PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JOSE DAVID MEJÍA GUZMÁN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
DIPLOMADO DE PROFUNDIZACIÓN CISCO (Diseño e implementación de Soluciones Integradas LAN/WAN)
BOGOTÁ D.C.
2019

JOSE DAVID MEJÍA GUZMÁN

INFORME

IVÁN GUSTAVO PEÑA
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
DIPLOMADO DE PROFUNDIZACIÓN CISCO (Diseño e implementación de Soluciones Integradas LAN/WAN)
BOGOTÁ D.C.
2019

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

INTRODUCCIÓN

Las redes han sido de gran impacto dentro del mundo tecnológico. Permiten llevar a cabo actividades que en épocas pasadas se creían imposibles o inalcanzables. En un mundo globalizado se pretende conectar a todos con todos y gracias a las redes dentro de sus diferentes ámbitos es posible. El funcionamiento puede ser algo complejo, pero cada dia que pasa, se solventan errores y realizan mejoras para brindar el mejor rendimiento en los distintos campos donde se aplican.

El siguiente informe es presentado con el fin de dar a conocer al lector sobre la correcta apropiación de conocimiento por parte del estudiante en cuanto a la comprensión y aplicación de la gran mayoría de las temáticas abordadas durante el desarrollo del diplomado de profundización CISCO (Diseño e Implementación de Soluciones Integradas LAN/WAN), a través de la lectura de documentación disponible en la plataforma CISCO y la plataforma de la Universidad Nacional Abierta y a Distancia (UNAD) y el desarrollo de la Prueba de Habilidades Pácticas compuesta por dos escenarios realizados en el software Packet Tracer, utilizado para simular y analizar el comportamiento de topologías de red, que permite a las personas inmersas en el tema de redes, comprender los fundamentos básicos para aplicar en soluciones integradas LAN/WAN.

OBJETIVOS

OBJETIVO GENERAL

Aplicar el conocimiento adquirido a partir de la lectura de los módulos y desarrollo de prácticas de laboratorio propuestas en CCNA-1 y CCNA-2 durante el desarrollo del diplomado de profundización CISCO (Diseño e Implementación de Soluciones Integradas LAN/WAN)

OBJETIVOS ESPECÍFICOS

- Realizar rutinas de diagnóstico y resolución de problemas.
- Realizar las configuraciones básicas en los diferentes dipositivos que componen las redes.
- Establecer la conexión lógica de los equipos con base en las topologías.
- Configurar el enrutamiento en la red usando el protocolo RIP versión 2 y OSPF versión 2.
- Configurar enrutamiento estático y rutas predeterminadas IPv4.
- Calcular rutas resumidas IPv4.
- Aplicar la división de subredes VLSM.
- Analizar los resultados de la tabla de routing.
- Configurar encapsulamiento PPP y autenticación PAP y CHAP.
- Configurar la traducción de direcciones NAT con sobrecarga para IPv4.
- Configurar enrutamiento dinámico mediante DHCPv4.
- Permitir difusión de rutas a traves de routers.
- Configurar el routing entre VLAN basado en enlaces troncales 802.1Q
- Realizar la configuración de ACLs estándar, ACLs estándar con nombre y ACLs en líneas VTY.
- Establecer conexiones remotas mediante SSH.
- Verificar todas las configuraciones realizadas con el uso de los diferentes comandos show.
- Verificar la convergencia y conectividad de las redes.

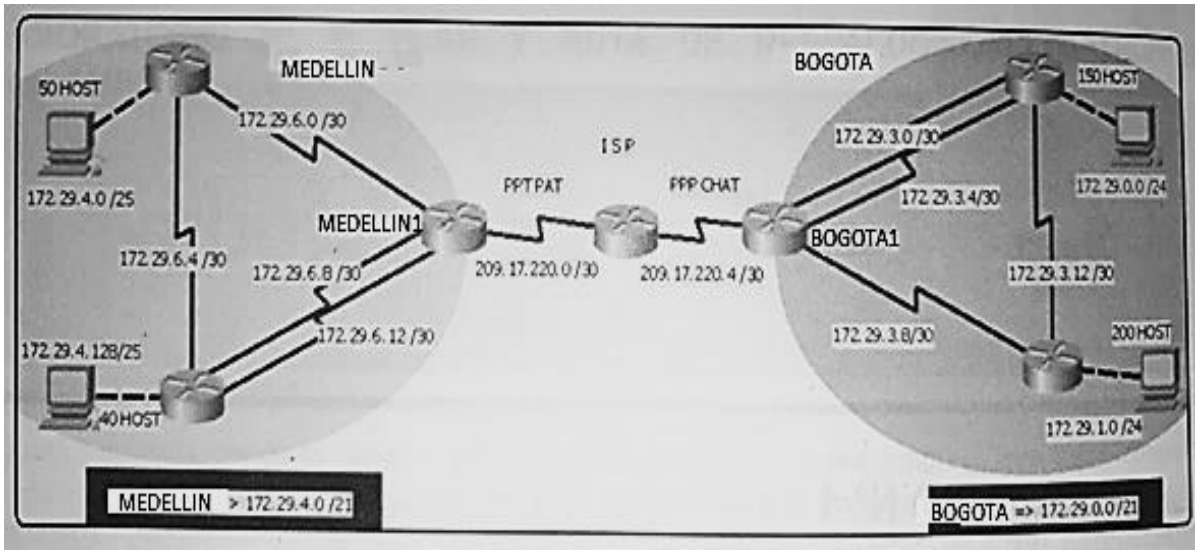
1. DESARROLLO

1.1. ESCENARIO 1

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 de red

Figura 1 Topología Escenario 1



Fuente: Cisco. Evaluación – Prueba de Habildiades Prácticas CCNA.

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

TENER EN CUENTA

- Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.
- Se debe configurar PPP en los enlaces hacia el ISP, con autenticación.
- Se 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).
- Realizar la conexión física de los equipos con base en la topología de red

Recursos Necesarios

- Terminales.
- 7 routers 1941.
- Cables de conexión para enlaces directos y seriales.

Montar el cableado de red

En Packet Tracer, en la parte inferior izquierda de la pantalla se seleccionan los PC Genéricos, los los routers 1941 y se arrastran al panel de diseño lógico de la topologìa de red y se colocan notas para identificar las interfaces y redes.

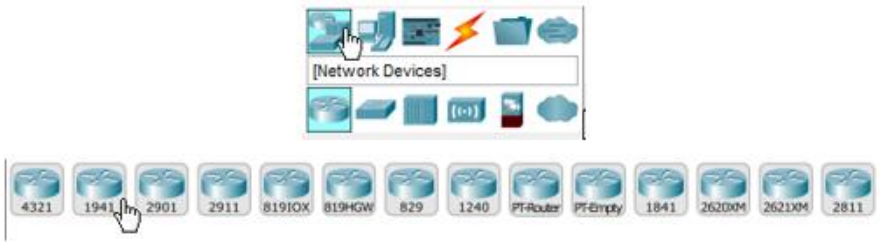
- PC

Figura 2 Connections End Devices - PC

Fuente: Cisco Packet Tracer 7.0.2.0226.

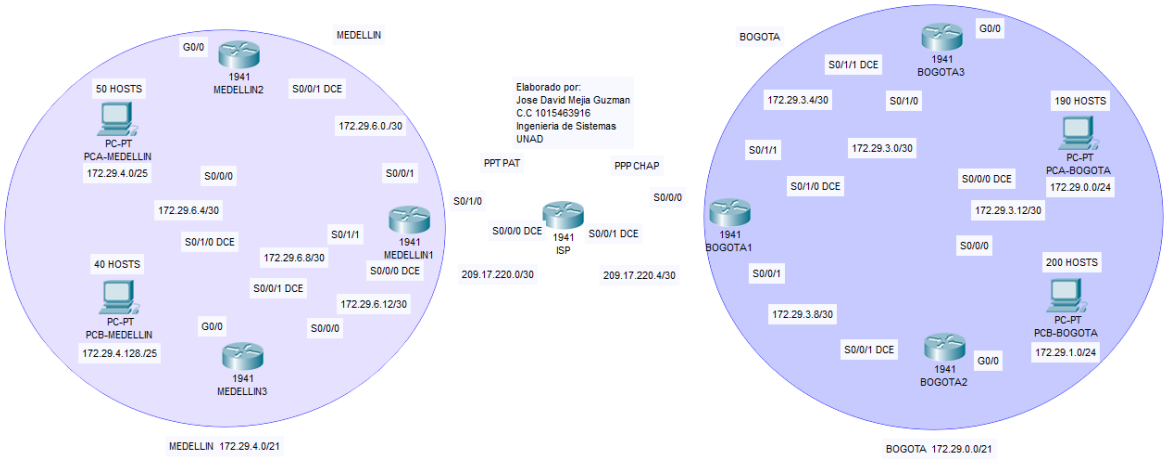
- Routers

Figura 3 Routers - 1941



Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 4 Esquema Topología de Red Escenario 1

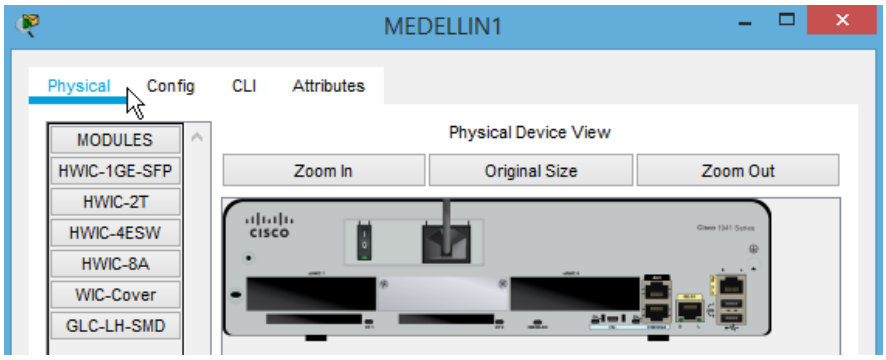


Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

En una conexión WAN se requieren enlaces seriales entre los routers, pero en Packet Tracer los routers 1941 no traen los módulos con interfaces seriales, pero están disponibles y se agregan de la siguiente manera:

- ✓ Se hace clic sobre el router y a continuación, se ubica la pestaña **Physical.**

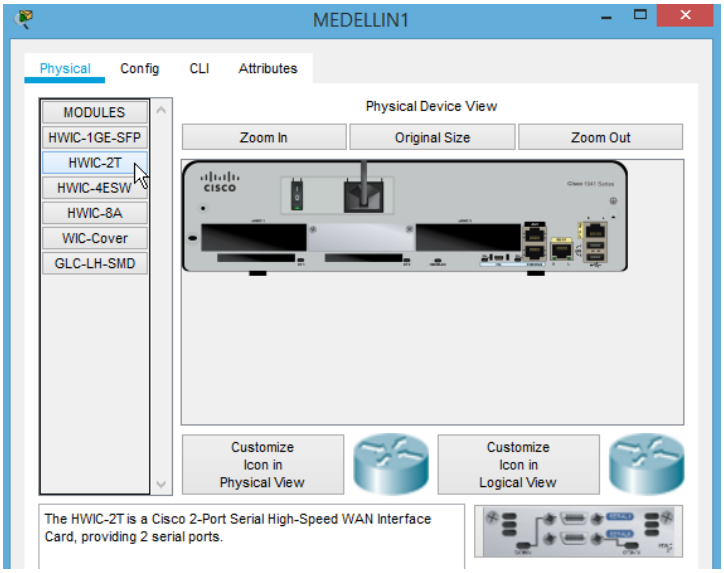
Figura 5 Pestaña Physical Router 2960



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se ubica el módulo HWIC-2T. En la parte inferior de la ventana se muestra una breve descripción y la imagen del módulo.

Figura 6 Descripción Módulo HWIC-2T

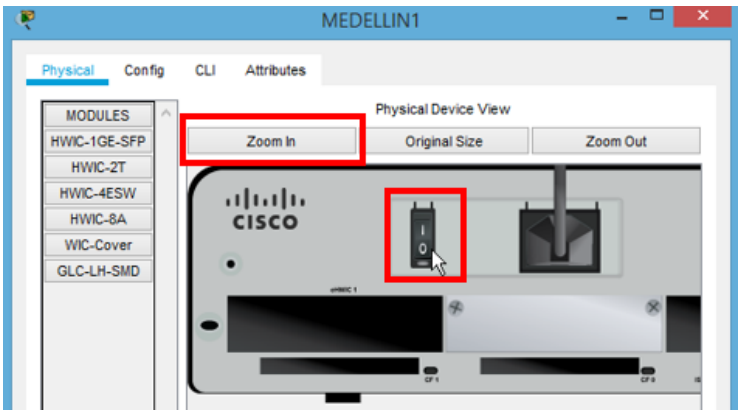


Fuente: Cisco Packet Tracer 7.0.2.0226.

Como se indica en la descripción de la parte inferior izquierda de la ventana, HWIC-2T es una tarjeta de interfaz WAN de alta velocidad serie de 2 puertos de Cisco, que proporciona 2 puertos serie.

- ✓ Se procede a agregar la tarjeta al router pero este debe estar apagado. Se hace clic en el botón **On/Off** del router para apagarlo. Cuando no se muestre el led verde, el router estará apagado. Se puede hacer clic en la pestaña **Zoom In** para una mejor visualización.

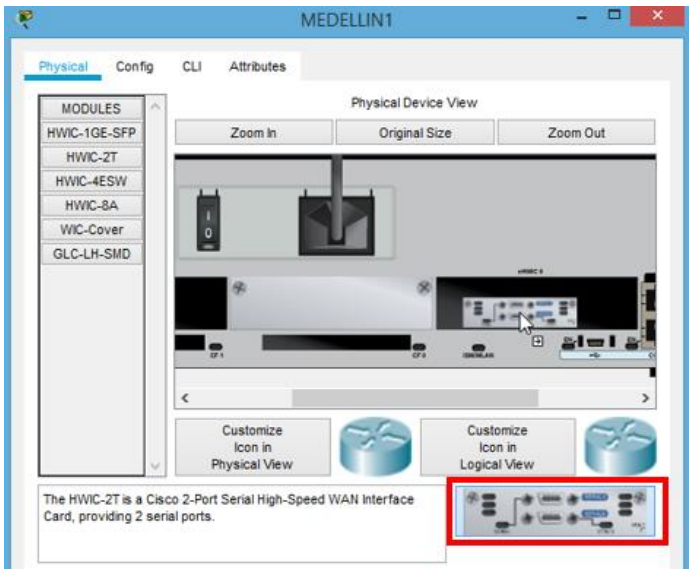
Figura 7 Apagado router



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se selecciona la tarjeta de interfaz, se arrastra y suelta en cualquiera de las ranuras.

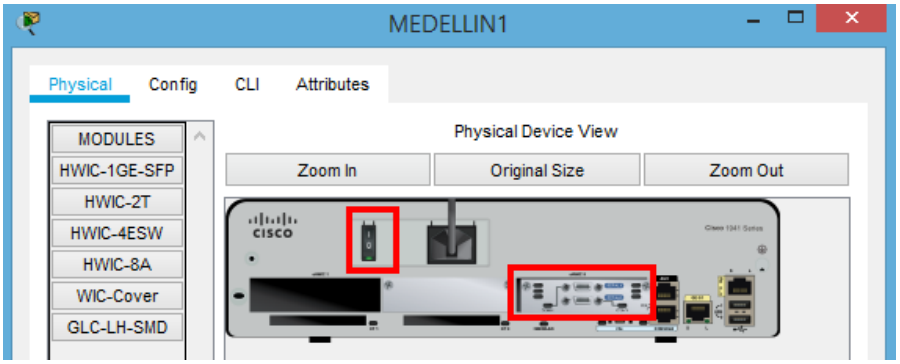
Figura 8 Colocación Módulo HWIC-2T en router



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Una vez colocada, se enciende el router.

Figura 9 Encendido de router con módulo HWIC-2T colocado

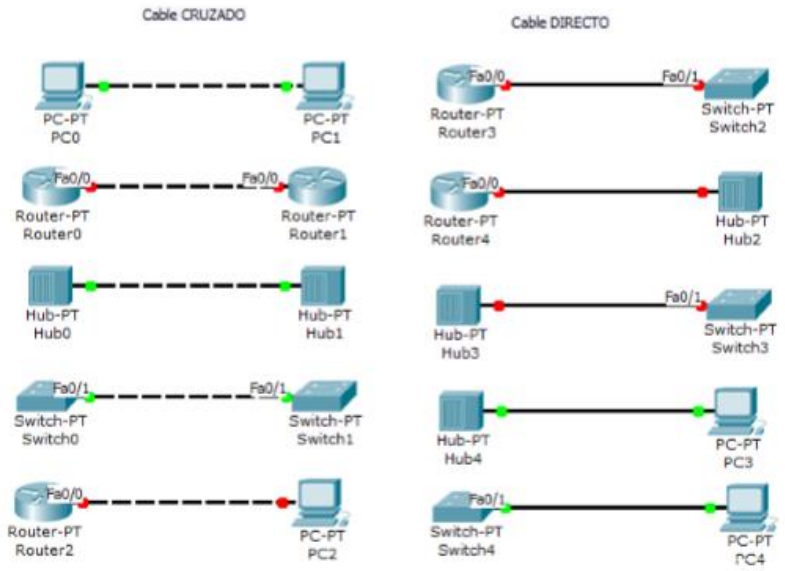


Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Cada tarjeta de interfaz proporciona dos interfaces seriales, en caso de requerir mas se añade otra tarjeta en la ranura correspondiente.
- ✓ Se repite el procedimiento para los demás routers.

- Conexiones de PC a Router

Figura 10 Conexiones entre dipositivos (Packet Tracer)

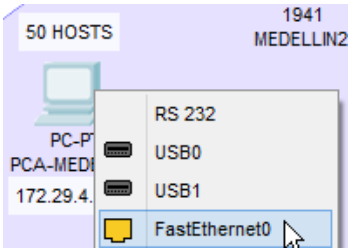


Fuente: http://blog.juliopari.com/packet-tracer-cable-cruzado-y-cable-directo/

Los routers cisco 1941 tienen detección automática y se puede usar un cable de Ethernet pero para fines prácticos se siguen los lineamientos de conexión de la imagen y se utiliza un cable cruzado para conectar los terminales a los terminales a los routers.

- ✓ En Packet Tracer dentro del apartado de conexiones se ubica aquella que indique **Cooper Cross-Over** y a continuación, se selecciona.
- ✓ Se hace clic sobre el PC y a continuación en la ventana emergente se hace clic sobre la opción **FastEthernet0.**

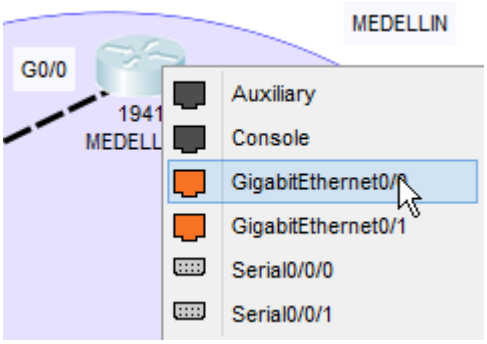
Figura 11 PCA-MEDELLIN Puerto FastEthernet0



Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

✓ Se hace clic sobre el router y a continuación en la ventana emergente se hace clic sobre una de las interfaces **GigabitEthernet**. En este caso **GigabitEthernet 0/0**.

Figura 12 MEDELLIN2 Interfaz GigabitEthernet0/0



Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

✓ Se repite el procedimiento para las otras conexiones de este tipo.

- Conexiones de Router a Router

En esta topología los routers no se encuentran conectados directamente por lo que se deben utilizar conexiones seriales entre estos.

Las interfaces seriales requieren una señal de sincronización que controle la comunicación. En la mayoría de los casos, un dispositivo DCE brinda dicha señal.

Para configurar PPP en los enlaces hacia el ISP, con autenticación, uno de los dispositivos (el que tenga el extremo DCE) debe tener configurado el **clock rate** (mide la transferencia de datos).

Además, con se debe configurar NAT en los routers MEDELLIN1 y BOGOTA1, el ISP debe tener interfaces DCE.

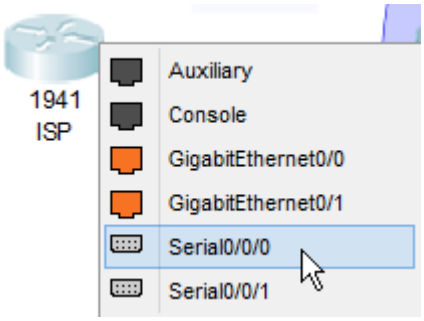
✓ En el apartado de conexiones, se ubica aquella que indica **Serial DCE.**

Figura 13 Conexión Serial DCE

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se hace clic sobre el router ISP y a continuación, en la ventana emergente se hace clic sobre una de las interfaces **seriales**. En este caso la interfaz Serial0/0/0.

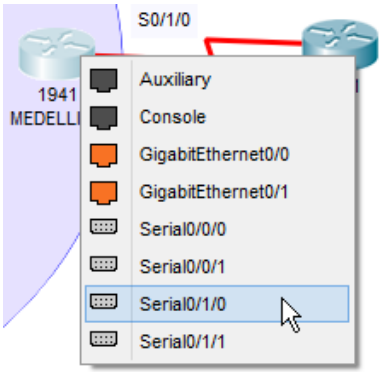
Figura 14 ISP Interfaz Serial0/1/0



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se hace clic sobre el router **MEDELLIN1** y a continuación, en la ventana emergente se hace clic sobre la interfaz **Serial0/1/0**.

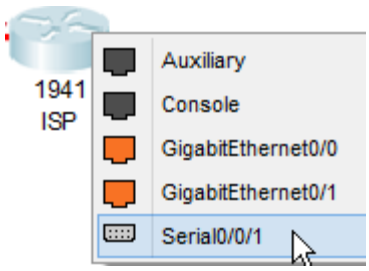
Figura 15 MEDELLIN1 Interfaz S0/1/0



Fuente: Cisco Packet Tracer 7.0.2.0226.

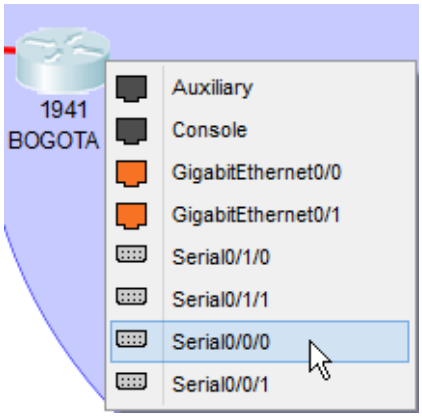
- ✓ Se repite el procedimiento para el router **BOGOTA1**. En el ISP se hace clic sobre la interfaz **Serial0/0/1** y en el router **BOGOTA1** se selecciona la interfaz **Serial0/0/0**.

Figura 16 ISP Interfaz Serial0/0/1



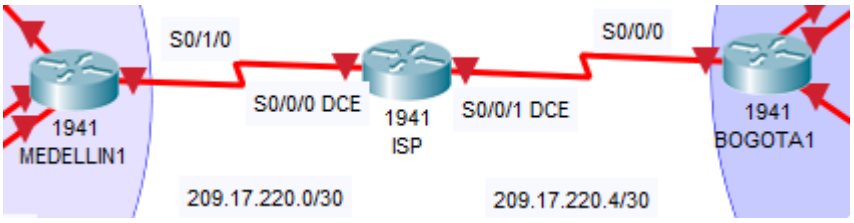
Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 17 BOGOTA1 Interfaz Serial0/0/0



Fuente: Cisco Packet Tracer 7.0.2.0226.

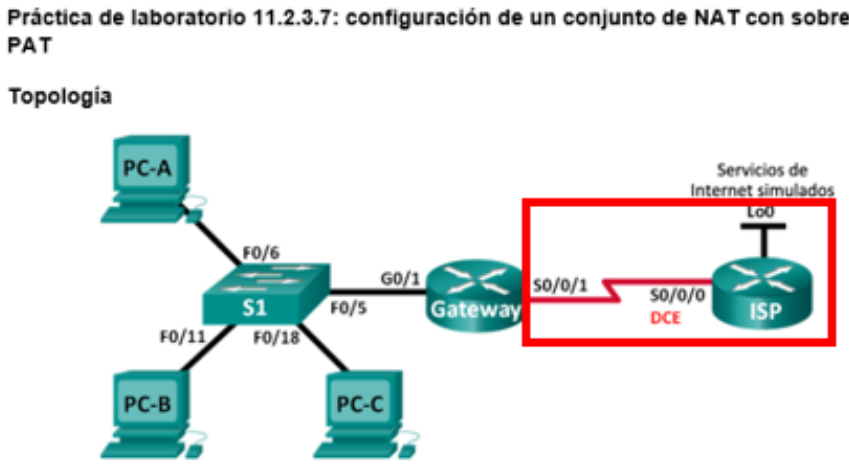
Figura 18 Conexión ISP MEDELLIN1 y BOGOTA1



Fuente: Cisco Packet Tracer 7.0.2.0226.

Configuración basada en el **Laboratorio 11.2.3.7** correspondiente a la Tarea 4.

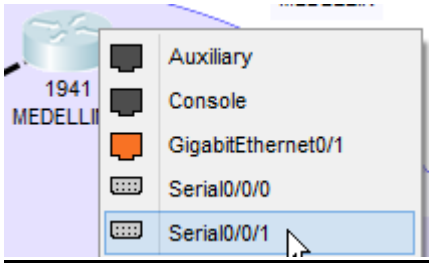
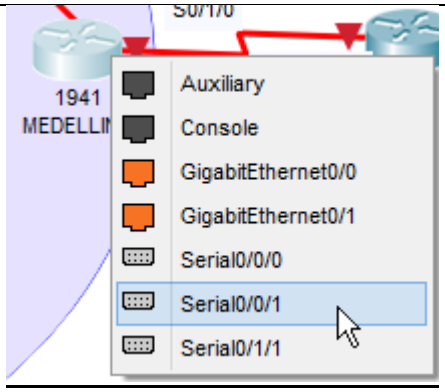
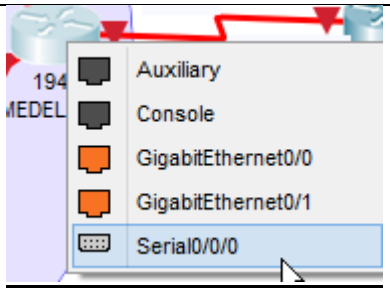
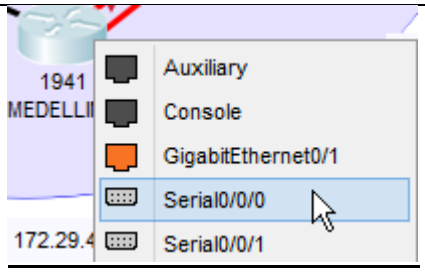
Figura 19 Topologìa Laboratorio 11.3.2.7 Tarea 4

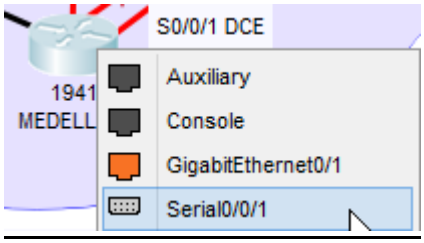
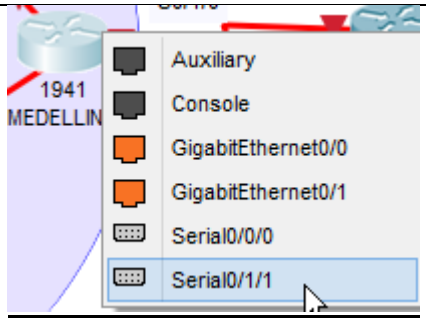
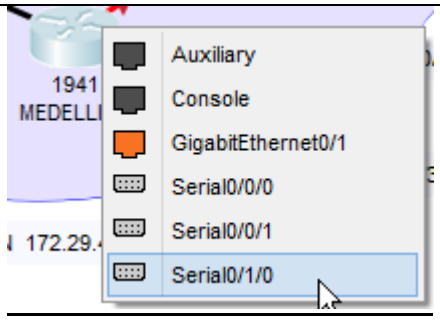
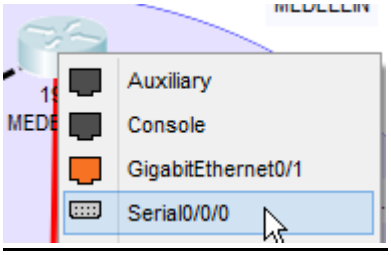


Fuente: Cisco Packet Tracer 7.0.2.0226.

Conexiones de Red MEDELLIN

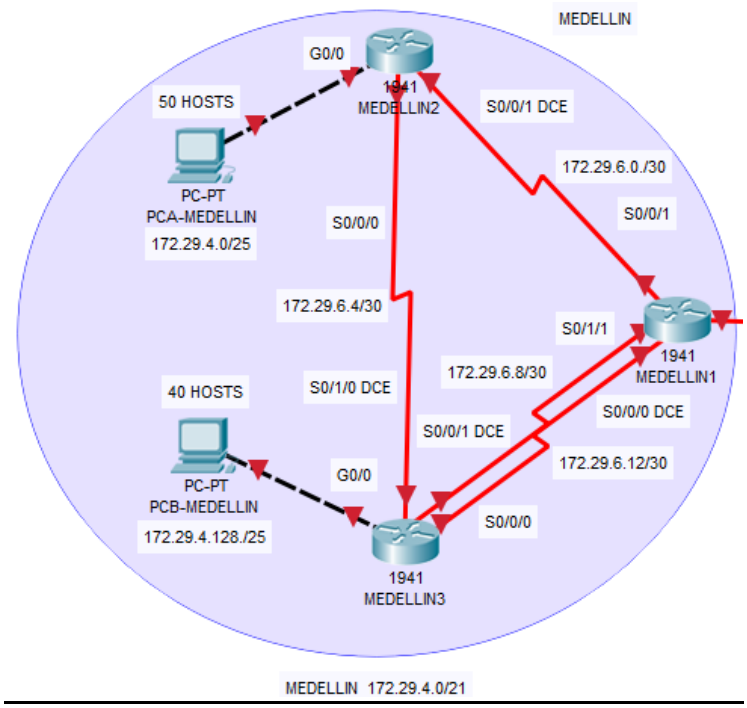
Tabla 1 Conexiones de Red MEDELLIN

MEDELLIN2 Interfaz S0/0/1 (DCE) a MEDELLIN1 Interfaz S0/0/1	
	
MEDELLIN1 Interfaz S0/0/0 (DCE) a MEDELLIN3 Interfaz S0/0/0	
	

MEDELLIN3 Interfaz S0/1/1 (DCE) a MEDELLIN1 Interfaz S0/1/1	
	
MEDELLIN3 Interfaz S0/1/0 (DCE) a MEDELLIN2 Interfaz S0/0/0	
	

Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

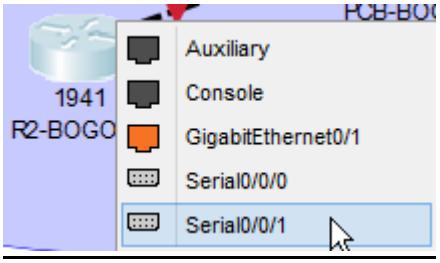
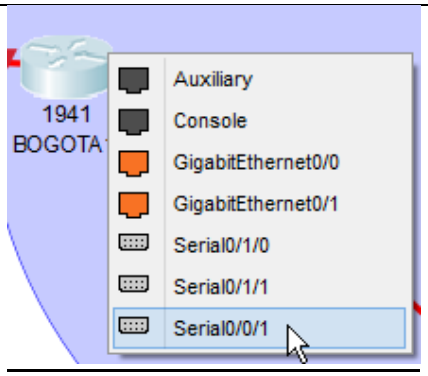
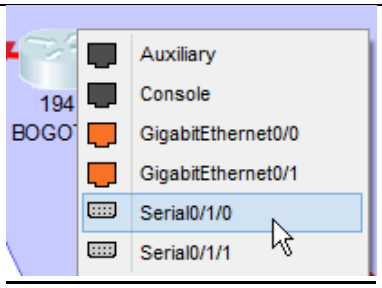
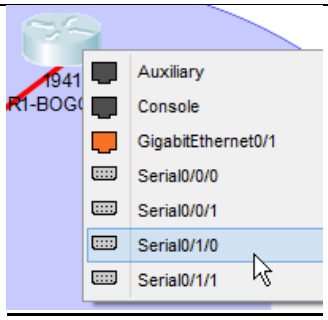
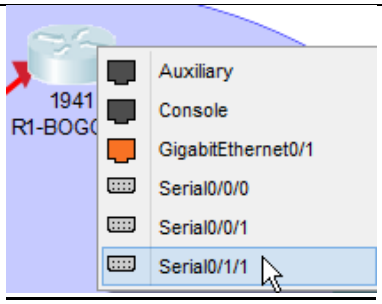
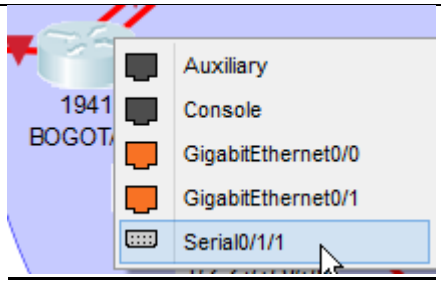
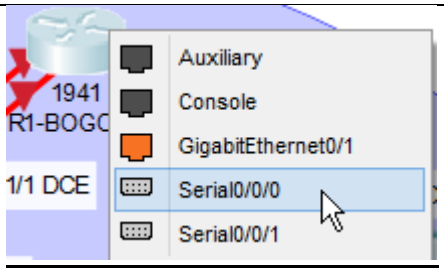
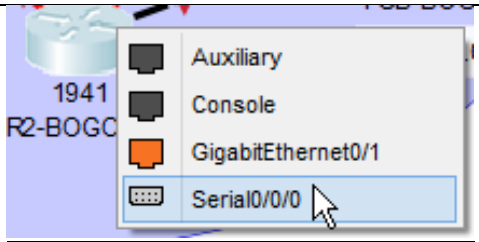
Figura 20 Conexiones de Red MEDELLIN



Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

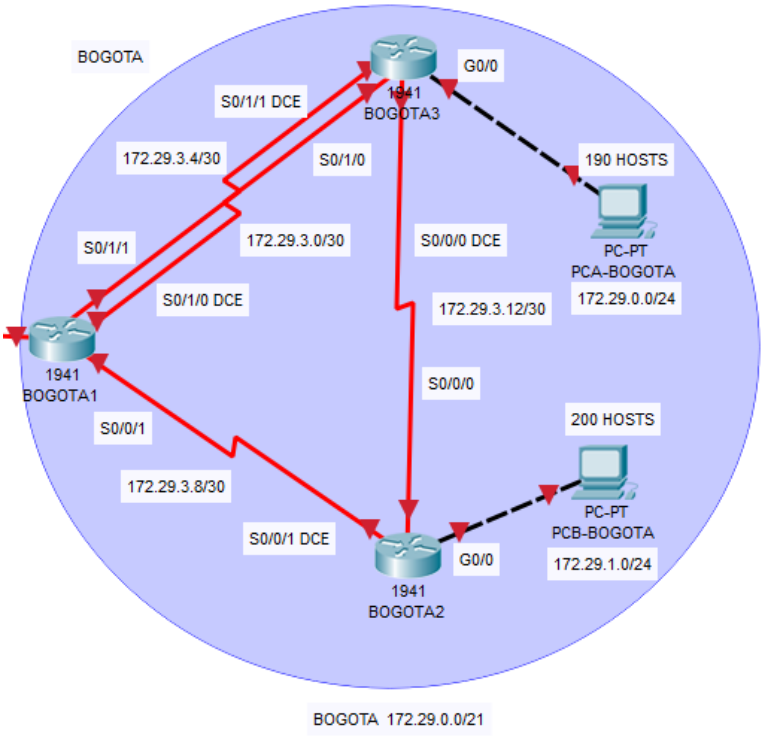
Conexiones de Red BOGOTA

Tabla 2 Conexiones de Red BOGOTA

BOGOTA2 Interfaz S0/0/1 (DCE) a BOGOTA1 Interfaz S0/0/1	
	
BOGOTA1 Interfaz S0/1/0 (DCE) a BOGOTA3 Interfaz.S0/1/0	
	
BOGOTA3 Interfaz S0/1/1 (DCE) a BOGOTA1 Interfaz S0/1/1	
	
BOGOTA3 Interfaz S0/0/0 (DCE) a BOGOTA2 Interfaz S0/0/0	
	

Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

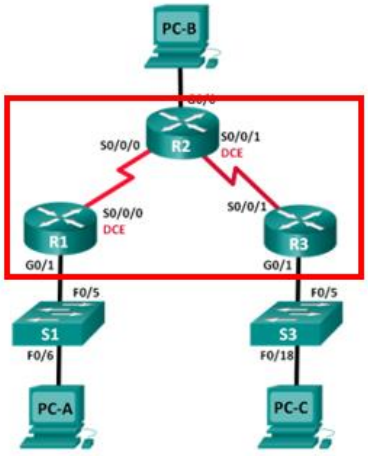
Figura 21 Conexiones de Red BOGOTA



Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

Configuración basada en el **Laboratorio 7.3.2.4** correspondiente a la Tarea 4.

Figura 22 Topología Laboratorio 7.3.2.4 Tarea 4



Fuente: [Practicas Tarea 4]

Configuración Básica de dispositivos

RIP versión 2 (RIPv2) se utiliza para enrutar direcciones IPv4 en redes pequeñas. RIPv2 es un protocolo de routing vector distancia sin clase, según la definición de RFC 1723. Debido a que RIPv2 es un protocolo de routing sin clase, las máscaras de subred se incluyen en las actualizaciones de routing. De manera predeterminada, RIPv2 resume automáticamente las redes en los límites de redes principales. Cuando se deshabilita la sumarización automática, RIPv2 ya no resume las redes a su dirección con clase en routers fronterizos.

1.1.1. Parte 1: Configuración del enrutamiento

a. Configurar el enrutamiento en la red usando el protocolo RIP versión 2, declarar la red principal y desactivar la sumarización automática.

Las direcciones IP están compuestas por cuatro octetos, cada uno de 8 bits para un total de 32 bits.

Máscaras de Red

Delimitan el ámbito de una red. Indican a un host cual es la porción de red y cuál es la porción de host de acuerdo con su dirección IP.

Se suele trabajar con tres clases de direcciones:

Clase A: 0.0.0.0 – 127.255.255.255.
Clase B: 128.0.0.0 – 191.255.255.255.
Clase C 192.0.0.0 – 223.255.255.255.

Cada clase lleva un prefijo asignado (máscara), este permite determinar cuántos bits corresponden a la porción de red y por consiguiente a la porción de host.

Clase A: /8
Clase B: /16.
Clase C: /24.

En la notación binaria se representarían de la siguiente manera:

Tabla 3 Notación binaria de clases de direcciones IP

Clase A	**11111111**	.	**00000000**	.	**00000000**	.	**00000000**
Clase B	**11111111**	.	**11111111**	.	**00000000**	.	**00000000**
Clase C	**11111111**	.	**11111111**	.	**11111111**	.	**00000000**

Fuente: Autoria Propia.

Octetos **11111111**: para la porción de red.
Octetos **00000000**: para la porción de host.

Si se convierte al sistema decimal, se obtienen las siguientes máscaras de red para cada clase de dirección IP:

Tabla 4 Notación decimal de clases de direcciones IP

Clase A	255	.	0	.	0	.	0
Clase B	255	.	255	.	0	.	0
Clase C	255	.	255	.	255	.	0

Fuente: Autoria Propia.

Máscaras de Subred

Al realizar direccionamiento se suelen dividir las redes para ajustarlas a los requerimientos y evitar el menor desperdicio de direcciones IPv4.

Siempre se especifica el prefijo y dependiendo de la clase, este determina cuantos bits se toman prestados de la porción de host. Por ejemplo:

Dirección IP 192.168.10.3/**29**

Para determinar la máscara de subred se realiza lo siguiente:

- ✓ Determinar la clase de la dirección IP:

Clase C.

- ✓ Tomar la máscara de red correspondiente a la clase:

255.255.255.0.

- ✓ Convertir la máscara de red al sistema binario:

11111111.11111111.11111111.00000000

- ✓ Se completa el prefijo indicado, tomando bits de la porción de host. Cada bit que se tome aumenta en una unidad el prefijo, como se sabe que para esta dirección es /**24**, se toman prestados **5 bits** de la porción de host. Al tomarse prestados su valor binario cambia a 1:

11111111.11111111.11111111.**11111**000

- ✓ Se convierte la máscara de subred al sistema decimal:

255.255.255.248

De esta manera se puede determinar rápidamente una máscara de red o subred cuando se indica el prefijo.

En una dirección IP deben quedar como mínimo 2 bits en la porción de host.

Al momento de asignar una dirección IP se debe tener en cuenta lo siguiente:

- ✓ La dirección de red no se asigna a ningún host.
- ✓ Desde la primera hasta la última dirección dentro del rango de direcciones de host utilizables se pueden asignar.
- ✓ La dirección de broadcast no se asigna a ningún host porque es la dirección de difusión. Esta dirección suele ser la última dentro del rango de direcciones.

Como no se especifican las divisiones de redes se asignarán a los hosts la primera, segunda o tercera dirección utilizable después de la dirección de red.

Ejemplo:

RED 192.168.25.0/24 Direcciones de host utilizables: 172.168.25.1, 192.168.25.2, etc.

Direccionamiento VLSM

De acuerdo con las necesidades se suelen desperdiciar muchas direcciones IP y se limita el crecimiento de la red. Esto caracteriza la división de redes tradicional que busca satisfacer la subred mas grande independiente de la cantidad de direcciones que sobren.

Las Máscaras de Subred de Longitud Variable (VLSM) se diseñaron para evitar desperdicios en la división de subredes tradicional.

Se tiene en cuenta la siguiente tabla para direcciones Clase B:

Tabla 5 División de una red /16 en subredes

Numero de bits prestados	**Cantidad de Subredes 2^n n = número de bits prestados**	**Cantidad de Host Utilizables 2^n-2 n = número de bits restantes**
1	2	32564
2	4	16282
3	8	8190
4	16	4094
5	32	2046
6	64	1022

7	128	510
8	256	254
9	512	126
10	1024	62
11	2048	30
12	4096	14
13	8192	6
14	16384	2

Fuente: Asignacion de Direcciones IP

SUBRED MEDELLIN

- ✓ LAN MEDELLIN2 (PCA-MEDELLIN) 172.29.4.0/25 requiere 50 direcciones IP de host.

La máscara de subred para esta dirección esta dada por el prefijo /25. El prefijo indica que la porción de red está compuesta por 25 bits y la porción de host por 7 bits.

Tabla 6 Notación decimal dirección de subred y máscara LAN MEDELLIN2

	Notación decimal Punteada						
Direccion de Subred	172	.	29	.	4	.	0
Mascara de Subred	255	.	255	.	255	.	128

Fuente: Autoria Propia.

Notacion Binaria

Tabla 7 Notación binaria dirección de subred y máscara LAN MEDELLIN2

	Notación Binaria						
Direccion de Subred	10101100	.	00011101	.	00000100	.	00000000
Mascara de Subred	11111111	.	11111111	.	11111111	.	10000000

Fuente: Autoria Propia.

La mascará de subred actual indica que se tomaron prestados 9 bits, por lo tanto admitirá **126 direcciones de host utilizables**.

Nueva Mascara de subred

Se toma 1 bit prestado.

Tabla 8 Notación binaria nueva máscara LAN MEDELLIN2

255	.	255	.	255	.	192							
11111111	.	11111111	.	11111111	.	1	**1**	1	0	0	0	0	0

Fuente: Autoria Propia.

Esta subred admitirá **62 direcciones de host utilizables**.

- ✓ LAN MEDELLIN3 (PCB-MEDELLIN) 172.29.4.128/25 requiere 40 direcciones IP de host.

La máscara de subred para esta dirección esta dada por el prefijo /25. El prefijo indica que la porción de red está compuesta por 25 bits y la porción de host por 7 bits.

Tabla 9 Notación decimal dirección de subred y máscara LAN MEDELLIN3

	Notación decimal Punteada						
Direccion de Subred	172	.	29	.	4	.	128
Mascara de Subred	255	.	255	.	255	.	128

Fuente: Autoria Propia.

Notacion Binaria

Tabla 10 Notación binaria dirección de subred y máscara LAN MEDELLIN3

	Notación Binaria						
Direccion de Subred	10101100	.	00011101	.	00000100	.	10000000
Mascara de Subred	11111111	.	11111111	.	**11111111**	.	**1**0000000

Fuente: Autoria Propia.

La mascará de subred actual indica que se tomaron prestados 9 bits, por lo tanto admitirá **126 direcciones de host utilizables**.

Nueva Mascara de subred

Se toma 1 bit prestado.

Tabla 11 Notación binaria nueva máscara LAN MEDELLIN3

255	.	255	.	255	.	192							
11111111	.	11111111	.	11111111	.	1	**1**	1	0	0	0	0	0

Fuente: Autoria Propia.

Esta subred admitirá **62 direcciones de host utilizables**.

SUBRED BOGOTA

- LAN BOGOTA3 172.29.0.0/24 (PCA-BOGOTA) requiere 190 direcciones IP de host.

La máscara de subred para esta dirección esta dada por el prefijo /24. El prefijo indica que la porción de red está compuesta por 24 bits y la porción de host por 8 bits.

Tabla 12 Notación decimal dirección de subred y máscara LAN BOGOTA3

	Notación decimal Punteada						
Direccion de Subred	172	.	29	.	0	.	0
Mascara de Subred	255	.	255	.	255	.	0

Fuente: Autoria Propia.

Notacion Binaria

Tabla 13 Notación binaria dirección de subred y máscara LAN BOGOTA3

	Notación Binaria						
Direccion de Subred	10101100	.	00011101	.	00000000	.	00000000
Mascara de Subred	11111111	.	11111111	.	**11111111**	.	00000000

Fuente: Autoria Propia.

La mascará de subred actual admitirá **256** direcciones de host utilizables.

Esta subred admitirá **62 direcciones de host utilizables**.

- LAN BOGOTA2 172.29.0.1/24 (PCB-BOGOTA) requiere 200 direcciones IP de host.

La máscara de subred para esta dirección esta dada por el prefijo /24. El prefijo indica que la porción de red está compuesta por 24 bits y la porción de host por 8 bits.

Tabla 14 Notación decimal dirección de subred y máscara LAN BOGOTA2

	Notación decimal Punteada						
Direccion de Subred	172	.	29	.	0	.	1
Mascara de Subred	255	.	255	.	255	.	0

Fuente: Autoria Propia.

Notacion Binaria

Tabla 15 Notación binaria dirección de subred y máscara LAN BOGOTA2

	Notación Binaria						
Direccion de Subred	10101100	.	00011101	.	00000000	.	00000001
Mascara de Subred	11111111	.	11111111	.	**11111111**	.	00000000

Fuente: Autoria Propia.
La mascará de subred actual admitirá **256 direcciones de host utilizables**.

Tabla de Direccionamiento

Tabla 16 Tabla de Direccionamiento Escenario 1

Dispositivo	**Interfaz**	**Direccion IP**	**Mascara de Subred**	**Gateway Pred.**
MEDELLIN1	S0/1/0	209.17.220.2	255.255.255.252	No aplica
	S0/0/0 DCE	172.29.6.13	255.255.255.252	No aplica
	S0/0/1	172.29.6.1	255.255.255.252	No aplica
	S0/1/1	172.29.6.9	255.255.255.252	No aplica
MEDELLIN2	G0/0	172.29.4.1	255.255.255.192	No aplica
	S0/0/0	172.29.6.5	255.255.255.252	No aplica
	S0/0/1 DCE	172.29.6.2	255.255.255.252	No aplica
MEDELLIN3	G0/0	172.29.4.129	255.255.255.192	No aplica
	S0/0/0	172.29.6.14	255.255.255.252	No aplica

	S0/1/0 DCE	172.29.6.6	255.255.255.252	No aplica
	S0/0/1 DCE	172.29.6.10	255.255.255.252	No aplica
BOGOTA1	S0/0/0	209.17.220.6	255.255.255.252	No aplica
	S0/0/1	172.29.3.9	255.255.255.252	No aplica
	S0/1/0 DCE	172.29.3.1	255.255.255.252	No aplica
	S0/1/1	172.29.3.5	255.255.255.252	No aplica
BOGOTA2	G0/0	172.29.1.1	255.255.255.0	No aplica
	S0/0/0	172.29.3.13	255.255.255.252	No aplica
	S0/0/1 DCE	172.29.3.10	255.255.255.252	No aplica
BOGOTA3	G0/0	172.29.0.1	255.255.255.0	No aplica
	S0/0/0 DCE	172.29.3.14	255.255.255.252	No aplica
	S0/1/0	172.29.3.2	255.255.255.252	No aplica
	S0/1/1 DCE	172.29.3.6	255.255.255.252	No aplica
ISP	S0/0/0 DCE	209.17.220.1	255.255.255.252	No aplica
	S0/0/1 DCE	209.17.220.5	255.255.255.252	No aplica
PCA-MEDELLIN	NIC	172.29.4.2	255.255.255.192	172.29.4.1
PCB-MEDELLIN	NIC	172.29.4.130	255.255.255.192	172.29.4.129
PCA-BOGOTA	NIC	172.29.0.2	255.255.255.0	172.29.0.1
PCB-BOGOTA	NIC	172.29.1.2	255.255.255.0	172.29.1.1

Fuente: Autoria Propia.

Configuracion de parámetros básicos

- **Routers**

✓ En Packet Tracer se hace clic sobre el dispositivo y a continuación, se ubica la pestaña **CLI.**

Figura 23 Pestaña CLI MEDELLIN1

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se ingresa al modo EXEC privilegiado con el comando **enable** o su abreviatura **en**. La petición de entrada cambia.

Dispositivo>en

Dispositivo #

- ✓ Se ingresa al modo de configuración global con el comando **configure** terminal o abreviado **config t**. La petición de entrada cambia.

Dispositivo #config t

Dispositivo (config)#

- ✓ Se cambia el nombre del host con el comando **hostname** *nombre-host.*
- ✓ Se deshabilita la búsqueda DNS con el comando de configuración global **no ip domain-lookup**. Esto se hace para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- ✓ Se asigna una contraseña para el modo EXEC privilegiado con el comando de configuración global **enable secret** *contraseña*.
- ✓ Se asigna una contraseña de consola. Para esto se ingresa al modo de configuración de consola con el comando de configuración global **line console 0** o abreviado **line con 0**:
  - ✓ Se asigna la contraseña con el comando **password** *contraseña.*
  - ✓ Se establece un tiempo de espera para la sesión con el comando **exec-timeout** *minutos segundos.*
  - ✓ Se habilita el inicio se sesión con el comando **login.**
  - ✓ Se sincroniza la depuración y el resultado del software IOS de Cisco, y evita que estos mensajes interrumpan la entrada del teclado con el comando **logging synchronous.**
  - ✓ Se sale de la configuración de consola con el comando **exit**.
- ✓ Se asigna una contraseña a las líneas vty. Esta configuración permite el acceso remoto. Se ingresa al modo de configuración de línea con el comando **line vty 0 15.**
  - ✓ Se repiten los pasos de la configuración de consola.
- ✓ Se cifran las contraseñas actuales y futuras de texto no cifrado con el comando de configuración global **service password-encryption.**
- ✓ Se crea un mensaje del día con el comando de configuración global **banner motd #***mensaje***#**. El carácter delimitador # puede cambiarse por otro que sea válido en la versión de IOS. Este mensaje advierte a aquel que acceda al dispositivo que el acceso no autorizado está prohibido.

