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

CRISTIAN DE JESUS SALAZAR PERTUZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

INGENIERIA ELECTRONICA

CARTAGENA, BOLIVAR

2020

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

CRISTIAN DE JESUS SALAZAR PERTUZ

PRESENTACIÓN DE INFORME DE PRUEBA DE HABILIDADES PRACTICAS

ASESOR

NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

INGENIERIA ELECTRONICA

CARTAGENA, BOLIVAR

2020

CONTENIDO

INDICE DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACL: Standard access control lists o lista de control de acceso estándar es un Sistema de seguridad que se implementa en un router de perímetro para restringir las conexiones entrantes a un determinado Puerto y por ende impedir ataques o conexiones no deseadas.

CHAP: Challenge Handshake Authentication Protocol (CHAP). Es un Sistema de autenticación que permite establecer un canal de comunicación cifrado por medio de contraseñas establecidas en un router cliente y un router autenticador.

CLI: Commands line o línea de comandos del os, es el área donde se introducen los comandos y/o configuraciones que permiten cambiar los parámetros del router o switch de acuerdo a una configuración predeterminada, en este apartado se puede ajustar puertos, interfaces, asignaciones de direcciones y funcionalidades que incluya el router.

DHCP: El protocolo de configuración dinámica de host (DHCP) es un sistema de asignación automática direcciones a los hosts solicitantes a través de una lista de direcciones disponibles configuradas previamente, en ellas se incluyen direcciones reservadas, dirección del GATEWAY, DNS, mascara de subred. Esta configuración se puede aplicar para funcionar desde un router o un servidor dedicado.

DNS: Domain Name System o Sistema de Nombres de Dominio, es un sistema de traducción de direcciones ip, nombres de dominio, es decir, que funciona para traducir el nombre de un sitio web a su dirección ip donde se encuentra alojado el sitio web. Esta configuración se puede realizar en un router o un servidor donde se almacenan las páginas web o las traducciones.

ENLACE: Es el medio de comunicación por el cual se interconectan dos o más dispositivos, adicionalmente también se identifica sobre la configuración de la conexión entre dos interfaces, es decir, modo trunk o access.

GATEWAY: Puerto de salida (interfaz de salida), es la interfaz que usara un dispositivo o red para tener acceso a través de este a otro conjunto de redes, es decir, una red de 150 host tendría múltiples switch y un router, el Gateway sería la interfaz del router conectada al puerto de uno de los switch. De esta forma la red

tendría una puerta de salida hacia otro conjunto de red (internet) también sirve como punto de acceso para la traducción del protocolo de la red exterior a la red interna.

HOST: Es el cliente o dispositivo final de una red. La cantidad de host conectados o por conectar en una red determina su tamaño y la infraestructura a diseñar para brindar conexión y soporte.

IPV4: Internet protocols v4. Protocolo de internet versión 4, es el sistema de direcciones que permite asignar un numero de dirección a una interfaz, puerto o red para que esta a su vez se pueda conectar con otras de forma precisa. La versión 4 se implementó en 1983 para ARPANET y tiene una capacidad de 116.777.216 direcciones.

IPV6: Internet protocols v6. Protocolo de internet versión 6, es una actualización del sistema de direcciones ipv4, dado que el sistema actual sufre de una escases de direcciones y el nuevo protocolo tiene la capacidad de 2´128 logrando proveer de direcciones para la creciente demanda a nivel mundial.

LOOPBACK: Es un dispositivo virtual que se crea dentro de otro, en el software packet Tracer, se crean dentro de un router para desarrollar funciones de re-direccionamiento de tráfico hacia al mismo router, es decir, se utiliza como un dispositivo (host) de destino virtual sin la necesidad de estar conectado directamente o físicamente a dicho router.

MASCARA DE RED: Es un conjunto de datos representados en forma de dirección ipv4 (para ipv4) que indica el límite del área de la red a la cual pueden pertenecer un conjunto de host, es decir, la máscara de red indica que el host se comunica con un host de red local o una interfaz o host de una red externa al verificar que la máscara es diferente.

NAT: Conversión de Dirección de Red (NAT). Básicamente el sistema NAT traduce direcciones de host de una red a otra para establecer conectividad, este proceso de configuración se realiza en CLI de un router.

NTP: Network Timing Protocol (NTP) o protocolo de tiempo de red, es una configuración que sincroniza el reloj de un router o switch dentro de una red para

que los dispositivos de conectividad tengan la misma marcación de tiempo de ejecución.

PAP: Password Authentication Protocol (PAP). Al igual que el sistema de autenticación CHAP; PAP es un sistema que se configura para brindar seguridad de comunicaciones entre dispositivos, a través de enlaces cifrados por contraseñas, el cual funciona sobre ipv4 y el ipv6.

PING: Es una utilidad de diagnóstico en redes para realizar pruebas de enlaces punto a punto, es decir, desde un host local hasta un destino específico, en los dispositivos switch y router el comando ping se ejecuta acompañado de la dirección ip a la cual se quiere alcanzar, en los hosts se realiza de la misma forma que en un router o switch, pero en el cmd del sistema operativo del host.

RIP V2: Routing Information Protocol (RIP) o protocolo de Información de enrutamiento, Se utiliza para configurar en un enrutador o router la forma en que estos comparten información de las redes conectados a ellos, RIP es un protocolo de enlace interno de código abierto el cual puede ser utilizado por varios fabricantes a diferencia de los protocolos propietarios que son exclusivos para un fabricante.

ROUTER: enrutador o router, es el dispositivo que se utiliza para interconectar dispositivos o redes equidistantes a través de enlaces (serial, gigabit, fastethernet, coaxial u otro) sobre el cual se establecen varias configuraciones para lograr una o varias funcionalidades desde el router, entre ellas, enlaces cifrados, servicios de dhcp, puertos loopback, redes virtuales y demás funciones que se permiten establecer dentro del sistema operativo del router.

SWITCH: Los switch son dispositivos que permiten la multiplicación y distribución de puertos de enlace para una red local, un switch puede ofrecer enlace wi-fi o gigabit Ethernet para conectarse con un dispositivo de entrada (router). O interconectar host dentro de una misma red local (pc, impresoras, telefonía ip)

VLAN: virtual LAN, es una utilidad de configuración sobre la cual se pueden establecer un numero de redes virtuales sobre la misma infraestructura de red, decir, en una red local física se pueden segmentar las conexiones a través de redes virtuales que funcionan sobre esta infraestructura (oficinas, producción, ventas, soporte técnico u otras) se pueden dividir en vlan diferentes.

RESUMÉN

A través de la aplicación Packet Tracer de Cisco se desarrollan dos simulaciones de estudio donde se plantean dos escenarios sobre los cuales se han aplicado las distintas configuraciones de dispositivos aprendidas durante el desarrollo del diplomado de redes ccna, este documento describe el proceso de configuración que ha empleado en los diferentes hosts que componen cada simulación a si mismo se muestran las respuestas que se obtienen durante la ejecución de cada comando en el CLI, se parte de una configuración básica (nombre del host, contraseña, puertos habilitados, direcciones ipv4 y ipv6, puertos virtuales y redes virtuales) posteriormente las opciones de configuración propias de cada escenario para lograr conectividad de acuerdo a la premisa y condiciones iniciales.

ABSTRACT

Through the Cisco Packet Tracer application, two study simulations are developed where two scenarios are proposed on which the different device configurations learned during the development of the ccna network diploma have been applied, this document describes the configuration process that has Used in the different hosts that make up each simulation, the responses that are obtained during the execution of each command in the CLI are shown. It starts with a basic configuration (hostname, password, enabled ports, ipv4 and ipv6 addresses, virtual ports and virtual networks) then the configuration options for each scenario to achieve connectivity according to the premise and initial conditions.

INTRODUCCIÓN

El presente trabajo muestra el aprendizaje obtenido a través del desarrollo del curso, aplicando la dinámica de aprendizaje basado en tareas, en esta última actividad se pretenden aplicar los conceptos adquiridos durante el proceso de estudio del diplomado redes ccna; gracias a la práctica sobre entornos simulados donde estas habilidades se ponen a prueba, la ejecución de comandos, resolución de problemas y logro de los objetivos propuestos desde la perspectiva de las condiciones iniciales. Los softwares de estudio y simulación de redes como Packet Tracer fueron de gran ayuda para alcanzar esta finalidad.

OBJETIVOS

Este documento tiene como finalidad utilizar el conocimiento adquirido en el transcurso de las actividades del diplomado de profundización Cisco para desarrollar y brindar solución a dos casos de estudio bajo tecnología Cisco, la cual se adquirió a través de la práctica de escenarios de estudio y laboratorio durante el desarrollo del curso.

Objetivo específico:

- Lograr conectividad completa en cada escenario y/o topología propuesta.
- Configurar los distintos hosts siguiendo los lineamientos establecidos en la guía de la actividad.
- Brindar aclaraciones durante los procedimientos y muestras de ejecución de instrucciones en pro de materializar las soluciones de conectividad.

PRACTICA 1

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.

Topología.

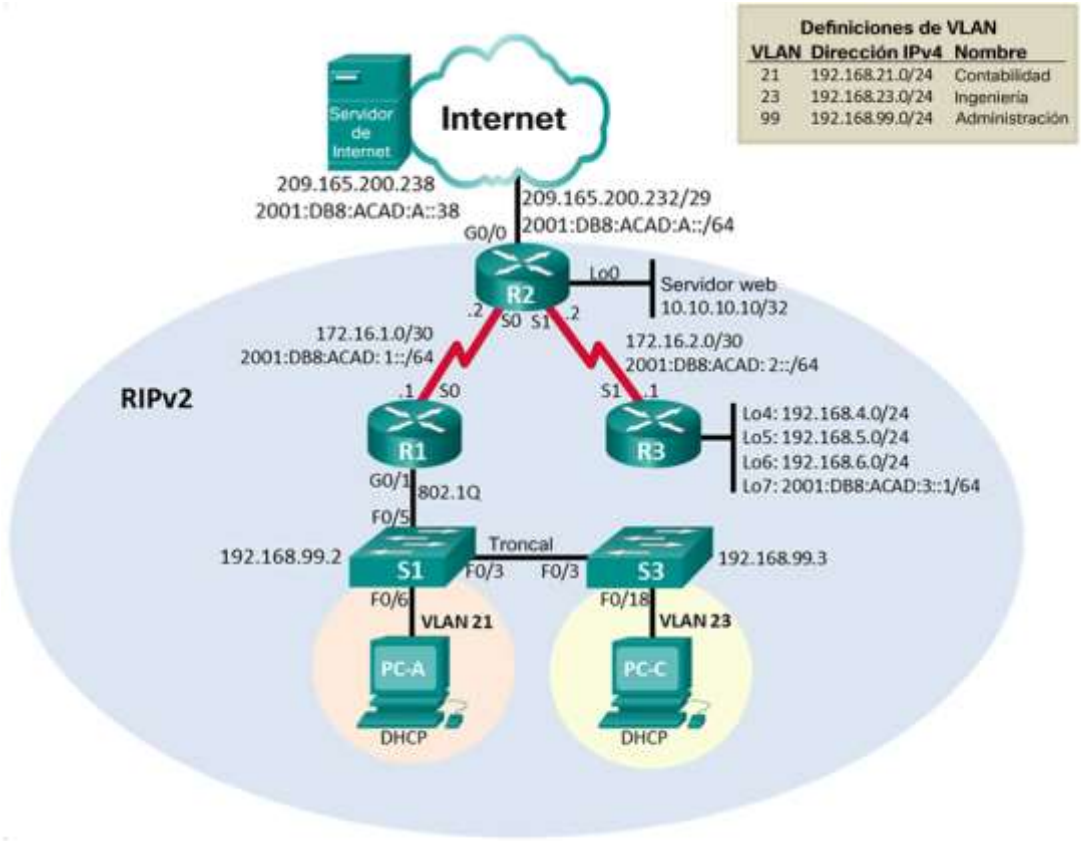

Figure 1. Topología de la red

Fuente: Documento de la actividad – prueba de habilidades practicas

PARTE 1: INICIALIZAR DISPOSITIVOS.

PASO 1: Inicializar y volver a cargar los routers y los switches

R1> Enable

R1# erase startup-config

R1# reboot

R1# reload

R2> Enable

R2# erase startup-config

R2# reboot

R2# reload

R3> Enable

R3# erase startup-config

R3# reboot

R3# reload

S1> Enable

S1# erase startup-config

S1# delete flash: vlan.dat

S1# reboot

S1# reload

S1> show vlan brief

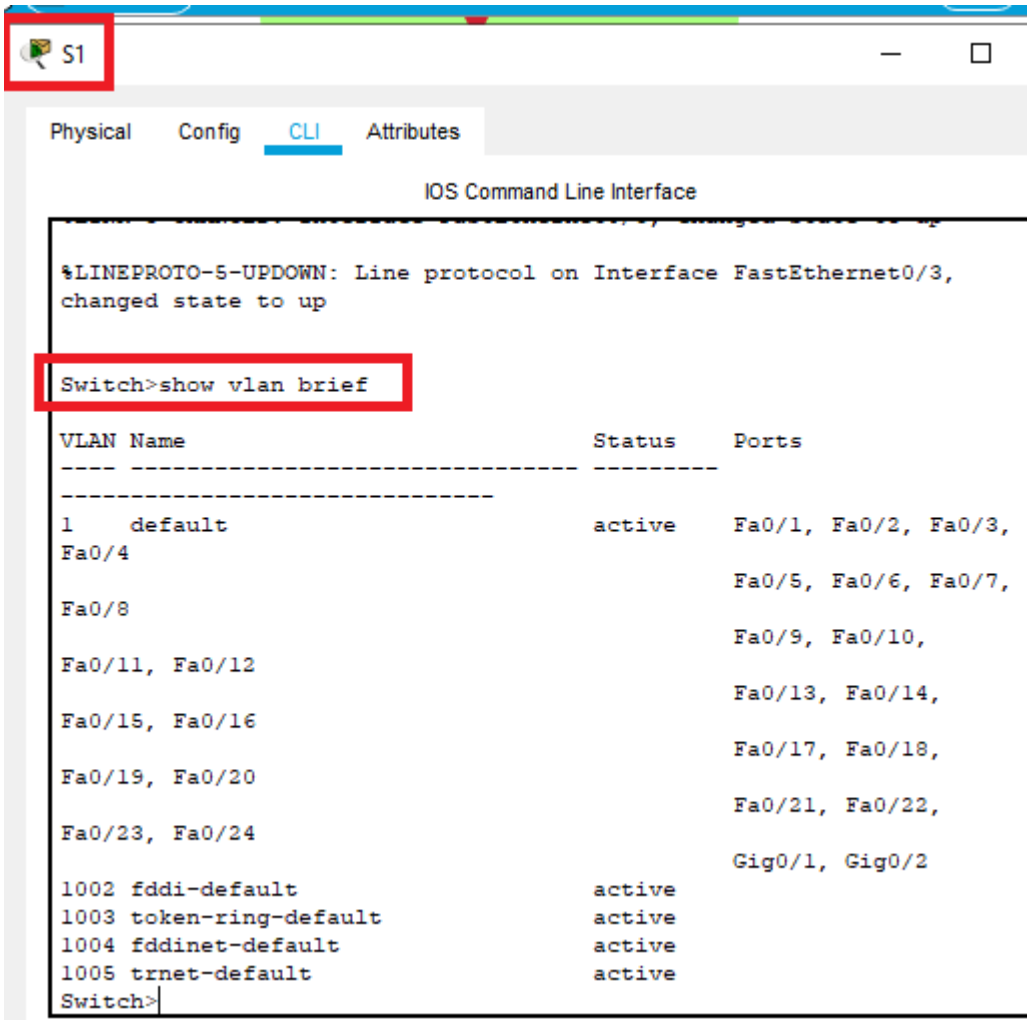

Figure 2. Tabla vlan de S1, después del borrado manual de memoria.

Fuente: Archivo personal. Ejecución del comando en S1.

Borrar la memoria de redes, memoria interna y memoria de trabajo tiene como finalidad no presentar inconsistencias de conectividad y programación al momento de iniciar el proceso de configuración de los router y switch.

S3> Enable

S3# erase startup-config

S3# delete flash: vlan.dat

S3# reboot

S3# reload

S3> show vlan brief

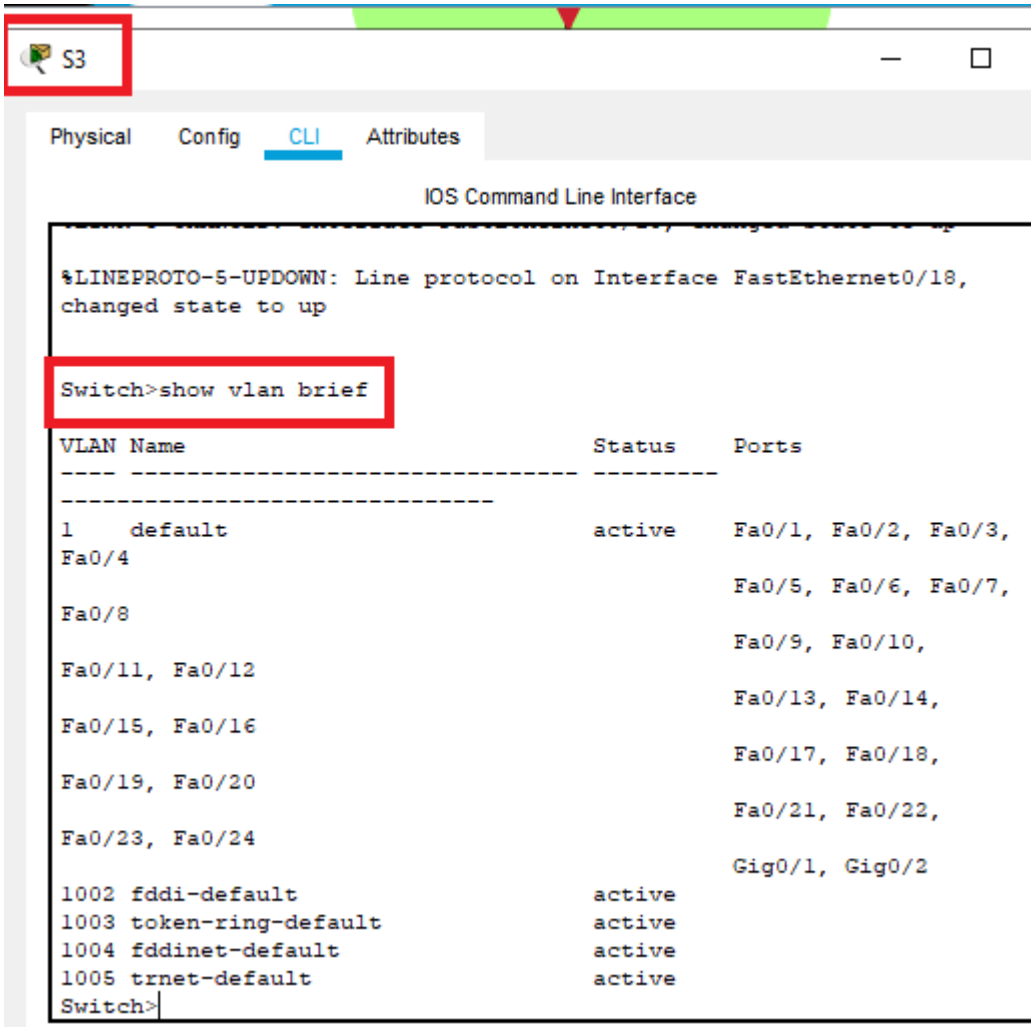

Figure 3 Tabla vlan de S3, después del borrado manual de memoria.

Fuente: Archivo personal. Ejecución del comando en S3.

Posterior al proceso de borrado de memoria se confirma si los puertos se entran en la vlan por defecto, lo que indica que el switch tiene la configuración por defecto activada.

PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

PASO 1: Configurar la computadora de Internet

Línea de comandos de configuración inicial del pc y/o servidor; este proceso se repite para cada host dentro de la topología, algunos tienen parámetros de ajuste diferentes o adicionales de acuerdo a la necesidad de configuración.

Tabla 1 Configuración ipv4 del servidor de servicios http.

