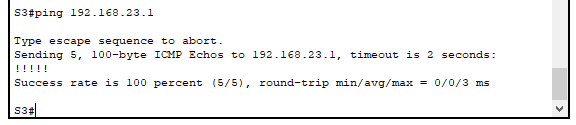
Fuente: Autor

Fígura 8. Prueba de ping desde S1 a R1, dirección VLAN 21



Fuente: Autor

Fígura 9. Prueba de ping desde S3 a R1, dirección VLAN 23

.

Fuente: Autor

## Parte 4: Configurar el protocolo de routing dinámico RIPv2

## Paso 1: Configurar RIPv2 en el R1.

Las tareas de configuración para R1 incluyen las siguientes:

Configurar RIP versión 2

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 rip

R1(config-router)#version 2

R1(config-router)#do show ip route connected

C 172.16.1.0/30 is directly connected, Serial0/0/0

C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21

C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23

C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99

R1(config-router)#network 172.16.1.0

R1(config-router)#network 192.168.21.0

R1(config-router)#network 192.168.23.0

R1(config-router)#network 192.168.99.0

R1(config-router)#passive-interface g0/1.21

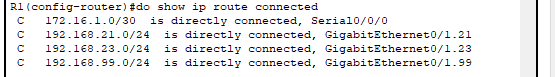
R1(config-router)#passive-interface g0/1.23

R1(config-router)#passive-interface g0/1.99

R1(config-router)#no auto-summary

R1(config-router)#

Fígura 10. Ver las redes conectadas directamente en R1



Fuente: Autor

## Paso 2: Configurar RIPv2 en el R2.

La configuración del R2 incluye las siguientes tareas:

Configurar RIP versión 2

Anunciar las redes conectadas directamente

* **Nota:** Omitir la red G0/0.

Establecer la interfaz LAN (loopback) como pasiva

Desactive la sumarización automática

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#do show ip route connected

C 10.10.10.10/32 is directly connected, Loopback0

C 172.16.1.0/30 is directly connected, Serial0/0/0

C 172.16.2.0/30 is directly connected, Serial0/0/1

C 209.165.200.232/29 is directly connected, GigabitEthernet0/0

R2(config-router)#network 10.10.10.10

R2(config-router)#network 172.16.1.0

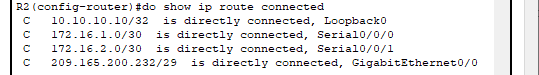
R2(config-router)#network 172.16.2.0

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

R2(config-router)#no auto-summary

R2(config-router)#

Fígura 11. Ver las redes conectadas directamente en R2



Fuente: Autor

## Paso 3: Configurar RIPv2 en el R2.

La configuración del R3 incluye las siguientes tareas:

Configurar RIP versión 2

Anunciar redes Ipv4 conectadas directamente

Establecer todas las interfaces de LAN Ipv4 (Loopback) como pasivas

Desactive la sumarización automática

R3(config)#router rip

R3(config-router)#version 2

R3(config-router)# do show ip route connected

C 172.16.2.0/30 is directly connected, Serial0/0/1

C 192.168.4.0/24 is directly connected, Loopback4

C 192.168.5.0/24 is directly connected, Loopback5

C 192.168.6.0/24 is directly connected, Loopback6

R3(config-router)#network 172.16.2.0

R3(config-router)#network 172.16.4.0

R3(config-router)#network 172.16.5.0

R3(config-router)#network 172.16.6.0

R3(config-router)#passive-interface loopback 4

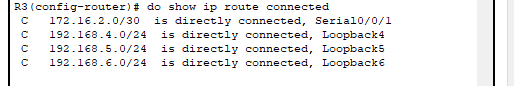
R3(config-router)#passive-interface loopback 5

R3(config-router)#passive-interface loopback 6

R3(config-router)#no auto-summary

R3(config-router)#

Fígura 12. Ver las redes conectadas directamente en R3



Fuente: Autor

## Paso 4: Verificar la información de RIP.

Verifique que RIP 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 RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?

Show ip protocols

¿Qué comando muestra solo las rutas RIP?

Show ip route rip

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

Show run

## 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

Crear un pool de DHCP para la VLAN 23

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

R1(config)#ip dhcp 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 ENGNR

R1(dhcp-config)#network 192.168.23.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.23.1

R1(dhcp-config)#dns-server 10.10.10.10

R1(dhcp-config)#ip domain-name ccna-sa.com

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 suario: 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

Crear una NAT estática al servidor web

* Dirección global interna: 209.165.200.237

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: 209.165.200.233 – 209.165.200.236

Definir la traducción de NAT dinámica

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.

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

R2(config)#int g0/0

R2(config-if)#ip nat outside

R2(config-if)#int s0/0/0

R2(config-if)#ip nat inside

R2(config-if)#int s0/0/1

R2(config-if)#ip nat inside

R2(config-if)#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 255.255.255.248

R2(config)#ip nat inside source list 1 pool INTERNET

R2(config)#

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

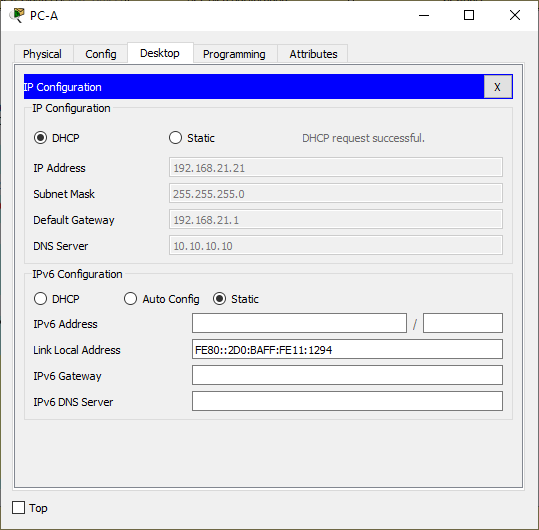
* ip http server
* ip http authentication local
* ip http secure-server

## 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

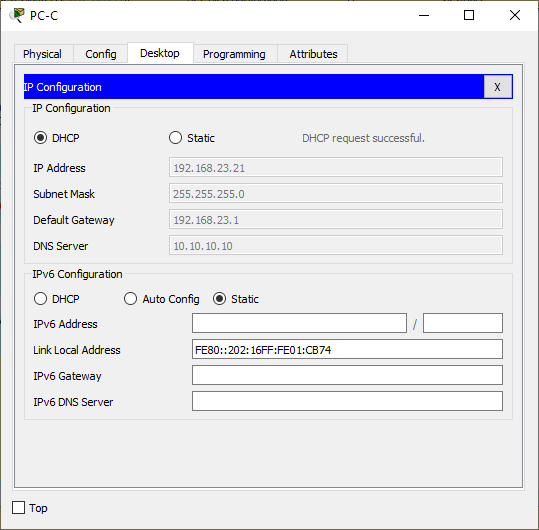
Fígura 13. Información de IP del servidor de DHCP en el PC-A



Fuente: Autor

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

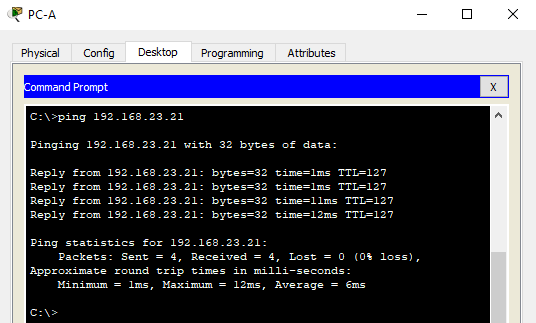
Fígura 14. Información de IP del servidor de DHCP en el PC-C



Fuente: Autor

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

Fígura 15. Verificación de ping PC-A a la PC-C

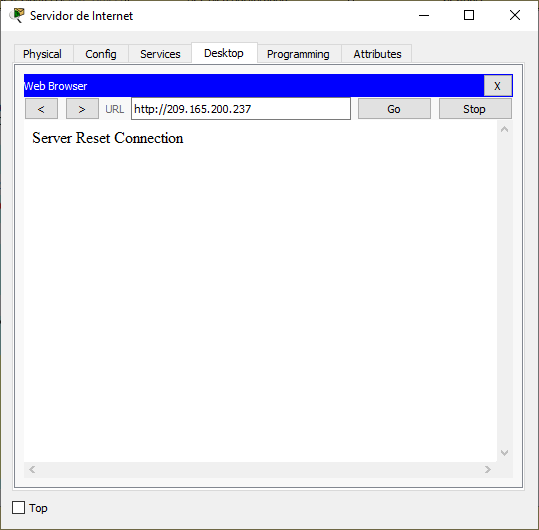


Fuente: Autor

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

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

Fígura 16. Acceso Servidor Web desde el Servidor de Internet



Fuente: Autor

**Nota:** Server Reset Connection. La conexión del Servidor Web no responde porque Packet tracer no soportó el comando ip http server en R2 para activar el servicio.

## Parte 6: Configurar NTP.

Ajuste la fecha y hora en R2 ( 30 de abril de 2020, 12:40 a. m.)