- ✓ Se procede con la configuración de direccionamiento ingresando al modo de configuración de interfaz con el comando de configuración global **interface** *id-interfaz.*
  - ✓ Se añade una descripción a la interfaz con el comando **description** *descripción.*
  - ✓ Se asigna la dirección IP y la máscara de subred con el comando **ip address** *dirección-IP mascara.*
  - ✓ En las **interfaces seriales** se debe configurar la frecuencia del reloj con el comando **clock rate** *frecuencia*.
  - ✓ Se activa la interfaz con el comando **no shutdown** o abreviado **no shut. Nota:** las interfaces seriales cuando se comienzan a activar se puede mostrar que su estado cambio de **Administratively Down** a **Down**, esto se debe a que se deben activar las demás interfaces seriales para que se active automáticamente.
  - ✓ Se regresa al modo EXEC privilegiado con el comando **end.**
- ✓ Se guarda la configuración de ejecución en la NVRAM con el comando del modo EXEC privilegiado **copy running-config startup-config.** Se especifica el destino o se puede dejar en blanco.

MEDELLIN1

Router>en

Router#config t

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

Router(config)#hostname MEDELLIN1

MEDELLIN1(config)#no ip domain-lookup

MEDELLIN1(config)#enable secret cisco2019

MEDELLIN1(config)#line con 0

MEDELLIN1(config-line)#password class2019

MEDELLIN1(config-line)#exec-timeout 15 0

MEDELLIN1(config-line)#login

MEDELLIN1(config-line)#logging synchronous

MEDELLIN1(config-line)#exit

MEDELLIN1(config)#line vty 0 4

MEDELLIN1(config-line)#password cisco2019

MEDELLIN1(config-line)#exec-timeout 15 0

MEDELLIN1(config-line)#login

MEDELLIN1(config-line)#logging synchronous

MEDELLIN1(config-line)#exit

MEDELLIN1(config)#service password-encryption

MEDELLIN1(config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

MEDELLIN1(config)#

Configuración Direccionamiento

ENLACE WAN MEDELLIN1 - ISP

- ✓ Interfaz S0/1/0

Subred: 209.17.220.0

Mascara: 255.255.255.252

MEDELLIN1(config)#int s0/1/0

MEDELLIN1 (config-if)#description ENLACE WAN MEDELLIN1 – ISP SUBRED 209.17.220.0/30

MEDELLIN1 (config-if)#ip address 209.17.220.2 255.255.255.252

MEDELLIN1 (config-if)#no shutdown

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

MEDELLIN1 (config-if)#exit

ENLACE WAN MEDELLIN1 – MEDELLIN3

- ✓ Interfaz S0/0/0 DCE

Subred: 172.29.6.12

Mascara: 255.255.255.252

MEDELLIN1(config)#int s0/0/0

MEDELLIN1 (config-if)#description ENLACE WAN MEDELLIN1 – MEDELLIN3 SUBRED 172.29.6.12/30

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 Serial0/0/0, changed state to down

MEDELLIN1 (config-if)#exit

ENLACE WAN MEDELLIN1 – MEDELLIN2

- ✓ Interfaz S0/0/1

Subred: 172.29.6.0

Mascara: 255.255.255.252

MEDELLIN1(config)#int s0/0/1

MEDELLIN1 (config-if)#description ENLACE WAN MEDELLIN1 – MEDELLIN2 SUBRED 172.29.6.0/30

MEDELLIN1 (config-if)#ip address 172.29.6.1 255.255.255.252

MEDELLIN1 (config-if)#no shutdown

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

MEDELLIN1 (config-if)#exit

ENLACE WAN MEDELLIN1 – MEDELLIN3

- ✓ Interfaz S0/1/1

Subred: 172.29.6.8

Mascara: 255.255.255.252

MEDELLIN1(config)#int s0/1/1

MEDELLIN1 (config-if)#description ENLACE WAN MEDELLIN1 – MEDELLIN3 SUBRED 172.29.6.8/30

MEDELLIN1 (config-if)#ip address 172.29.6.9 255.255.255.252

MEDELLIN1 (config-if)#no shutdown

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

MEDELLIN1 (config-if)#

Configuración guardada en la NVRAM

MEDELLIN1 (config-if)#end

MEDELLIN1 #

%SYS-5-CONFIG_I: Configured from console by console

MEDELLIN1 #copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

MEDELLIN1 #

MEDELLIN2

Router>en

Router#config t

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

Router(config)#hostname MEDELLIN2

MEDELLIN2 (config)#no ip domain-lookup

MEDELLIN2 (config)#enable secret cisco2019

MEDELLIN2 (config)#line con 0

MEDELLIN2 (config-line)#password class2019

MEDELLIN2 (config-line)#exec-timeout 15 0

MEDELLIN2 (config-line)#login

MEDELLIN2 (config-line)#logging synchronous

MEDELLIN2 (config-line)#exit

MEDELLIN2 (config)#line vty 0 4

MEDELLIN2 (config-line)#password cisco2019

MEDELLIN2 (config-line)#exec-timeout 15 0

MEDELLIN2 (config-line)#login

MEDELLIN2 (config-line)#logging synchronous

MEDELLIN2 (config-line)#exit

MEDELLIN2 (config)#service password-encryption

MEDELLIN2 (config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

Configuración Direccionamiento

ENLACE LAN MEDELLIN2 – PCA-MEDELLIN (50 HOSTS)

- ✓ Interfaz G0/0

Subred: 172.29.4.0

Mascara: 255.255.255.128

MEDELLIN2 (config)#int g0/0

MEDELLIN2 (config-if)#description ENLACE LAN MEDELLIN2 – PCA-MEDELLIN (50 HOSTS) SUBRED 172.29.4.0/26

MEDELLIN2 (config-if)#ip address 172.29.4.1 255.255.255.192

MEDELLIN2 (config-if)#no shutdown

%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

ENLACE WAN MEDELLIN2 – MEDELLIN3

- ✓ Interfaz S0/0/0

Subred: 172.29.6.4

Mascara: 255.255.255.252

MEDELLIN2 (config)#int s0/0/0

MEDELLIN2 (config-if)#description ENLACE WAN MEDELLIN2 – MEDELLIN3 SUBRED 172.29.6.4/30

MEDELLIN2 (config-if)#ip address 172.29.6.5 255.255.255.252

MEDELLIN2 (config-if)#no shutdown

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

MEDELLIN1 (config-if)#exit

ENLACE WAN MEDELLIN2 – MEDELLIN1

- ✓ Interfaz S0/0/1 DCE

Subred: 172.29.6.0

Mascara: 255.255.255.252

MEDELLIN2 (config)#int s0/0/1

MEDELLIN2 (config-if)#description ENLACE WAN MEDELLIN2 – MEDELLIN1 SUBRED 172.29.6.0/30

MEDELLIN2 (config-if)#ip address 172.29.6.2 255.255.255.252

MEDELLIN2 (config-if)#clock rate 128000

MEDELLIN2 (config-if)#no shutdown

MEDELLIN2(config-if)#

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

MEDELLIN2(config-if)#

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

MEDELLIN2 (config-if)#exit

Configuración guardada en la NVRAM

MEDELLIN2 (config-if)#end

MEDELLIN2 #

%SYS-5-CONFIG_I: Configured from console by console

MEDELLIN2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

MEDELLIN2#

MEDELLIN3

Router>en

Router#config t

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

Router(config)#hostname MEDELLIN3

MEDELLIN3 (config)#no ip domain-lookup

MEDELLIN3 (config)#enable secret cisco2019

MEDELLIN3 (config)#line con 0

MEDELLIN3 (config-line)#password class2019

MEDELLIN3 (config-line)#exec-timeout 15 0

MEDELLIN3 (config-line)#login

MEDELLIN3 (config-line)#logging synchronous

MEDELLIN3 (config-line)#exit

MEDELLIN3 (config)#line vty 0 4

MEDELLIN3 (config-line)#password cisco2019

MEDELLIN3 (config-line)#exec-timeout 15 0

MEDELLIN3 (config-line)#login

MEDELLIN3 (config-line)#logging synchronous

MEDELLIN3 (config-line)#exit

MEDELLIN3 (config)#service password-encryption

MEDELLIN3 (config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

MEDELLIN1(config)#

Configuración Direccionamiento

ENLACE LAN MEDELLIN3 – PC-B MEDELLIN (40 HOSTS)

- ✓ Interfaz G0/0

Subred: 172.29.4.128

Mascara: 255.255.255.128

MEDELLIN3 (config)#int g0/0

MEDELLIN3 (config-if)#description ENLACE LAN MEDELLIN3 – PC-B MEDELLIN (40 HOSTS) SUBRED 172.29.4.128/26

MEDELLIN3 (config-if)#ip address 172.29.4.129 255.255.255.192

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

ENLACE WAN MEDELLIN3 – MEDELLIN1

- ✓ Interfaz S0/0/0

Subred: 172.29.6.12

Mascara: 255.255.255.252

MEDELLIN3 (config)#int s0/0/0

MEDELLIN3 (config-if)#description ENLACE WAN MEDELLIN3 – MEDELLIN1 SUBRED 172.29.6.12/30

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 Serial0/0/0, changed state to up

MEDELLIN3 (config-if)#

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

MEDELLIN3 (config-if)#exit

ENLACE WAN MEDELLIN3 – MEDELLIN2

- ✓ Interfaz S0/1/0 DCE

Subred: 172.29.6.4

Mascara: 255.255.255.252

MEDELLIN3 (config)#int s0/1/0

MEDELLIN3 (config-if)#description ENLACE WAN MEDELLIN3 – MEDELLIN2 SUBRED 172.29.6.4/30

MEDELLIN3 (config-if)#ip address 172.29.6.6 255.255.255.252

MEDELLIN3 (config-if)#clock rate 128000

MEDELLIN3 (config-if)#no shutdown

MEDELLIN3 (config-if)#

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

MEDELLIN3(config-if)#

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

MEDELLIN3 (config-if)#exit

ENLACE WAN MEDELLIN3 – MEDELLIN1

- ✓ Interfaz S0/0/1 DCE

Subred: 172.29.6.8

Mascara: 255.255.255.252

MEDELLIN3 (config)#int s0/0/1

MEDELLIN3 (config-if)#description ENLACE WAN MEDELLIN3 – MEDELLIN1 SUBRED 172.29.6.8/30

MEDELLIN3 (config-if)#ip address 172.29.6.10 255.255.255.252

MEDELLIN3 (config-if)#clock rate 128000

MEDELLIN3 (config-if)#no shutdown

MEDELLIN3(config-if)#

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

MEDELLIN3(config-if)#

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

MEDELLIN3 (config-if)#

Configuración guardada en la NVRAM

MEDELLIN3(config-if)#end

MEDELLIN3#

%SYS-5-CONFIG_I: Configured from console by console

MEDELLIN3#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

MEDELLIN3#

BOGOTA1

Router>en

Router#config t

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

Router(config)#hostname BOGOTA1

BOGOTA1 (config)#no ip domain-lookup

BOGOTA1 (config)#enable secret cisco2019

BOGOTA1 (config)#line con 0

BOGOTA1 (config-line)#password class2019

BOGOTA1 (config-line)#exec-timeout 15 0

BOGOTA1 (config-line)#login

BOGOTA1 (config-line)#logging synchronous

BOGOTA1 (config-line)#exit

BOGOTA1 (config)#line vty 0 4

BOGOTA1 (config-line)#password cisco2019

BOGOTA1 (config-line)#exec-timeout 15 0

BOGOTA1 (config-line)#login

BOGOTA1 (config-line)#logging synchronous

BOGOTA1 (config-line)#exit

BOGOTA1 (config)#service password-encryption

BOGOTA1 (config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

BOGOTA1 (config)#

Configuración Direccionamiento

ENLACE WAN BOGOTA1 - ISP

- ✓ Interfaz S0/0/0

Subred: 209.17.220.4

Mascara: 255.255.255.252

BOGOTA1 (config)#int s0/0/0

BOGOTA1 (config-if)#description ENLACE WAN BOGOTA1 – ISP SUBRED 209.17.220.4/30

BOGOTA1 (config-if)#ip address 209.17.220.6 255.255.255.252

BOGOTA1 (config-if)#no shutdown

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

BOGOTA1 (config-if)#exit

ENLACE WAN BOGOTA1 – BOGOTA2

- ✓ Interfaz S0/0/1

Subred: 172.29.3.8

Mascara: 255.255.255.252

BOGOTA1 (config)#int s0/0/1

BOGOTA1 (config-if)#description ENLACE WAN BOGOTA1 – BOGOTA2 SUBRED 172.29.3.8/30

BOGOTA1 (config-if)#ip address 172.29.3.9 255.255.255.252

BOGOTA1 (config-if)#no shutdown

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

BOGOTA1 (config-if)#exit

ENLACE WAN BOGOTA1 – BOGOTA3

- ✓ Interfaz S0/1/0 DCE

Subred: 172.29.3.0

Mascara: 255.255.255.252

BOGOTA1 (config)#int s0/1/0

BOGOTA1 (config-if)#description ENLACE WAN BOGOTA1 – BOGOTA3 SUBRED 172.29.3.0/30

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 Serial0/1/0, changed state to down

BOGOTA1 (config-if)#exit

ENLACE WAN BOGOTA1 – BOGOTA3

- ✓ Interfaz S0/1/1

Subred: 172.29.3.4

Mascara: 255.255.255.252

BOGOTA1 (config)#int s0/1/1

BOGOTA1 (config-if)#description ENLACE WAN BOGOTA1 – BOGOTA3 SUBRED 172.29.3.4/30

BOGOTA1 (config-if)#ip address 172.29.3.5 255.255.255.252

BOGOTA1 (config-if)#no shutdown

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

BOGOTA1 (config-if)#

Configuración guardada en la NVRAM

BOGOTA1 (config-if)#end

BOGOTA1 #

%SYS-5-CONFIG_I: Configured from console by console

BOGOTA1 #copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

BOGOTA1 #

BOGOTA2

Router>en

Router#config t

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

Router(config)#hostname BOGOTA2

BOGOTA2 (config)#no ip domain-lookup

BOGOTA2 (config)#enable secret cisco2019

BOGOTA2 (config)#line con 0

BOGOTA2 (config-line)#password class2019

BOGOTA2 (config-line)#exec-timeout 15 0

BOGOTA2 (config-line)#login

BOGOTA2 (config-line)#logging synchronous

BOGOTA2 (config-line)#exit

BOGOTA2 (config)#line vty 0 4

BOGOTA2 (config-line)#password cisco2019

BOGOTA2 (config-line)#exec-timeout 15 0

BOGOTA2 (config-line)#login

BOGOTA2 (config-line)#logging synchronous

BOGOTA2 (config-line)#exit

BOGOTA2 (config)#service password-encryption

BOGOTA2 (config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

Configuración Direccionamiento

ENLACE LAN BOGOTA – PCB-BOGOTA (200 HOSTS)

- ✓ Interfaz G0/0

Subred: 172.29.1.0

Mascara: 255.255.255.0

BOGOTA2 (config)#int g0/0

BOGOTA2 (config-if)#description LAN BOGOTA – PCB-BOGOTA (200 HOSTS) SUBRED 172.29.1.0/24

BOGOTA2 (config-if)#ip address 172.29.1.1 255.255.255.0

BOGOTA2 (config-if)#no shutdown

%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)#exit

ENLACE WAN BOGOTA2 – BOGOTA3

- ✓ Interfaz S0/0/0

Subred: 172.29.3.12

Mascara: 255.255.255.252

BOGOTA2 (config)#int s0/0/0

BOGOTA2 (config-if)#description ENLACE WAN BOGOTA2 – BOGOTA3 SUBRED 172.29.3.12/30

BOGOTA2 (config-if)#ip address 172.29.3.13 255.255.255.252

BOGOTA2 (config-if)#no shutdown

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

BOGOTA2 (config-if)#exit

ENLACE WAN BOGOTA2 – BOGOTA1

- ✓ Interfaz S0/0/1 DCE

Subred: 172.29.3.8

Mascara: 255.255.255.252

BOGOTA2 (config)#int s0/0/1

BOGOTA2 (config-if)#description ENLACE WAN BOGOTA2 – BOGOTA1 SUBRED 172.29.3.8/30

BOGOTA2 (config-if)#ip address 172.29.3.10 255.255.255.252

BOGOTA2 (config-if)#clock rate 128000

BOGOTA2 (config-if)#no shutdown

BOGOTA2 (config-if)#

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

BOGOTA2 (config-if)#

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

BOGOTA2 (config-if)#exit

Configuración guardada en la NVRAM

BOGOTA2 (config-if)#end

BOGOTA2#

%SYS-5-CONFIG_I: Configured from console by console

BOGOTA2 #copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

BOGOTA2 #

BOGOTA3

Router>en

Router#config t

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

Router(config)#hostname BOGOTA3

BOGOTA3 (config)#no ip domain-lookup

BOGOTA3 (config)#enable secret cisco2019

BOGOTA3 (config)#line con 0

BOGOTA3 (config-line)#password class2019

BOGOTA3 (config-line)#exec-timeout 15 0

BOGOTA3 (config-line)#login

BOGOTA3 (config-line)#logging synchronous

BOGOTA3 (config-line)#exit

BOGOTA3 (config)#line vty 0 4

BOGOTA3 (config-line)#password cisco2019

BOGOTA3 (config-line)#exec-timeout 15 0

BOGOTA3 (config-line)#login

BOGOTA3 (config-line)#logging synchronous

BOGOTA3 (config-line)#exit

BOGOTA3 (config)#service password-encryption

BOGOTA3 (config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

MEDELLIN1(config)#

Configuración Direccionamiento

ENLACE LAN BOGOTA3 – PC-A BOGOTA (190 HOSTS)

- ✓ Interfaz G0/0

Subred: 172.29.0.0

Mascara: 255.255.255.0

BOGOTA3 (config)#int g0/0

BOGOTA3 (config-if)#description LAN BOGOTA3 – PC-A BOGOTA (190 HOSTS) SUBRED 172.29.0.0/24

BOGOTA3 (config-if)#ip address 172.29.0.1 255.255.255.0

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

ENLACE WAN BOGOTA3 – BOGOTA2

- ✓ Interfaz S0/0/0 DCE

Subred: 172.29.3.12

Mascara: 255.255.255.252

BOGOTA3 (config)#int s0/0/0

BOGOTA3 (config-if)#description ENLACE WAN BOGOTA3 – BOGOTA2 SUBRED 172.29.3.12/30

BOGOTA3 (config-if)#ip address 172.29.3.14 255.255.255.252

BOGOTA3 (config-if)#clock rate 128000

BOGOTA3 (config-if)#no shutdown

BOGOTA3 (config-if)#

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

BOGOTA3(config-if)#

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

BOGOTA3 (config-if)#exit

ENLACE WAN BOGOTA3 – BOGOTA1

- ✓ Interfaz S0/1/0

Subred: 172.29.3.0

Mascara: 255.255.255.252

BOGOTA3 (config)#int s0/1/0

BOGOTA3(config-if)#description ENLACE WAN BOGOTA3 – BOGOTA1 SUBRED 172.29.3.0/30

BOGOTA3 (config-if)#ip address 172.29.3.2 255.255.255.252

BOGOTA3 (config-if)#no shutdown

BOGOTA3(config-if)#

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

BOGOTA3(config-if)#

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

BOGOTA3 (config-if)#exit

ENLACE WAN BOGOTA3 – BOGOTA1

- ✓ Interfaz S0/1/1 DCE

Subred: 172.29.3.4

Mascara: 255.255.255.252

BOGOTA3 (config)#int s0/1/1

BOGOTA3 (config-if)#description ENLACE WAN BOGOTA3 – BOGOTA1 SUBRED 172.29.3.4/30

BOGOTA3 (config-if)#ip address 172.29.3.6 255.255.255.252

BOGOTA3 (config-if)#clock rate 128000

BOGOTA3 (config-if)#no shutdown

BOGOTA3 (config-if)#

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

BOGOTA3(config-if)#

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

BOGOTA3 (config-if)#

Configuración guardada en la NVRAM

BOGOTA3 (config-if)#end

BOGOTA3 #

%SYS-5-CONFIG_I: Configured from console by console

BOGOTA3 #copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

BOGOTA3 #

ISP

Router>en

Router#config t

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

Router(config)#hostname ISP

ISP (config)#no ip domain-lookup

ISP (config)#enable secret cisco2019

ISP (config)#line con 0

ISP (config-line)#password class2019

ISP (config-line)#exec-timeout 15 0

ISP (config-line)#login

ISP (config-line)#logging synchronous

ISP (config-line)#exit

ISP (config)#line vty 0 4

ISP (config-line)#password cisco2019

ISP (config-line)#exec-timeout 15 0

ISP (config-line)#login

ISP (config-line)#logging synchronous

ISP (config-line)#exit

ISP (config)#service password-encryption

ISP (config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

ISP (config)#

Configuración Direccionamiento

ENLACE WAN ISP – MEDELLIN1

- ✓ Interfaz S0/0/0 DCE

Subred: 209.17.220.0/30

Mascara: 255.255.255.252

ISP (config)#int S0/0/0

ISP (config-if)#description ENLACE WAN ISP – MEDELLIN1 SUBRED 209.17.220.0/30

ISP (config-if)#ip address 209.17.220.1 255.255.255.252

ISP (config-if)#clock rate 128000

ISP (config-if)#no shutdown

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

ISP(config-if)#

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

ISP (config-if)#exit

ENLACE WAN ISP – BOGOTA1

- ✓ Interfaz S0/0/1 DCE

Subred: 209.17.220.4/30

Mascara: 255.255.255.252

ISP (config)#int S0/0/1

ISP (config-if)#description ENLACE WAN ISP – BOGOTA1 SUBRED 209.17.220.4/30

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 up

ISP(config-if)#

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

ISP (config-if)#

Configuración guardada en la NVRAM

ISP (config-if)#end

ISP #

%SYS-5-CONFIG_I: Configured from console by console

ISP #copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

ISP #

ACTIVACIONES AUTOMATICAS

MEDELLIN

- ✓ Interfaz S0/0/0 DCE de MEDELLIN1 después de activar la interfaz S0/0/0 en MEDELLIN3.

MEDELLIN1#

%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

MEDELLIN1#

- ✓ Interfaz S0/0/1 de MEDELLIN1 después de activar la interfaz S0/0/1 DCE en MEDELLIN2.

MEDELLIN1#

%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

MEDELLIN1#

- ✓ Interfaz S0/1/1 de MEDELLIN1 después de activar la interfaz S0/0/1 DCE en MEDELLIN3.

MEDELLIN1#

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

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

MEDELLIN1#

- ✓ Interfaz S0/0/0 de MEDELLIN2 después de activar la interfaz S0/1/0 DCE en MEDELLIN3.

MEDELLIN2#

%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

MEDELLIN2#

- ✓ Interfaz S0/1/0 de MEDELLIN1 después de activar la interfaz S0/0/0 DCE en ISP.

MEDELLIN1#

%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

MEDELLIN1#

BOGOTA

- ✓ Interfaz S0/0/1 de BOGOTA1 después de activar la interfaz S0/0/1 DCE en BOGOTA2.

BOGOTA1#

%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

BOGOTA1#

- ✓ Interfaz S0/1/0 DCE de BOGOTA1 después de activar la interfaz S0/1/0 en BOGOTA3.

BOGOTA1#

%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

BOGOTA1#

- ✓ Interfaz S0/1/1 de BOGOTA1 después de activar la interfaz S0/1/1 DCE en BOGOTA3.

BOGOTA1#

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

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

BOGOTA1#

- ✓ Interfaz S0/0/0 de BOGOTA2 después de activar la interfaz S0/0/0 DCE en BOGOTA3.

BOGOTA2#

%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#

- ✓ Interfaz S0/0/0 de BOGOTA1 después de activar la interfaz S0/0/1 DCE en ISP.

BOGOTA1#

%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

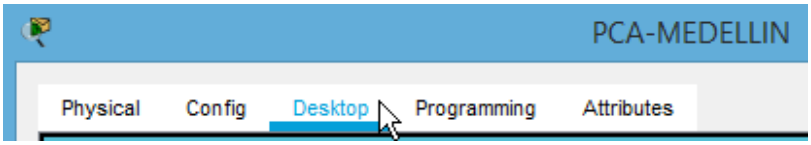
BOGOTA1#

- **PC**

PCA-MEDELLIN

- ✓ Se hace clic sobre la PC y a continuación, se hace clic sobre la pestaña **Desktop.**

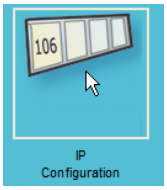
Figura 24 Pestaña Desktop PCA-MEDELLIN Configuración



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se hace clic en el botón **IP Configuration.**

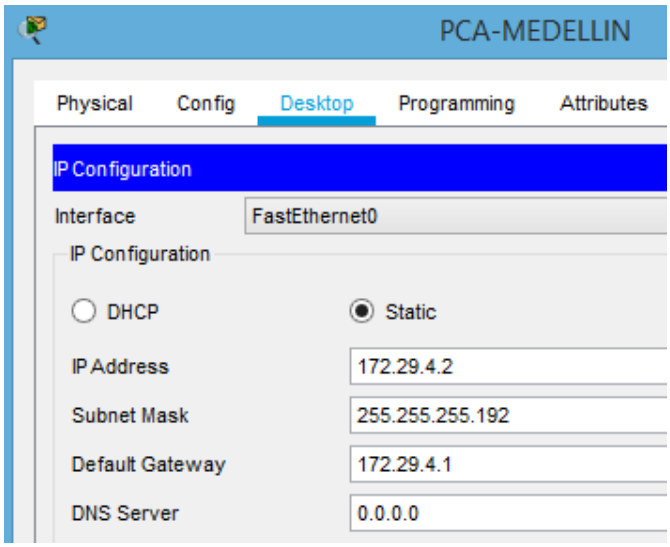
Figura 25 Botón IP Configuration PCA-MEDELLIN



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se ubica en el apatado **IP Configuration** y a continuación, se llenana los campos con los datos de la tabla de direccionamiento. El servidor DNS se peude quitar o dejar el que se muestra por defecto.

Figura 26 Configuración direccionamiento PCA-MEDELLIN

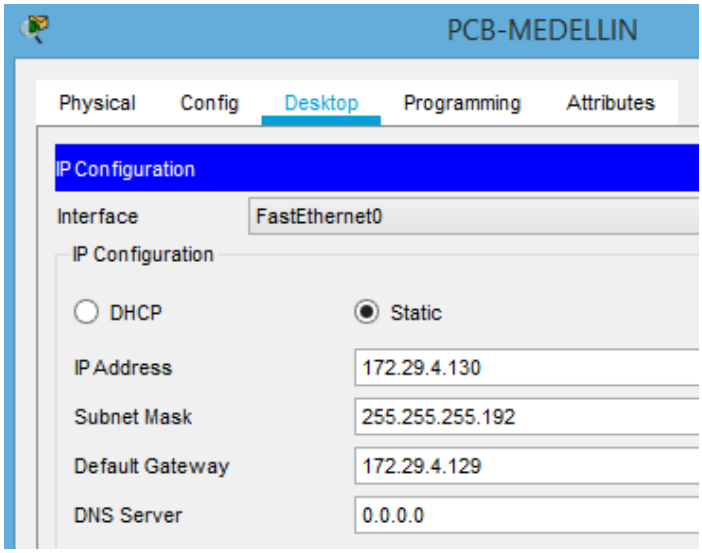


Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se repite el proedimiento para los demás dispositivos.

PCB-MEDELLIN

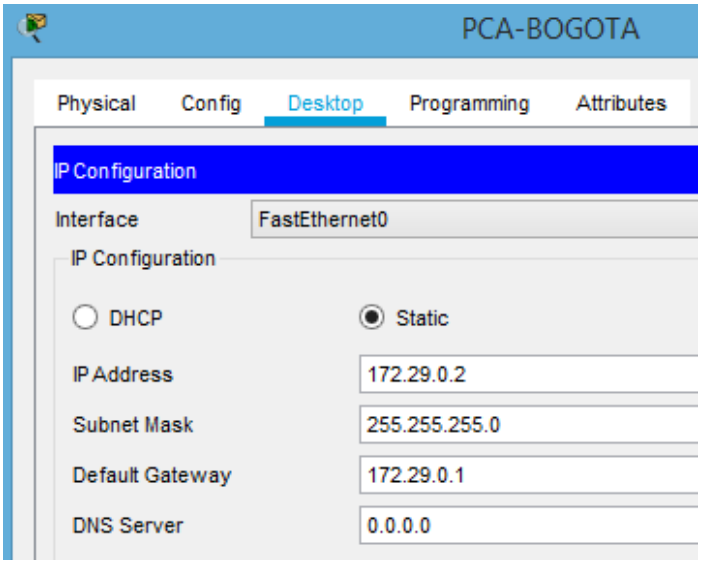
Figura 27 Configuración direccionamiento PCB-MEDELLIN



Fuente: Cisco Packet Tracer 7.0.2.0226.

PCA-BOGOTA

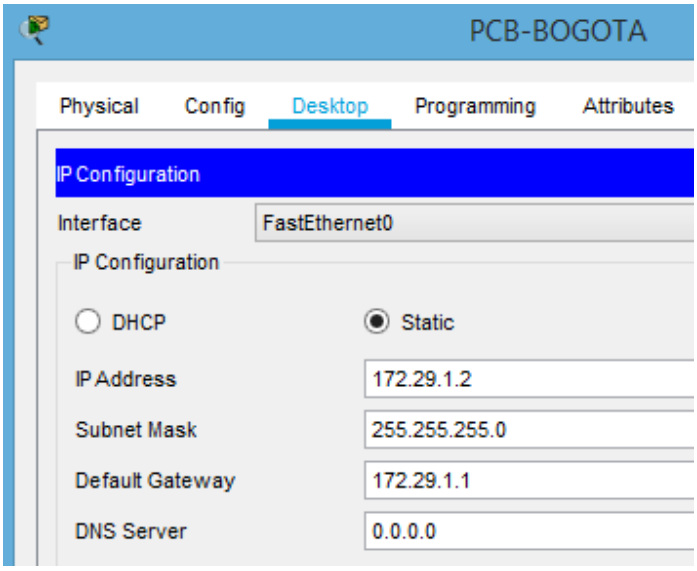
Figura 28 Configuración direccionamiento PCA-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

PCB-BOGOTA

Figura 29 Configuración direccionamiento PCB.BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

Nota: se configura el direccionamiento estático para probar conectividad, esta configuración se cambiará más adelante.

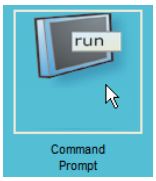
- **Verificación Conectividad antes de configuración de protocolo RIPv2.**

Cada PC debe poder hacer ping al host al que se encuentra conectado y los routers deben poder hacer ping entre si.

PING DESDE PC

- ✓ Se hace clic sobre el PC y a continuación, se hace clic sobre sobre la pestaña **Desktop.**
- ✓ Se hace clic en el botón **Command Prompt** (Consola de Comandos)**.**

Figura 30 Conectividad antes de RIPv2. Command Prompt PCA-MEDELLIN



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ En la consola de comando se escribe el comando **ping** *IP-Destino*

PING DESDE ROUTER

- ✓ Se hace clic sobre el router y a continuación, se hace clic sobre sobre la pestaña **CLI**

Figura 31 Conectividad antes de RIPv2. Pestaña CLI MEDELLIN2

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se ingresan las credenciales de usuario y se accede al modo consola o modo EXEC privilegiado. Al digitar la contraseña esta no se visualiza.

Figura 32 Vista CLI MEDELLIN2

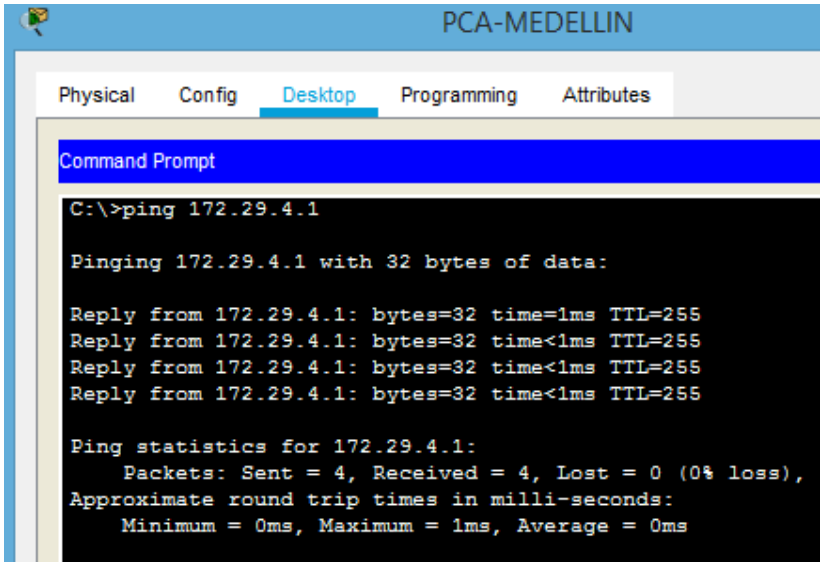
```
El acceso no autorizado esta estrictamente prohibido !

User Access Verification

Password:

MEDELLIN2>
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

MEDELLIN

- ✓ Ping PCA-MEDELLIN a MEDELLIN2.

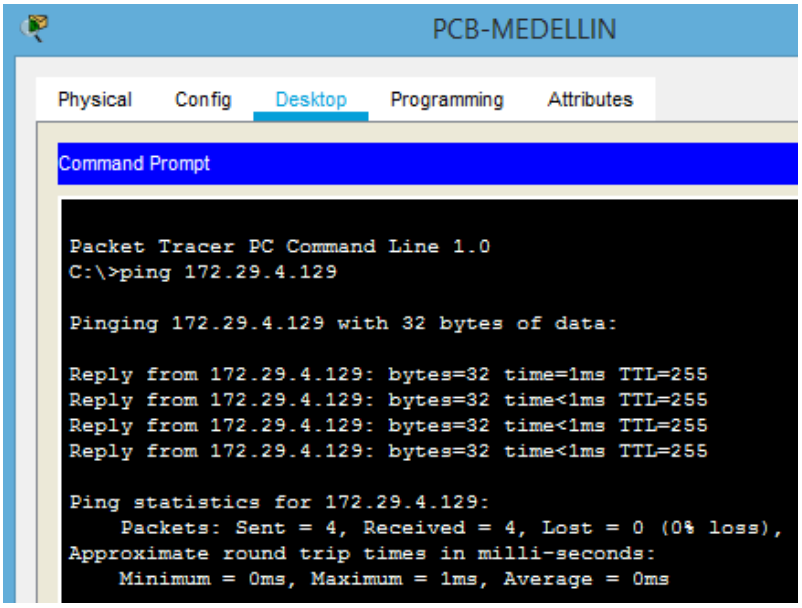
Figura 33 Conectividad antes de RIPv2. Ping PCA-MEDELLIN a MEDELLIN2



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping PCB-MEDELLIN a MEDELLIN3.

Figura 34 Conectividad antes de RIPv2. Ping PCB-MEDELLIN a MEDELLIN3



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN2 a PCA-MEDELLIN.

Figura 35 Conectividad antes de RIPv2. Ping MEDELLIN2 a PCA-MEDELLIN

```
MEDELLIN2>ping 172.29.4.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.4.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN3 a PCB-MEDELLIN.

Figura 36 Conectividad antes de RIPv2. Ping MEDELLIN3 a PCB-MEDELLIN

```
MEDELLIN3>ping 172.29.4.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.4.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN1 a MEDELLIN2.

Figura 37 Conectividad antes de RIPv2. Ping MEDELLIN1 a MEDELLIN2

```
MEDELLIN1>ping 172.29.6.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN2 a MEDELLIN1.

Figura 38 Conectividad antes de RIPv2. Ping MEDELLIN2 a MEDELLIN1

```
MEDELLIN2>ping 172.29.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN1 a MEDELLIN3.

Figura 39 Conectividad antes de RIPv2. Ping MEDELLIN1 a MEDELLIN3

```
MEDELLIN1>ping 172.29.6.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/10 ms


MEDELLIN1>ping 172.29.6.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/11 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN3 a MEDELLIN1.

Figura 40 Conectividad antes de RIPv2. Ping MEDELLIN3 a MEDELLIN1

```
MEDELLIN3>ping 172.29.6.13

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms


MEDELLIN3>ping 172.29.6.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/19 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN2 a MEDELLIN3.

Figura 41 Conectividad antes de RIPv2. Ping MEDELLIN2 a MEDELLIN3

```
MEDELLIN2>ping 172.29.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN3 a MEDELLIN2.

Figura 42 Conectividad antes de RIPv2. Ping MEDELLIN3 a MEDELLIN2

```
MEDELLIN3>ping 172.29.6.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN1 a ISP.

Figura 43 Conectividad antes de RIPv2. Ping MEDELLIN1 a ISP

```
MEDELLIN1>ping 209.17.220.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/11 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping ISP a MEDELLIN1.

Figura 44 Conectividad antes de RIPv2. Ping ISP a MEDELLIN1

```
ISP>ping 209.17.220.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/18 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA

- ✓ Ping BOGOTA3 a PCA-BOGOTA.

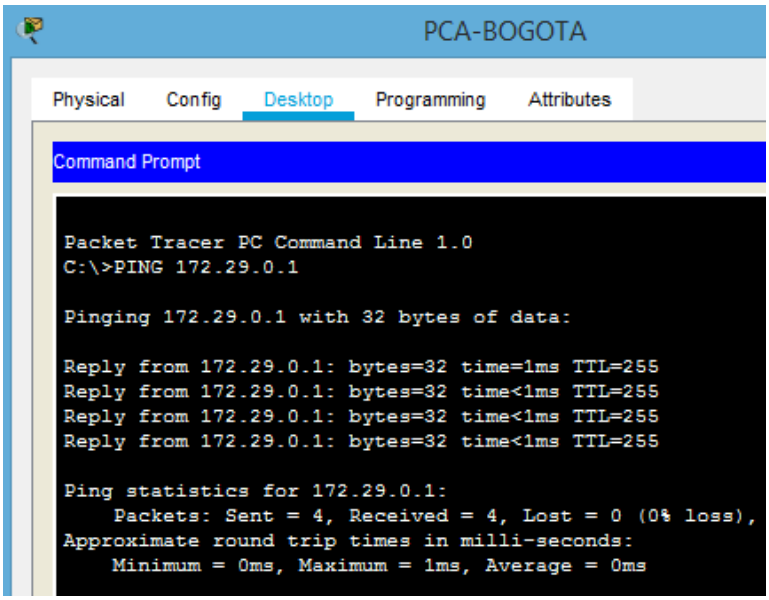
Figura 45 Conectividad antes de RIPv2. Ping BOGOTA3 a PCA-BOGOTA

```
BOGOTA3>ping 172.29.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping PCA-BOGOTA a BOGOTA3.

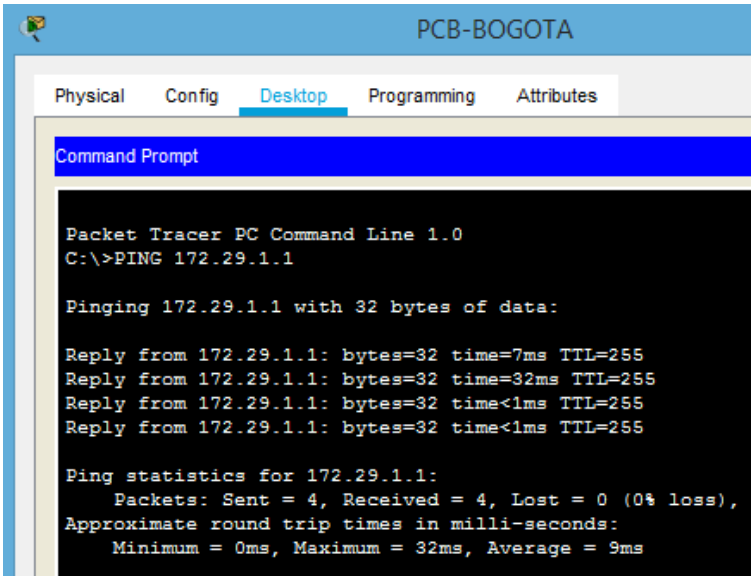
Figura 46 Conectividad antes de RIPv2. Ping PCA-BOGOTA a BOGOTA3



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping PCB-BOGOTA a BOGOTA2.

Figura 47 Conectividad antes de RIPv2. Ping PCB-BOGOTA a BOGOTA2



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA2 a PCB-BOGOTA.

Figura 48 Conectividad antes de RIPv2. Ping BOGOTA2 a PCB-BOGOTA

```
BOGOTA2>PING 172.29.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA1 a BOGOTA2.

Figura 49 Conectividad antes de RIPv2. Ping BOGOTA1 a BOGOTA2

```
BOGOTA1>ping 172.29.3.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA2 a BOGOTA1.

Figura 50 Conectividad antes de RIPv2. Ping BOGOTA2 a BOGOTA1

```
BOGOTA2>ping 172.29.3.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA1 a BOGOTA3.

Figura 51 Conectividad antes de RIPv2. Ping BOGOTA1 a BOGOTA3

```
BOGOTA1>ping 172.29.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/21 ms


BOGOTA1>ping 172.29.3.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/27 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA3 a BOGOTA1.

Figura 52 Conectividad antes de RIPv2. Ping BOGOTA3 a BOGOTA1

```
BOGOTA3>ping 172.29.3.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/14 ms


BOGOTA3>ping 172.29.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/31 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA2 a BOGOTA3.

Figura 53 Conectividad antes de RIPv2. Ping BOGOTA2 a BOGOTA3

```
BOGOTA2>ping 172.29.3.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/21 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA3 a BOGOTA2.

Figura 54 Conectividad antes de RIPv2. Ping BOGOTA3 a BOGOTA2

```
BOGOTA3>ping 172.29.3.13

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/30 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA1 a ISP.

Figura 55 Conectividad antes de RIPv2. Ping BOGOTA1 a ISP

```
BOGOTA1>ping 209.17.220.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/27 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping ISP a BOGOTA.

Figura 56 Conectividad antes de RIPv2. Ping ISP a BOGOTA

```
ISP>ping 209.17.220.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/16 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Configuracion Protocolo RIPv2

- ✓ Se ingresa al modo de configuración global con el comando de modo EXEC privilegiado **configure terminal** o abreviado **config t.**
- ✓ Se define RIP como protocolo con el comando **router rip.** La petición de entrada cambia y ahora se encuentra en el modo de configuración de router.
- ✓ Se define la versión de RIP con el comando **versión** *numero.*
- ✓ Se establecen las interfaces pasivas con el comando **passive-interface** *ID-Interfaz***.**

Este comando evita que las actualizaciones de routing se envíen a través de la interfaz especificada. Este proceso evita tráfico de routing innecesario en la LAN. Sin embargo, la red a la que pertenece la interfaz especificada aún se anuncia en las actualizaciones de routing enviadas por otras interfaces.

- ✓ Se declara la red principal con el comando **network** *red.*
- ✓ Se deshabilita la sumarización automática con el comando **no auto-summary.**

La sumarización automática resume las rutas en los límites de las redes principales con clase. Al desactivarla ya no se resumirán.

Para los routers de la red de medellin la red principal se peude definir de dos formas: cada una de las redes que se muestran al emitir el comando del modo de configuración de router **do show ip route connected** o la subred sumarizada. Cualquiera de las dos opciones es valida en la configuración.

La red del **ISP** no se declara como principal en los routers porque se supone que este es un destino que se encuentra muy lejos y su enrutamiento no se configura con RIP sino con rutas estáticas.

MEDELLIN1

MEDELLIN1# config t

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

MEDELLIN1 (config)# router rip

MEDELLIN1 (config-router)# version 2

MEDELLIN1 (config-router)# network 172.29.0.0

MEDELLIN1 (config-router)# no auto-summary

MEDELLIN2

MEDELLIN2# config t

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

MEDELLIN2 (config)# router rip

MEDELLIN2 (config-router)# version 2

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

MEDELLIN2 (config-router)# network 172.29.0.0

MEDELLIN2 (config-router)# no auto-summary

MEDELLIN3

MEDELLIN3# config t

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

MEDELLIN3 (config)# router rip

MEDELLIN3 (config-router)# version 2

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

MEDELLIN3 (config-router)# network 172.29.0.0

MEDELLIN3 (config-router)# no auto-summary

BOGOTA1

BOGOTA1# config t

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

BOGOTA1 (config)# router rip

BOGOTA1 (config-router)# version 2

BOGOTA1 (config-router)# network 172.29.0.0

BOGOTA1 (config-router)# no auto-summary

BOGOTA2

BOGOTA2# config t

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

BOGOTA2 (config)# router rip

BOGOTA2 (config-router)# version 2

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

BOGOTA2 (config-router)# network 172.29.0.0

BOGOTA2 (config-router)# no auto-summary

BOGOTA3

BOGOTA3# config t

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

BOGOTA3 (config)# router rip

BOGOTA3 (config-router)# version 2

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

BOGOTA3 (config-router)# network 172.29.0.0

BOGOTA3 (config-router)# no auto-summary

Verificacion del estado de la red

En cada router se utiliza el comando de modo EXEC privilegiado **show ip interface brief** para verificar la configuración y estado de las interfaces. Tanto el protocolo como el estado deben estar en **up** en todas las interfaces configuradas.

- ✓ MEDELLIN1

Figura 57 Verificación de interfaces MEDELLIN1

```
MEDELLIN1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            172.29.6.13     YES manual up                    up
Serial0/0/1            172.29.6.1      YES manual up                    up
Serial0/1/0            209.17.220.2    YES manual up                    up
Serial0/1/1            172.29.6.9      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ MEDELLIN2

Figura 58 Verificación de interfaces MEDELLIN2

```
MEDELLIN2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     172.29.4.1      YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            172.29.6.5      YES manual up                    up
Serial0/0/1            172.29.6.2      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ MEDELLIN3

Figura 59 Verificación de interfaces MEDELLIN3

```
MEDELLIN3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     172.29.4.129    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            172.29.6.14     YES manual up                    up
Serial0/0/1            172.29.6.10     YES manual up                    up
Serial0/1/0            172.29.6.6      YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ BOGOTA1

Figura 60 Verificación de interfaces BOGOTA1

```
BOGOTA1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            209.17.220.6    YES manual up                    up
Serial0/0/1            172.29.3.9      YES manual up                    up
Serial0/1/0            172.29.3.1      YES manual up                    up
Serial0/1/1            172.29.3.5      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ BOGOTA2

Figura 61 Verificación de interfaces BOGOTA2

```
BOGOTA2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     172.29.1.1      YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            172.29.3.13     YES manual up                    up
Serial0/0/1            172.29.3.10     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ BOGOTA3

Figura 62 Verificación de interfaces BOGOTA3

```
BOGOTA3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     172.29.0.1      YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            172.29.3.14     YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Serial0/1/0            172.29.3.2      YES manual up                    up
Serial0/1/1            172.29.3.6      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ ISP

Figura 63 Verificación de interfaces ISP

```
ISP>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            209.17.220.1    YES manual up                    up
Serial0/0/1            209.17.220.5    YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

a. 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 RIP.

Configuración de rutas por defecto hacia ISP

Desde MEDELLIN1 y BOGOTA1 se crean rutas estáticas a la red 0.0.0.0 0.0.0.0, con el comando de configuacion global **ip route**. Esto envía todo tráfico de dirección de destino desconocida a las interfaces **S0/0/0 DCE** y **S0/0/1 DCE** hacia la ISP y simula Internet al establecer un gateway de último recurso en MEDELLIN1 Y BOGOTA1.

MEDELLIN1

MEDELLIN1#config t

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

MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

MEDELLIN1(config)#

BOGOTA1

BOGOTA1#config t

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

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5

BOGOTA1(config)#

Configuración redistribución de rutas dentro de las publicaciones de RIP

Para que MEDELLIN1 Y BOGOTA1 redistribuyan una ruta hacia otros routers se agrega el comando **default-information originate** a la configuración de RIP.

MEDELLIN1

MEDELLIN1(config)#router rip

MEDELLIN1(config-router)#default-information originate

MEDELLIN1(config-router)#

BOGOTA1

BOGOTA1(config)#router rip

BOGOTA1(config-router)#default-information originate

BOGOTA1(config-router)#

b. 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.

Redes Internas

MEDELLIN

- ✓ MEDELLIN1 y MEDELLIN2.

Red Interna 1: 172.29.6.0/30.

- ✓ MEDELLIN2 y MEDELLIN3.

Red Interna 2: 172.29.6.4/30.

- ✓ MEDELLIN1 y MEDELLIN3.

Rede Interna 3: 172.29.6.8/30.

Rede Interna 4: 172.29.6.12/30.

- ✓ MEDELLIN2 y LAN PCA.MEDELLIN.

Rede Interna 5: 172.29.4.0/26.

- ✓ MEDELLIN3 y LAN PCB-MEDELLIN.

Rede Interna 6: 172.29.4.128/26.

Para sumarizar las redes se convierten a su equivalente en binario y se examinan las coincidencias

Tabla 17 Configuración ISP. Redes Internas MEDELLIN1

Red Interna 1	10101100	.	00011101	.	00000110	.	00000000
Red Interna 2	10101100	.	00011101	.	00000110	.	00000100
Red Interna 3	10101100	.	00011101	.	00000110	.	00001000
Red Interna 4	10101100	.	00011101	.	00000110	.	00001100
Red Interna 5	10101100	.	00011101	.	00000100	.	00001100
Red Interna 6	10101100	.	00011101	.	00000100	.	00001100
Se coloca un cero en todos los bits que no coinciden.							
Red Sumarizada	10101100	.	00011101	.	00000100	.	00000000

Fuente: Autoría Propia.

Se convierte a su equivalente en decimal.

Red Interna Sumarizada: 172.29.4.0/22.

BOGOTA

- ✓ BOGOTA1 y BOGOTA2.

Red Interna 1: 172.29.3.8/30.

- ✓ BOGOTA2 y BOGOTA3.

Red Interna 2: 172.29.3.12/30.

- ✓ BOGOTA1 y BOGOTA3.

Rede Interna 3: 172.29.3.0/30.

Red Interna 4: 172.29.3.4/30.

- ✓ BOGOTA2 y LAN PCB-BOGOTA.

Rede Interna 5: 172.29.1.0/24.

- ✓ BOGOTA3 y LAN PCA-BOGOTA.