Pc internet / servidor	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	209:db8:acad:a::2
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

PASO 2: Configuración de R1

Router> Enable

Router# config t

Router (config)# hostname R1

R1 (config)# no ip Domain-lookup

R1 (config)# Enable password cisco

R1 (config)# line console 0

R1 (config-line)# password class

R1 (config-line)# login

R1 (config-line)# exit

R1 (config)# line vty 0 15

R1 (config-line)# password cisco

R1 (config-line)# login

R1 (config-line)# exit

R1 (config)# service password-encryption

R1 (config)# banner motd “Se prohíbe el acceso no autorizado”

R1 (config)# int s0/0/0

R1 (config-if)# ip address 172.16.1.1 255.255.255.252

R1 (config-if)#exit

R1 (config)#ipv6 unicast-routing

R1 (config)# int s0/0/0

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

R1 (config-if)# ipv6 address fe80::1 link-local

R1 (config-if)# no shutdown

R1 (config-if)# clock rate 128000

PASO 3: Configuración de R2

Router> Enable

Router# config t

Router (config)# hostname R2

R2 (config)# no ip Domain-lookup

R2 (config)# Enable password cisco

R2 (config)# line console 0

R2 (config-line)# password class

R2 (config-line)# login

R2 (config-line)# exit

R2 (config)# line vty 0 15

R2 (config-line)# password cisco

R2 (config-line)# login

R2 (config-line)# exit

R2 (config)# service password-encryption

R2 (config)# banner motd “Se prohíbe el acceso no autorizado”

```
R2 (config)# int s0/0/0
R2 (config-if)# ip address 172.16.1.2 255.255.255.252
R2 (config-if)#exit
R2 (config)#ipv6 unicast-routing
R2 (config)# int s0/0/0
R2 (config-if)# ipv6 address 2001:db8:acad::2/64
R2 (config-if)# ipv6 address fe80::1 link-local
R2 (config-if)# no shutdown
R2 (config-if)# clock rate 128000
R2 (config-if)#exit
R2 (config)# int s0/0/1
R2 (config-if)# ip address 172.16.2.2 255.255.255.252
R2 (config-if)#exit
R2 (config)# int s0/0/1
R2 (config-if)# ipv6 address 2001:db8:acad:2::2/64
R2 (config-if)# ipv6 address fe80::1 link-local
R2 (config-if)# no shutdown
R2 (config-if)# clock rate 128000
R2 (config-if)#exit
R2 (config)# int g0/0
R2 (config-if)# ip address 209.165.200.233 255.255.255.248
R2 (config-if)#exit
R2 (config)# int g0/0
R2 (config-if)# ipv6 address 2001:db8:acad:a::2/64
R2 (config-if)# ipv6 address fe80::1 link-local
R2 (config-if)# no shutdown
R2 (config-if)#exit
R2 (config)# int loopback 0
```

R2 (config-if)# ip address 10.10.10.10 255.255.255.255

R2 (config-if)#exit

PASO 4: Configuración de R3

Router> Enable

Router# config t

Router (config)# hostname R3

R3 (config)# no ip Domain-lookup

R3 (config)# Enable password cisco

R3 (config)# line console 0

R3 (config-line)# password class

R3 (config-line)# login

R3 (config-line)# exit

R3 (config)# line vty 0 15

R3 (config-line)# password cisco

R3 (config-line)# login

R3 (config-line)# exit

R3 (config)# service password-encryption

R3 (config)**#** banner motd “Se prohibe el acceso no autorizado”

R3 (config)# int s0/0/1

R3 (config-if)# ip address 172.16.2.1 255.255.255.252

R3 (config-if)#exit

R3 (config)#ipv6 unicast-routing

R3 (config)# int s0/0/1

R3 (config-if)# ipv6 address 2001:db8:acad:2::1/64

R3 (config-if)# ipv6 address fe80::1 link-local

R3 (config-if)# clock rate 128000

R3 (config-if)# no shutdown

R3 (config)# int loopback 4

R3 (config-if)# ip address 192.168.4.1 255.255.255.0

R3 (config-if)# exit

R3 (config)# int loopback 5

R3 (config-if)# ip address 192.168.5.1 255.255.255.0

R3 (config-if)# exit

R3 (config)# int loopback 6

R3 (config-if)# ip address 192.168.6.1 255.255.255.0

R3 (config-if)# exit

R3 (config)# int loopback 7

R3 (config-if)# ipv6 address 2001:db8:acad:3::1/64

R3 (config-if)# exit

PASO 5: Configurar S1

Switch> Enable

Switch# config t

Switch (config)# hostname S1

S1 (config)# no ip Domain-lookup

S1 (config)# Enable password cisco

S1 (config)# line console 0

S1 (config-line)# password class

S1 (config-line)# login

S1 (config-line)# exit

S1 (config)# line vty 0 15

S1 (config-line)# password cisco

S1 (config-line)# login

S1 (config-line)# exit

S1 (config)# service password-encryption

S1 (config)# banner motd “Se prohibe el acceso no autorizado”

PASO 6: Configurar S3

Switch> Enable

Switch# config t

Switch (config)# hostname S3

S3 (config)# no ip Domain-lookup

S3 (config)# Enable password cisco

S3 (config)# line console 0

S3 (config-line)# password class

S3 (config-line)# login

S3 (config-line)# exit

S3 (config)# line vty 0 15

S3 (config-line)# password cisco

S3 (config-line)# login

S3 (config-line)# exit

S3 (config)# service password-encryption

S3 (config)# banner motd “Se prohíbe el acceso no autorizado”

PASO 7: Verificar la conectividad de la red

Tabla 2 Prueba de conectividad R1, R2 y Servidor

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2, 172.16.2.2	5/5
R2	R3, S0/0/1	172.16.2.1	5/5
Servidor	Gateway predeterminado	209.165.200.229	5/5

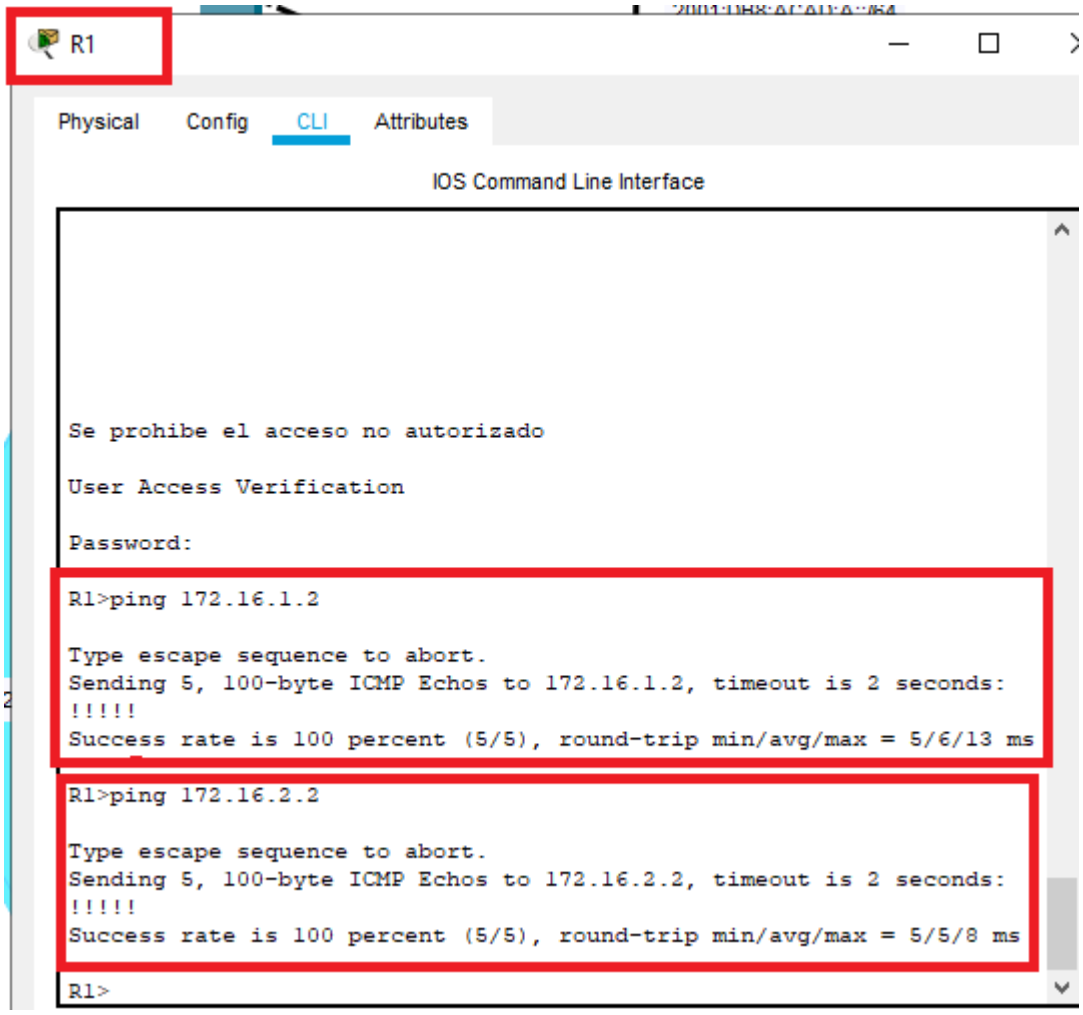

Figure 4 Ping hacia la interfaz s0/0/0.

Fuente: Archivo personal. Ejecución del comando ping en R1.

Se ejecuta el comando ping desde la línea de comandos router 1 hacia las direcciones IPv4 172.16.1.2 (interfaz s0/0/0 de R2) y 172.16.2.2 (interfaz s0/0/1 de R2) con resultado satisfactorio.

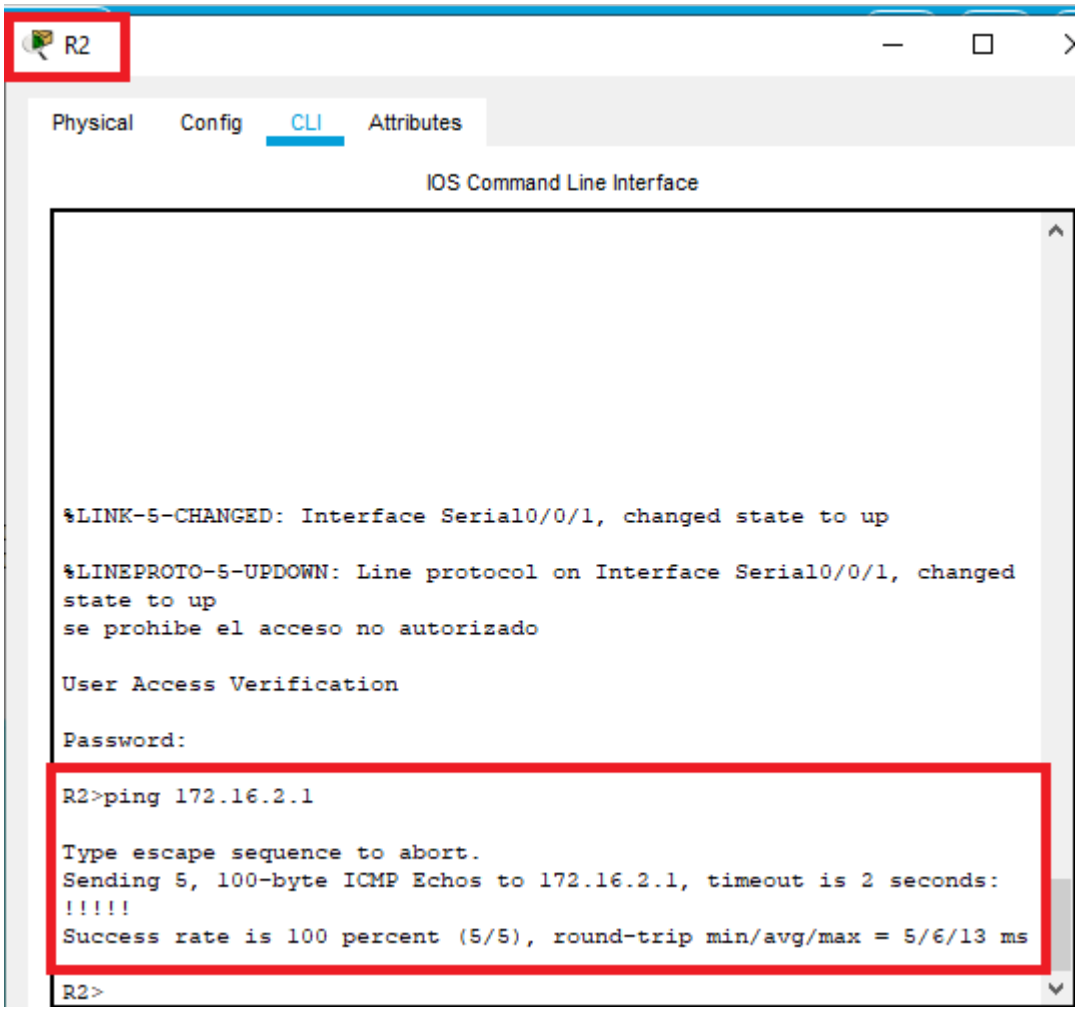

Figure 5 Ping hacia la interfaz s0/0/0 de R3.

Fuente: Archivo personal. Ejecución del comando ping en R2.

Ping desde R2 hacia la interfaz de R3, utilizando la dirección IPv4 asignada al puerto. Con resultado satisfactorio.

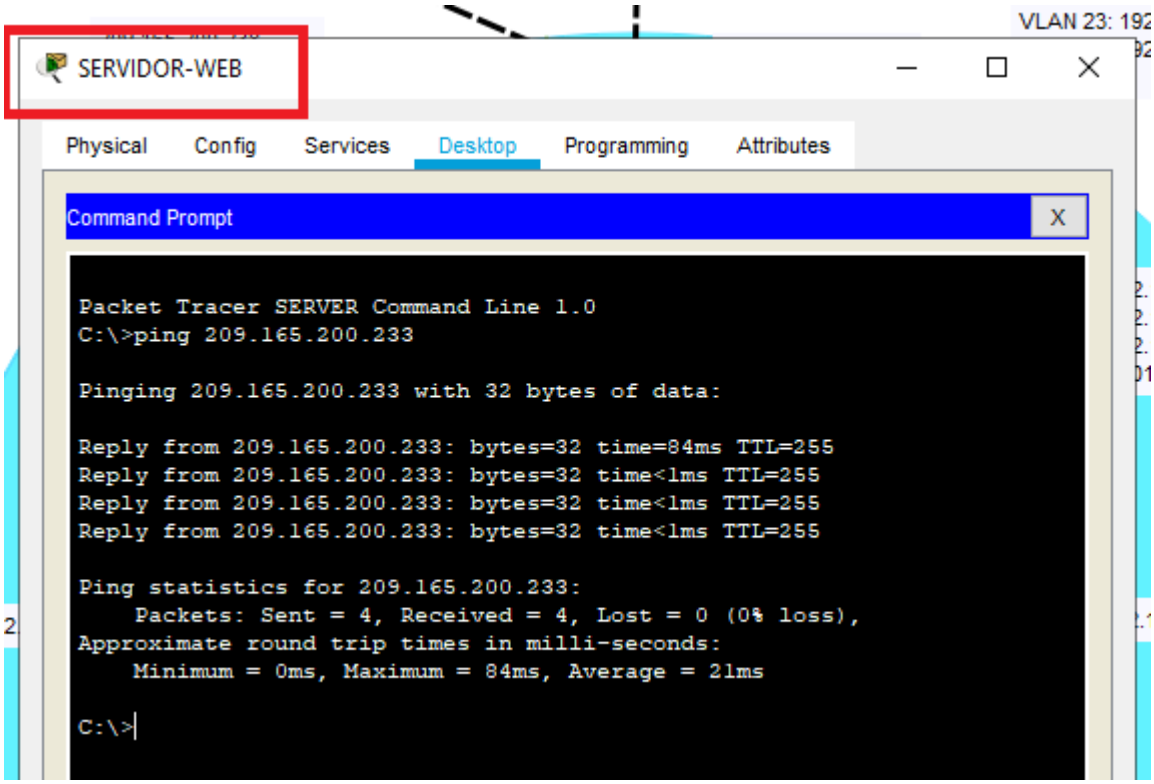

Figure 6 Ping hacia el gateway en R2.

Fuente: Archivo personal. Ejecución del comando ping en el servidor.

Ping desde el servidor con funciones web, hasta el puerto gigabit Ethernet de R2 (g0/0). [1]

[1] Se utiliza un servidor con funciones web en reemplazo de la configuración que utiliza el comando http server en R2 la cual no es soportada en simulaciones.

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

PASO 1: Configurar S1

S1(config)# vlan 21

S1(config-vlan)# exit

S1(config) interface vlan 21

S1(config-if)# ip address 192.168.21.1 255.255.255.0

S1(config-if)# no shutdown

S1(config-if)# exit

S1(config)# interface vlan 23

S1(config-if)# ip address 192.168.23.1 255.255.255.0

S1(config-if)# no shutdown

S1(config-if)# exit

S1(config)# interface vlan 99

S1(config-if)# ip address 192.168.99.1 255.255.255.0

S1(config-if)# no shutdown

S1(config-if)# exit

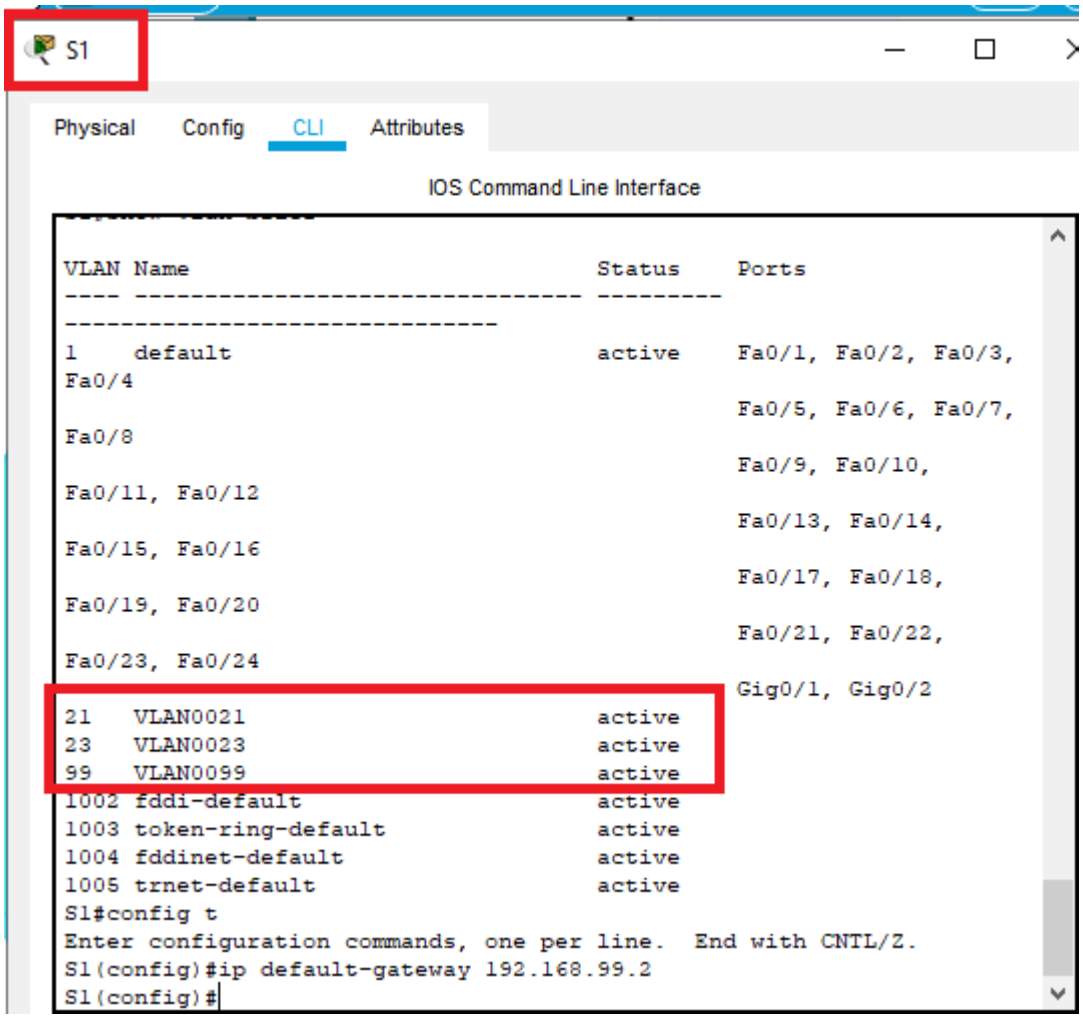

Figure 7 Show vlan brief en S1, con redes vlan 21, 23 y 99.