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

Configure R2 como un maestro NTP (Nivel de estrato: 5)

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 prohibe el acceso no autorizado.

User Access Verification

Password:

R2>exit

[Connection to 172.16.1.2 closed by foreign host]

R1#

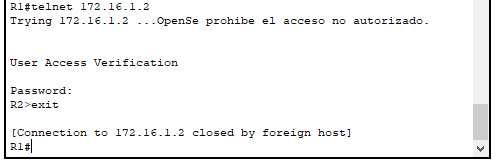
R3#telnet 172.16.1.2

Trying 172.16.1.2 …

% Connection refused by remote host

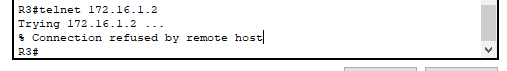
R3#

Fígura 17. Prueba de Telnet de R1 a R2



Fuente: Autor

Fígura 18. Prueba de Telnet de R3 a R2



Fuente: Autor

## Paso 2: Introducir el comando de CLI .

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

^

% Invalid input detected at ‘^’ marker.

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#

**Nota:** Este comando no es compatible con Packet Tracer.

¿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 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

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 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

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 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

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

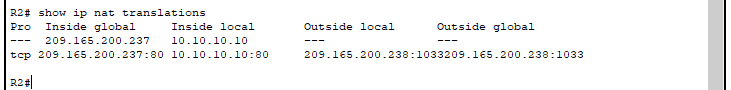
Pro Inside global Inside local Outside local Outside global

--- 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

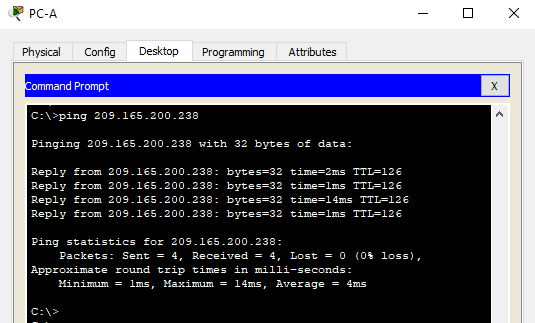
R2#

Fígura 19. Ver las las traducciones NAT en el R3



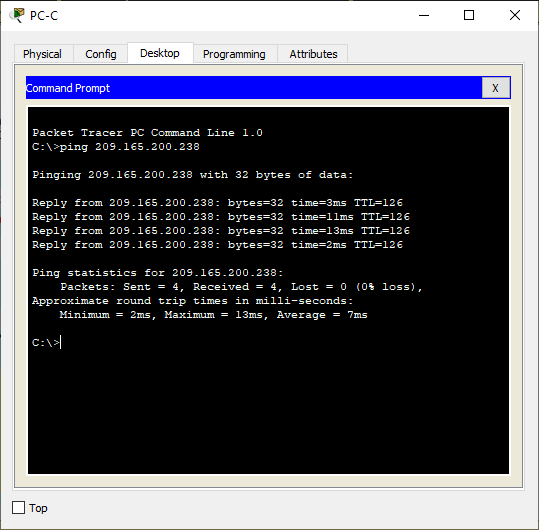
Fuente: Autor

Fígura 20. Prueba de ping al Servidor de Internet desde la PC-A



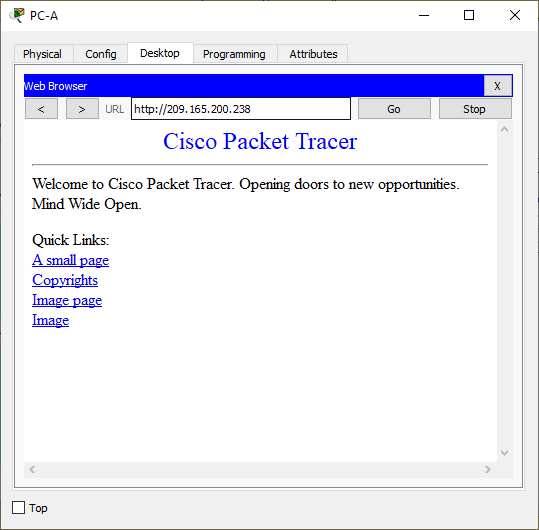
Fuente: Autor

Fígura 21. Prueba de ping al Servidor de Internet desde la PC-C



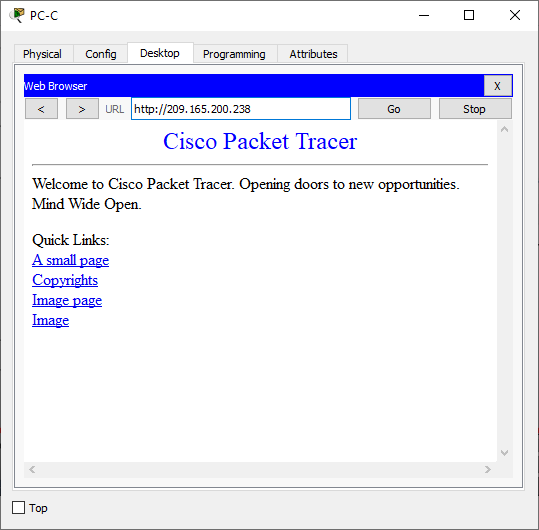
Fuente: Autor

Fígura 22. Prueba de acceso al Servidor de Web desde PC-A



Fuente: Autor

Fígura 23. Prueba de acceso al Servidor de Web desde PC-C



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 \*

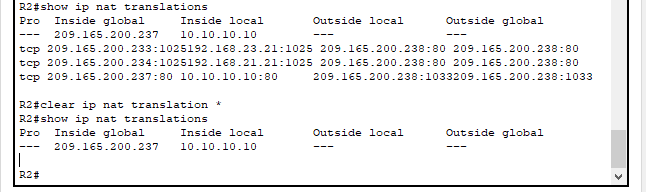
R2#show ip nat translations

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.237 10.10.10.10 --- ---

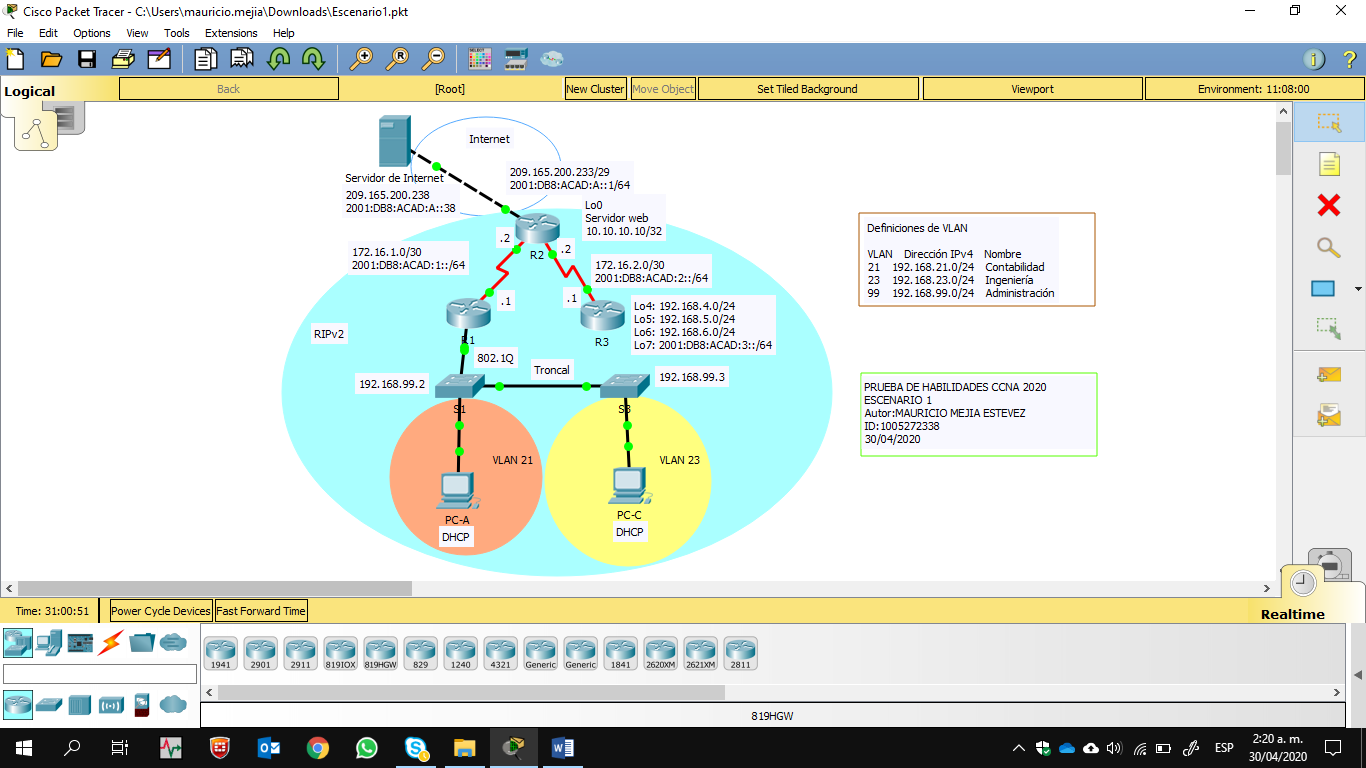
R2#

Fígura 24. Eliminar las traducciones de NAT dinámicas



Fuente: Autor

Fígura 25. Topología de red del escenario – Cisco Packet Tracer

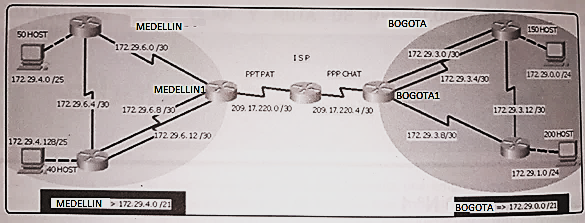


Fuente: Autor

# ESCENARIO 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Fígura 26. Topología de red escenario 2



Fuente: Prueba de habilidades CCNA 2020, Cisco Academy.

Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendran rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

* Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

Router>enable

Router#configure terminal

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

Router(config)#hostname ISP

ISP(config)#enable secret class

ISP(config)#line console 0

ISP(config-line)#password cisco

ISP(config-line)#login

ISP(config-line)#line vty 0 15

ISP(config-line)#password cisco

ISP(config-line)#login

ISP(config-line)#service password-encryption

ISP(config)# banner motd %Se prohibe el acceso no autorizado.%

ISP(config)#

Router>enable

Router#configure terminal

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

Router(config)#hostname Medellin1

Medellin1(config)#enable secret class

Medellin1(config)#line console 0

Medellin1(config-line)#password cisco

Medellin1(config-line)#login

Medellin1(config-line)#line vty 0 15

Medellin1(config-line)#password cisco

Medellin1(config-line)#login

Medellin1(config-line)#service password-encryption

Medellin1(config)# banner motd %Se prohibe el acceso no autorizado.%

Medellin1(config)#

Router>enable

Router#configure terminal

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

Medellin2(config)#hostname Medellin2

Medellin2(config)#enable secret class

Medellin2(config)#line console 0

Medellin2(config-line)#password cisco

Medellin2(config-line)#login

Medellin2(config-line)#line vty 0 15

Medellin2(config-line)#password cisco

Medellin2(config-line)#login

Medellin2(config-line)#service password-encryption

Medellin2(config)#banner motd %Se prohibe el acceso no autorizado.%

Medellin2(config)#

Router>enable

Router#configure terminal

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

Router(config)#hostname Medellin3

Medellin3(config)#enable secret class

Medellin3(config)#line console 0

Medellin3(config-line)#password cisco

Medellin3(config-line)#login

Medellin3(config-line)#line vty 0 15

Medellin3(config-line)#password cisco

Medellin3(config-line)#login

Medellin3(config-line)#service password-encryption

Medellin3(config)#banner motd %Se prohibe el acceso no autorizado.%

Medellin3(config)#

Router>enable

Router#configure terminal

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

Router(config)#hostname Bogota1

Bogota1(config)#enable secret class

Bogota1(config)#line console 0

Bogota1(config-line)#password cisco

Bogota1(config-line)#login

Bogota1(config-line)#line vty 0 15

Bogota1(config-line)#password cisco

Bogota1(config-line)#login

Bogota1(config-line)#service password-encryption

Bogota1(config)#banner motd %Se prohibe el acceso no autorizado.%

Bogota1(config)#

Router>enable

Router#configure terminal

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

Router(config)#hostname Bogota2

Bogota2(config)#enable secret class

Bogota2(config)#line console 0

Bogota2(config-line)#password cisco

Bogota2(config-line)#login

Bogota2(config-line)#line vty 0 15

Bogota2(config-line)#password cisco

Bogota2(config-line)#login

Bogota2(config-line)#service password-encryption

Bogota2(config)#banner motd %Se prohibe el acceso no autorizado.%

Bogota2(config)#

Router>enable

Router#configure terminal

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

Router(config)#hostname Bogota3

Bogota3(config)#enable secret class

Bogota3(config)#line console 0

Bogota3(config-line)#password cisco

Bogota3(config-line)#login

Bogota3(config-line)#line vty 0 15

Bogota3(config-line)#password cisco

Bogota3(config-line)#login

Bogota3(config-line)#service password-encryption

Bogota3(config)#banner motd %Se prohibe el acceso no autorizado.%

Bogota3(config)#

* Realizar la conexión fisica de los equipos con base en la topología de red

Configurar la topología de red, de acuerdo con las siguientes especificaciones:

Tabla 6 . Especificaciones de la topologia de red

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Dispositivo** | **Interfaz** | **Dirección IP** | **Máscara de subred** | **Máscara wildcard** | **Gateway predeterminado** |
| Medellin1 | S0/0/0 | 172.29.6.9 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/0/1 | 172.29.6.1 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/1/0 | 172.29.6.13 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/1/1 | 209.17.220.1 | 255.255.255.252 | 0.0.0.3 | NA |
| Medellin2 | S0/0/0 | 172.29.6.5 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/0/1 | 172.29.6.2 | 255.255.255.252 | 0.0.0.3 | NA |
| G0/0 | 172.29.4.1 | 255.255.255.128 | 0.0.0.127 | NA |
| Medellin3 | S0/0/0 | 172.29.6.6 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/0/1 | 172.29.6.10 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/1/0 | 172.29.6.14 | 255.255.255.252 | 0.0.0.3 | NA |
| G0/0 | 172.29.4.129 | 255.255.255.128 | 0.0.0.127 | NA |
| ISP | S0/0/0 | 209.17.220.2 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/0/1 | 209.17.220.5 | 255.255.255.252 | 0.0.0.3 | NA |
| Bogota1 | S0/0/0 | 209.17.220.6 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/0/1 | 172.29.3.1 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/1/0 | 172.29.3.9 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/1/1 | 172.29.3.5 | 255.255.255.252 | 0.0.0.3 | NA |
| Bogota2 | S0/0/0 | 172.29.3.2 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/0/1 | 172.29.3.13 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/1/0 | 172.29.3.6 | 255.255.255.252 | 0.0.0.3 | NA |
| G0/0 | 172.29.0.1 | 255.255.255.0 | 0.0.0.255 | NA |
| Bogota3 | S0/0/0 | 172.29.3.10 | 255.255.255.252 | 0.0.0.3 | NA |
| S0/0/1 | 172.29.3.14 | 255.255.255.252 | 0.0.0.3 | NA |
| G0/0 | 172.29.1.1 | 255.255.255.0 | 0.0.0.255 | NA |
| PC1\_Med | NIC | DHCP | 255.255.255.128 | 0.0.0.127 | 172.29.4.1 |
| PC2\_Med | NIC | DHCP | 255.255.255.128 | 0.0.0.127 | 172.29.4.129 |
| PC1\_Bog | NIC | DHCP | 255.255.255.0 | 0.0.0.255 | 172.29.0.1 |
| PC2\_Bog | NIC | DHCP | 255.255.255.0 | 0.0.0.255 | 172.29.1.1 |