Rede Interna 6: 172.29.0.0/24.

Para sumarizar las redes se convierten a su equivalente en binario y se examinan las coincidencias.

Tabla 18 Configuración ISP. Redes Internas BOGOTA1

Red Interna 1	10101100	.	00011101	.	00000011	.	00001000
Red Interna 2	10101100	.	00011101	.	00000011	.	00001100
Red Interna 3	10101100	.	00011101	.	00000011	.	00000000
Red Interna 4	10101100	.	00011101	.	00000011	.	00000100
Red Interna 5	10101100	.	00011101	.	00000001		00000000
Red Interna 6	10101100	.	00011101	.	00000000		00000000
Se coloca un cero en todos los bits que no coinciden.							
Red Sumarizada	10101100	.	00011101	.	00000000	.	00000000

Fuente: Autoría Propia.

Se convierte a su equivalente en decimal.

Red Interna Sumarizada: 172.29.0.0/22.

Configuracion rutas estáticas

Se crean las rutas estaticas hacia las redes internas de MEDELLIN y BOGOTA en el **ISP** con el comando de configuración global **ip route** *Direccion-IP Mascara Direccion-Siguiente-Salto***. La dirección de siguiente salto será la interfaz serial de cada router que conecta con el ISP.**

- ✓ Ruta estatica hacia MEDELLIN.

ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2

ISP(config)#

- ✓ Ruta estatica hacia BOGOTA.

ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

ISP(config)#

1.1.2. Parte 2: Tabla de Enrutamiento

a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

La tabla de routing o enrutamiento almacena las diferentes rutas hacia diferentes destinos que provienen de de las interfaces activas del router o algún protocolo de enrutamiento.

Es un archivo de datos que se encuentra en la RAM.

Contiene asociaciones de red o de siguiente salto. Estas asociaciones le indican al router que un destino en particular se puede alcanzar de forma óptima si se envía el paquete hacia un router en particular que representa el siguiente satto en el camino hacia el destino final.

Origenes de la tabla de routing

Se utiliza el comando de configuración global **show ip route** para visualizar la tabla de routing IPv4 de un router**.**

Las entradas se pueden agregar como:

- Interfaces de ruta local: se agregan cuando la interfaz está configurada y activa.
- Interfaces conectadas directamente: se agregan a la tabla de routing cuando la interfaz esta configurada y activa.
- Rutas Estáticas: se agregan cuando una ruta se configura manualmente y la interfaz de salida esta activa.
- Protocolo de Routing Dinámico: se agrega cuando se implementan protocolos de descubrimiento de red de manera dinámica y cuando se identifican las redes.

Códigos que identifican los orígenes de las rutas:

- L: identifica la dirección asignada a la interfaz del router. Asi, el router determina si recibe el paquete para la interfaz o para reenviar.
- C: identifica una red conectada directamente.
- S: identifica una red estática creada para llegar a una red específica.
- D: identifica una red que se descubre de forma dinámica de otro router con EIGRP.
- O: indica una red que se descubre de foma dinámica de otro router con OSPF.
- R: indica una red que se descubre de foma dinámica de otro router con RIP.

Ejemplo de entrada de tabla de routing IPv4:

Tabla 19 Ejemplo entrada en tabla de ruta de routing. Red Remota.

1	2	3	4		5	6	7
R	172.16.4.0/28	[120,	2]	via	209.165.220.226	00:00:12	Serial0/0/0

Convenciones

1	Origen de la ruta.
2	Red de destino o dirección de la red remota.
3	Distancia Administrativa.
4	Metrica.
5	Direccion de siguiente salto a donde se debe reenviar el paquete.
6	Marca de hora de la ruta. Indica la ultima comunicación con la ruta.
7	Interfaz de Salida que se utiliza para reenviar el paquete.

Fuente: Tabla de Routing

b. Verificar el balanceo de carga que presentan los routers.

Cuando un router tiende dos o mas rutas hacia un destino con métrica de mismo costo, el router reenvía los paquetes usando ambas rutas por igual. La tabla de routing contiene la única red de destino, pero tiene varias interfaces de salida, una para cada ruta del mismo costo.

El balanceo de carga es la capacidad de un router para transmitir paquetes a una dirección IP de destino a través de más de una ruta. Si el balance esta bien configurado, puede aumentar la efectividad y rendimiento de la red. Se puede configurar para usar protocolos de enrutamiento dinámico como rutas estáticas.

Solo EIGRP (Protocolo de Enrutamiento de Puerta de Enlace Interior Mejorado) admite balanceo de carga con diferente costo.

Distancia Administrativa

Un router se puede configurar con varios protocolos de routing y rutas estáticas. De ser asi, la tabla de routing tiene más de un origen de ruta para la misma red de desino. Cada protocolo decide de manera diferente la ruta. El router determina la ruta que debe utilizar e instalar en la tabla de routing mediante la distancia administrativa.

La distancia adminsitrativa (AD) representa la confiabilidad del origen de la ruta.

Cuanto menor sea la AD, mas confiable será el origen de la ruta.

Tabla 20 Distancias Administrativas de los protocolos

Fuente de la Ruta	Valores Predeterminados AD
Interfaz conectada directamente	0
Ruta estática	1
Ruta de resumen del Enhanced Interior Gateway Routing Protocol (EIGRP).	5
External Border Gateway Protocol (BGP)	20
EIGRP Interno	90
IGRP	100

OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
Ruteo a pedido (ODR)	160
EIGRP externo	170
BGP interno	200
Unknown*	255

Fuente: Distancia Administrativa

Metrica

Identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas. La métrica para rutas estáticas y conectadas directamente es de 0.

Revision tabla de routing

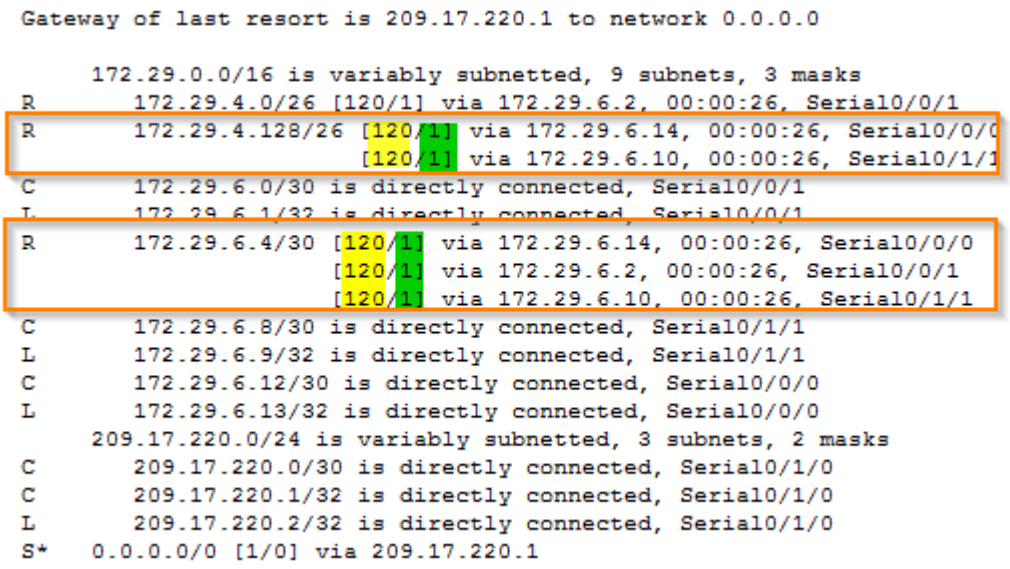
Tabla 21 Convenciones para la verificación de balanceo de carga

	Distancia Administrativa
	Metrica
	BALANCEO DE CARGA

Fuente: Autoría Propia.

MEDELLIN1

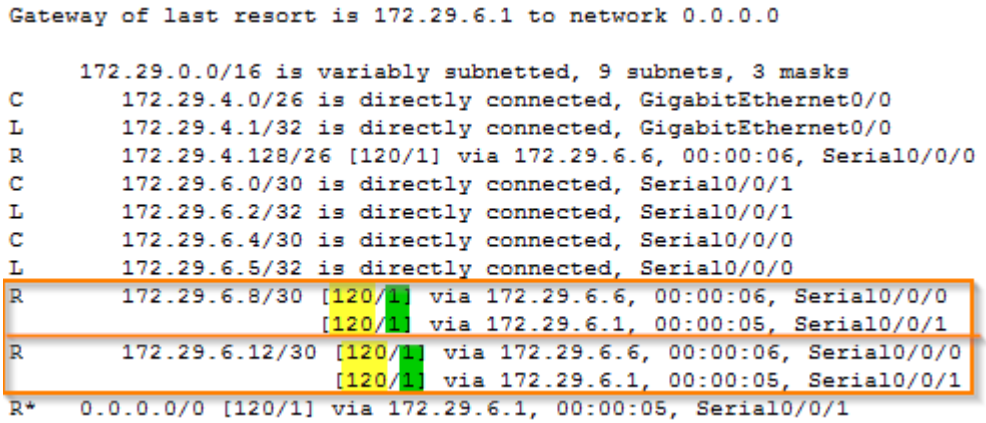
Figura 64 Balanceo de carga MEDELLIN1



Fuente: Cisco Packet Tracer 7.0.2.0226.

MEDELLIN2

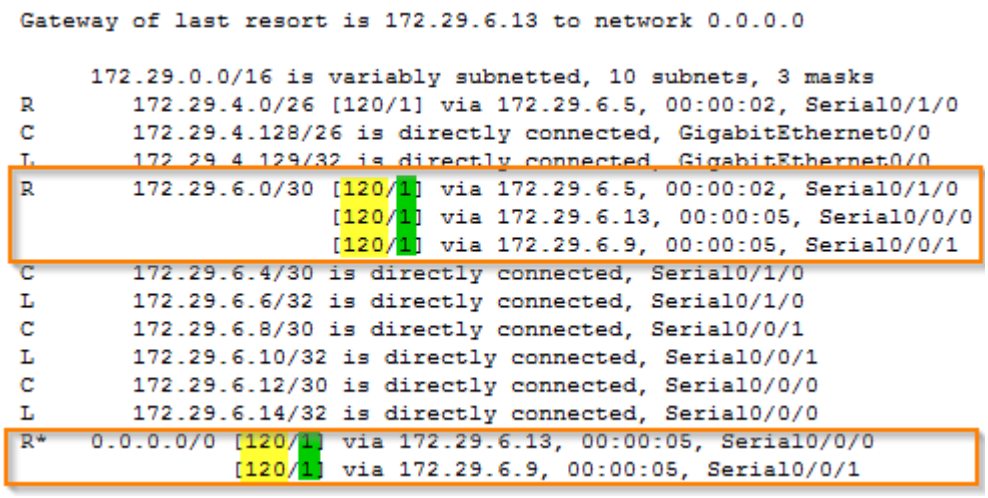
Figura 65 Balanceo de carga MEDELLIN2



Fuente: Cisco Packet Tracer 7.0.2.0226.

MEDELLIN3

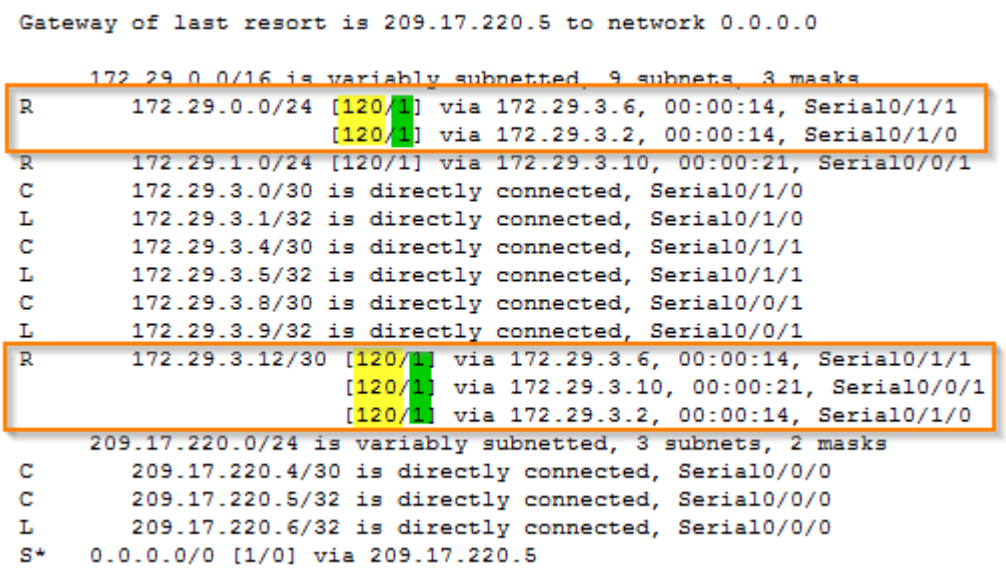
Figura 66 Balanceo de carga MEDELLIN3



Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA1

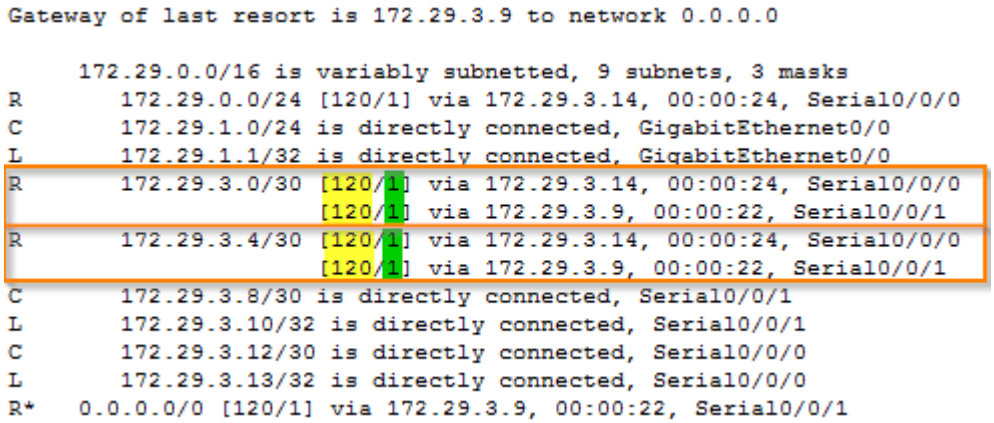
Figura 67 Balanceo de carga BOGOTA1



Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA2

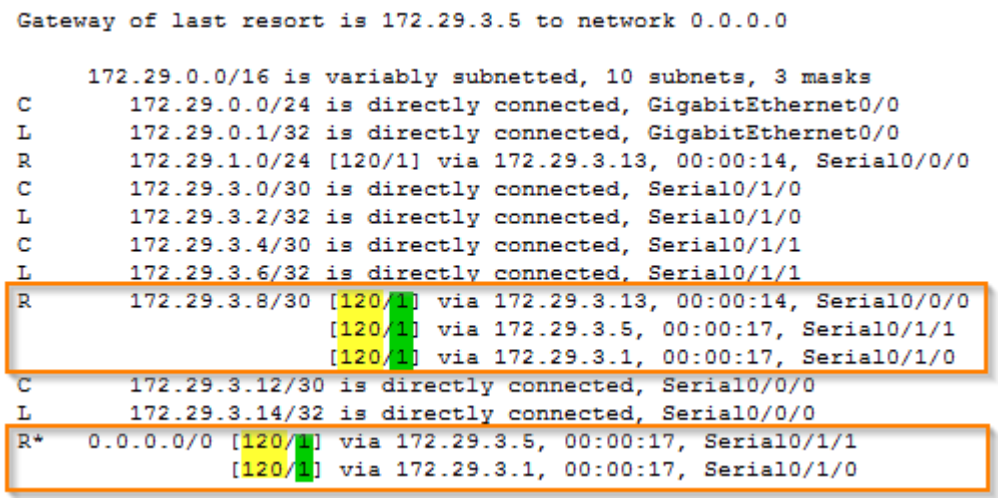
Figura 68 Balanceo de carga BOGOTA2



Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA3

Figura 69 Balanceo de carga BOGOTA3



Fuente: Cisco Packet Tracer 7.0.2.0226.

ISP

Figura 70 Balanceo de carga ISP

```
Gateway of last resort is not set

     172.29.0.0/22 is subnetted, 2 subnets
S       172.29.0.0/22 [1/0] via 209.17.220.6
S       172.29.4.0/22 [1/0] via 209.17.220.2
     209.17.220.0/24 is variably subnetted, 6 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
L       209.17.220.1/32 is directly connected, Serial0/0/0
C       209.17.220.2/32 is directly connected, Serial0/0/0
C       209.17.220.4/30 is directly connected, Serial0/0/1
L       209.17.220.5/32 is directly connected, Serial0/0/1
C       209.17.220.6/32 is directly connected, Serial0/0/1
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

El ISP no cuenta con balanceo de carga.

c. 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.

Ambos son routers fronterizos porque se encuentran al limite de cada red antes de la conexión con el ISP.

BOGOTA1

Figura 71 Enlaces y Ruta Predeterminada BOGOTA1

```
Gateway of last resort is 209.17.220.5 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.0.0/24 [120/1] via 172.29.3.6, 00:00:14, Serial0/1/1
                      [120/1] via 172.29.3.2, 00:00:14, Serial0/1/0
R       172.29.1.0/24 [120/1] via 172.29.3.10, 00:00:21, Serial0/0/1
C       172.29.3.0/30 is directly connected, Serial0/1/0
L       172.29.3.1/32 is directly connected, Serial0/1/0
C       172.29.3.4/30 is directly connected, Serial0/1/1
L       172.29.3.5/32 is directly connected, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/0/1
L       172.29.3.9/32 is directly connected, Serial0/0/1
R       172.29.3.12/30 [120/1] via 172.29.3.6, 00:00:14, Serial0/1/1
                       [120/1] via 172.29.3.10, 00:00:21, Serial0/0/1
                       [120/1] via 172.29.3.2, 00:00:14, Serial0/1/0
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.4/30 is directly connected, Serial0/0/0
C       209.17.220.5/32 is directly connected, Serial0/0/0
L       209.17.220.6/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.5
```

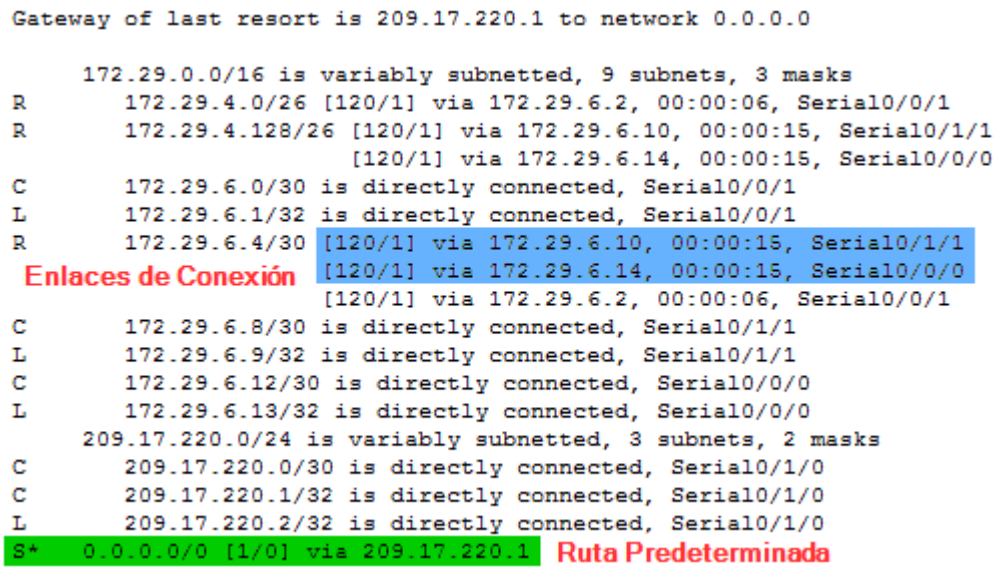
Enlaces de Conexion

Ruta Predeterminada

Fuente: Cisco Packet Tracer 7.0.2.0226.

MEDELLIN1

Figura 72 Enlaces y Ruta Predeterminada MEDELLIN1

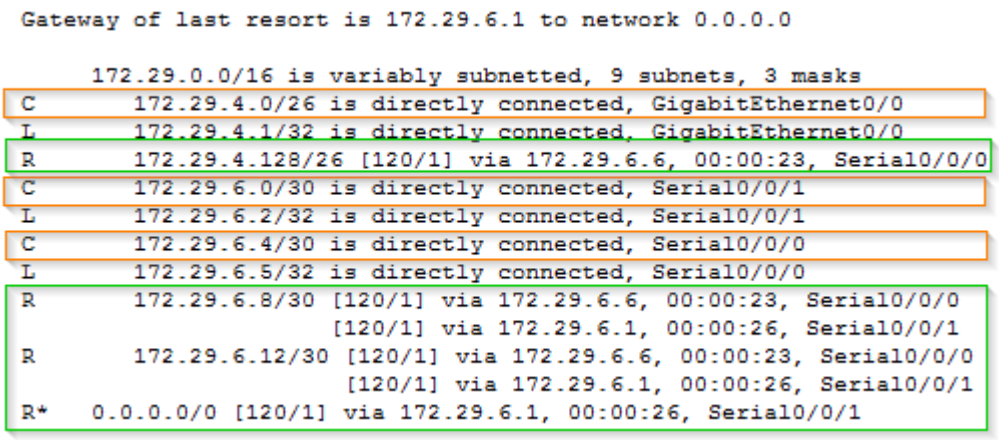


Fuente: Cisco Packet Tracer 7.0.2.0226.

d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente (**C**) y recibidas mediante RIP (**R**).

MEDELLIN2

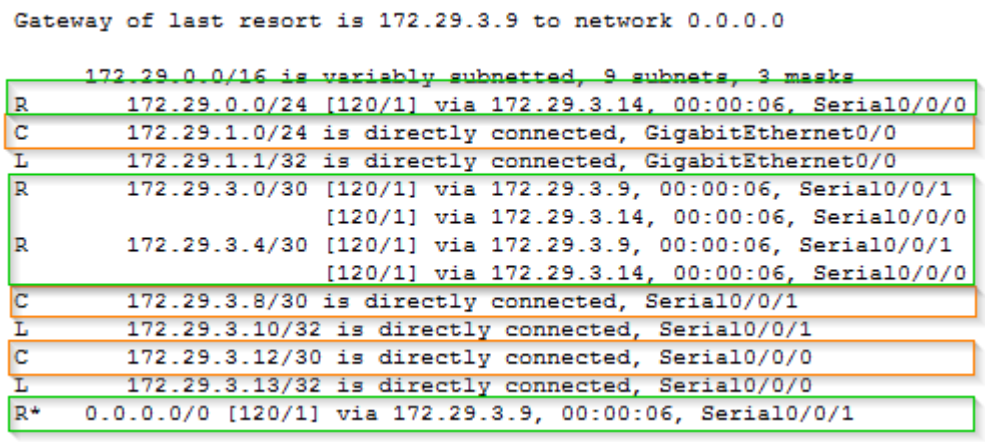
Figura 73 Redes C y R MEDELLIN2



Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA2

Figura 74 Redes C y R BOGOTA2

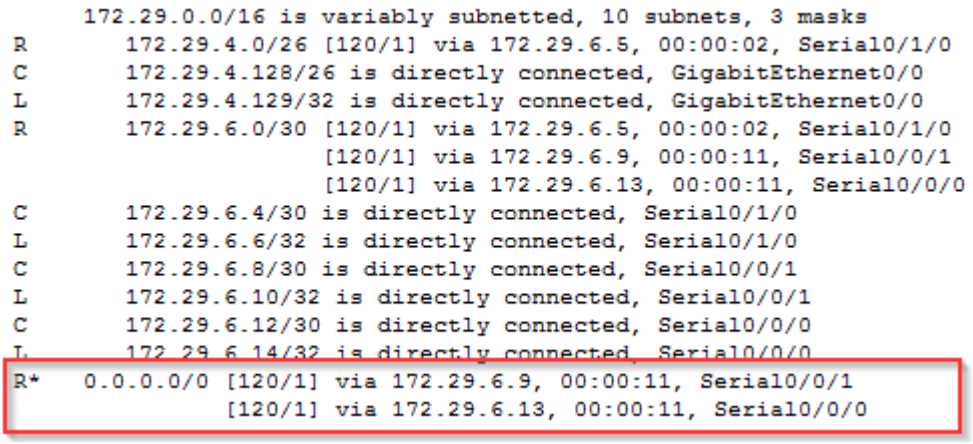


Fuente: Cisco Packet Tracer 7.0.2.0226.

e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto (**R***).

MEDELLIN3

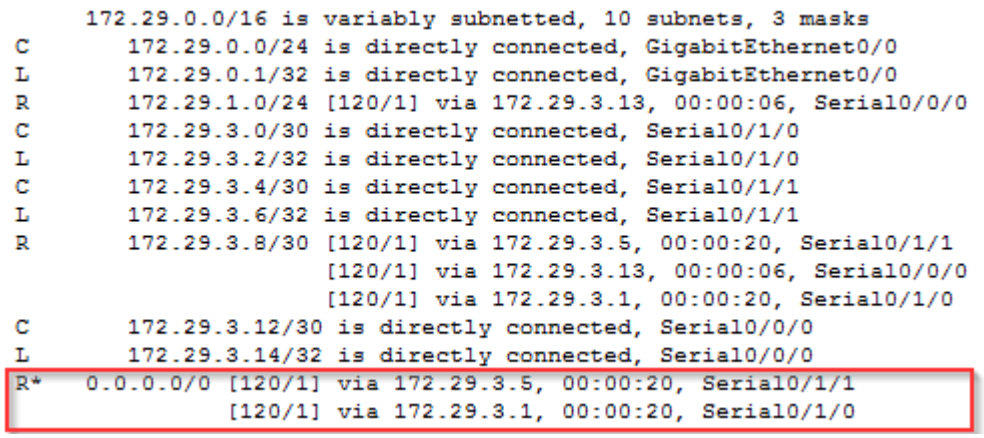
Figura 75 Rutas redundantes MEDELLIN3



Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA3

Figura 76 Rutas redundantes BOGOTA3

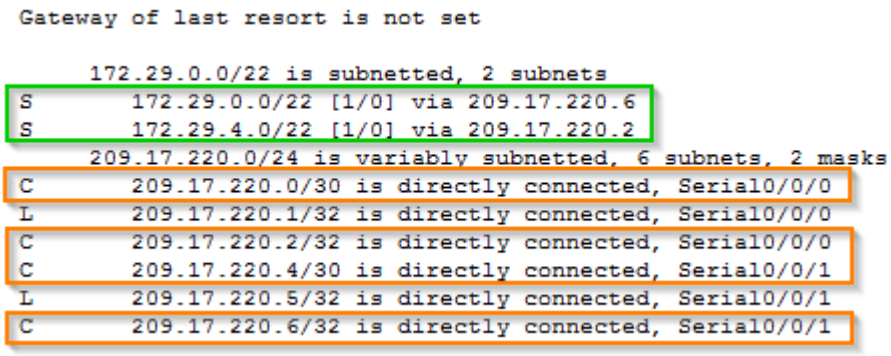


Fuente: Cisco Packet Tracer 7.0.2.0226.

f. El router ISP solo debe indicar sus rutas estáticas adicionales (**S**) a las directamente conectadas (**C**).

ISP

Figura 77 Rutas Estáticas y Directamente conectadas ISP



Fuente: Cisco Packet Tracer 7.0.2.0226.

1.1.3. Parte 3: Deshabilitar la propagación del protocolo RIP

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

Tabla 22 Interfaces activas para la propagación RIP

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/1/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/1/1; SERIAL0/1/0
ISP	No lo requiere

Fuente: Cisco. Evaluación – Prueba de Habildiades Prácticas CCNA.

En los router MEDELLIN2, MEDELLIN3, BOGOTA2 y BOGOTA3 se deshabilitó la propagación del proocolo RIP con el comando de configuración de router **passive-interface** *ID-Interfaz* a las interfaces GigabitEthernet0/0.

Se deshabilita la propagación de RIP en las interfaces restantes:

BOGOTA1

- ✓ Interfaces GigabitEthernet0/0 y GigabitEthernet0/1.

BOGOTA1(config)#router rip

BOGOTA1(config-router)#passive-interface g0/0

BOGOTA1(config-router)#passive-interface g0/1

BOGOTA1(config-router)#

BOGOTA2

- ✓ Interfaz GigabitEthernet0/1.

BOGOTA2(config)#router rip

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

BOGOTA2(config-router)#

BOGOTA3

- ✓ Interfaces GigabitEthernet0/1 Y Serial0/1/1.

BOGOTA3(config)#router rip

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

BOGOTA3(config-router)#passive-interface s0/1/1

MEDELLIN1

- ✓ Interfaces GigabitEthernet0/0 y GigabitEthernet0/1.

MEDELLIN1(config)#router rip

MEDELLIN1(config-router)#passive-interface g0/0

MEDELLIN1(config-router)#passive-interface g0/1

MEDELLIN1(config-router)#

MEDELLIN2

- ✓ Interfaz GigabitEthernet0/1.

MEDELLIN2(config)#router rip

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

MEDELLIN2(config-router)#

MEDELLIN3

- ✓ Interfaces GigabitEthernet0/1 y Serial0/1/0.

MEDELLIN3(config)#router rip

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

MEDELLIN3(config-router)#passive-interface s0/1/1

1.1.4. Parte 4: Verificación del protocolo RIP

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

Para verificar el protocolo en los routers se puede utilizar el comando de configuración global **show ip protocols.**

Convenciones

Tabla 23 Convenciones de la verificación de opciones de enrutamiento

	Protocolo de enrutamiento y versión.
	Interfaces que participan en la publicación de otros datos.
	Interfaces pasivas.

Fuente: Autoría Propia.

MEDELLIN1

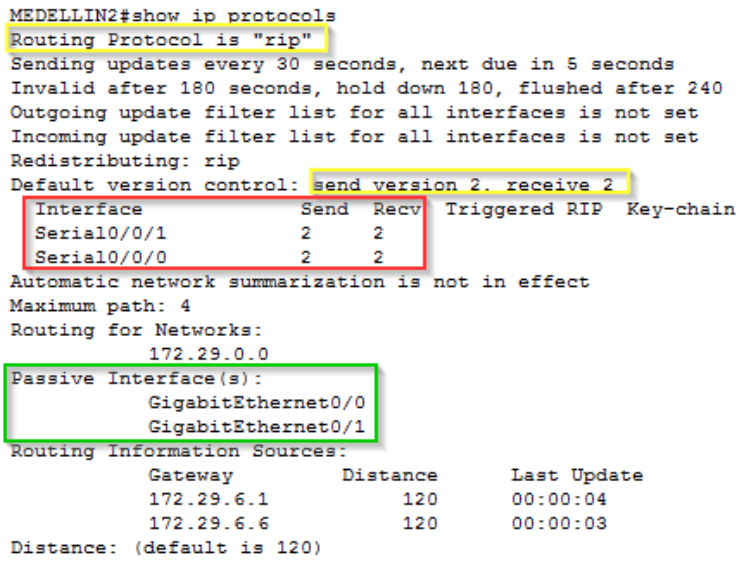
Figura 78 Verificación Protocolo RIP MEDELLIN1

```
MEDELLIN1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 11 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0            2     2
  Serial0/0/1            2     2
  Serial0/1/1            2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
            172.29.0.0
Passive Interface(s):
            GigabitEthernet0/0
            GigabitEthernet0/1
            Serial0/1/0
Routing Information Sources:
            Gateway         Distance      Last Update
            172.29.6.2           120      00:00:16
            172.29.6.14          120      00:00:17
            172.29.6.10          120      00:00:17
Distance: (default is 120)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

MEDELLIN2

Figura 79 Verificación Protocolo RIP MEDELLIN2

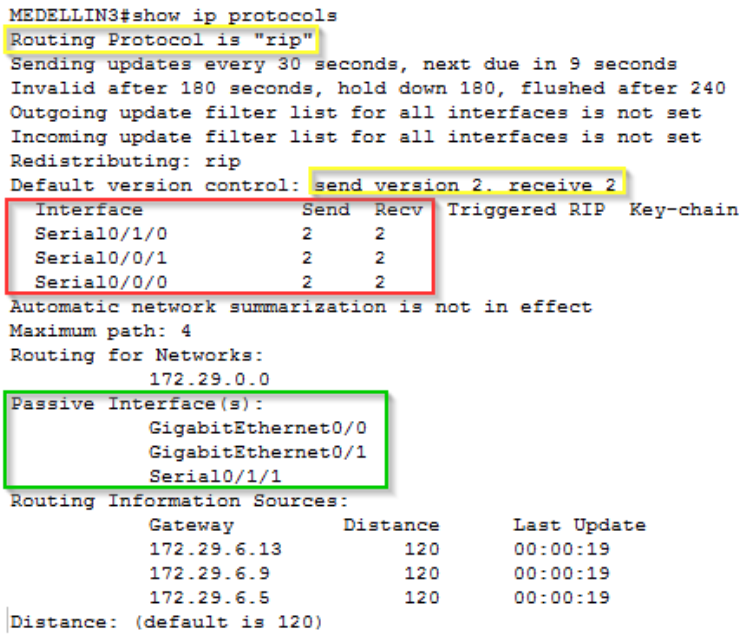


```
MEDELLIN2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 5 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  Serial0/0/1            2     2
  Serial0/0/0            2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
          172.29.0.0
Passive Interface(s):
          GigabitEthernet0/0
          GigabitEthernet0/1
Routing Information Sources:
          Gateway         Distance      Last Update
          172.29.6.1           120      00:00:04
          172.29.6.6           120      00:00:03
Distance: (default is 120)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

MEDELLIN3

Figura 80 Verificación Protocolo RIP MEDELLIN3

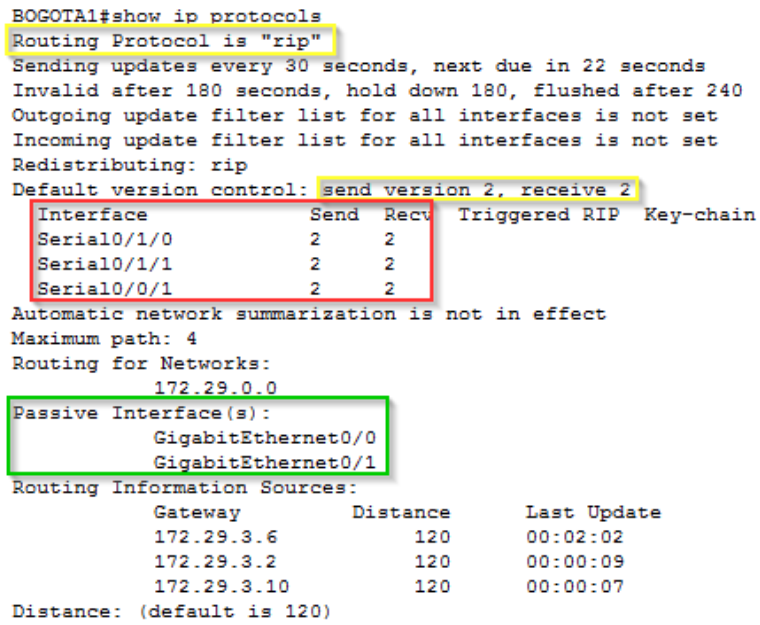


```
MEDELLIN3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 9 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  Serial0/1/0            2     2
  Serial0/0/1            2     2
  Serial0/0/0            2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
          172.29.0.0
Passive Interface(s):
          GigabitEthernet0/0
          GigabitEthernet0/1
          Serial0/1/1
Routing Information Sources:
          Gateway         Distance      Last Update
          172.29.6.13          120      00:00:19
          172.29.6.9           120      00:00:19
          172.29.6.5           120      00:00:19
Distance: (default is 120)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA1

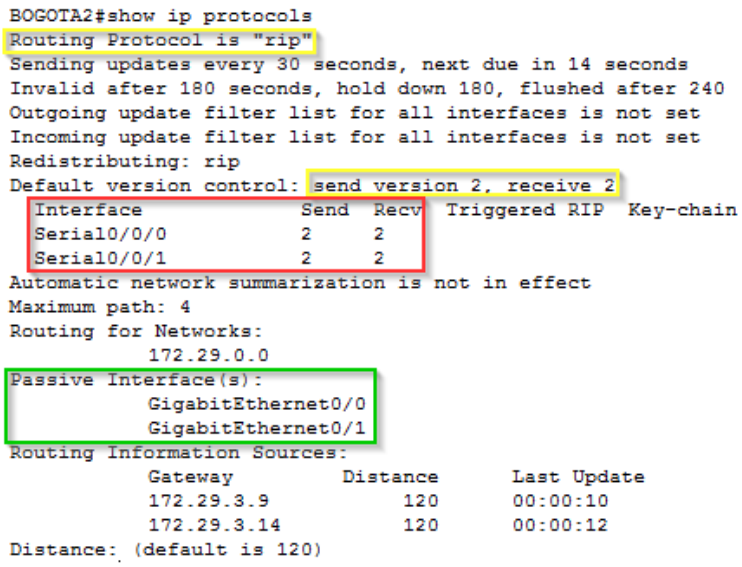
Figura 81 Verificación Protocolo RIP BOGOTA1



Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA2

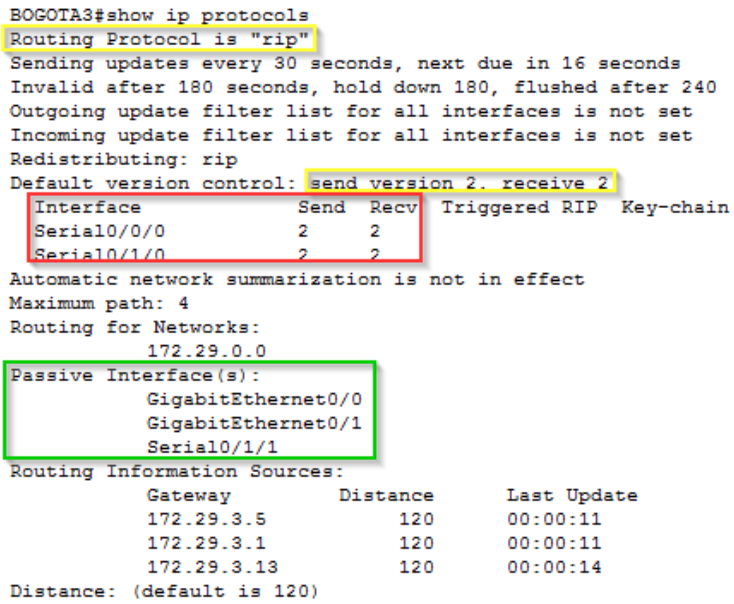
Figura 82 Verificación Protocolo RIP BOGOTA2



Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA3

Figura 83 Verificación Protocolo RIP BOGOTA3



Fuente: Cisco Packet Tracer 7.0.2.0226.

ISP

ISP#show ip protocols

ISP#

No se muestra ningún resultado porque no participa en RIP.

Tambien se muestra información sobre:

- ✓ La sumarización automática: si esta en efecto (**is in effect**) o no está en efecto (**is not in effect**).
- ✓ Las redes principales (**networks**) configuradas en cada router.
- ✓ Fuentes de información de routing (**Routing Information Sources**).

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

Se utiliza el comando de modo EXEC privilegiado **show ip rip database.**

MEDELLIN1

Figura 84 Base de datos RIP MEDELLIN1

```
MEDELLIN1#show ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0
    [0] via 0.0.0.0, 00:00:00
172.29.4.0/26    auto-summary
172.29.4.0/26
    [1] via 172.29.6.2, 00:00:11, Serial0/0/1
172.29.4.128/26    auto-summary
172.29.4.128/26
    [1] via 172.29.6.14, 00:00:09, Serial0/0/0    [1] via 172.29.6.10, 00:00:09, Serial0/1/1
172.29.6.0/30    auto-summary
172.29.6.0/30    directly connected, Serial0/0/1
172.29.6.4/30    auto-summary
172.29.6.4/30
    [1] via 172.29.6.14, 00:00:09, Serial0/0/0    [1] via 172.29.6.2, 00:00:11, Serial0/0/1
[1] via 172.29.6.10, 00:00:09, Serial0/1/1
172.29.6.8/30    auto-summary
172.29.6.8/30    directly connected, Serial0/1/1
172.29.6.12/30    auto-summary
172.29.6.12/30    directly connected, Serial0/0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

MEDELLIN2

Figura 85 Base de datos RIP MEDELLIN2

```
MEDELLIN2# show ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0
    [1] via 172.29.6.1, 00:00:10, Serial0/0/1
172.29.4.0/26    auto-summary
172.29.4.0/26    directly connected, GigabitEthernet0/0
172.29.4.128/26    auto-summary
172.29.4.128/26
    [1] via 172.29.6.6, 00:00:06, Serial0/0/0
172.29.6.0/30    auto-summary
172.29.6.0/30    directly connected, Serial0/0/1
172.29.6.4/30    auto-summary
172.29.6.4/30    directly connected, Serial0/0/0
172.29.6.8/30    auto-summary
172.29.6.8/30
    [1] via 172.29.6.6, 00:00:06, Serial0/0/0    [1] via 172.29.6.1, 00:00:10, Serial0/0/1
172.29.6.12/30    auto-summary
172.29.6.12/30
    [1] via 172.29.6.6, 00:00:06, Serial0/0/0    [1] via 172.29.6.1, 00:00:10, Serial0/0/1
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

MEDELLIN3

Figura 86 Base de datos RIP MEDELLIN3

```
MEDELLIN3#show ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0
    [1] via 172.29.6.13, 00:00:16, Serial0/0/0    [1] via 172.29.6.9, 00:00:16, Serial0/0/1
172.29.4.0/26    auto-summary
172.29.4.0/26
    [1] via 172.29.6.5, 00:00:16, Serial0/1/0
172.29.4.128/26    auto-summary
172.29.4.128/26    directly connected, GigabitEthernet0/0
172.29.6.0/30    auto-summary
172.29.6.0/30
    [1] via 172.29.6.5, 00:00:16, Serial0/1/0    [1] via 172.29.6.13, 00:00:16, Serial0/0/0
[1] via 172.29.6.9, 00:00:16, Serial0/0/1
172.29.6.4/30    auto-summary
172.29.6.4/30    directly connected, Serial0/1/0
172.29.6.8/30    auto-summary
172.29.6.8/30    directly connected, Serial0/0/1
172.29.6.12/30    auto-summary
172.29.6.12/30    directly connected, Serial0/0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA1

Figura 87 Base de datos RIP BOGOTA1

```
BOGOTA1#show ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0
    [0] via 0.0.0.0, 00:00:00
172.29.0.0/24    auto-summary
172.29.0.0/24
    [1] via 172.29.3.2, 00:00:25, Serial0/1/0
172.29.1.0/24    auto-summary
172.29.1.0/24
    [1] via 172.29.3.10, 00:00:17, Serial0/0/1
172.29.3.0/30    auto-summary
172.29.3.0/30    directly connected, Serial0/1/0
172.29.3.4/30    auto-summary
172.29.3.4/30    directly connected, Serial0/1/1
172.29.3.8/30    auto-summary
172.29.3.8/30    directly connected, Serial0/0/1
172.29.3.12/30    auto-summary
172.29.3.12/30
    [1] via 172.29.3.10, 00:00:17, Serial0/0/1    [1] via 172.29.3.2, 00:00:25, Serial0/1/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA2

Figura 88 Base de datos RIP BOGOTA2

```
BOGOTA2# show ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0
    [1] via 172.29.3.9, 00:00:27, Serial0/0/1
172.29.0.0/24    auto-summary
172.29.0.0/24
    [1] via 172.29.3.14, 00:00:01, Serial0/0/0
172.29.1.0/24    auto-summary
172.29.1.0/24    directly connected, GigabitEthernet0/0
172.29.3.0/30    auto-summary
172.29.3.0/30
    [1] via 172.29.3.14, 00:00:01, Serial0/0/0    [1] via 172.29.3.9, 00:00:27,
Serial0/0/1
172.29.3.4/30    auto-summary
172.29.3.4/30
    [1] via 172.29.3.14, 00:00:01, Serial0/0/0    [1] via 172.29.3.9, 00:00:27,
Serial0/0/1
172.29.3.8/30    auto-summary
172.29.3.8/30    directly connected, Serial0/0/1
172.29.3.12/30    auto-summary
172.29.3.12/30    directly connected, Serial0/0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA3

Figura 89 Base de datos RIP BOGOTA3

```
BOGOTA3#show ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0
    [1] via 172.29.3.5, 00:00:02, Serial0/1/1    [1] via 172.29.3.1, 00:00:02,
Serial0/1/0
172.29.0.0/24    auto-summary
172.29.0.0/24    directly connected, GigabitEthernet0/0
172.29.1.0/24    auto-summary
172.29.1.0/24
    [1] via 172.29.3.13, 00:00:27, Serial0/0/0
172.29.3.0/30    auto-summary
172.29.3.0/30    directly connected, Serial0/1/0
172.29.3.4/30    auto-summary
172.29.3.4/30    directly connected, Serial0/1/1
172.29.3.8/30    auto-summary
172.29.3.8/30
    [1] via 172.29.3.13, 00:00:27, Serial0/0/0    [1] via 172.29.3.5, 00:00:02,
Serial0/1/1    [1] via 172.29.3.1, 00:00:02, Serial0/1/0
172.29.3.12/30    auto-summary
172.29.3.12/30    directly connected, Serial0/0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

ISP

ISP#show ip rip database

ISP#

No se muestra ningún resultado porque no participa en RIP.

1.1.5. Parte 5: Configurar encapsulamiento y autenticación PPP

Encapsulamiento

Point-to-point Protocol (en español Protocolo punto a punto), también conocido por su acrónimo PPP, es un protocolo de nivel de enlace estandarizado en el documento RFC 1661.

Este protocolo permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico.

Para realizar el encapsulamiento se siguen los siguientes pasos:

- ✓ Se ingresa al modo de configuración global con el comando de modo EXEC privilegiado **config t.**
- ✓ Se ingresa al modo de configuración de interfaz con el comando **int** *ID-Interfaz.*
- ✓ Se establece el encapsulamiento con el comando **encapsulation ppp.** Despúes de emitir este comando, se desactiva el protocolo de la interfaz. En ambos dispositivos conectados y al configurar la autenticación la red vuelve a tener convergencia.

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.

PAP (Password Authentication Protocol) un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet. PAP es usado por la autenticación del protocolo PPP (Point to Point Protocol), validando a un usuario que accede a ciertos recursos. PAP transmite contraseñas o passwords en ASCII sin cifrar, por lo que se considera inseguro. PAP se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte.

Se realiza una autenticación bidireccional entre MEDELLIN1 y el ISP

- ✓ Se define el usuario y la clave del otro dispositivo con el comando **username** *usuario* **password** *contraseña*. El usuario es el hostname del otro dispositivo.
- ✓ Se ingresa al modo de configuración de interfaz con el comando **int** *ID-Interfaz*.
- ✓ Se establece la autenticación el comando **ppp authentication pap.**
- ✓ Se define el usuario y la contraseña con el comando **ppp pap sent-username** *usuario* **password** *contraseña.* El usuario debe ser el hostname.

ISP

ISP(config)#username **MEDELLIN1** password **cisco2019**

ISP(config)#

ISP(config)#int s0/0/0

ISP(config-if)#encapsulation ppp

ISP(config-if)#

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

ISP(config-if)#ppp authentication pap

ISP(config-if)#ppp pap sent-username **ISP** password **cisco2019**

ISP(config-if)#

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

ISP(config-if)#

MEDELLIN1

MEDELLIN1(config)#username **ISP** password **cisco2019**

MEDELLIN1(config)#

MEDELLIN1(config)#

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

MEDELLIN1(config)#int s0/1/0

MEDELLIN1(config-if)#encapsulation ppp

MEDELLIN1(config-if)#ppp authentication pap

MEDELLIN1(config-if)#ppp pap sent-username **MEDELLIN1** password **cisco2019**

MEDELLIN1(config-if)#

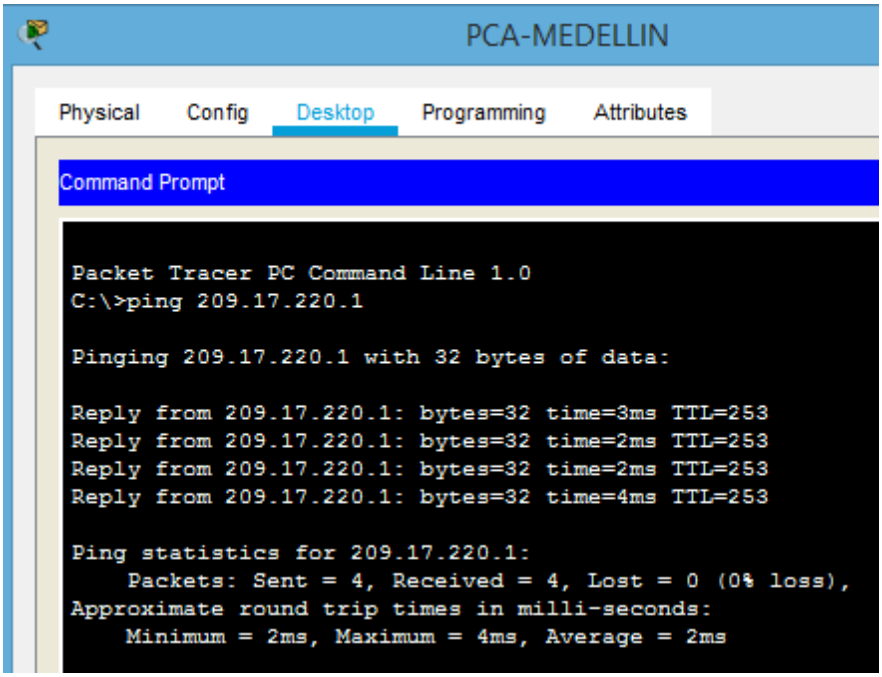
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

MEDELLIN1(config-if)#

Verificacion Conectividad

- ✓ Ping PCA-MEDELLIN a ISP.

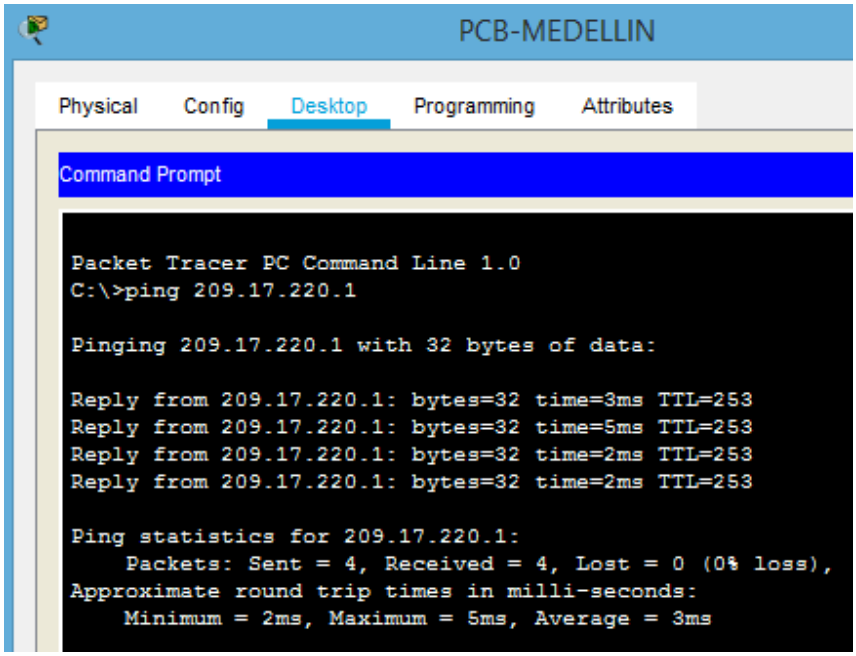
Figura 90 Verificación PPP y PAP. Ping PCA-MEDELLIN a ISP



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping PCB-MEDELLIN a ISP.