Fuente Archivo personal. Ejecución del comando show vlan brief.

Se emite el comando show vlan brief en S1 para constatar que las vlan se han configurado adecuadamente, posteriormente se utilizara la vlan de acuerdo al requerimiento de configuración. [2]

S1(config)# ip default-gateway 192.168.99.2

S1(config)# int f0/3

S1(config-if)# switchport mode trunk

[2] La configuración de direcciones directas vlan en el switch S1 y S3 fue deshabilitada, se tenían conflictos de conectividad para las sub redes vlan 21, 23 y 99.

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

PASO 2: Configurar en S3

S3(config)# int f0/18

S3(config-if)# ip address 192.168.21.1 255.255.255.0

S3(config-if)# no shutdown

S3(config-if)# exit

S3(config)# interface vlan 23

S3(config-if)# ip address 192.168.23.1 255.255.255.0

S3(config-if)# no shutdown

S3(config-if)# exit

S3(config)# interface vlan 99

S3(config-if)# ip address 192.168.99.1 255.255.255.0

S3(config-if)# no shutdown

S3(config-if)# exit

S3(config)# ip default-gateway 192.168.99.3

S3(config)# vlan 1

S3(config-vlan)# exit

S3(config)# interface f0/3

S3(config-if)# switchport mode trunk

S3(config-if)# exit

S3(config)# interface f0/18

S3(config-if)# switchport access vlan 23

S3(config-if)# exit

S3(config)# interface range f0/1 – 2

S3(config-if-range)# switchport mode access

S3(config-if)# shutdown

S3(config-if-range)# exit

```
S3(config)# interface range f0/4 – 17
S3(config-if-range)# switchport mode access
S3(config-if-range)# shutdown
S3(config-if-range)# exit
S3(config)# interface range f0/19 – 24, g0/1 – 2
S3(config-if-range)# switchport mode access
S3(config-if-range)# shutdown
S3(config-if-range)# exit
```

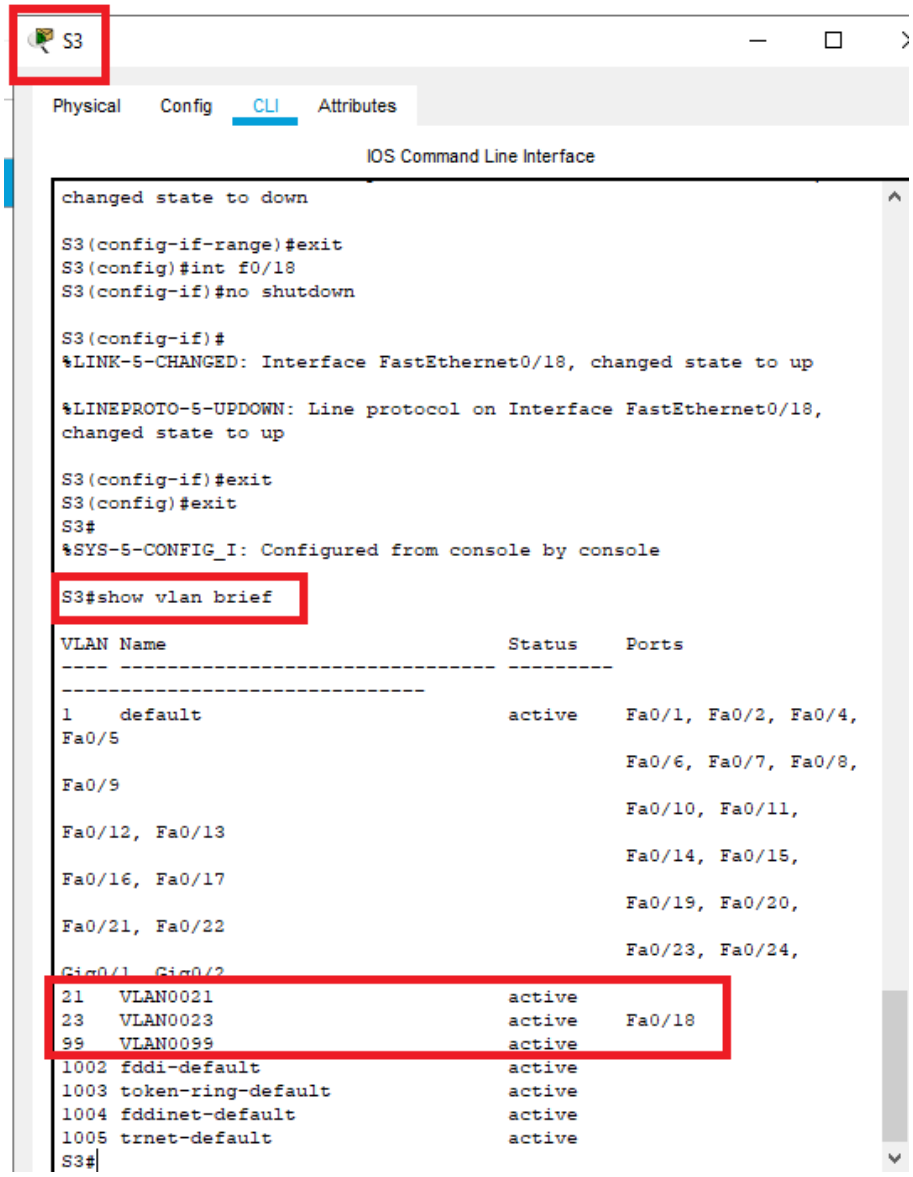

Figure 8 Show vlan brief en S3, con f0/18 a vlan 23.

Fuente: Archivo personal. Ejecución del comando en S3.

Se emite el comando show vlan brief en S3: verificar las vlan creadas y constatar que la interfaz f0/18 utiliza una vlan para comunicación cambiándola por la vlan nativa.

PASO 3: Configurar R1

R1(config)# int g0/1.21

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)# 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)# encapsulation dot1Q 99

R1(config-subif)# ip address 192.168.99.1 255.255.255.0

R1(config-subif)# exit

R1(config)# int g0/1

R1(config-if)# no shutdown

PASO 4: Verificar la conectividad de la red

Tabla 3 Pruebas de conectividad desde S1 y S3

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	5/5
S3	R1, dirección VLAN 99	192.168.99.1	5/5
S1	R1, dirección VLAN 21	192.168.21.1	5/5
S3	R1, dirección VLAN 23	192.168.23.1	5/5

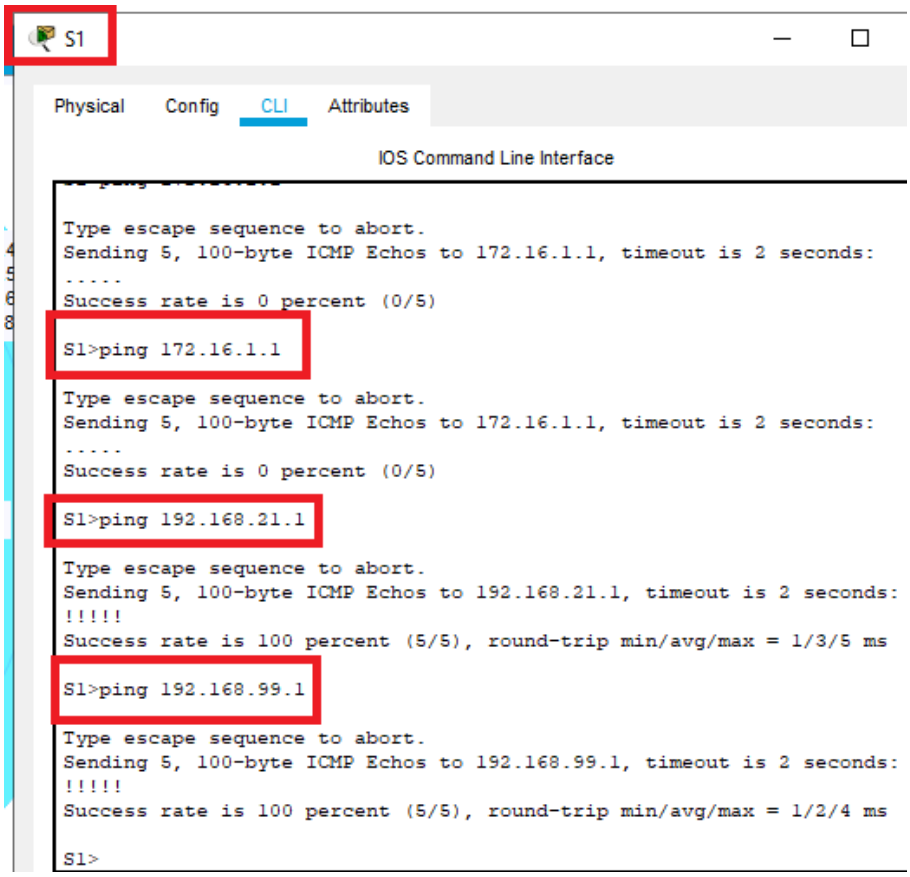

Figure 9 Ping desde S1 hasta R1, vlan 99 y vlan 21.

Fuente: Archivo personal. Prueba de conexión punto a punto en S1

Se realiza la prueba de conexión desde el switch S1 hasta las interfaces virtuales en R1, utilizando el enlace de f0/5 a gigabit Ethernet de R1.

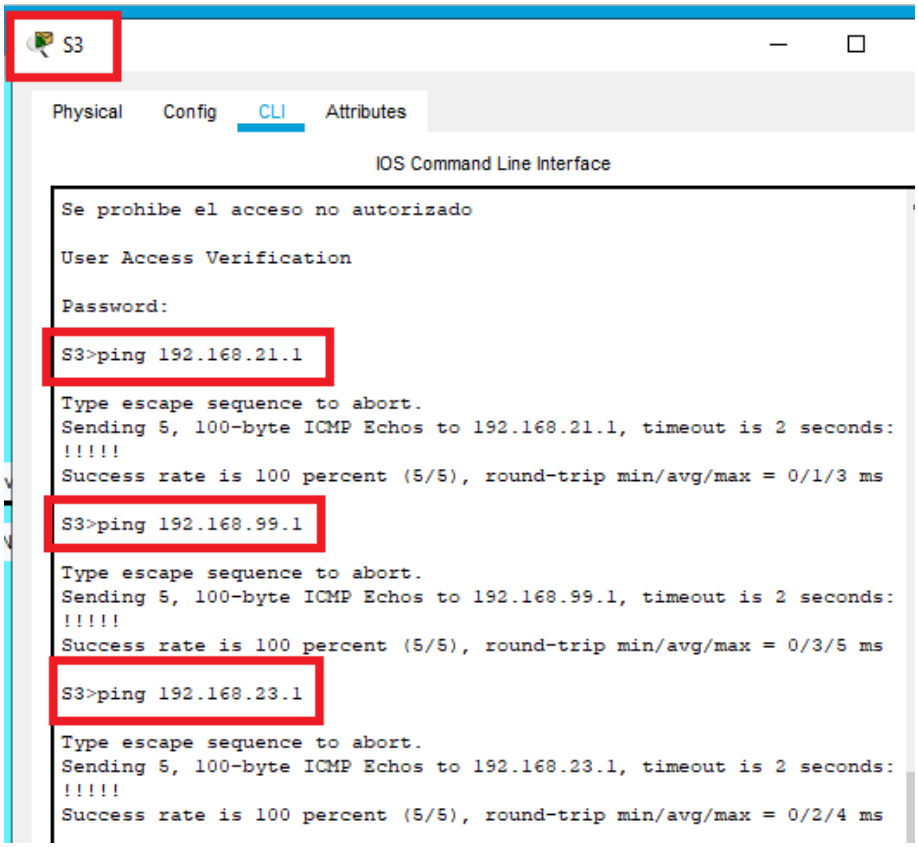

Figure 10 Ping desde S3 hasta R1 vlan 99 y vlan 23

Fuente: Archivo personal. Prueba de conexión punto a punto en S3.

Se repite la misma prueba de conexión que en S1; S3 se comunica con R1 a través del enlace de la interfaz f0/3 de S1 (modo trunk) y F0/5, hasta alcanzar los puertos virtuales de R1.

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

PASO 1: Configurar RIPv2 en el R1

R1(config)# router rip

R1(config-router)# version 2

R1(config-router)# passive-interface g0/0

R1(config-router)# passive-interface g0/1

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

R1(config-router)# network 192.168.0.0

R1(config-router)# network 172.16.0.0

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

R1(config-router)# network 192.168.0.0

R1(config-router)# network 172.16.0.0

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

R1(config-router)# network 192.168.0.0

R1(config-router)# network 172.16.0.0

R1(config-router)# exit

R1(config)# router rip

R1(config-router)# no auto-summary

R1(config-router)# exit

PASO 2: Configurar RIPv2 en el R2

R2(config)# router rip

R2(config-router)# version 2

R2(config-router)# passive-interface s0/0/0

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

R2(config-router)# network 10.10.10.10

R2(config-router)# exit

R2(config)# router rip

R2(config-router)# no auto-summary

PASO 3: Configurar RIPv2 en el R3

R3(config)# router rip

R3(config-router)# version 2

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

R3(config-router)# network 192.168.4.0

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

R3(config-router)# network 192.168.5.0

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

R3(config-router)# network 192.168.6.0

R3(config-router)# exit

R3(config)# router rip

R3(config-router)# no auto-summary

R3(config-router)# exit

PASO 4: Verificar la información de RIP

Tabla 4 Verificación y configuraciones de RIP

Pregunta	Respuesta
¿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, show run, show ip interface brief, show ip route,
¿Qué comando muestra solo las rutas RIP?	show ip rip database.
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show ip rip database, show ip route

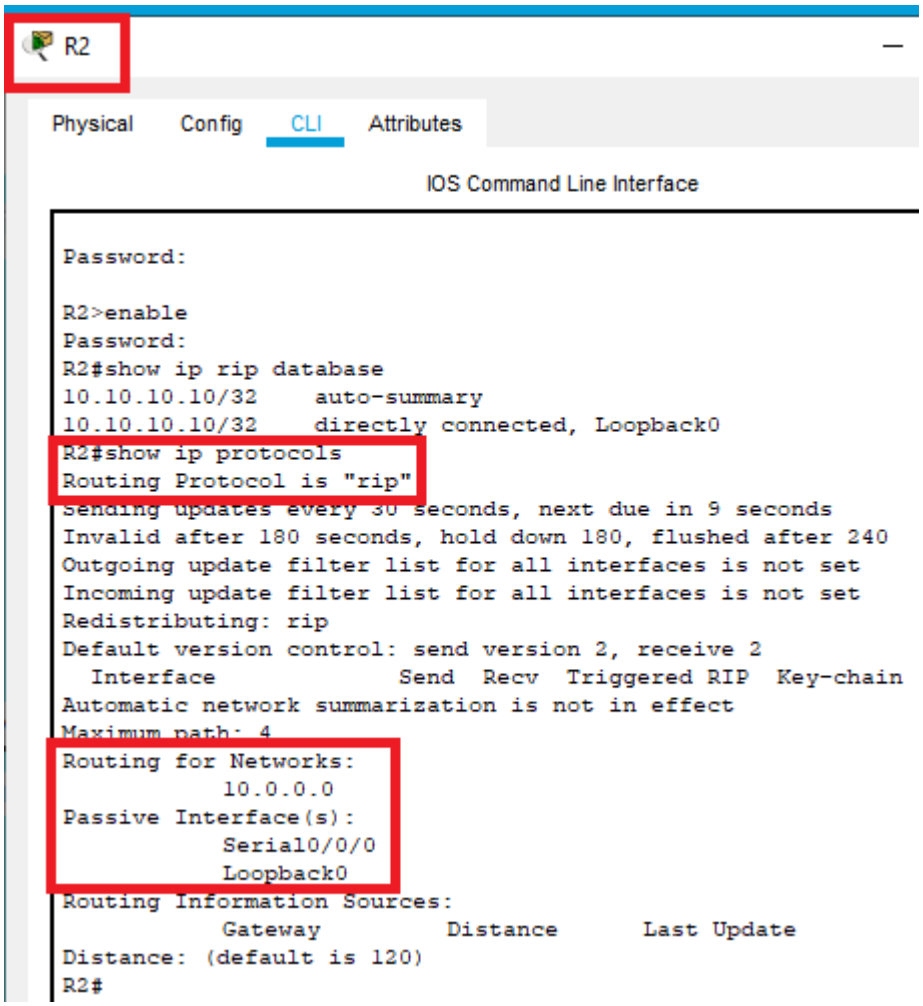

Figure 11Comando show ip protocols en R2 con verificación de rip v2

Fuente: Archivo personal. Ejecución del comando en R2

Se ejecuta un comando de diagnóstico (show ip protocols) para determinar el protocolo de ruting, versión, ruting for networks y las interfaces configuradas como pasivas. También permite verificar proceso de sumarización, tiempo de envió de actualizaciones.

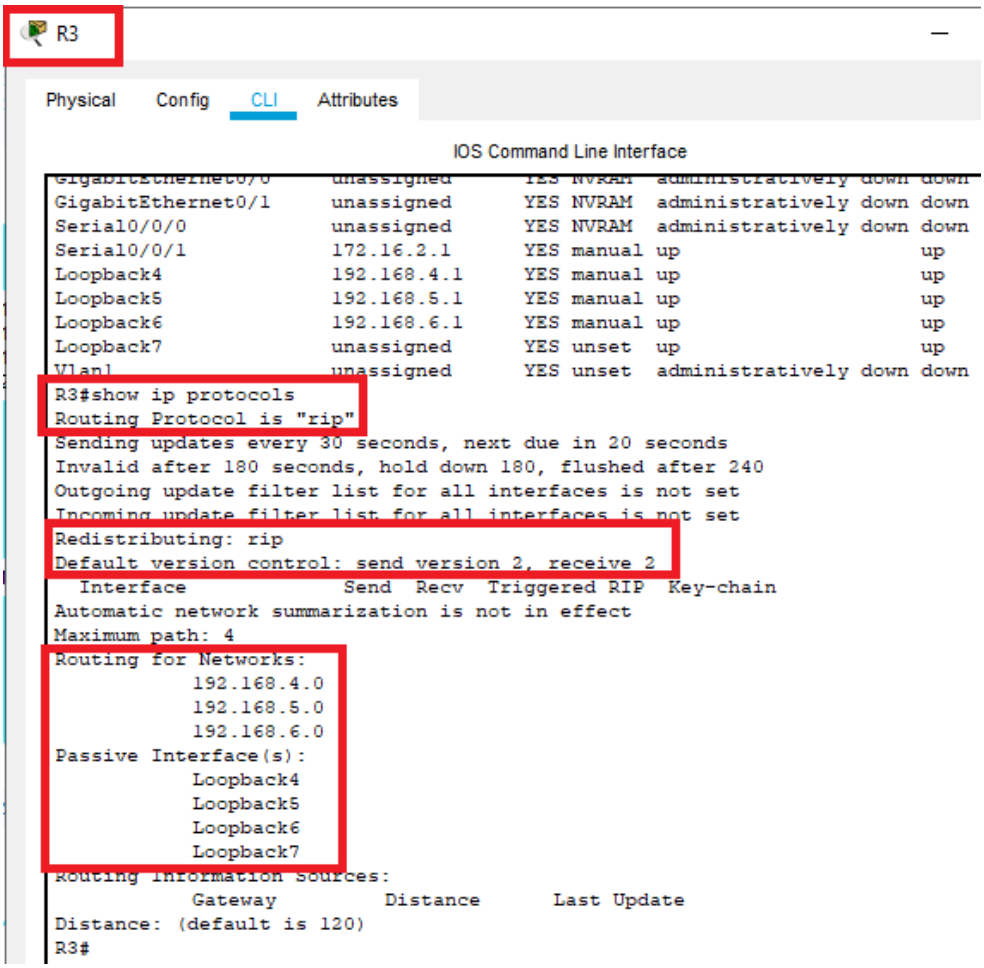

Figure 12 Comando show ip protocols en R3 con verificación de rip v2

Fuente: Archivo personal. Ejecución del comando en R3

Se ejecuta un comando de diagnóstico (show ip protocols en R3) para determinar el protocolo de ruting, versión, ruting for networks y las interfaces configuradas como pasivas. También permite verificar proceso de sumarización, tiempo de envió de actualizaciones.