Fuente: Autor

Medellin1(config)#int s0/0/0

Medellin1(config-if)#description Connection to Medellin3

Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252

Medellin1(config-if)#clock rate 128000

Medellin1(config-if)#no shutdown

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

Medellin1(config-if)#exit

Medellin1(config)#int s0/0/1

Medellin1(config-if)#description Connection to Medellin2

Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252

Medellin1(config-if)#clock rate 128000

Medellin1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

Medellin1(config-if)#exit

Medellin1(config)#int s0/1/0

Medellin1(config-if)#description Connection to Medellin3

Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252

Medellin1(config-if)#clock rate 128000

Medellin1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down

Medellin1(config-if)#exit

Medellin1(config)#int s0/1/1

Medellin1(config-if)#description Connection to ISP

Medellin1(config-if)#ip address 209.17.220.1 255.255.255.252

Medellin1(config-if)#no shutdown

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

Medellin1(config-if)#exit

Medellin1(config)#

Medellin2(config)#int s0/0/0

Medellin2(config-if)#description Connection to Medellin3

Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252

Medellin2(config-if)#clock rate 128000

Medellin2(config-if)#no shutdown

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

Medellin2(config-if)#exit

Medellin2(config)#int s0/0/1

Medellin2(config-if)#description Connection to Medellin1

Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252

Medellin2(config-if)#no shutdown

Medellin2(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

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

Medellin2(config-if)#exit

Medellin2(config)#int g0/0

Medellin2(config-if)#description Connection to PC1\_Med

Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128

Medellin2(config-if)#no shutdown

Medellin2(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

Medellin2(config-if)#exit

Medellin2(config)#

Medellin3(config)#int s0/0/0

Medellin3(config-if)#description Connection to Medellin2

Medellin3(config-if)#ip address 172.29.6.6 255.255.255.252

Medellin3(config-if)#no shutdown

Medellin3(config-if)#

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

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

Medellin3(config-if)#exit

Medellin3(config)#int s0/0/1

Medellin3(config-if)#description Connection to Medellin1

Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252

Medellin3(config-if)#no shutdown

Medellin3(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

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

Medellin3(config-if)#exit

Medellin3(config)#int s0/1/0

Medellin3(config-if)#description Connection to Medellin1

Medellin3(config-if)#ip address 172.29.6.14 255.255.255.252

Medellin3(config-if)#no shutdown

Medellin3(config-if)#

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

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

Medellin3(config-if)#exit

Medellin3(config)#int g0/0

Medellin3(config-if)#description Connection to PC2\_Med

Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128

Medellin3(config-if)#no shutdown

Medellin3(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

Medellin3(config-if)#exit

Medellin3(config)#

ISP(config)#int s0/0/0

ISP(config-if)#description Connection to Medellin1

ISP(config-if)#ip address 209.17.220.2 255.255.255.252

ISP(config-if)#clock rate 128000

ISP(config-if)#no shutdown

ISP(config-if)#

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

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

ISP(config-if)#exit

ISP(config)#int s0/0/1

ISP(config-if)#description Connection to Bogota1

ISP(config-if)#ip address 209.17.220.5 255.255.255.252

ISP(config-if)#clock rate 128000

ISP(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

ISP(config-if)#exit

ISP(config)#

Bogota1(config)#int s0/0/0

Bogota1(config-if)#description Connection to ISP

Bogota1(config-if)#ip address 209.17.220.6 255.255.255.252

Bogota1(config-if)#no shutdown

Bogota1(config-if)#

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

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

Bogota1(config-if)#exit

Bogota1(config)#int s0/0/1

Bogota1(config-if)#description Connection to Bogota2

Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252

Bogota1(config-if)#clock rate 128000

Bogota1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

Bogota1(config-if)#exit

Bogota1(config)#int s0/1/0

Bogota1(config-if)#description Connection to Bogota3

Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252

Bogota1(config-if)#clock rate 128000

Bogota1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down

Bogota1(config-if)#exit

Bogota1(config)#int s0/1/1

Bogota1(config-if)#description Connection to Bogota2

Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252

Bogota1(config-if)#clock rate 128000

Bogota1(config-if)#no shutdown

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

Bogota1(config-if)#exit

Bogota2(config)#int s0/0/0

Bogota2(config-if)#description Connection to Bogota1

Bogota2(config-if)#ip address 172.29.3.2 255.255.255.252

Bogota2(config-if)#no shutdown

Bogota2(config-if)#

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

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

Bogota2(config-if)#exit

Bogota2(config)#int s0/0/1

Bogota2(config-if)#description Connection to Bogota3

Bogota2(config-if)#ip address 172.29.3.13 255.255.255.252

Bogota2(config-if)#clock rate 128000

Bogota2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

Bogota2(config-if)#exit

Bogota2(config)#int s0/1/0

Bogota2(config-if)#description Connection to Bogota1

Bogota2(config-if)#ip address 172.29.3.6 255.255.255.252

Bogota2(config-if)#no shutdown

Bogota2(config-if)#

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

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

Bogota2(config-if)#exit

Bogota2(config)#int g0/0

Bogota2(config-if)#description Connection to PC1\_Bog

Bogota2(config-if)#ip address 172.29.0.1 255.255.255.0

Bogota2(config-if)#no shutdown

Bogota2(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

Bogota2(config-if)#

Bogota3(config)#int s0/0/0

Bogota3(config-if)#description Connection to Bogota1

Bogota3(config-if)#ip address 172.29.3.10 255.255.255.252

Bogota3(config-if)#no shutdown

Bogota3(config-if)#

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

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

Bogota3(config-if)#exit

Bogota3(config)#int s0/0/1

Bogota3(config-if)#description Connection to Bogota2

Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252

Bogota3(config-if)#no shutdown

Bogota3(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

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

Bogota3(config-if)#exit

Bogota3(config)#int g0/0

Bogota3(config-if)#description Connection to PC2\_Bog

Bogota3(config-if)#ip address 172.29.1.1 255.255.255.0

Bogota3(config-if)#no shutdown

Bogota3(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

Bogota3(config-if)#exit

Bogota3(config)#

## Parte 1: Configuración del enrutamiento

1. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

Medellin1(config)#router ospf 1

Medellin1(config-router)#router-id 1.1.1.1

Medellin1(config-router)#do show ip route connected

C 172.29.6.0/30 is directly connected, Serial0/0/1

C 172.29.6.8/30 is directly connected, Serial0/0/0

C 172.29.6.12/30 is directly connected, Serial0/1/0

C 209.17.220.0/30 is directly connected, Serial0/1/1

Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0

Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0

Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0

Medellin1(config-router)#network 209.17.220.0 0.0.0.3 area 0

Medellin1(config-router)#exit

Medellin1(config)#

Medellin2(config)#router ospf 1

Medellin2(config-router)#router-id 2.2.2.2

Medellin2(config-router)#do show ip route connected

C 172.29.4.0/25 is directly connected, GigabitEthernet0/0

C 172.29.6.0/30 is directly connected, Serial0/0/1

C 172.29.6.4/30 is directly connected, Serial0/0/0

Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0

Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0

Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0

05:52:57: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done

Medellin2(config-router)#exit

Medellin2(config)#

Medellin3(config)#router ospf 1

Medellin3(config-router)#router-id 3.3.3.3

Medellin3(config-router)#do show ip route connected

C 172.29.4.128/25 is directly connected, GigabitEthernet0/0

C 172.29.6.4/30 is directly connected, Serial0/0/0

C 172.29.6.8/30 is directly connected, Serial0/0/1

C 172.29.6.12/30 is directly connected, Serial0/1/0

Medellin3(config-router)#network 172.29.4.128 0.0.0.127 area 0

Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0

05:57:42: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done

Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0

Medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 0

Medellin3(config-router)#

05:58:13: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/1/0 from LOADING to FULL, Loading Done

Medellin3(config-router)#exit

Medellin3(config)#

Bogota1(config)#router ospf 1

Bogota1(config-router)#router-id 4.4.4.4

Bogota1(config-router)#do show ip route connected

C 172.29.3.0/30 is directly connected, Serial0/0/1

C 172.29.3.4/30 is directly connected, Serial0/1/1

C 172.29.3.8/30 is directly connected, Serial0/1/0

C 209.17.220.4/30 is directly connected, Serial0/0/0

Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0

Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0

Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 0

Bogota1(config-router)#network 209.17.220.4 0.0.0.3 area 0

Bogota1(config-router)#exit

Bogota1(config)#

Bogota2(config)#router ospf 1

Bogota2(config-router)#router-id 5.5.5.5

Bogota2(config-router)#do show ip route connected

C 172.29.0.0/24 is directly connected, GigabitEthernet0/0

C 172.29.3.0/30 is directly connected, Serial0/0/0

C 172.29.3.4/30 is directly connected, Serial0/1/0

C 172.29.3.12/30 is directly connected, Serial0/0/1

Bogota2(config-router)#network 172.29.0.0 0.0.0.255 area 0

Bogota2(config-router)#network 172.29.3.0 0.0.0.3 area 0

Bogota2(config-router)#network 172.29.3.4 0.0.0.3 area 0

Bogota2(config-router)#

06:14:17: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/0 from LOADING to FULL, Loading Done

Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0

Bogota2(config-router)#exit

Bogota2(config)#

Bogota3(config)#router ospf 1

Bogota3(config-router)#router-id 6.6.6.6

Bogota3(config-router)#do show ip route connected

C 172.29.1.0/24 is directly connected, GigabitEthernet0/0

C 172.29.3.8/30 is directly connected, Serial0/0/0

C 172.29.3.12/30 is directly connected, Serial0/0/1

Bogota3(config-router)#network 172.29.1.0 0.0.0.255 area 0

Bogota3(config-router)#network 172.29.3.8 0.0.0.3 area 0

06:23:06: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/0 from LOADING to FULL, Loading Done

Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0

Bogota3(config-router)#

06:23:35: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING to FULL, Loading Done

Bogota3(config-router)#exit

Bogota3(config)#

ISP(config)#router ospf 1

ISP(config-router)#router-id 7.7.7.7

ISP(config-router)#do show ip route connected

C 209.17.220.0/30 is directly connected, Serial0/0/0

C 209.17.220.4/30 is directly connected, Serial0/0/1

ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0

ISP(config-router)#

03:18:36: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0

ISP(config-router)#

03:18:53: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/1 from LOADING to FULL, Loading Done

ISP(config-router)#exit

ISP(config)#

1. Los routers Bogota1 y Medellín1 deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Medellin1(config)#ip route 0.0.0.0 209.17.220.1

% Incomplete command.

Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.2

Medellin1(config)#router ospf 1

Medellin1(config-router)#default-information originate

Medellin1(config-router)#exit

Medellin1(config)#

Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5

Bogota1(config)#router ospf 1

Bogota1(config-router)#default-information originate

Bogota1(config-router)#exit

Bogota1(config)#

1. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1

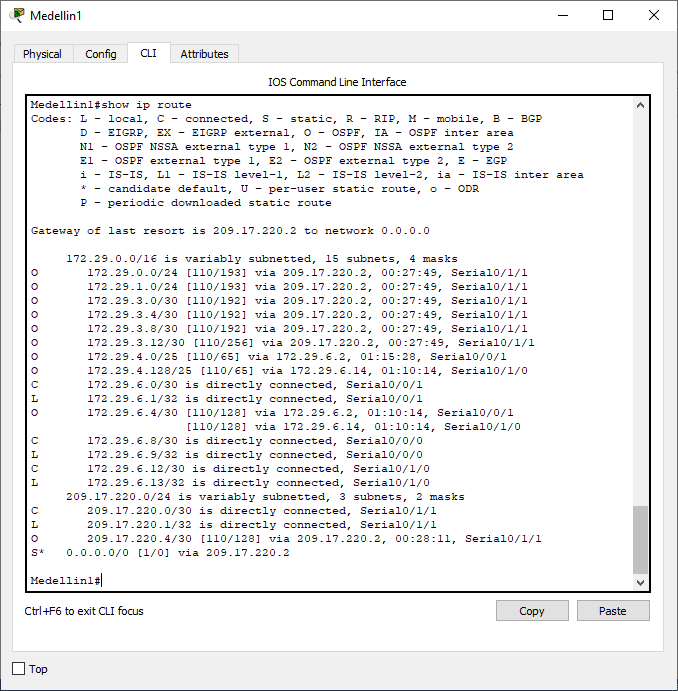
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

ISP(config)#

## Parte 2: Tabla de Enrutamiento

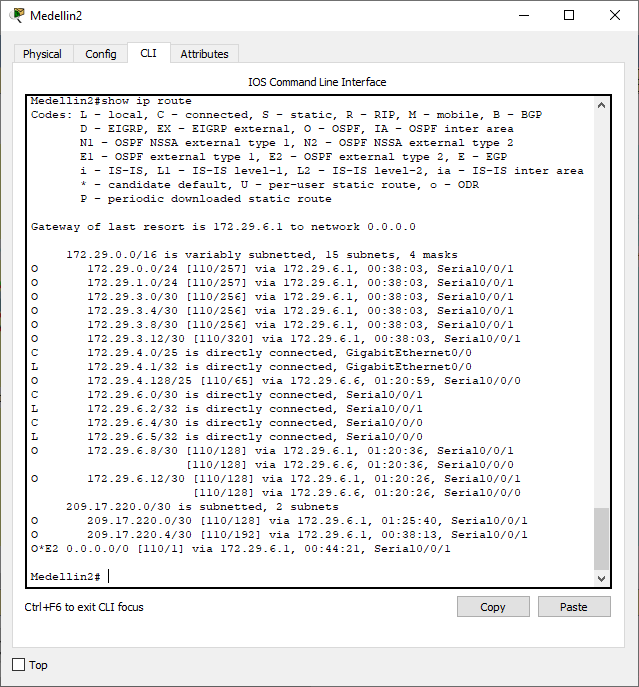
1. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
2. Verificar el balanceo de carga que presentan los routers.
3. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.
4. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.
5. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
6. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Fígura 27. Show ip route en Router Medellin1.



Fuente: Autor.

Fígura 28. Show ip route en Router Medellin2



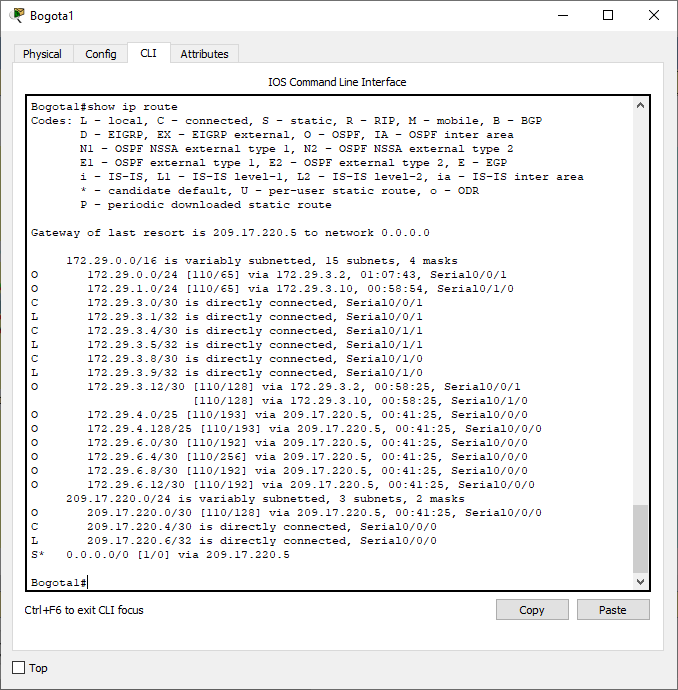
Fuente: Autor.

Fígura 29. Show ip route en Router Medellin3



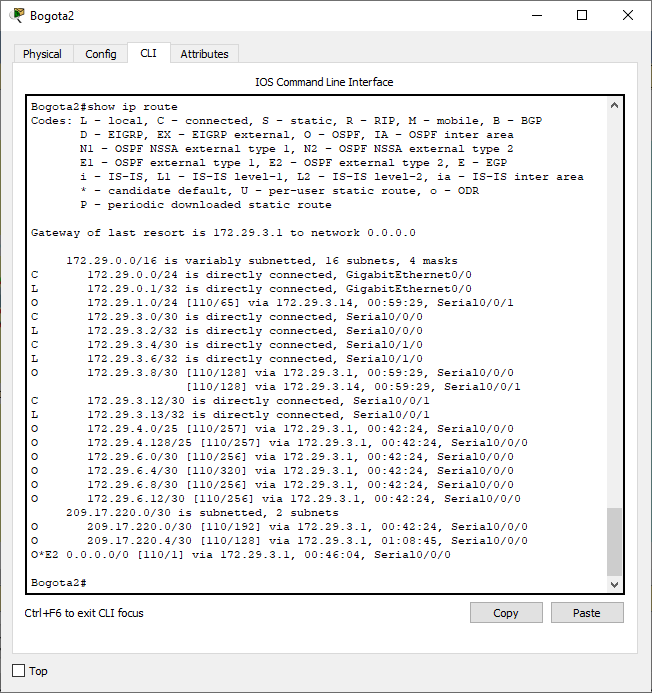
Fuente: Autor.

Fígura 30. Show ip route en Router Bogota1



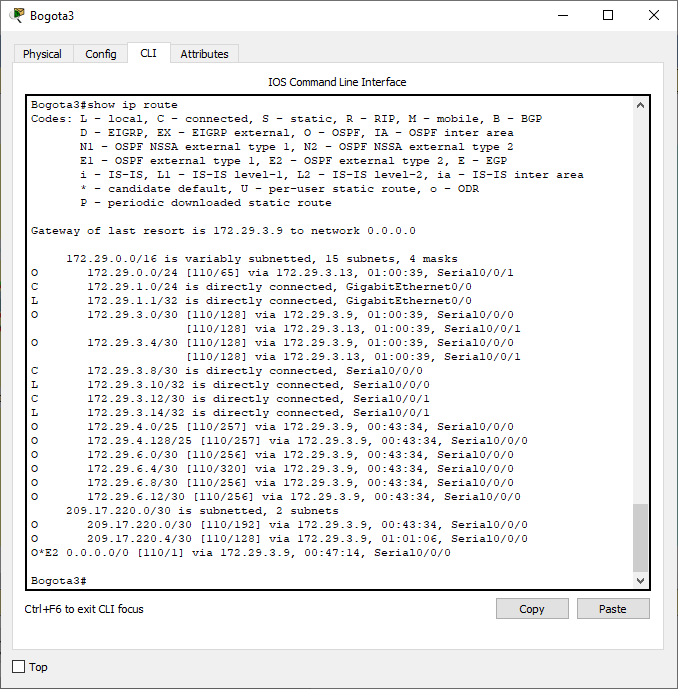
Fuente: Autor.

Fígura 31. Show ip route en Router Bogota2



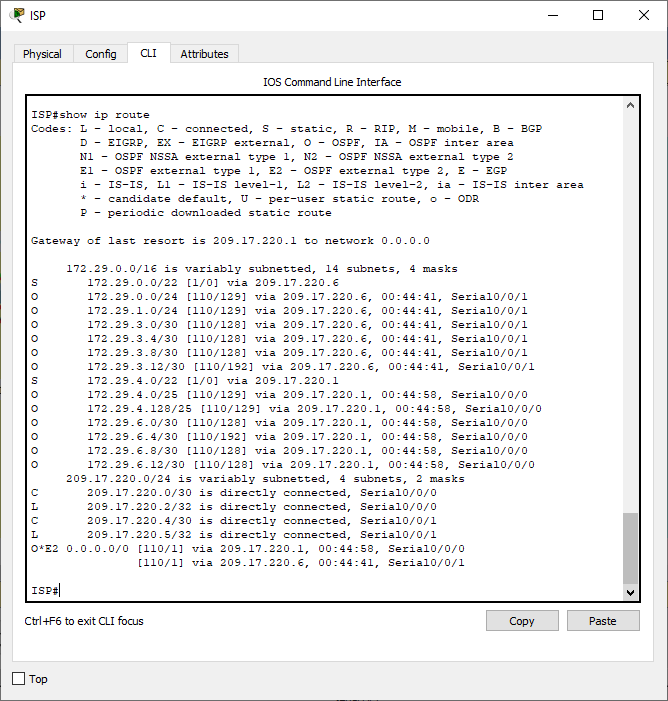
Fuente: Autor.