Figura 91 Verificación PPP y PAP. Ping PCB-MEDELLIN a ISP



Fuente: Cisco Packet Tracer 7.0.2.0226.

b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

CHAP es un método de autentificación usado por servidores accesibles vía PPP. CHAP verifica periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas. Esto ocurre cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación. La verificación se basa en un secreto compartido (como una contraseña).

Se realiza una autenticación bidireccional entre BOGOTA1 y el ISP

- ✓ Se define el usuario del otro dispositivo con el comando **username** *nombrehost* **password** *contraseña*. La contraseña es la misma para ambos dispositivos
- ✓ Se ingresa al modo de configuración de interfaz con el comando **int** *ID-Interfaz*.
- ✓ En el modo de configuración de interfaz se establece la autenticación el comando **ppp authentication chap.**

ISP

ISP(config)#username BOGOTA1 password class2019

ISP(config)# int s0/0/1

ISP(config-if)#encapsulation ppp

ISP(config-if)#

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

ISP(config-if)#ppp authentication chap

ISP#

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

ISP#

BOGOTA1

BOGOTA1(config)#username ISP password class2019

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

BOGOTA1(config)#int s0/0/0

BOGOTA1(config-if)#encapsulation ppp

BOGOTA1(config-if)#ppp authentication chap

BOGOTA1#

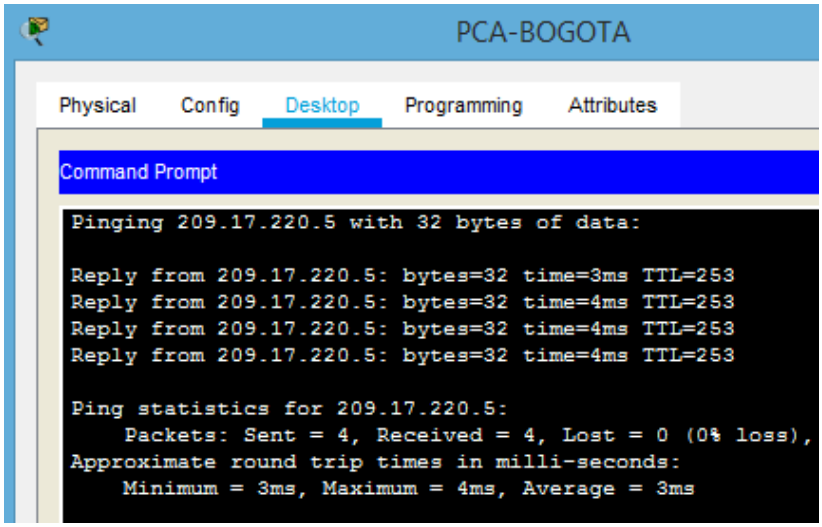
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

BOGOTA1#

Verificacion Conectividad

- ✓ Ping PCA-BOGOTA a ISP.

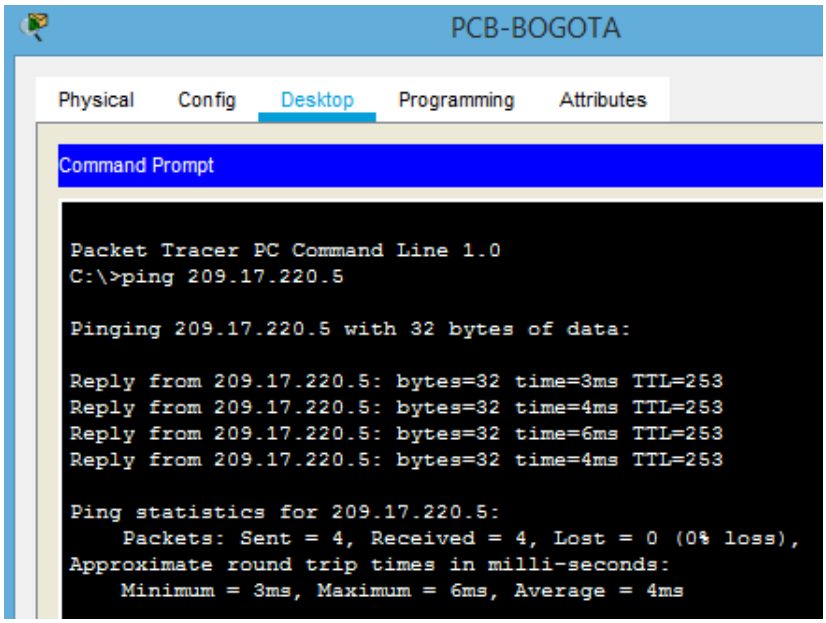
Figura 92 Verificación PPP y CHAP. Ping PCA-BOGOTA a ISP



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping PCB-BOGOTA a ISP

Figura 93 Verificación PPP y CHAP. Ping PCB-BOGOTA a ISP



Fuente: Cisco Packet Tracer 7.0.2.0226.

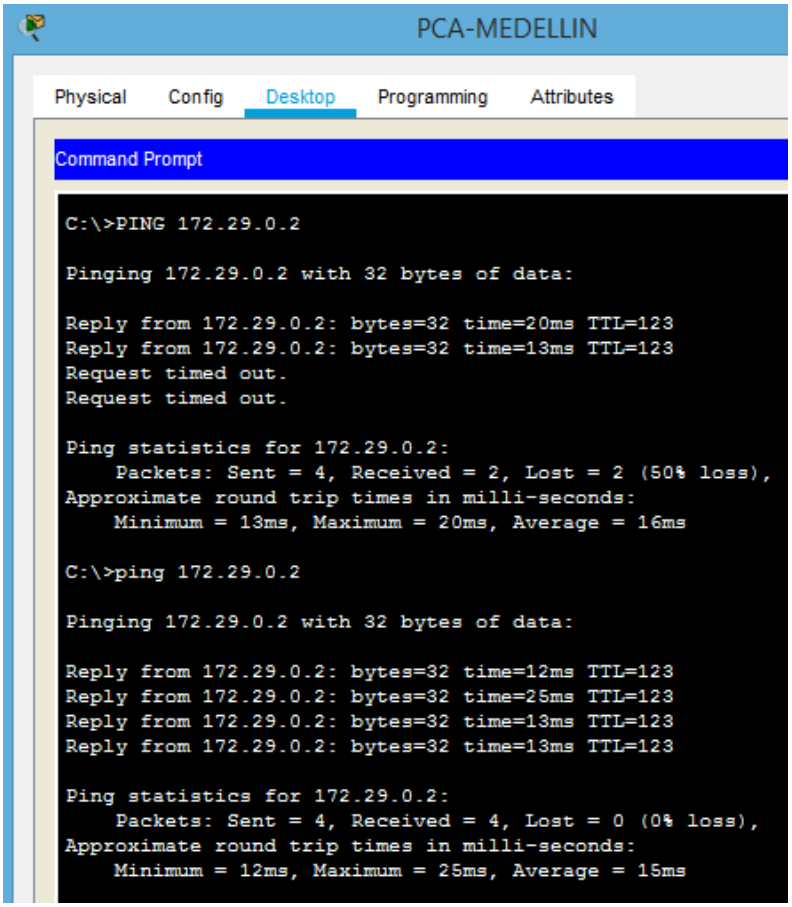
1.1.6. Parte 6: Configuración de PAT

a. 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.

Verificacion Extremo a Extremo

- ✓ Ping PCA-MEDELLIN a PCA-BOGOTA.

Figura 94 Conectividad antes de PAT. Ping PCA-MEDELLIN a PCA-BOGOTA



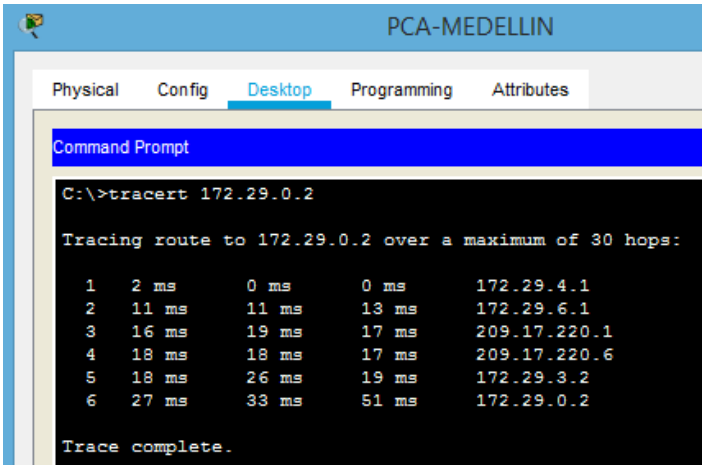
Fuente: Cisco Packet Tracer 7.0.2.0226.

El primer ping se completo en un 50% por el proceso ARP.

- El comando **tracert** permite apreciar los saltos del} los paquetes hacia el destino.
- El primer ping puede completarse en un 75% por el proceso ARP.

✓ Tracert PCA-MEDELLIN a PCA-BOGOTA.

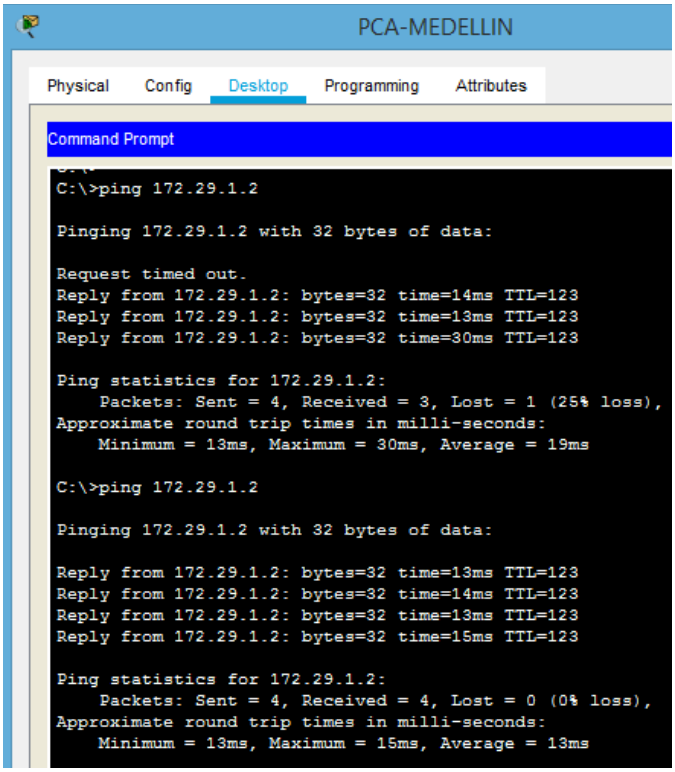
Figura 95 Conectividad sin PAT. Tracert PCA-MEDELLIN a PCA-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Ping PCA-MEDELLIN a PCB-BOGOTA.

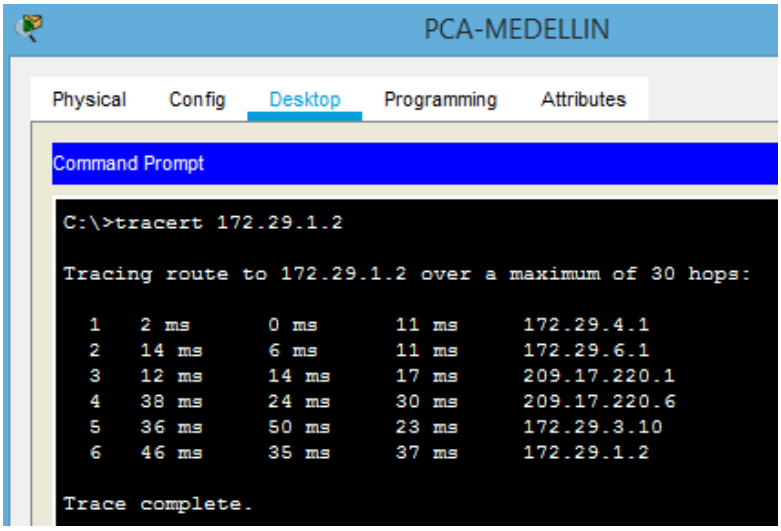
Figura 96 Conectividad sin PAT. Ping PCA-MEDELLIN a PCB-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Tracert PCA-MEDELLIN a PCB-BOGOTA.

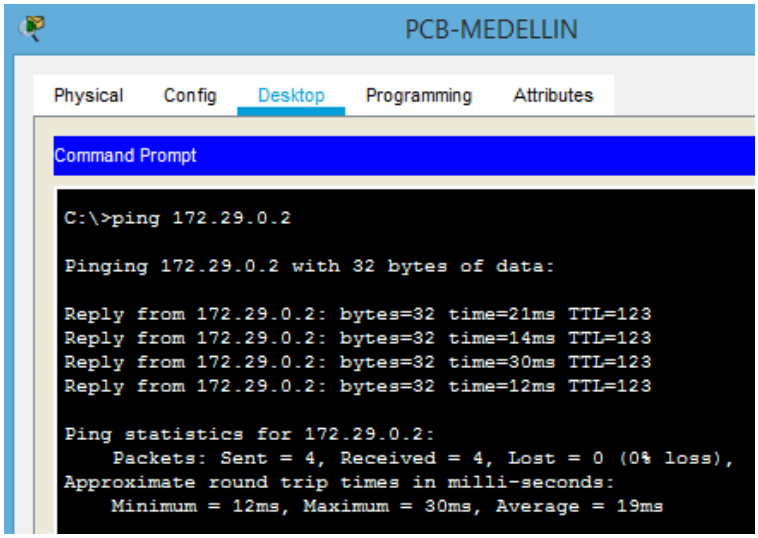
Figura 97 Conectividad sin PAT. Tracert PCA-MEDELLIN a PCB-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Ping PCB-MEDELLIN a PCA-BOGOTA.

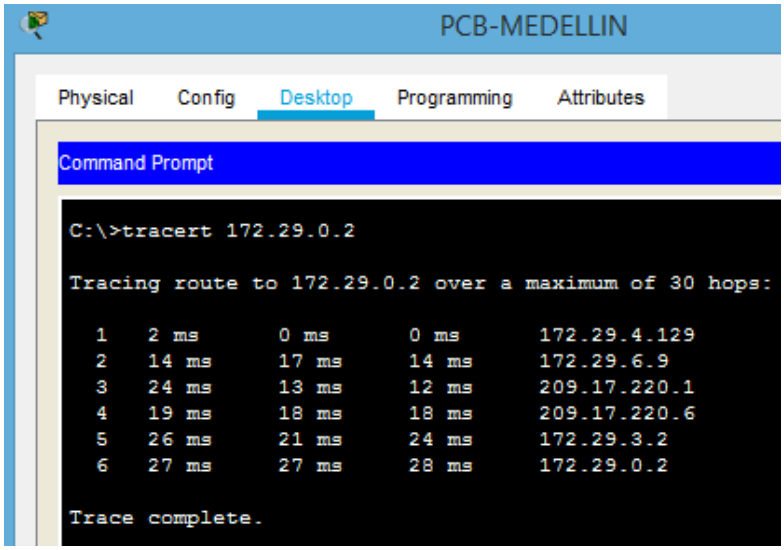
Figura 98 Conectividad sin PAT. Ping PCB-MEDELLIN a PCA-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Tracert PCB-MEDELLIN a PCA-BOGOTA.

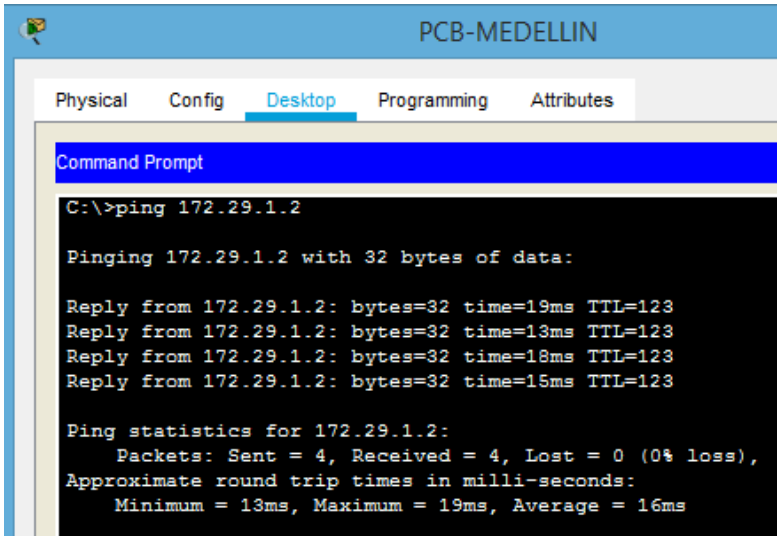
Figura 99 Conectividad sin PAT. Tracert PCB-MEDELLIN a PCA-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Ping PCB-MEDELLIN a PCB-BOGOTA.

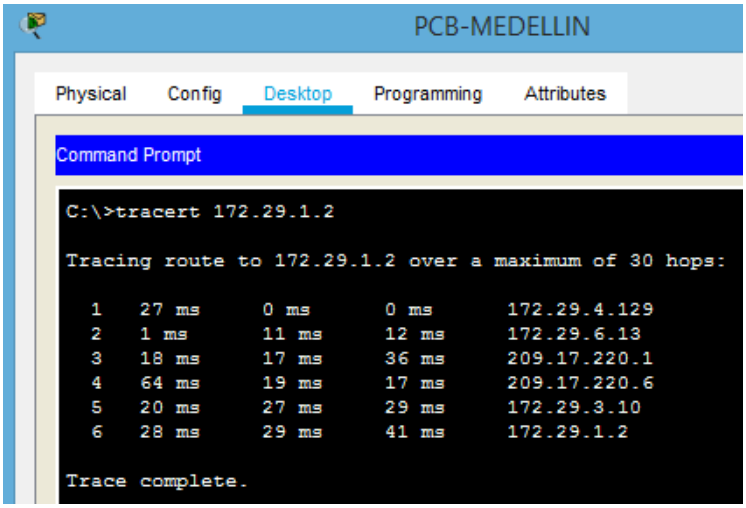
Figura 100 Conectividad sin PAT. Ping PCB-MEDELLIN a PCB-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Tracert PCB-MEDELLIN a PCB-BOGOTA.

Figura 101 Conectividad sin PAT. Tracert PCB-MEDELLIN a PCB-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

Configuracion NAT

NAT (Network Address Translate) o Traduccion de Direcciones de Red.

Es una alternativa de solución para el agotamiento de direcciones IPv4.

La conservación de direcciones se logra al permitir que se utilicen direcciones IPv4 privadas internamente y la traducción a una dirección IPv4 publica solo cuando sea estrictamente necesario.

NAT siempre se aplica desde la perspectiva del dispositivo con la dirección traducida. Maneja la siguiente terminología:

- Dirección Interna: la dirección del dispositivo que se traduce por medio de NAT.
- Dirección Externa: la dirección del dispositivo de destino.
- Dirección Local: cualquier dirección que aparece en la porción interna de la red.
- Dirección Global: cualquier dirección que aparece en la porción externa de la red.

Se combinan de la siguiente manera:

- Dirección Local Interna: la dirección de origen vista desde el interior de la red.

- Dirección Global Interna: la dirección de origen vista desde la red externa después de ser traducida.
- Dirección Global Externa: la dirección de desino vista desde la red externa. Es una dirección IPv4 enrutable globalmente y asignada a un host en internet. Por lo general, las direcciones externas globales y locales son iguales.
- Dirección Local Externa: la dirección de destino vista desde la red interna. Esta dirección puede ser diferente de la dirección globalmente enrutable del destino.

Hay tres tipos de NAT:

- NAT Estática: consiste en la asignación de direcciones uno a uno entre una dirección local y una global. Se configuran manualmente. Las direcciones locales internas se traducen en direcciones globales internas configuradas. Para redes externas tienen direcciones IPv4 publicas.
- NAT Dinámica: asignación de varias direcciones a varias direcciones entre direcciones locales y globales. Las traducciones se realizan en función de disponibilidad. Utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada.
- Traducción de la dirección de puerto (PAT) o NAT con sobrecarga: asignación de varias direcciones a una entre direcciones locales y globales. Asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública a algunas direcciones. Cada dirección pivada se rastrea con un numero de puerto. En una sesión TCP/IP el dispositivo genera un valor de puerto de origen TCP o UDP o un ID de consulta para ICMP, asi se evitan ambigüedades.

El router NAT al recibir el paquete del cliente utiliza el puerto de origen para identificarde forma exclusva la traducción NAT. Se utiliza un número distinto de puerto para cada sesión con un servidoren internet. En el destino este número de puerto permite identificar a que dispositivo se reenvía el paquete.

PAT se puede configurar de dos formas:

- Para un conjunto de direcciones IPv4 públicas: si se emitió mas de una dirección IPv4 pública para un sitio, esas direcciones pueden ser parte de un conjunto utilizado por PAT.
- Para una dirección única IPv4 pública: si solo hay una única dirección IPv4 pública disponible, la configuración de sobrecarga asigna la dirección pública a la interfaz externa que conecta al ISP. Todas las direcciones internas se traducen a la única dirección IPv4 cuando salen de la interfaz externa.

Para verificar la configuración de PAT se utilizan los comandos de modo EXEC privilegiado:

show ip nat translations: se verifican las traduccionesde NAT.

show ip nat statistics: se controlan las estadísticas de NAT.

Para configurar NAT con sobrecarga se realiza lo siguiente:

- ✓ Se identifica la interfaz externa de cada router como la dirección global interna que se debe sobrecargar con la ACL 1. Se utiliza el comando de configuración global **ip nat inside source list 1 int** *interfaz-salida* **overload**
- ✓ Se configura la ACL 1 para permitir que NAT traduzca los dispositivos de la red en cuestión. Comando **access-list 1 permit** *Direccion-Red Mascara de Wildcard.*
- ✓ Se configura la interfaz NAT externa adecuada con el comando **ip nat outside** dentro de la configuración de interfaz.
- ✓ Se configura la interfaz NAT Interna adecuada con el comando **ip nat inside** dentro de la configuración de interfaz.

MEDELLIN

MEDELLIN1#config t

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

MEDELLIN1(config)#ip nat inside source list 1 int s0/1/0 overload

MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255

MEDELLIN1(config-if)#int s0/1/0

MEDELLIN1(config-if)#ip nat outside

MEDELLIN1(config)#int s0/0/1

MEDELLIN1(config-if)#ip nat inside

MEDELLIN1(config-if)#int s0/1/1

MEDELLIN1(config-if)#ip nat inside

MEDELLIN1(config-if)#int s0/0/0

MEDELLIN1(config-if)#ip nat inside

MEDELLIN1(config-if)#

BOGOTA

BOGOTA1#config t

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

BOGOTA1(config)#ip nat inside source list 1 int s0/0/0 overload

BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255

BOGOTA1(config-if)#int s0/0/0

BOGOTA1(config-if)#ip nat outside

BOGOTA1(config)#int s0/1/1

BOGOTA1(config-if)#ip nat inside

BOGOTA1(config-if)#int s0/1/0

BOGOTA1(config-if)#ip nat inside

BOGOTA1(config-if)#int s0/0/1

BOGOTA1(config-if)#ip nat inside

BOGOTA1(config-if)#

Verificacion Conectividad

MEDELLIN

- ✓ Ping MEDELLIN2 a MEDELLIN3.

Figura 102 Verificación Conectividad NAT. Ping MEDELLIN2 a MEDELLIN3

```
MEDELLIN2>ping 172.29.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/19 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN2 a MEDELLIN1.

Figura 103 Verificación Conectividad NAT. Ping MEDELLIN2 a MEDELLIN1

```
MEDELLIN2>ping 172.29.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/30 ms

MEDELLIN2>ping 172.29.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/40 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN3 a MEDELLIN1.

Figura 104 Verificación Conectividad NAT. Ping MEDELLIN3 a MEDELLIN1

```
MEDELLIN3>ping 172.29.6.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms

MEDELLIN3>ping 172.29.6.13

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/37 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN3 a ISP.

Figura 105 Verificación Conectividad NAT. Ping MEDELLIN3 a ISP

```
MEDELLIN3>ping 209.17.220.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/12/21
ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN2 a ISP.

Figura 106 Verificación Conectividad NAT. Ping MEDELLIN2 a ISP

```
MEDELLIN2>ping 209.17.220.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 13/25/49
ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN1 a ISP.

Figura 107 Verificación Conectividad NAT. Ping MEDELLIN1 a ISP

```
MEDELLIN1#ping 209.17.220.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/31 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN1 a BOGOTA1.

Figura 108 Verificación Conectividad NAT. Ping MEDELLIN1 a BOGOTA 1

```
MEDELLIN1#PING 209.17.220.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/18/61
ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

BOGOTA

- ✓ Ping BOGOTA2 a BOGOTA3.

Figura 109 Verificación Conectividad NAT. Ping BOGOTA2 a BOGOTA3

```
BOGOTA2>ping 172.29.3.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/34 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA2 a BOGOTA1.

Figura 110 Verificación Conectividad NAT. Ping BOGOTA2 a BOGOTA1

```
BOGOTA2>ping 172.29.3.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/53
ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA3 a BOGOTA1.

Figura 111 Verificación Conectividad NAT. Ping BOGOTA3 a BOGOTA1

```
BOGOTA3>ping 172.29.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/27 ms

BOGOTA3>ping 172.29.3.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/13/61
ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA2 a ISP.

Figura 112 Verificación Conectividad NAT. Ping BOGOTA2 a ISP

```
BOGOTA2>ping 209.17.220.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/14/26
ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA3 a ISP.

Figura 113 Verificación Conectividad NAT. Ping BOGOTA3 a ISP

```
BOGOTA3>ping 209.17.220.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/11/18
ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA1 a ISP.

Figura 114 Verificación Conectividad NAT. Ping BOGOTA1 a ISP

```
BOGOTA1>ping 209.17.220.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/40 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping BOGOTA1 a MEDELLIN1.

Figura 115 Verificación Conectividad NAT. Ping BOGOTA1 a MEDELLIN1

```
BOGOTA1>ping 209.17.220.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 13/19/40
ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Pings fallidos de routers internos de MEDELLIN a routers internos de BOGOTA

- ✓ Ping MEDELLIN2 a BOGOTA2.

Figura 116 Verificación Conectividad NAT. Ping MEDELLIN2 a BOGOTA2

```
MEDELLIN2>ping 172.29.3.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN2 a BOGOTA3.

Figura 117 Verificación Conectividad NAT. Ping MEDELLIN2 a BOGOTA3

```
MEDELLIN2>ping 172.29.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

MEDELLIN2>ping 172.29.3.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN3 a BOGOTA2

Figura 118 Verificación Conectividad NAT. Ping MEDELLIN3 a BOGOTA2

```
MEDELLIN3>ping 172.29.3.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping MEDELLIN3 a BOGOTA3

Figura 119 Verificación Conectividad NAT. Ping MEDELLIN3 a BOGOTA3

```
MEDELLIN3>ping 172.29.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

MEDELLIN3>ping 172.29.3.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

b. 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 del router Medellín1, cómo diferente puerto.

Figura 120 Traducciones NAT MEDELLIN1

```
MEDELLIN1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.2:31   172.29.6.10:31     209.17.220.1:31    209.17.220.1:31
icmp 209.17.220.2:32   172.29.6.14:32     209.17.220.1:32    209.17.220.1:32
icmp 209.17.220.2:33   172.29.6.10:33     209.17.220.1:33    209.17.220.1:33
icmp 209.17.220.2:34   172.29.6.14:34     209.17.220.1:34    209.17.220.1:34
icmp 209.17.220.2:35   172.29.6.10:35     209.17.220.1:35    209.17.220.1:35
icmp 209.17.220.2:37   172.29.6.2:37      209.17.220.1:37    209.17.220.1:37
icmp 209.17.220.2:38   172.29.6.2:38      209.17.220.1:38    209.17.220.1:38
icmp 209.17.220.2:39   172.29.6.2:39      209.17.220.1:39    209.17.220.1:39
icmp 209.17.220.2:40   172.29.6.2:40      209.17.220.1:40    209.17.220.1:40
icmp 209.17.220.2:41   172.29.6.2:41      209.17.220.1:41    209.17.220.1:41
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

c. 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.

Figura 121 Traducciones NAT BOGOTA1

```
BOGOTA1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.6:25   172.29.3.10:25     209.17.220.5:25    209.17.220.5:25
icmp 209.17.220.6:26   172.29.3.10:26     209.17.220.5:26    209.17.220.5:26
icmp 209.17.220.6:27   172.29.3.10:27     209.17.220.5:27    209.17.220.5:27
icmp 209.17.220.6:28   172.29.3.10:28     209.17.220.5:28    209.17.220.5:28
icmp 209.17.220.6:29   172.29.3.10:29     209.17.220.5:29    209.17.220.5:29
icmp 209.17.220.6:31   172.29.3.2:31      209.17.220.5:31    209.17.220.5:31
icmp 209.17.220.6:32   172.29.3.6:32      209.17.220.5:32    209.17.220.5:32
icmp 209.17.220.6:33   172.29.3.2:33      209.17.220.5:33    209.17.220.5:33
icmp 209.17.220.6:34   172.29.3.6:34      209.17.220.5:34    209.17.220.5:34
icmp 209.17.220.6:35   172.29.3.2:35      209.17.220.5:35    209.17.220.5:35
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

1.1.7. Parte 7: Configuración del servicio DHCP

El Protocolo de Configuración Dinámica de Host o DHCPv4 por sus siglas en ingles, asigna direcciones IPv4 y otra información de configuración de la red de forma dinámica. Las direcciones son asignadas de un conjunto de direcciones durante un periodo limitado escogido por el servidoro hasta que el cliente no necesite la dirección.

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.

Para configurar DHCPv4 en un router cisco se realiza lo siguiente:

- ✓ Se excluye un conjunto de direcciones con el comando de configuración global **ip dhcp excluded-adresss** *Direccion 1-Direccion n.*

Algunas direcciones IPv4 de un conjunto se asignan a dispositivos de red que requiren asignaciones de direcciones estáticas y no deben ser asignadas de manera dinámica.

- ✓ Se configura un pool o conjunto de direcciones con nombre especificado de DHCPv4 con el comando **ip dhcp pool** *nombre-pool.*

Cuando se configura un servidor de DHCPv4 se debe definir un conjunto de direcciones que se deben asignar. Tras ejecutar el comando, el router entra en el modo de configuración de DHCPv4.

- ✓ Para finalizar la configuración de un pool DHCPv4 se debe realizar una serie de tareas, algunas son optativas pero otras requeridas:

Tareas requeridas

- ✓ Se define un conjunto de direcciones con el comando de configuración de DHCPv4 **network** *número-red* [*mask* | *prefix-length*].
- ✓ Se define el router o gateway predeterminado con el comando de configuración de DHCPv4 **default-router** *address* [*address 1*…*address 8*]. El Gateway suele ser la interfaz LAN del router mas cercano a los terminales cliente. Se debe especificar un gateway pero se pueden indicar hasta 8 direcciones si existen varios gateways.

Tareas Optativas

Entre las tareas optativas se encuentran:

- ✓ Definir un servidor DNS. Comando de configuración de DHCPv4 **dns-server address** [*address 1*…*address 8*].
- ✓ Definir nombre de dominio con el comando de configuración de DHCPv4 **domain-name** *dominio*.
- ✓ Definir la duración de la concesión de DHCP. Comando de configuración de DHCPv4 **lease** { [*hours*] [*minutes*] | infinite }
- ✓ Este comando permite especificar el tiempo máximo que puede asignarse una dirección IP a un nodo de la red. Por ejemplo, se define lease 1, esto quiere decir que el tiempo especificado es un dia. Después de las 24 horas, el nodo se refrescará y se le asignará una nueva dirección IP. Generalmente se asigna la misma dirección.
- ✓ Definir el servidor WINS de NetBIOS. Comando de configuración de DHCPv4 **netbios-name-server** *address* [*address 2*…*address 8*].

Para el ejercicio no se utilizan todas estas opciones. Se mencionan con fines informativos.

MEDELLIN

MEDELLIN2#config t

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

- Se excluyen 10 direcciones en cada subred.

MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.10

MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.138

- Se configura el POOL para MEDELLIN2.

MEDELLIN2(config)#ip dhcp pool POOL-MEDELLIN2

- En el conjunto de direcciones se debe colocar la mascara de subred de la subred dividida es decir, /25.

MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.192

- El Gateway predeterminado será la dirección de la interfaz G0/0 de MEDELLIN2.

MEDELLIN2(dhcp-config)#default-router 172.29.4.1

- Se asigna cualquier servidor DNS. En este caso es indiferente.

MEDELLIN2(dhcp-config)#dns-server 0.0.0.0

MEDELLIN2(dhcp-config)#exit

- Se configura el POOL para MEDELLIN3.

MEDELLIN2(config)#ip dhcp pool POOL-MEDELLIN3

- En el conjunto de direcciones se debe colocar la mascara de subred de la subred dividida es decir, /25.

MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.192

- El Gateway predeterminado será la dirección de la interfaz G0/0 de MEDELLIN3.

MEDELLIN2(dhcp-config)#default-router 172.29.4.129

MEDELLIN2(dhcp-config)#dns-server 0.0.0.0

MEDELLIN2(dhcp-config)#exit

MEDELLIN2(config)#

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

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

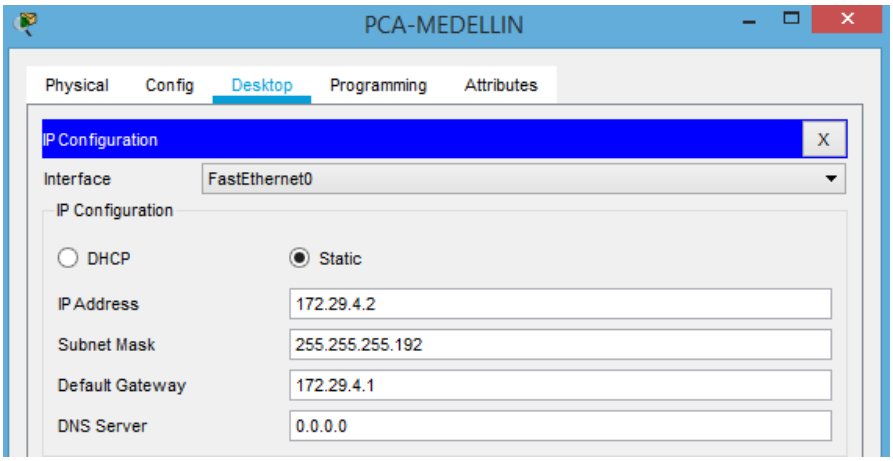
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

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

Configuracion DHCP en las PC

- LAN MEDELLIN2 PCA-MEDELLIN (50 HOSTS) SUBRED 172.29.4.0/26.

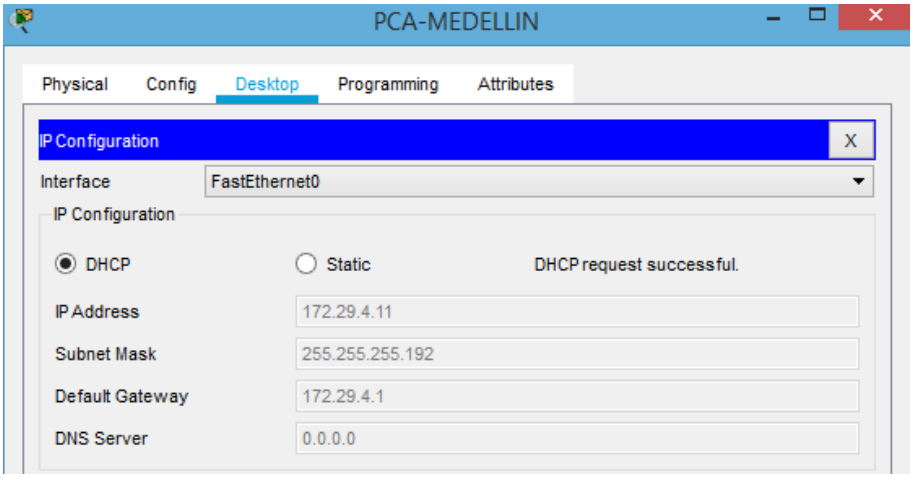
Figura 122 DHCP. Configuración estática previa PCA-MEDELLIN



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se hace clic sobre el botón DHCP y se debe mostrar un mensaje de solicitud DHCP exitoso (DHCP request successful).

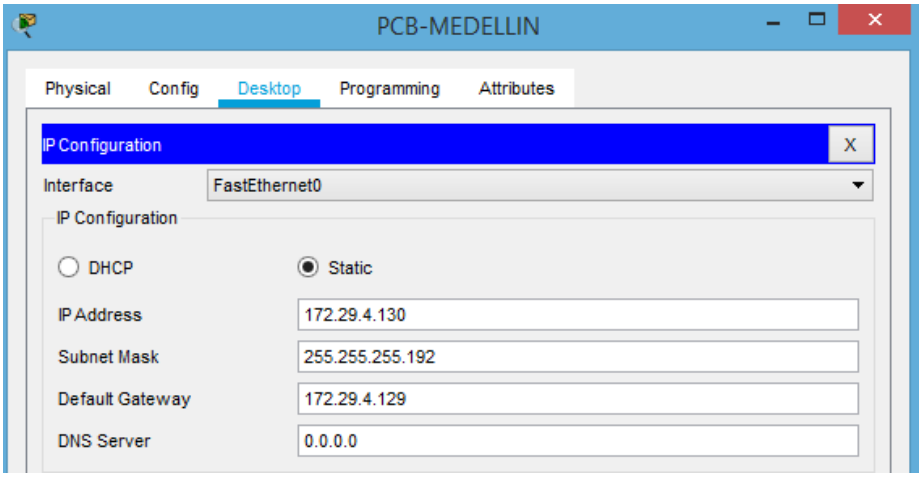
Figura 123 DHCP. Configuración dinámica exitosa PCA-MEDELLIN



Fuente: Cisco Packet Tracer 7.0.2.0226.

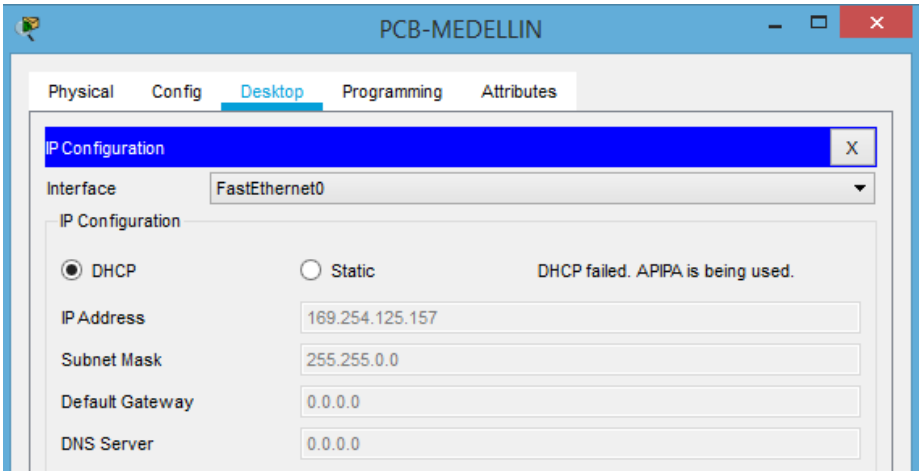
- LAN MEDELLIN3 PCB-MEDELLIN (40 HOSTS) SUBRED 172.29.4.128/26.

Figura 124 DHCP. Configuración estática previa PCB-MEDELLIN



Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 125 DHCP. Configuración dinámica fallida PCB-MEDELLIN



Fuente: Cisco Packet Tracer 7.0.2.0226.

Esto se debe a que MEDELLIN3 al encontrarse en otra red requiere de un router que retranmita su solicitud de DHCP hacia MEDELLIN2.

MEDELLIN3 actuará como retransmisor de DHCP4.

Para configurar un router como retransmisor de DHCPv4 se ingresa a la interfaz donde se encuentre conectado el PC y se emite el comando **ip helper-address** *Direccion IP del servidor DHCP.*

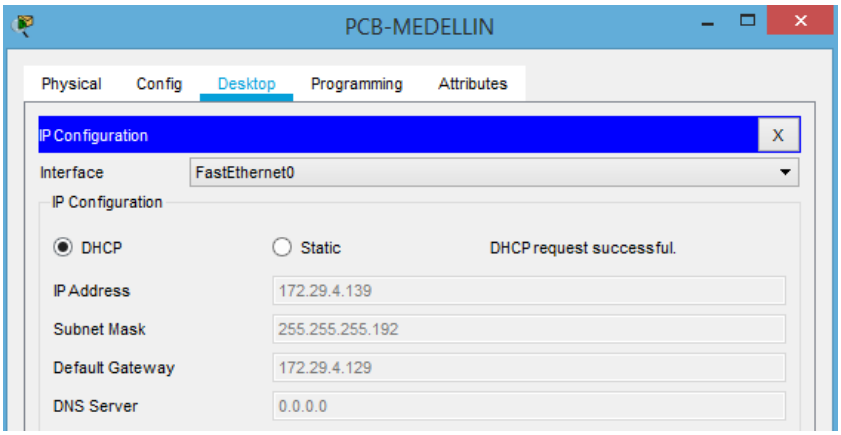
MEDELLIN3(config)#int g0/0

MEDELLIN3(config-if)#ip helper-address 172.29.6.5

MEDELLIN3(config-if)#

- ✓ Se repite el procedimiento de configuración y debe ser exitoso.

Figura 126 DHCP. Configuración dinámica exitosa PCB-MEDELLIN

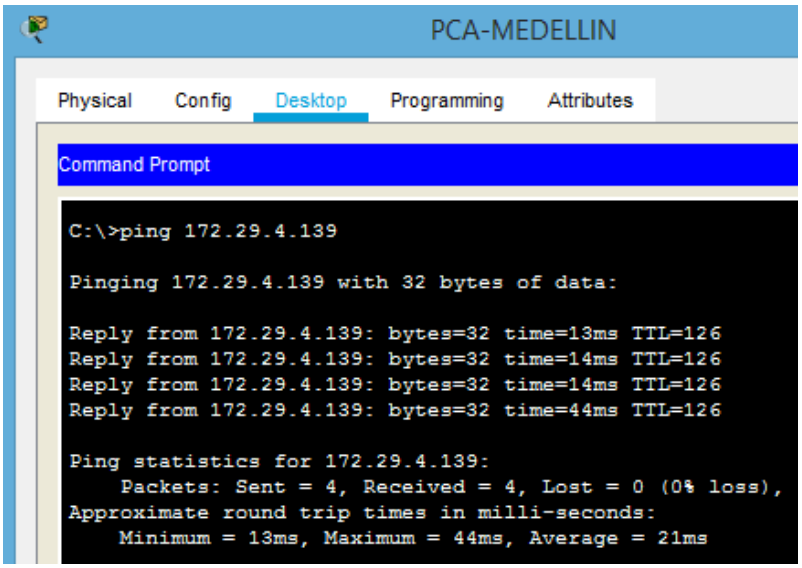


Fuente: Cisco Packet Tracer 7.0.2.0226.

Verificación Conectividad

- ✓ Ping PCA-MEDELLIN a PCB-MEDELLIN.

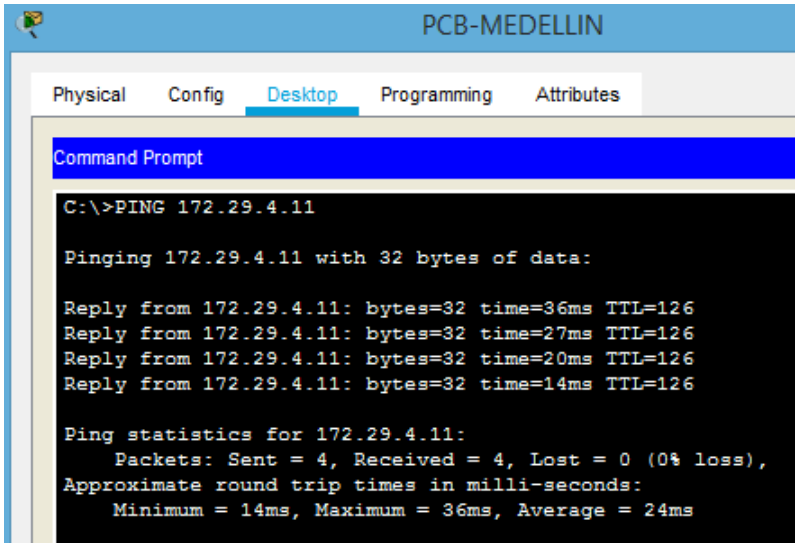
Figura 127 Verificación DHCP. Ping PCA-MEDELLIN a PCB-MEDELLIN



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Ping PCB-MEDELIN a PCA-MEDELLIN

Figura 128 Verificación DHCP. Ping PCB-MEDELLIN a PCA-MEDELLIN



Fuente: Cisco Packet Tracer 7.0.2.0226.

b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

MEDELLIN3#show running-config | include ip helper-addres

ip helper-address 172.29.6.5

MEDELLIN3#

c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

Para conseguir que MEDELLIN2 sea el servidor DHCP de BOGOTA2 y BOGOTA3 primero se debe dehabilitar NAT en los routers MEDELLIN1 y BOGOTA1. Para estos se utilizan dos comandos:

- Comando de configuración global: **no ip nat inside/outside source list 1 interface** *ID-Interfaz* **overload.**
- Comando de modo EXEC privilegiado: **clear ip nat translation:** permite limpiar las traducciones NAT.

MEDELLIN1

MEDELLIN1#config t

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

MEDELLIN1(config)#no ip nat inside source list 1 interface Serial0/1/0 overload

MEDELLIN1(config)#exit

MEDELLIN1#clear ip nat translation *

MEDELLIN1#

BOGOTA1

BOGOTA1#config t

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

BOGOTA1(config)#no ip nat inside source list 1 interface Serial0/0/0 overload

BOGOTA1(config)#exit

BOGOTA1#

%SYS-5-CONFIG_I: Configured from console by console

BOGOTA1#clear ip nat translation *

BOGOTA1#

En MEDELLIN2 se configuran DHCP para las redes de BOGOTA, uno para cada red:

MEDELLIN2#config t

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

MEDELLIN2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10

MEDELLIN2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10

MEDELLIN2(config)#ip dhcp pool POOL-BOGOTA2

MEDELLIN2(dhcp-config)#network 172.29.1.0 255.255.255.0

MEDELLIN2(dhcp-config)#default-router 172.29.1.1

MEDELLIN2(dhcp-config)#dns-server 0.0.0.0

MEDELLIN2(dhcp-config)#exit

MEDELLIN2(config)#ip dhcp pool POOL-BOGOTA3

MEDELLIN2(dhcp-config)#network 172.29.0.1 255.255.255.0

MEDELLIN2(dhcp-config)#default-router 172.29.0.1

MEDELLIN2(dhcp-config)#dns-server 0.0.0.0

MEDELLIN2(dhcp-config)#exit

MEDELLIN2(config)#

Desactivacion y activación automática de interfaces

MEDELLIN1

MEDELLIN1#

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

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

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

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

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

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

MEDELLIN1#

BOGOTA1

BOGOTA1#

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

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

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

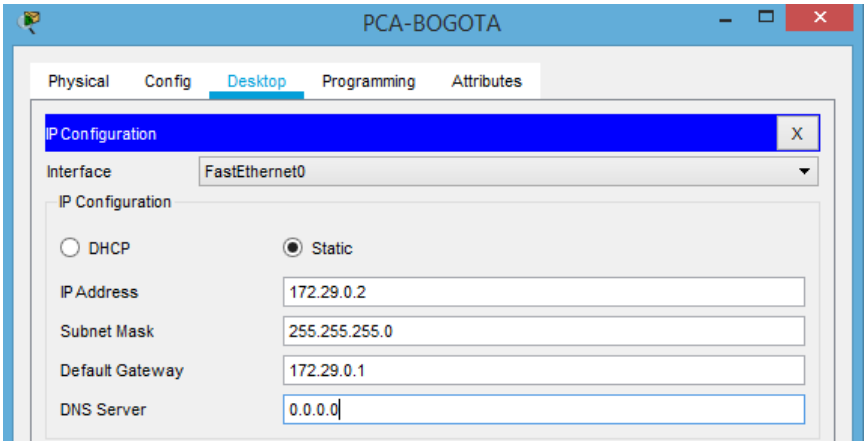
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

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

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

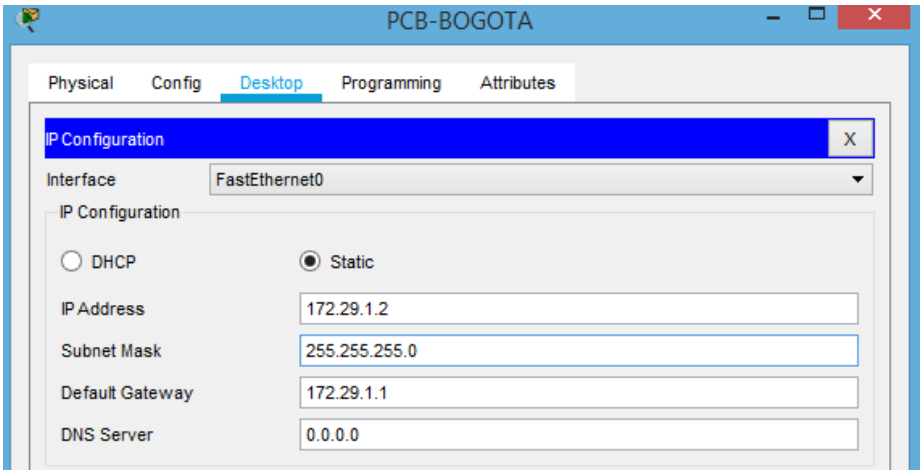
BOGOTA1#

Figura 129 DHCP. Configuración estática previa PCA-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 130 DHCP. Configuración estática previa PCB-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

Se configura BOGOTA1, BOGOTA2 y BOGOTA 3 como router de retranmisión de DHCP. La dirección IP asociada corresponde a la interfaz Serial0/0/1 DCE de MEDELLIN2.