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

PASO 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

```
R1(config)# ip dhcp excluded-address 192.168.21.0 192.168.21.19
R1(config)# ip dhcp excluded-address 192.168.23.0 192.168.23.19
R1(config)# ip dhcp pool ACCT
R1(dhcp-config)# network 192.168.21.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.21.1
R1(dhcp-config)# dns-server 10.10.10.10
R1(dhcp-config)# domain-name ccna-sa.com
R1(dhcp-config)# exit
R1(config)# ip dhcp pool ENGNR
R1(dhcp-config)# network 192.168.23.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.23.1
R1(dhcp-config)# dns-server 10.10.10.10
R1(dhcp-config)# domain-name ccna-sa.com
R1(dhcp-config)# exit
```

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

```
R2(config)# domain-name ccna-sa.com
R2(config)# username webuser privilege 15 secret cisco12345
R2(config)# line vty 0 4
R2(config-line)# transport input ssh
R2(config-line)# login local
R2(config-line)# exit
R2(config)# crypto key generate rsa
```

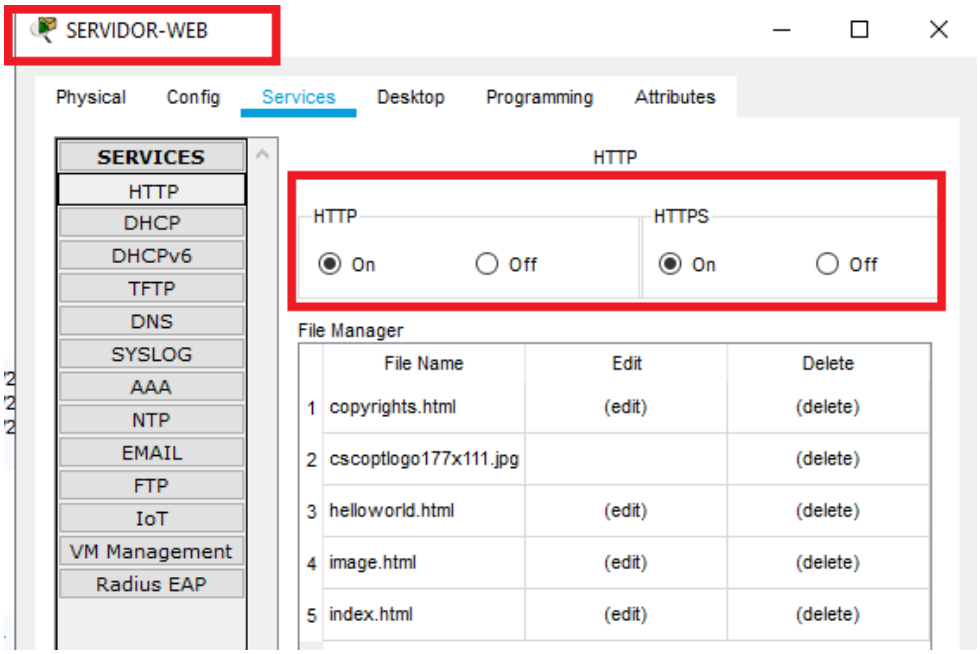

Figure 13 Activación del servicio de http en servidor web y apagado de las configuración no utilizadas.

Fuente: Archivo personal. Servidor web.

Dado que en la topología se establece un servidor web, se utiliza un servidor con la configuración web habilitada únicamente (los demás servicios están apagados) y se establece una dirección ip estática. (209.165.200.234).

R2(config)# ip nat inside source static 209.165.200.238 209.165.200.229

R2(config)# int g0/0

R2(config-if)# ip nat inside

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

R2(config-if)#ip nat outside

R2(config-if)# exit

R2(config)# ip nat pool public_access 192.168.21.0 192.168.21.254 netmask 255.255.255.0

R2(config)# ip nat pool public_access 192.168.23.0 192.168.23.254 netmask 255.255.255.0

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

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

PASO 2.1 Ajustes en R1:

R1(config)# int g0/1

R1(config-if)# ip nat inside

R1(config-if)# int s0/0/0

R1(config-if)# ip nat outside

R1(config-if)# exit

R1(config)# access-list 1 permit 192.168.21.0 0.0.0.255

R1(config)# access-list 2 permit 192.168.23.0 0.0.0.255

R1(config)# ip nat pool public_access_1 192.168.21.0 192.168.21.254 netmask 255.255.255.0

R1(config)# ip nat pool public_access_2 192.168.23.0 192.168.23.254 netmask 255.255.255.0

R1(config)# ip nat inside source list 1 pool public_access_1

R1(config)# ip nat inside source list 2 pool public_access_2

PASO 2.2 Ajustes en R3:

R3(config)# int s0/0/1

R3(config-if)# ip nat inside

R3(config-if)# int range loopback 4 – 6

R3(config-if-range)# ip nat outside

R3(config-if-range)# exit

R3(config)# access-list 1 permit 192.168.0.0 0.0.0.255

R3(config)# ip nat pool public_access 192.168.0.0 192.168.0.254 netmask 255.255.255.0

R3(config)# ip nat inside source list 1 pool public_access_1

PASO 2.3 Ajustes en R2:

R2(config)# ip nat pool public_access_1 209.165.200.209.165.200.228 netmask 255.255.255.248

R2(config)# ip nat INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

R3(config)# ip nat inside source list 1 pool INTERNET.

PASO 3: Verificar el protocolo DHCP y la NAT estática

Tabla 5 Verificación de los servicios DHCP

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Obtiene ip 192.168.21.20
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Obtiene ip 192.168.23.20
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	La configuración de vlan realizada en R1 permite comunicar satisfactoriamente las vlan de S1 y S3.
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	El comando ip server y http server no es soportado en la simulación. [3]

[3] La configuración del servidor con acceso remoto no es posible habilitarla debido a que los comandos no son soportados en simulaciones y la alternativa es utilizar un servidor dedicado con utilidad http.

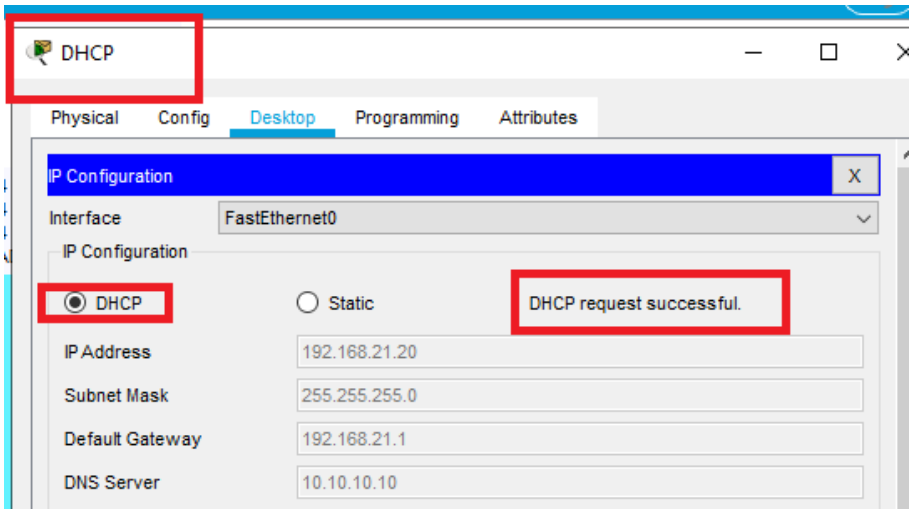

Figure 14 Dhcp solicitado desde el pc vlan 21

Fuente: Archivo personal. Solicitud de dirección ipv4.

El pc dhcp obtiene dirección ipv4 desde el router R1 donde se encuentra alojado el pool para su vlan (21).

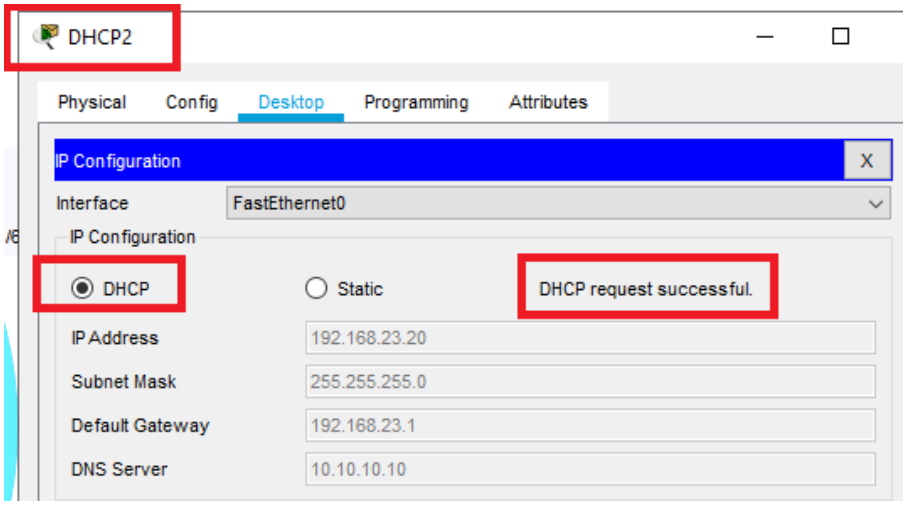

Figure 15 Dhcp solicitado desde el pc vlan 23

Fuente: Archivo personal. Solicitud de dirección ipv4.

El pc dhcp2 obtiene dirección ipv4 desde el router R1 donde se encuentra alojado el pool para su vlan (23), gracias a la comunicación trunk de S3 y S1 que alcanza a R1.

PARTE 6: CONFIGURAR NTP

R2# clock set 20:38:00 05 may 2020

R2# copy running-config startup-config

R2(config)# ntp master

R2(config)# int loopback 0

R2(config-if)# exit

R1(config)# ntp server 10.10.10.10

R1(config)# int s0/0/0

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

R1(config-if)# exit

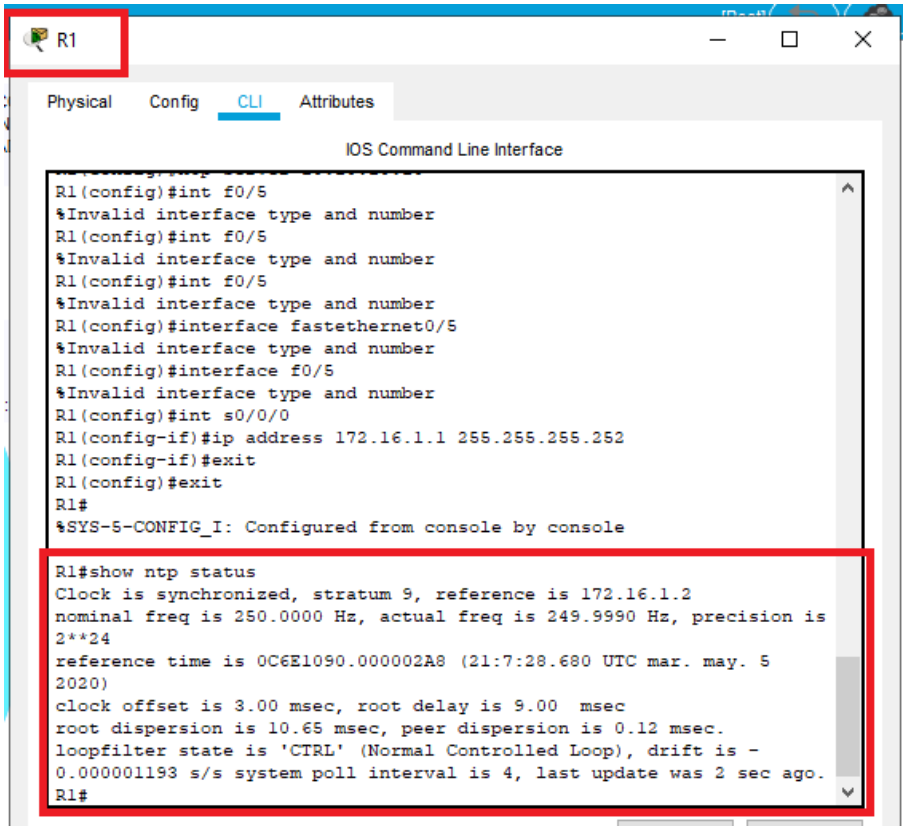

Figure 16 Comando show ntp status en R1, verificando sincronización con R2

Fuente: Archivo personal. Ejecución del comando en R1.

La configuración de ntp facilita la sincronización de reloj con otros dispositivos de la red, al mismo tiempo que permite mejorar la comunicación entre ellos. En el status se muestran los parámetros de ajuste y respuesta, también la dirección de referencia junto con la hora establecida.

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

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

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

R2(config-std-nacl)# permit host 192.168.21.20

R2(config-std-nacl)# deny any

R2(config-std-nacl)# exit

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

R2(config-std-nacl)# permit host 192.168.21.0

R2(config-std-nacl)# deny any

R2(config-std-nacl)# exit

R2(config)# line vty 0 15

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

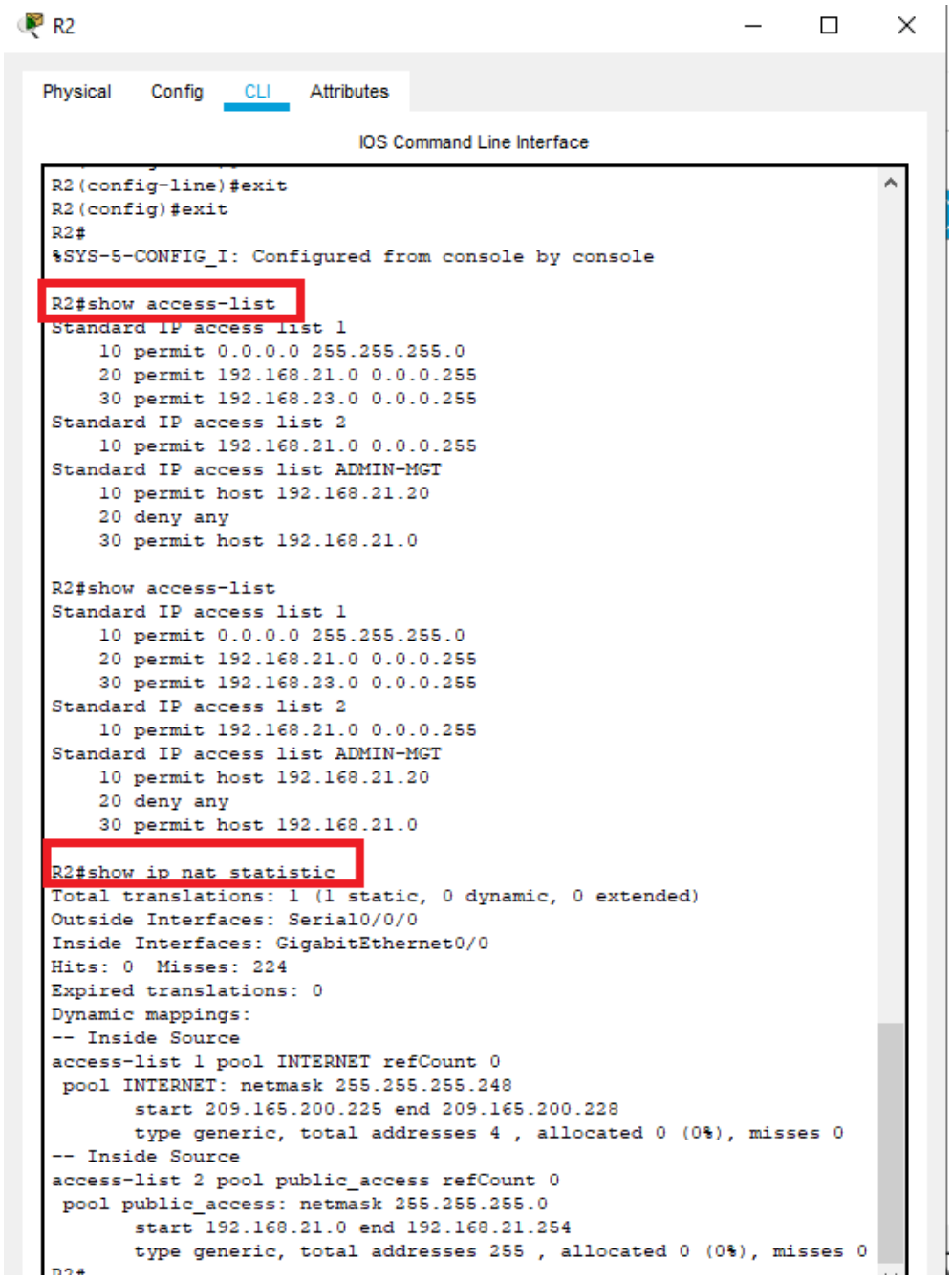

Figure 17 Comandos show access-list y show ip nat statistic

Fuente: Archivo personal Ejecución del comando en R2.

Se configura la lista de control de acceso (ACL), para evitar que direcciones ajenas a las listadas puedan conectarse a la red, se utilizan los comandos de verificación (show) para corroborar que las redes se han listado correctamente.

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

Tabla 6 Aplicación de los comandos show para verificación de información.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show ip nat statistic
Restablecer los contadores de una lista de acceso	Clear ip nat translation *, clear ip nat statistic
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show Access-list
¿Con qué comando se muestran las traducciones NAT?	Show ip nat statistic, show ip nat translations **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	no ip nat inside source static i.p. mascara de red

PARTE 8: PRUEBA DE CONECTIVIDAD Y ACTUALIZACIONES

PASO 1: Cambio de protocolo

Se actualiza la configuración del protocolo de routing en R1, R2 y R3 para superar la conectividad limitada en los distintos router, se habilita el servidor web (no se habilita el servicio dns).

R1(config)# router ospf 1

R1(config-router)# network 172.16.1.0 0.0.0.3 area 0

R1(config-router)# network 172.16.2.0 0.0.0.3 area 0

R1(config-router)# network 192.168.21.0 0.0.0.255 area 0

R1(config-router)# network 192.168.23.0 0.0.0.255 area 0

R1(config-router)# network 192.168.99.0 0.0.0.255 area 0

R2(config)# router ospf 1

R2(config-router)# network 209.165.200.0 0.0.0.3 area 0

R2(config-router)# network 10.10.10.8 0.0.0.3 area 0

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

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

R3(config)# router ospf 1

R3(config-router)# network 192.168.4.0 0.0.0.255 area 0

R3(config-router)# network 192.168.5.0 0.0.0.255 area 0

R3(config-router)# network 192.168.6.0 0.0.0.255 area 0

R3(config-router)# network 172.16.2.0 0.0.0.3 area 0

PASO 2: Prueba de conectividad de la red

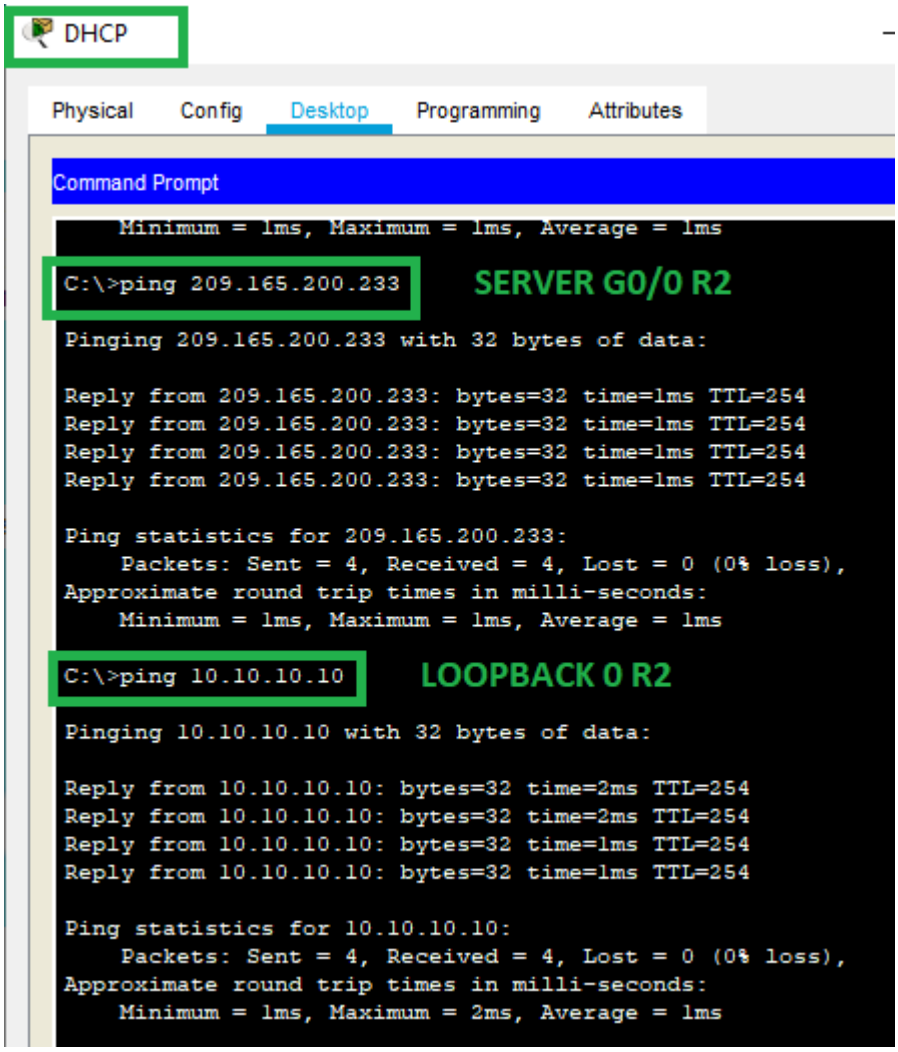

Figure 18 Ping desde dhcp pc a R2

Fuente: Archivo personal. Prueba de conectividad desde pc dhcp en S1 hasta R2.