Fígura 32. Show ip route en Router Bogota3



Fuente: Autor.

Fígura 33. Show ip route en Router ISP



Fuente: Autor.

## Parte 3: Deshabilitar la propagación del protocolo OSPF

1. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 7. Interfaces de los Router

|  |  |
| --- | --- |
| **Router** | **Interface** |
| Bogota1 | SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0 |
| Bogota2 | SERIAL0/0/0; SERIAL0/0/1 |
| Bogota3 | SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0 |
| Medellín1 | SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1 |
| Medellín2 | SERIAL0/0/0; SERIAL0/0/1 |
| Medellín3 | SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0 |
| ISP | No lo requiere |

Fuente: Autor

Medellin1(config)#router ospf 1

Medellin1(config-router)#passive-interface s0/1/0

00:01:20: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/0 from LOADING to FULL, Loading Done

Medellin1(config-router)#

Medellin2(config)#router ospf 1

Medellin2(config-router)#passive-interface g0/0

Medellin2(config-router)#exit

Medellin2(config)#

Medellin3(config)#router ospf 1

Medellin3(config-router)#passive-interface g0/0

Medellin3(config-router)#exit

Medellin3(config)#

Bogota1(config)#router ospf 1

Bogota1(config-router)#passive-interface s0/1/1

Bogota1(config-router)#exit

Bogota2(config)#router ospf 1

Bogota2(config-router)#passive-interface s0/1/0

Bogota2(config-router)#passive-interface g0/0

Bogota2(config-router)#exit

Bogota3(config)#router ospf 1

Bogota3(config-router)#passive-interface g0/0

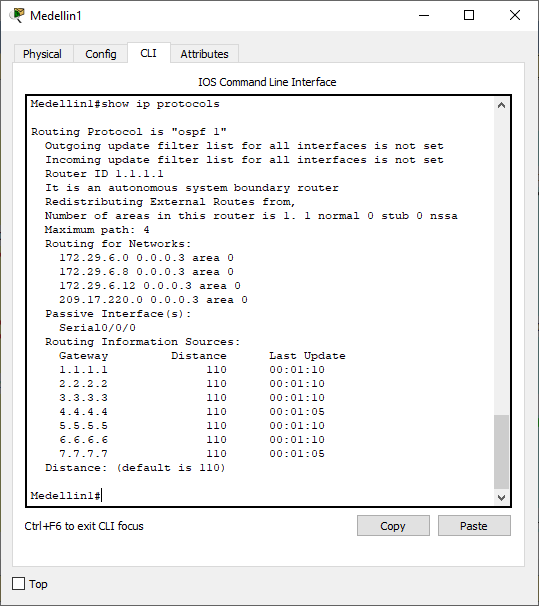
Bogota3(config-router)#exit

Bogota3(config)#

## Parte 4: Verificación del protocolo OSPF.

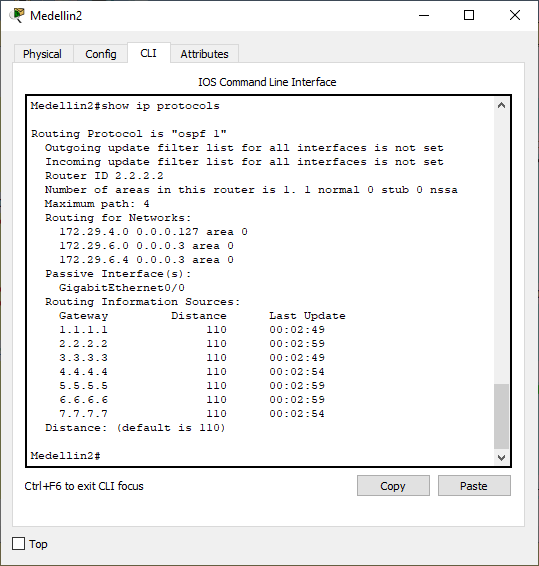
1. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

Fígura 34. Show ip route protocols en Router Medellin1



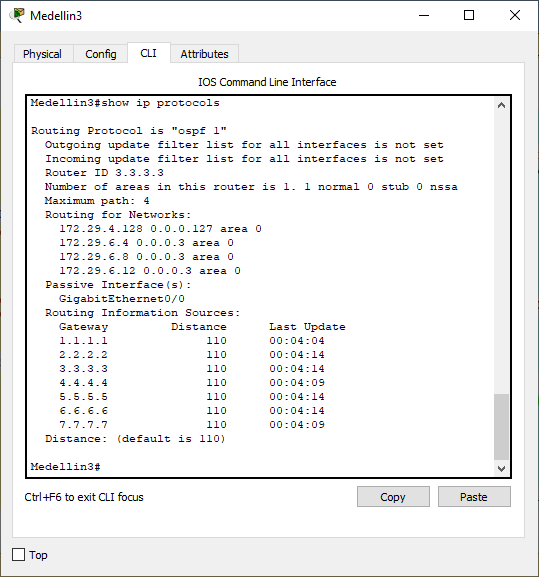
Fuente: Autor.

Fígura 35. Show ip route protocols en Router Medellin2



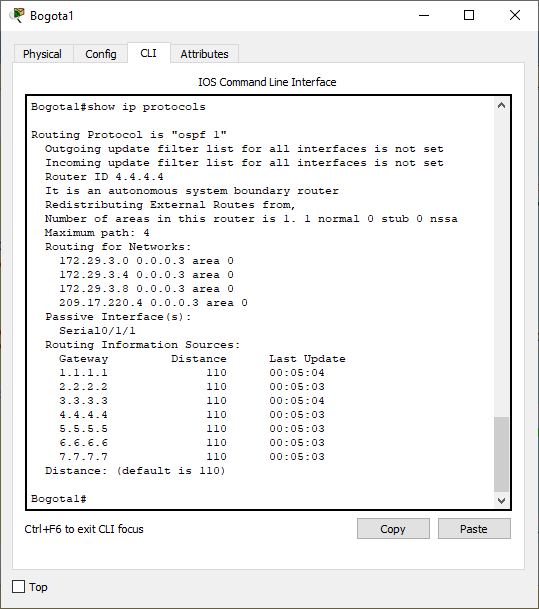
Fuente: Autor.

Fígura 36. Show ip route protocols en Router Medellin3.



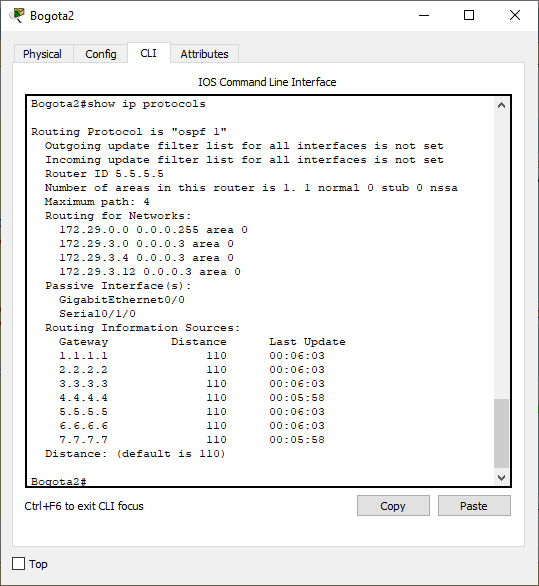
Fuente: Autor.

Fígura 37. Show ip route protocols en Router Bogota1



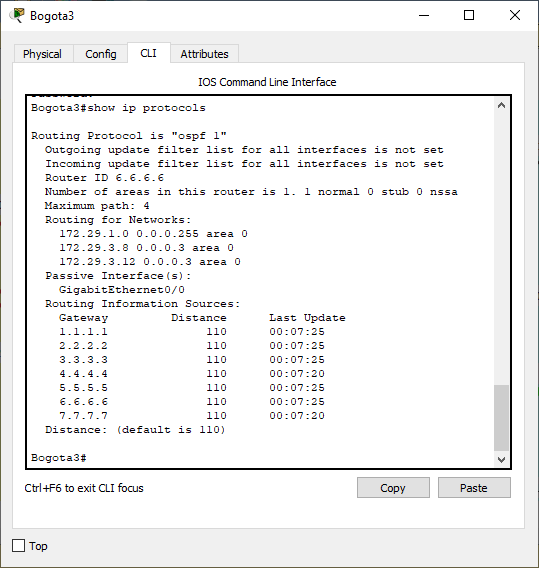
Fuente: Autor.