BOGOTA1

BOGOTA1(config-if)#int s0/0/1

BOGOTA1(config-if)#ip helper-address 172.29.6.2

BOGOTA1(config-if)#

BOGOTA2

BOGOTA2(config)#int g0/0

BOGOTA2(config-if)#ip helper-address 172.29.6.2

BOGOTA2(config-if)#

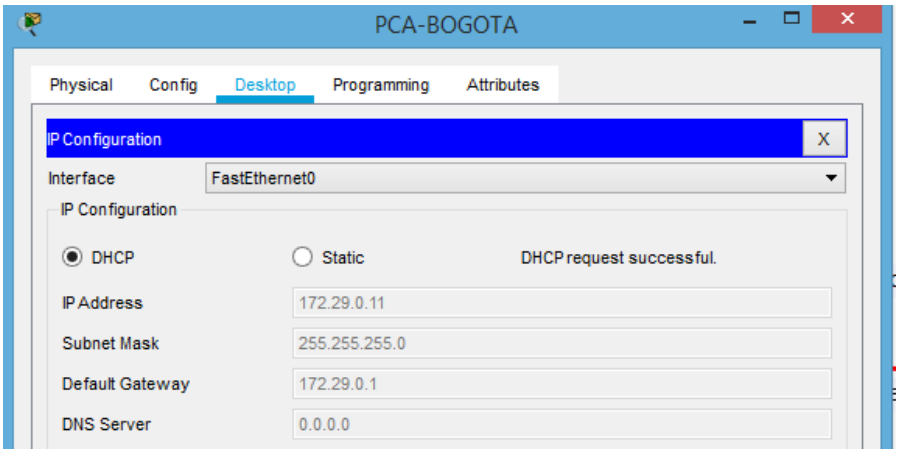
BOGOTA3

BOGOTA3(config)#int g0/0

BOGOTA3(config-if)#ip helper-address 172.29.6.2

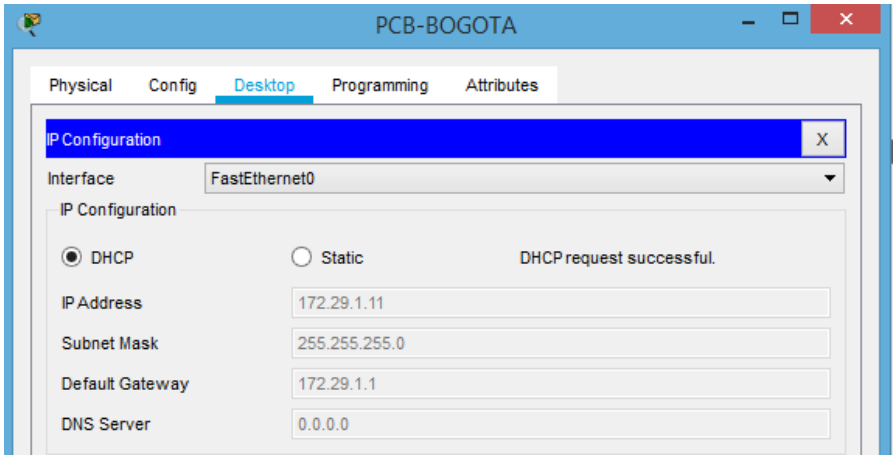
BOGOTA3(config-if)#

Figura 131 DHCP. Configuración dinámica exitosa PCA-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 132 DHCP. Configuración dinámica exitosa PCB-BOGOTA

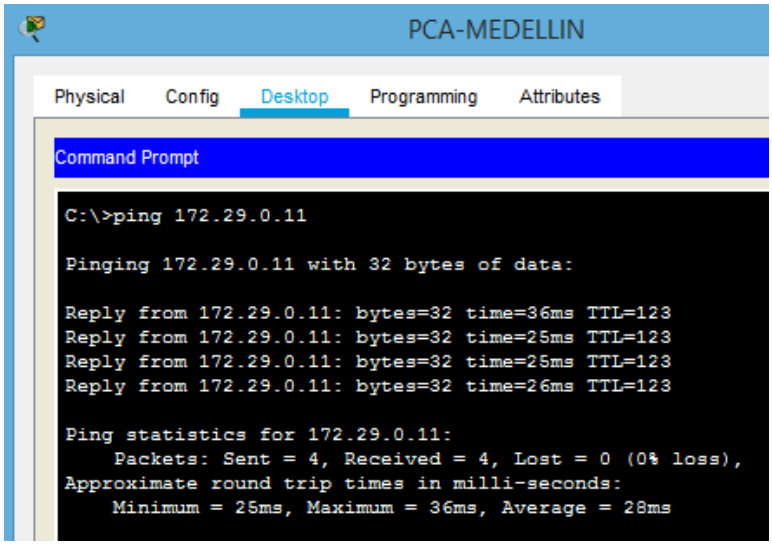


Fuente: Cisco Packet Tracer 7.0.2.0226.

Verificación Conectividad

- ✓ Ping PCA-MEDELLIN a PCA-BOGOTA.

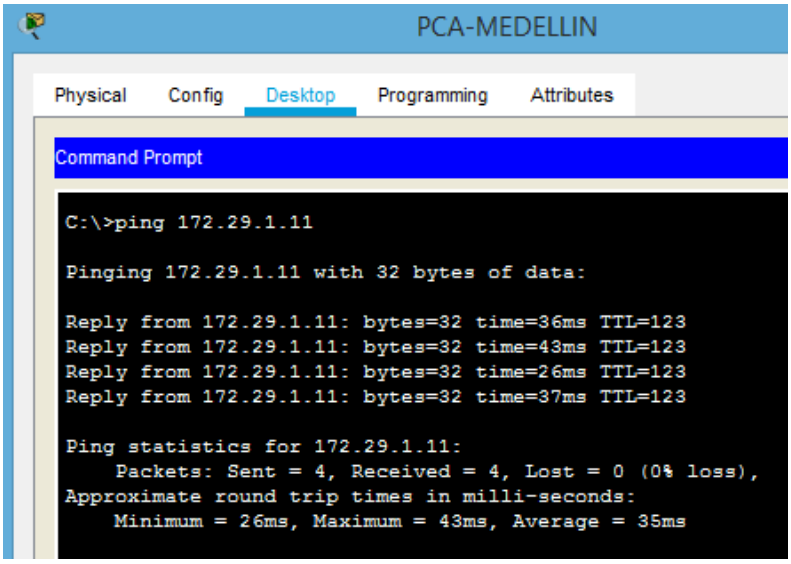
Figura 133 Verificación DHCP. Ping PCA-MEDELLIN a PCA-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Ping PCA-MEDELLIN a PCB-BOGOTA.

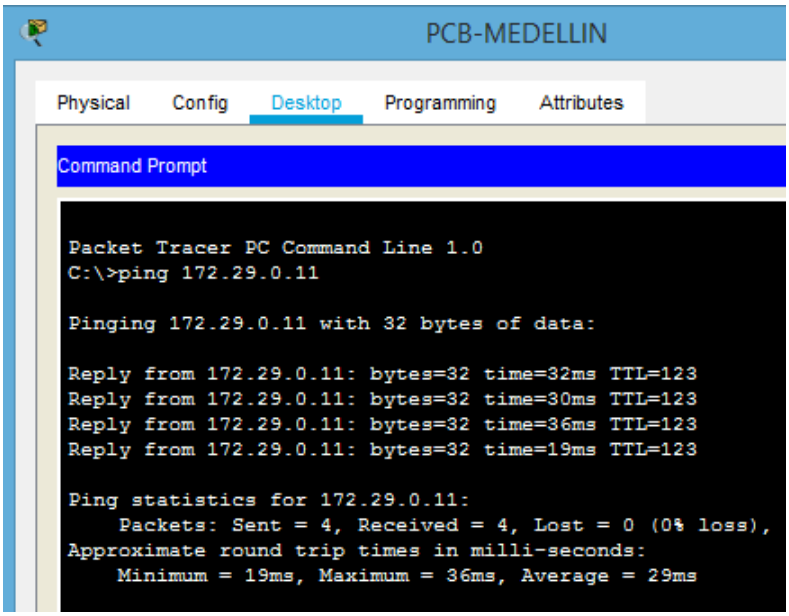
Figura 134 Verificación DHCP. Ping PCA-MEDELLIN a PCB-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Ping PCB-MEDELLIN a PCA-BOGOTA.

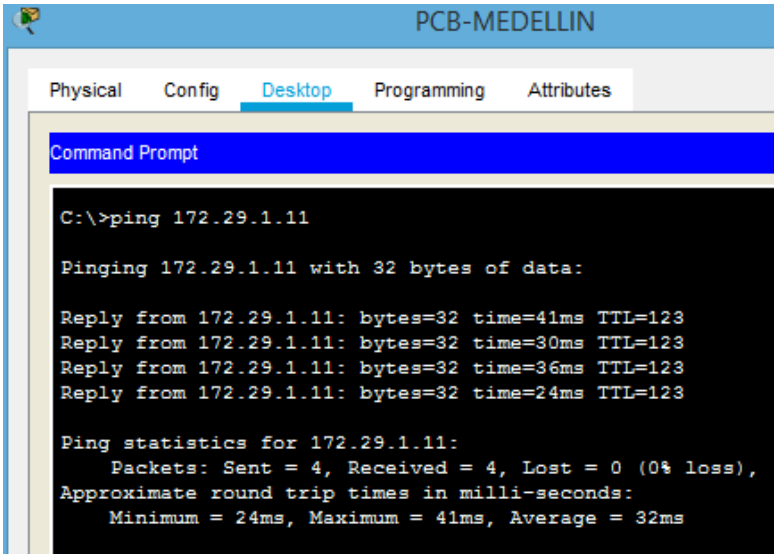
Figura 135 Verificación DHCP. Ping PCB-MEDELLIN a PCA-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Ping PCB-MEDELLIN a PCB-BOGOTA.

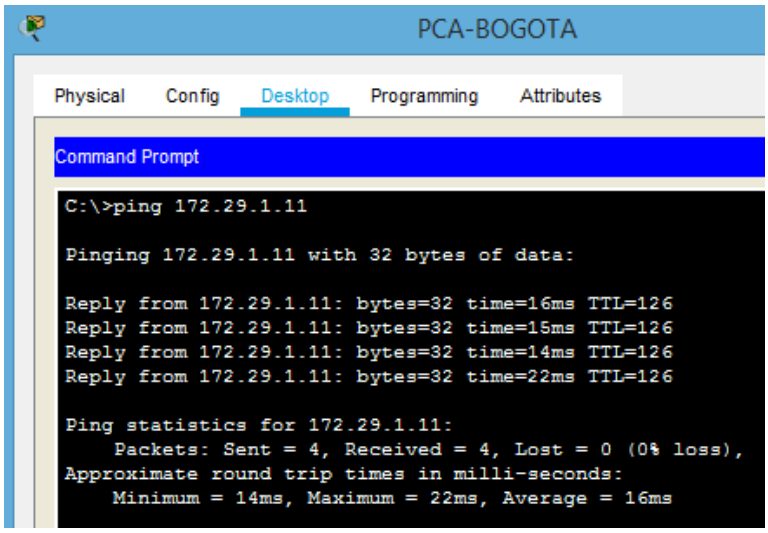
Figura 136 Verificación DHCP. Ping PCB-MEDELLIN a PCB-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Ping PCA-BOGOTA a PCB-BOGOTA.

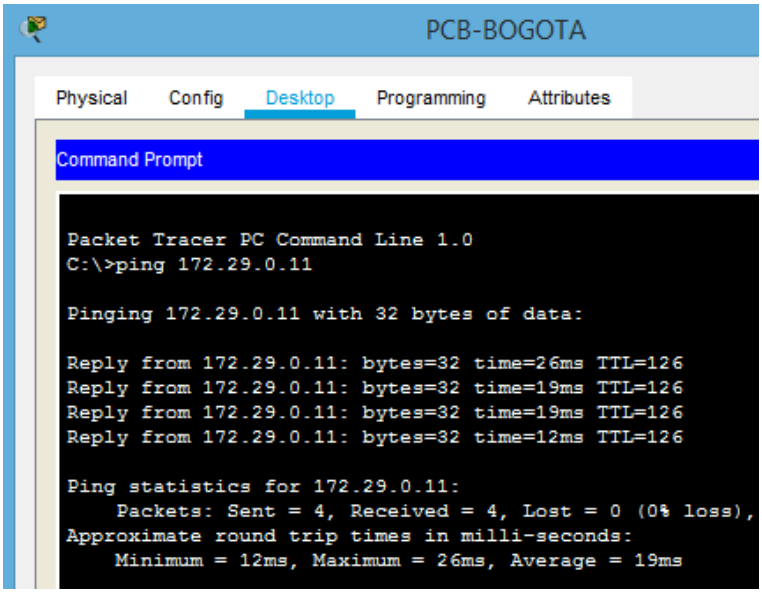
Figura 137 Verificación DHCP. Ping PCA-BOGOTA a PCB-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Ping PCB-BOGOTA a PCA-BOGOTA.

Figura 138 Verificación DHCP. Ping PCB-BOGOTA a PCA-BOGOTA



Fuente: Cisco Packet Tracer 7.0.2.0226.

d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

BOGOTA1#show running-config | include ip helper-address

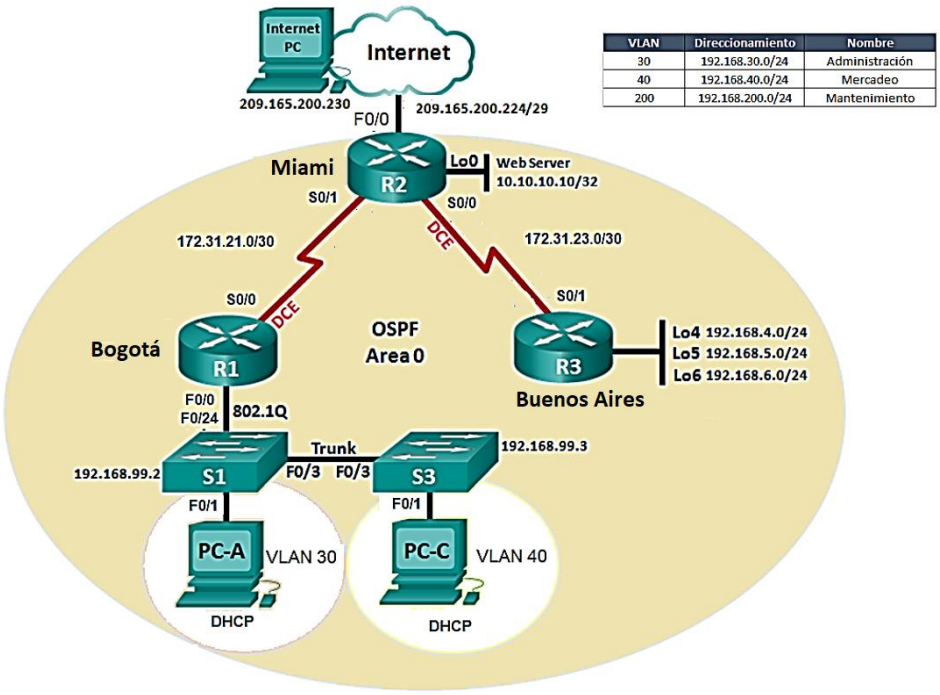
ip helper-address 172.29.6.2

BOGOTA1#

1.2. ESCENARIO 2

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, 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.

Figura 139 Topología Escenario 2



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

Fuente: Cisco. Evaluación – Prueba de Habildiades Prácticas CCNA.

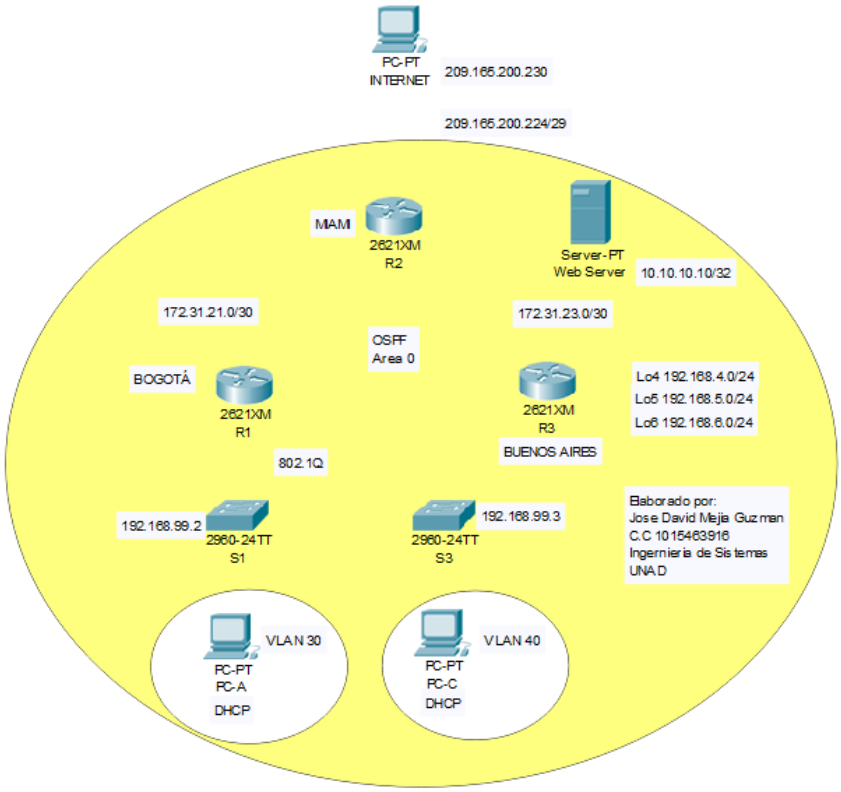
Recursos necesarios

- Cisco Packet Tracer Version 7.2.0.
- 3 Routers (Cisco 2621XM).
- 2 Switches (Cisco 2960 con Cisco IOS Release 15.0 (2) lanbasek9 image o similar).
- Ethernet y cables serie como se muestra en la topología.

Montar el cableado de red

En Packet Tracer se arrastran los elementos que componen la topología de red y se colocan notas para identificar los elementos, redes y subredes.

Figura 140 Esquema Topología de Red Escenario 2

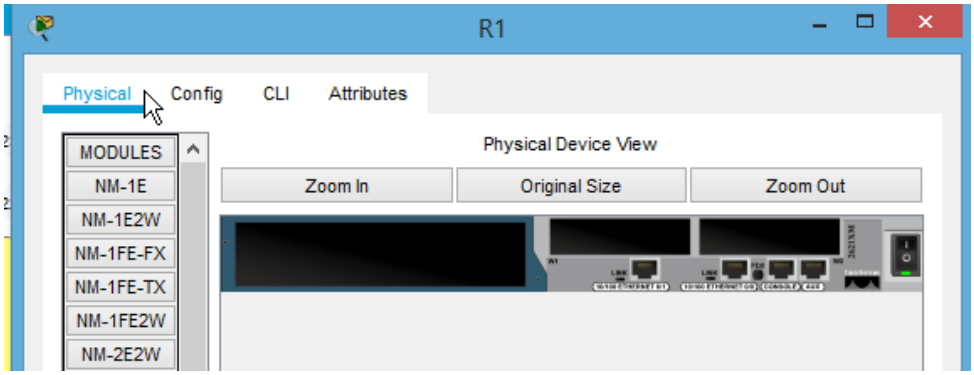


Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

En una conexión WAN se requieren enlaces seriales entre los routers, pero en Packet Tracer los routers **2621XM** no traen los módulos con interfaces seriales, pero están disponibles y se agregan de la siguiente manera:

- ✓ Se hace clic sobre el router y a continuación, se ubica la pestaña **Physical.**

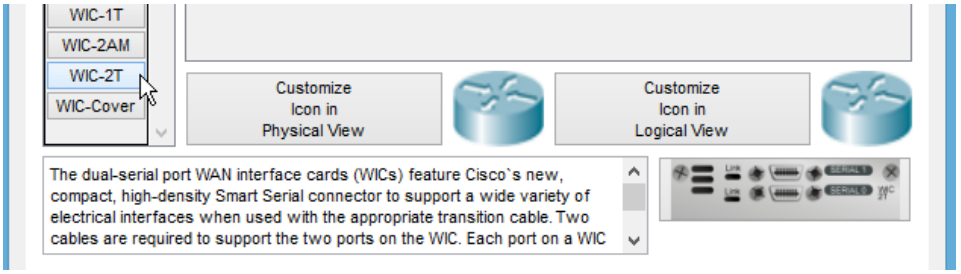
Figura 141 Pestña PhysIcal router 2621XM



Fuente: Cisco Packet Tracer 7.0.2.0226

- ✓ Se ubica el módulo WIC-2T. En la parte inferior de la ventana se muestra una breve descripción y la imagen del módulo.

Figura 142 Módulo WIC-2T router 2621XM

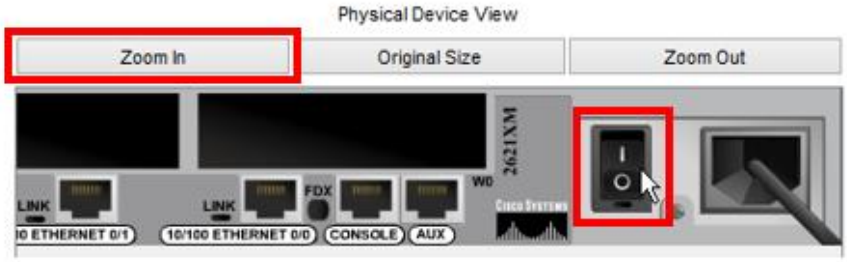


Fuente: Cisco Packet Tracer 7.0.2.0226.

Como se indica, las tarjetas de interfaz WAN (WIC) de doble puerto serie presentan el nuevo conector serial inteligente, compacto y de alta densidad de Cisco para admitir una amplia variedad de interfaces eléctricas cuando se usan con el cable de transición adecuado. Se requieren dos cables para soportar los dos puertos en el WIC. Cada puerto en un WIC es una interfaz física diferente y puede admitir diferentes protocolos, como el Protocolo punto a punto (PPP) o el Equipo de retransmisión de tramas y el Terminal de datos / Equipo de comunicaciones de datos (DTE / DCE).

- ✓ Se procede a agregar el módulo al router pero este debe estar apagado. Se hace clic en el botón **On/Off** para apagarlo. Cuando no se muestre el led verde, el router estará apagado. Se puede hacer clic en la pestaña **Zoom In** para una mejor visualización.

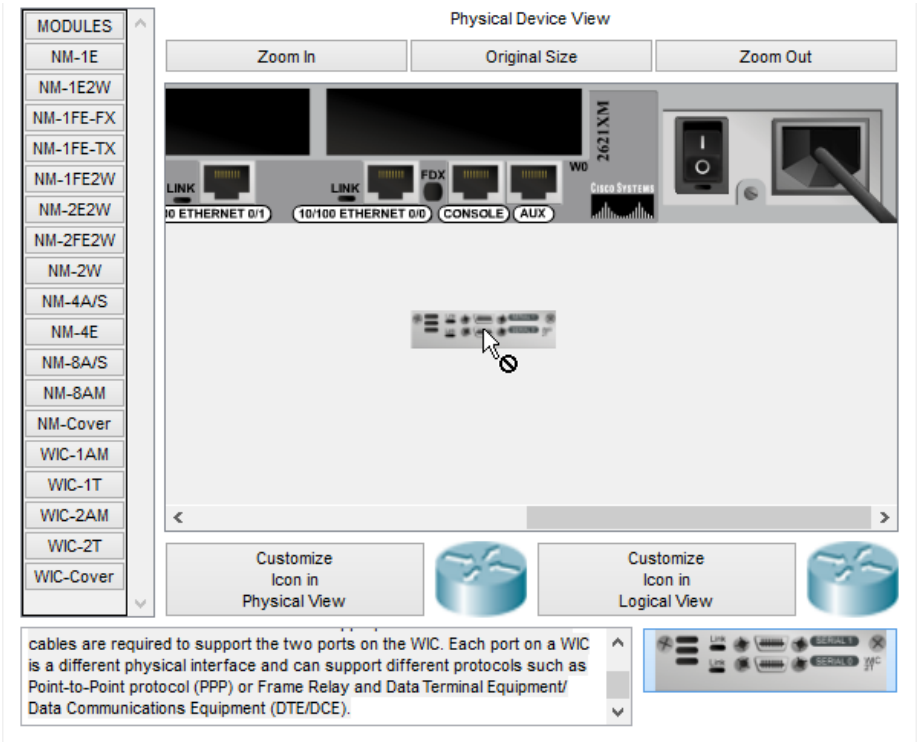
Figura 143 Apagado router 2621XM



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se selecciona el módulo, se arrastra y suelta en cualquiera de las ranuras.

Figura 144 Colocación módulo WIC-2T router 2621XM



Fuente: Cisco Packet Tracer 7.0.2.0226.

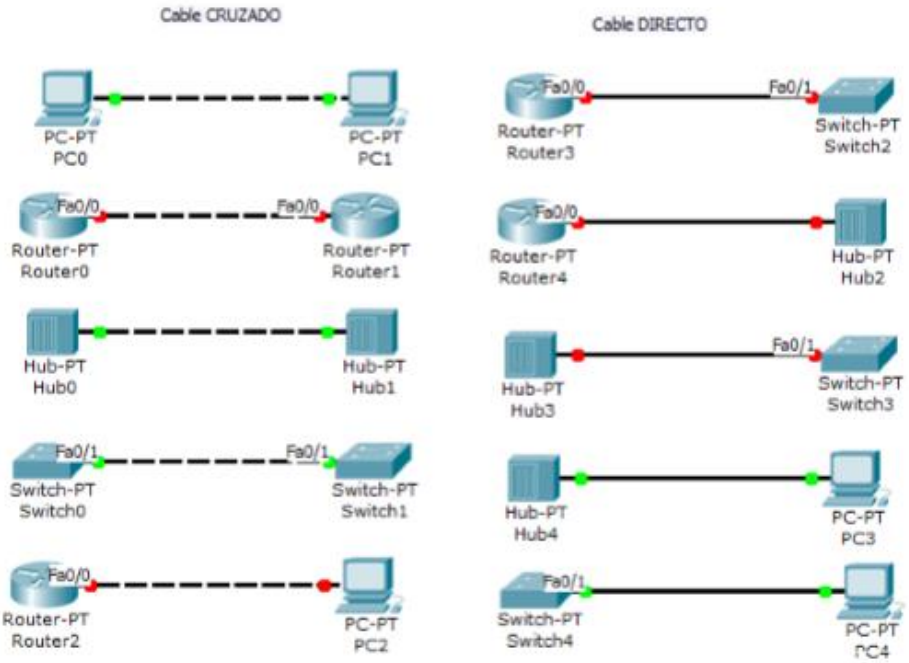
✓ Una vez colocado, se enciende el router.

Figura 145 Encendido de router 2621XM con módulo WIC-2T colocado

Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Se repite el procedimiento para los demás routers.

Figura 146 Conexiones entre dipositivos (Packet Tracer)

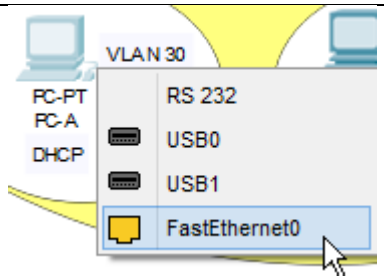
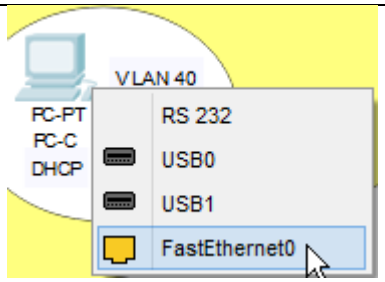


Fuente: http://blog.juliopari.com/packet-tracer-cable-cruzado-y-cable-directo/

Conexiones de PC a Switch

En Packet Tracer, dentro del apartado de conexiones se selecciona **Copper Straight-Through.**

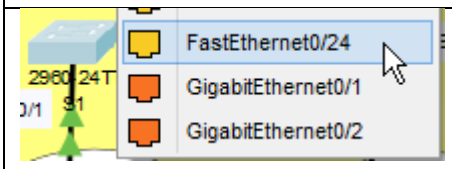
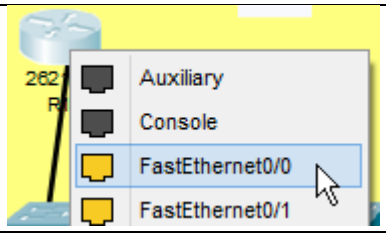
Tabla 24 Conexiones de PC a Switch

PC-A Interfaz FastEthernet0 a **S1** Interfaz FastEthernet0/1	
	
PC-C Interfaz FastEthernet0 a **S3** Interfaz FastEthernet0/1	
	

Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

Conexión de Switch a Router

Tabla 25 Conexión de Switch a Router

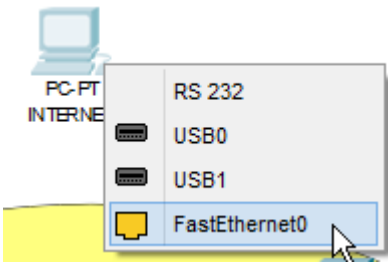
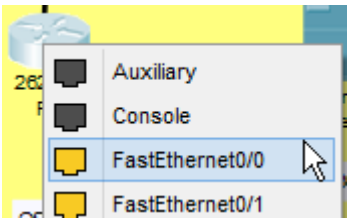
S1 Interfaz FastEthernet0/24 a **R1** Interfaz FastEthernet0/0	
	

Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

Conexión de PC a Router

En Packet Tracer, dentro del apartado de conexiones se selecciona **Copper Cross-Over.**

Tabla 26 Conexión de PC a Router

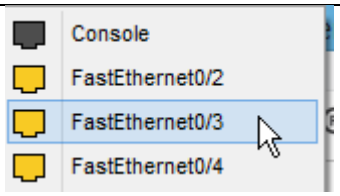
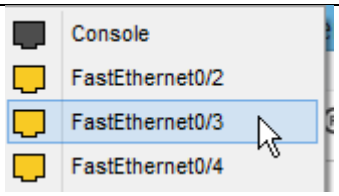
INTERNET Interfaz FastEthernet0 a **R2** Interfaz FastEthernet0/0	
	

Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

Conexión de Switch a Switch

En Packet Tracer, dentro del apartado de conexiones se selecciona **Copper Cross-Over.**

Tabla 27 Conexión de Switch a Switch

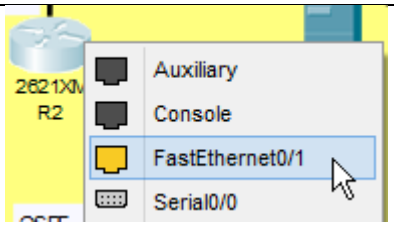
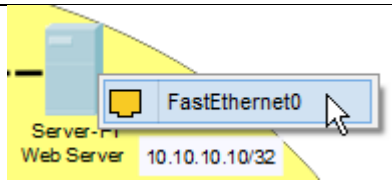
S1 Interfaz FastEthernet0/3 a **S3** Interfaz FastEthernet0/3	
	

Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

Conexión de Router a Server

En Packet Tracer, dentro del apartado de conexiones se selecciona **Copper Cross-Over.**

Tabla 28 Conexión de Router a Server

R2 Interfaz FastEthernet0/1 a **Web Server** FastEthernet0	
	

Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

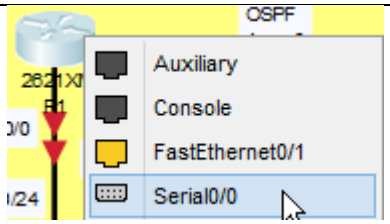
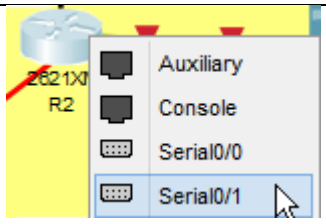
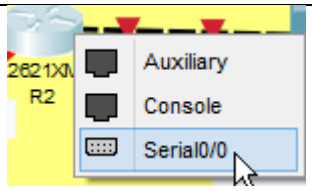
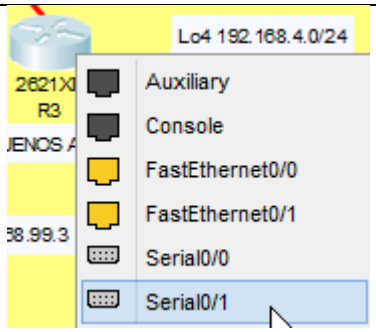
Conexiones de Router a Router

En esta topología los routers no se encuentran conectados directamente por lo que se deben utilizar conexiones seriales entre estos.

Las interfaces seriales requieren una señal de sincronización que controle la comunicación. En la mayoría de los casos, un dispositivo DCE brinda dicha señal.

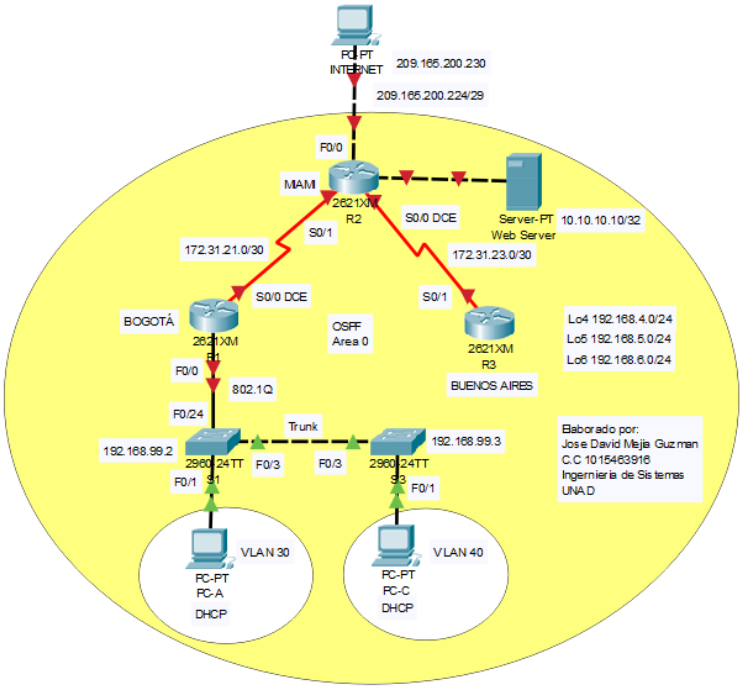
En Packet Tracer, dentro del apartado de conexiones se selecciona **Serial DCE**.

Tabla 29 Conexiones de Router a Router

R1 Interfaz Serial0/0 (DCE) a **R2** Interfaz Serial0/1	
	
R2 Interfaz Serial0/0 (DCE) a **R3** Interfaz Serial0/1	
	

Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

Tabla 30 Toplogía de Red Escenario 2 montada



Fuente: Autoria Propia. Cisco Packet Tracer 7.0.2.0226.

1.2.1. Parte 1: Configuración del direccionamiento IP

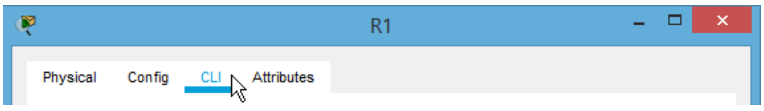
Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

- **Configuración de parámetros básicos**

Routers y Switches

- ✓ En Packet Tracer se hace clic sobre el dispositivo y a continuación, se ubica la pestaña **CLI.**

Figura 147 Pestaña CLI R1



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se ingresa al modo EXEC privilegiado con el comando **enable** o su abreviatura **en**. La petición de entrada cambia.

Dispositivo>en

Dispositivo #

- ✓ Se ingresa al modo de configuración global con el comando **configure** terminal o abreviado **config t**. La petición de entrada cambia.

Dispositivo #config t

Dispositivo (config)#

- ✓ Se cambia el nombre del host con el comando **hostname** *nombre-host.*
- ✓ Se deshabilita la búsqueda DNS con el comando de configuración global **no ip domain-lookup**. Esto se hace para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- ✓ Se asigna una contraseña para el modo EXEC privilegiado con el comando de configuración global **enable secret** *contraseña*.
- ✓ Se asigna una contraseña de consola. Para esto se ingresa al modo de configuración de consola con el comando de configuración global **line console 0** o abreviado **line con 0**:
  - ✓ Se asigna la contraseña con el comando **password** *contraseña.*
  - ✓ Se establece un tiempo de espera para la sesión con el comando **exec-timeout** *minutos segundos.*
  - ✓ Se habilita el inicio se sesión con el comando **login.**
  - ✓ Se sincroniza la depuración y el resultado del software IOS de Cisco, y evita que estos mensajes interrumpan la entrada del teclado con el comando **logging synchronous.**
  - ✓ Se sale de la configuración de consola con el comando **exit**.
- ✓ Se asigna una contraseña a las líneas vty. Esta configuración permite el acceso remoto. Se ingresa al modo de configuración de línea con el comando **line vty 0 15.**
  - ✓ Se repiten los pasos de la configuración de consola.
- ✓ Se cifran las contraseñas actuales y futuras de texto no cifrado con el comando de configuración global **service password-encryption.**
- ✓ Se crea un mensaje del día con el comando de configuración global **banner motd #***mensaje***#**. El carácter delimitador # puede cambiarse por otro que sea válido en la versión de IOS. Este mensaje advierte a aquel que acceda al dispositivo que el acceso no autorizado está prohibido.

- ✓ Se procede con la configuración de direccionamiento ingresando al modo de configuración de interfaz con el comando de configuración global **interface** *id-interfaz.* Solo para routers,
  - ✓ Se añade una descripción a la interfaz con el comando **description** *descripción.*
  - ✓ Se asigna la dirección IP y la máscara de subred con el comando **ip address** *dirección-IP mascara.*
  - ✓ En las **interfaces seriales** se debe configurar la frecuencia del reloj con el comando **clock rate** *frecuencia*.
  - ✓ Se activa la interfaz con el comando **no shutdown** o abreviado **no shut. Nota:** las interfaces seriales cuando se comienzan a activar se puede mostrar que su estado cambio de **Administratively Down** a **Down**, esto se debe a que se deben activar las demás interfaces seriales para que se active automáticamente.
  - ✓ Se regresa al modo EXEC privilegiado con el comando **end.**
- ✓ Se guarda la configuración de ejecución en la NVRAM con el comando del modo EXEC privilegiado **copy running-config startup-config.** Se especifica el destino o se puede dejar en blanco.

Se asignaron esas contraseñas y tiempos de espera con fines prácticos y de aprendizaje.

La hora se recomienda configurarla con un servidor de NTP para que se sincronicen los relojes.

S1 configuración parámetros básicos

Switch>en

Switch#config t

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

Switch(config)#hostname S1

S1(config)#no ip domain-lookup

S1(config)#enable secret jdmgcisco2019

S1(config)#line con 0

S1(config-line)#password jdmgclass2019

S1(config-line)#exec-timeout 10 0

S1(config-line)#login

S1(config-line)#logging synchronous

S1(config-line)#exit

S1(config)#line vty 0 15

S1(config-line)#password jdmgunad2019

S1(config-line)#exec-timeout 15 0

S1(config-line)#login

S1(config-line)#logging synchronous

S1(config-line)#exit

S1(config)#service password-encryption

S1(config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

S1(config)#end

S1#

%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

S1#

S3 configuración parámetros básicos

Switch>en

Switch#config t

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

Switch(config)#hostname S1

S3(config)#no ip domain-lookup

S3(config)#enable secret jdmgcisco2019

S3(config)#line con 0

S3(config-line)#password jdmgclass2019

S3(config-line)#exec-timeout 10 0

S3(config-line)#login

S3(config-line)#logging synchronous

S3(config-line)#exit

S3(config)#line vty 0 15

S3(config-line)#password jdmgunad2019

S3(config-line)#exec-timeout 15 0

S3(config-line)#login

S3(config-line)#logging synchronous

S3(config-line)#exit

S3(config)#service password-encryption

S3(config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

S3(config)#end

S3#

%SYS-5-CONFIG_I: Configured from console by console

S3#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

S3#

R1

Configuración Parámetros Básicos

Router>en

Router#config t

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

Router(config)#hostname R1

R1(config)#no ip domain-lookup

R1(config)#enable secret jdmgcisco2019

R1(config)#line con 0

R1(config-line)#password jdmgclass2019

R1(config-line)#exec-timeout 10 0

R1(config-line)#login

R1(config-line)#logging synchronous

R1(config-line)#exit

R1(config)#line vty 0 15

R1(config-line)#password jdmgunad2019

R1(config-line)#exec-timeout 15 0

R1(config-line)#login

R1(config-line)#logging synchronous

R1(config-line)#exit

R1(config)#service password-encryption

R1(config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

Configuración Direccionamiento

ENLACE LAN R1– S1

- ✓ Interfaz F0/0

Red: 192.168.30.0/24.

Mascara: 255.255.255.0.

R1(config)#int f0/0

R1(config-if)#description ENLACE LAN R2 - S1 RED 192.168.30.0/24

R1(config-if)#ip address 192.168.30.1 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

ENLACE WAN R1 – R2

- ✓ Interfaz S0/0 DCE

Subred: 172.31.21.0/30.

Mascara: 255.255.255.252.

R1(config-if)#int s0/0

R1(config-if)#description ENLACE WAN R1 - R2 SUBRED 172.31.21.0/30

R1(config-if)#ip address 172.31.21.1 255.255.255.252

R1(config-if)#clock rate 250000

R1(config-if)#no shutdown

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

Configuración guardada en la NVRAM

R1(config-if)#end

R1#

%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

R1#

Activación de la interfaz Serial0/0 DCE después de activar la interfaz Serial0/1 de R2.

R1#

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

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

R1#

R2

Configuración Parámetros Básicos

Router>en

Router#config t

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

Router(config)#hostname R2

R2(config)#no ip domain-lookup

R2(config)#enable secret jdmgcisco2019

R2(config)#line con 0

R2(config-line)#password jdmgclass2019

R2(config-line)#exec-timeout 10 0

R2(config-line)#login

R2(config-line)#logging synchronous

R2(config-line)#exit

R2(config)#line vty 0 15

R2(config-line)#password jdmgunad2019

R2(config-line)#exec-timeout 15 0

R2(config-line)#login

R2(config-line)#logging synchronous

R2(config-line)#exit

R2(config)#service password-encryption

R2(config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

Configuración Direccionamiento

ENLACE WAN R2 – R1

- ✓ Interfaz S0/1

Subred: 172.31.21.0/30.

Mascara: 255.255.255.252.

R2(config)#int s0/1

R2(config-if)#description ENLACE WAN R2 - R1 SUBRED 172.31.21.0/30

R2(config-if)#ip address 172.31.21.2 255.255.255.252

R2(config-if)#no shutdown

R2(config-if)#

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

R2(config-if)#

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

ENLACE LAN PC-INTERNET – R2

- ✓ Interfaz F0/0

Subred: 209.165.200.224/29.

Mascara 255.255.255.248.

R2(config-if)#int f0/0

R2(config-if)#description ENLACE LAN PC- INTERNET - R2 SUBRED 209.165.200.224/29

R2(config-if)#ip address 209.165.200.225 255.255.255.248

R2(config-if)#no shutdown

R2(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

ENLACE LAN R2 – Web Server

- ✓ Interfaz F0/1

Subred: 10.10.10.10/32.

Mascara 255.0.0.0

Se asigna la máscara correspondiente a la red porque no hay definida una macara con prefijo /32.

R2(config-if)#int f0/1

R2(config-if)#description ENLACE LAN R2 - Web Server SUBRED 10.10.10.10/32

R2(config-if)#ip address 10.10.10.1 255.0.0.0

R2(config-if)#no shutdown

R2(config-if)#

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

ENLACE WAN R2 – R3

- ✓ Interfaz S0/0 DCE

Subred: 172.31.23.0/30.

Mascara 255.255.255.252.

R2(config-if)#int s0/0

R2(config-if)#description ENLACE WAN R2 - R3 SUBRED 172.31.23.0/30

R2(config-if)#ip address 172.31.23.1 255.255.255.252

R2(config-if)#clock rate 250000

R2(config-if)#no shutdown

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

Configuración guardada en la NVRAM

R2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

R2#

Activación de la interfaz Serial0/0 DCE después de activar la interfaz Serial0/1 de R3.

R2#

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

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

R2#

R3

Configuración Parámetros Básicos

Router>en

Router#config t

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

Router(config)#hostname R3

R3(config)#no ip domain-lookup

R3(config)#enable secret jdmgcisco2019

R3(config)#line con 0

R3(config-line)#password jdmgclass2019

R3(config-line)#exec-timeout 10 0

R3(config-line)#login

R3(config-line)#logging synchronous

R3(config-line)#exit

R3(config)#line vty 0 15

R3(config-line)#password jdmgunad2019

R3(config-line)#exec-timeout 15 0

R3(config-line)#login

R3(config-line)#logging synchronous

R3(config-line)#exit

R3(config)#service password-encryption

R3(config)#banner motd #El acceso no autorizado esta estrictamente prohibido !#

Configuración Direccionamiento

ENLACE WAN R3 – R2

- ✓ Interfaz S0/1

Subred: 172.31.23.0/30.

Mascara 255.255.255.252.

R3(config)#int s0/1

R3(config-if)#description ENLACE WAN R3 - R2 SUBRED 172.31.23.0/30

R3(config-if)#ip address 172.31.23.2 255.255.255.252

R3(config-if)#no shutdown

R3(config-if)#

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

R3(config-if)#

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

Configuración de las interfaces loopback.

La interfaz loopback es una interfaz lógica interna del router. Esta no se asigna a un puerto físico y, por ende, no se puede conectar a otro dispositivo. Se la considera una interfaz de software que se coloca automáticamente en estado UP (activo), siempre que el router esté en funcionamiento.
Para configurar una interfaz loopback en un router se realiza lo siguiente:

- ✓ Se ingresa al modo de configuración global con el comando de modo EXEC privilegiado **config t.**
- ✓ Se asigna la interfaz con el comando **int loopback** *numero.*
- ✓ Se mostrarán dos avisos de notificación indicando la activación de la interfaz.
- ✓ Dentro del modo de configuración de interfaz se establece la dirección IP y la mascara de red con el comando **ip address** *Direccion-IP Mascara-Red*

R3#config t

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

R3(config)#int loopback 4

R3(config-if)#

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

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

R3(config-if)#ip address 192.168.4.1 255.255.255.0

R3(config-if)#exit

R3(config)#int loopback 5

R3(config-if)#

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

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

R3(config-if)#ip address 192.168.5.1 255.255.255.0

R3(config-if)#exit

R3(config)#int loopback 6

R3(config-if)#

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

R3(config-if)#ip address 192.168.6.1 255.255.255.0

R3(config-if)#exit

R3(config)#

Configuración guardada en la NVRAM

R3#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

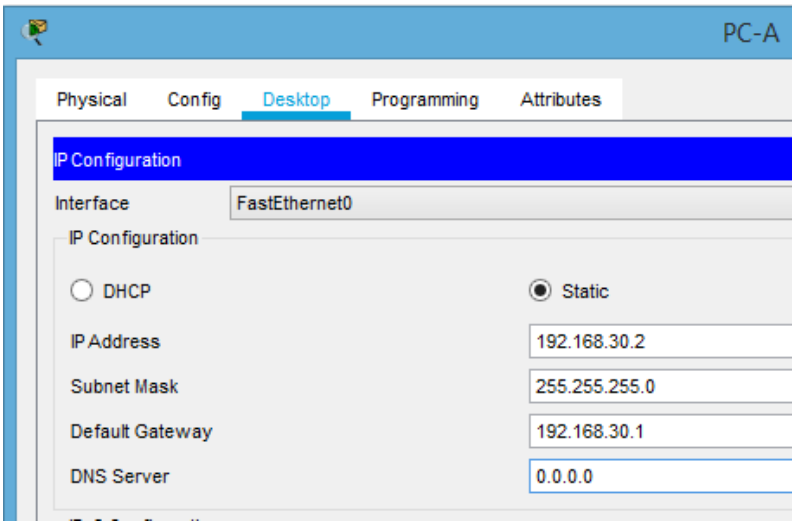
[OK]

R3#

Direccionamiento PC-A

La PC-A hace parte de la VLAN 30 cuyo direccionamiento es 192.168.30.0/24. Por el momento se configura de manera estática, más adelante estos parámetros cambian por la configuración DHCP.

Figura 148 Direccionamiento PC-A



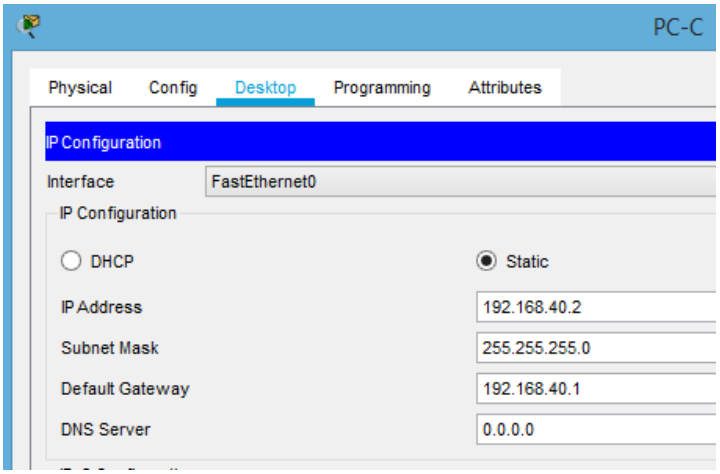
Fuente: Cisco Packet Tracer 7.0.2.0226.

Direccionamiento PC-C

La PC-C hace parte de la VLAN 40 cuyo direccionamiento es 192.168.40.0/24.

La dirección de Gateway Predeterminado es la dirección de la VLAN asociada.

Figura 149 Direccionamiento PC-C

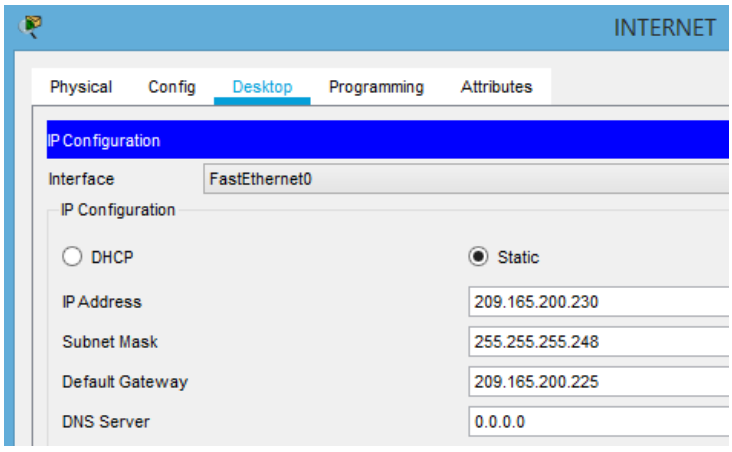


Fuente: Cisco Packet Tracer 7.0.2.0226.

Direccionamiento PC-INTERNET

Red: 209.165.200.224.
Mascara 255.255.255.248.