Posterior a la nueva configuración se verifica la conectividad desde pc dhcp de la red S1 hasta R2 y la interfaz loopback 0 y gigabit Ethernet 0/0.

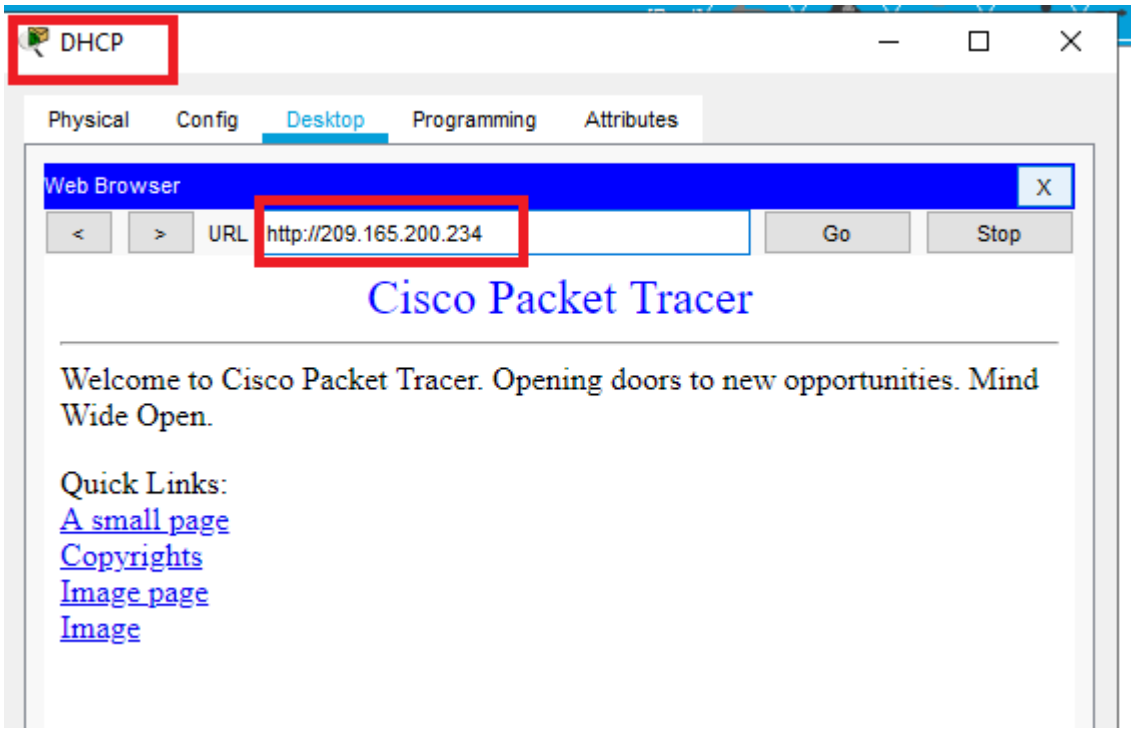

Figure 19 Pagina web del servidor.

Fuente: Archivo personal. Se verifica página web desde un navegador.

Utilizando el pc dhcp de la red S1 se accede a la página web del servidor por la dirección ipv4 asignada, no se habilita el servicio dns.

PRACTICA 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.

Topología.

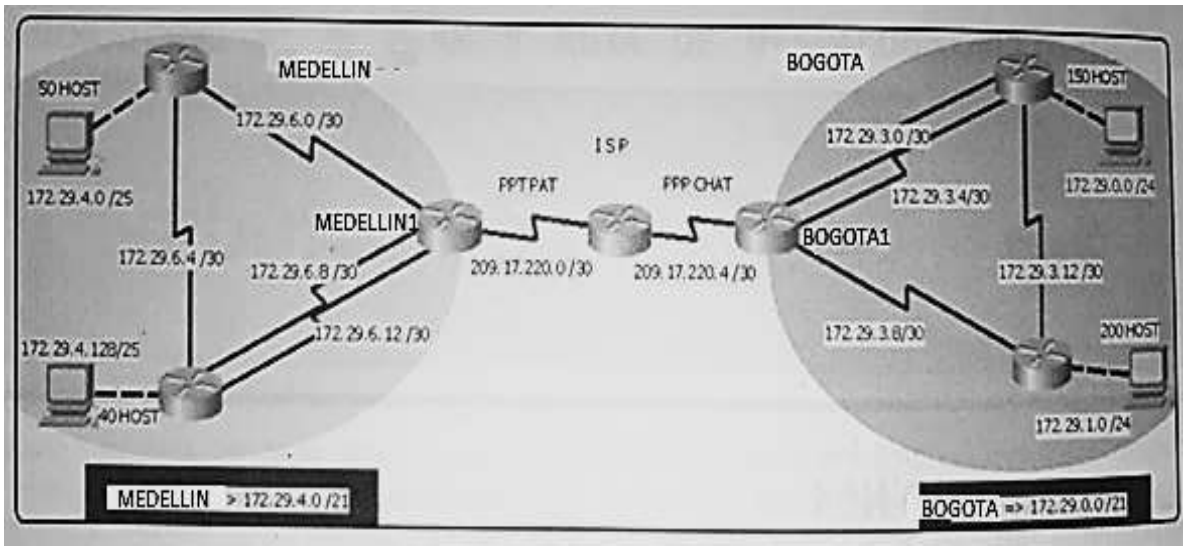

Figure 20 Topología de la red a simular.

Fuente: Documento de la actividad – prueba de habilidades practicas

PARTE 1: CONFIGURACIÓN INICIAL

PASO 1: configurar router Medellín 1, 2 y 3

Router> Enable

Router# config t

Router (config)# hostname MEDELLIN1

MEDELLIN1(config)# no ip Domain-lookup

MEDELLIN1(config)# Enable password cisco

MEDELLIN1(config)# line console 0

MEDELLIN1(config-line)# password class

MEDELLIN1(config-line)# login

MEDELLIN1(config-line)# exit

MEDELLIN1(config)# line vty 0 15

MEDELLIN1(config-line)# password cisco

MEDELLIN1(config-line)# login

MEDELLIN1(config-line)# exit

MEDELLIN1(config)# service password-encryption

MEDELLIN1(config)# banner motd “Se prohibe el acceso no autorizado”

Router> Enable

Router# config t

Router (config)# hostname MEDELLIN2

MEDELLIN2(config)# no ip Domain-lookup

MEDELLIN2(config)# Enable password cisco

MEDELLIN2(config)# line console 0

MEDELLIN2(config-line)# password class

MEDELLIN2(config-line)# login

MEDELLIN2(config-line)# exit

MEDELLIN2(config)# line vty 0 15

MEDELLIN2(config-line)# password cisco

MEDELLIN2(config-line)# login

MEDELLIN2(config-line)# exit

MEDELLIN2(config)# service password-encryption

MEDELLIN2(config)# banner motd “Se prohibe el acceso no autorizado”

Router> Enable

Router# config t

Router (config)# hostname MEDELLIN3

MEDELLIN3(config)# no ip Domain-lookup

MEDELLIN3(config)# Enable password cisco

MEDELLIN3(config)# line console 0

MEDELLIN3(config-line)# password class

MEDELLIN3(config-line)# login

MEDELLIN3(config-line)# exit

MEDELLIN3(config)# line vty 0 15

MEDELLIN3(config-line)# password cisco

MEDELLIN3(config-line)# login

MEDELLIN3(config-line)# exit

MEDELLIN3(config)# service password-encryption

MEDELLIN3(config)# banner motd “Se prohibe el acceso no autorizado”

PASO 2: configurar router Bogotá 1, 2 y 3

Router> Enable

Router# config t

Router (config)# hostname BOGOTA1

BOGOTA1(config)# no ip Domain-lookup

BOGOTA1(config)# Enable password cisco

BOGOTA1(config)# line console 0

BOGOTA1(config-line)# password class

BOGOTA1(config-line)# login

BOGOTA1(config-line)# exit

BOGOTA1(config)# line vty 0 15

BOGOTA1(config-line)# password cisco

BOGOTA1(config-line)# login

BOGOTA1(config-line)# exit

BOGOTA1(config)# service password-encryption

BOGOTA1(config)# banner motd “Se prohibe el acceso no autorizado”

Router> Enable

Router# config t

Router (config)# hostname BOGOTA2

BOGOTA2(config)# no ip Domain-lookup

BOGOTA2(config)# Enable password cisco

BOGOTA2(config)# line console 0

BOGOTA2(config-line)# password class

BOGOTA2(config-line)# login

BOGOTA2(config-line)# exit

BOGOTA2(config)# line vty 0 15

BOGOTA2(config-line)# password cisco

BOGOTA2(config-line)# login

BOGOTA2(config-line)# exit

BOGOTA2(config)# service password-encryption

BOGOTA2(config)# banner motd “Se prohibe el acceso no autorizado”

Router> Enable

Router# config t

Router (config)# hostname BOGOTA1

BOGOTA3(config)# no ip Domain-lookup

BOGOTA3(config)# Enable password cisco

BOGOTA3(config)# line console 0

BOGOTA3(config-line)# password class

BOGOTA3(config-line)# login

BOGOTA3(config-line)# exit

BOGOTA3(config)# line vty 0 15

BOGOTA3(config-line)# password cisco

BOGOTA3(config-line)# login

BOGOTA3(config-line)# exit

BOGOTA3(config)# service password-encryption

BOGOTA3(config)# banner motd “Se prohibe el acceso no autorizado”

PASO 3: configurar router ISP

Router> Enable

Router# config t

Router (config)# hostname ISP

ISP(config)# no ip Domain-lookup

ISP(config)# Enable password cisco

ISP(config)# line console 0

ISP(config-line)# password class

ISP(config-line)# login

ISP(config-line)# exit

ISP(config)# line vty 0 15

ISP (config-line)# password cisco

ISP (config-line)# login

ISP(config-line)# exit

ISP(config)# service password-encryption

ISP(config)# banner motd “Se prohibe el acceso no autorizado”

PASO 4: configurar OSPF en los routers

MEDELLIN1(config)# router ospf 1

MEDELLIN1(config-router)# network 172.29.6.0 0.0.0.255 area 0

MEDELLIN1(config-router)# network 172.29.6.8 0.0.0.255 area 0

MEDELLIN1(config-router)# network 172.29.6.12 0.0.0.255 area 0

MEDELLIN1(config-router)# network 209.17.220.0 0.0.0.255 area 0

```
MEDELLIN1(config-router)# exit

MEDELLIN2(config)# router ospf 1
MEDELLIN2(config-router)# network 172.29.4.0 0.0.0.255 area 0
MEDELLIN2(config-router)# network 172.29.6.0 0.0.0.255 area 0
MEDELLIN2(config-router)# exit

MEDELLIN3(config)# router ospf 1
MEDELLIN3(config-router)# network 172.29.6.0 0.0.0.255 area 0
MEDELLIN3(config-router)# network 172.29.6.8 0.0.0.255 area 0
MEDELLIN3(config-router)# network 172.29.6.12 0.0.0.255 area 0
MEDELLIN3(config-router)# network 172.29.4.0 0.0.0.255 area 0
MEDELLIN3(config-router)# exit

ISP(config)# router ospf 1
ISP(config-router)# network 209.17.220.0 0.0.0.255 area 0
ISP(config-router)# network 209.17.220.4 0.0.0.255 area 0
ISP(config-router)# exit

BOGOTA1(config)# router ospf 1
BOGOTA1(config-router)# network 209.17.220.4 0.0.0.255 area 0
BOGOTA1(config-router)# network 172.29.3.0 0.0.0.255 area 0
BOGOTA1(config-router)# network 172.29.3.4 0.0.0.255 area 0
BOGOTA1(config-router)# network 172.29.3.8 0.0.0.255 area 0
BOGOTA1(config-router)# exit
```

BOGOTA2(config)# router ospf 1

BOGOTA2(config-router)# network 172.29.3.0 0.0.0.255 area 0

BOGOTA2(config-router)# network 172.29.3.4 0.0.0.255 area 0

BOGOTA2(config-router)# network 172.29.3.12 0.0.0.255 area 0

BOGOTA2(config-router)# network 172.29.0.0 0.0.0.255 area 0

BOGOTA2(config-router)# exit

BOGOTA3(config)# router ospf 1

BOGOTA3(config-router)# network 172.29.1.0 0.0.0.255 area 0

BOGOTA3(config-router)# network 172.29.3.0 0.0.0.255 area 0

BOGOTA3(config-router)# network 172.29.3.8 0.0.0.255 area 0

BOGOTA3(config-router)# network 172.29.3.12 0.0.0.255 area 0

BOGOTA3(config-router)# exit

PASO 5: Enrutamiento y asignación de direcciones

ISP(config)# int s0/0/0

ISP(config-if)# ip address 209.17.220.1 255.255.255.252

ISP(config-if)# no shutdown

ISP(config-if)# clock rate 128000

ISP(config)# int s0/0/1

ISP(config-if)# ip address 209.17.220.5 255.255.255.252

ISP(config-if)# no shutdown

ISP(config-if)# clock rate 128000

ISP(config-if)# exit

ISP(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1

ISP(config)# ip route 209.17.220.0 255.255.255.252 s0/0/1

ISP(config)# ip route 209.17.220.0 s0/0/0

```
MEDELLIN1(config)# int s0/0/0
MEDELLIN1(config-if)# clock rate 128000
MEDELLIN1(config-if)# ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)# no shutdown
MEDELLIN1(config)# int s0/0/1
MEDELLIN1(config-if)# clock rate 128000
MEDELLIN1(config-if)# ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)# no shutdown
MEDELLIN1(config)# int s0/1/1
MEDELLIN1(config-if)# clock rate 128000
MEDELLIN1(config-if)# ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)# no shutdown
MEDELLIN1(config)# int s0/1/0
MEDELLIN1(config-if)# clock rate 128000
MEDELLIN1(config-if)# ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)# no shutdown

MEDELLIN2(config)# int s0/0/1
MEDELLIN2(config-if)# clock rate 128000
MEDELLIN2(config-if)# ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)# no shutdown
MEDELLIN2(config)# int s0/0/0
MEDELLIN2(config-if)# clock rate 128000
MEDELLIN2(config-if)# ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)# no shutdown
```

```
MEDELLIN3(config)# int s0/1/1
MEDELLIN3(config-if)# clock rate 128000
MEDELLIN3(config-if)# ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)# no shutdown

BOGOTA1(config)# int s0/0/1
BOGOTA1(config-if)# clock rate 128000
BOGOTA1(config-if)# ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)# no shutdown
BOGOTA1(config)# int s0/1/0
BOGOTA1(config-if)# clock rate 128000
BOGOTA1(config-if)# ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)# no shutdown
BOGOTA1(config)# int s0/0/0
BOGOTA1(config-if)# clock rate 128000
BOGOTA1(config-if)# ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)# no shutdown
BOGOTA1(config-if)# exit
BOGOTA1(config)#ip route 172.29.3.0 255.255.255.252 209.17.220.6
BOGOTA1(config)#ip route 172.29.3.0 255.255.255.252 209.17.220.4
BOGOTA1(config)#ip route 172.29.3.0 255.255.255.252 209.17.220.0

BOGOTA2(config)# int s0/0/1
BOGOTA2(config-if)# clock rate 128000
BOGOTA2(config-if)# ip address 172.29.3.2 255.255.255.252
BOGOTA2(config-if)# no shutdown
```

BOGOTA3(config)# int s0/0/1

BOGOTA3(config-if)# clock rate 128000

BOGOTA3(config-if)# ip address 172.29.3.13 255.255.255.252

BOGOTA3(config-if)# no shutdown

BOGOTA3(config-if)# int g0/1

BOGOTA3(config-if)# ip address 172.29.1.1 255.255.255.0

BOGOTA3(config-if)# no shutdown

PARTE 2: TABLA DE ENRUTAMIENTO

PASO 1: Verificación de la tabla de rutas

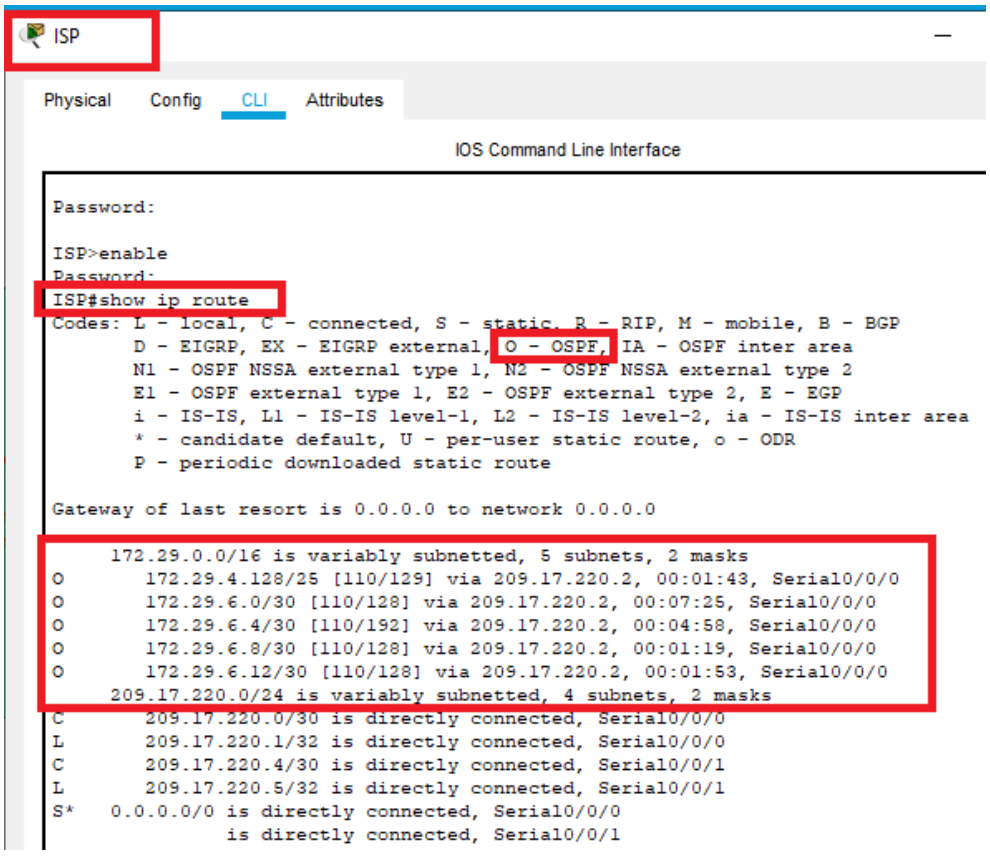

Figure 21 Comando show ip route en ISP, con rutas obtenidas por ospf y las direcciones estáticas configuradas.

Fuente: Archivo personal. Rutas del router ISP.

Se emite el comando show ip route en el CLI del router ISP para verificar las rutas obtenidas mediante actualizaciones del protocolo OSPF, en la totalidad de las rutas el puerto s0/0/0 es el utilizado para el tráfico de la red.

Figure 22 Comando show ip route en MEDELLIN1, con rutas obtenidas por ospf y las direcciones estáticas configuradas.

Fuente: Archivo personal. Rutas del router MEDELLIN1.

Se emite el comando show ip route en el CLI del router MEDELLIN-1 para verificar las rutas obtenidas mediante actualizaciones del protocolo OSPF, las rutas utilizan el puerto s0/0/0, s0/1/0 y s0/0/1 para manejar el tráfico de la red, es decir los puertos con los que se comunica con los otros router.