Fígura 38. Show ip route protocols en Router Bogota2



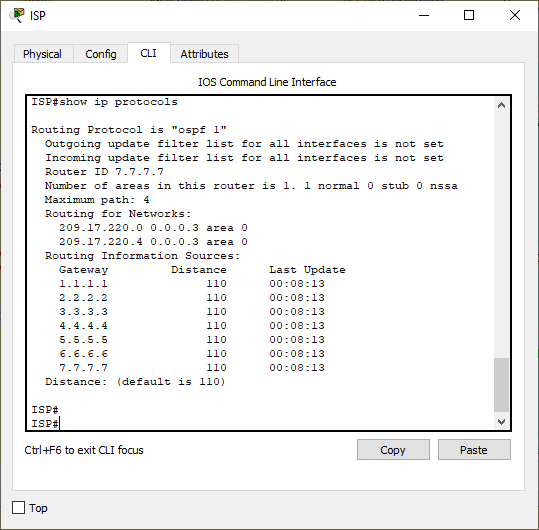
Fuente: Autor.

Fígura 39. Show ip route protocols en Router Bogota3



Fuente: Autor.

Fígura 40. Show ip route protocols en Router ISP



Fuente: Autor.

1. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Este paso fue resuelto en el punto anterior con el comando show ip route.

## Parte 5: Configurar encapsulamiento y autenticación PPP

1. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.
2. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

Medellin1(config)#interface Serial0/1/1

Medellin1(config-if)#encapsulation ppp

Medellin1(config-if)#no shutdown

Medellin1(config-if)#exit

Medellin1(config)#username ISP secret cisco

Medellin1(config)#int s0/1/1

Medellin1(config-if)#ppp authentication pap

Medellin1(config-if)#ppp pap sent-username MEDELLIN password cisco

Medellin1(config-if)#exit

Medellin1(config)#

Bogota1(config)#interface Serial0/0/0

Bogota1(config-if)#encapsulation ppp

Bogota1(config-if)#no shutdown

Bogota1(config-if)#exit

Bogota1(config)#

Bogota1(config)#username ISP secret cisco

Bogota1(config)#int s0/0/0

Bogota1(config-if)#ppp authentication chap

Bogota1(config-if)#exit

Bogota1(config)#

ISP(config)#interface Serial0/0/0

ISP(config-if)#encapsulation ppp

ISP(config-if)#no shutdown

ISP(config-if)#exit

ISP(config)#interface Serial0/0/1

ISP(config-if)#encapsulation ppp

ISP(config-if)#no shutdown

ISP(config-if)#exit

ISP(config)#username MEDELLIN secret cisco

ISP(config)#int s0/0/0

ISP(config-if)#ppp authentication pap

ISP(config-if)#ppp pap sent-username ISP password cisco

ISP(config-if)#exit

ISP(config)#username BOGOTA secret cisco

ISP(config)#int s0/0/1

ISP(config-if)#ppp authentication chap

ISP(config-if)#exit

ISP(config)#

## Parte 6: Configuración de PAT

1. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
2. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial ~~0/1/0 (~~s0/1/1) del router Medellín1, cómo diferente puerto.
3. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

Medellin1(config)#ip access-list standard HOST

Medellin1(config-std-nacl)#permit 172.29.4.0 0.0.0.127

Medellin1(config-std-nacl)#exit

Medellin1(config)#ip nat inside source list HOST interface s0/1/1 overload

Medellin1(config)#int s0/0/0

Medellin1(config-if)#ip nat inside

Medellin1(config-if)#exit

Medellin1(config)#int s0/0/1

Medellin1(config-if)#ip nat inside

Medellin1(config-if)#exit

Medellin1(config)#int s0/1/0

Medellin1(config-if)#ip nat inside

Medellin1(config-if)#exit

Medellin1(config)#int s0/1/1

Medellin1(config-if)#ip nat outside

Medellin1(config-if)#exit

Medellin1(config)#exit

Medellin1#show ip nat translation

Medellin1#

Bogota1(config)#ip access-list standard HOST

Bogota1(config-std-nacl)#permit 172.29.0.0 0.0.0.255

Bogota1(config-std-nacl)#exit

Bogota1(config)#ip nat inside source list HOST interface s0/0/0 overload

Bogota1(config)#int s0/0/0

Bogota1(config-if)#ip nat outside

Bogota1(config-if)#exit

Bogota1(config)#int s0/0/1

Bogota1(config-if)#ip nat inside

Bogota1(config-if)#exit

Bogota1(config)#int s0/1/0

Bogota1(config-if)#ip nat inside

Bogota1(config-if)#exit

Bogota1(config)#int s0/1/1

Bogota1(config-if)#ip nat inside

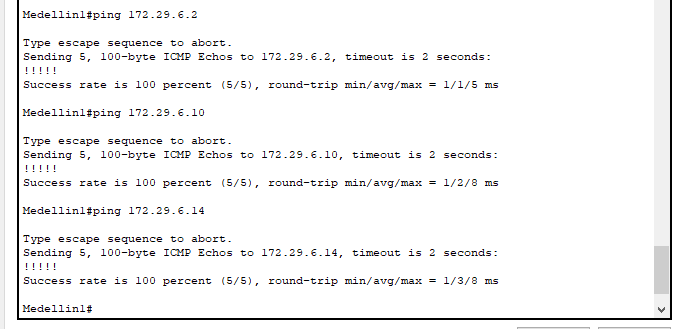
Bogota1(config-if)#exit

Bogota1(config)#exit

Bogota1#show ip nat translation

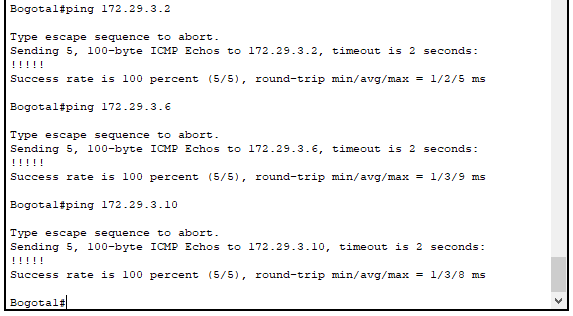
Bogota1#

Fígura 41. Prueba de ping de Medellin1 a Medellin2 y Medellin3



Fuente: Autor.

Fígura 42 Prueba de ping de Bogota1 a Bogota2 y Bogota3



Fuente: Autor.

## Parte 7: Configuración del servicio DHCP

1. Configurar la red Medellín2 y Medellín3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.
2. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

Medellin2(config)#ip dhcp excluded-address 172.29.4.1

Medellin2(config)#ip dhcp pool MEDELLIN2

Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128

Medellin2(dhcp-config)#default-router 172.29.4.1

Medellin2(dhcp-config)#dns-server 8.8.8.8

Medellin2(dhcp-config)#exit

Medellin2(config)#ip dhcp excluded-address 172.29.4.29

Medellin2(config)#ip dhcp pool MEDELLIN3

Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128

Medellin2(dhcp-config)#default-router 172.29.4.129

Medellin2(dhcp-config)#dns-server 8.8.8.8

Medellin2(dhcp-config)#exit

Medellin2(config)#

Como el router Medellin3 tiene una red LAN conectada pero no realizará las veces de servidor DHCP, es necesario configurar “ip helper” el cual permitirá ser un router de tránsito para llegar al router con el rol de DHCP. Por lo anterior utilizamos el comando ip helper-addres para atrapar los broadcasts y redireccionarlos hacia la IP del router de Medellin2, se debe utilizar la dirección IP de la interfaz de salida Medellin2 (s0/0/0 - 172.29.6.5):

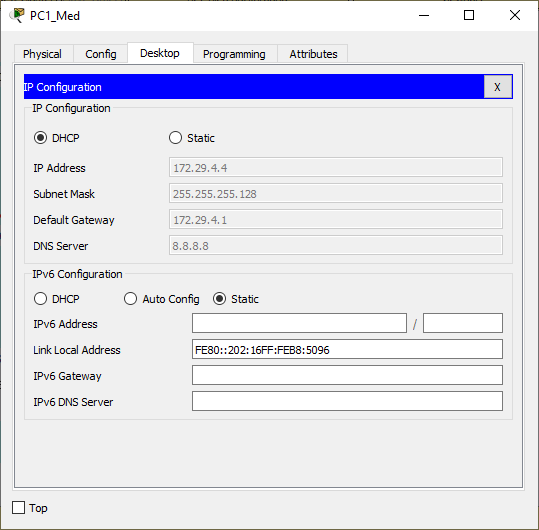
Medellin3(config)#int g0/0

Medellin3(config-if)#ip helper-address 172.29.6.5

Medellin3(config-if)#exit

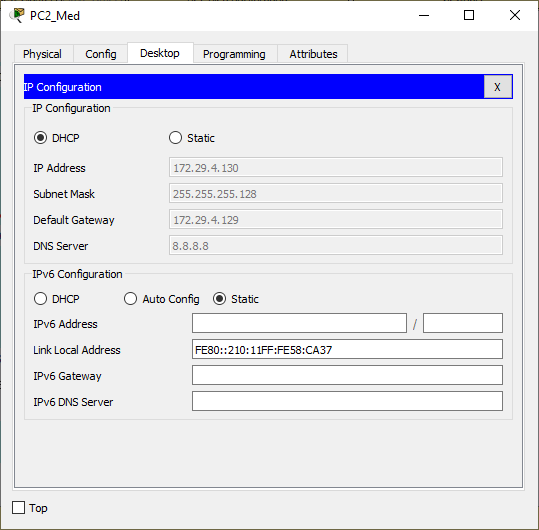
Medellin3(config)#

Fígura 43. Configuración IP PC1\_Med



Fuente: Autor.