Figura 150 Direccionamiento PC-INTERNET



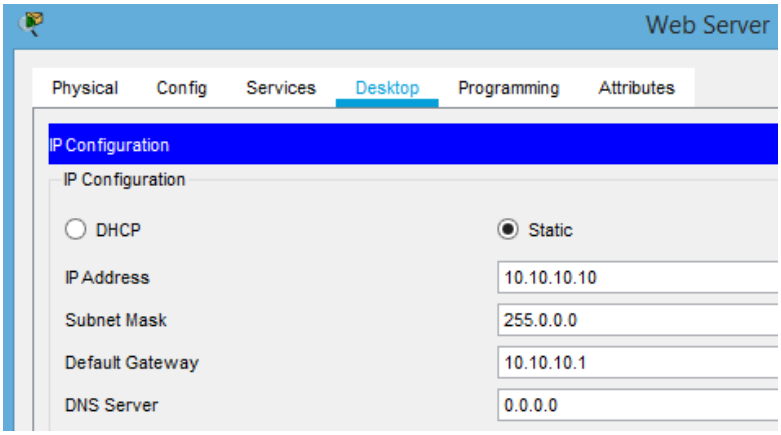
Fuente: Cisco Packet Tracer 7.0.2.0226.

Direccionamiento Web Server

Red: 10.10.10.10.
Mascara 255.0.0.0.

La dirección de Gateway Predeterminado es la dirección del router asociado a la PC.

Figura 151 Direccionamiento Web Server



Fuente: Cisco Packet Tracer 7.0.2.0226.

Tabla de Direccionamiento

Tabla 31 Tabla de Direccionamiento Escenario 2

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway Ped.
R1	F0/0	192.168.30.1	255.255.255.0	No Aplica
	S0/0 DCE	172.31.21.1	255.255.255.252	No Aplica
R2	F0/0	209.165.200.225	255.255.255.248	No Aplica
	F0/1	10.10.10.1	255.0.0.0	No Aplica
	S0/1	172.31.21.2	255.255.255.252	No Aplica
	S0/0 DCE	172.31.23.1	255.255.255.252	No Aplica
R3	S0/1	172.31.23.2	255.255.255.252	No Aplica
	Lo4	192.168.4.0	255.255.255.0	No Aplica
	Lo5	192.168.5.0	255.255.255.0	No Aplica
	Lo6	192.168.6.0	255.255.255.0	No Aplica
Web Server	F0/0	10.10.10.10	255.255.255.0	10.10.10.1
PC-INTERNET	NIC	209.165.200.230	255.255.255.248	209.165.200.225

PC-A	NIC	192.168.30.2	255.255.255.0	192.168.30.1
PC-C	NIC	192.168.40.2	255.255.255.0	192.168.40.1

Fuente: Autoría Propia.

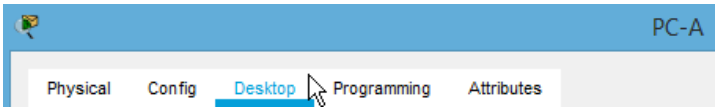
- **Verificación conectividad antes de configuración de protocolo OSPFv2**

Los routers deben poder hacerse ping entre sí, y cada computadora debe poder hacer ping a su gateway predeterminado. Las computadoras no pueden hacer ping a otras computadoras hasta que no se haya configurado el routing OSPF.

PING DESDE UNA PC

✓ Se hace clic sobre el host y a continuación se ubica la pestaña **Desktop.**

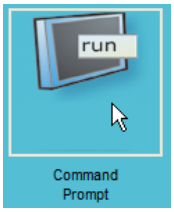
Figura 152 Conectividad sin OSPFv2. Pestaña Desktop PC-A



Fuente: Cisco Packet Tracer 7.0.2.0226.

✓ Se hace clic en el botón **Command Prompt** (Consola de Comandos).

Figura 153 Conectividad sin OSPFv2. Botón Command Prompt PC-A



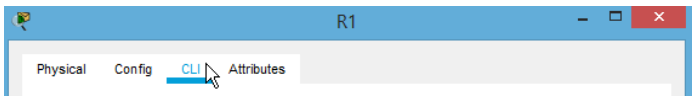
Fuente: Cisco Packet Tracer 7.0.2.0226.

En la consola se escribe el comando **ping** seguido de la dirección IP del dispositivo con el cual se desea probar la conectividad.

PING DESDE UN ROUTER

✓ Se hace clic sobre el router y a continuación se ubica la pestaña **CLI.**

Figura 154 Conectividad sin OSPFv2. Pestaña CLI R1



Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se ingresa la contraseña de consola y a continuación, se escribe el comando **ping** seguido de la dirección IP del dispositivo con el cual se desea probar la conectividad.

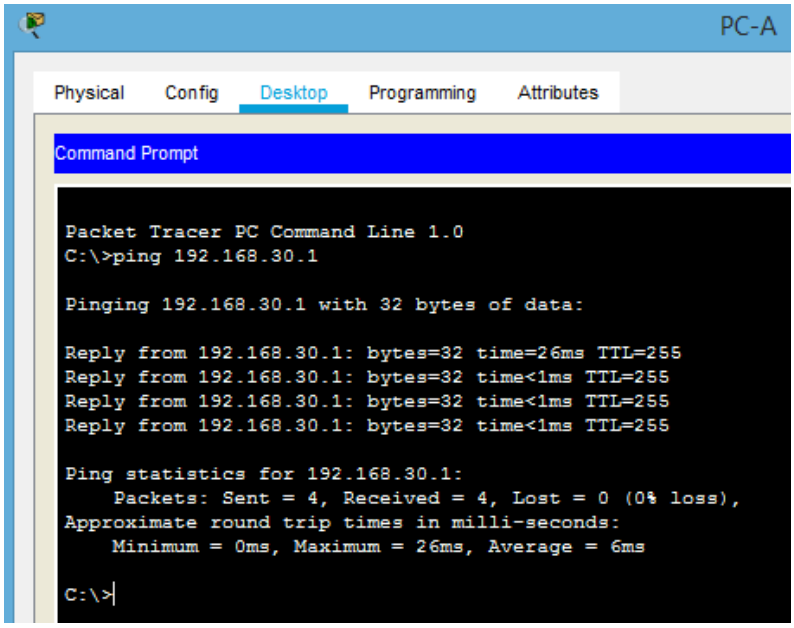
Figura 155 Conectividad sin OSPFv2. CLI R1

```
Press RETURN to get started!

El acceso no autorizado esta estrictamente prohibido !

User Access Verification

Password:

R1>ping direccion-ip
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping PC-A a R1

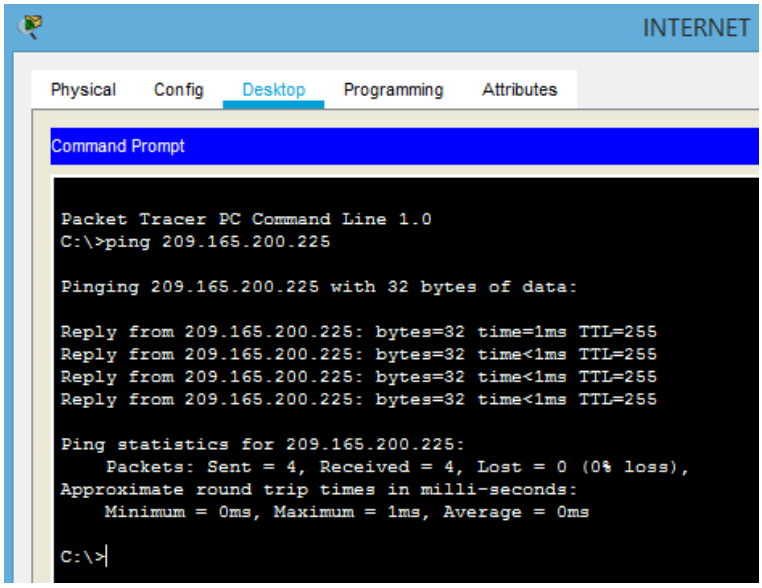
Figura 156 Conectividad sin OSPFv2. Ping exitoso PC-A a R1



Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping PC-INTERNET a R2

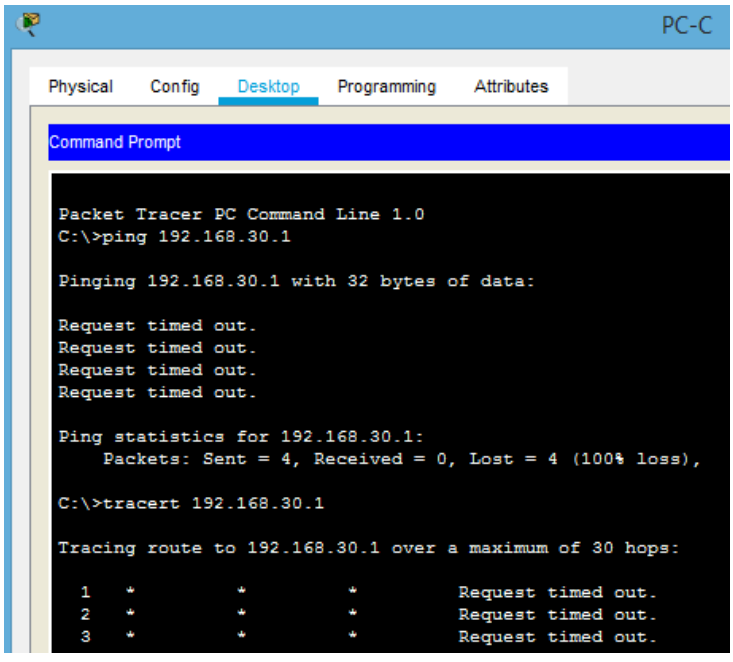
Figura 157 Conectividad sin OSPFv2. Ping exitoso PC-INTERNET a R2



Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping PC-C a R1

Figura 158 Conectividad sin OSPFv2. Ping y Tracert Fallido PC-C a R1



Fuente: Cisco Packet Tracer 7.0.2.0226.

Diagnostico

Este ping no funciona porque el switch no está configurado con una VLAN y un enlace troncal. Este proceso se realiza más adelante.

Ping R1 a PC1

Figura 159 Conectividad sin OSPFv2. Ping R1 a PC1

```
R1>ping 192.168.30.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping R1 a R2

Figura 160 Conectividad sin OSPFv2. Ping R1 a R2

```
R1>ping 172.31.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping R1 a R3

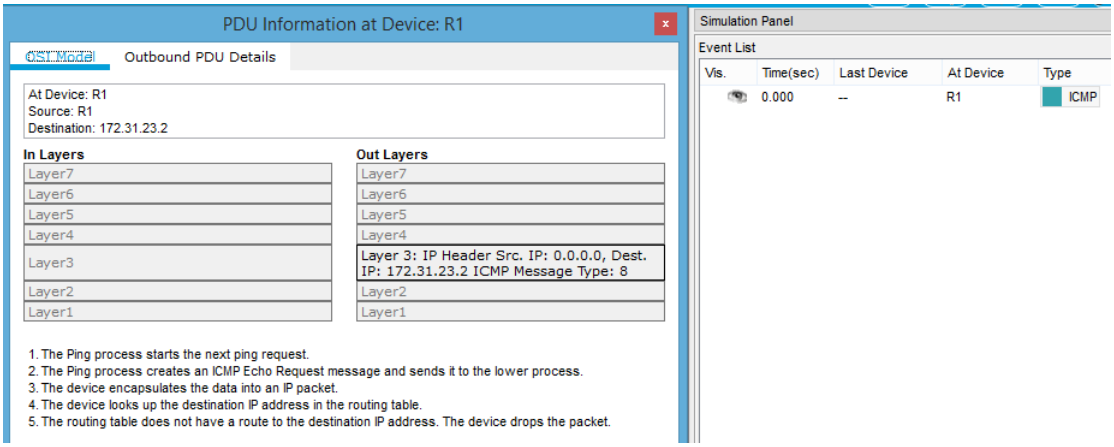
Figura 161 Conectividad sin OSPFv2. Ping fallido R1 a R3

```
R1>ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Diagnostico

Figura 162 Conectividad sin OSPFv2. Diagnóstico ping R1 a R3 O



Fuente: Cisco Packet Tracer 7.0.2.0226.

Este ping no funciona porque no hay una ruta en la tabla de routing, según lo indican los mensajes ECO y el numeral 6 de la PDU.

Se soluciona configurando una ruita estática hacia R3 y una ruta estática de R3 hacia R1.

Se revisa la tabla de routing del router con el comando de modo EXEC privilegiado **show ip route.**

Figura 163 Conectividad sin OSPFv2. Tabla de routing R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.31.0.0/30 is subnetted, 1 subnets
C       172.31.21.0 is directly connected, Serial0/0
C    192.168.30.0/24 is directly connected, FastEthernet0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

R1 no tiene conocimiento de la subred 172.31.23.0 que es el Enlace WAN entre R2 y R3.

Se debe configurar una ruta estática de siguiente salto donde se especifica la dirección de siguiente salto que debe seguir el paquete y la interfaz de salida deriva del próximo salto.

R2 si tiene conocimiento de la red 172.31.23.0. Esta información se corrobora revisando la tabla de routing de R2.

Figura 164 Conectividad sin OSPFv2. Tabla de routing R2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
     172.31.0.0/30 is subnetted, 2 subnets
C       172.31.21.0 is directly connected, Serial0/1
C       172.31.23.0 is directly connected, Serial0/0
     209.165.200.0/29 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, FastEthernet0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

De esta manera, se configura la ruta en R1 de la siguiente manera:

- ✓ Se ingresa al modo de configuracion global.
- ✓ Se escribe el comando **ip route** seguido de la dirección de red, la máscara y a la dirección de siguiente salto, en este caso esta dirección corresponde a la interfaz s0/1 de R2.

R1(config)#ip route 172.31.23.0 255.255.255.252 172.31.21.2

R1(config)#exit

R1#

%SYS-5-CONFIG_I: Configured from console by console

✓ Se revisa nuevamente la tabla de routing.

Figura 165 Conectividad sin OSPFv2. Tabla de routing R1 con ruta S

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.31.0.0/30 is subnetted, 2 subnets
C       172.31.21.0 is directly connected, Serial0/0
S       172.31.23.0 [1/0] via 172.31.21.2
C    192.168.30.0/24 is directly connected, FastEthernet0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Este proceso debe realizarse en el otro router porque si se hace ping después de configurar esta ruta, el paquete llegará a R3 pero este no podrá enviar un acuse de recibo porque no conoce la red 172.31.21.0 como se aprecia en su tabla de routing.

Figura 166 Conectividad sin OSPFv2. Tabla de routing R3

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.31.0.0/30 is subnetted, 1 subnets
C       172.31.23.0 is directly connected, Serial0/1
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

R3 no tiene conocimiento de la subred 172.31.21.0 que es el Enlace WAN entre R2 y R1. Se configura la ruta estática hacia la red indicando como dirección de siguiente salto la interfaz s0/0 de R2.

R3(config)#ip route 172.31.21.0 255.255.255.252 172.31.23.1

R3(config)#exit

R3#

%SYS-5-CONFIG_I: Configured from console by console

- ✓ Se revisa nuevamente la tabla de routing.

Figura 167 Conectividad sin OSPFv2. Tabla de routing R3 con nueva ruta S

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.31.0.0/30 is subnetted, 2 subnets
S       172.31.21.0 [1/0] via 172.31.23.1
C       172.31.23.0 is directly connected, Serial0/1
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Se repite el ping:

Figura 168 Conectividad sin OSPFv2. Ping exitoso R1 a R3

```
R1#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/17 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping R2 a PC-INTERNET

Figura 169 Conectividad sin OSPFv2. Ping exitoso R2 a PC-INTERNET

```
R2>ping 209.165.200.230

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/6 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping R2 a Web Server

Figura 170 Conectividad sin OSPFv2. Ping exitoso R2 a Web Server

```
R2>ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/10/30
ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping R2 a R3

Figura 171 Conectividad sin OSPFv2. Ping exitoso R2 a R3

```
R2>ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/19 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping R2 a R1

Figura 172 Conectividad sin OSPFv2. Ping exitoso R2 a R1

```
R2>ping 172.31.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping R3 a R1

Figura 173 Conectividad sin OSPFv2. Ping exitoso R3 a R1

```
R3#ping 172.31.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/10/41
ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

S se hubiera realizado primero este ping antes que el ping de R1 a R3 se visualizaría el siguiente resultado y se deberían configurar las rutas estáticas tal cual como se realizó anteriormente.

Figura 174 Conectividad sin OSPFv2. Ping fallido R3 a R1

```
R3>ping 172.31.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping R3 a R2

Figura 175 Conectividad sin OSPFv2. Ping exitoso R3 a R2

```
R3>ping 172.31.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

1.2.2. Parte 2: Configuración de enrutamiento

Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 area 0

Tabla 32 Parámetros Configuración Protocolo OSPFv2

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

Fuente: Cisco. Evaluación – Prueba de Habildiades Prácticas CCNA.

- ✓ Se ingresa al modo de configuración global.
- ✓ Se ingresa al modo de configuración de router con el comando **router ospf** *ID-proceso-OSPF*.

El ID del proceso OSPF se mantiene localmente y no tiene sentido para los otros routers de la red.

- ✓ Se especifica el ID del router con el comando **router-id** *id-router.*

- ✓ Se configuran las instrucciones **network** para las redes en el router con el comando **network** *dirección-red mascara-wildcard ID-area.*
- ✓ Se configuran las interfaces pasivas con el comando passive**-interface** *id-interfaz*.
- ✓ Se ajusta el ancho de banda de referencia con el comando **auto-cost reference-bandwidth** *ancho-banda-Mb/s.*
- ✓ Se sale del modo de configuración del router con el comando **exit.**
- ✓ Se ingresa al modo de configuración de interfaz con el comando **interface** *id-interfaz*.
- ✓ Se configura el ancho de banda con el comando **bandwidth** *ancho-banda***.**
- ✓ Se ajusta el costo de la métrica con el comando **id ospf cost** *metrica*.

Instrucciones Network

Se configuran de acuerdo con las redes conectadas directamente en el router. En el modo de configuración de router se utiliza el comando **do show ip route connected** para ver las redes y las rutas.

Máscara de Wildcard

Es una cadena de 32 dígitos binarios que el router utiliza para determinar qué bits de la dirección debe examinar para obtener una coincidencia para llevar a cabo determinada acción. Se usa para configurar listas de control de acceso (ACLs) y al configurar el protocolo de enrutamiento OSPF.

Para determinarla de la manera más sencilla, se resta la máscara de red o subred a 255.255.255.255. Ejemplo:

Red: 192.168.34.0/26

Mascara de Subred: 255.255.255.192

Calculo:

	255	.	255	.	255	.	255
-	255	.	255	.	255	.	192
	0	.	0	.	0	.	63

R1

R1#config t

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

R1(config)#router ospf 1

R1(config-router)#router-id 1.1.1.1

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

C 172.31.21.0/30 is directly connected, Serial0/0

C 192.168.30.0/24 is directly connected, FastEthernet0/0

Determinación máscaras de wildcard

ENLACE WAN R1 – R2

- ✓ Interfaz S0/0 DCE

Subred: 172.31.21.0/30.

Mascara: 255.255.255.252.

Mascara de Wildcard

	255	.	255	.	255	.	255
-	255	.	255	.	255	.	252
	0	.	0	.	0	.	3

ENLACE LAN R1– S1

- ✓ Interfaz F0/0

Red: 192.168.30.0/24.

Mascara: 255.255.255.0.

Mascara de Wildcard

	255	.	255	.	255	.	255
-	255	.	255	.	255	.	0
	0	.	0	.	0	.	255

R1(config-router)#network 172.31.21.0 0.0.0.3 area 0

R1(config-router)#network 192.168.30.0 0.0.0.255 area 0

R1(config-router)#passive-interface f0/0

R1(config-router)#auto-cost reference-bandwidth 9500

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

R1(config-router)#exit

R1(config)#int s0/0

R1(config-if)#bandwidth ?

<1-10000000> Bandwidth in kilobits

R1(config-if)#bandwidth 256

R1(config-if)#ip ospf cost 9500

R1(config-if)#

20:33:57: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0 from LOADING to FULL, Loading Done

R1(config-if)#

R2

R2#config t

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

R2(config)#router ospf 1

R2(config-router)#router-id 5.5.5.5

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

C 10.0.0.0/8 is directly connected, FastEthernet0/1

C 172.31.21.0/30 is directly connected, Serial0/1

C 172.31.23.0/30 is directly connected, Serial0/0

C 209.165.200.224/29 is directly connected, FastEthernet0/0

Determinación máscaras de wildcard

ENLACE LAN R2 – Web Server

- ✓ Interfaz F0/1

Subred: 10.10.10.10/32.

Mascara 255.0.0.0

Mascara de Wildcard

	255	.	255	.	255	.	255
-	255	.	0	.	0	.	0
	0	.	255	.	255	.	255

ENLACE WAN R2 – R1

- ✓ Interfaz S0/1

Subred: 172.31.21.0/30.

Mascara: 255.255.255.252.

Mascara de Wildcard

	255	.	255	.	255	.	255
-	255	.	255	.	255	.	252
	0	.	0	.	0	.	3

ENLACE WAN R2 – R3

- ✓ Interfaz S0/0 DCE

Subred: 172.31.23.0/30.

Mascara 255.255.255.252.

Mascara de Wildcard

	255	.	255	.	255	.	255
-	255	.	255	.	255	.	252
	0	.	0	.	0	.	3

ENLACE LAN PC-INTERNET – R2

- ✓ Interfaz F0/0

Subred: 209.165.200.224/29.

Mascara 255.255.255.248.

Mascara de Wildcard

	255	.	255	.	255	.	255
-	255	.	255	.	255	.	248
	0	.	0	.	0	.	7

R2(config-router)#network 10.0.0.0 0.255.255.255 area 0

R2(config-router)#network 172.31.21.0 0.0.0.3 area 0

R2(config-router)#

06:54:19: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/1 from LOADING to FULL, Loading Done

R2(config-router)#network 172.31.23.0 0.0.0.3 area 0

R2(config-router)#network 209.165.200.224 0.0.0.7 area 0

R2(config-router)#passive-interface f0/1

R2(config-router)#passive-interface f0/0

R2(config-router)#auto-cost reference-bandwidth 9500

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

R2(config-router)#exit

R2(config)#int s0/0

R2(config-if)#bandwidth 256

R2(config-if)#ip ospf cost 9500

R2(config-if)#

07:04:46: %OSPF-5-ADJCHG: Process 1, Nbr 8.8.8.8 on Serial0/0 from LOADING to FULL, Loading Done

R2(config-if)#int s0/1

R2(config-if)#bandwidth 256

R2(config-if)#

R3

R3#config t

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

R3(config)#router ospf 1

R3(config-router)#router-id 8.8.8.8

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

C 172.31.23.0/30 is directly connected, Serial0/1

Determinación máscaras de wildcard

ENLACE WAN R3 – R2

- ✓ Interfaz S0/1

Subred: 172.31.23.0/30.

Mascara 255.255.255.252.

Mascara de Wildcard

	255	.	255	.	255	.	255
-	255	.	255	.	255	.	252
	0	.	0	.	0	.	3

R3(config-router)#network 172.31.23.0 0.0.0.3 area 0

R3(config-router)#

07:04:23: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/1 from LOADING to FULL, Loading Done

R3(config-router)#passive-interface f0/1

R3(config-router)#passive-interface f0/0

R3(config-router)#auto-cost reference-bandwidth 9500

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

R3(config-router)#int s0/1

R3(config-if)#bandwidth 256

R3(config-if)#int s0/0

R3(config-if)#bandwidth 256

R3(config-if)#ip ospf cost 9500

R3(config-if)#

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Tablas de Enrutamiento

Comando de modo EXEC privilegiado **show ip route o**.

R1

Figura 176 Verificación OSPFv2.Tabla de routing R1 Entradas O

```
R1#show ip route o
O    10.0.0.0 [110/9595] via 172.31.21.2, 00:20:55, Serial0/0
     209.165.200.0/29 is subnetted, 1 subnets
O       209.165.200.224 [110/9595] via 172.31.21.2, 00:20:45, Serial0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

R2

Figura 177 Verificación OSPFv2.Tabla de routing R2 Entradas O

```
R2#show ip route o
O    192.168.30.0 [110/6247] via 172.31.21.1, 00:22:47, Serial0/1
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

R3

Figura 178 Verificación OSPFv2.Tabla de routing R3 Entradas O

```
R3#show ip route o
O    10.0.0.0 [110/6247] via 172.31.23.1, 00:16:03, Serial0/1
O    192.168.30.0 [110/12399] via 172.31.23.1, 00:16:03, Serial0/1
     209.165.200.0/29 is subnetted, 1 subnets
O       209.165.200.224 [110/6247] via 172.31.23.1, 00:16:03, Serial0/1
```

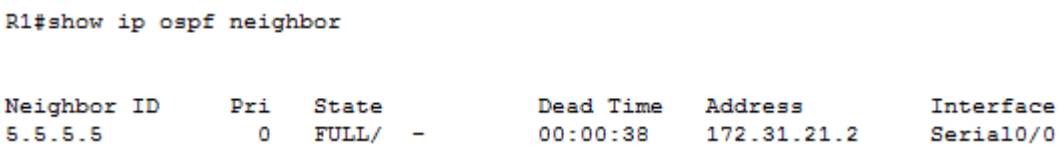
Fuente: Cisco Packet Tracer 7.0.2.0226.

Routers conectados por OSPFV2

Comando de modo EXEC privilegiado **show ip ospf neighbor**

R1

Figura 179 Verificación routers conectados por OSPF en R1

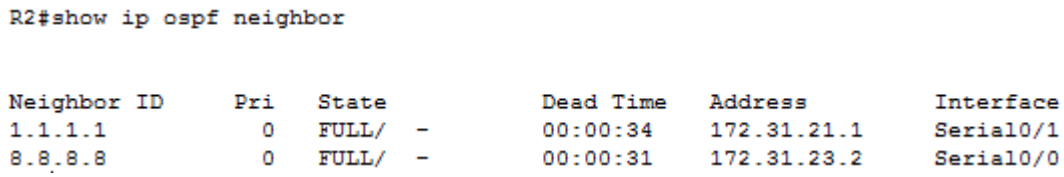


```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           0   FULL/  -        00:00:38    172.31.21.2     Serial0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

R2

Figura 180 Verificación routers conectados por OSPF en R2

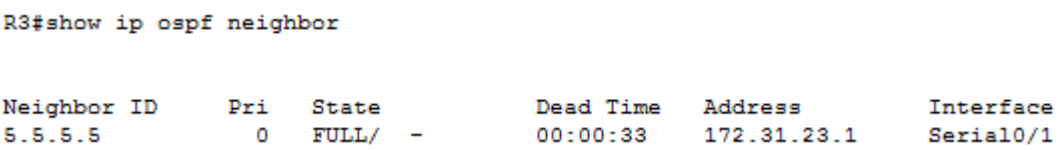


```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:34    172.31.21.1     Serial0/1
8.8.8.8           0   FULL/  -        00:00:31    172.31.23.2     Serial0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

R3

Figura 181 Verificación routers conectados por OSPF en R3



```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           0   FULL/  -        00:00:33    172.31.23.1     Serial0/1
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interfaz

Se utilizaría el comando del modo EXEC privilegiado **show ip ospf interface brief** pero en Packet Tracer no se encuentra disponible.

Figura 182 Opciones disponibles comando show ip ospf interface

```
R1#show ip ospf interface ?
  Ethernet         IEEE 802.3
  FastEthernet     FastEthernet IEEE 802.3
  GigabitEthernet  GigabitEthernet IEEE 802.3z
  Loopback         Loopback interface
  Serial           Serial
  <cr>
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Se utiliza el comando **show ip ospf interface**

R1

Figura 183 Verificación OSPF. Costo de Interfaz S0/0 en R1

```
R1#show ip ospf interface

Serial0/0 is up, line protocol is up
  Internet address is 172.31.21.1/30, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 9500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 5.5.5.5
  Suppress hello for 0 neighbor(s)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 184 Verificación OSPF. Costo de Interfaz F0/0 en R1

```
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.30.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 95
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

R2

Figura 185 Verificación OSPF. Costo de Interfaz F0/1 en R2

```
R2#show ip ospf interface

FastEthernet0/1 is up, line protocol is up
  Internet address is 10.10.10.1/8, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type BROADCAST, Cost: 95
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 186 Verificación OSPF. Costo de Interfaz S0/1 en R2

```
Serial0/1 is up, line protocol is up
  Internet address is 172.31.21.2/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT, Cost: 6152
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 187 Verificación OSPF. Costo de Interfaz S0/0 en R2

```
Serial0/0 is up, line protocol is up
  Internet address is 172.31.23.1/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT, Cost: 9500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 8.8.8.8
  Suppress hello for 0 neighbor(s)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 188 Verificación OSPF. Costo de Interfaz F0/0 en R2

```
FastEthernet0/0 is up, line protocol is up
  Internet address is 209.165.200.225/29, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type BROADCAST, Cost: 95
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 4/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

R3

Figura 189 Verificación OSPF. Costo de Interfaz S0/1 en R3

```
R3#show ip ospf interface

Serial0/1 is up, line protocol is up
  Internet address is 172.31.23.2/30, Area 0
  Process ID 1, Router ID 8.8.8.8, Network Type POINT-TO-POINT, Cost: 6152
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 5.5.5.5
  Suppress hello for 0 neighbor(s)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Se utiliza el comando de modo EXEC privilegiado **show ip protocols.**

Tabla 33 Convenciones para la verificación de información de OSPF

	ID Process
	Router ID
	Addess Summarizations
	Routing Networks
	Passive Interfaces

Fuente: Autoría Propia.

R1

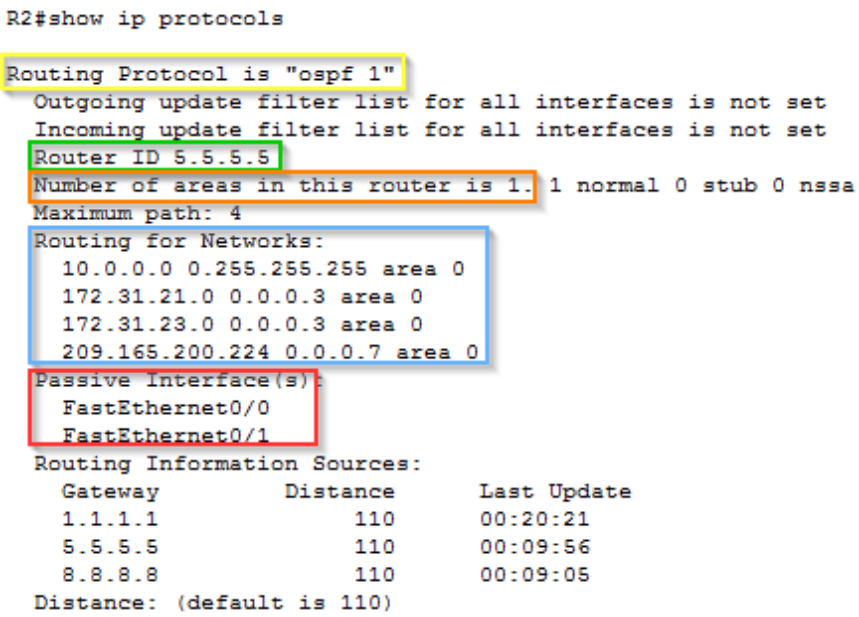
Figura 190 Verificación Protocolo OSPF en R1

```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    192.168.30.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:20:41
    5.5.5.5              110      00:10:18
    8.8.8.8              110      00:09:26
  Distance: (default is 110)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

R2

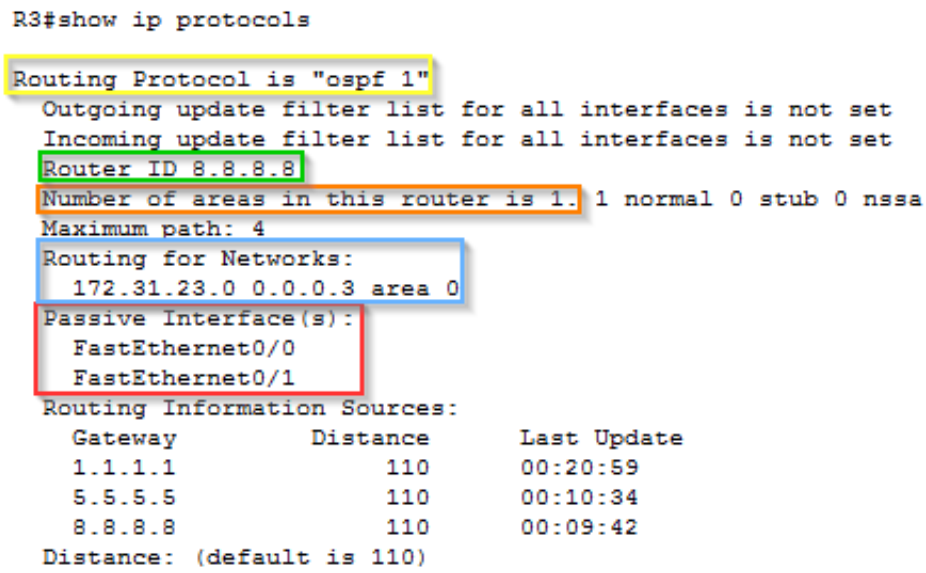
Figura 191 Verificación Protocolo OSPF en R2



Fuente: Cisco Packet Tracer 7.0.2.0226.

R3

Figura 192 Verificación Protocolo OSPF en R3



Fuente: Cisco Packet Tracer 7.0.2.0226.

1.2.3. Parte 3: Configuración de VLAN

Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter - VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

- **Visualizar configuración de VLANs.**

Se utiliza el comando de modo EXEC privilegiado **show vlan brief.** Se muestran todas las VLAN, nombre, estado y puertos de cada una.

S1

Figura 193 Configuración actual de VLAN en S1

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

S3

Figura 194 Configuración actual de VLAN en S3

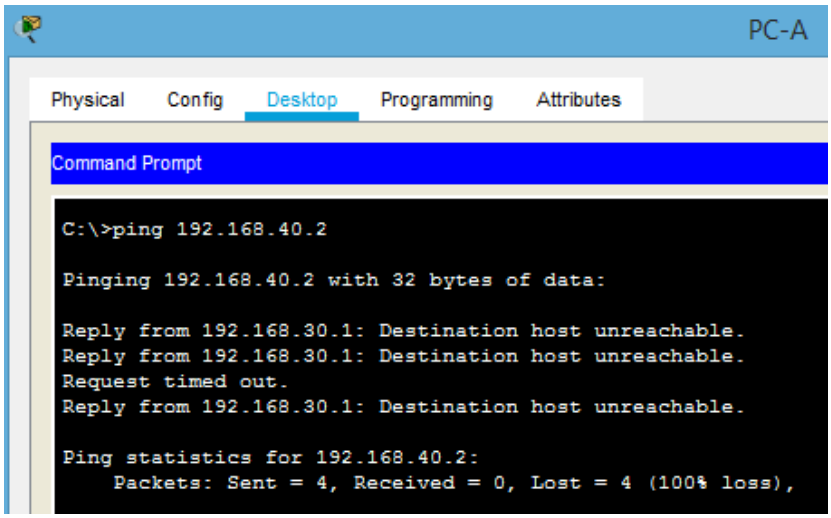
```
S3#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Verficar conectividad entre PCs

Ping PC-A a PC-C Fallido Destino inalcanzable.

Figura 195 Conectividad entre PCs. Ping Fallido PC-A a PC-C



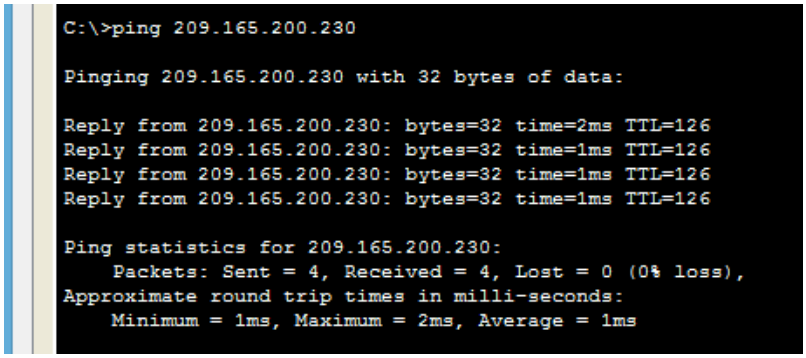
Fuente: Cisco Packet Tracer 7.0.2.0226.

Diagnóstico

Este ping falla porque no se han configurado las VLANS.

Ping PC-A a PC-INTERNET Exitoso**.**

Figura 196 Conectividad entre PCs. Ping exitoso PC-A a PC-INTERNET



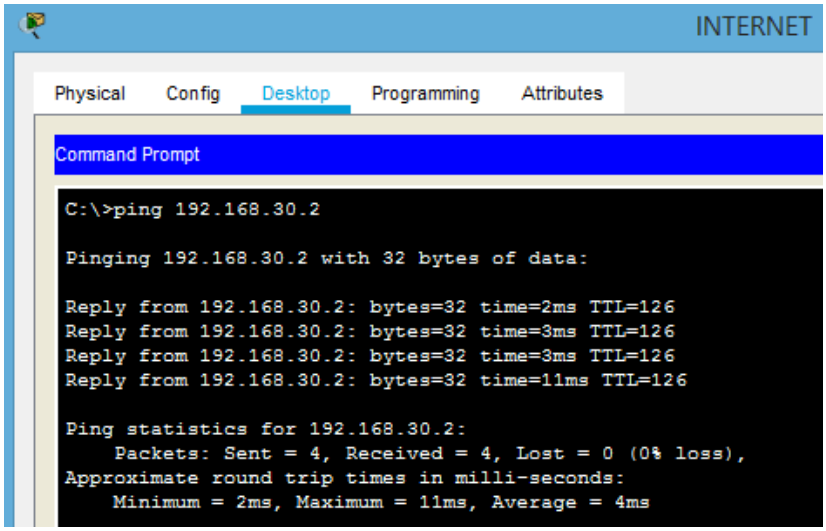
Fuente: Cisco Packet Tracer 7.0.2.0226.

Diagnóstico

El primer ping no se ejecuta en un ciento por ciento por el proceso ARP.

Ping PC-INTERNET a PC-A Exitoso**.**

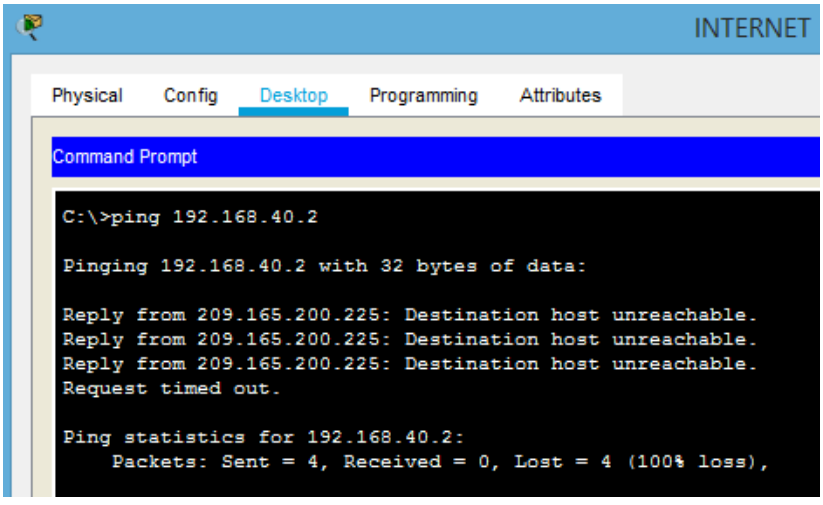
Figura 197 Conectividad entre PCs. Ping exitoso PC-INTERNET a PC-A



Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping PC-INTERNET a PC-C Fallido Destino inalcanzable**.**

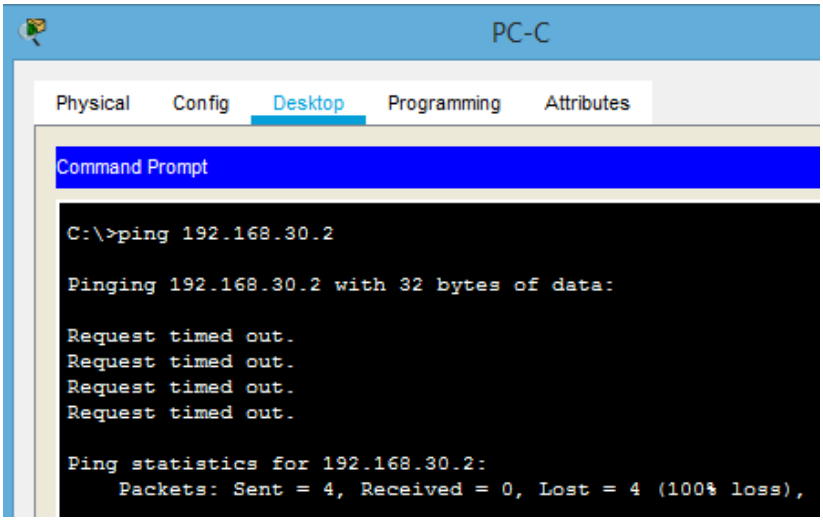
Figura 198 Conectividad entre PCs. Ping fallido PC-INTERNET a PC-C



Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping PC-C a PC-A Fallido.Tiempo de espera superado**.**

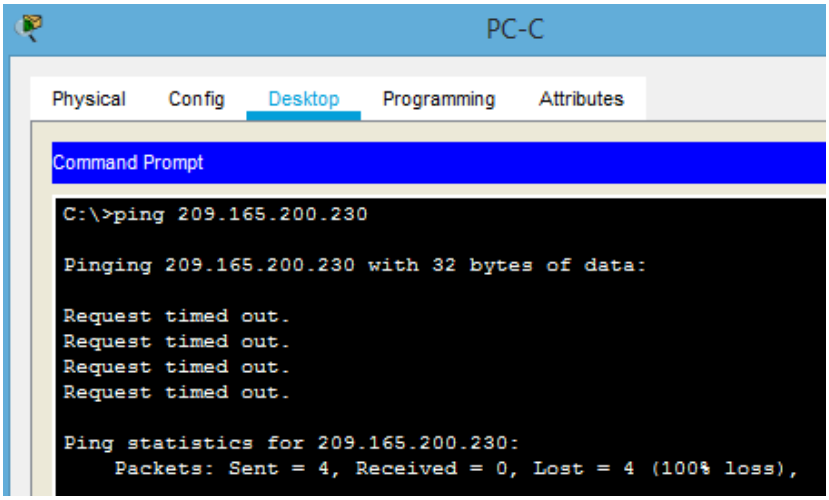
Figura 199 Conectividad entre PCs. Ping fallido PC-C a PC-A



Fuente: Cisco Packet Tracer 7.0.2.0226.

Ping PC-C a PC-INTERNET Fallido. Tiempo de espera superado**.**

Figura 200 Conectividad entre PCs. Ping fallido PC-C a PC-INTERNET



Fuente: Cisco Packet Tracer 7.0.2.0226.

- **Crear VLANS**

VLAN 30 administración.

VLAN 40 mercadeo.

VLAN 200 mantenimiento.

S1

El acceso no autorizado esta estrictamente prohibido !

User Access Verification

Password:

S1>en

Password:

S1#config t

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

S1(config)#vlan 30

S1(config-vlan)#name administracion

S1(config-vlan)#vlan 40

S1(config-vlan)#name mercadeo

S1(config-vlan)#vlan 200

S1(config-vlan)#name mantenimiento

S1(config-vlan)#

S3

El acceso no autorizado esta estrictamente prohibido !

User Access Verification

Password:

S3>en

Password:

S3#config t

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

S3(config)#vlan 30

S3(config-vlan)#name administracion

S3(config-vlan)#vlan 40

S3(config-vlan)#name mercadeo

S3(config-vlan)#vlan 200

S3(config-vlan)#name mantenimiento

S3(config-vlan)#

Verificar la configuración de VLAN

S1

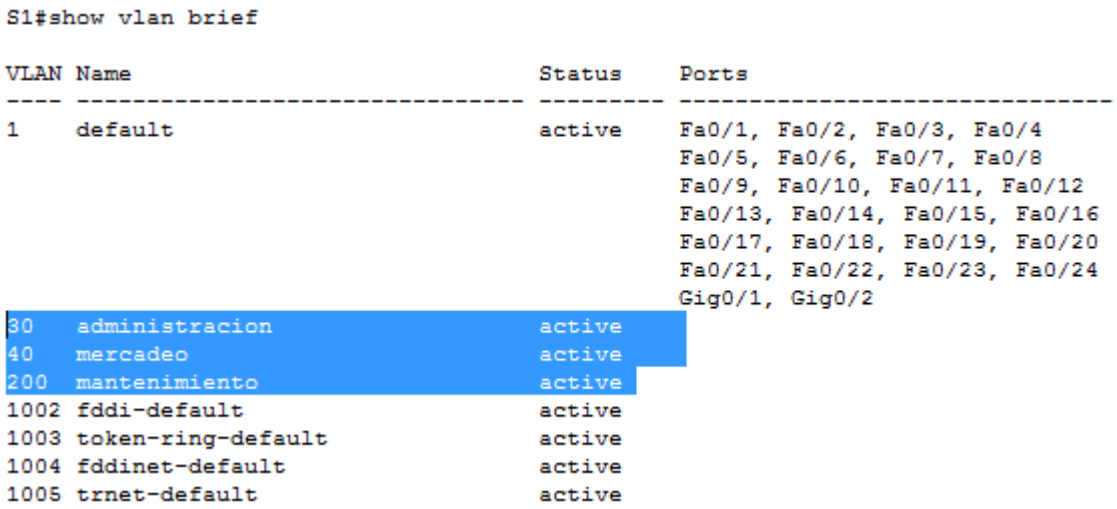
S1(config-vlan)#end

S1#

%SYS-5-CONFIG_I: Configured from console by console

S1#show vlan brief

Figura 201 Verificación de VLAN. VLANs creadas en S1



Fuente: Cisco Packet Tracer 7.0.2.0226.

S3

S3(config-vlan)#end

S3#

%SYS-5-CONFIG_I: Configured from console by console

S3#show vlan brief

Figura 202 Verificación de VLAN. VLANs creadas en S3

```
S3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
30   administracion                   active
40   mercadeo                         active
200  mantenimiento                    active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- **Configuración enlaces troncales**

Se requieren enlaces troncales para tranferir información de VLAN entre switches. Un puerto en un switch es un puerto de acceso o un puerto troncal. Los puertos de acceso transportan el tráfico desde una VLAN específica asignada al puerto.

Un puerto troncal por defecto es miembro de todas las VLAN; por lo tanto, transporta tráfico para todas las VLAN.

Se configuran las interfaces **F0/3** y **F0/24** en **S1** y **F0/3** en **S3** como enlaces troncales. Para esto:

- ✓ Si se agoto el tiempo de sesión, se ingresan nuevamente las credenciales de usuario para cada modo.
- ✓ Se ingresa al modo de configuración de interfaz con el comando de configuración global **interface** *ID-Interfaz.*
- ✓ Se habilita el enlace troncal con el comando **switchport mode trunk**.

S1

El acceso no autorizado esta estrictamente prohibido !

User Access Verification

Password:

S1>en

Password:

S1#config t

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

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

S1(config-if)#int f0/24

S1(config-if)#switchport mode trunk

S1(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

S1(config-if)#

Como se aprecia, el protocolo de las interfaces se desactiva y activa nuevamente en modo troncal.

S3

S3(config-if)#int f0/3

S3(config-if)#switchport mode trunk

S3(config-if)#

Configuración enlace troncal VLAN nativa

Como se configuraron estos enlaces de sebe configurar también el enlace troncal en la VLAN nativa en cada interfaz. Para esto, dentro del modo de configuración de interfaz se escribe el comando **switchport trunk native vlan 1**

S1

S1(config-if)#int f0/3

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#

S1(config-if)#int f0/24

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#

S3

S3(config-if)#int f0/3

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

S3(config-if)#

Desactivación de enlaces troncales en los puertos de acceso

Se deshabilitan los enlaces troncales en los puertos de acceso de cada interfaz,

- ✓ Se ingresa al modo de configuración de rango de interfaz con el comando de configuración global **int range** *rango 1*, *rango 2…rango n*.