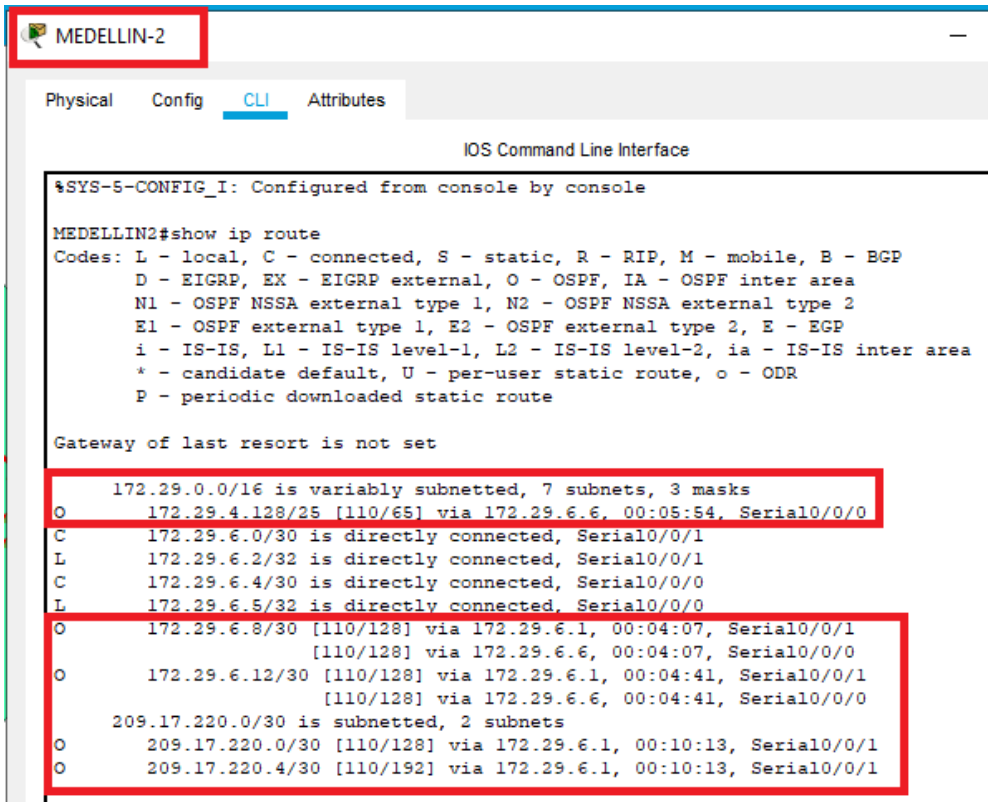

Figure 23 Comando show ip route en MEDELLIN2, con rutas obtenidas por ospf y las direcciones estáticas configuradas.

Fuente: Archivo personal. Rutas del router MEDELLIN2.

Se emite el comando show ip route en el CLI del router MEDELLIN-2 para verificar las rutas obtenidas mediante actualizaciones del protocolo OSPF, las rutas utilizan el puerto s0/0/0, s0/1/0 y s0/0/1 para manejar el tráfico de la red, es decir los puertos con los que se comunica con los otros router.

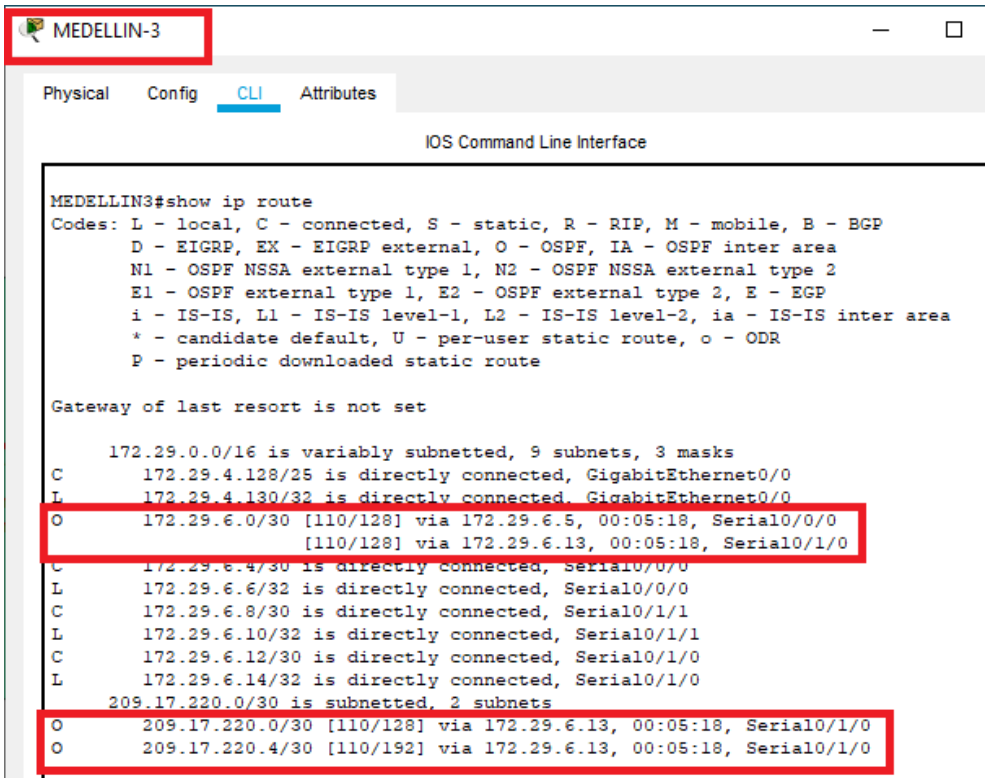

Figure 24 Comando show ip route en MEDELLIN3, con rutas obtenidas por ospf y las direcciones estáticas configuradas

Fuente: Archivo personal. Rutas del router MEDELLIN3.

Se emite el comando show ip route en el CLI del router MEDELLIN-3 para verificar las rutas obtenidas mediante actualizaciones del protocolo OSPF, las rutas utilizan el puerto s0/0/0, s0/1/0 y s0/0/1 para manejar el tráfico de la red, es decir los puertos con los que se comunica con los otros router.

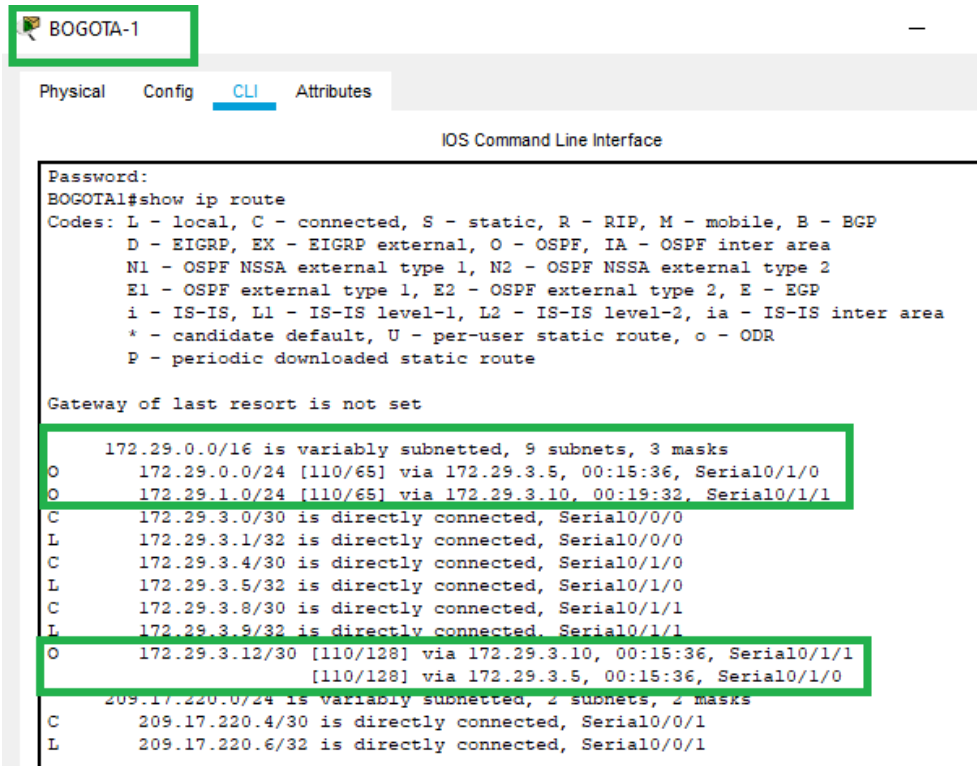

Figure 25 Comando show ip route en BOGOTA1, con rutas obtenidas por ospf y las direcciones estáticas configuradas.

Fuente: Archivo personal. Rutas del router BOGOTA1.

Se emite el comando show ip route en el CLI del router BOGÓTA-1 para verificar las rutas obtenidas mediante actualizaciones del protocolo OSPF, las rutas utilizan el puerto s0/0/0, s0/1/0 y s0/0/1 para manejar el tráfico de la red, es decir los puertos con los que se comunica con los otros router.

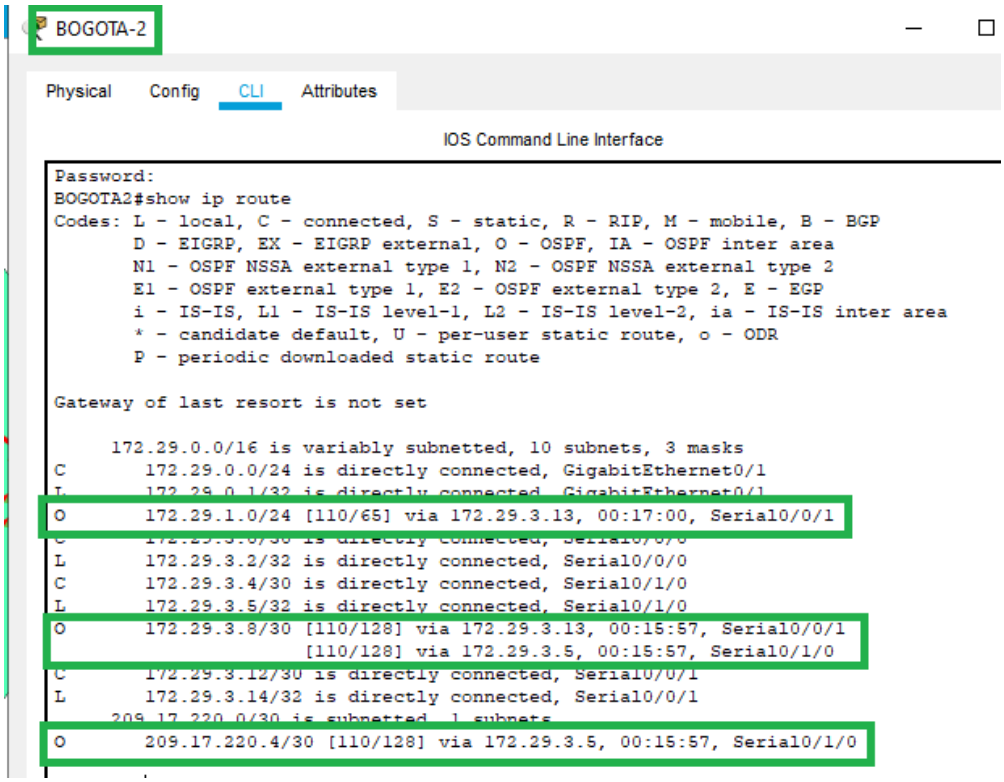

Figure 26 Comando show ip route en BOGOTA2, con rutas obtenidas por ospf y las direcciones configuradas

Fuente: Archivo personal. Rutas del router BOGOTA2.

Se emite el comando show ip route en el CLI del router BOGÓTA2 para verificar las rutas obtenidas mediante actualizaciones del protocolo OSPF, las rutas utilizan el puerto s0/0/0, s0/1/0 y s0/0/1 para manejar el tráfico de la red, es decir los puertos con los que se comunica con los otros router.

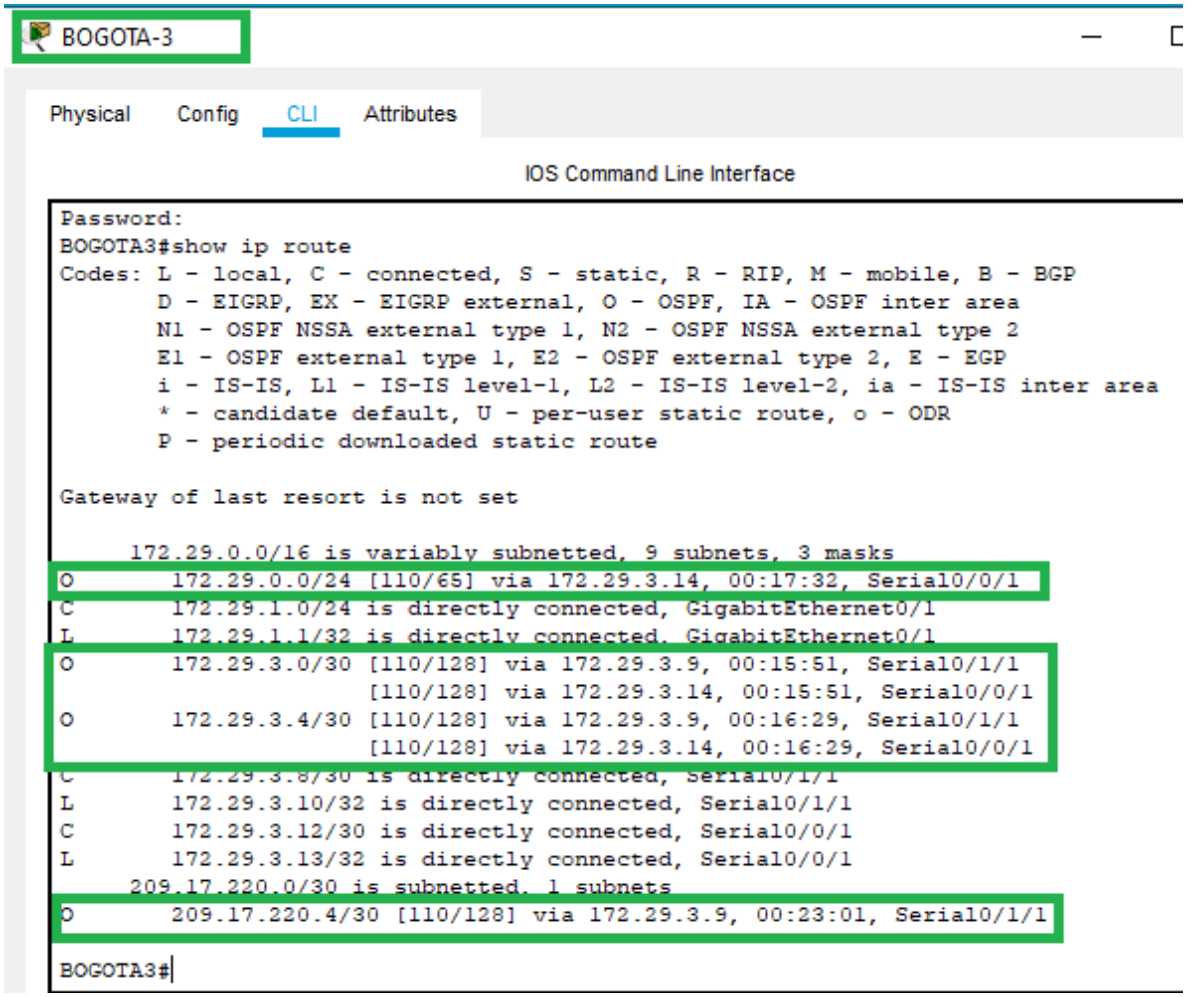

Figure 27 Comando show ip route en BOGOTA3, con rutas obtenidas por ospf y las direcciones configuradas

Fuente: Archivo personal. Rutas del router BOGOTA3.

Se emite el comando show ip route en el CLI del router BOGÓTA3 para verificar las rutas obtenidas mediante actualizaciones del protocolo OSPF, las rutas utilizan el puerto s0/0/0, s0/1/0 y s0/0/1 para manejar el tráfico de la red, es decir los puertos con los que se comunica con los otros router.

En síntesis, se realiza la verificación de los mapas de rutas en cada router, debido a que el escenario solicita una ruta directa y la configuración que se está usando.

PARTE 3: INTERFACES PASIVAS

PASO 1: Configurar las interfaces pasivas en los router de Medellín y Bogotá.

MEDELLIN3(config)# router ospf 1

MEDELLIN3(config-router)# passive-interface g0/0

MEDELLIN3(config-router)# passive-interface g0/1

MEDELLIN2(config)# router ospf 1

MEDELLIN2(config-router)# passive-interface g0/0

MEDELLIN2(config-router)# passive-interface g0/1

BOGOTA2(config)# router ospf 1

BOGOTA2(config-router)# passive-interface g0/0

BOGOTA2(config-router)# passive-interface g0/1

BOGOTA3(config)# router ospf 1

BOGOTA3(config-router)# passive-interface g0/0

BOGOTA3(config-router)# passive-interface g0/1

PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF.

PASO 1: Verificación de puertos con ospf

Posterior a la configuración inicial de las interfaces y el establecimiento del protocolo se ha realizado la siguiente tabla donde se especifica el router, interfaz, protocolo, actualización y versión.

Tabla 7 Lista de interfaz y puerto ospf.

Router	Interfaz	Protocolo	Actualización	Versión
ISP	S0/0/0	OSPF	SI	1
ISP	S0/0/1	OSPF	SI	1

MEDELLIN1	S0/0/0	OSPF	SI	1
	S0/0/1	OSPF	SI	1
	S0/1/1	OSPF	SI	1
	S0/1/0	OSPF	SI	1
MEDELLIN2	S0/0/0	OSPF	SI	1
	S0/0/1	OSPF	SI	1
	G0/0	OSPF	NO	1
	G0/1	OSPF	NO	1
MEDELLIN3	S0/0/0	OSPF	SI	1
	S0/0/1	OSPF	SI	1
	S0/1/1	OSPF	SI	1
	S0/1/0	OSPF	SI	1
	G0/0	OSPF	NO	1
	G0/1	OSPF	NO	1
BOGOTA1	S0/0/0	OSPF	SI	1
	S0/0/1	OSPF	SI	1
	S0/1/1	OSPF	SI	1
	S0/1/0	OSPF	SI	1
BOGOTA2	S0/0/0	OSPF	SI	1
	S0/1/0	OSPF	SI	1
	S0/0/1	OSPF	SI	1
	G0/0	OSPF	NO	1
	G0/1	OSPF	NO	1
BOGOTA3	S0/0/0	OSPF	SI	1
	S0/0/1	OSPF	SI	1
	G0/0	OSPF	NO	1
	G0/1	OSPF	NO	1

[4]

[4] La información de la tabla se puede encontrar de forma detallada a través del comando show ip rote y show ip protocols, imágenes suministradas en otras páginas de este documento.

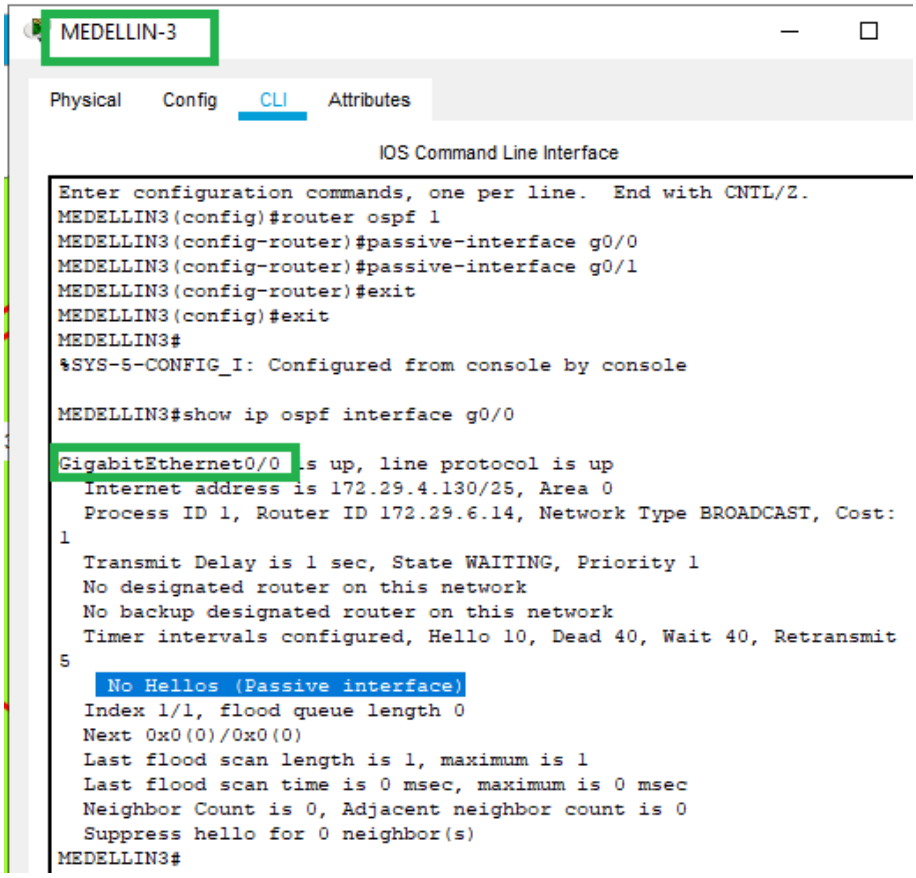

Figure 28 Interfaz pasiva en Router medellin-3.