Fígura 44. Configuración IP PC2\_Med



Fuente: Autor.

1. Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes LAN.
2. Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Bogota2(dhcp-config)#ip dhcp excluded-address 172.29.0.1

Bogota2(config)#ip dhcp pool BOGOTA2

Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0

Bogota2(dhcp-config)#default-router 172.29.0.1

Bogota2(dhcp-config)#dns-server 8.8.8.8

Bogota2(dhcp-config)#exit

Bogota2(config)#ip dhcp excluded-address 172.29.1.1

Bogota2(config)#ip dhcp pool BOGOTA3

Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0

Bogota2(dhcp-config)#default-router 172.29.1.1

Bogota2(dhcp-config)#dns-server 8.8.8.8

Bogota2(dhcp-config)#exit

Bogota2(config)#

Como el router Bogota3 tiene una red LAN conectada pero no realizará las veces de servidor DHCP, es necesario configurar “ip helper” el cual permitirá ser un router de tránsito para llegar al router con el rol de DHCP. Por lo anterior utilizamos el comando ip helper-addres para atrapar los broadcasts y redireccionarlos hacia la IP del router de Bogota2, se debe utilizar la dirección IP de la interfaz de salida Bogota2 (s0/0/1 - 172.29.3.13):

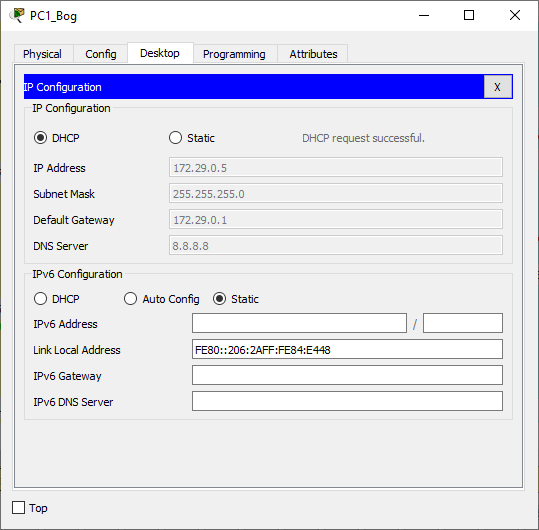
Bogota3(config)#int g0/0

Bogota3(config-if)#ip helper-address 172.29.3.13

Bogota3(config-if)#exit

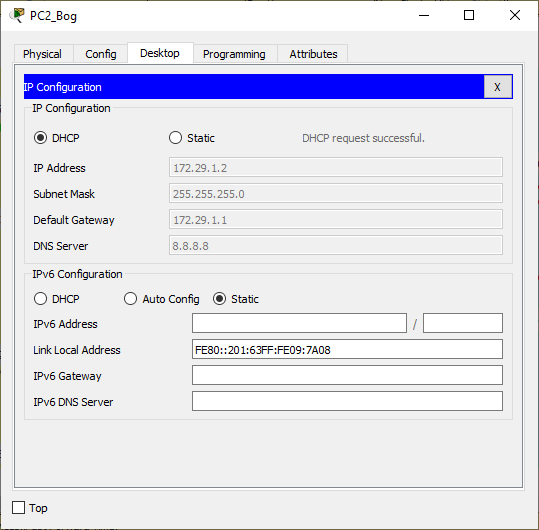
Bogota3(config)#

Fígura 45. Configuración IP PC1\_Bog



Fuente: Autor.

Fígura 46. Configuración IP PC2\_Bog



Fuente: Autor.

## Parte adicional: Guardar los cambios

Guardar los cambios realizados en la configuración activa (RAM) a un archivo de configuración de respaldo (NVRAM ) que es el que será utilizado en caso de que por cualquier motivo el dispositivo sea reiniciado.

ISP#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

ISP#

Medellin1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Medellin1#

Medellin2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Medellin2#

Medellin3#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Medellin3#

Bogota1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Bogota1#

Bogota2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Bogota2#

Bogota3#copy running-config startup-config

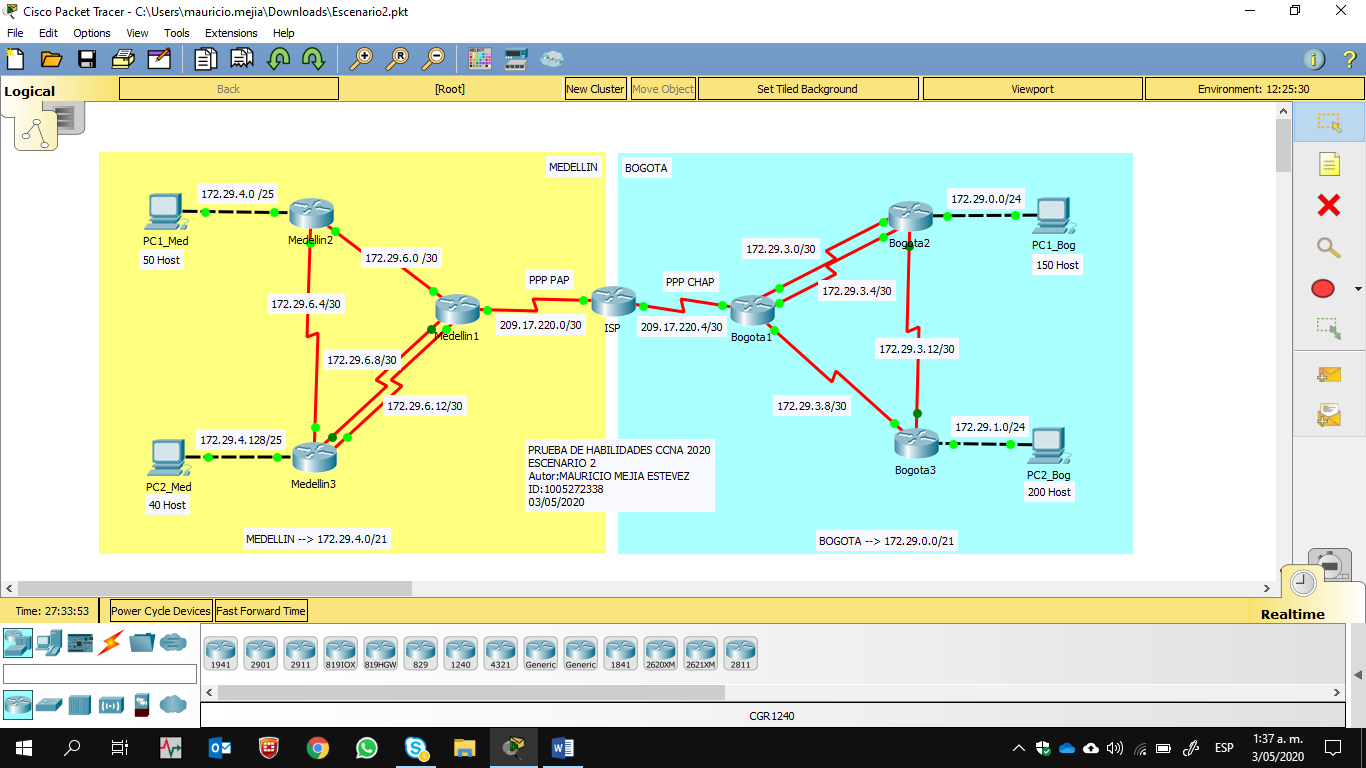
Destination filename [startup-config]?

Building configuration...

[OK]

Bogota3#

Fígura 47. Topologia de red escenario 2 - Cisco Packet Tracer



Fuente: Autor.

# CONCLUSIONES

El estudiante emplea comandos de configuración avanzada en routers, implementando RIP, OSPF y enrutamiento estático; bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.

El estudiante utiliza herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento, evaluando el comportamiento de enrutadores, mediante el uso de comandos de administración de tablas de enrutamiento, bajo el uso de protocolos de vector distancia y estado enlace.

El estudiante configura esquemas de conmutación soportadas en Switches, mediante el uso de protocolos basados en STP y VLANs en escenarios corporativos y residenciales, con el fin de comprender el modo de operación de las VLAN y las bondades de administrar dominios de broadcast independientes, en escenarios soportados a nivel de capa 2 al interior de una red jerárquica convergente.

# BIBLIOGRAFÍA

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de

<https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>

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>

CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1>

CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1>

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>

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1>

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>

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

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

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

CISCO. (2017). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>

CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>

CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

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

UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9>

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3>

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