S1

S1(config)#int range f0/1-2, f0/4-23, g0/1-2

S1(config-if-range)#switchport mode access

S1(config-if-range)#exit

S3

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

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

S3(config-if-range)#exit

- ✓ Se asigna la interfaz de acceso F0/1 para la PC-A a la VLAN 30 con los comandos de configuración de interfaz **switchport mode access** y **switchport Access vlan** *numero-vlan.*

S1

S1(config)#int f0/1

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 30

S3

S3(config)#int f0/1

S3(config-if)#switchport mode access

S3(config-if)#switchport access vlan 40

- ✓ Se verifica la configuración de asignación de puertos con el comando de modo EXEC privilegiado **show vlan brief.**
- ✓ Se verifica la configuración de enlaces troncales con el comando de modo EXEC privilegiado **show interfaces** *ID-INTERFAZ* **switchport.**

Figura 203 Verificación de VLAN. Configuración de asignación de puertos S1

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Gig0/1, Gig0/2
30   administracion                   active    Fa0/1
40   mercadeo                         active
200  mantenimiento                    active
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 204 Verificación de VLAN. Configuración enlaces troncales en S1

```
S1#show interfaces F0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)

S1#show interfaces f0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 205 Verificación de VLAN. Configuración de asignación de puertos S3

```
S3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
30   administracion                   active
40   mercadeo                         active    Fa0/1
200  mantenimiento                    active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 206 Verificación de VLAN. Configuración enlaces troncales en Fa0/3 S3

```
S3#show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- **Desactivar negociación**

Cisco utiliza un protocolo exclusivo conocido como “protocolo de enlace troncal dinámico” (DTP) en los switches. Algunos puertos negocian el enlace troncal de manera automática. Se recomienda desactivar la negociación. Puede ver este comportamiento predeterminado mediante la emisión del comando de modo EXEC privilegiado **show interface f0/3 switchport**

Figura 207 Verificación de VLAN. Negociación activada en Fa0/3 de S1

```
S1#show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation:
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 208 Verificación de VLAN. Negociación activada en Fa0/3 de S3

```
S3#show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- ✓ Para desactivar la negociación se ingresa al modo de configuración de inetrfaz con el comando de configuración global **interface** *ID-Interfaz.*
- ✓ Se ingresa el comando **switchport nonegotiate**.

S1

S1(config)#int f0/3

S1(config-if)#switchport nonegotiate

S1(config-if)#end

S1#

%SYS-5-CONFIG_I: Configured from console by console

S3

S3(config)#int f0/3

S3(config-if)#switchport nonegotiate

S3(config-if)#end

S3#

%SYS-5-CONFIG_I: Configured from console by console

- ✓ Se verifica que la negociación este desactivada con el comando de configuración global **show interface f0/3 switchport** en cada switch.

Figura 209 Verificación de VLAN. Negociación desactivada en Fa0/3 de S1

```
S1#show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation:
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 210 Verificación de VLAN. Negociación desactivada en Fa0/3 de S3

```
S3#show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

- **Verificación interfaces en modo acceso**

Se verifica que las interfaces desactivadas se encuentren en modo acceso con el comando de modo EXEC privilegiado **show interface f0/2 switchport.**

Figura 211 Verificación de VLAN. Interfaz Fa0/2 en modo acceso de S1j

```
S1#show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation:
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Figura 212 Verificación de VLAN. Interfaz Fa0/2 en modo acceso de S3

```
S3# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Nota: Solo se verifica esta interfaz, las demás deben visualizarse igual.

1.2.4. Parte 4: Deshabilitación DNS lookup

En el Switch 3 deshabilitar DNS lookup.

- ✓ En S1 se encuentra deshabilitado. Se activa DNS lookup en S3 con el comando de configuración global **ip domain-lookup**.

S1

S1#config t

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

S1(config)#ip domain-lookup

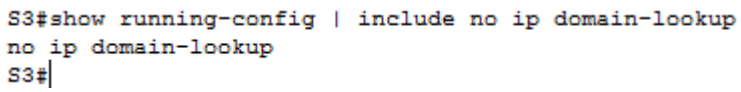
S1(config)#exit

S1#

- ✓ En S3 se desactivo con el comando de configuracion global **no ip domain-lookup**. Se comprueba con el comando de modo EXEC privilegiado **show run.**

S3

Figura 213 Deshabilitación DNS lookup en S3



Fuente: Cisco Packet Tracer 7.0.2.0226.

1.2.5. Parte 5: Asignación de Direcciones IP

Asignar direcciones IP a los Switches acorde a los lineamientos.

- ✓ Se ingresa al modo de configuración global con el comando de modo EXEC privilegiado **config t.**

Nueva Tabla de Direcionamiento

Tabla 34 Nueva Tabla de Direccionamiento Escenario 2

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway Pred.
R1	**F0/0**	-	255.255.255.0	No Aplica
	F0/0.30	**192.168.30.1**	**255.255.255.0**	**No Aplica**
	F0/0.40	**192.168.40.1**	**255.255.255.0**	**No Aplica**
	S0/0 DCE	172.31.21.1	255.255.255.252	No Aplica
R2	F0/0	209.165.200.225	255.255.255.248	No Aplica
	F0/1	10.10.10.1	255.0.0.0	No Aplica
	S0/1	172.31.21.2	255.255.255.252	No Aplica
	S0/0 DCE	172.31.23.1	255.255.255.252	No Aplica
R3	S0/1	172.31.23.2	255.255.255.252	No Aplica
S1	**VLAN 1**	**192.168.99.2**	**255.255.255.0**	**192.168.30.1**
S3	**VLAN 1**	**192.168.99.3**	**255.255.255.0**	**192.168.40.1**
Web Server	F0/0	10.10.10.10	255.255.255.0	10.10.10.1
PC-INTERNET	NIC	209.165.200.230	255.255.255.248	209.165.200.225
PC-A	NIC	192.168.30.2	255.255.255.0	192.168.30.1
PC-C	NIC	192.168.40.2	255.255.255.0	192.168.40.1

Fuente: Autoría Propia.

Tabla 35 Direccionamiento VLAN Escenario 2

Interfaces	Asignaciones	Red	Mascara
S1 F0/1	VLAN 30: administración	192.168.30.0	255.255.255.0
S3 F0/1	VLAN 40: mercadeo	192.168.40.0	255.255.255.0

Fuente: Autoría Propia.

- **Configuración VLAN 1**

✓ Se ingresa al modo de configuración de interaz con el comando de configuración global **int** *ID-Interfaz.*

✓ Se asigna la dirección IP y máscara con el comando **ip address** *Direccion-ip Mascara.*

✓ Se activa la interfaz con el comando **no shutdown** o abreviado **no shut.**

✓ Se sale del modo de configuración de interfaz con el comando **exit.**

✓ Se establece el Gateway Predeterminado con el comando **ip default-gateway** *Direccion-IP.*

S1

S1#config t

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

S1(config)#int vlan 1

S1(config-if)#ip address 192.168.99.3 255.255.255.0

S1(config-if)#no shutdown

S1(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit

S1(config)#ip default-gateway 192.168.30.1

S1(config)#

S3

S3#config t

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

S3(config)#int vlan 1

S3(config-if)#ip address 192.168.99.2 255.255.255.0

S3(config-if)#no shutdown

S3(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S3(config-if)#exit

S3(config)#ip default-gateway 192.168.40.1

S3(config)#

- **Configuración VLAN 30**

S1

S1(config)#int vlan 30

S1(config-if)#ip address 192.168.30.5 255.255.255.0

S3

S3(config)#int vlan 30

S3(config-if)#ip address 192.168.30.5 255.255.255.0

- **Configuración VLAN 40**

S1

S1(config)#int vlan 40

S1(config-if)#ip address 192.168.40.5 255.255.255.0

S3

S3(config)#int vlan 40

S3(config-if)#ip address 192.168.40.5 255.255.255.0

Activación VLAN administración

- ✓ Se ingresa a la VLAN 30 con el comando de configuración global **int vlan** *ID-vlan.*

S1

S1(config)#int vlan 30

S1(config-if)#

%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

S3

S3(config)#int vlan 40

S3(config-if)#

%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

Activación VLAN mercadeo

- ✓ Se ingresa a la VLAN 40 con el comando de configuración global **int vlan** *ID-vlan.*

S1

S1(config-if)#int vlan 40

S1(config-if)#

%LINK-5-CHANGED: Interface Vlan40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

S1(config-if)#

S3

S3(config-if)#int vlan 40

S3(config-if)#

%LINK-5-CHANGED: Interface Vlan40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

S3(config-if)#

Activación VLAN mantenimiento

- ✓ Se ingresa a la VLAN 200 con el comando de configuración global **int vlan** *ID-vlan.*

S1

S1#config t

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

S1(config)#int vlan 200

S1(config-if)#

%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S1(config-if)#

S3

S3(config-if)#int vlan 200

S3(config-if)#

%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S3(config-if)#

- **Configuración R1**

Se debe aplicar el nuevo direccionamiento, se elimina la dirección IP y la descripción de R1 con el comando **no** seguido de la instrucción que se desea eliminar.

R1(config)#int f0/0

R1(config-if)#no ip address 192.168.30.1 255.255.255.0

R1(config-if)#no description ENLACE LAN R2 - S1 RED 192.168.99.0/24

Se crean las **subinterfaces** en la interfaz **F0/1** del **R1** para la VLAN 30 con ID 30 y para la VLAN 40 con ID 40.

- ✓ Se utiliza el comando de configuración de interfaz **int** *interfaz-principal.ID.* Se accede al modo de configuración de subinterfaz.
- ✓ Se configura el encapsulamiento con el comando de configuración de subinterfaz **encapsulation dot1Q** *ID.*

SUBINTERFAZ F0/0.30 (VLAN 30)

R1(config-if)#int f0/0.30

R1(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

R1(config-subif)#encapsulation dot1Q 30

R1(config-subif)#ip address 192.168.30.1 255.255.255.0

R1(config-subif)#exit

SUBINTERFAZ F0/0.40 (VLAN 40)

R1(config-if)#int f0/0.40

R1(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.40, changed state to up

R1(config-subif)#encapsulation dot1Q 40

R1(config-subif)#ip address 192.168.40.1 255.255.255.0

R1(config-subif)#exit

Verificaión Tabla de routing R1

Figura 214 Reconfiguración Direccionamiento. Tabla de routing R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.31.0.0/30 is subnetted, 2 subnets
C       172.31.21.0 is directly connected, Serial0/0
S       172.31.23.0 [1/0] via 172.31.21.2
C    192.168.30.0/24 is directly connected, FastEthernet0/0.3
C    192.168.40.0/24 is directly connected, FastEthernet0/0.4
```

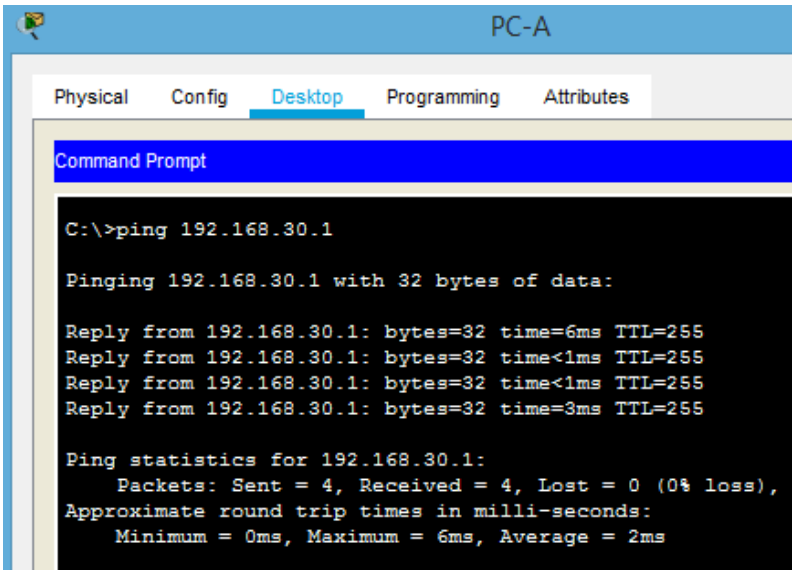
Fuente: Cisco Packet Tracer 7.0.2.0226

Se aprecian las rutas conectadas directamente de las VLANs.

Prueba conectividad entre VLANs

Ping PC-A a Gateway predeterminado de la VLAN 30

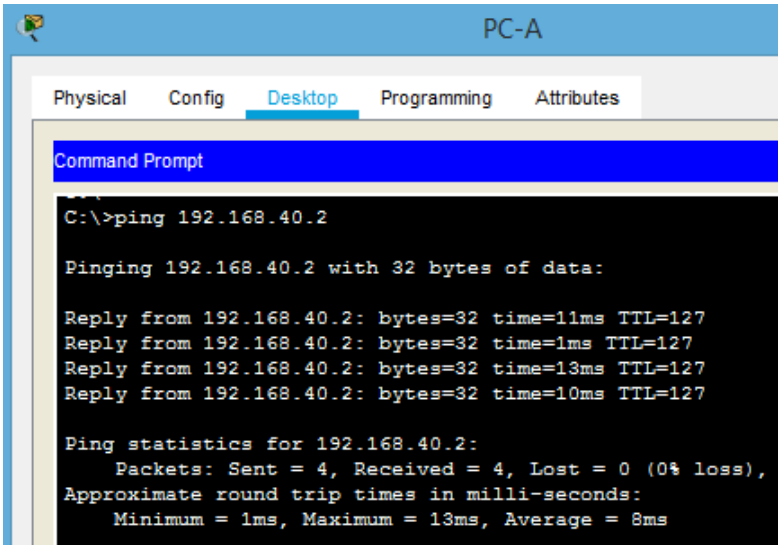
Figura 215 Reconfiguración Direccionamiento. Ping PC-A a GP VLAN 30



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-A a PC-C

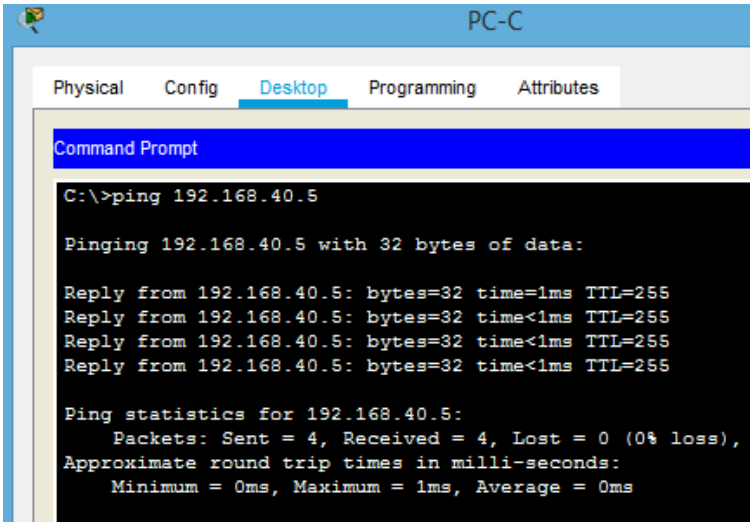
Figura 216 Reconfiguración Direccionamiento. Ping PC-A a PC-C



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-C a Gateway Predeterminado de la VLAN 40

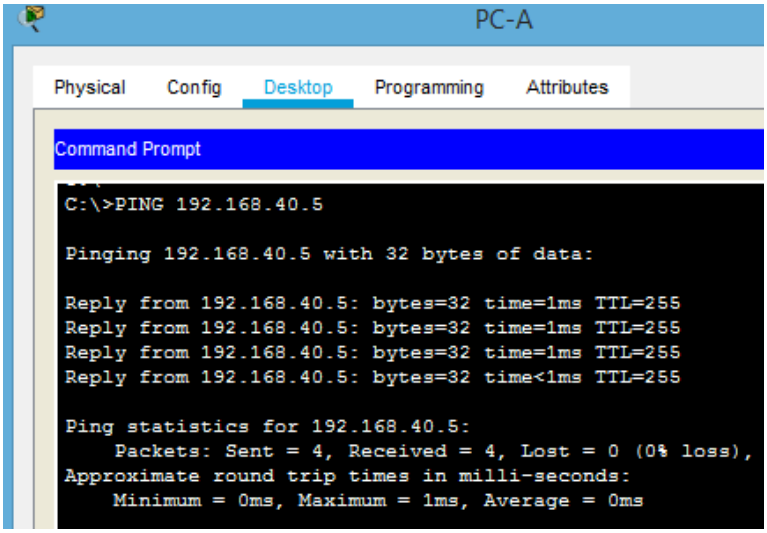
Figura 217 Reconfiguración Direccionamiento. Ping PC-C a GP VLAN 40



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-A a Gateway Predeterminado VLAN 40

Figura 218 Reconfiguración Direccionamiento. Ping PC-A a GP VLAN 40



Fuente: Cisco Packet Tracer 7.0.2.0226

Direccionamiento de VLANs

Tabla 36 Nuevo Direccionamiento de VLANs

VLAN	Dirección IP	Mascara de Subred	Gateway Pred.
VLAN 1 en S1	192.168.99.2	255.255.255.0	192.168.30.1
VLAN 1 en S3	192.168.99.3	255.255.255.0	192.168.40.1
VLAN 30	192.168.30.5	255.255.255.0	192.168.30.1
VLAN 40	192.168.40.5	255.255.255.0	192.168.40.1

Fuente: Autoría Propia.

Reconfiguración OSPFv2

Como se cambio el direccionamiento en la interfaz F0/0 del R1, se realiza la configuración de OSPF y validar la conectividad.

ENLACE LAN R1– S1

- ✓ Subinterfaz F0/0.3

Red: 192.168.30.1/24.

Mascara: 255.255.255.0.

- ✓ Subinterfaz F0/0.4

Red: 192.168.40.1/24.

Mascara: 255.255.255.0.

Estas subinterfaces ya se configuraron y se puede validar con el comando **show ip interface brief** del modo EXEC privilegiado.

Figura 219 Reconfiguración OSPFv2. Estado subinterfaces R1

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES manual up                    up
FastEthernet0/0.3      192.168.30.1    YES manual up                    up
FastEthernet0/0.4      192.168.40.1    YES manual up                    up
FastEthernet0/1        unassigned      YES NVRAM  administratively down down
Serial0/0              172.31.21.1     YES NVRAM  up                    up
Serial0/1              unassigned      YES NVRAM  administratively down down
```

Fuente: Cisco Packet Tracer 7.0.2.0226

R1

R1#config t

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

R1(config)#router ospf 1

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

C 172.31.21.0/30 is directly connected, Serial0/0

C 192.168.30.0/24 is directly connected, FastEthernet0/0.3

C 192.168.40.0/24 is directly connected, FastEthernet0/0.4

Determinación mascaras de wildcard

ENLACE WAN R1 – R2

- ✓ Interfaz S0/0 DCE

Subred: 172.31.21.0/30.

Mascara: 255.255.255.252.

Mascara de Wildcard

	255	.	255	.	255	.	255
-	255	.	255	.	255	.	252
	0	.	0	.	0	.	3

ENLACE LAN R1– S1

- ✓ Subinterfaz F0/0.3

Red: 192.168.30.0/24.

Mascara: 255.255.255.0.

	255	.	255	.	255	.	255
-	255	.	255	.	255	.	0
	0	.	0	.	0	.	255

- ✓ Subinterfaz F0/0.4

Red: 192.168.40.0/24.

Mascara: 255.255.255.0.

		255	.	255	.	255	.	255
-		255	.	255	.	255	.	0
		0	.	0	.	0	.	255

R1(config-router)#network 172.31.21.0 0.0.0.3 area 0

R1(config-router)#network 192.168.30.0 0.0.0.255 area 0

R1(config-router)#network 192.168.40.0 0.0.0.255 area 0

R1(config-router)#passive-interface f0/0.3

R1(config-router)#passive-interface f0/0.4

R1(config-router)#auto-cost reference-bandwidth 9500

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

R1(config-router)#exit

R1(config-if)#

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Tablas de Enrutamiento

Comando de modo EXEC privilegiado **show ip route o**.

R1

Figura 220 Reconfiguración OSPFv2.Tabla de routing R1 Entradas O

```
R1#show ip route o
O    10.0.0.0 [110/9595] via 172.31.21.2, 00:20:55, Serial0/0
     209.165.200.0/29 is subnetted, 1 subnets
O       209.165.200.224 [110/9595] via 172.31.21.2, 00:20:45, Serial0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226

R2

Figura 221 Reconfiguración OSPFv2.Tabla de routing R2 Entradas O

```
R2#show ip route o
O    192.168.30.0 [110/485] via 172.31.21.1, 00:03:29, Serial0/1
O    192.168.40.0 [110/485] via 172.31.21.1, 00:03:29, Serial0/1
```

Fuente: Cisco Packet Tracer 7.0.2.0226

R3

Figura 222 Reconfiguración OSPFv2.Tabla de routing R3 Entradas O

```
R3#show ip route o
O    10.0.0.0 [110/391] via 172.31.23.1, 10:18:35, Serial0/1
O    192.168.30.0 [110/875] via 172.31.23.1, 00:04:49, Serial0/1
O    192.168.40.0 [110/875] via 172.31.23.1, 00:04:49, Serial0/1
     209.165.200.0/29 is subnetted, 1 subnets
O       209.165.200.224 [110/391] via 172.31.23.1, 10:18:35, Serial0/1
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Routers conectados por OSPFV2

Comando de modo EXEC privilegiado **show ip ospf neighbor**

R1

Figura 223 Reconfiguración OSPFv2. Routers conectados en R1

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           0   FULL/  -        00:00:38    172.31.21.2     Serial0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226

R2

Figura 224 Reconfiguración OSPFv2. Routers conectados en R2

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:34    172.31.21.1     Serial0/1
8.8.8.8           0   FULL/  -        00:00:31    172.31.23.2     Serial0/0
```

Fuente: Cisco Packet Tracer 7.0.2.0226

R3

Figura 225 Reconfiguración OSPFv2. Routers conectados en R3

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           0   FULL/  -        00:00:33    172.31.23.1     Serial0/1
```

Fuente: Cisco Packet Tracer 7.0.2.0226

- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interfaz.

Se utiliza el comando **show ip ospf interface**

R1

Figura 226 Reconfiguración OSPFv2. Costo de Interfaz S0/0 en R1

```
R1#show ip ospf interface

Serial0/0 is up, line protocol is up
  Internet address is 172.31.21.1/30, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 9500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 5.5.5.5
  Suppress hello for 0 neighbor(s)
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Figura 227 Reconfiguración OSPFv2. Costo de subinterfaz Fa0/0.3 en R1

```
FastEthernet0/0.3 is up, line protocol is up
  Internet address is 192.168.30.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 95
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Figura 228 Reconfiguración OSPFv2. Costo de subinterfaz Fa0/0.4 en R1

```
FastEthernet0/0.4 is up, line protocol is up
  Internet address is 192.168.40.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 95
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Fuente: Cisco Packet Tracer 7.0.2.0226

- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Se utiliza el comando de modo EXEC privilegiado **show ip protocols.**

Tabla 37 Convenciones para la verificación de OSPFv2 reconfigurado

	ID Process
	Router ID
	Addess Summarizations
	Routing Networks
	Passive Interfaces

Fuente: Autoría Propia.

R1

Figura 229 Reconfiguración Protocolo OSPFv2 en R1

```
R1# show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    192.168.30.0 0.0.0.255 area 0
    192.168.40.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/0.3
    FastEthernet0/0.4
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:07:09
    5.5.5.5              110      00:10:06
    8.8.8.8              110      00:17:16
  Distance: (default is 110)
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

Verificar conectividad OSPF

PINGS ENTRE ROUTERS

Ping R1 a R2.

Figura 230 Reconfiguración OSPFv2. Ping exitoso R1 a R2

```
R1#ping 172.31.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/3 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Ping R1 a R3.

Figura 231 Reconfiguración OSPFv2. Ping exitoso R1 a R3

```
R1#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/9/37 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Ping R2 a R1.

Figura 232 Reconfiguración OSPFv2. Ping exitoso R2 a R1

```
R2#ping 172.31.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/13 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Ping R2 a R3.

Figura 233 Reconfiguración OSPFv2. Ping exitoso R2 a R3

```
R2#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/14 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Ping R3 a R2.

Figura 234 Reconfiguración OSPFv2. Ping exitoso R3 a R2

```
R3#ping 172.31.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Ping R3 a R1.

Figura 235 Reconfiguración OSPFv2. Ping exitoso R3 a R1

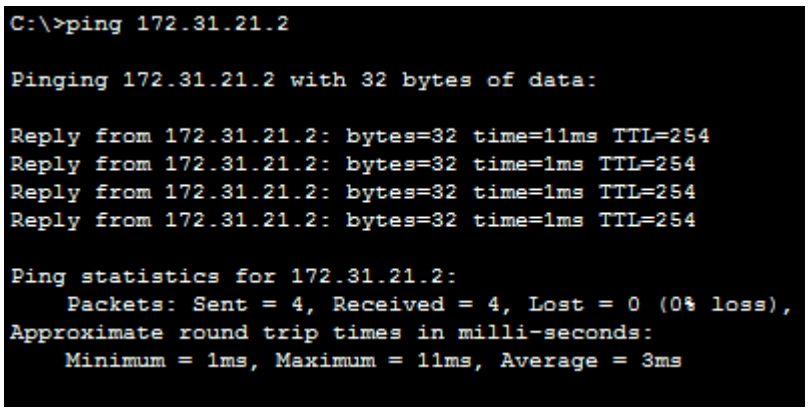
```
R3#ping 172.31.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/6/22 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226

PINGS ENTRE DISPOSITIVOS

Ping PC-A a R2.

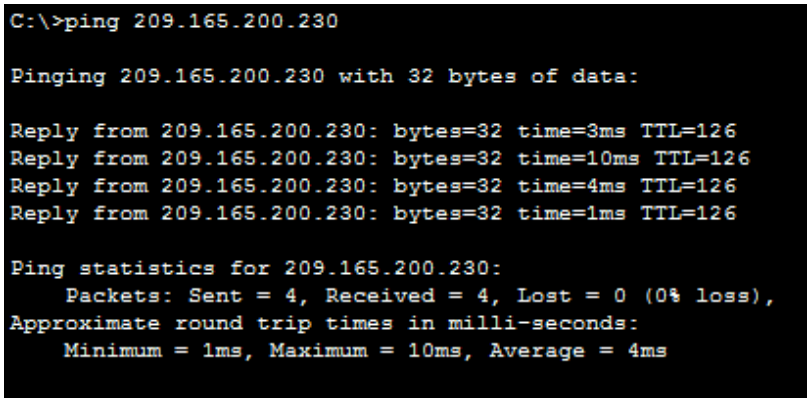
Figura 236 Reconfiguración OSPFv2. Ping exitoso PC-A a R2



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-A a PC-INTERNET.

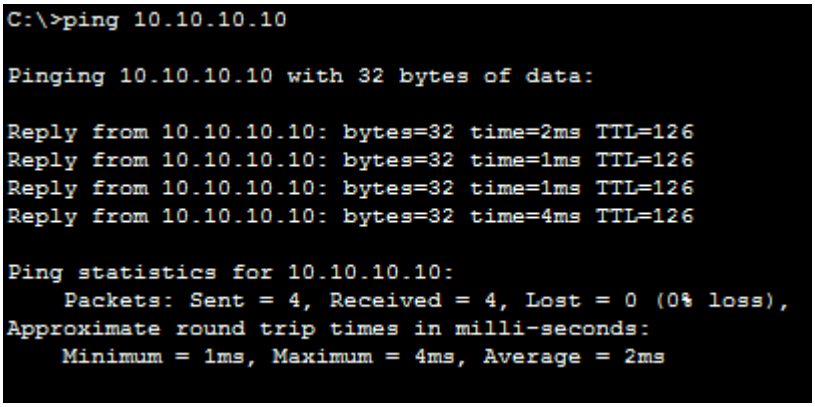
Figura 237 Reconfiguración OSPFv2. Ping exitoso PC-A a PC-INTERNET



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-A a Web Server.

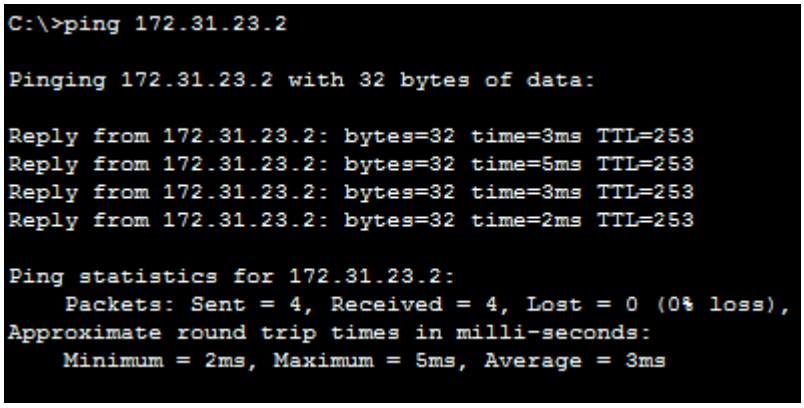
Figura 238 Reconfiguración OSPFv2. Ping exitoso PC-A a Web Server



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-A a R3.

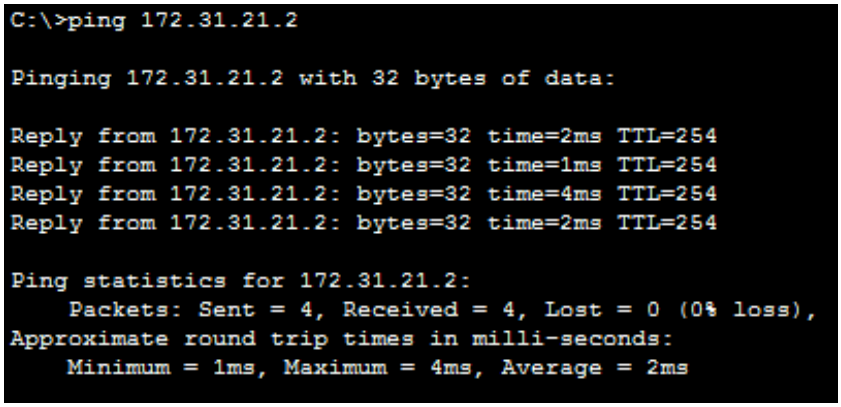
Figura 239 Reconfiguración OSPFv2.exitoso Ping PC-A a R3



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-C a R2.

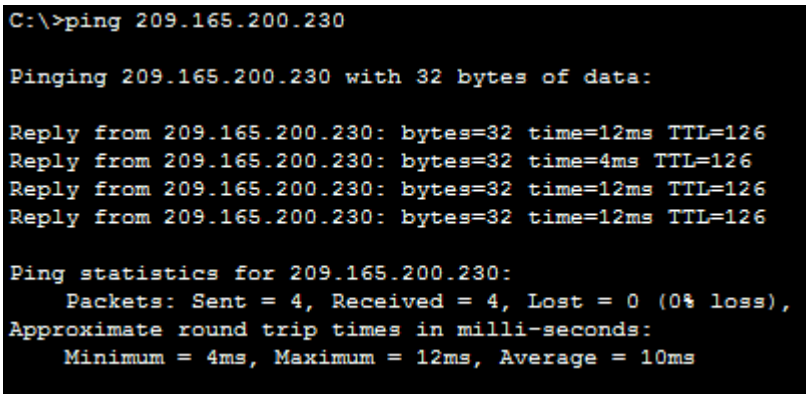
Figura 240 Reconfiguración OSPFv2. Ping exitoso PC-C a R2



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-C a PC-INTERNET.

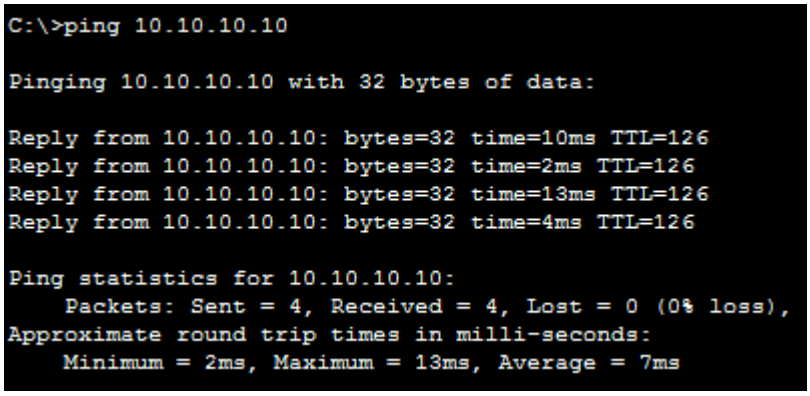
Figura 241 Reconfiguración OSPFv2. Ping exitoso PC-C a PC-INTERNET



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-C a Web Server.

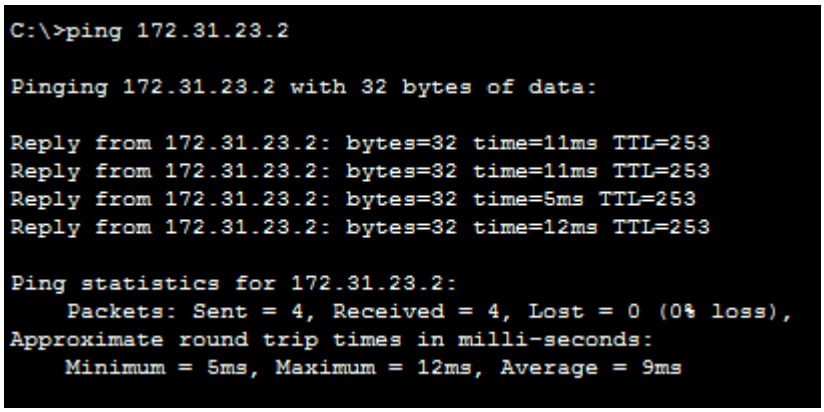
Figura 242 Reconfiguración OSPFv2. Ping exitoso PC-C a Web Server



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-C a R3.

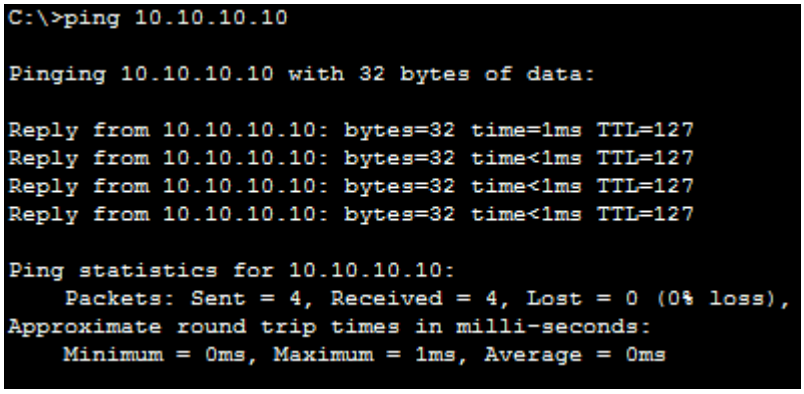
Figura 243 Reconfiguración OSPFv2. Ping exitoso PC-C a R3



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-INTERNET a Web Server.

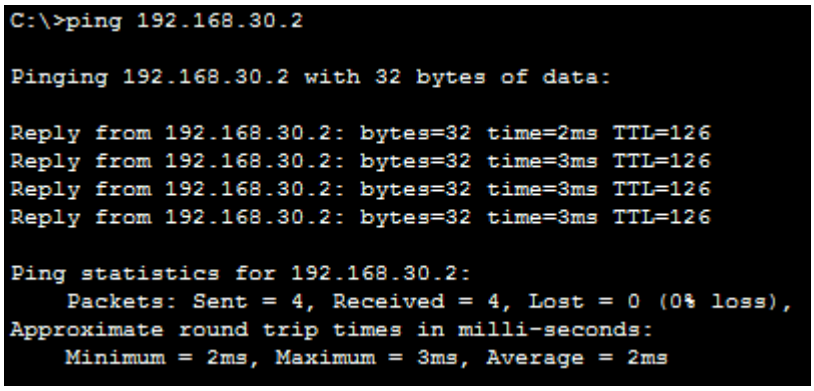
Figura 244 Reconfiguración OSPFv2 Ping exitoso PC-INTERNET a WebServer



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-INTERNET a PC-A.

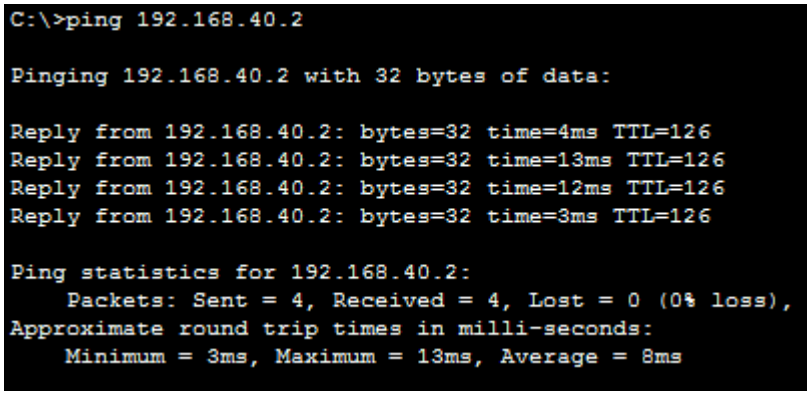
Figura 245 Reconfiguración OSPFv2. Ping exitoso PC-INTERNET a PC-A



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-INTERNET a PC-C.

Figura 246 Reconfiguración OSPFv2. Ping exitoso PC-INTERNET a PC-C



Fuente: Cisco Packet Tracer 7.0.2.0226

1.2.6. Parte 6 Desactivación de Interfaces

Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

Desactivación de interfaces

- ✓ Se ingresa nuevamente al modo de configuración de rangos de interfaz con el comando **int rango** *ID-Interfaz1, ID-Interfaz2,…ID-Interfazn***.**
- ✓ Se deshabilitan las interfaces definidas dentro del rango con el comando **shutdown.**

S1

S1(config-if)#int range f0/2, f0/4-23, g0/1-2

S1(config-if-range)#shutdown

%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 FastEthernet0/18, 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 GigabitEthernet0/1, changed state to administratively down

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

S1(config-if-range)#

S3

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

S3(config-if-range)#shutdown

%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 FastEthernet0/18, 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

S3(config-if-range)#

Esta configuración se puede comprobar con el comando de configuración global **show ip interface brief | include down** para mostrar solo las interfaces desactivadas.

S1

Figura 247 Interfaces deshabilitadas S1

```
S1#show ip interface brief | include down
FastEthernet0/2        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES manual administratively down down
```

Fuente: Cisco Packet Tracer 7.0.2.0226.

S3

Figura 248 Interfaces deshabilitadas S3

```
S3#show ip interface brief | include down
FastEthernet0/2        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES manual administratively down down
```

Fuente: Cisco Packet Tracer 7.0.2.0226

1.2.7. Parte 7: Implementar DHCP y NAT para IPv4

1.2.8. Parte 8: Configurar R1 como servidor DHCP

Se configura R1 como servidor DHCP para las VLANs 30 y 40

1.2.9. Parte 9: Reservar direcciones IP

Se deben reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas

La siguiente información se extrajo del **Laboratorio 10.3.1.1 IoE y DHCP.** Este laboratorio corresponde a la Tarea 4.

Se realiza la configuración de la siguiente manera:

- ✓ Dentro del modo de configuración global se excluyen las direcciones IP

Algunas direcciones IPv4 de un conjunto se asignan a dispositivos de red que requieren direcciones estáticas. Por tal motivo, estas direcciones deben estar reservadas. Para este caso se excluyen 30 direcciones IP de las VLAN 30 y 40 que pueden ser utilizadas en configuraciones estáticas.

Comando **ip dhcp excluded-address** *Direccion-IP-inicial Direccion-IP-final*

- ✓ Se configura un pool de DHCPv4 con el comando **ip dhcp pool** *nombre-pool*.

Cuando se configura un servidor de DHCPv4 se debe definir un conjunto de direcciones que se deben asignar. El comando anterior permite crear un conjunto de direcciones con nombre especificado.

Después de ejecutar el comando el router ingresa al modo de configuración de DHCPv4.

- ✓ Para finalizar la configuración de un pool DHCPv4 se debe realizar una serie de tareas, algunas son optativas pero otras requeridas:

Tareas requeridas

- ✓ Se define un conjunto de direcciones con el comando de configuración de DHCPv4 **network** *número-red* [*mask* | *prefix-length*].
- ✓ Se define el router o gateway predeterminado con el comando de configuración de DHCPv4 **default-router address** [*address 1…address 8]*. El Gateway suele ser la interfaz LAN del router más cercano a los terminales cliente. Se debe especificar un gateway pero se pueden indicar hasta 8 direcciones si existen varios gateways.

Tareas Optativas

Entre las tareas optativas se encuentran:

- ✓ Definir un servidor DNS. Comando de configuración de DHCPv4 **dns-server** *address [address 1…address 8*].
- ✓ Definir nombre de dominio. Comando de configuración de DHCPv4 **domain-name** *dominio*.
- ✓ Definir la duración de la concesión de DHCP. Comando de configuración de DHCPv4 **lease** { [*hours*] [*minutes*] | *infinite* }

Este comando permite especificar el tiempo máximo que puede asignarse una dirección IP a un nodo de la red. Por ejemplo, se define lease 1, esto quiere decir que el tiempo especificado es un dia. Después de las 24 horas, el nodo se refrescará y se le asignará una nueva dirección IP. Generalmente se asigna la misma dirección.

- ✓ Definir el servidor WINS de NetBIOS. Comando de configuración de DHCPv4 netbios name-server address [address 2…address 8].

Tabla 38 Parámetros configuración DHCPv4

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

Fuente: Cisco. Evaluación – Prueba de Habildiades Prácticas CCNA.

CONFIGURAR DHCP POOL PARA VLAN 30

R1#config t

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

R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30

R1(config)#ip dhcp pool ADMINISTRACION

R1(dhcp-config)#network 192.168.30.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.30.1

R1(dhcp-config)#dns-server 10.10.10.11

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

R1(dhcp-config)#exit

CONFIGURAR DHCP POOL PARA VLAN 40

R1#config t

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

R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30

R1(config)#ip dhcp pool MERCADEO

R1(dhcp-config)#network 192.168.40.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.40.1

R1(dhcp-config)#dns-server 10.10.10.11

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

R1(dhcp-config)#exit

Verificación Configuración

Se verifica la configuración con el comando de modo EXEC privilegiado **show running-config | begin dhcp.**

Figura 249 Verificación configuración DHCPv4 en R1

```
R1#show running-config | include dhcp
ip dhcp excluded-address 192.168.30.1 192.168.30.30
ip dhcp excluded-address 192.168.40.1 192.168.40.30
ip dhcp pool ADMINISTRACION
ip dhcp pool MERCADEO
R1#show running-config | begin dhcp
ip dhcp excluded-address 192.168.30.1 192.168.30.30
ip dhcp excluded-address 192.168.40.1 192.168.40.30
!
ip dhcp pool ADMINISTRACION
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 10.10.10.11
 domain-name ccna-unad.com
ip dhcp pool MERCADEO
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 10.10.10.11
 domain-name ccna-unad.com
!
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Configuración DHCP en las PC-A y PC-C

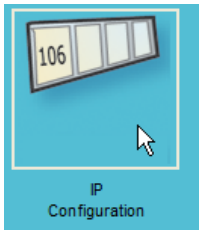
- ✓ Se hace clic sobre la PC y a continuación, se hace clic sobre la pestaña **Desktop.**

Figura 250 Configuración DHCPv4. Pestaña Desktop PC-A

Fuente: Cisco Packet Tracer 7.0.2.0226

- ✓ Se hace clic sobre **IP Configuration.**

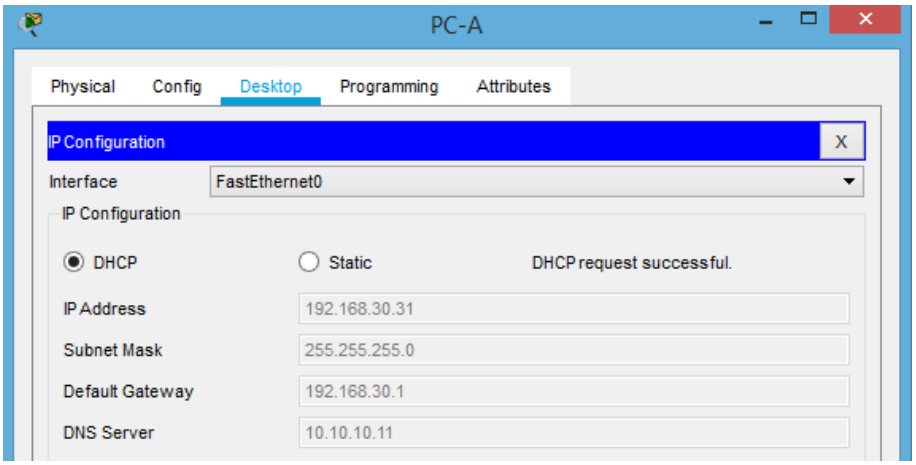
Figura 251 Configuración DHCPv4. Botón IP Configuration



Fuente: Cisco Packet Tracer 7.0.2.0226

- ✓ En el apartado **IP Configuration** se hace clic sobre **DHCP.** Se debe mostrar el direccionamiento automático y un mensaje que indique **DHCP request successful**.

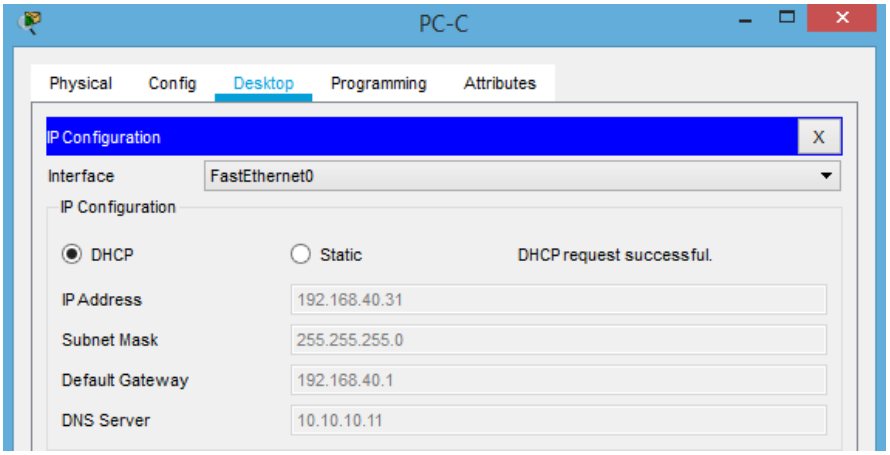
Figura 252 Configuración Direccionamiento DHCPv4 exitoso en PC-A



Fuente: Cisco Packet Tracer 7.0.2.0226

✓ Se repite el proceso para el PC-C.

Figura 253 Configuración Direccionamiento DHCPv4 exitoso en PC-C

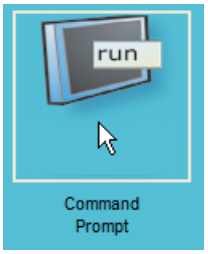


Fuente: Cisco Packet Tracer 7.0.2.0226

Verificación Direccionamiento

Se cierra la ventana y a continuación, se hace clic sobre **Command Prompt** (Consola de Comandos) en la PC.

Figura 254 Verificación Direccionamiento DHCPv4. Command Prompt PC-A

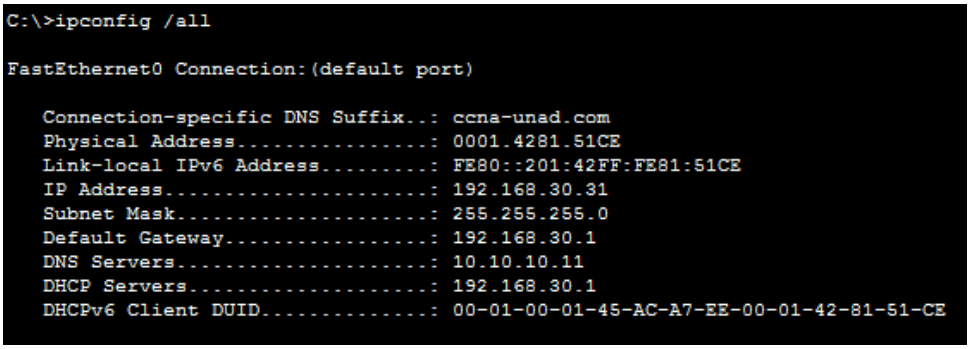


Fuente: Cisco Packet Tracer 7.0.2.0226

Se escribe el comando **ipconfig /all** para mostrar toda la configuración de direccionamiento.

PC-A

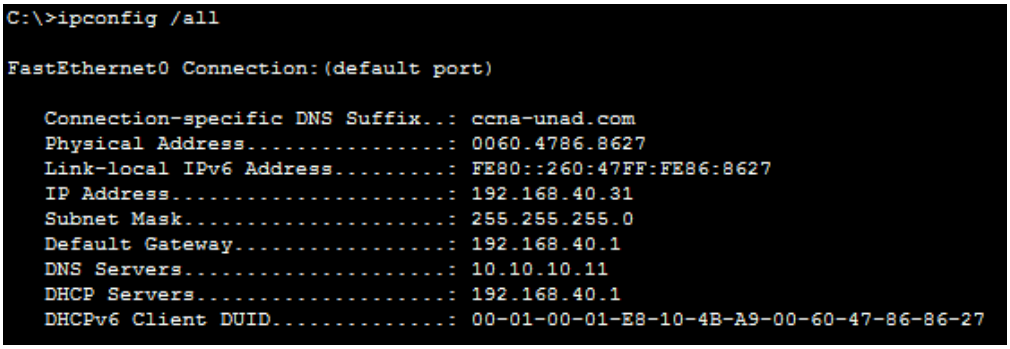
Figura 255 Verificación Direccionamiento DHCPv4 PC-A



Fuente: Cisco Packet Tracer 7.0.2.0226

PC-C

Figura 256 Verificación Direccionamiento DHCPv4 PC-C

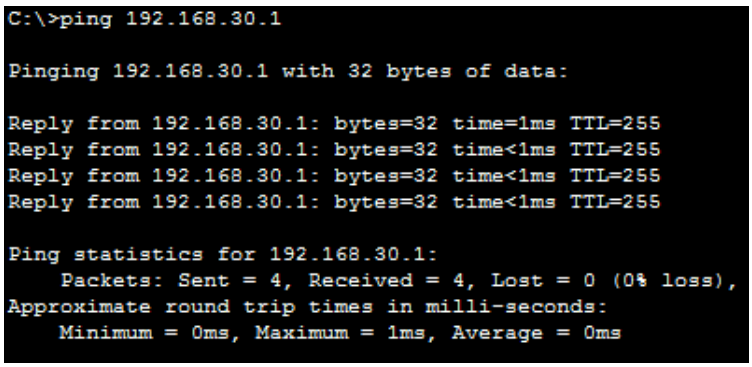


Fuente: Cisco Packet Tracer 7.0.2.0226

Verificación de conectividad

Ping PC-A a R1.

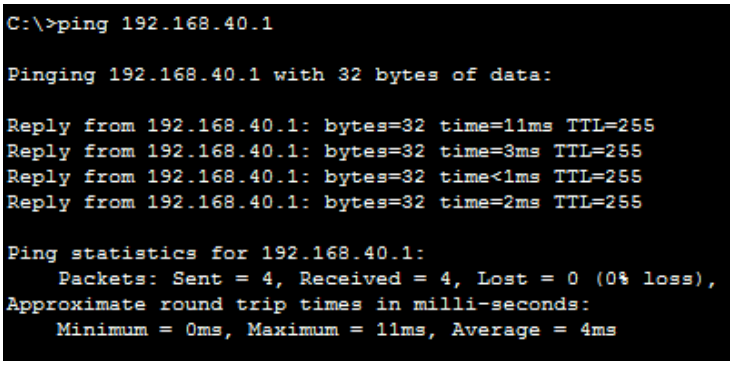
Figura 257 Verificación Conectividad DHCPv4. Ping PC-A a R1



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-C a R1.

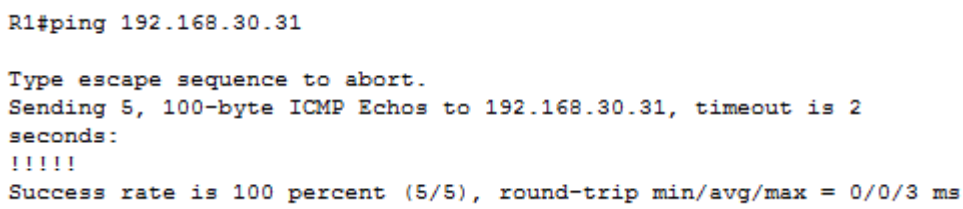
Figura 258 Verificación Conectividad DHCPv4. Ping PC-C a R1



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping R1 a PC-A.

Figura 259 Verificación Conectividad DHCPv4. Ping R1 a PC-A.



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping R1 a PC-C.

Figura 260 Verificación Conectividad DHCPv4. Ping R1 a PC-C

```
R1#ping 192.168.40.31

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.31, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms
```

Fuente: Cisco Packet Tracer 7.0.2.0226

1.2.10. Parte 10: Configurar NAT

Configurar NAT en R2 para permitir que los hosts puedan salir a internet.

Configuración del servidor web simulado

- ✓ Se crea un usuario local denominado con una contraseña cifrada con el comando de configuración global **username** *usuario* **privilege 15 secret** *contraseña.*
- ✓ Se habilita el servicio del servidor HTTP con el comando de configuración global **ip http server.**
- ✓ Se configura el servicio HTTP para utilizar la base de datos local con el comando de configuración global **ip http authentication local**.

R2#config t

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

R2(config)#username webuser privilege 15 secret webpass

R2(config)#ip http server

^

% Invalid input detected at '^' marker.

R2 no soporta la configuración para simular el servidor, NO PERMITE habilitar el servicio del servidor HTTP.