Fuente: Archivo personal. Router medellin-3.

El SO del router marca las interfaces pasivas como “no hellos (passive interface)” para distinguir de las interfaces que si reciben actualizaciones de tipo “hello” al igual que brinda más información acerca de la interfaz.

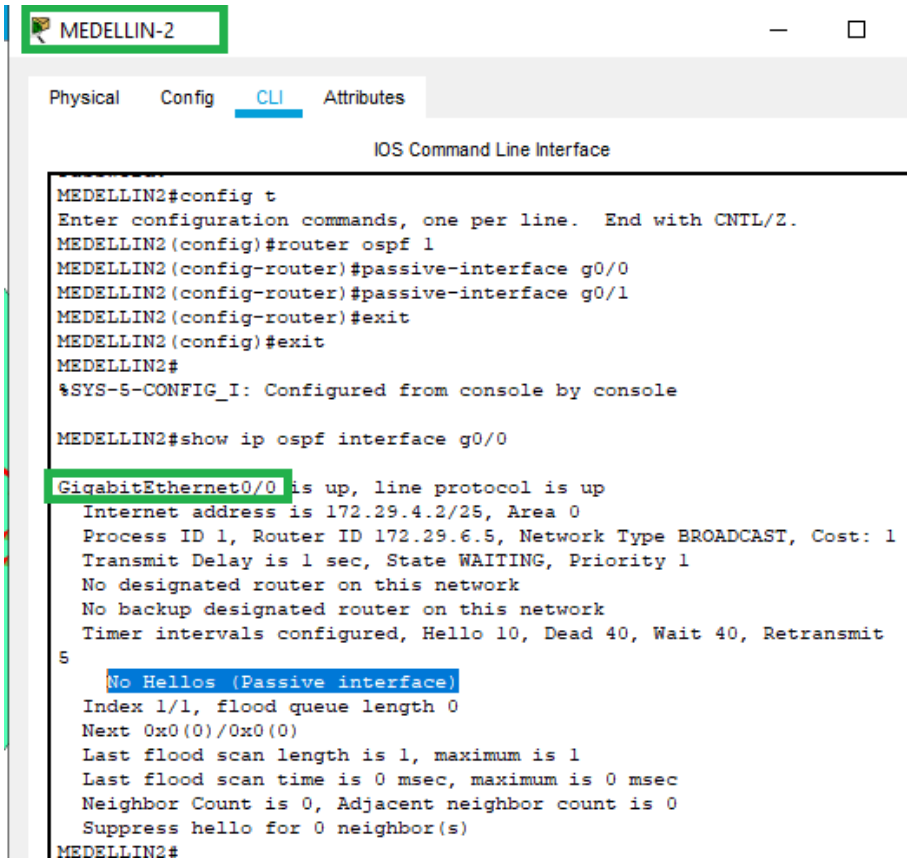

Figure 29 interfaz g0/0 del router medellin2.

Fuente: Archivo personal. Router medellin-2

El SO del router marca las interfaces pasivas como “no hellos (passive interface)” para distinguir de las interfaces que, si reciben actualizaciones de tipo “hello” al igual que brinda más información acerca de la interfaz, al igual que medellin-2 este puerto utiliza las interfaces gigabit ethernet y para distribuir a una sub red local.

PASO 2: Rutas ospf

Basados en la información de las tablas de routing de los router se sintetizo la información en una única tabla de direcciones donde se encuentra la dirección ipv4 de la red, la dirección ipv4 de uso (vía) y la interfaz del router a utilizar:

Tabla 8 Lista de rutas ospf por router e interfaz

Router	Protocolo	Ruta	Interfaz
ISP	OSPF	172.29.0.0/24 vía 209.17.220.6	S0/0/1
	OSPF	172.29.1.0/24 vía 209.17.220.6	S0/0/1
	OSPF	172.29.3.0/30 vía 209.17.220.6	S0/0/1
	OSPF	172.29.3.4/30 vía 209.17.220.6	S0/0/1
	OSPF	172.29.3.8/30 vía 209.17.220.6	S0/0/1
	OSPF	172.29.3.12/30 vía 209.17.220.6	S0/0/1
	OSPF	172.29.4.0/25 vía 209.17.220.2	S0/0/0
	OSPF	172.29.4.128/25 vía 209.17.220.2	S0/0/0
	OSPF	172.29.6.0/30 vía 209.17.220.2	S0/0/0
	OSPF	172.29.6.4/30 vía 209.17.220.2	S0/0/0
	OSPF	172.29.6.8/30 vía 209.17.220.2	S0/0/0
	OSPF	172.29.6.12/30 vía 209.17.220.2	S0/0/0
	OSPF	172.29.0.0/24 vía 209.17.220.6	S0/0/1
MEDELLIN1	OSPF	172.29.0.0/24 vía 209.17.220.1	S0/0/0
	OSPF	172.29.1.0/24 vía 209.17.220.1	S0/0/0
	OSPF	172.29.3.0/30 vía 209.17.220.1	S0/0/0
	OSPF	172.29.3.4/30 vía 209.17.220.1	S0/0/0
	OSPF	172.29.3.8/30 vía 209.17.220.1	S0/0/0
	OSPF	172.29.3.12/30 vía 209.17.220.1	S0/0/0
	OSPF	172.29.4.0/25 vía 172.29.6.2	S0/0/1
	OSPF	172.29.4.128/25 vía 172.29.6.10	S0/1/1
	OSPF	172.29.6.4/30 vía 172.29.6.2	S0/0/1
	OSPF	172.29.6.4/30 vía 172.29.6.10	S0/1/1
	OSPF	209.17.220.4/30 vía 209.17.220.1	S0/0/0
MEDELLIN2	OSPF	172.29.0.0/24 vía 172.29.6.1	S0/0/1
	OSPF	172.29.1.0/24 vía 172.29.6.1	S0/0/1
	OSPF	172.29.3.0/30 vía 172.29.6.1	S0/0/1
	OSPF	172.29.3.4/30 vía 172.29.6.1	S0/0/1
	OSPF	172.29.3.8/30 vía 172.29.6.1	S0/0/1
	OSPF	172.29.3.12/30 vía 172.29.6.1	S0/0/1
	OSPF	172.29.4.128/25 vía 172.29.6.6	S0/0/0
	OSPF	172.29.6.8/30 vía 172.29.6.1	S0/0/1
	OSPF	172.29.6.8/30 vía 172.29.6.6	S0/0/0
	OSPF	172.29.6.12/30 vía 172.29.6.1	S0/0/1
	OSPF	172.29.6.12/30 vía 172.29.6.1	S0/0/1
	OSPF	172.29.6.12/30 vía 172.29.6.6	S0/0/0
MEDELLIN3	OSPF	172.29.0.0/24 vía 172.29.6.9	S0/1/1
	OSPF	172.29.1.0/24 vía 172.29.6.9	S0/1/1
	OSPF	172.29.3.0/30 vía 172.29.6.9	S0/1/1
	OSPF	172.29.3.4/30 vía 172.29.6.9	S0/1/1
	OSPF	172.29.3.8/30 vía 172.29.6.9	S0/1/1
	OSPF	172.29.3.12/30 vía 172.29.6.9	S0/1/1
	OSPF	172.29.4.0/25 vía 172.29.6.5	S0/0/0
	OSPF	172.29.6.0/30 vía 172.29.6.5	S0/0/0

	OSPF	172.29.6.0/30 vía 172.29.6.9	S0/1/1
	OSPF	209.17.220.0/30 vía 172.29.6.9	S0/1/1
	OSPF	209.17.220.4/30 vía 172.29.6.9	S0/1/1
BOGOTA1	OSPF	172.29.0.0/24 vía 172.29.3.5	S0/0/0
	OSPF	172.29.1.0/24 vía 172.29.3.10	S0/1/1
	OSPF	172.29.3.12/30 vía 172.29.3.5	S0/1/0
	OSPF	172.29.3.12/30 vía 172.29.3.10	S0/1/1
	OSPF	172.29.4.0/25 vía 209.17.220.5	S0/0/1
	OSPF	172.29.4.128/25 vía 209.17.220.5	S0/0/1
	OSPF	172.29.6.0/30 vía 209.17.220.5	S0/0/1
	OSPF	172.29.6.4/30 vía 209.17.220.5	S0/0/1
	OSPF	172.29.6.8/30 vía 209.17.220.5	S0/0/1
	OSPF	172.29.6.12/30 vía 209.17.220.5	S0/0/1
BOGOTA2	OSPF	172.29.1.0/24 vía 172.29.3.13	S0/0/1
	OSPF	172.29.3.8/30 vía 172.29.3.13	S0/0/1
	OSPF	172.29.3.8/30 vía 172.29.3.1	S0/0/0
	OSPF	172.29.4.0/25 vía 172.29.3.1	S0/0/0
	OSPF	172.29.4.128/25 vía 172.29.3.1	S0/0/0
	OSPF	172.29.6.0/30 vía 172.29.3.1	S0/0/0
	OSPF	172.29.6.4/30 vía 172.29.3.1	S0/0/0
	OSPF	172.29.6.8/30 vía 172.29.3.1	S0/0/0
	OSPF	172.29.6.12/30 vía 172.29.3.1	S0/0/0
	OSPF	209.17.220.0/30 vía 172.29.3.1	S0/0/0
	OSPF	209.17.220.4/30 vía 172.29.3.1	S0/0/0
BOGOTA 3	OSPF	172.29.0.0/24 vía 172.29.3.14	S0/0/1
	OSPF	172.29.3.0/30 vía 172.29.3.9	S0/1/1
	OSPF	172.29.3.0/30 vía 172.29.3.14	S0/0/1
	OSPF	172.29.3.4/30 vía 172.29.3.9	S0/1/1
	OSPF	172.29.3.4/30 vía 172.29.3.14	S0/0/1
	OSPF	172.29.4.0/25 vía 172.29.3.9	S0/1/1
	OSPF	172.29.4.128/25 vía 172.29.3.9	S0/1/1
	OSPF	172.29.6.0/30 vía 172.29.3.9	S0/1/1
	OSPF	172.29.6.4/30 vía 172.29.3.9	S0/1/1
	OSPF	172.29.6.8/30 vía 172.29.3.9	S0/1/1
	OSPF	172.29.6.12/30 vía 172.29.3.9	S0/1/1
	OSPF	209.17.220.0/30 vía 172.29.3.9	S0/1/1
	OSPF	209.17.220.4/30 vía 172.29.3.9	S0/1/1

[5]

[5] La información de la anterior tabla se puede encontrar de forma detallada en las imágenes de los comandos de verificación show ip route y show ip protocols de este documento.

PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP

PASO 1: Habilitar pap

ISP(config)# int s0/0/0

ISP(config-if)# encapsulation ppp

ISP(config-if)# no shutdown

ISP(config-if)# ppp pap sent-username MED1 password c1sc0

ISP(config-if)# exit

ISP(config)# username ISP password c1sc0

ISP(config)# int s0/0/0

ISP(config-if)# no shutdown

ISP(config-if)# ppp authentication pap

ISP(config-if)# no shutdown

ISP(config-if)# exit

MEDELLIN1(config)# int s0/0/0

MEDELLIN1(config-if)# encapsulation ppp

MEDELLIN1(config-if)# no shutdown

MEDELLIN1(config-if)# exit

MEDELLIN1(config)# username MED1 password c1sc0

MEDELLIN1(config)# int s0/0/0

MEDELLIN1(config-if)# ppp authentication pap

MEDELLIN1(config-if)# no shutdown

MEDELLIN1(config-if)# ppp pap sent-user ISP password c1sc0

MEDELLIN1(config-if)# no shutdown

[6]

[6] La configuración CHAP sobre los router ISP y BOGOTA1 para ser habilitada se debe suprimir el ajuste PAP de seguridad en el canal, puesto que, la configuración ospf comparte este parámetro de router BOGOTA1, es decir, que bajo estas condiciones solo un ajuste trabajaría desde MED1 A BOG1

PARTE 6: CONFIGURACIÓN DEL SERVICIO DHCP.

PASO 1: servicio dhcp en MEDELLIN2 y 3

MEDELLIN2(config)# ip dhcp excluded-address 172.29.4.0 172.29.4.5

MEDELLIN2(config)# ip dhcp excluded-address 172.29.4.128 172.29.4.135

MEDELLIN2(config)# ip dhcp pool MED1

MEDELLIN2(dhcp-config)# network 172.29.4.3 255.255.255.128

MEDELLIN2(dhcp-config)# default-router 172.29.4.2

MEDELLIN2(dhcp-config)# dns-server 209.165.200.225

MEDELLIN2(dhcp-config)# domain-name ccna-lab.com

MEDELLIN2(dhcp-config)# exit

MEDELLIN2(config)# ip dhcp pool MED3

MEDELLIN2(dhcp-config)# network 172.29.4.130 255.255.255.128

MEDELLIN2(dhcp-config)# default-router 172.29.4.129

MEDELLIN2(dhcp-config)# dns-server 209.165.200.225

MEDELLIN2(dhcp-config)# domain-name ccna-lab.com

MEDELLIN3(config)# int g0/0

MEDELLIN2(config-if)# ip helper-address 172.6.5

PASO 2: servicio dhcp en BOGOTA2 y 3

BOGOTA2(config)# ip dhcp excluded-address 172.29.0.0 172.29.0.10

BOGOTA2(config)# ip dhcp excluded-address 172.29.1.0 172.29.1.10

BOGOTA2(config)# ip dhcp pool BOG2

BOGOTA2(dhcp-config)# network 172.29.0.3 255.255.255.0

BOGOTA2(dhcp-config)# default-router 172.29.0.1

BOGOTA2(dhcp-config)# dns-server 209.165.200.225

BOGOTA2(dhcp-config)# domain-name ccna-lab.com

BOGOTA2(dhcp-config)# exit

BOGOTA2(config)# ip dhcp pool BOG3

BOGOTA2(dhcp-config)# network 172.29.1.3 255.255.255.0

BOGOTA2(dhcp-config)# default-router 172.29.1.1

BOGOTA2(dhcp-config)# dns-server 209.165.200.225

BOGOTA2(dhcp-config)# domain-name ccna-lab.com

BOGOTA3(config)# int g0/0

BOGOTA3(config-if)# ip helper-address 172.3.14

[7]

[7] El servicio dhcp esta configurado en los router MEDELLIN 2 y BOGOTA 2, debido a que el comando IP-HELPER no funciona con conexión directa a la interfaz del servicio dhcp y no a traves de una red diferente.

PASO 3: Verificación de ipv4 por servicio de dhcp

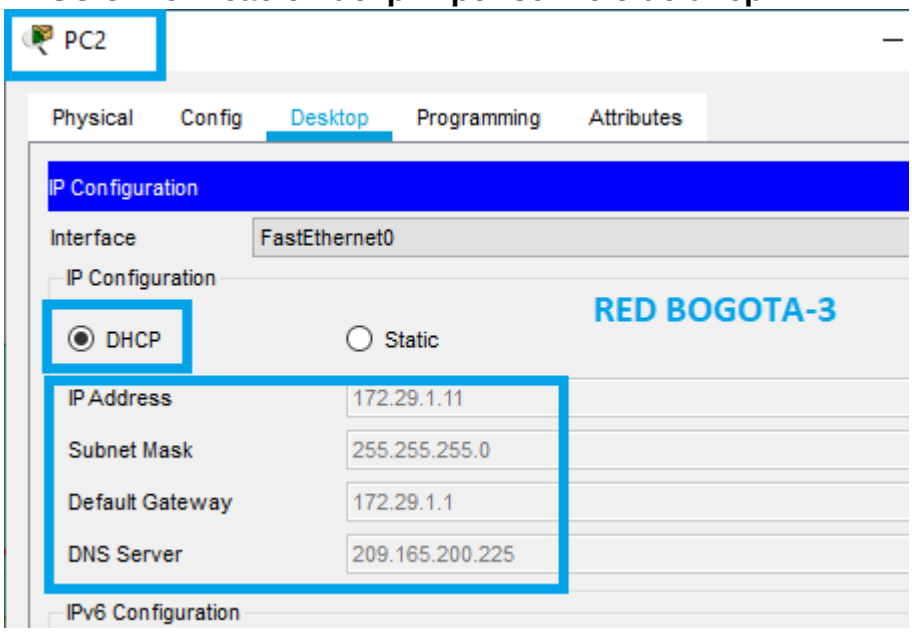

Figure 30 ipv4 de pc2 por solicitud dhcp a BOGOTA2.

Fuente: Archivo personal. Configuración ipv4 de pc2

El servicio dhcp del router Bogotá-3 está alojado en el router Bogotá – 2 gracias la utilidad de configuración de ip helper.

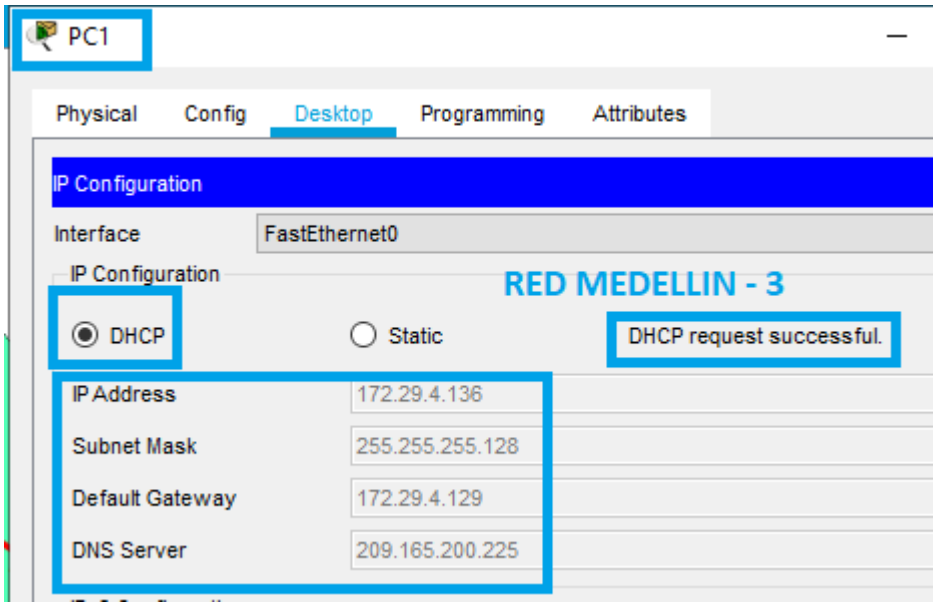

Figure 31 Ipv4 de pc1 por solicitud dhcp a MEDELLIN2

Fuente: Archivo personal. Configuración ipv4 de pc1.

El servicio dhcp del router MEDELLIN-3 está alojado en el router MEDELLIN – 2 gracias la utilidad de configuración de ip helper; de la misma forma que en los router de la red BOGOTÁ.

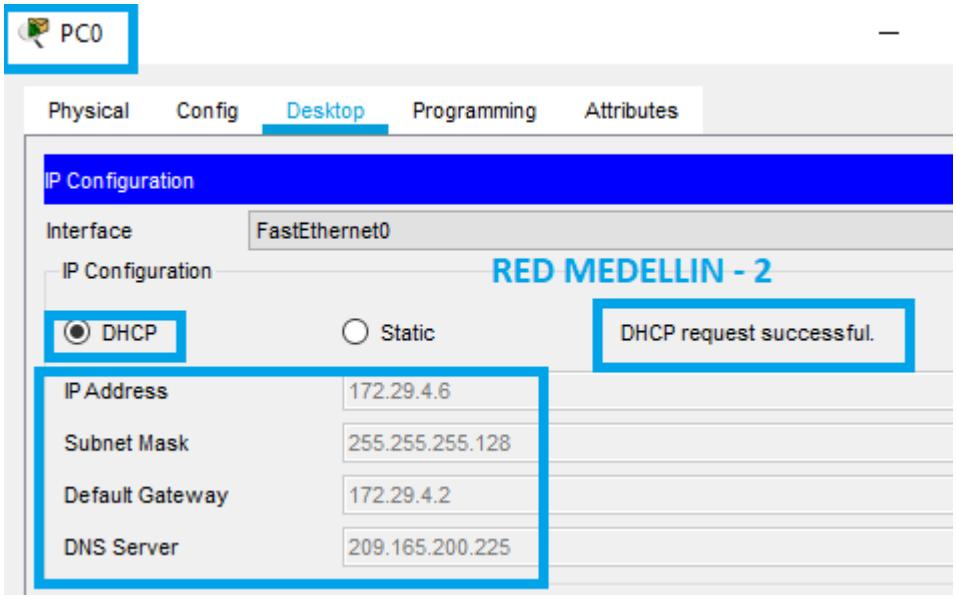

Figure 32 PC-0 con servicio dhcp desde router Medellín 2

Fuente: Archivo personal. Lista de dirección ipv4 obtenida por dhcp en pc0.

El router MEDELLIN -2 tiene la configuración del pool de direcciones dhcp para su propia red y para la red de MEDELLIN – 3, es posible porque se encuentran conectados directamente y en la misma red.

PARTE 7: PRUEBAS DE CONECTIVIDAD:

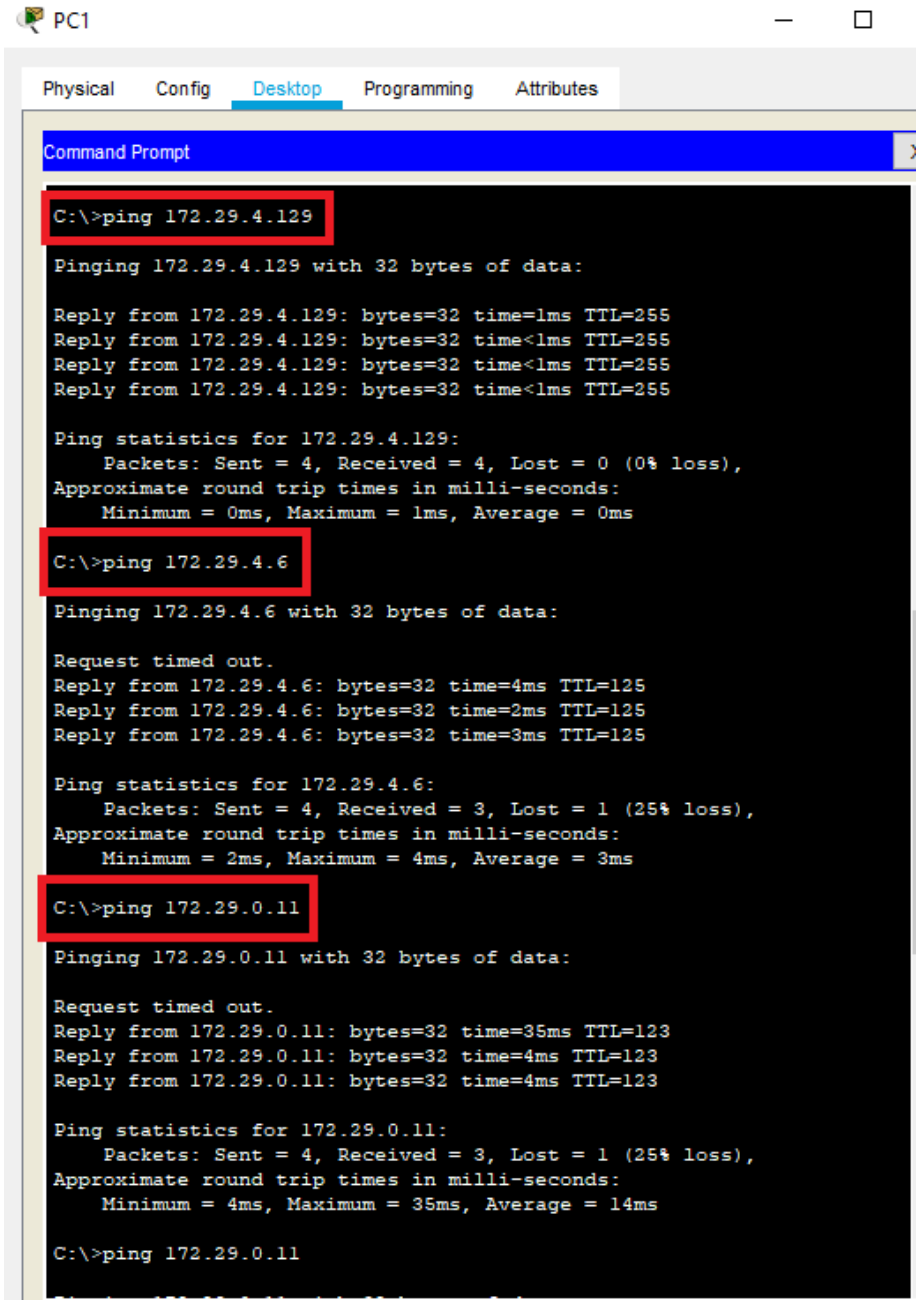

Figure 33 Ping desde pc1 a pc2, pc3 y pc0 utilizando la dirección ipv4 obtenida por dhcp.

Fuente: Archivo personal. Comando ping desde pc1.

Se emite el comando ping (prueba de conexión punto a punto) desde Pc1 hasta los otros hosts de la red. Validando el estado de la conectividad.

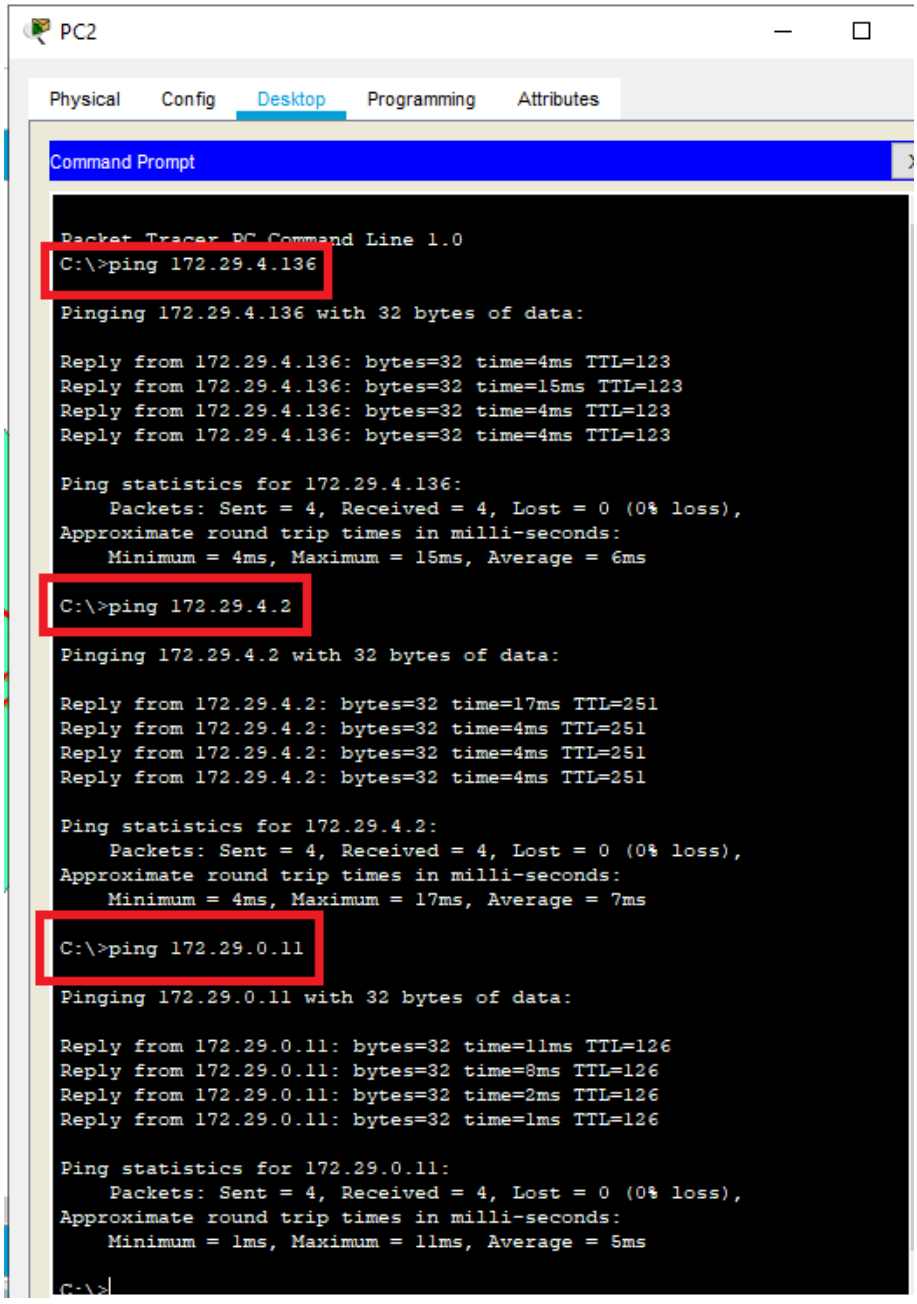

Figure 34 Ping desde pc2 a pc1, pc3 y pc0 utilizando la dirección ipv4 obtenida por dhcp.

Fuente: Archivo personal. Comando ping desde pc2.

Se emite el comando ping (prueba de conexión punto a punto) desde Pc2 hasta los otros hosts de la red. Validando el estado de la conectividad. Se utiliza la dirección ipv4 obtenida por el servicio dhcp.

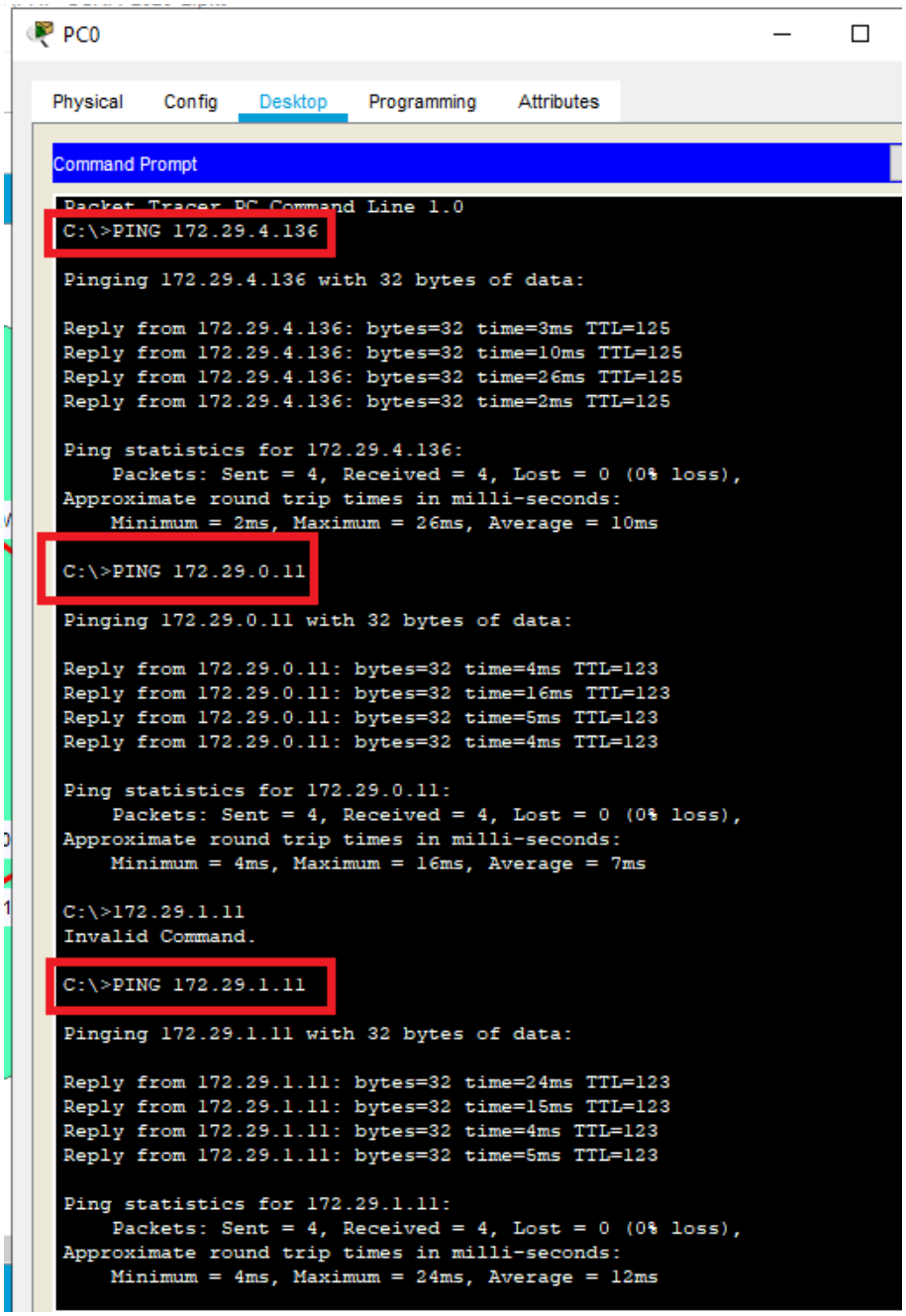

Figure 35 Ping desde pc0 a pc1, pc2 y pc3 utilizando la dirección ipv4 obtenida por dhcp.

Fuente: Archivo personal. Comando ping desde pc0.

Se emite el comando ping (prueba de conexión punto a punto) desde Pc0 hasta los otros hosts de la red. Validando el estado de la conectividad. Se utiliza la dirección ipv4 obtenida por el servicio dhcp.

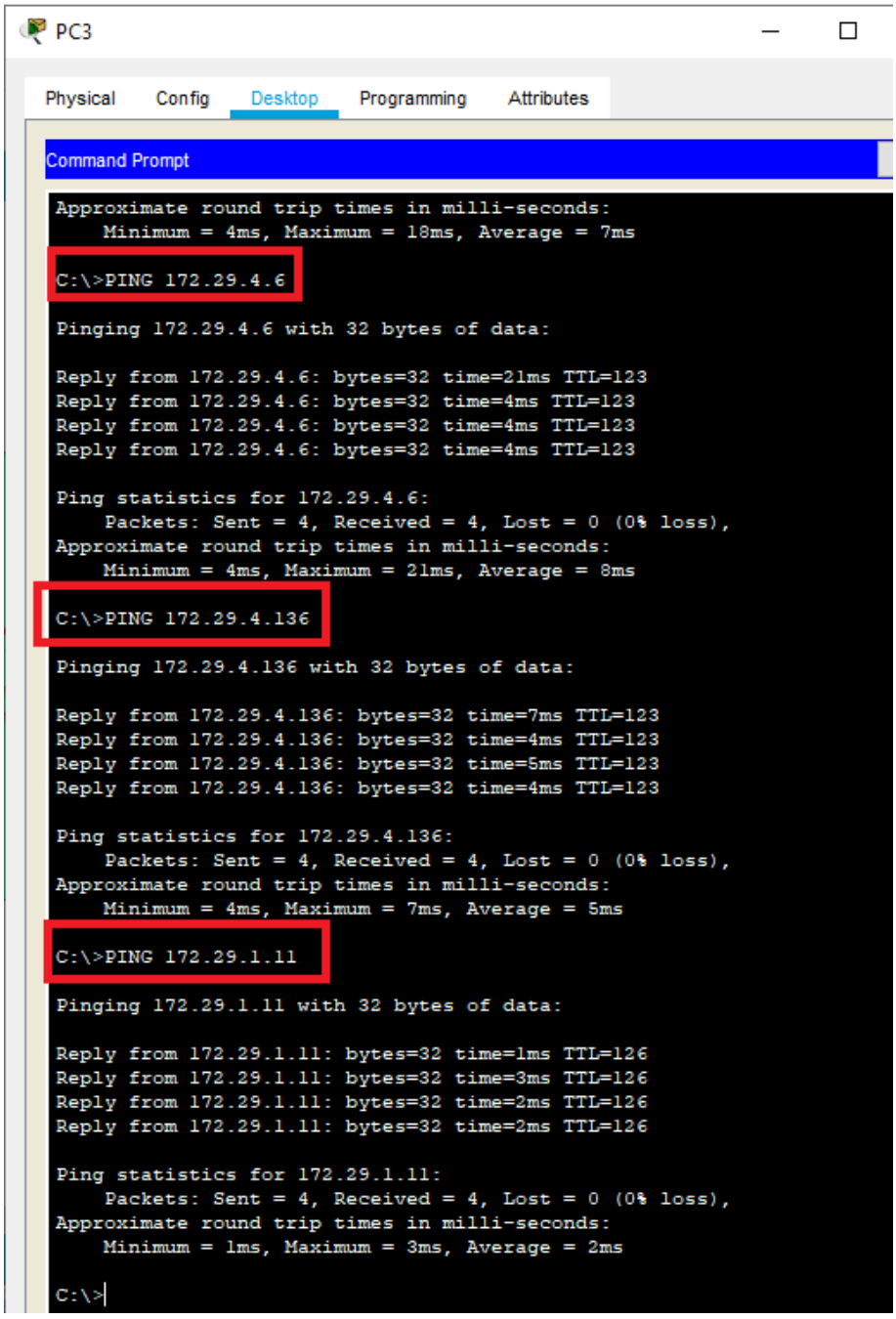

Figure 36 Ping desde pc3 a pc1, pc2 y pc0.

Fuente: Archivo personal. Comando ping desde pc3.

Se emite el comando ping (prueba de conexión punto a punto) desde Pc3 hasta los otros hosts de la red. Validando el estado de la conectividad. Se utiliza la dirección ipv4 obtenida por el servicio dhcp.

CONCLUSIONES

En el marco del desarrollo de las actividades de configuración para los dos escenarios es posible resaltar que el aprendizaje basado en tareas ayuda a la búsqueda de respuestas ante dificultades y obstáculos, las actividades son el punto de partida para comenzar la búsqueda del conocimiento requerido para lograr los anteriores resultados, el sistema simulaciones ha permitido aplicar dichas habilidades durante el desarrollo y finalización de la actividad propuesta.

Uno de los apartes importantes de esta actividad y de otras a futuro debe ser la validación de información de configuración, debido a que la mecánica de del ser humano puede errar, desde un carácter, un número y el trabajo individual ralentiza el proceso de revisión, pero mejora el desarrollo individual en pro de la resolución de problemas.

RECOMENDACIONES

Para el desarrollo de otras actividades se debe de analizar el conjunto de instrucciones y requerimientos de configuración buscando que sean aplicables a entornos simulados, esto permitiría analizar el comportamiento de dichas instrucciones en una situación hipotética, ejemplo: ACL. El cual se puede configurar.

Las ilustraciones referentes a la topología a implementar deben de ser puntuales, es decir, utilizar elementos únicos evitando la súper posición de objetos para evitar generar errores de diseño o mal interpretación de la información.

Las configuraciones a poner en práctica por parte del trabajo final teóricamente deben de ser el 100% pero esto en muchos casos no es posible aplicarlo; los comandos no son soportados por simulaciones, las configuraciones no son estructuradas, es decir, una no optimiza a la otra y/o son redundantes. En este contexto es de utilidad realizar escenarios más reducidos donde sean homogéneas las configuraciones y requerimientos, se requerirían más simulaciones, pero sería posible utilizar más configuraciones y comandos.

BIBLIOGRAFIA

DI TOMMASO, Leandro. “Configuración PPP y PAP en Cisco” (en línea). 28 de febrero de 2010. Disponible en: https://www.mikroways.net/2010/02/28/configuracion-de-ppp-y-pap-en-cisco/

APRENDA REDES, Sin autor. “Calculadora IP” (en línea). Sin fecha. Disponible en: https://www.aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi?host=192.168.99.0&mask1=24&mask2=

CISCO, sin autor. “Definiciones engine browser”. (en línea). Sin fecha. Disponible en: https://search.cisco.com/search?query=dhcp&locale=enUS&bizcontext=&cat=&mode=text&clktyp=enter&autosuggest=false