No se puede continuar con las demás configuraciones:

- ✓ Configuración de routing estático donde se crean rutas estáticas de R2 a R1 y R3 usando el rango asignado de direcciones de red publicas con el comando **ip route** y la creación de rutas predeterminadas de R1 y R3 a R2 con el comando **ip route 0.0.0.0 0.0.0.0** *Direccion-R2*.
- ✓ Configuración de la asignación estática donde se indica al router que traduzca entre la dirección privada del servidor interno y la dirección pública. El comando de configuración global seria **ip nat inside source static** *Dirección-Servidor-Interno Dirección-Publica.*

NAT CON SOBRECARGA

Para configurar NAT con sobrecarga se realiza lo siguiente:

- ✓ Se identifica la interfaz externa de cada router como la dirección global interna que se debe sobrecargar con la ACL 1. Se utiliza el comando de configuración global **ip nat inside source list 1 int** *interfaz-salida* **overload**
- ✓ Se configura la ACL 1 para permitir que NAT traduzca los dispositivos de la red en cuestión. Comando **access-list 1 permit** *Direccion-Red Mascara de Wildcard.*
- ✓ Se configura la interfaz NAT externa adecuada con el comando **ip nat outside** dentro de la configuración de interfaz.
- ✓ Se configura la interfaz NAT Interna adecuada con el comando **ip nat inside** dentro de la configuración de interfaz.

Se sumarizan las las redes y subredes.

R1 (BOGOTA)

- ✓ VLAN 40.

Red Interna 1: 192.168.99.3/24

- ✓ VLAN 30

Red Interna 2: 192.168.99.2/24

OSPF Area 0

- ✓ R1 y R2.

Subred Interna 1: 172.31.21.0/30.

- ✓ R2 y R3.

Subred Interna 2: 172.31.23.0/30.

R2 (MIAMI) PC-INTERNET

Red Interna: 209.165.200.224/29. No es encesario sumarizar.

Para sumarizar las redes se convierten a su equivalente en binario y se examinan las coincidencias

R1 (BOGOTA)

Tabla 39 Sumarización R1

Red Interna 1	11000000	.	10101000	.	01100011	.	00000011
Red Interna 2	11000000	.	10101000	.	00000110	.	00000010
Se coloca un cero en todos los bits que no coinciden.							
Red Sumarizada	11000000	.	10101000	.	00000000	.	00000000

Fuente: Autoría Propia.

Se convierte a su equivalente en decimal: 192.168.0.0/17.

OSPF Area 0

Tabla 40 Sumarización OSPF Area 0

Subred Interna 1	10101100	.	00011111	.	00010101	.	00000011
Subred Interna 2	10101100	.	00011111	.	00010111	.	00000010
Se coloca un cero en todos los bits que no coinciden.							
Subred Sumarizada	10101100	.	00011111	.	00010100	.	00000000

Fuente: Autoría Propia.

Se convierte a su equivalente en decimal 172.31.20.0/22.

Configuracion NAT

R2(config)#ip nat inside source list 1 int f0/1 overload

R2(config)#access-list 1 permit 192.168.0.0 0.0.127.255

R2(config)#access-list 1 permit 172.31.20.0 0.0.7.255

R2(config)#access-list 1 permit 209.165.200.224 0.0.0.7

R2(config)#int f0/1

R2(config-if)#ip nat outside

R2(config-if)#int f0/0

R2(config-if)#ip nat inside

R2(config-if)#int s0/0

R2(config-if)#ip nat inside

R2(config-if)#int s0/1

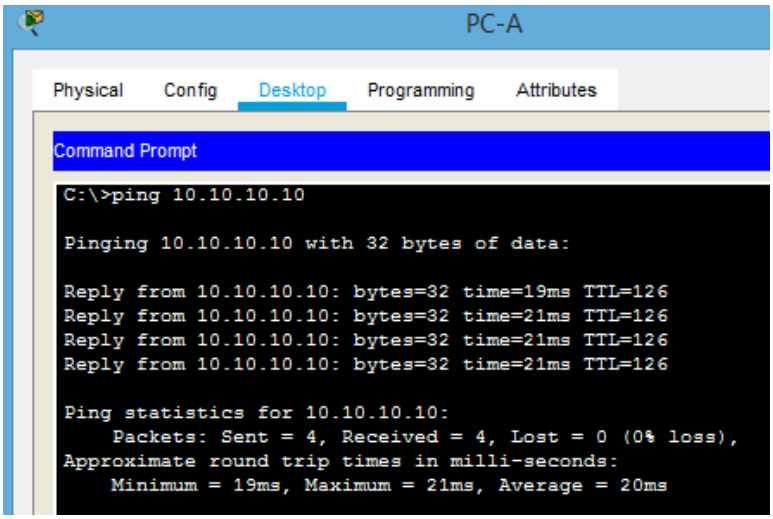
R2(config-if)#ip nat inside

R2(config-if)#

Verificación Conectividad

Ping PC-A a Web Server

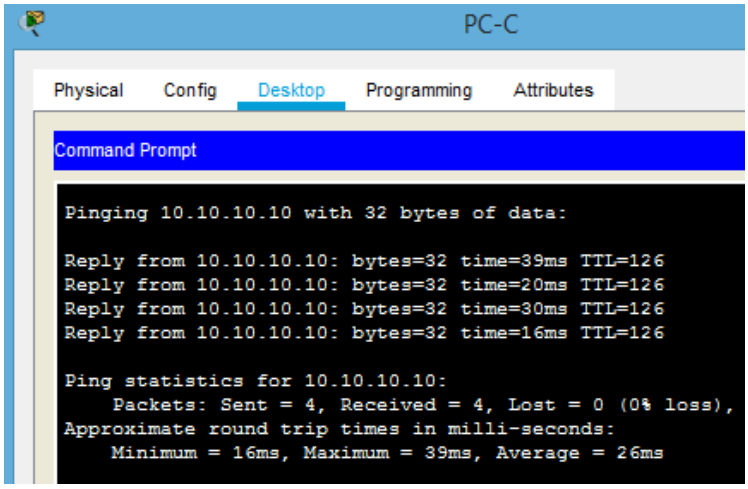
Figura 261 Verificación Conectividad. Ping PC-A a Web Server



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC-C a Web Server

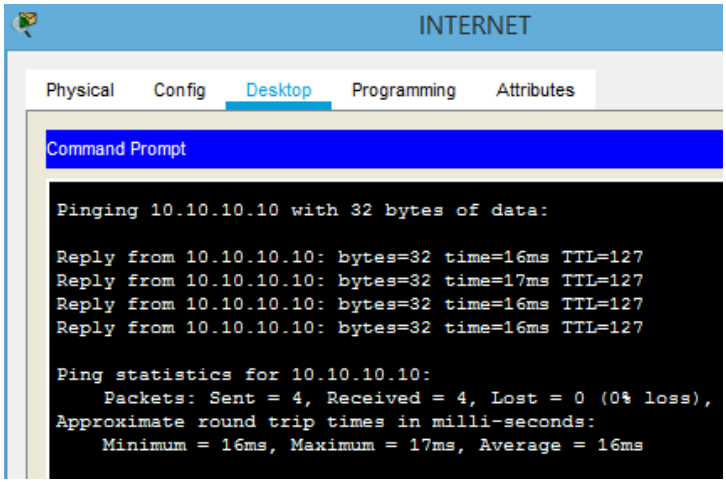
Figura 262 Verificación Conectividad. Ping PC-C a Web Server



Fuente: Cisco Packet Tracer 7.0.2.0226

Ping PC--INTERNET a Web Server

Figura 263 Verificación Conectividad. Ping PC-INTERNET a Web Server



Fuente: Cisco Packet Tracer 7.0.2.0226

Verificacipón Traducciones de NAT en R2

Figura 264 Tabla de Traducciones NAT R2

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 10.10.10.1:1024   209.165.200.230:5  10.10.10.10:5      10.10.10.10:1024
icmp 10.10.10.1:1025   209.165.200.230:6  10.10.10.10:6      10.10.10.10:1025
icmp 10.10.10.1:1026   209.165.200.230:7  10.10.10.10:7      10.10.10.10:1026
icmp 10.10.10.1:1027   209.165.200.230:8  10.10.10.10:8      10.10.10.10:1027
icmp 10.10.10.1:5      192.168.40.31:5    10.10.10.10:5      10.10.10.10:5
icmp 10.10.10.1:6      192.168.40.31:6    10.10.10.10:6      10.10.10.10:6
icmp 10.10.10.1:7      192.168.40.31:7    10.10.10.10:7      10.10.10.10:7
icmp 10.10.10.1:8      192.168.40.31:8    10.10.10.10:8      10.10.10.10:8
```

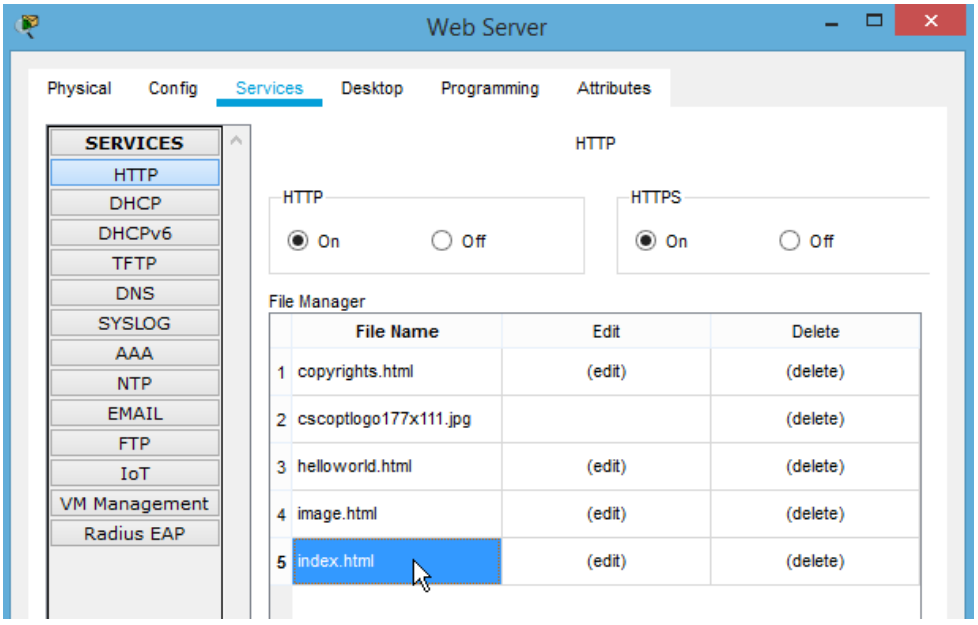
Fuente: Cisco Packet Tracer 7.0.2.0226

CONFIGURACIÓN WEB SERVER

Servicios web en Web Server

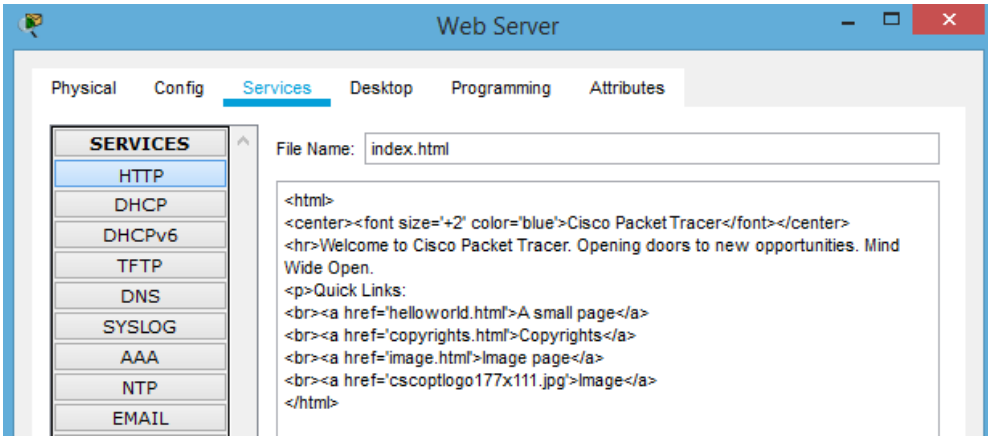
- ✓ Se hace clic en Web Server y, a continuación, se hace clic en la ficha **Services** > **HTTP**.
- ✓ Se hace clic en On (Activar) para habilitar **HTTP** y **HTTP** seguro (**HTTPS**).
- ✓ Optativo: se personaliza el código HTML.

Figura 265 Configuración de servicios Web Server



Fuente: Cisco Packet Tracer 7.0.2.0226

Figura 266 Index Editable Web Server

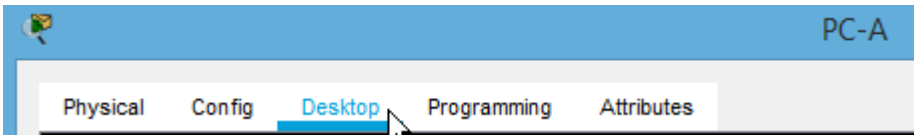


Fuente: Cisco Packet Tracer 7.0.2.0226

Verificar los servidores web mediante el acceso a las páginas web

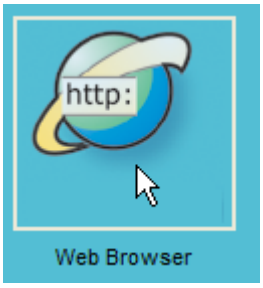
- ✓ Se hace clic en PC-A y, a continuación, se hace clic en la ficha **Desktop > Web Browser** (**Escritorio** > **Explorador Web**).

Figura 267 Verificar servicio web. Pestaña Desktop PC-A



Fuente: Cisco Packet Tracer 7.0.2.0226

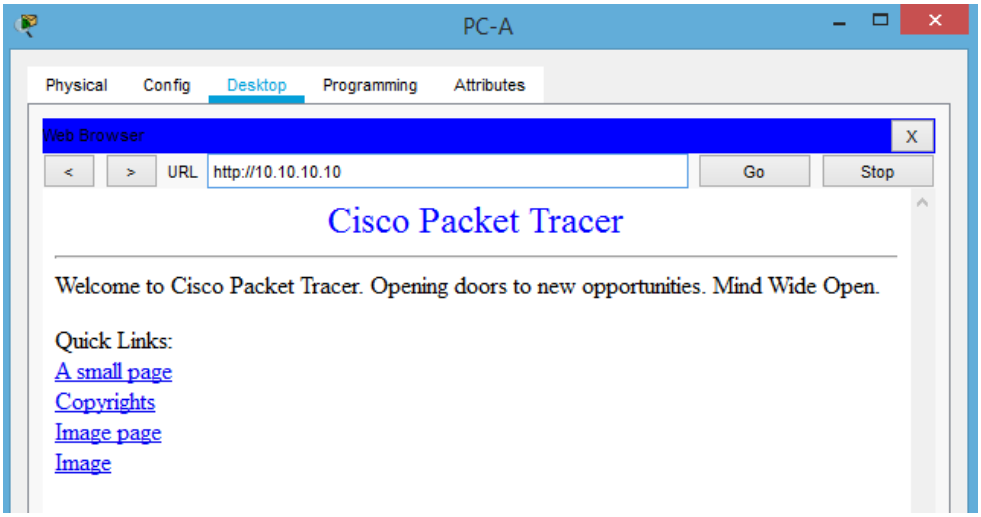
Figura 268 Botón Web Browser



Fuente: Cisco Packet Tracer 7.0.2.0226

✓ En el cuadro de dirección URL, se introduce **10.10.10.10** (dirección IP del servidor) y se hace clic en **Go** (Ir). Aparece el sitio Web de **Web Server**.

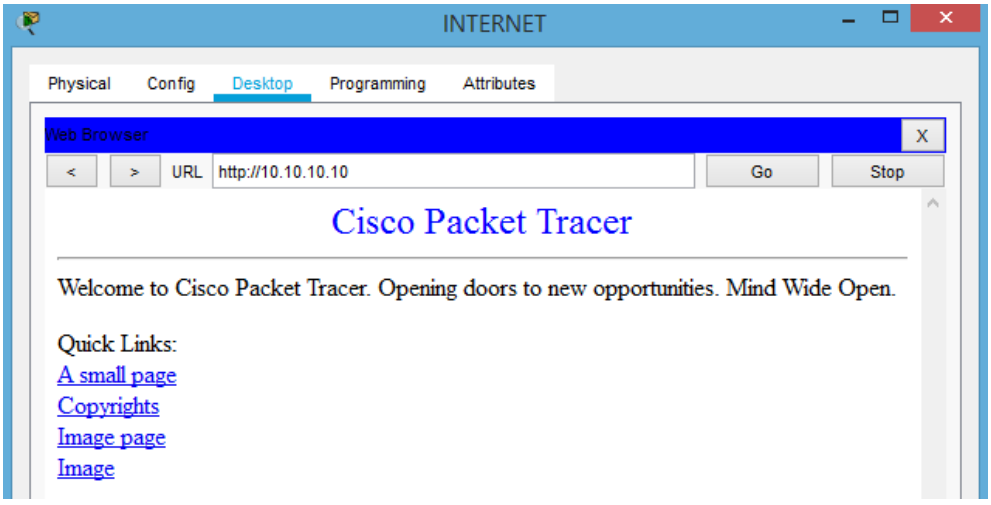
Figura 269 Acceso a internet PC-A



Fuente: Cisco Packet Tracer 7.0.2.0226

✓ Acceso a internet PC-INTERNET

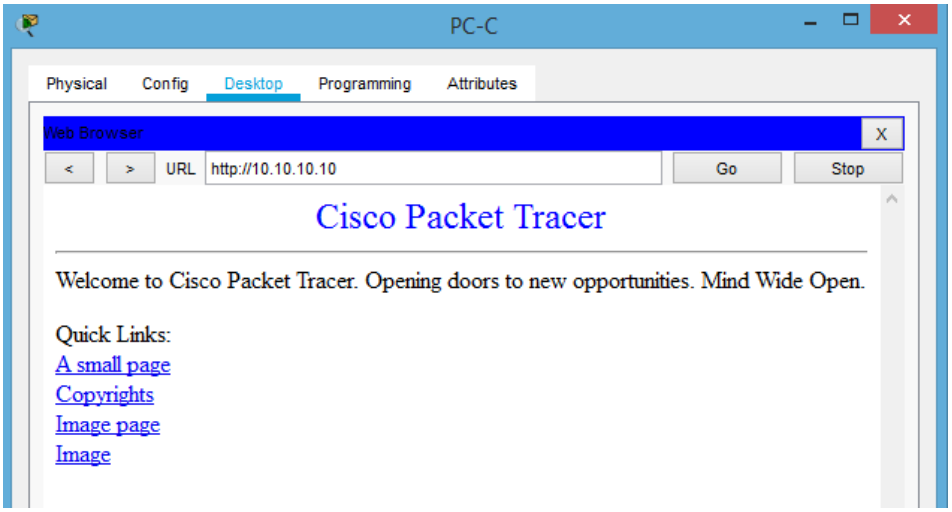
Figura 270 Acceso a internet PC-INTERNET



Fuente: Cisco Packet Tracer 7.0.2.0226

✓ Acceso a internet PC-C

Figura 271 Acceso a internet PC-C



Fuente: Cisco Packet Tracer 7.0.2.0226

1.2.11. Parte 11: Configurar Listas de Acceso Estándar

Una lista de control de acceso (ACL) es una lista de comandos del IOS que permite controlar si un router permite o descarta paquetes de acuerdo con la información que se encuentra en el encabezado del paquete. Este filtro se realiza a través de la información con la tabla de routing. Al aplicarla en una interfaz se realiza el proceso adicional para determinar si el paquete se puede reenviar.

Una ACL es una lista secuencial de instrucciones **permit** (permitir) o **deny** (denegar) conocidas como entradas de control de acceso (ACE).

El filtrado de paquetes consiste en la comparación de la información dentro del paquete con cada ACE, en orden secuencial y con esto, determinar si el paquete coincide con una de las ACE. El filtrado controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o descarte de estos de acuerdo con criterios determinados. Puede producirse en la capa 3 o capa 4.

ACL Estándar: filtran solo en la capa 3 (Red). Esta capa proporciona servicios para intercambiar los datos individuales en la red entre terminales identificados. Se suelen colocar lo mas cerca posible del destino.

ACL Extendida: filtran en las capas 3 y 4. La capa 4 (transporte) define los servicios para segmentar, transferir y reensamblar los datos para las comunicaciones individuales entre terminales. Se suelen colocar lo mas cerca posible del origen.

MASCARA DE WILDCARD

Permite determinar que bits de la dirección se deben examinar para obtener una coincidencia.

Palabras clave

Host: reemplaza la mascara 0.0.0.0. Esta mascara indica que todos los bits de las direcciones IPv4 deben coincidir para filtrar solo una dirección de host.

Any: reemplaza la dirección IP 0.0.0.0 y la máscara 255.255.255.255. Esta mascara establece que se omita la dirección IPv4 completa o se acepte cualquier dirección.

Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

Para crear una lista de control de acceso estándar se realiza lo siguiente:

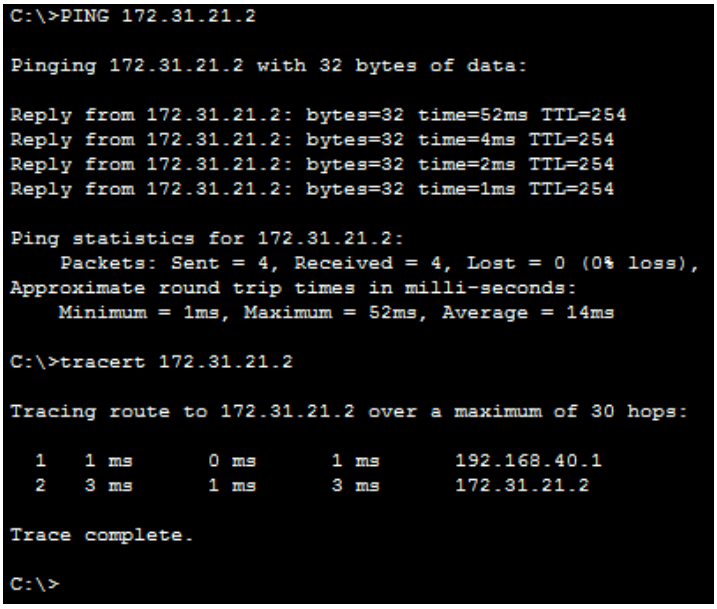
- ✓ Se define una ACL estándar numerada con un número entre 1 y 99 con el comando de configuración global **access-list** *numero.*
- ✓ Se define una ACL estándar nombre con el comando de configuración global **ip access-list standard** *nombre-alfanumerico.* Después de emitir este comando el router entra en la configuración estándar (std) de ACL con nombre (nacl).
- ✓ Se define un comentario sobre la ACL para mayor comprensión y análisis con el comando **remark** *descripción.* Este paso es optativo.
- ✓ Se deniega o permite el acceso con las palabras reservadas **permit** o **deny.**
- ✓ Se define el origen, bien sea la dirección IP desde donde se envía el paquete o se utiliza la palabra clave **any** como abreviatura.
- ✓ Se define la máscara de wildcard para aplicar al origen. Este paso es optativo.

- **ACL 1**

Se crea una lista de acceso en R1 y R2 para que ningún host de la VLAN 30 pueda generar tráfico hacia R2.

Primero se verifica la conectividad entre PC-C y R2.

Figura 272 Verificación Ping y Tracert PC-A a R2



Fuente: Cisco Packet Tracer 7.0.2.0226

Se aprecia un ping exitoso y los saltos que hace el paquete.

Configuracion SSH en R2

- ✓ Se ingresa al modo de configuración global del router.
- ✓ Se restablecen los valores por defecto de las líneas vty previamente configuradas con ayuda del comando **no** seguido de las instrucciones.
- ✓ Se configura nombre del dominio con el comando **ip domain-name** *dominio*.
- ✓ Se genera una llave publica de 1024 bits con el comando **crypto key generate rsa** y luego se especifican los bits. El protocolo SSH cifra todos los datos enviados y recibidos a través del puerto 22.
- ✓ Se configura el tiempo de espera con el comando **ip ssh time-out** *tiempo-segundos*. Despues del tiempo en segundos establecido de inicializar la conexión, el usuario no introduce su usuario y contraseña, se cierra la conexión y deberá establecer una nueva sesion.
- ✓ Se establece un máximo de tres intentos para que un con el comando **ip ssh authentication-retries** *numero-intentos*. De esta manera el usuario se autentica en el sistema. De lo contrario el usuario deberá restablecer una nueva sesión.

- ✓ Se establece la versión del protocolo SSH que se utiliza con el comando **ip ssh version 2**. Para este caso se establece la versión 2. La versión 1 tiene un fallo de seguridad terrible. No se recomienda su uso bajo ninguna circunstancia.
- ✓ Se habilitan cinco puertos virtuales para las conexiones VTY con el comando **line vty 0 4**. Tras hacer esto se mostrará un mensaje de habilitación de SSH.
- ✓ Se establece que el protocolo a utilizar para conexiones remotas será SSH con el comando **transport input ssh**
- ✓ Se configura que la validación de los usuarios que ingresen al equipo a través de SSH. Se realizará de manera local, es decir, verificando el **usuario** y **contraseña** estén debidamente creados en el Cisco IOS. Se utiliza le comando login local
- ✓ Se sale del modo de configuración de línea con el comando **exit**.
- ✓ Se crea un **usuario** y **contraseña** para poder establecer la conexión al equipo a través de SSH. Se utiliza el comando **username** *usuario* **password** *contraseña*.

R2

R2#config t

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

R2(config-line)#no password

R2 (config-line)# no exec-timeout 15 0

R2 (config-line)# no login

R2 (config-line)# no logging synchronous

R2(config)#ip domain-name R2

R2(config)#crypto key generate rsa

The name for the keys will be: R2.R2

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R2(config)#ip ssh time-out 60

R2(config)#ip ssh authentication-retries 3

R2(config)#ip ssh version 2

R2(config)#line vty 0 4

*mar 1 2:43:3.129: %SSH-5-ENABLED: SSH 2 has been enabled

R2(config-line)#transport input ssh

R2(config-line)#login local

R2(config-line)#exit

R2(config)#username davidadmin01 password jdmgcisco2019

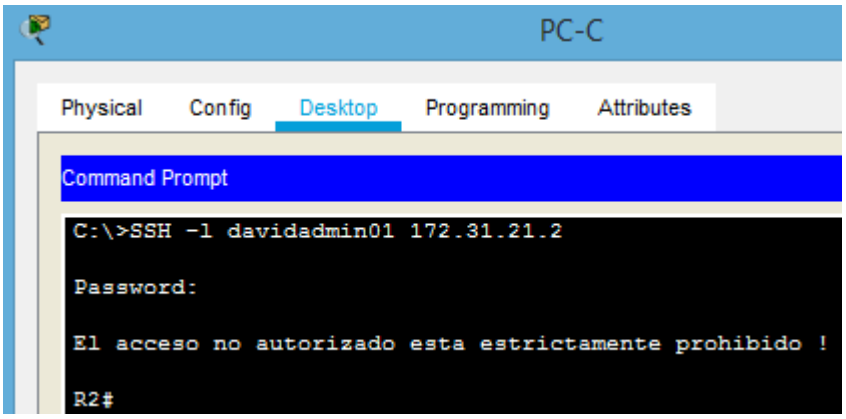
Verificacion conexión SSH

Desde la PC-C se establece una conexión SSH con R2 a la interfaz S0/1.

En la consola de comandos se utiliza la siguiente isntruccion:

ssh -letra ele minúscula *usuario-SSH dirección-destino*

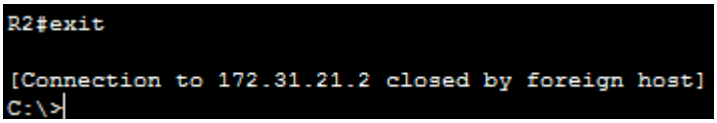
Figura 273 Acceso SSH a R2 desde PC-C



Fuente: Cisco Packet Tracer 7.0.2.0226

Para cerrar la conexión se ingresa el comando **exit.**

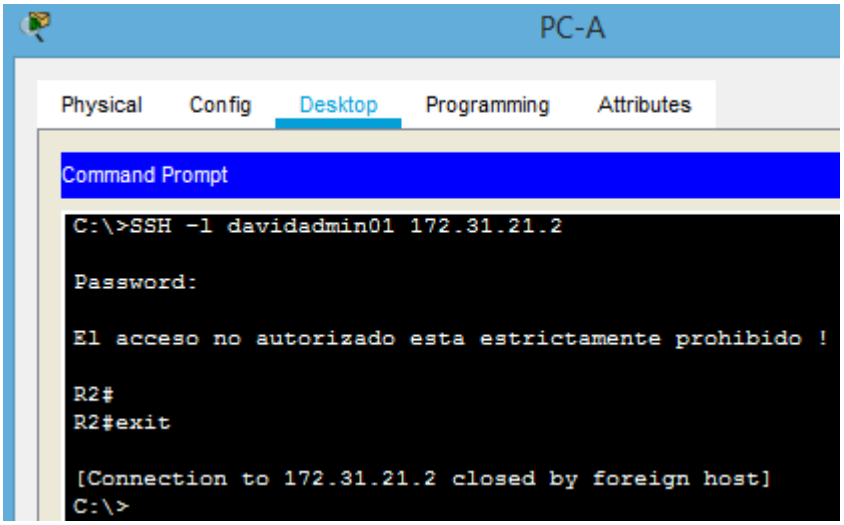
Figura 274 Cerrar conexión entre PC-C y R2



Fuente: Cisco Packet Tracer 7.0.2.0226

- ✓ Acceso a R2 desde PC-A

Figura 275 Acceso SSH a R2 desde PC-A



Fuente: Cisco Packet Tracer 7.0.2.0226

Se configuran dos listas de acceso: una para R1 y una para R2 especificando que solo se permite el trafico de la red 192.168.40.0.

Comando access-class

Restringe las conexiones de entrada y salida entre la vty determinada y las direcciones de la lista de acceso.

- ✓ Se ingresa al modo de configuración de líneas vty con el comando de confioguracion global **line vty** *líneas.*
- ✓ Se configura el trafico entrante con el comando **access-class** *ID o nombre de ACL* **in/out**
  - ✓ **in:** limita las conexiones de entrada entre las direcciones de la ACL y el dispositivo.

- ✓ **out:** limita las conexiones de salida entre un dispositivo en particular y las direcciones en la ACL.

R1

R1(config)#ip access-list standard ACL-R1-2019

R1(config-std-nacl)#remark Permite el trafico de la red 192.168.40.0 de la VLAN 40 hacia R2

R1(config-std-nacl)#permit 192.168.40.0 0.0.0.255

R1(config-std-nacl)#exit

R1(config)#line vty 0 4

R1(config-line)#access-class ACL-R1-2019 out

R1(config-line)#

R2

R2(config)#ip access-list standard ACL-R1-2019

R2(config-std-nacl)#remark Permite el trafico de la red 192.168.40.0 de la VLAN 40 hacia R2

R2(config-std-nacl)#permit 192.168.40.0 0.0.0.255

R2(config-std-nacl)#exit

R2(config)#line vty 0 4

R2(config-line)#access-class ACL-R1-2019 in

R2(config-line)#

Verificacion de listas

- ✓ Se escribe el comando de configuración global **do show access-list** para visualizar las listas de acceso creadas.
- ✓ Para visualizar la descripción de la lista de acceso con nombre se revisa la configuración de ejecución con el comando del modo EXEC privilegiado **show running-config | begin ip access-list** para filtrar los resultados**.**

R1

Figura 276 Verificación ACL 1 Estándar nombrada en R1

```
R1(config)#do show access-list
Standard IP access list ACL-R1-2019
    10 permit 192.168.40.0 0.0.0.255

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show running-config | begin ip access-list
ip access-list standard ACL-R1-2019
 remark Permite el trafico de la red 192.168.40.0 de la VLAN 40 hacia R2
 permit 192.168.40.0 0.0.0.255
!
```

Fuente: Cisco Packet Tracer 7.0.2.0226

R2

Figura 277 Verificación ACL 1 Estándar nombrada en R2

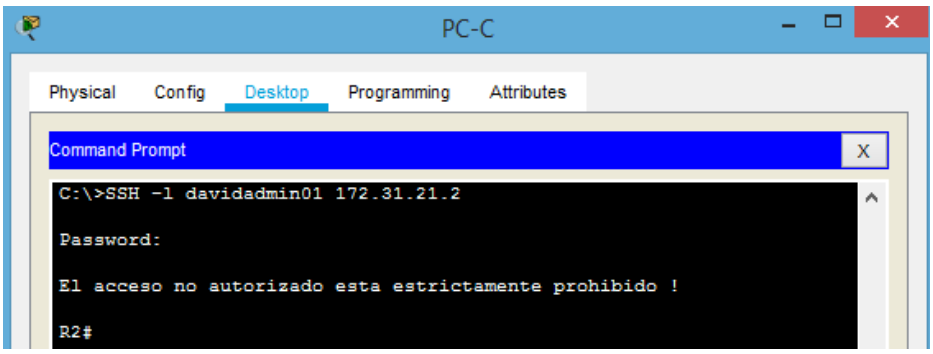
```
R2(config)#do show access-lis
Standard IP access list 1
    10 permit 192.168.0.0 0.0.127.255 (26 match(es))
    20 permit 172.31.16.0 0.0.7.255
    30 permit 209.165.200.224 0.0.0.7 (8 match(es))
Standard IP access list ACL-R1-2019
    10 permit 192.168.40.0 0.0.0.255

R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show running-config | begin ip access-list
ip access-list standard ACL-R1-2019
 remark Permite el trafico de la red 192.168.40.0 de la VLAN 40 hacia R2
 permit 192.168.40.0 0.0.0.255
!
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Verificacion de conectividad SSH

- ✓ PC-C

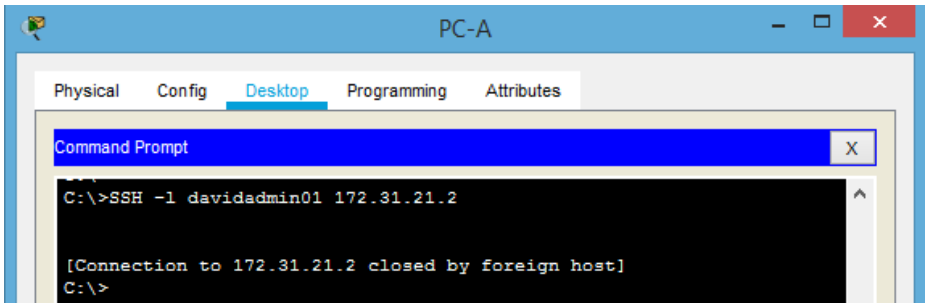
Figura 278 Acceso SSH a R2 desde PC-C con ACL 1



Fuente: Cisco Packet Tracer 7.0.2.0226

- ✓ PC-A

Figura 279 Acceso SSH a R2 desde PC-C con ACL 1



Fuente: Cisco Packet Tracer 7.0.2.0226

- **ACL 2**

Se crea una lista de acceso para permitir trafico solo de PC-A a R2.

R1

R1(config)#access-list 11 permit 192.168.30.1 0.0.0.255

R1(config)#line vty 0 4

R1(config-line)#access-class 11 out

R1(config-line)#

R2

R2(config)#access-list 11 permit 192.168.30.1 0.0.0.255

R2(config)#line vty 0 4

R2(config-line)#access-class 11 in

R2(config-line)#

Nota: La clase de acceso en R1 se configura como saliente porque se busca estar lo mas cerca posible al destino.

Claro esta que configurar una dirección IP que se obtuvo por DHCP no es muy practico porque esta dirección cambia pero se realiza con fines prácticos.

Verificacion de listas

R1

Figura 280 Verificación ACL 2 Estándar numerada en R1

```
R1(config)#do show access-list
Standard IP access list ACL-R1-2019
    10 permit 192.168.40.0 0.0.0.255
Standard IP access list 11
    10 permit 192.168.30.0 0.0.0.255
```

Fuente: Cisco Packet Tracer 7.0.2.0226

R2

Figura 281 Verificación ACL 2 Estándar numerada en R2

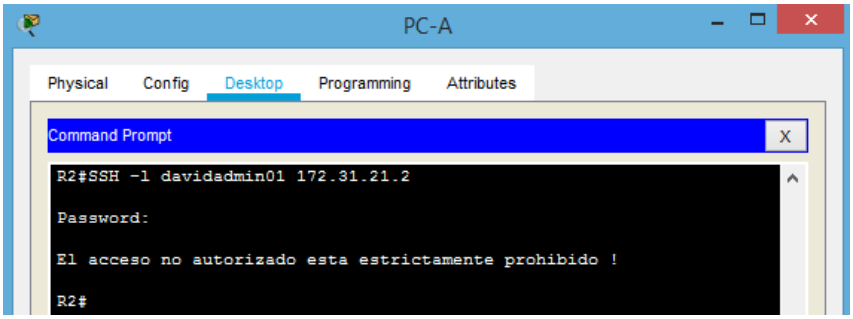
```
R2(config)#do show access-list
Standard IP access list 1
    10 permit 192.168.0.0 0.0.127.255 (26 match(es))
    20 permit 172.31.16.0 0.0.7.255
    30 permit 209.165.200.224 0.0.0.7 (8 match(es))
Standard IP access list ACL-R1-2019
    10 permit 192.168.40.0 0.0.0.255 (2 match(es))
Standard IP access list 11
    10 permit 192.168.30.0 0.0.0.255
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Las instrucciones **deny** y **permit** hacen seguimiento dee las estadísticas de coincidencias. Cada ACL posee una instrucción deny any implícita como ultima instruccion La palabra **match** indica el seguimiento.

Verificacion Conexión

Figura 282 Acceso SSH desde PC-A a R2 con ACL 2



Fuente: Cisco Packet Tracer 7.0.2.0226

1.2.12. Parte 12: Configurar Listas de Acceso Extendidas

Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

El proceso es similar a la creación de una ACL Estandar, la diferencia radica en que se especifica el protocolo al cual se le dará permiso junto con otros parámetros de configuración.

- **ACL1**

Una ACL extendida permite indicar el protocolo que se permitirá o denegará.

R1(config)#ip access-list extended ACL-EXTENDIDA-2019
R1(config-ext-nacl)#permit icmp 192.168.30.0 0.0.0.255 host 172.31.21.2 echo
R1(config-ext-nacl)#deny icmp 192.168.40.0 0.0.0.255 host 172.31.21.2 echo
R1(config-ext-nacl)#exit

- ✓ Se asigna la lista a la interfaz.
- ✓ Se ingresa al modo de configuración de interfaz con el comando de configuración global **int** *ID-Interfaz.*
- ✓ Se asigna la ACL a la interfaz con el comando **ip access-group** *ID-ACL/Nombre-ACL* **in/out.**

Como es una ACL extendida se debe asignar a la interfaz mas cercana al origen, por tal motivo se asigna a la **interfaz f0/0 entrante** para que se ejecute la acción apenas entra el paquete.
R1(config)#int f0/0
R1(config-if)#ip access-group ACL-EXTENDIDA-2019 in

R1(config-if)#

Nota: siempre que se configure una lista de acceso se debe primero indicar que se permite y luego lo que se deniega porque las listas de acceso se ejecutan en forma secuencial.

Verificacion de lista

Figura 283 Verificación ACL Extendida 1 numerada en R1

```
R1(config)#do show access-list
Standard IP access list 11
    10 permit 192.168.30.0 0.0.0.255
Extended IP access list ACL-EXTENDIDA-2019
    10 permit icmp 192.168.30.0 0.0.0.255 host 172.31.21.2 echo (4 match(es))
    20 deny icmp 192.168.40.0 0.0.0.255 host 172.31.21.2 echo (4 match(es))
```

Fuente: Cisco Packet Tracer 7.0.2.0226

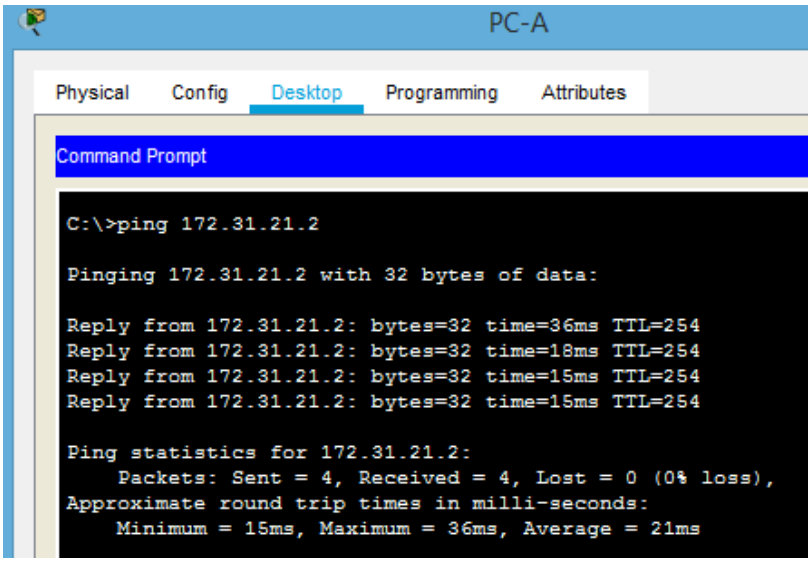
Verificacion Conectividad

Esta lista no permite hacer ping de ningún host que pertenezca a la VLAN 30.

Se intenta hacer ping a R2 desde la PC-A pero si a los PC que pertenezcan a la VLAN 40.

Ping PC-A a R2

Figura 284 Conectividad. Ping PC-A a R2 con ACL Extendida 1

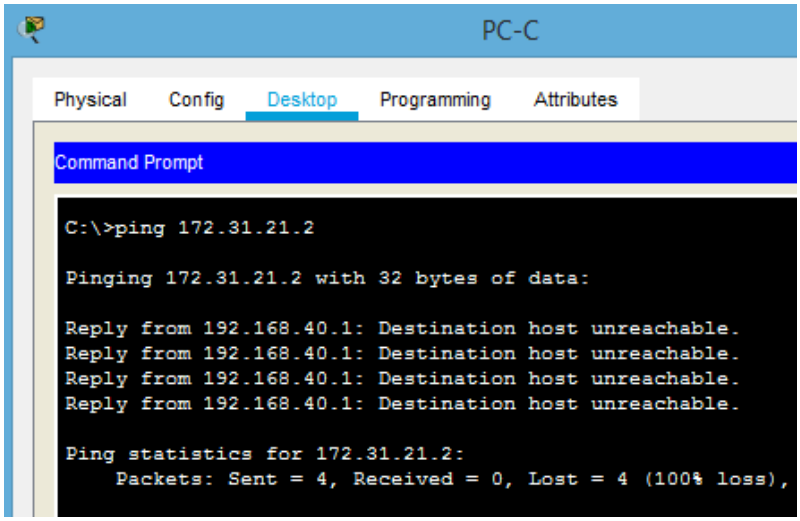


Fuente: Cisco Packet Tracer 7.0.2.0226

Se muestra mensaje de destino inalcanzable.

Ping PC-C a R2

Figura 285 Conectividad. Ping PC-C a R2 con ACL Extendida 1



Fuente: Cisco Packet Tracer 7.0.2.0226

- **ACL 2**

Se crea una lista de acceso que no permite el trafico ICMP RESPUESTA ECO de R3 a R2.

R3(config)#access-list 170 deny icmp any host 172.31.23.1 echo-reply

- ✓ Tras configurar la lista de acceso se muestran dos mensajes de notificación donde se indica que el vecino de R3 es decir, R2 se ha dado de baja.

07:37:33: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/1 from FULL to DOWN, Neighbor Down: Dead timer expired

07:37:33: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

- ✓ Se asigna la lista de acceso a la interfaz.

R3(config-if)#int s0/0

R3(config-if)#ip access-group 170 out

R3(config-if)#exit

Verificacion de lista.

Figura 286 Verificación ACL Extendida 2 en R3

```
R3(config)#do show access-list
Extended IP access list 170
    10 deny icmp any host 172.31.23.1 echo-reply
```

Fuente: Cisco Packet Tracer 7.0.2.0226

Verificacion de conectividad

Ping de R3 a R2

Figura 287 Conectividad. Ping R3 a R2

```
R3#ping 172.31.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Fuente: Cisco Packet Tracer 7.0.2.0226

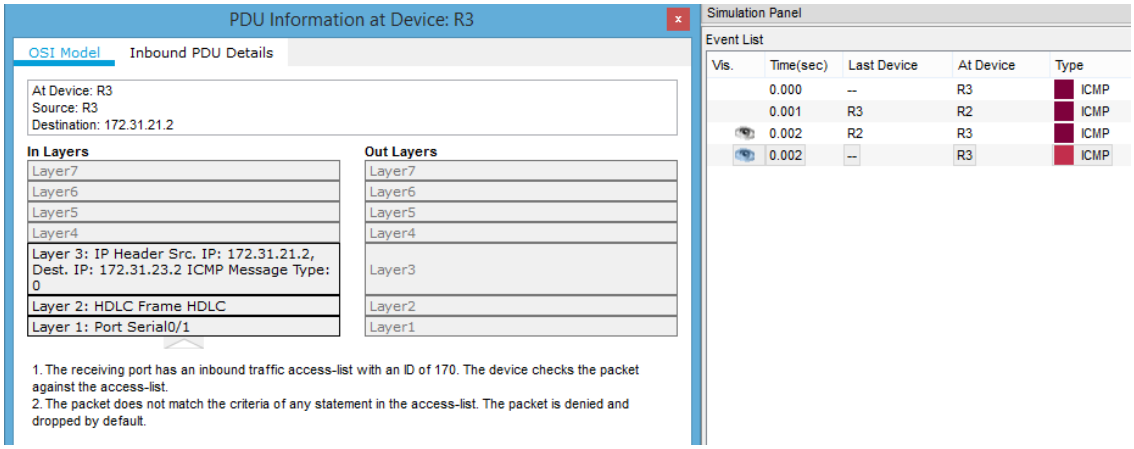
Diagnóstico

La PDU de R3, en la capa de entrada 3 indica:

1. El puerto de recepción tiene una lista de acceso de tráfico entrante con una ID de 170. El dispositivo compara el paquete con la lista de acceso.
2. El paquete no coincide con los criterios de ninguna declaración en la lista de acceso. El paquete es denegado y eliminado de forma predeterminada.

3.

Figura 288 Comprobación funcionamiento ACL Extendida 2 en R3



Fuente: Cisco Packet Tracer 7.0.2.0226

NOTA ADICIONAL:

Se guardo toda la configuración de ejecución en la configuración de inicio para cada dispositivo.

CONCLUSIONES

- Se aplica el conocimiento adquirido a partir de la lectura de los módulos y desarrollo de prácticas de laboratorio propuestas en CCNA-1 y CCNA-2 durante el desarrollo del diplomado de profundización CISCO (Diseño e Implementación de Soluciones Integradas LAN/WAN)
- Se realizan rutinas de diagnóstico y resolución de problemas.
- Se realizan las configuraciones básicas en los diferentes dipositivos que componen las redes.
- Se establece la conexión lógica de los equipos con base en las topologías.
- Se configura el enrutamiento en la red usando el protocolo RIP versión 2 y OSPF versión 2.
- Se configura el enrutamiento estático y rutas predeterminadas IPv4.
- Se calculan rutas resumidas IPv4.
- Se aplica la división de subredes VLSM.
- Se analizan los resultados de la tabla de routing.
- Se configura el encapsulamiento PPP y autenticación PAP y CHAP.
- Se configura la traducción de direcciones NAT con sobrecarga para IPv4.
- Se configura enrutamiento dinámico mediante DHCPv4.
- Se premite difusión de rutas a traves de routers.
- Se configura el routing entre VLAN basado en enlaces troncales 802.1Q
- Se realiza la configuración de ACLs estándar, ACLs estándar con nombre y ACLs en líneas VTY..
- Se establecen conexiones remotas mediante SSH.
- Se verifican todas las configuraciones realizadas con el uso de los diferentes comandos show.
- Se verifica la convergencia y conectividad de las redes.

BIBLIOGRAFÍA

Cisco Networking Academy. Asignación de direcciones IP. Fundamentos de Networking [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1.

Cisco Networking Academy. Capa de red. Fundamentos de Networking [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1.

Cisco Networking Academy. Capa de Transporte. Fundamentos de Networking [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1.

Rm-rf Administración de Sistemas. Cisco IOS Interface status Codes *[en linea], 26 de agosto de 2012. [revisado 10 Mayo 2019]. Disponible en Internet:* http://rm-rf.es/cisco-ios-interface-status-codes/*.*

Cisco Networking Academy. Conceptos de Routing. Principios de Enrutamiento y Conmutación [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1.

Universidad Nacional Abierta y a Distancia. Configuración de Switches y Routers [OVA en linea], 18 de marzo de 2012. [revisado 10 Mayo 2019]. Disponible en Internet: https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC.

Cisco Networking Academy. Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1.

Cisco Networking Academy. DHCP. Principios de Enrutamiento y Conmutación *[en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet:* https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1*.*

Cisco Networking Academy. Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación *[en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet:* https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1*.*

Cisco Networking Academy. Enrutamiento Estático. Principios de Enrutamiento y Conmutación [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1.

Cisco Networking Academy. Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1.

Cisco Networking Academy. Ethernet. Fundamentos de Networking [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1.

Cisco Networking Academy. Exploración de la red. Fundamentos de Networking [en linea], 2014 [revisado 10 Mayo 2019]. Disponible en Internet. https://static-courseassets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1.

Cisco Networking Academy. Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1.

Cisco Networking Academy. Listas de control de acceso. Principios de Enrutamiento y Conmutación *[en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet:* https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1.

Cisco Networking Academy.Soluciones de Red. Fundamentos de Networking [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1.

Cisco Networking Academy. SubNetting. Fundamentos de Networking [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1.

Cisco Networking Academy. OSPF de una sola área. Principios de Enrutamiento y Conmutación *[en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet:* https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1.

Cisco Networking Academy. Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación *[en linea], 2014. [revisado 10 Mayo 2019]. Disponible*

en Internet: https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1.

Cisco Networking Academy. VLANs. Principios de Enrutamiento y Conmutación [en linea], 2014. [revisado 10 Mayo 2019]. Disponible en Internet: https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1.

Pizarro, Valeria. Citas y referencias eléctronicas en normas ICONTEC [en linea], 8 de marzo de 2017 [revisado 13 Mayo 2019]. Disposnible en Internet: http://www.normasicontec.org/referencias-electronicas-normas-icontec/.

Universidad Nacional Abierta y a Distancia. Diseño y configuración de redes con Packet Tracer [OVA en línea], 09 de abril de 2012 [revisado 10 Mayo 2019]. Disponible en Internet: https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9.

Universidad Nacional Abierta y a Distancia. PING y TRACER como estrategia en procesos de Networking [OVA en línea], 09 de abril de 2012 [revisado 10 Mayo 2019]. Disponible en Internet: https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3.

Universidad Nacional Abierta y a Distancia. Principios de Enrutamiento *[en linea], 9 de abril de 2012. [revisado 10 Mayo 2019]. Disponible en Internet:* https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm.