



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

DIPLOMADO DE PROFUNDIZACIÓN CISCO
UNIDAD 2 – MODELO OSI Y DIRECCIONAMIENTO IP
PASO 3: ACTIVIDAD COLABORATIVA 2

Edgar Yessid Ladino Abril COD. 1015412504
Carlos Manuel Mesa Méndez COD. 98632570
Juan David Rodríguez Gómez COD. 1019047577
Juan Camilo Bejarano Alarcón COD. 1019010161
Luis Fernando Quimbayo Calderon COD. 93134684

Grupo 203092_38

Presentado a

ING. JUAN CARLOS VESGA
Director del Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS – ECBTI
Noviembre de 2018

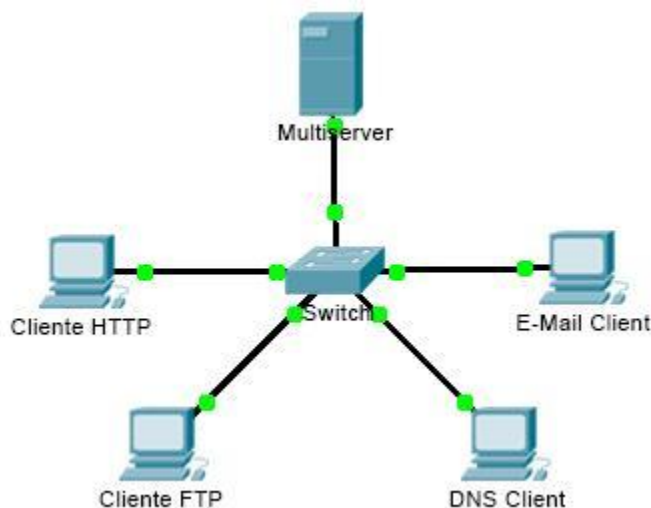
INTRODUCCIÓN

En el desarrollo del presente trabajo se pondrán en práctica los temas estudiados en la unidad dos del diplomado de profundización CISCO, en total se desarrollarán 22 ejercicios utilizando el simulador de red Packet Tracer.

Se identificarán y solucionarán problemas propios de las sub-redes y direccionamiento IP mediante el uso adecuado de estrategias basadas en comandos y estadísticas del IOS, con el cual se pretende fortalecer el desarrollo de competencias en el área de las redes orientadas al enrutamiento avanzado.

Ejercicio 7.3.1.2: Comunicaciones TCP y UDP

Topología



Objetivos

Parte 1: Generar tráfico de red en modo de simulación

Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

Información básica

El objetivo de esta actividad de simulación es proporcionar una base para comprender en detalle los protocolos TCP y UDP. El modo de simulación permite ver la funcionalidad de los diferentes protocolos.

A medida que los datos se trasladan por la red, se dividen en partes más pequeñas y se identifican de forma tal que se puedan volver a juntar. A cada una de estas partes se le asigna un nombre específico (unidad de datos del protocolo [PDU, protocol data unit]) y se la asocia a una capa específica. El modo de simulación de Packet Tracer le permite al usuario ver cada uno de los protocolos y las PDU asociadas. Los pasos que se detallan a continuación guían al usuario en el proceso de solicitud de servicios mediante diversas aplicaciones disponibles en una PC cliente.

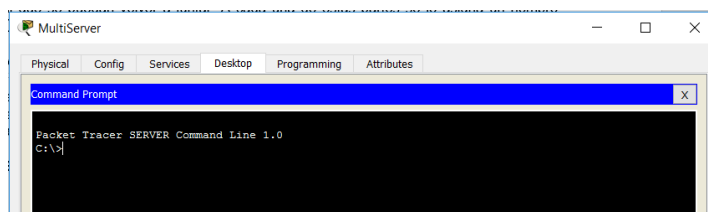
Esta actividad proporciona la oportunidad de explorar la funcionalidad de los protocolos TCP y UDP, la multiplexación y la función que cumplen los números de puerto para determinar qué aplicación local solicita o envía los datos.

Parte 1: Generar tráfico de red en modo de simulación

Paso 1: Generar tráfico para completar las tablas del protocolo de resolución de direcciones (ARP)

Para reducir la cantidad de tráfico de red que se ve en la simulación, realice lo siguiente:

- Haga clic en **MultiServer** y, a continuación, haga clic en la ficha **Desktop > Command Prompt** (Escritorio > Símbolo del sistema).



- Introduzca el comando **ping 192.168.1.255**. Esto toma unos segundos, ya que todos los dispositivos en la red responden a **MultiServer**.

```

Command Prompt
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=9ms TTL=128
Reply from 192.168.1.3: bytes=32 time=9ms TTL=128
Reply from 192.168.1.4: bytes=32 time=9ms TTL=128
Reply from 192.168.1.1: bytes=32 time=26ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 4, Received = 16, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 26ms, Average = 3ms

C:\>|

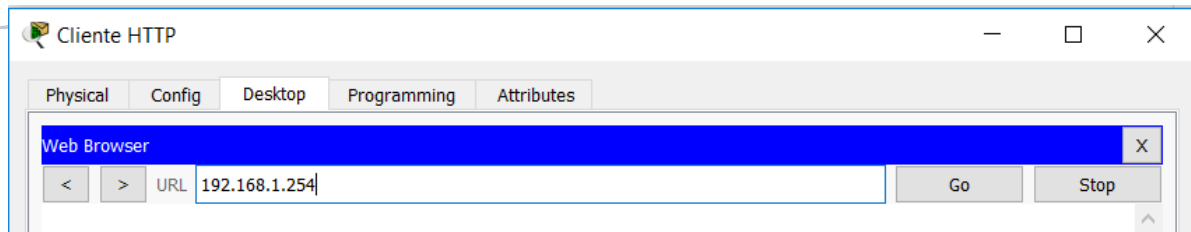
```

- Cierre la ventana de **MultiServer**.

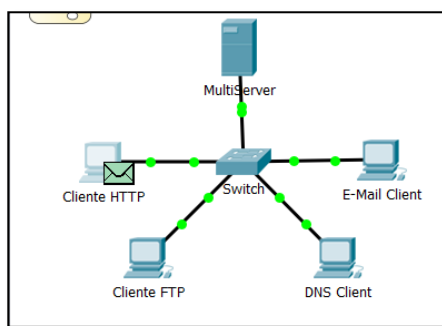
Paso 2: Genere tráfico web (HTTP).

- Cambie a modo de simulación.
- Haga clic en **HTTP Client** (Cliente HTTP) y, a continuación, haga clic en la ficha **Desktop > Web Browser** (Explorador Web).

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



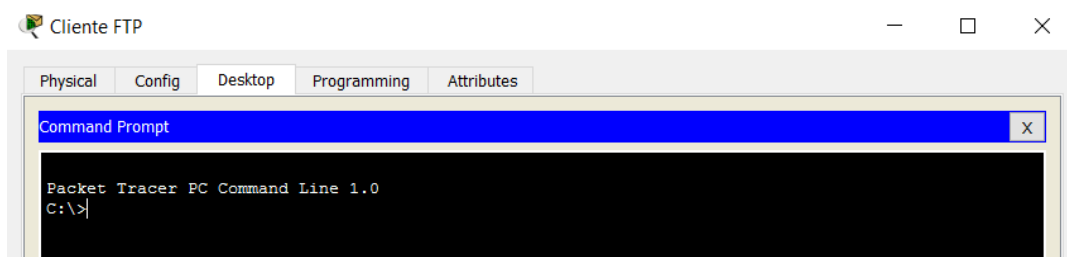
- c. En el campo de dirección URL, introduzca **192.168.1.254** y haga clic en **Go** (Ir). En la ventana de simulación, aparecerán sobres (PDU).



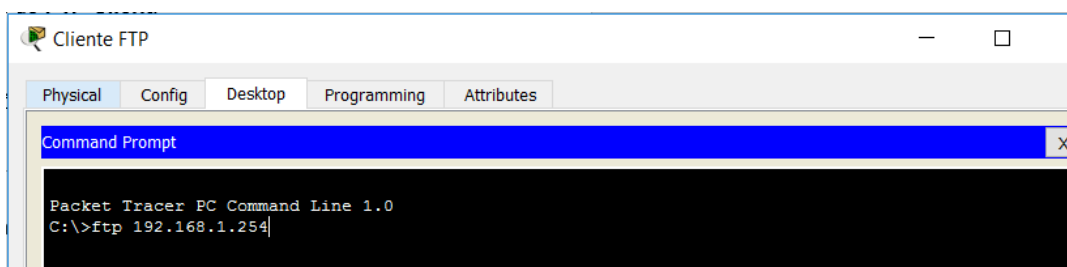
- d. Minimice (pero no cierre) la ventana de configuración de **HTTP Client**.

Paso 3: Generar tráfico FTP

- a. Haga clic en **FTP Client** (Cliente FTP) y, a continuación, haga clic en la ficha **Desktop > Command Prompt**.

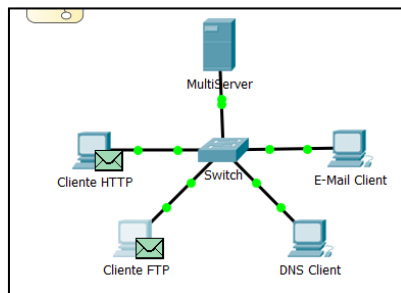


- b. Introduzca el comando **ftp 192.168.1.254**. En la ventana de simulación, aparecerán PDU.



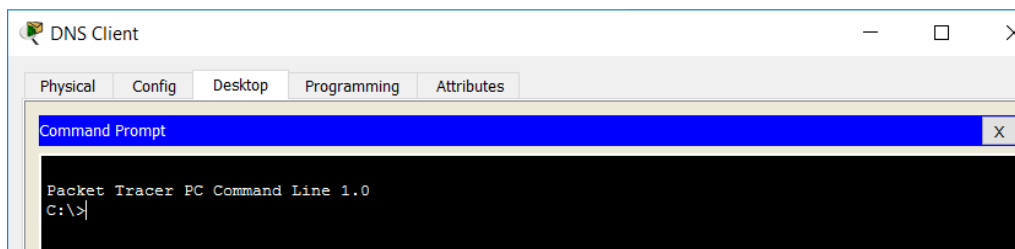
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- c. Minimice (pero no cierre) la ventana de configuración de **FTP Client**.

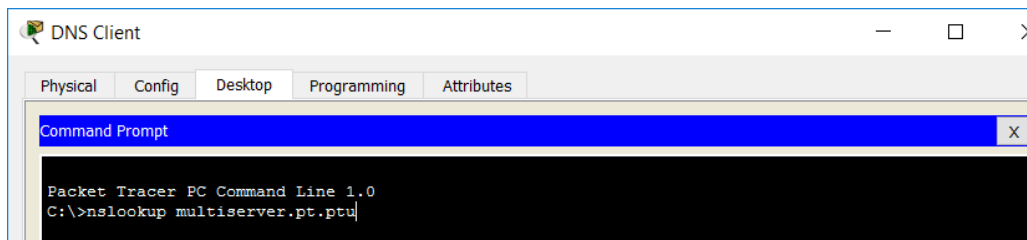


Paso 4: Generar tráfico DNS

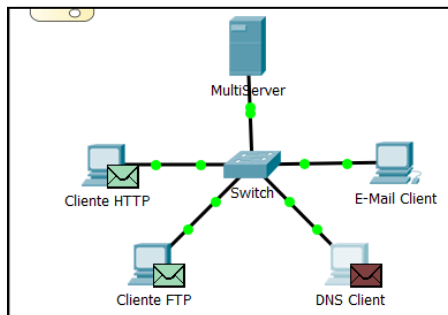
- a. Haga clic en **DNS Client** (Cliente DNS) y, a continuación, haga clic en la ficha **Desktop > Command Prompt**.



- b. Introduzca el comando **nslookup multiserver.pt.ptu**. En la ventana de simulación, aparecerá una PDU.

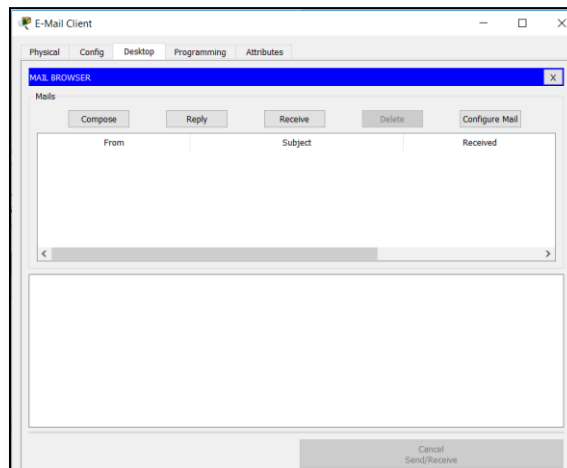


- c. Minimice (pero no cierre) la ventana de configuración de **DNS Client**.



Paso 5: Generar tráfico de correo electrónico

- a. Haga clic en **E-Mail Client** (Cliente de correo electrónico) y, a continuación, haga clic en la ficha **Desktop** y seleccione la herramienta **E Mail** (Correo electrónico).

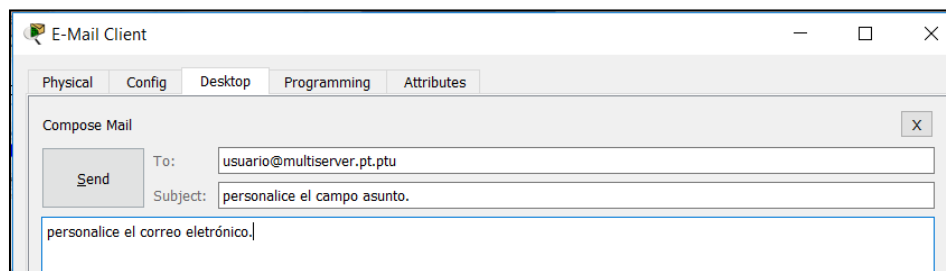


- b. Haga clic en **Compose** (Redactar) e introduzca la siguiente información:

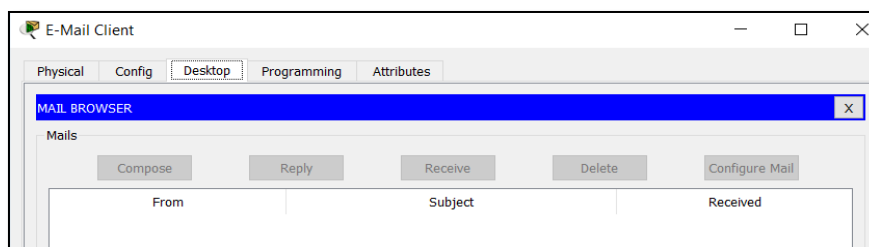
To: (Para:) usuario@multiserver.pt.ptu.

Subject: (Asunto:) personalice el campo de asunto.

E-Mail Body: (Cuerpo del correo electrónico:) personalice el correo electrónico.

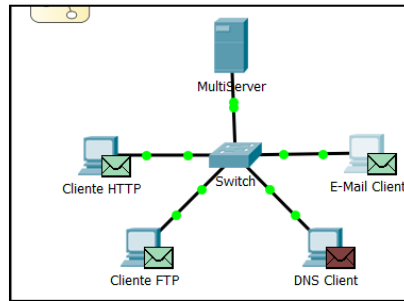


- c. Haga clic en **Send** (Enviar).



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

d. Minimice (pero no cierre) la ventana de configuración de **E-Mail Client**.



Paso 6: Verifique que se haya generado tráfico y que esté preparado para la simulación.

Cada equipo cliente debe tener PDU enumeradas en el panel de simulación.

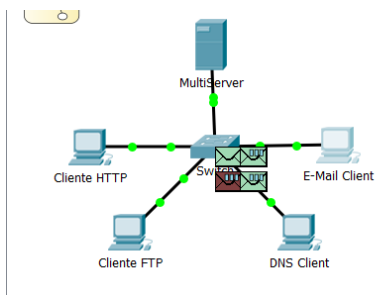
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	Cliente ...	TCP	
	0.000	--	Cliente ...	TCP	
	0.000	--	DNS Cli...	DNS	
	0.000	--	E-Mail ...	TCP	

Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

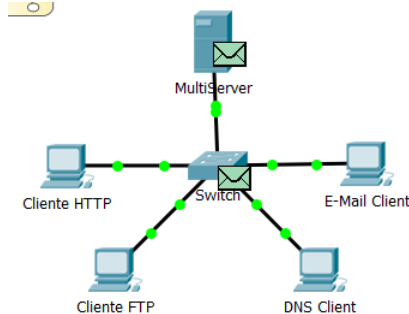
Paso 1: Examinar la multiplexación a medida que el tráfico cruza la red

Ahora utilizará los botones **Capture/Forward** (Capturar/avanzar) y **Back** (Atrás) del panel de simulación.

- Haga clic en **Capture/Forward** (Capturar/avanzar) una vez. Todas las PDU se transfieren al switch.

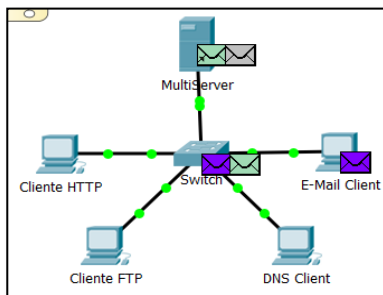


- Haga clic en **Capture/Forward** nuevamente. Algunas de las PDU desaparecen. ¿Qué cree que ocurrió?



Están almacenadas en el switch

- Haga clic en **Capture/Forward** seis veces. Todos los clientes deberían haber recibido una respuesta. Observe que solo una PDU puede cruzar un cable en cada dirección en cualquier momento dado. ¿Cómo se denomina este proceso?



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

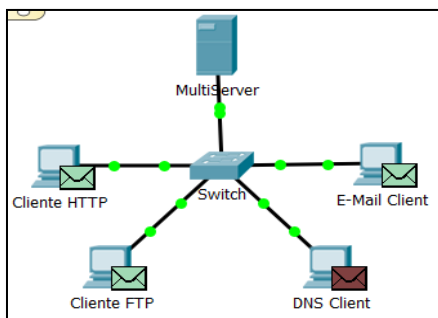
Multiplexación.

- c. En la lista de eventos en el panel superior derecho de la ventana de simulación aparecen una variedad de PDU. ¿Por qué hay tantos colores diferentes?

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.005	Cliente H...	Switch	TCP	Green
	0.005	--	Cliente ...	HTTP	Purple
	0.006	Cliente H...	Switch	HTTP	Purple
	0.006	MultiServer	Switch	TCP	Green
	0.006	Switch	DNS Cli...	DNS	Brown
	0.006	Cliente FTP	Switch	TCP	Green
	0.006	Switch	MultiSe...	TCP	Green
	0.007	Switch	MultiSe...	HTTP	Purple

Representan diferentes protocolos.

- d. Haga clic en **Back** ocho veces. Esto restablecerá la simulación.

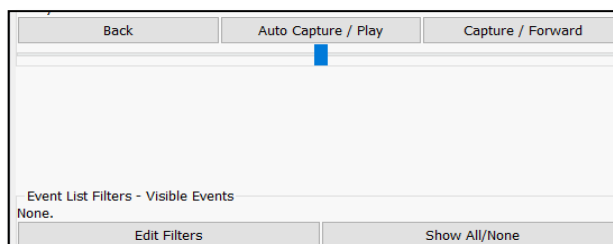


NOTA: no haga clic en **Reset Simulation** (Restablecer simulación) en ningún momento durante esta actividad; si lo hace, deberá repetir los pasos de la parte 1.

Paso 2: Examinar el tráfico HTTP cuando los clientes se comunican con el servidor

- a. Filtre el tráfico que se muestra actualmente para que solo se muestren las PDU de **HTTP** y **TCP**:

Haga clic en **Edit Filters** (Editar filtros) y cambie el estado de la casilla de verificación **Show All/None** (Mostrar todos/ninguno).

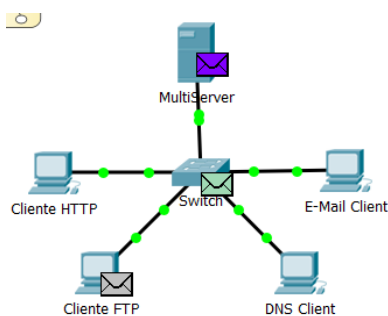


ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Seleccione **HTTP** y **TCP**. Haga clic en cualquier lugar fuera del cuadro Edit Filters (Editar filtros) para ocultarlo. En Visible Events (Eventos visibles), ahora solo se deberían mostrar las PDU de **HTTP** y **TCP**.



- b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el mouse sobre cada PDU hasta que encuentre una que se origine en **HTTP Client**. Haga clic en el sobre de PDU para abrirlo.



- c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

TCP			
SOURCE PORT:1025		DESTINATION PORT:80	
SEQUENCE NUMBER:103			
ACKNOWLEDGEMENT NUMBER:234			
OFFSE T:0x0	RESERVED: 0b000000	FLAGS:0b01 0001	WINDOW:65535
CHECKSUM:0x0000		URGENT POINTER:0x0000	
OPTION			
DATA (VARIABLE LENGTH)			PADDING: 0b000 ...000

TCP

¿Estas comunicaciones se consideran confiables?

Si.

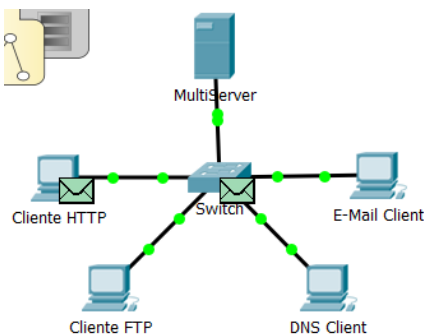
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO).

SRC IP:192.168.1.1	
DST IP:192.168.1.254	
OPT:0x000000	PADDING:0x00
DATA (VARIABLE LENGTH)	
TCP	
0 4 10 16 24 E	
SOURCE PORT:1025	DESTINATION PORT:80
SEQUENCE NUMBER:103	
ACKNOWLEDGEMENT NUMBER:234	

¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** Ventana)?
1025 (puede ser diferente), 80, 0, 0 SYN

- e. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **HTTP Client** con una marca de verificación.



- f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

TCP	
0 4 10 16 24 Bits	
SOURCE PORT:80	DESTINATION PORT:1025
SEQUENCE NUMBER:234	
ACKNOWLEDGEMENT NUMBER:104	
OFFSE T:0x0	RESERVED: 0b000000
FLAGS:0b01 0001	WINDOW:16151
CHECKSUM:0x0000	URGENT POINTER:0x0000
OPTION	
DATA (VARIABLE LENGTH)	PADDING: 0b000 ...000

80, 1025, 0, 1. SYN+ACK. Se invierten los puertos de origen y de destino, y el número de acuse de recibo es 1. SYN cambió por SYN+ACK.

- g. Hay otra **PDU** de un color diferente, que **HTTP Client** preparó para enviar a **MultiServer**. Este es el comienzo de la comunicación HTTP. Haga clic en este segundo sobre de PDU y seleccione **Outbound PDU Details** (Detalles de PDU saliente).

TCP					
0		4		10	
0		4		16	
0		4		24	
Bits					
SOURCE PORT:1025			DESTINATION PORT:80		
SEQUENCE NUMBER:104					
ACKNOWLEDGEMENT NUMBER:234					
OFFSE T:0x0	RESERVED: 0b000000	FLAGS:0b01 0000	WINDOW:65534		
CHECKSUM:0x0000			URGENT POINTER:0x0000		
OPTION					
DATA (VARIABLE LENGTH)					PADDING: 0b000 ...000

- h. ¿Qué información se indica ahora en la sección TCP? ¿En qué se diferencian los números de puerto y de secuencia respecto de las dos PDU anteriores?

1025, 80, 1, 1. PSH+ACK: los puertos de origen y destino están invertidos, y tanto el número de secuencia como el de acuse de recibo son 1.

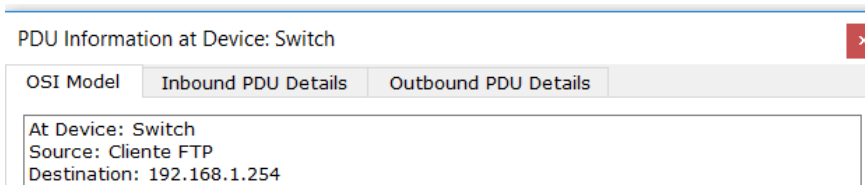
- i. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 3: Examine el tráfico FTP cuando los clientes se comunican con el servidor.

- a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **FTP** y **TCP**.



- b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el cursor sobre cada PDU hasta que encuentre una que se origine en **FTP Client**. Haga clic en el sobre de PDU para abrirlo.



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

TCP					
0	4	10	16	24	Bits
SOURCE PORT:1025		DESTINATION PORT:21			
SEQUENCE NUMBER:0					
ACKNOWLEDGEMENT NUMBER:0					
OFFSE T:0x0	RESERVED: 0b000000	FLAGS:0b00 0010	WINDOW:65535		
CHECKSUM:0x0000			URGENT POINTER:0x0000		
OPTION					
DATA (VARIABLE LENGTH)					PADDING: 0b000 ...000

TCP

¿Estas comunicaciones se consideran confiables?

Si.

- d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO).

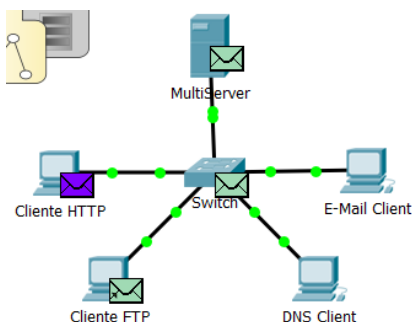
SRC IP:192.168.1.2	
DST IP:192.168.1.254	
OPT:0x000000	PADDING:0x00
DATA (VARIABLE LENGTH)	

TCP					
0	4	10	16	24	Bits
SOURCE PORT:1025		DESTINATION PORT:21			
SEQUENCE NUMBER:0					
ACKNOWLEDGEMENT NUMBER:0					

¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?

1025, 21, 0, 0. SYN

- e. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **FTP Client** con una marca de verificación.



- f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

TCP					
0	4	10	16	24	Bits
SOURCE PORT:21		DESTINATION PORT:1025			
SEQUENCE NUMBER:0					
ACKNOWLEDGEMENT NUMBER:1					
OFFSE T:0x0	RESERVED: 0b000000	FLAGS:0b01 0010	WINDOW:16384		
CHECKSUM:0x0000			URGENT POINTER:0x0000		
OPTION					
DATA (VARIABLE LENGTH)					PADDING: 0b000 ...000

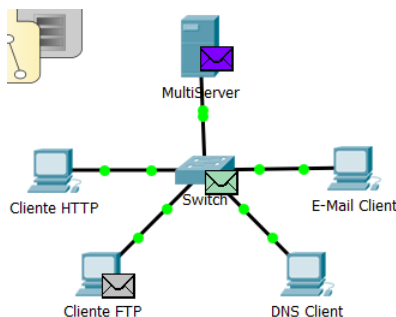
21, 1025, 0, 1. SYN+ACK. Se invierten los puertos de origen y de destino, y el número de acuse de recibo es 1.

- g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?

TCP					
0	4	10	16	24	Bits
SOURCE PORT:1025		DESTINATION PORT:21			
SEQUENCE NUMBER:1					
ACKNOWLEDGEMENT NUMBER:1					
OFFSE T:0x0	RESERVED: 0b000000	FLAGS:0b01 0000	WINDOW:65535		
CHECKSUM:0x0000			URGENT POINTER:0x0000		
OPTION					
DATA (VARIABLE LENGTH)					PADDING: 0b000 ...000

1025, 21, 1, 1. ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1.

- h. Cierre la PDU y haga clic en **Capture/Forward** hasta que una segunda PDU vuelva a **FTP Client**. La PDU es de un color diferente.



- i. Abra la PDU y seleccione **Inbound PDU Details**. Desplácese hasta después de la sección TCP. ¿Cuál es el mensaje del servidor?

FTP Response		Bytes
0	4	8
Code:220		
Message:Welcome to PT Ftp server		

Puede decir "Username ok, need password" (Nombre de usuario correcto, se necesita contraseña) o "Welcome to PT Ftp server" (Bienvenido al servidor FTP de PT).

- j. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 4: Examine el tráfico DNS cuando los clientes se comunican con el servidor.

- a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **DNS y UDP**.



- b. Haga clic en el sobre de PDU para abrirlo.

PDU Information at Device: DNS Client

OSI Model Outbound PDU Details

At Device: DNS Client
 Source: DNS Client
 Destination: 192.168.1.254

In Layers	Out Layers
Layer7	Layer 7: DNS
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: UDP Src Port: 1025, Dst Port: 53
Layer3	Layer 3: IP Header Src. IP: 192.168.1.3, Dst. IP: 192.168.1.254
Layer2	Layer 2: Ethernet II Header 000B.8E63.D2C3 >> 0001.96A9.401D
Layer1	Layer 1: Port(s): FastEthernet0

1. The DNS client sends a DNS query to the DNS server.

- c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

UDP		Bits
0	16	
SOURCE PORT:1025	DESTINATION PORT:53	
LENGTH:42	CHECKSUM:0	
DATA (VARIABLE LENGTH)		

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

UDP

¿Estas comunicaciones se consideran confiables?

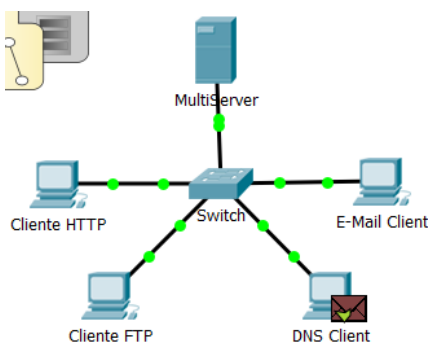
No

- d. Registre los valores de **SRC PORT** (Puerto de origen) y **DEST PORT** (Puerto de destino). ¿Por qué no hay números de secuencia ni de acuse de recibo?

SRC IP:192.168.1.3
DST IP:192.168.1.254

1025, 53. Porque UDP no necesita establecer una conexión confiable.

- e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva al **cliente DNS** con una marca de verificación.



- f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

UDP		16		Bits
SOURCE PORT:53	DESTINATION PORT:1025			
LENGTH:74	CHECKSUM:0			
DATA (VARIABLE LENGTH)				

53, 1025. Los puertos de origen y destino están invertidos.

g. ¿Cómo se llama la última sección de la **PDU**?

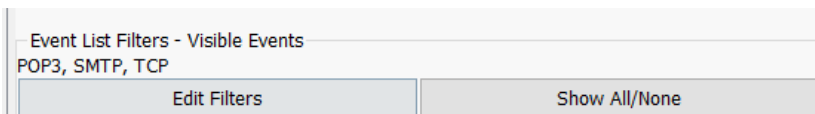
NAME:multiserver.pt.ptu	
TYPE:4	CLASS:1
TTL:86400	
LENGTH:4	IP:192.168.1.254

DNS ANSWER

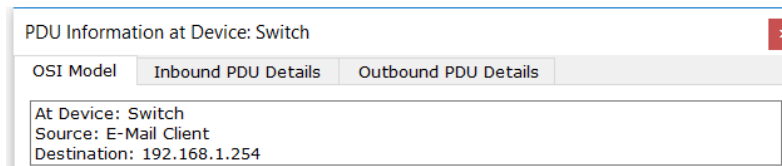
h. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 5: Examinar el tráfico de correo electrónico cuando los clientes se comunican con el servidor

a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestre **POP3, SMTP y TCP**.



b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el cursor sobre cada PDU hasta que encuentre una que se origine en **E-mail Client**. Haga clic en el sobre de PDU para abrirlo.



c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Qué protocolo de la capa de transporte utiliza el tráfico de correo electrónico?

SOURCE PORT:1025		DESTINATION PORT:25	
SEQUENCE NUMBER:0			
ACKNOWLEDGEMENT NUMBER:0			
OFFSE T:0x0	RESERVED: 0b000000	FLAGS:0b00 0010	WINDOW:65535
CHECKSUM:0x0000		URGENT POINTER:0x0000	
OPTION			
DATA (VARIABLE LENGTH)			PADDING: 0b000 ...000

TCP

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

¿Estas comunicaciones se consideran confiables?

Sí.

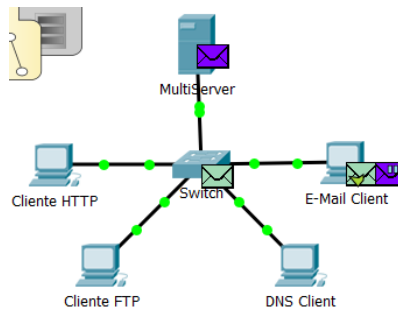
- d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO).

SRC IP:192.168.1.4	
DST IP:192.168.1.254	
OPT:0x000000	PADDING:0x00
DATA (VARIABLE LENGTH)	
TCP	
0	4
10	16
24	Bits
SOURCE PORT:1025	DESTINATION PORT:25
SEQUENCE NUMBER:0	
ACKNOWLEDGEMENT NUMBER:0	

¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?

1025, 25, 0, 0. SYN

- e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva a **E-Mail Client** con una marca de verificación.



- f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

TCP	
0	4
10	16
24	Bits
SOURCE PORT:25	DESTINATION PORT:1025
SEQUENCE NUMBER:0	
ACKNOWLEDGEMENT NUMBER:1	
OFFSE T:0x0	RESERVED: 0b000000
FLAGS:0b01 0010	WINDOW:16384
CHECKSUM:0x0000	URGENT POINTER:0x0000
OPTION	
DATA (VARIABLE LENGTH)	PADDING: 0b000 ...000

25, 1025, 0, 1. SYN+ACK. Se invierten los puertos de origen y de destino, y el número de acuse de recibo es 1.

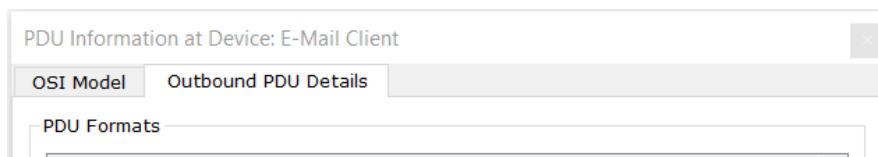
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?

TCP											
0		4		10		16		24		Bits	
SOURCE PORT:1025						DESTINATION PORT:25					
SEQUENCE NUMBER:1											
ACKNOWLEDGEMENT NUMBER:1											
OFFSE T:0x0		RESERVED: 0b000000		FLAGS:0b01 0000		WINDOW:65535					
CHECKSUM:0x0000						URGENT POINTER:0x0000					
OPTION											
DATA (VARIABLE LENGTH)										PADDING: 0b000 ...000	

1025, 25, 1, 1. ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1. ACK

- h. Hay otra PDU de un color diferente, que **HTTP Client** preparó para enviar a **MultiServer**. Este es el comienzo de la comunicación de correo electrónico. Haga clic en este segundo sobre de PDU y selecciones **Outbound PDU Details** (Detalles de PDU saliente)



- i. ¿En qué se diferencian los números de puerto y de secuencia respecto de las dos PDU anteriores?
j.

TCP											
0		4		10		16		24		Bits	
SOURCE PORT:1025						DESTINATION PORT:25					
SEQUENCE NUMBER:1											
ACKNOWLEDGEMENT NUMBER:1											
OFFSE T:0x0		RESERVED: 0b000000		FLAGS:0b01 1000		WINDOW:65535					
CHECKSUM:0x0000						URGENT POINTER:0x0000					
OPTION											
DATA (VARIABLE LENGTH)										PADDING: 0b000 ...000	

1025, 25, 1, 1. PSH+ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1.

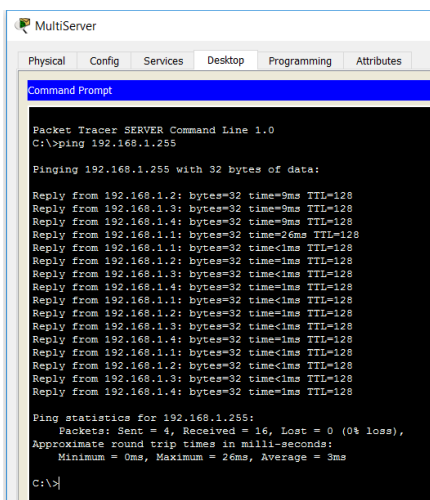
- k. ¿Qué protocolo de correo electrónico se relaciona con el puerto TCP 25? ¿Qué protocolo se relaciona con el puerto TCP 110?

SMTP. POP3.

- l. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 6: Examinar el uso de números de puerto del servidor

- a. Para ver las sesiones TCP activas, siga estos pasos en una secuencia rápida:
 - 1) Pase nuevamente al modo **Realtime** (Tiempo real).
 - 2) Haga clic en **Multiserver** y, a continuación, haga clic en la ficha **Desktop > Command Prompt** (Escritorio > Símbolo del sistema).



```

MultiServer
Physical Config Services Desktop Programming Attributes
Command Prompt
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.255

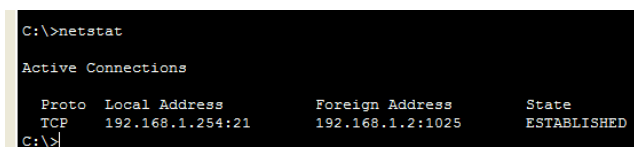
Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=9ms TTL=128
Reply from 192.168.1.3: bytes=32 time=9ms TTL=128
Reply from 192.168.1.4: bytes=32 time=9ms TTL=128
Reply from 192.168.1.1: bytes=32 time=26ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 4, Received = 16, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 26ms, Average = 3ms

C:\>
  
```

- b. Introduzca el comando **netstat**. ¿Qué protocolos se indican en la columna izquierda?
TCP



```

C:\>netstat

Active Connections

Proto Local Address Foreign Address State
TCP 192.168.1.254:21 192.168.1.2:1025 ESTABLISHED
C:\>
  
```

¿Qué números de puerto utiliza el servidor?

Las respuestas varían, pero los estudiantes pueden ver los tres: 21, 25 y 80. Definitivamente deben ver el puerto 21.

- c. ¿En qué estados están las sesiones?

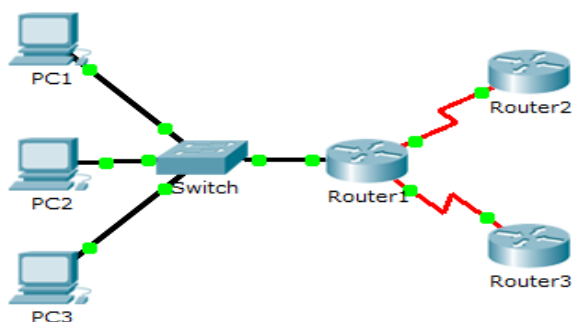
La respuesta varía. Entre los posibles estados se incluyen **CLOSED** (Cerrada), **ESTABLISHED** (Establecida), **LAST_ACK** (Último acuse de recibo).

- d. Repita el comando **netstat** varias veces hasta que vea solo una sola sesión con el estado **ESTABLISHED**. ¿Para qué servicio aún está abierta la conexión? **FTP**

¿Por qué esta sesión no se cierra como las otras tres? (Sugerencia: revise los clientes minimizados)
El servidor está esperando una contraseña del cliente.

Ejercicio 8.1.3.8: Investigación del tráfico unicast, broadcast y multicast

Topología



Objetivos

Parte 1: Generar tráfico de unicast

Parte 2: Generar tráfico de broadcast

Parte 3: Investigar el tráfico de multicast

Información básica/situación

En esta actividad, se examina el comportamiento de unicast, broadcast y multicast. La mayoría del tráfico de una red es unicast. Cuando una PC envía una solicitud de eco ICMP a un router remoto, la dirección de origen en el encabezado del paquete IP es la dirección IP de la PC emisora. La dirección de destino en el encabezado del paquete IP es la dirección IP de la interfaz del router remoto. El paquete se envía sólo al destino deseado.

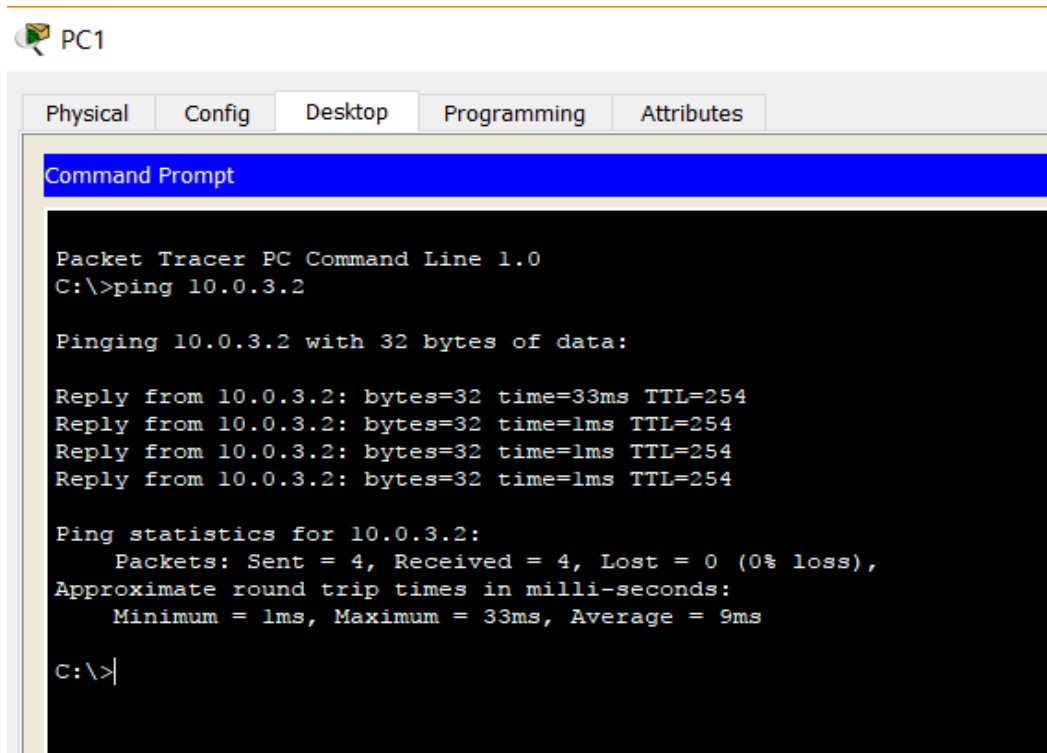
Mediante el comando **ping** o la característica Add Complex PDU (Agregar PDU compleja) de Packet Tracer, puede hacer ping directamente a las direcciones de broadcast para ver el tráfico de broadcast.

Para el tráfico de multicast, consultará el tráfico de EIGRP. Los routers Cisco utilizan EIGRP para intercambiar información de enrutamiento entre routers. Los routers que utilizan EIGRP envían paquetes a la dirección multicast 224.0.0.10, que representa el grupo de routers EIGRP. Si bien estos paquetes son recibidos por otros dispositivos, todos los dispositivos (excepto los routers EIGRP) los descartan en la capa 3, sin requerir otro procesamiento.

Parte 1: Generar tráfico de unicast

Paso 1: Utilizar el comando ping para generar tráfico

- Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop > Command Prompt** (Escritorio > Símbolo del sistema).
- Introduzca el comando **ping 10.0.3.2**. El ping debe tener éxito.



```

PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.3.2

Pinging 10.0.3.2 with 32 bytes of data:

Reply from 10.0.3.2: bytes=32 time=33ms TTL=254
Reply from 10.0.3.2: bytes=32 time=1ms TTL=254
Reply from 10.0.3.2: bytes=32 time=1ms TTL=254
Reply from 10.0.3.2: bytes=32 time=1ms TTL=254

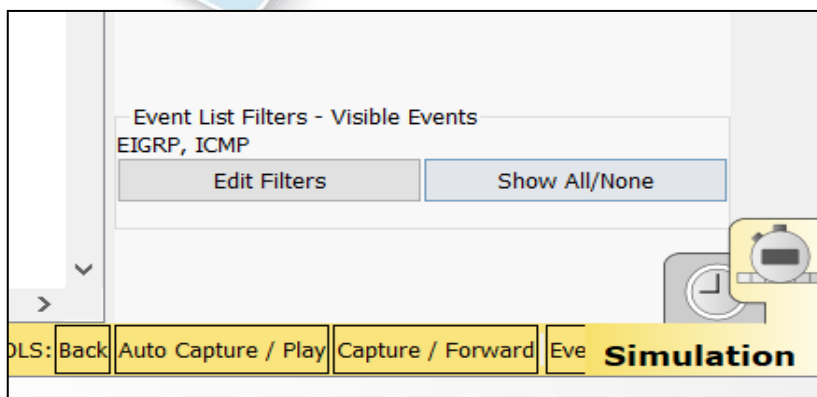
Ping statistics for 10.0.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 33ms, Average = 9ms

C:\>

```

Paso 2: Ingrese al modo de simulación.

- Haga clic en la ficha **Simulation** (Simulación) para ingresar al modo de simulación.
- Haga clic en **Edit Filters** (Editar filtros) y verifique que solo los eventos ICMP y EIGRP estén seleccionados.

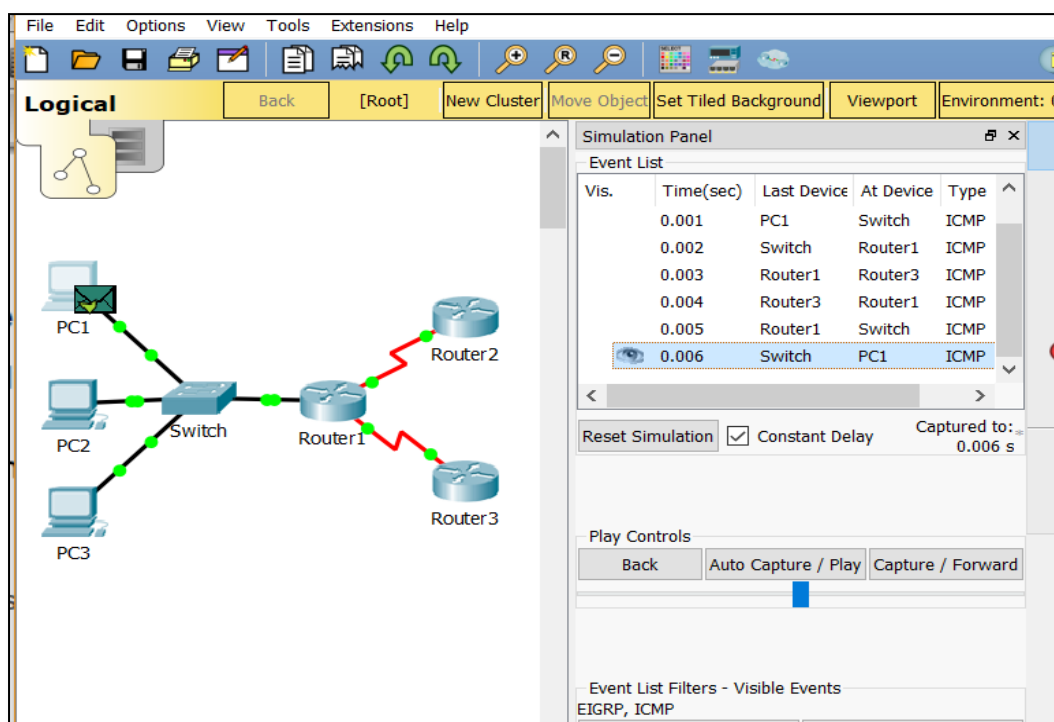


- c. Haga clic en **PC1** e introduzca el comando **ping 10.0.3.2**.

Paso 3: Examinar el tráfico de unicast

La PDU en la **PC1** es una solicitud de eco de ICMP dirigida a la interfaz serial en el **Router3**.

- a. Haga clic en **Capture/Forward** (Capturar/avanzar) varias veces y observe mientras se envía la solicitud de eco al **Router3** y la respuesta de eco se envía a la **PC1**. Deténgase cuando la primera respuesta de eco llegue a la PC1.



¿Qué dispositivos atravesó el paquete con la transmisión de unicast?

R/A: Los dispositivos que atravesó el paquete con la transmisión unicast fueron de host PC1 al Switch, posteriormente del Switch al Router1, luego del Router1 al Router3 y por último se devolvió por los mismos dispositivos.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- b. En la sección Simulation Panel Event List (Lista de eventos del panel de simulación), la última columna incluye un cuadro de color que proporciona acceso a información detallada sobre un evento. Haga clic en el cuadro de color de la última columna para obtener el primer evento. Se abre la ventana PDU Information (Información de PDU).

PDU Information at Device: PC1

OSI Model Outbound PDU Details

At Device: PC1
Source: PC1
Destination: 10.0.3.2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer 3: IP Header Src. IP: 10.0.1.2, Dest. IP: 10.0.3.2 ICMP Message Type: 8
Layer2	Layer 2: Ethernet II Header 0001.646C.4136 >> 00E0.A398.2C01
Layer1	Layer 1: Port(s): FastEthernet0

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address is not in the same subnet and is not the broadcast address.
5. The default gateway is set. The device sets the next-hop to default gateway.

¿En qué capa comienza esta transmisión y por qué?

R/A: La transmisión comienza en la capa 3, debido a que está relacionada con IP e ICMP

- c. Examine la información de la Capa 3 para todos los eventos. Observe que las direcciones IP de origen y de destino son direcciones unicast que hacen referencia a la PC1 y a la interfaz serial del Router3

PDU Information at Device: Router1

OSI Model Inbound PDU Details Outbound PDU Details

At Device: Router1
Source: PC1
Destination: 10.0.3.2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3: IP Header Src. IP: 10.0.1.2, Dest. IP: 10.0.3.2 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 10.0.1.2, Dest. IP: 10.0.3.2 ICMP Message Type: 8
Layer 2: Ethernet II Header 0001.646C.4136 >> 00E0.A398.2C01	Layer 2: HDLC Frame HDLC
Layer 1: Port FastEthernet0/0	Layer 1: Port(s): Serial0/0/1

1. The device looks up the destination IP address in the CEF table.
2. The CEF table does not have an entry for the destination IP address.
3. The device looks up the destination IP address in the routing table.

PDU Information at Device: Router3

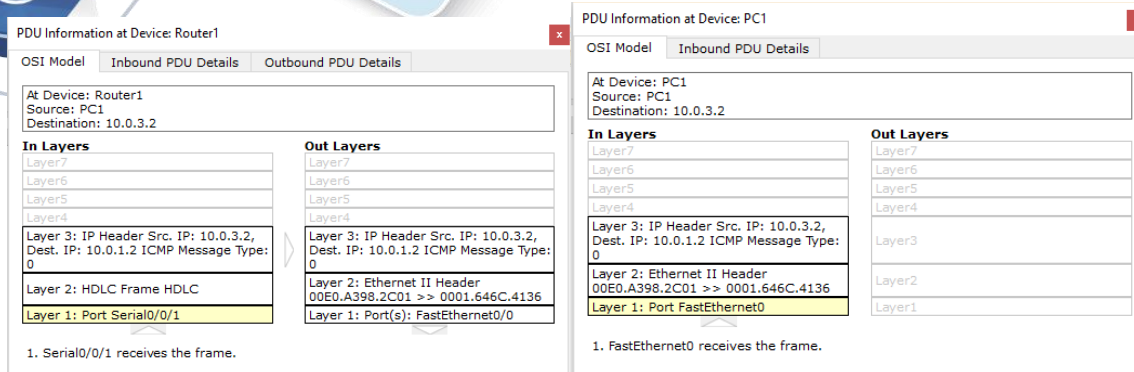
OSI Model Inbound PDU Details Outbound PDU Details

At Device: Router3
Source: PC1
Destination: 10.0.3.2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 10.0.1.2, Dest. IP: 10.0.3.2 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 10.0.3.2, Dest. IP: 10.0.1.2 ICMP Message Type: 0
Layer 2: HDLC Frame HDLC	Layer 2: HDLC Frame HDLC
Layer 1: Port Serial0/0/1	Layer 1: Port(s): Serial0/0/1

1. Serial0/0/1 receives the frame.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



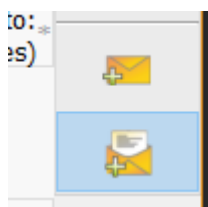
¿Cuáles son los dos cambios que ocurren en la capa 3 cuando un paquete llega al Router3?
 R/A: los dos cambios que ocurren es el intercambio de las direcciones IP de origen y destino, por otra parte, el tipo de mensaje de ICMP cambia de 8 a 0.

- d. Haga clic en **Reset Simulation** (Restablecer simulación).

Parte 2: Generar tráfico de broadcast

Paso 1: Agregar una PDU compleja

- a. Haga clic en **Add Complex PDU** (Agregar una PDU compleja). Este ícono se ubica en la barra de herramientas de la derecha y muestra un sobre abierto.



- b. Pase el cursor del mouse sobre la topología, y el puntero cambiará por un sobre con un signo más (+).
- c. Haga clic en **PC1** para que funcione como origen de este mensaje de prueba, y se abrirá la ventana de

diálogo **Create Complex PDU** (Crear una PDU compleja). Introduzca los siguientes valores:

- Dirección IP de destino: **255.255.255.255** (dirección de broadcast)
- Número de secuencia: 1
- Tiempo de intento único: **0**

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

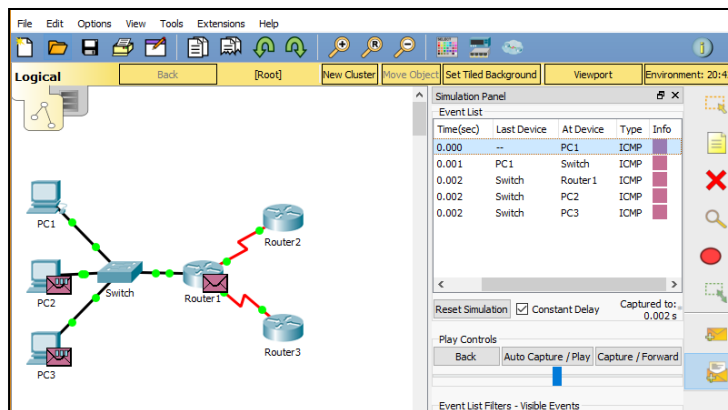
Dentro de la configuración de la PDU, el valor predeterminado para **Select Application** (Seleccionar aplicación) es PING. ¿Qué otras tres aplicaciones, como mínimo, están disponibles para utilizar?

R/A: las otras aplicaciones disponibles para utilizar son: DNS, FINGER, FTP, HTTP, HTTPS, IMAP, NETBIOS, PING, POP3, SFTP, entre otras.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- d. Haga clic en **Create PDU** (Crear PDU). Este paquete de broadcast de prueba ahora aparece en **Simulation Panel Event List** .También aparece en la ventana PDU List (Lista de PDU). Es la primera PDU para la Situación 0.

- e. Haga clic en **Capture/Forward** dos veces. Este paquete se envía al switch y después se transmite por broadcast a la **PC2**, la **PC3**, y el **Router1**. Examine la información de la Capa 3 para todos los eventos. Observe que la dirección IP de destino es 255.255.255.255, que es la dirección IP de broadcast que configuró cuando creó la PDU compleja.



PDU Information at Device: PC1

OSI Model Outbound PDU Details

At Device: PC1
Source: PC1
Destination: 255.255.255.255

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3: IP Header Src. IP: 10.0.1.2, Dest. IP: 255.255.255.255 ICMP Message Type: 8
Layer2	Layer2: Ethernet II Header 0001.646C.4136 >> FFFF.FFFF.FFFF
Layer1	Layer1: Port(s): FastEthernet0

- The Ping process starts the next ping request.
- The Ping process creates an ICMP Echo Request message and sends it to the lower process.
- The source IP address is not specified. The device sets it to the port's IP address.
- The device sets TTL in the packet header.
- The destination IP address is in the same subnet. The device sets the next-hop to destination.

PDU Information at Device: Router1

OSI Model Inbound PDU Details Outbound PDU Details

At Device: Router1
Source: PC1
Destination: 255.255.255.255

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3: IP Header Src. IP: 10.0.1.2, Dest. IP: 255.255.255.255 ICMP Message Type: 8
Layer2	Layer2: Ethernet II Header 0001.646C.4136 >> FFFF.FFFF.FFFF
Layer1	Layer1: Port FastEthernet0/0

1. FastEthernet0/0 receives the frame.

PDU Information at Device: PC2

OSI Model Inbound PDU Details Outbound PDU Details

At Device: PC2
Source: PC1
Destination: 255.255.255.255

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3: IP Header Src. IP: 10.0.1.2, Dest. IP: 255.255.255.255 ICMP Message Type: 8
Layer2	Layer2: Ethernet II Header 0001.646C.4136 >> FFFF.FFFF.FFFF
Layer1	Layer1: Port FastEthernet0

1. FastEthernet0 receives the frame.

PDU Information at Device: PC3

OSI Model Inbound PDU Details Outbound PDU Details

At Device: PC3
Source: PC1
Destination: 255.255.255.255

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3: IP Header Src. IP: 10.0.1.2, Dest. IP: 255.255.255.255 ICMP Message Type: 8
Layer2	Layer2: Ethernet II Header 0001.646C.4136 >> FFFF.FFFF.FFFF
Layer1	Layer1: Port FastEthernet0

1. FastEthernet0 receives the frame.

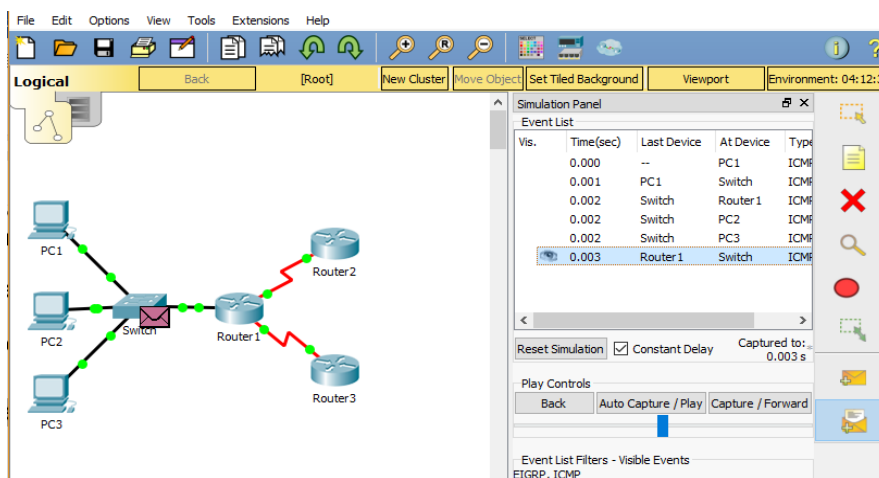
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Si analiza la información del modelo OSI, ¿qué cambios se produjeron en la información de la capa 3 en la columna Out Layers (Capas de salida) en el Router1, la PC2 y la PC3?

R/A: De acuerdo a lo observado, la PDU se convierte en un UNICAST que contesta a la PC1

f. Haga clic en **Capture/Forward** nuevamente. ¿La PDU de broadcast se reenvía en algún momento al Router2 o al Router3? ¿Por qué?

R/A: La PDU de broadcast no se reenvía ni al Router2 ni al Router3, debido a que éste se realiza dentro de la red local.



The screenshot shows a network simulation environment. On the left, a network diagram displays three PCs (PC1, PC2, PC3) connected to a central Switch. The Switch is connected to Router1, which is further connected to Router2 and Router3. On the right, the 'Simulation Panel' is open, showing an 'Event List' table. The table has columns for 'Vis.', 'Time(sec)', 'Last Device', 'At Device', and 'Type'. The following table represents the data from the event list:

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	Switch	ICMP
	0.002	Switch	Router1	ICMP
	0.002	Switch	PC2	ICMP
	0.002	Switch	PC3	ICMP
☑	0.003	Router1	Switch	ICMP

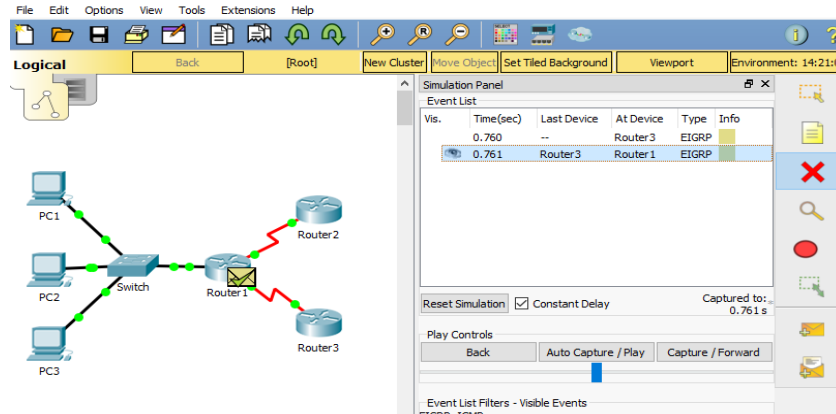
Below the table, there are controls for 'Reset Simulation', 'Constant Delay' (checked), and 'Captured to: 0.003 s'. There are also 'Play Controls' buttons: 'Back', 'Auto Capture / Play', and 'Capture / Forward'. At the bottom, 'Event List Filters - Visible Events' are listed as 'EIGRP, ICMP'.

g. Después de que termine de examinar el comportamiento de broadcast, elimine el paquete de prueba haciendo clic en **Delete** (Eliminar) debajo de **Scenario 0** (Situación 0).

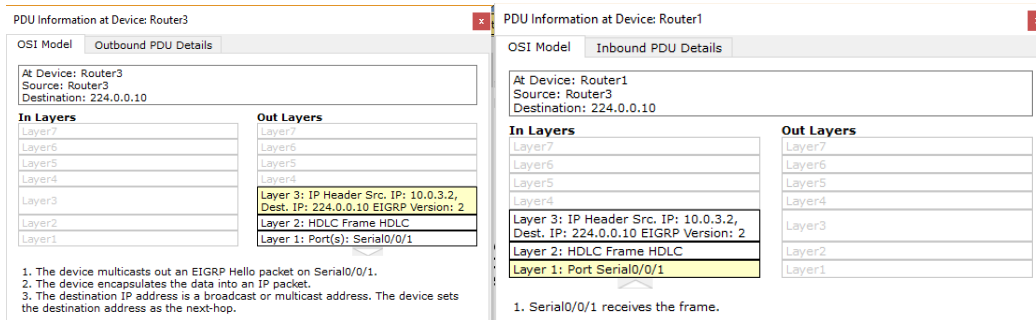
Parte 3: Investigar el tráfico de multicast

Paso 1: Examinar el tráfico que generan los protocolos de enrutamiento

- a. Haga clic en **Capture/Forward** (Capturar/avanzar). Los paquetes EIGRP están en el Router1 a la espera de que se los transmita por multicast a través de cada interfaz.

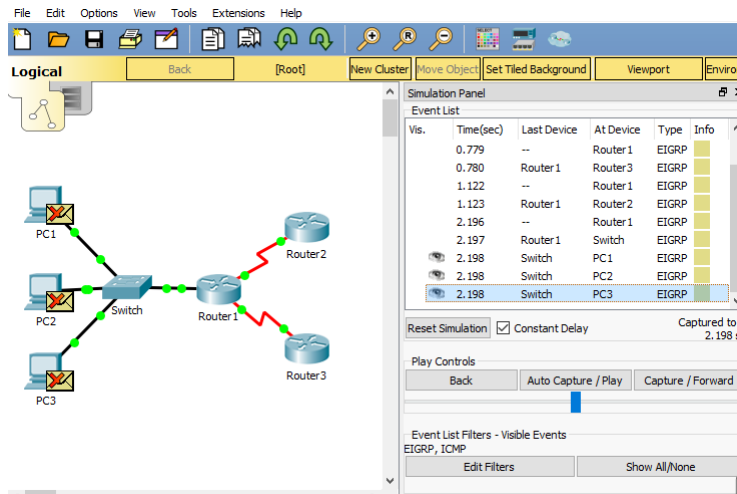


- b. Examine el contenido de estos paquetes abriendo la ventana de información de PDU y vuelva a hacer clic en **Capture/Forward**. Los paquetes se envían a los otros dos routers y al switch. Los routers aceptan y procesan los paquetes porque son parte del grupo multicast. El switch reenviará los paquetes a las PC.



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

b. Haga clic en **Capture/Forward** hasta que vea que el paquete EIGRP llega a las PC.



¿Qué hacen los hosts con los paquetes?

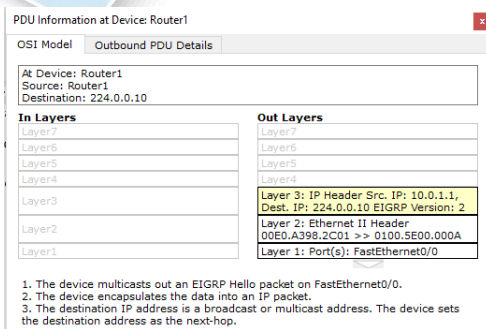
R/A: Los hosts rechazan y descartan los paquetes recibidos

Examine la información de las capas 3 y 4 para todos los eventos EIGRP.

The image contains four screenshots of the 'PDU Information at Device' window in Cisco Packet Tracer, showing the details of EIGRP packets at different stages:

- Top Left: PDU Information at Device: Router1 (Outbound PDU Details)**
 - At Device: Router1
 - Source: Router1
 - Destination: 224.0.0.10
 - In Layers:** Layer6, Layer5, Layer4, Layer3, Layer2, Layer1
 - Out Layers:** Layer6, Layer5, Layer4, Layer3, Layer2, Layer1
 - Layer 3: IP Header Src. IP: 10.0.3.1, Dest. IP: 224.0.0.10 EIGRP Version: 2
 - Layer 2: HDLC Frame HDLC
 - Layer 1: Port(s): Serial0/0/1
 - 1. The device multicasts out an EIGRP Hello packet on Serial0/0/1.
 - 2. The device encapsulates the data into an IP packet.
 - 3. The destination IP address is a broadcast or multicast address. The device sets the destination address as the next-hop.
- Top Right: PDU Information at Device: Router3 (Inbound PDU Details)**
 - At Device: Router3
 - Source: Router1
 - Destination: 224.0.0.10
 - In Layers:** Layer7, Layer6, Layer5, Layer4, Layer3, Layer2, Layer1
 - Out Layers:** Layer7, Layer6, Layer5, Layer4, Layer3, Layer2, Layer1
 - Layer 3: IP Header Src. IP: 10.0.3.1, Dest. IP: 224.0.0.10 EIGRP Version: 2
 - Layer 2: HDLC Frame HDLC
 - Layer 1: Port Serial0/0/1
 - 1. Serial0/0/1 receives the frame.
- Bottom Left: PDU Information at Device: Router1 (Outbound PDU Details)**
 - At Device: Router1
 - Source: Router1
 - Destination: 224.0.0.10
 - In Layers:** Layer7, Layer6, Layer5, Layer4, Layer3, Layer2, Layer1
 - Out Layers:** Layer7, Layer6, Layer5, Layer4, Layer3, Layer2, Layer1
 - Layer 3: IP Header Src. IP: 10.0.2.1, Dest. IP: 224.0.0.10 EIGRP Version: 2
 - Layer 2: HDLC Frame HDLC
 - Layer 1: Port(s): Serial0/0/0
 - 1. The device multicasts out an EIGRP Hello packet on Serial0/0/0.
 - 2. The device encapsulates the data into an IP packet.
 - 3. The destination IP address is a broadcast or multicast address. The device sets the destination address as the next-hop.
- Bottom Right: PDU Information at Device: Router2 (Inbound PDU Details)**
 - At Device: Router2
 - Source: Router1
 - Destination: 224.0.0.10
 - In Layers:** Layer7, Layer6, Layer5, Layer4, Layer3, Layer2, Layer1
 - Out Layers:** Layer7, Layer6, Layer5, Layer4, Layer3, Layer2, Layer1
 - Layer 3: IP Header Src. IP: 10.0.2.1, Dest. IP: 224.0.0.10 EIGRP Version: 2
 - Layer 2: HDLC Frame HDLC
 - Layer 1: Port Serial0/0/0
 - 1. Serial0/0/0 receives the frame.

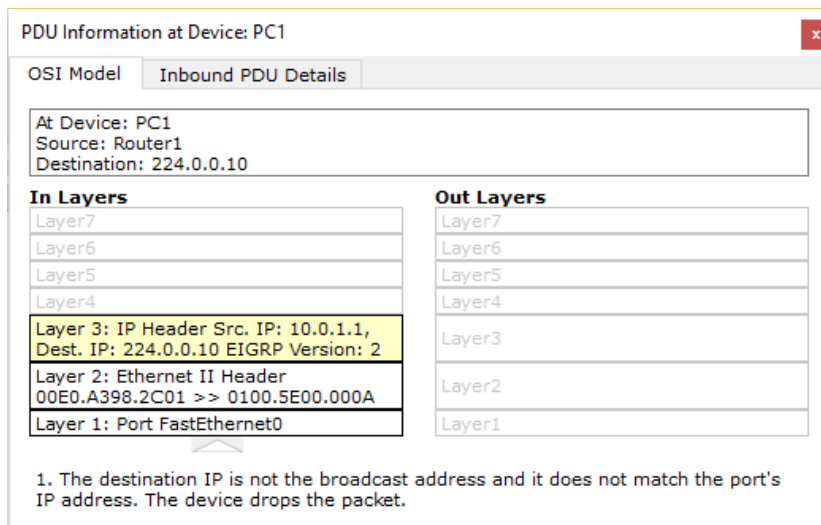
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



¿Cuál es la dirección de destino de cada uno de los paquetes?

R/A: Se observa que la dirección de destino de cada uno de los paquetes es la 224.0.0.10, la cual corresponde a la dirección IP de multicast para el protocolo EIGRP

d. Haga clic en uno de los paquetes entregados a una de las PC. ¿Qué sucede con esos paquetes?



R/A: Se observa que los paquetes se descartan por lo tanto no se realiza ningún procesamiento adicional. Según el tráfico que generan los tres tipos de paquetes IP, ¿cuáles son las principales diferencias en la entrega?

R/A: Las principales diferencias en la entrega, de acuerdo al tráfico generado por los tres tipos de paquetes IP son:

- El paquete unicast atraviesa la red debido a que está destinado a un dispositivo específico.
- El paquete broadcast se envía a cada dispositivo en la red de área local
- El paquete multicast se envía a todos los dispositivos (tanto de la red local como no local) pero éstos son procesados únicamente por los dispositivos que forman parte del grupo multicast, es decir los router

RESULTADOS:

Cisco Packet Tracer - C:\Users\user\OneDrive\Documents\Unad\2017-2\Diplomado Cisco... — □ ×

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:41:40

Congratulations Guest! You completed the activity.

Overall Feedback **Assessment Items** Connectivity Tests

If you are having difficulty completing this activity, revisit the following resources:

- Section: Network Protocols and Standards
- Activity - Mapping Protocols of the TCP/IP Suite
- Activity - Identify Layers and Functions
- Section: Moving Data in the Network
- Activity - Identify the PDU Layer

Ejercicio 8.2.5.3: Configuración de direccionamiento IPv6

Topología

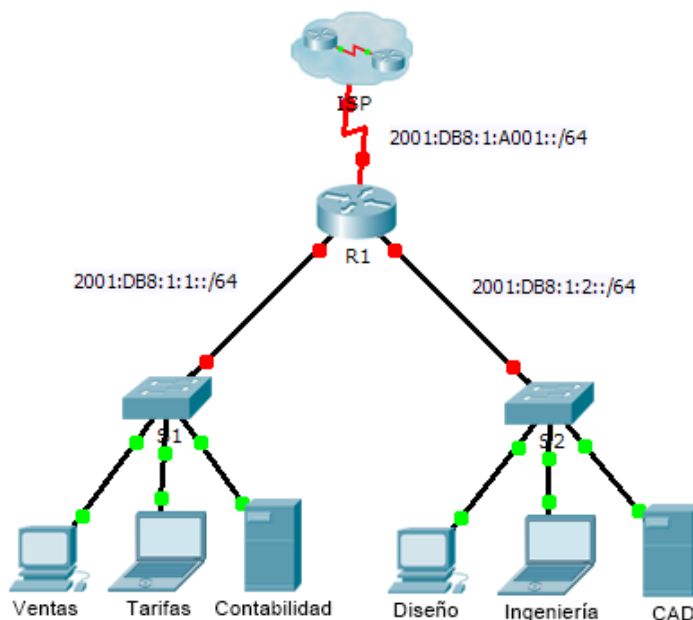


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminad
R1	G0/0	2001:DB8:1:1::1/64	No aplicable
	G0/1	2001:DB8:1:2::1/64	No aplicable
	S0/0/0	2001:DB8:1:A001::2/64	No aplicable
	Link-local	FE80::1	No aplicable
Ventas	NIC	2001:DB8:1:1::2/64	FE80::1
Tarifas	NIC	2001:DB8:1:1::3/64	FE80::1
Contabilidad	NIC	2001:DB8:1:1::4/64	FE80::1
Diseño	NIC	2001:DB8:1:2::2/64	FE80::1
Ingeniería	NIC	2001:DB8:1:2::3/64	FE80::1
CAD	NIC	2001:DB8:1:2::4/64	FE80::1

Objetivos

Parte 1: Configurar el direccionamiento IPv6 en el router

Parte 2: Configurar el direccionamiento IPv6 en los servidores.

Parte 3: Configurar el direccionamiento IPv6 en los clientes
Parte 4: Probar y verificar la conectividad de red

Información básica

En esta actividad, practicará la configuración de direcciones IPv6 en un router, en servidores y en clientes. También verificará la implementación de las direcciones IPv6.

Parte 1: Configurar el direccionamiento IPv6 en el router

Paso 1: Habilitar el router para reenviar paquetes IPv6

- Introduzca el comando de configuración global ipv6 unicast-routing. Este comando se debe configurar para habilitar el router para que reenvíe paquetes IPv6. Este comando se analizará en otro semestre.

```
R1(config)# ipv6 unicast-routing
```

```
R1>enable
```

```
R1#configure t
```

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

```
R1(config)#ipv6 unicast-routing
```

```
R1(config)#
```

Paso 2: Configurar el direccionamiento IPv6 en GigabitEthernet0/0

- Haga clic en **R1** y, a continuación, haga clic en la ficha **CLI**. Presione **Entrar**.
- Ingrese al modo EXEC privilegiado.
- Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para GigabitEthernet0/0.

- Configure la dirección IPv6 con el siguiente comando:

```
R1(config-if)# ipv6 address 2001:DB8:1:1::1/64
```

- Configure la dirección IPv6 link-local con el siguiente comando:

```
R1(config-if)# ipv6 address FE80::1 link-local
```

- Active la interfaz.

```
R1>enable
```

```
R1#configure t
```

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

```
R1(config)#ipv6 unicast-routing
```

```
R1(config)#int gigabitEthernet 0/0
```

```
R1(config-if)#ipv6 address 2001:DB8:1:1::1/64
```

```
R1(config-if)#ipv6 address FE80::1 link-local
```

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

Paso 3: Configurar el direccionamiento IPv6 en GigabitEthernet0/1

- Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para GigabitEthernet0/1.
- Consulte la **tabla de direccionamiento** para obtener la dirección IPv6 correcta.
- Configure la dirección IPv6, la dirección link-local y active la interfaz.

```
R1(config-if)#exit
R1(config)#int g0/1
R1(config-if)#ipv6 address 2001:DB8:1:2::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
```

Paso 4: Configurar el direccionamiento IPv6 en Serial0/0/0

- Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para Serial0/0/0.
- Consulte la **tabla de direccionamiento** para obtener la dirección IPv6 correcta.
- Configure la dirección IPv6, la dirección link-local y active la interfaz.

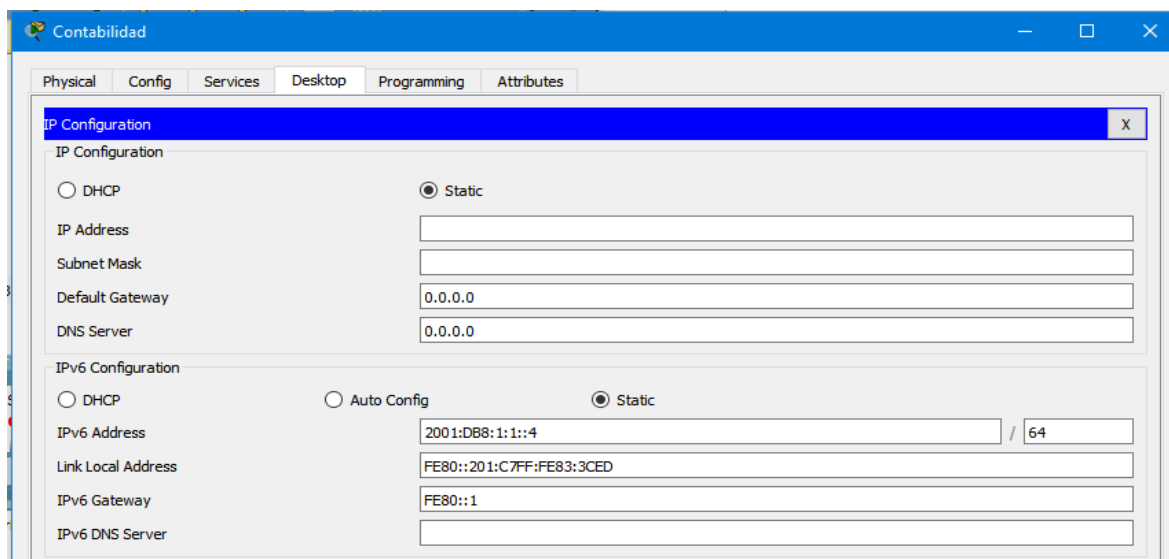
```
R1(config)#int s0/0/0
R1(config-if)#ipv6 address 2001:DB8:1:A001::2/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
```

Parte 2: Configurar el direccionamiento IPv6 en los servidores

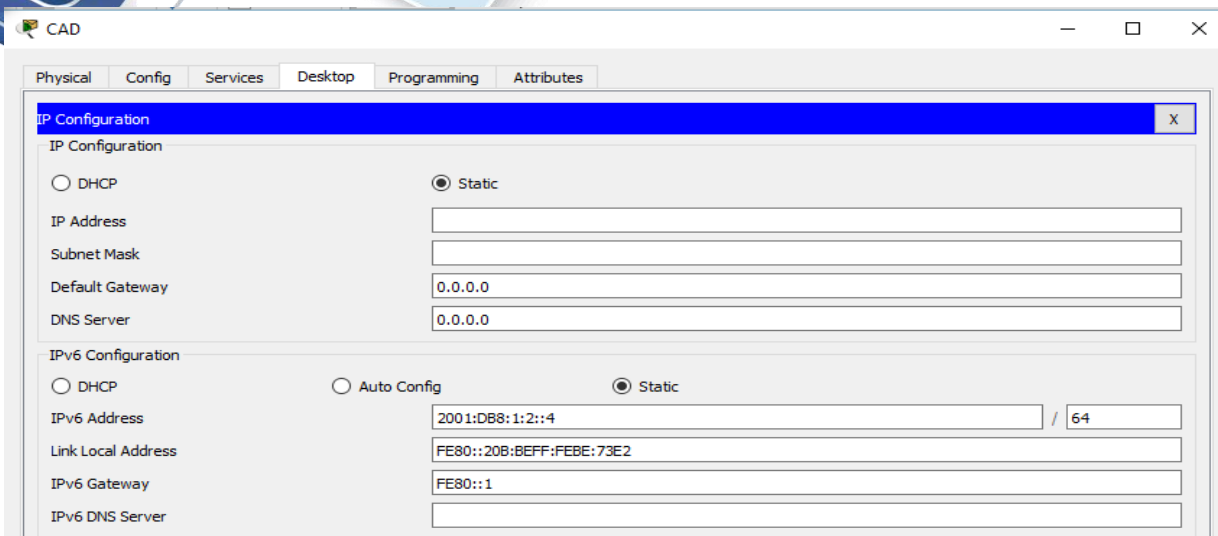
Paso 1: Configurar el direccionamiento IPv6 en el servidor de contabilidad

- a. Haga clic en **Accounting** (Contabilidad) y, a continuación, en la ficha **Desktop > IP Configuration**
(Escritorio > Configuración de IP).
- c. Establezca la **dirección IPv6 2001:DB8:1:1::4** con el prefijo **/64**. c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.



Paso 2: Configurar el direccionamiento IPv6 en el servidor CAD

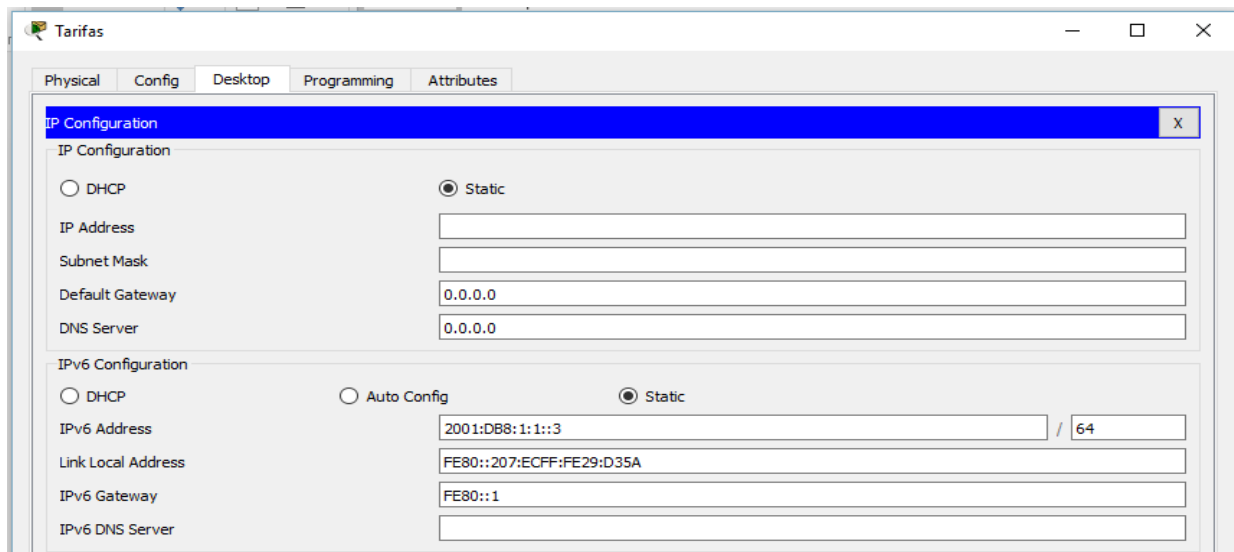
Repita los pasos 1a a 1c para el servidor **CAD**. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.



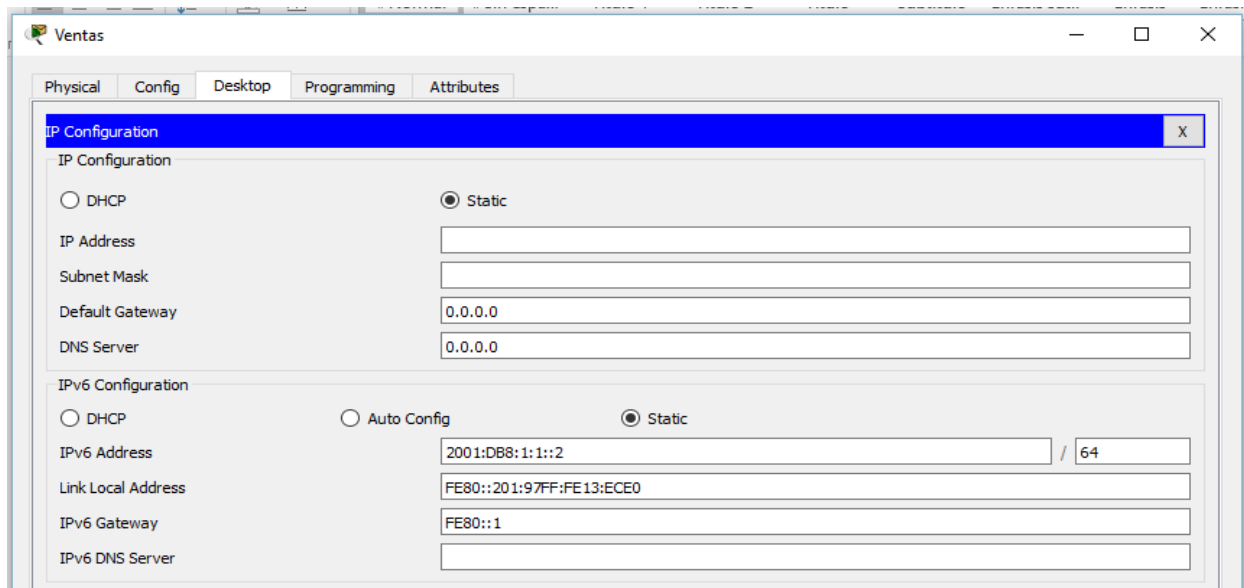
Parte 3: Configurar el direccionamiento IPv6 en los clientes

Paso 1: Configurar el direccionamiento IPv6 en los clientes de ventas y facturación

- a. Haga clic en **Billing** (Facturación) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.
- c. Establezca la **dirección IPv6 2001:DB8:1:1::3** con el prefijo **/64**. c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.

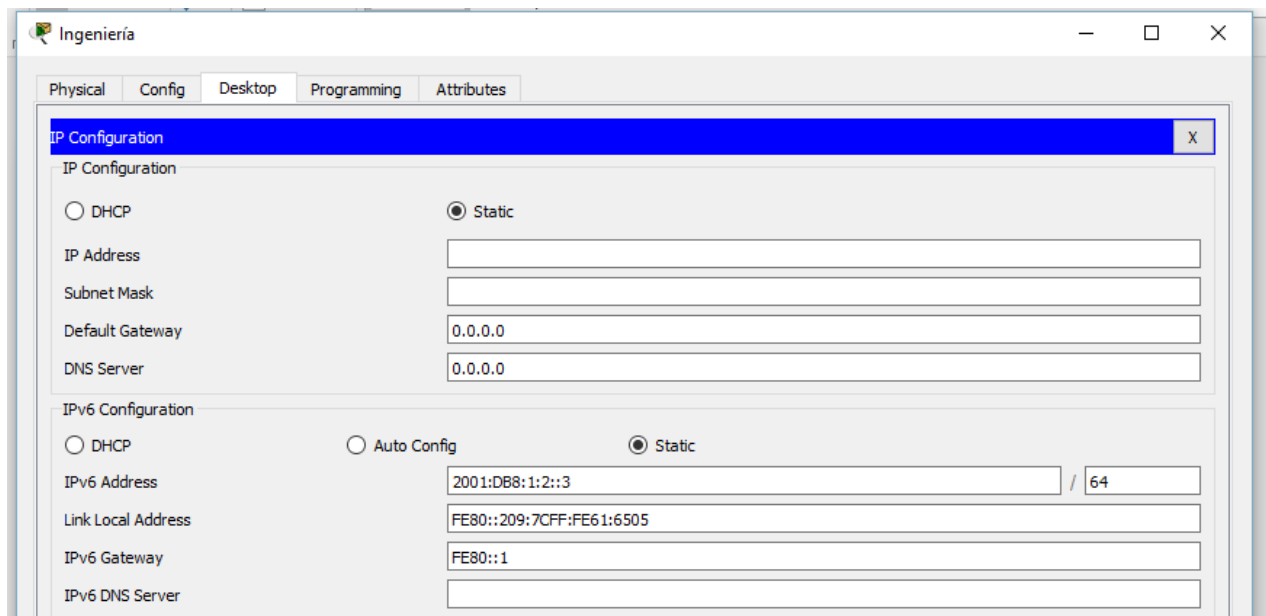


- d. Repita los pasos 1a a 1c para **Sales** (Ventas). Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.

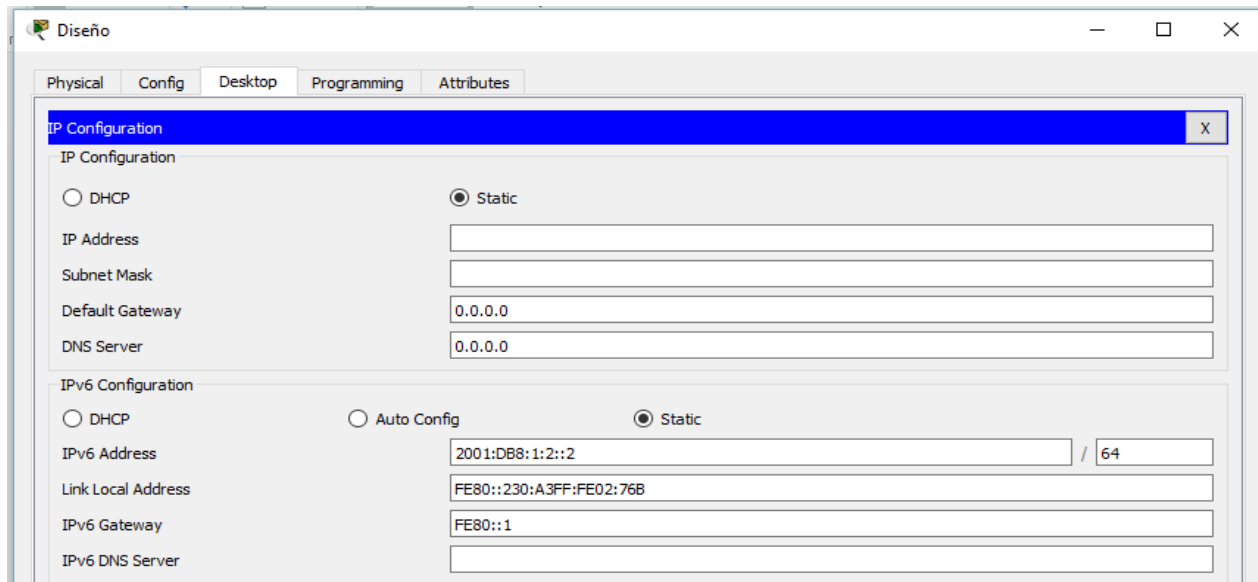


Paso 2: Configurar el direccionamiento IPv6 en los clientes de ingeniería y diseño

- a. Haga clic en **Engineering** (Ingeniería) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.
- b. Establezca la **dirección IPv6 2001:DB8:1:2::3** con el prefijo **/64**. c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.



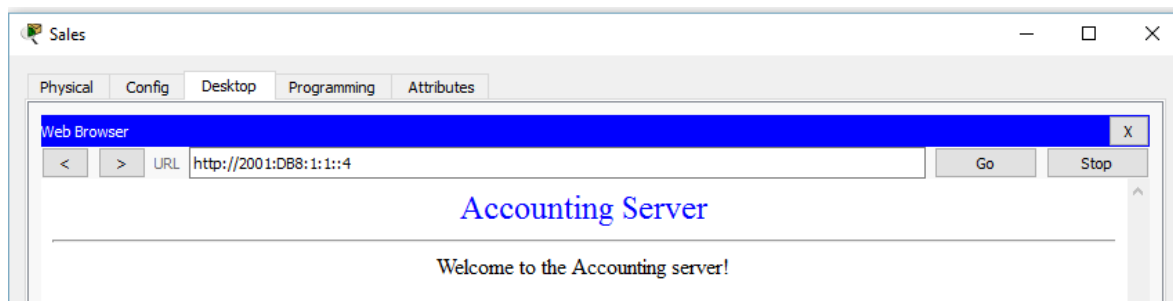
- d. Repita los pasos 1a a 1c para **Design** (Diseño). Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.



Parte 4: Probar y verificar la conectividad de la red

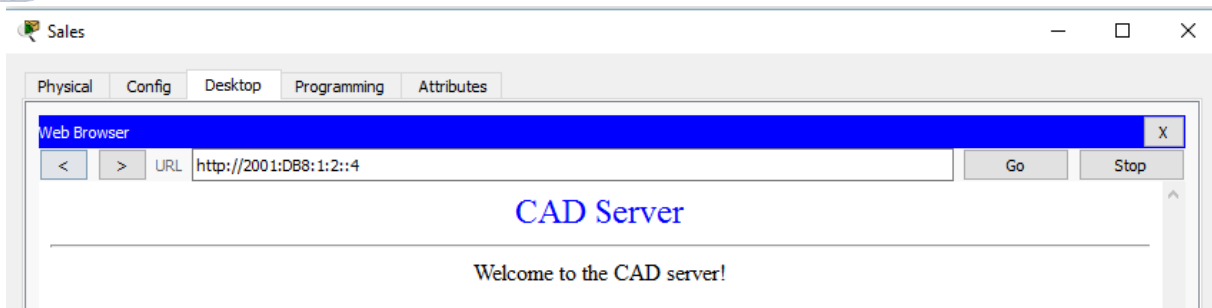
Paso 1: Abrir las páginas Web del servidor de los clientes

- Haga clic en **Sales** y, a continuación, en la ficha **Desktop**. Si es necesario, cierre la ventana **IP Configuration**.
- Haga clic en **Web Browser** (Explorador Web). Introduzca **2001:DB8:1:1::4** en el cuadro de dirección URL y haga clic en **Go** (Ir). Debería aparecer el sitio Web de **Accounting**.

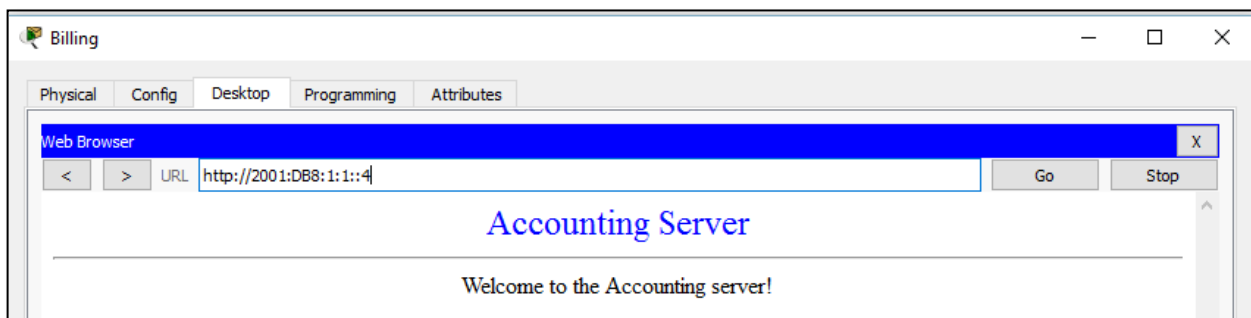
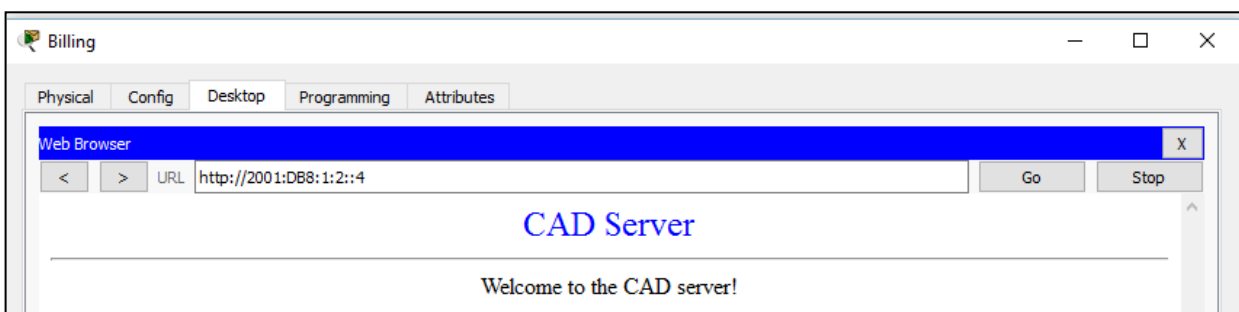


ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

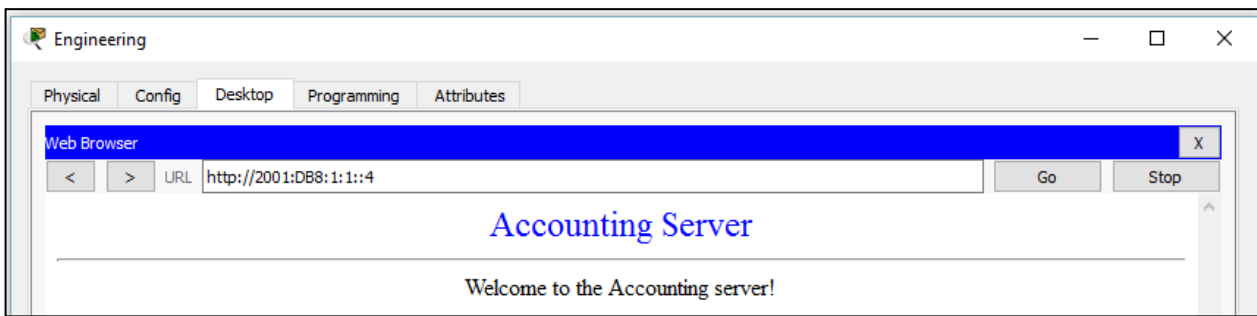
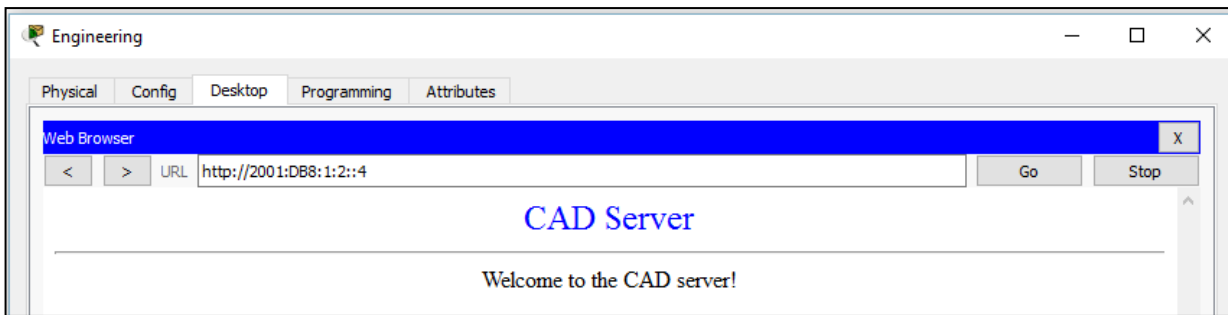
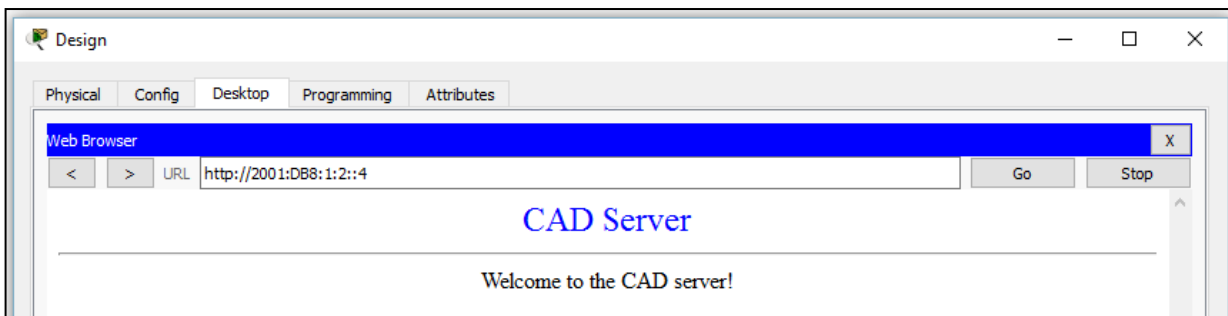
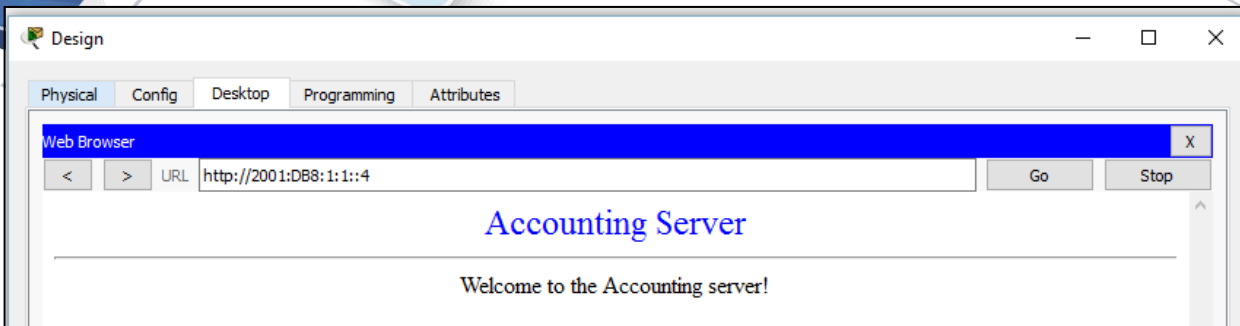
- c. Introduzca **2001:DB8:1:2::4** en el cuadro de dirección URL y haga clic en **Go**. Debería aparecer el sitio Web de **CAD**.



- d. Repita los pasos 1a a 1d para el resto de los clientes.

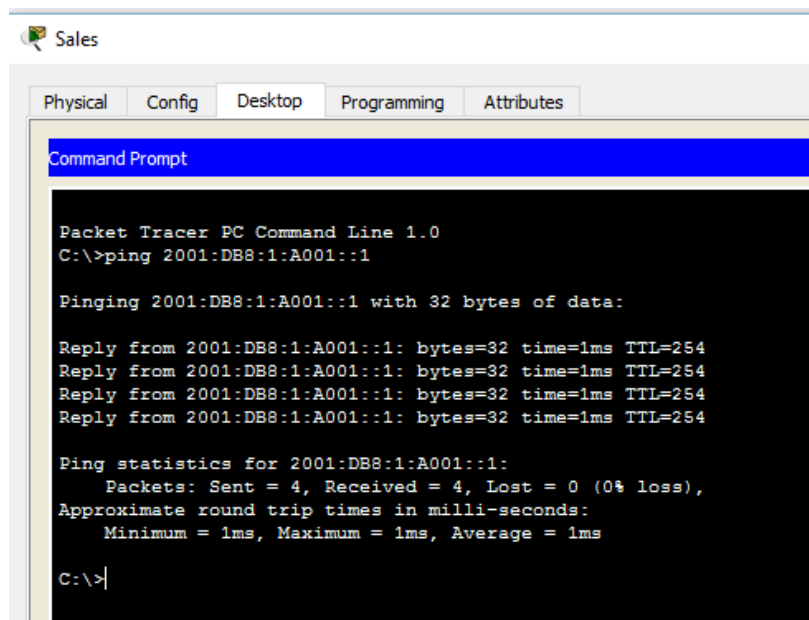


ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



Paso 2: Hacer ping al ISP

- Abra una ventana de configuración de cualquier equipo cliente haciendo clic en el ícono.
- Haga clic en la ficha **Desktop** > **Command Prompt** (Símbolo del sistema).
- Pruebe la conectividad al ISP con el siguiente comando:
PC> **ping 2001:DB8:1:A001::1**



```

Sales
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:A001::1

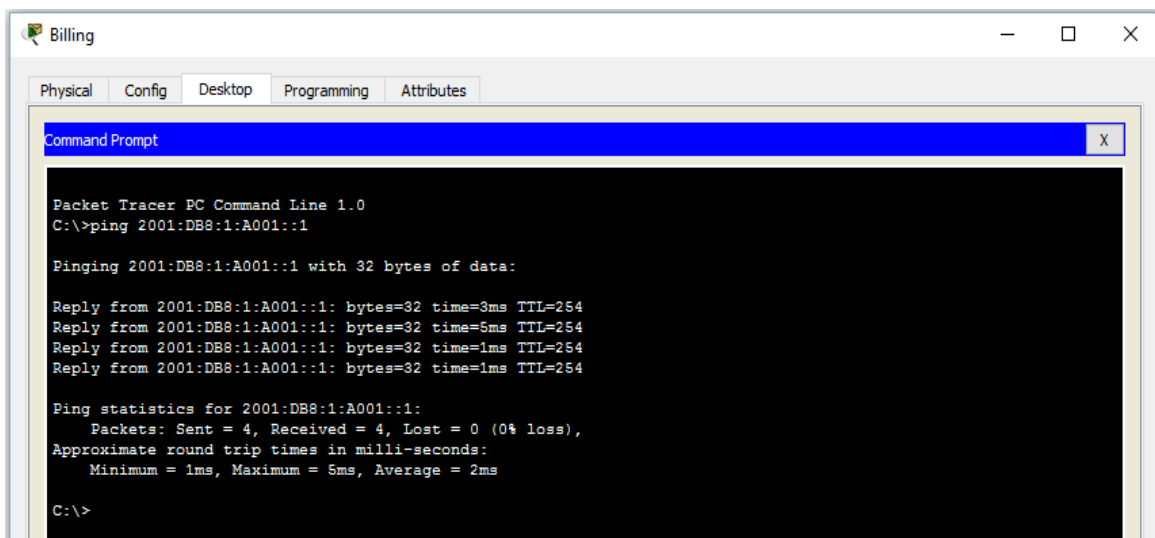
Pinging 2001:DB8:1:A001::1 with 32 bytes of data:

Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254

Ping statistics for 2001:DB8:1:A001::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>|
  
```

- Repita el comando **ping** con otros clientes hasta que se haya verificado la conectividad completa.



```

Billing
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:A001::1

Pinging 2001:DB8:1:A001::1 with 32 bytes of data:

Reply from 2001:DB8:1:A001::1: bytes=32 time=3ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=5ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254

Ping statistics for 2001:DB8:1:A001::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>
  
```

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Design

Physical Config Desktop Programming Attributes

Command Prompt

```

Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:A001::1

Pinging 2001:DB8:1:A001::1 with 32 bytes of data:

Reply from 2001:DB8:1:A001::1: bytes=32 time=3ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=4ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254

Ping statistics for 2001:DB8:1:A001::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\>

```

Engineering

Physical Config Desktop Programming Attributes

Command Prompt

```

Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:A001::1

Pinging 2001:DB8:1:A001::1 with 32 bytes of data:

Reply from 2001:DB8:1:A001::1: bytes=32 time=2ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=3ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=3ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=3ms TTL=254

Ping statistics for 2001:DB8:1:A001::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>

```

Ejercicio 8.3.2.5: Verificación del direccionamiento IPv4 e IPv6

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	10.10.1.97	255.255.255.224	No aplicable
		2001:DB8:1:1::1/64		No aplicable
	S0/0/1	10.10.1.6	255.255.255.252	No aplicable
		2001:DB8:1:2::2/64		No aplicable
Link-local	FE80::1		No aplicable	
R2	S0/0/0	10.10.1.5	255.255.255.252	No aplicable
		2001:DB8:1:2::1/64		No aplicable
	S0/0/1	10.10.1.9	255.255.255.252	No aplicable
		2001:DB8:1:3::1/64		No aplicable
Link-local	FE80::2		No aplicable	
R3	G0/0	10.10.1.17	255.255.255.240	No aplicable
		2001:DB8:1:4::1/64		No aplicable
	S0/0/1	10.10.1.10	255.255.255.252	No aplicable
		2001:DB8:1:3::2/64		No aplicable
Link-local	FE80::3		No aplicable	
PC1	NIC	10.10.1.100	255.255.255.224	10.10.1.97
		2001:DB8:1:1::A/64		FE80::1
PC2	NIC	10.10.1.20	255.255.255.240	10.10.1.17
		2001:DB8:1:4::A/64		FE80::3

Objetivos

Parte 1: Completar la documentación de la tabla de direccionamiento

Parte 2: Probar la conectividad mediante el comando ping

Parte 3: Descubrir la ruta mediante su rastreo

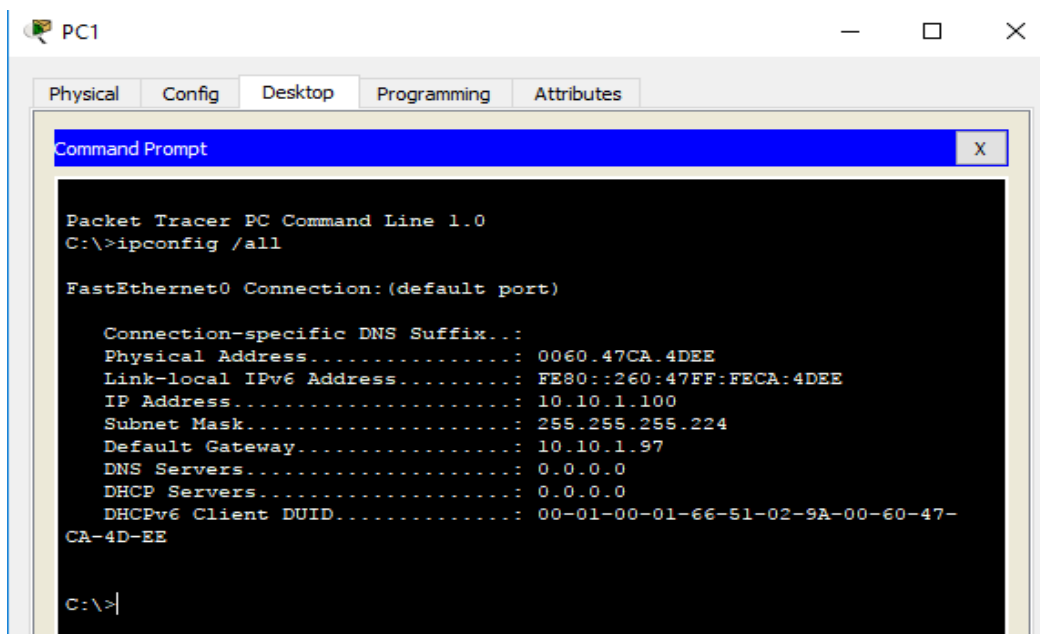
Información básica

La técnica dual-stack permite que IPv4 e IPv6 coexistan en la misma red. En esta actividad, investigará la implementación de una técnica dual-stack incluidos la documentación de la configuración de IPv4 e IPv6 para dispositivos finales, la prueba de conectividad para IPv4 e IPv6 mediante el comando **ping** y el rastreo de la ruta de extremo a extremo para IPv4 e IPv6.

Parte 1: Completar la documentación de la tabla de direccionamiento

Paso 1: Usar el comando ipconfig para verificar el direccionamiento IPv4

- Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop > Command Prompt** (Escritorio > Símbolo del sistema).
- Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.



```

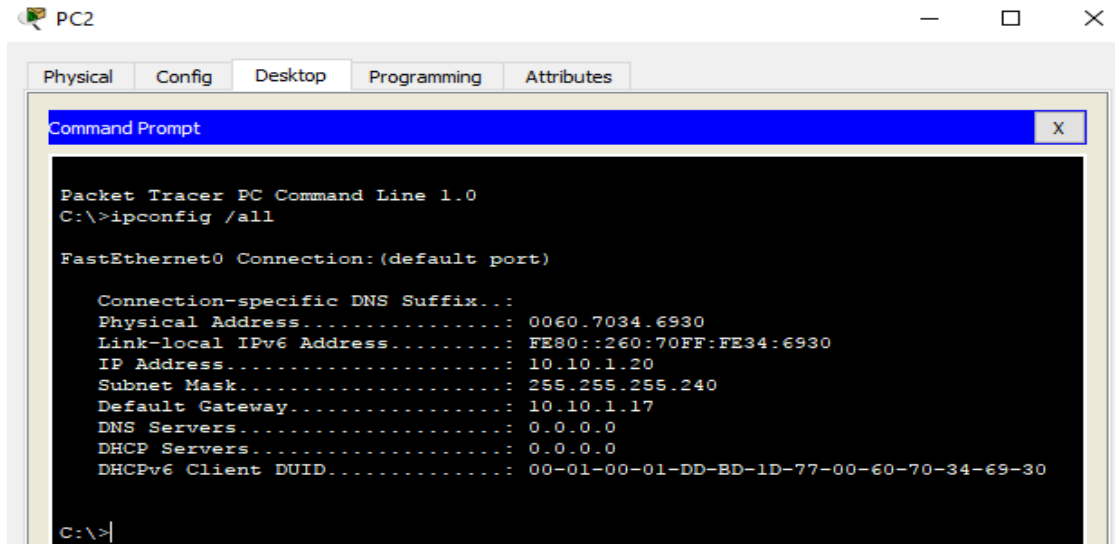
PC1
-----
Physical  Config  Desktop  Programming  Attributes
-----
Command Prompt
-----
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix... :
Physical Address. . . . . : 0060.47CA.4DEE
Link-local IPv6 Address . . . . . : FE80::260:47FF:FECA:4DEE
IP Address. . . . . : 10.10.1.100
Subnet Mask . . . . . : 255.255.255.224
Default Gateway . . . . . : 10.10.1.97
DNS Servers . . . . . : 0.0.0.0
DHCP Servers . . . . . : 0.0.0.0
DHCPv6 Client DUID. . . . . : 00-01-00-01-66-51-02-9A-00-60-47-
CA-4D-EE

C:\>
  
```

- Haga clic en **PC2** y, a continuación, haga clic en la ficha **Desktop > Command Prompt**.
- Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

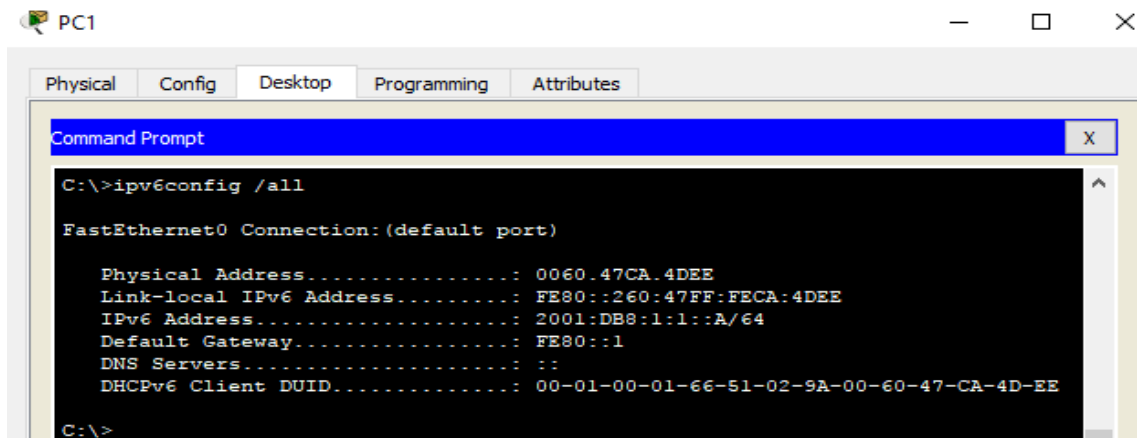
FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0060.7034.6930
Link-local IPv6 Address.....: FE80::260:70FF:FE34:6930
IP Address.....: 10.10.1.20
Subnet Mask.....: 255.255.255.240
Default Gateway.....: 10.10.1.17
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....: 00-01-00-01-DD-BD-1D-77-00-60-70-34-69-30

C:\>
```

Paso 2: Usar el comando **ipv6config** para verificar el direccionamiento IPv6

- a. En la **PC1**, introduzca el comando **ipv6config /all** para recopilar la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.



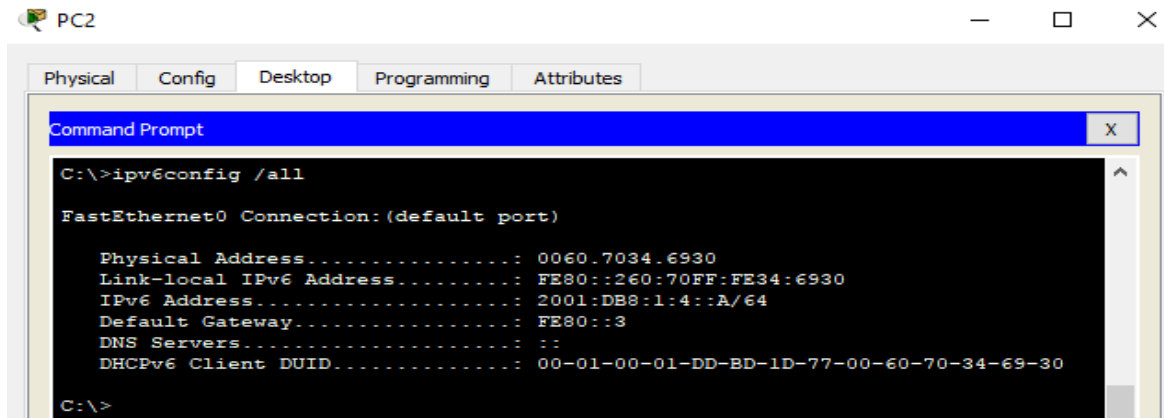
```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ipv6config /all

FastEthernet0 Connection: (default port)

Physical Address.....: 0060.47CA.4DEE
Link-local IPv6 Address.....: FE80::260:47FF:FECA:4DEE
IPv6 Address.....: 2001:DB8:1:1::A/64
Default Gateway.....: FE80::1
DNS Servers.....: ::
DHCPv6 Client DUID.....: 00-01-00-01-66-51-02-9A-00-60-47-CA-4D-EE

C:\>
```

- b. En la **PC2**, introduzca el comando **ipv6config /all** para recopilar la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.



```
C:\>ipv6config /all

FastEthernet0 Connection: (default port)

Physical Address.....: 0060.7034.6930
Link-local IPv6 Address.....: FE80::260:70FF:FE34:6930
IPv6 Address.....: 2001:DB8:1:4::A/64
Default Gateway.....: FE80::3
DNS Servers.....:
DHCPv6 Client DUID.....: 00-01-00-01-DD-BD-1D-77-00-60-70-34-69-30

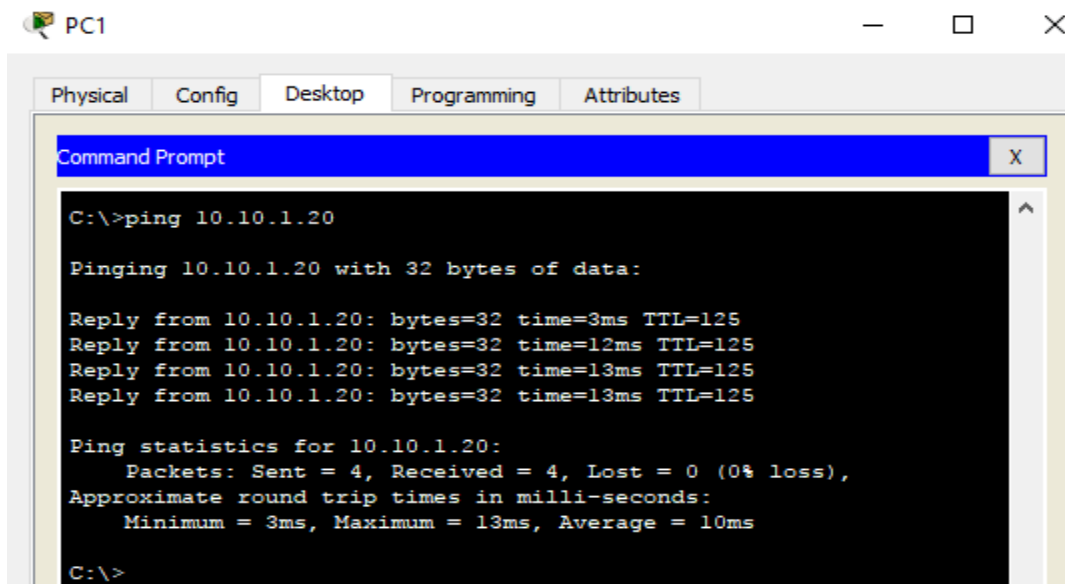
C:\>
```

Parte 2: Probar la conectividad mediante el comando ping

Paso 1: Usar el comando ping para verificar la conectividad IPv4

- e. Desde la **PC1**, haga ping a la dirección IPv4 de la **PC2**. ¿El resultado fue satisfactorio?

R: Si es satisfactorio



```
C:\>ping 10.10.1.20

Pinging 10.10.1.20 with 32 bytes of data:

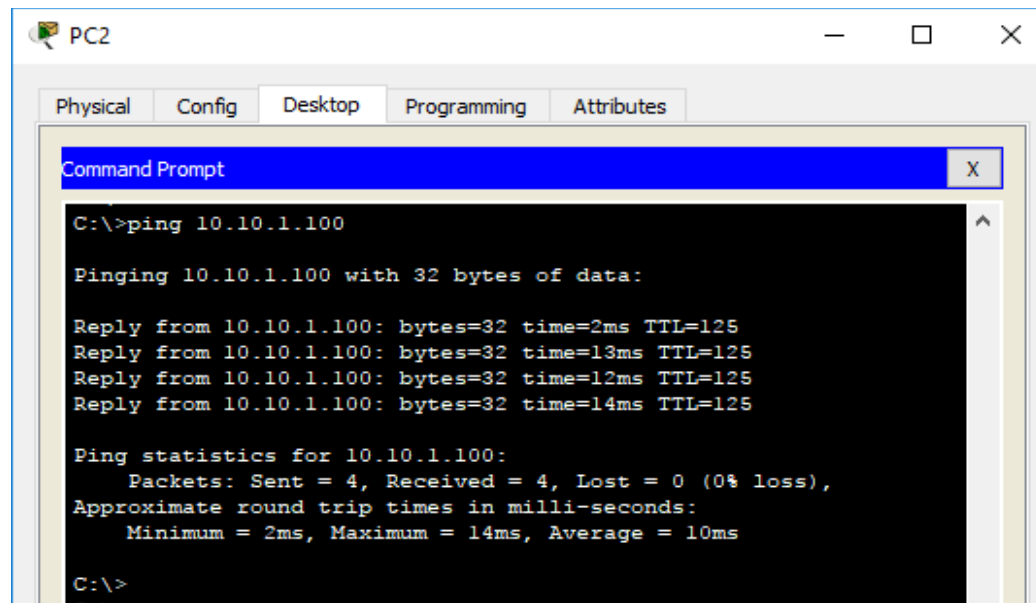
Reply from 10.10.1.20: bytes=32 time=3ms TTL=125
Reply from 10.10.1.20: bytes=32 time=12ms TTL=125
Reply from 10.10.1.20: bytes=32 time=13ms TTL=125
Reply from 10.10.1.20: bytes=32 time=13ms TTL=125

Ping statistics for 10.10.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 13ms, Average = 10ms

C:\>
```


f. Desde la **PC2**, haga ping a la dirección IPv4 de la **PC1**. ¿El resultado fue satisfactorio?

R: Si es satisfactorio



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.10.1.100

Pinging 10.10.1.100 with 32 bytes of data:

Reply from 10.10.1.100: bytes=32 time=2ms TTL=125
Reply from 10.10.1.100: bytes=32 time=13ms TTL=125
Reply from 10.10.1.100: bytes=32 time=12ms TTL=125
Reply from 10.10.1.100: bytes=32 time=14ms TTL=125

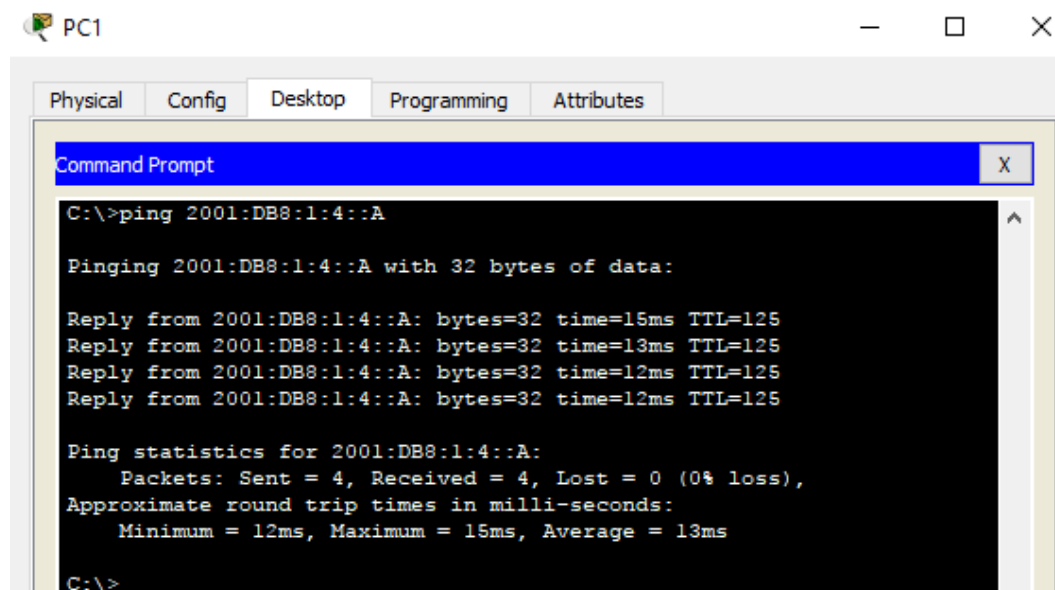
Ping statistics for 10.10.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 10ms

C:\>
```

Paso 2: Usar el comando ping para verificar la conectividad IPv6

d. Desde la **PC1**, haga ping a la dirección IPv6 de la **PC2**. ¿El resultado fue satisfactorio?

R: Si es satisfactorio



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:DB8:1:4::A

Pinging 2001:DB8:1:4::A with 32 bytes of data:

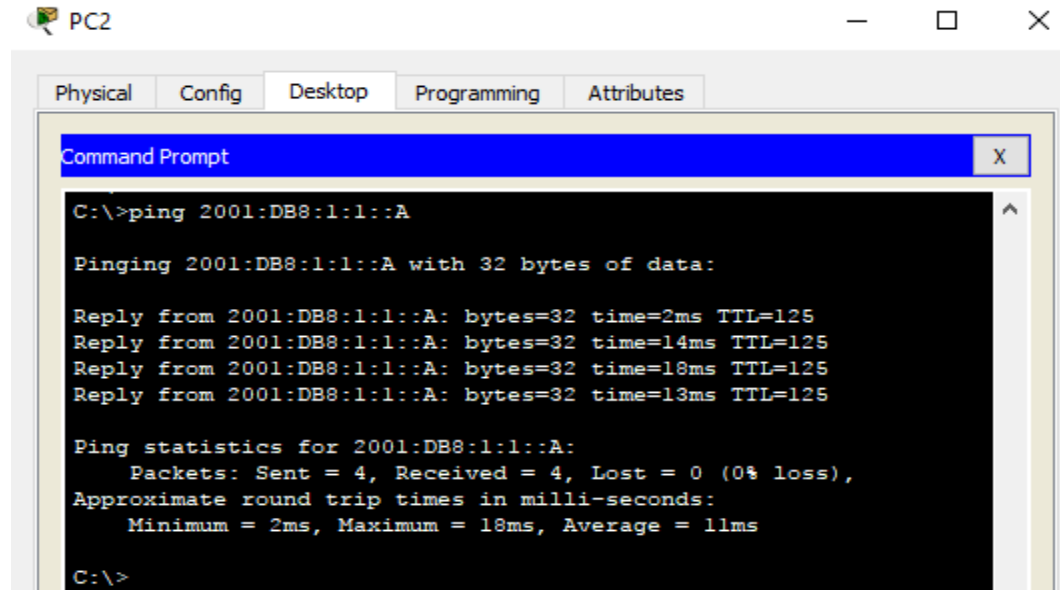
Reply from 2001:DB8:1:4::A: bytes=32 time=15ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=12ms TTL=125

Ping statistics for 2001:DB8:1:4::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 15ms, Average = 13ms

C:\>
```

e. Desde la **PC2**, haga ping a la dirección IPv6 de la **PC1**. ¿El resultado fue satisfactorio?

R: Si es satisfactorio



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:DB8:1:1::A

Pinging 2001:DB8:1:1::A with 32 bytes of data:

Reply from 2001:DB8:1:1::A: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:1::A: bytes=32 time=14ms TTL=125
Reply from 2001:DB8:1:1::A: bytes=32 time=18ms TTL=125
Reply from 2001:DB8:1:1::A: bytes=32 time=13ms TTL=125

Ping statistics for 2001:DB8:1:1::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 18ms, Average = 11ms

C:\>
```

Parte 3: Descubrir la ruta mediante su rastreo

Paso 1: Usar el comando tracert para descubrir la ruta IPv4

d. Desde la **PC1**, rastree la ruta a la **PC2**.

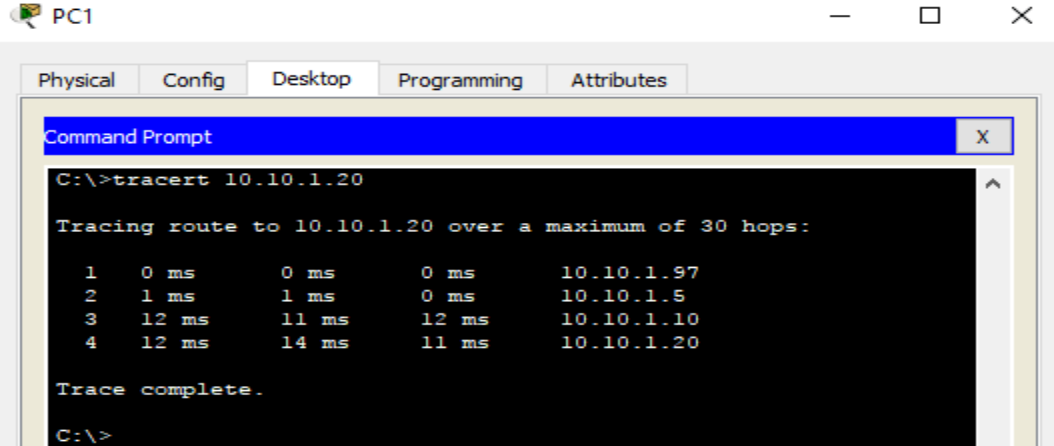
```
PC> tracert 10.10.1.20
```

¿Qué direcciones se encontraron a lo largo de la ruta?

R: 10.10.1.97, 10.10.1.5, 10.10.1.10, 10.10.1.20

¿Con qué interfaces se asocian las cuatro direcciones?

R: G0/0 del R1, S0/0/0 en el R2, S0/0/01 en el R3, NIC de la PC2



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>tracert 10.10.1.20

Tracing route to 10.10.1.20 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    10.10.1.97
  2  1 ms    1 ms    0 ms    10.10.1.5
  3  12 ms   11 ms   12 ms   10.10.1.10
  4  12 ms   14 ms   11 ms   10.10.1.20

Trace complete.

C:\>
```

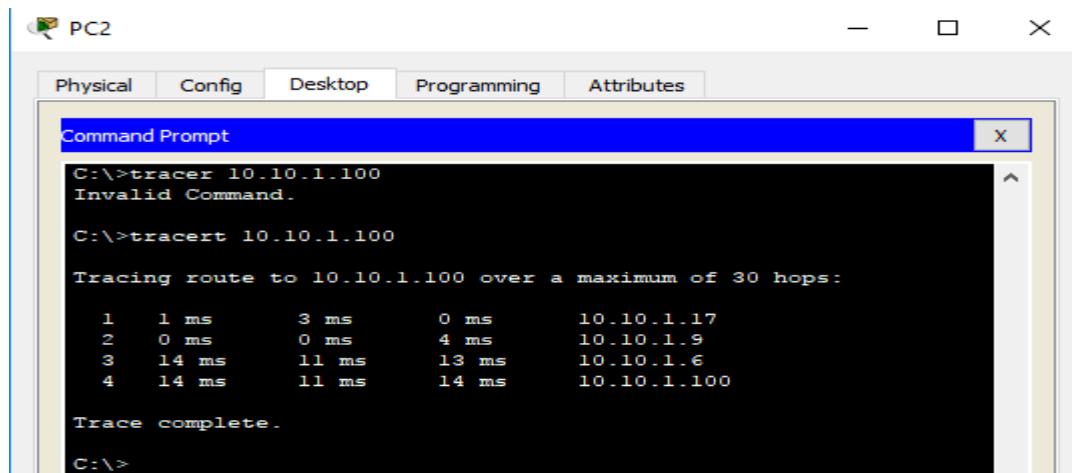
e. Desde la **PC2**, rastree la ruta a la **PC1**.

¿Qué direcciones se encontraron a lo largo de la ruta?

R: 10.10.1.17, 10.10.1.9, 10.10.1.6, 10.10.1.100

¿Con qué interfaces se asocian las cuatro direcciones?

R: G0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, NIC de la PC1



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>tracert 10.10.1.100
Invalid Command.

C:\>tracert 10.10.1.100

Tracing route to 10.10.1.100 over a maximum of 30 hops:

  1  1 ms    3 ms    0 ms    10.10.1.17
  2  0 ms    0 ms    4 ms    10.10.1.9
  3  14 ms   11 ms   13 ms   10.10.1.6
  4  14 ms   11 ms   14 ms   10.10.1.100

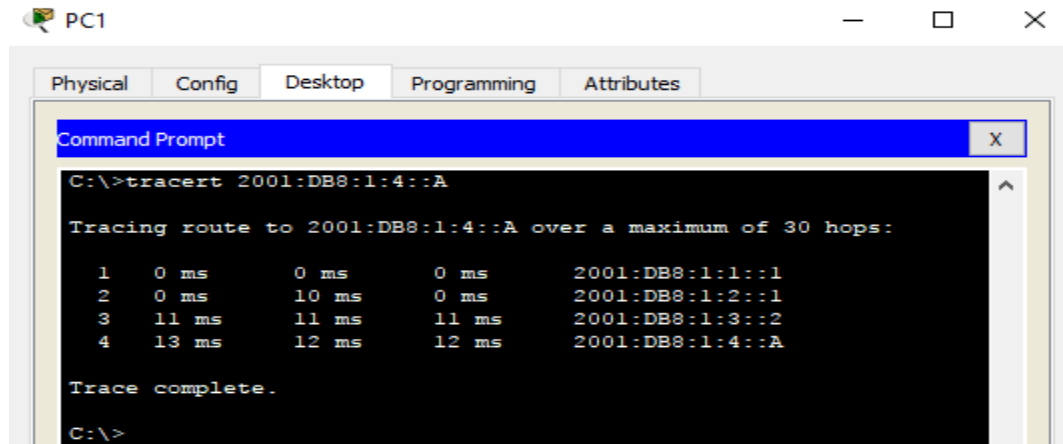
Trace complete.

C:\>
```

Paso 2: Usar el comando tracer para descubrir la ruta IPv6

- e. Desde la **PC1**, rastree la ruta a la dirección IPv6 de la **PC2**.

```
PC> tracer 2001:DB8:1:4::A
```



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>tracer 2001:DB8:1:4::A

Tracing route to 2001:DB8:1:4::A over a maximum of 30 hops:

 1  0 ms    0 ms    0 ms    2001:DB8:1:1::1
 2  0 ms    10 ms   0 ms    2001:DB8:1:2::1
 3  11 ms   11 ms   11 ms   2001:DB8:1:3::2
 4  13 ms   12 ms   12 ms   2001:DB8:1:4::A

Trace complete.

C:\>
```

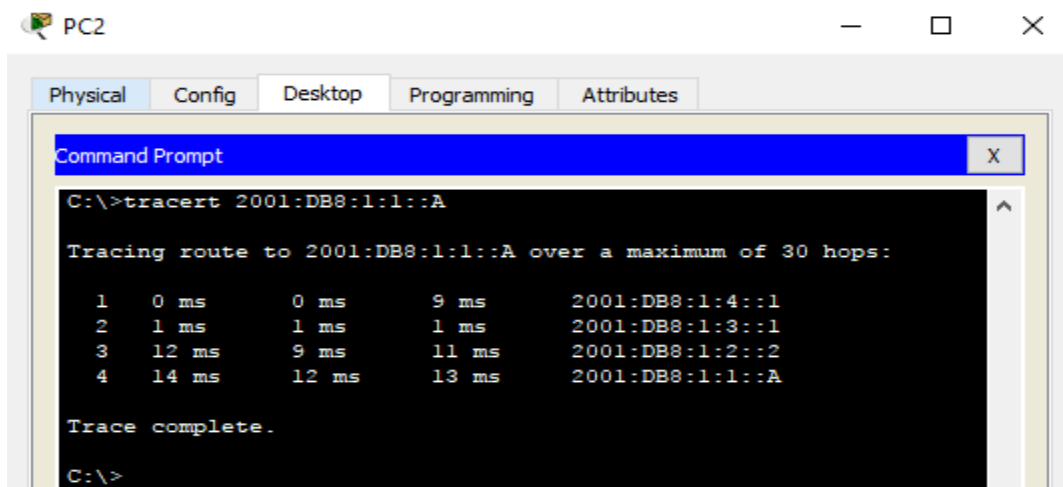
¿Qué direcciones se encontraron a lo largo de la ruta?

R: 2001:DB8:1:1::1, 2001:DB8:1:2::1, 2001:DB8:1:3::2, 2001:DB8:1:4::A

¿Con qué interfaces se asocian las cuatro direcciones?

R: G0/0 del R1, S0/0/0 del R2, S0/0/1 del R3, NIC de la PC2

- f. Desde la **PC2**, rastree la ruta a la dirección IPv6 de la **PC1**.



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>tracer 2001:DB8:1:1::A

Tracing route to 2001:DB8:1:1::A over a maximum of 30 hops:

 1  0 ms    0 ms    9 ms    2001:DB8:1:4::1
 2  1 ms    1 ms    1 ms    2001:DB8:1:3::1
 3  12 ms   9 ms    11 ms   2001:DB8:1:2::2
 4  14 ms   12 ms   13 ms   2001:DB8:1:1::A

Trace complete.

C:\>
```

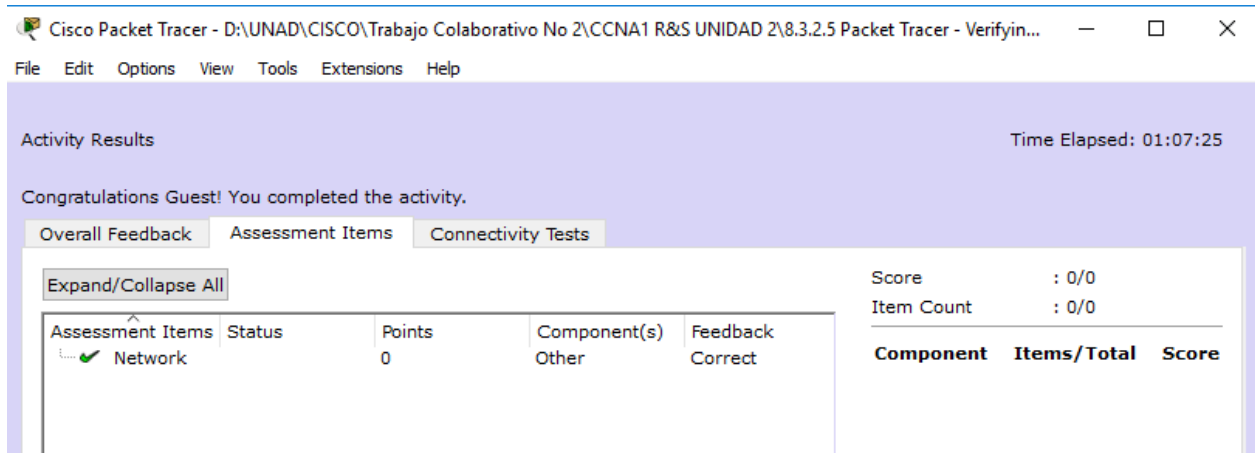
¿Qué direcciones se encontraron a lo largo de la ruta?

R: 2001:DB8:1:4::1, 2001:DB8:1:3::1, 2001:DB8:1:2::2, 2001:DB8:1:1::A

¿Con qué interfaces se asocian las cuatro direcciones?

R: Ga0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, NIC de la PC1

Ítems Resueltos



Cisco Packet Tracer - D:\UNAD\CISCO\Trabajo Colaborativo No 2\CCNA1 R&S UNIDAD 2\8.3.2.5 Packet Tracer - Verifyin... — □ ×

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 01:07:25

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
✓ Network		0	Other	Correct

Score : 0/0
Item Count : 0/0

Component	Items/Total	Score
-----------	-------------	-------

Ejercicio 8.3.2.6: Ping y rastreo para probar rutas

Topología

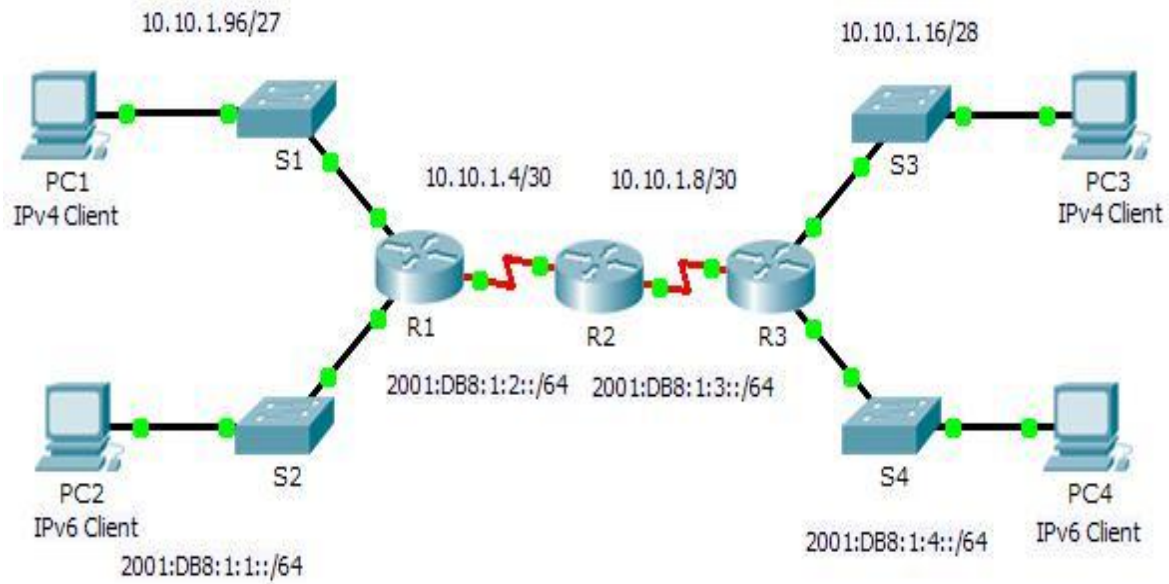


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	2001:DB8:1:1::1/64		No aplicable
	G0/1	10.10.1.97	255.255.255.224	No aplicable
	S0/0/1	10.10.1.6	255.255.255.252	No aplicable
		2001:DB8:1:2::2/64		No aplicable
	Link-local	FE80::1		No aplicable
R2	S0/0/0	10.10.1.5	255.255.255.252	No aplicable
		2001:DB8:1:2::1/64		No aplicable
	S0/0/1	10.10.1.9	255.255.255.252	No aplicable
		2001:DB8:1:3::1/64		No aplicable
	Link-local	FE80::2		No aplicable
R3	G0/0	2001:DB8:1:4::1/64		No aplicable
	G0/1	10.10.1.17	255.255.255.240	No aplicable
	S0/0/1	10.10.1.10	255.255.255.252	No aplicable
		2001:DB8:1:3::2/64		No aplicable
	Link-local	FE80::3		No aplicable
PC1	NIC	10.10.1.98	255.255.255.224	10.10.1.97
PC2	NIC	2001:DB8:1:1::2/64		FE80::1
PC3	NIC	10.10.1.18	255.255.255.240	10.10.1.17
PC4	NIC	2001:DB8:1:4::2/64		FE80::1

Objetivos

Parte 1: Probar y restaurar la conectividad IPv4

Parte 2: Probar y restaurar la conectividad IPv6

Situación

En esta actividad, hay problemas de conectividad. Además de recopilar y registrar información acerca de la red, localizará los problemas e implementará soluciones razonables para restaurar la conectividad. **Nota:** la contraseña de EXEC del usuario es **cisco**. La contraseña de EXEC privilegiado es **class**.

Packet Tracer: uso de herramientas de ping y rastreo para probar la ruta

Parte 1: Probar y restaurar la conectividad IPv4

Paso 1: Usar los comandos ipconfig y ping para verificar la conectividad a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop > Command Prompt** (Escritorio > Símbolo del sistema).

The screenshot displays a network simulation in Packet Tracer. The main window shows a logical network topology with the following components and connections:

- PC1 (IPv4 Client):** IP address 10.10.1.96/27, connected to switch S1.
- PC2 (IPv6 Client):** IP address 2001:DB8:1:1::/64, connected to switch S2.
- Switches:** S1 and S2 are connected to each other and to routers R1 and R2.
- Routers:** R1 and R2 are connected to each other. R1 has IP 10.10.1.4/30 on its interface connected to S1. R2 has IP 2001:DB8:1:2::/64 on its interface connected to S2.

A **Command Prompt** window is open for PC1, showing the output of a Packet Tracer PC Command Line 1.0 session. The window title is "Command Prompt" and the content is:

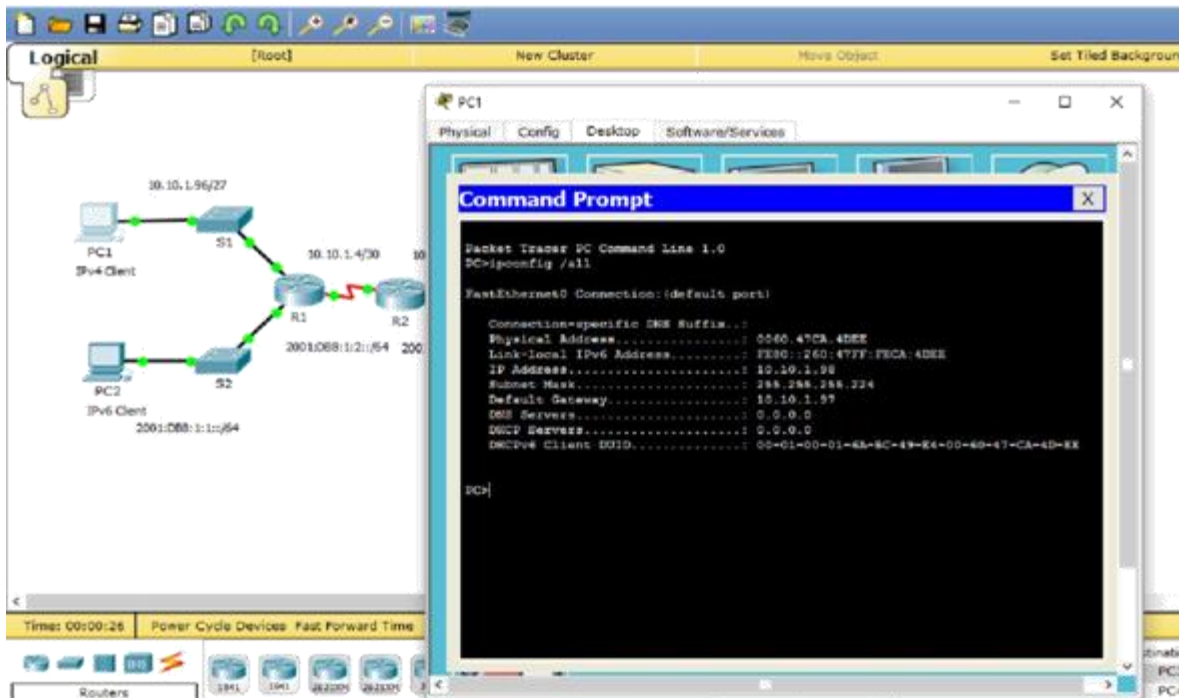
```
Packet Tracer PC Command Line 1.0
PC>
```

At the bottom of the Packet Tracer interface, a table shows the results of a real-time trace:

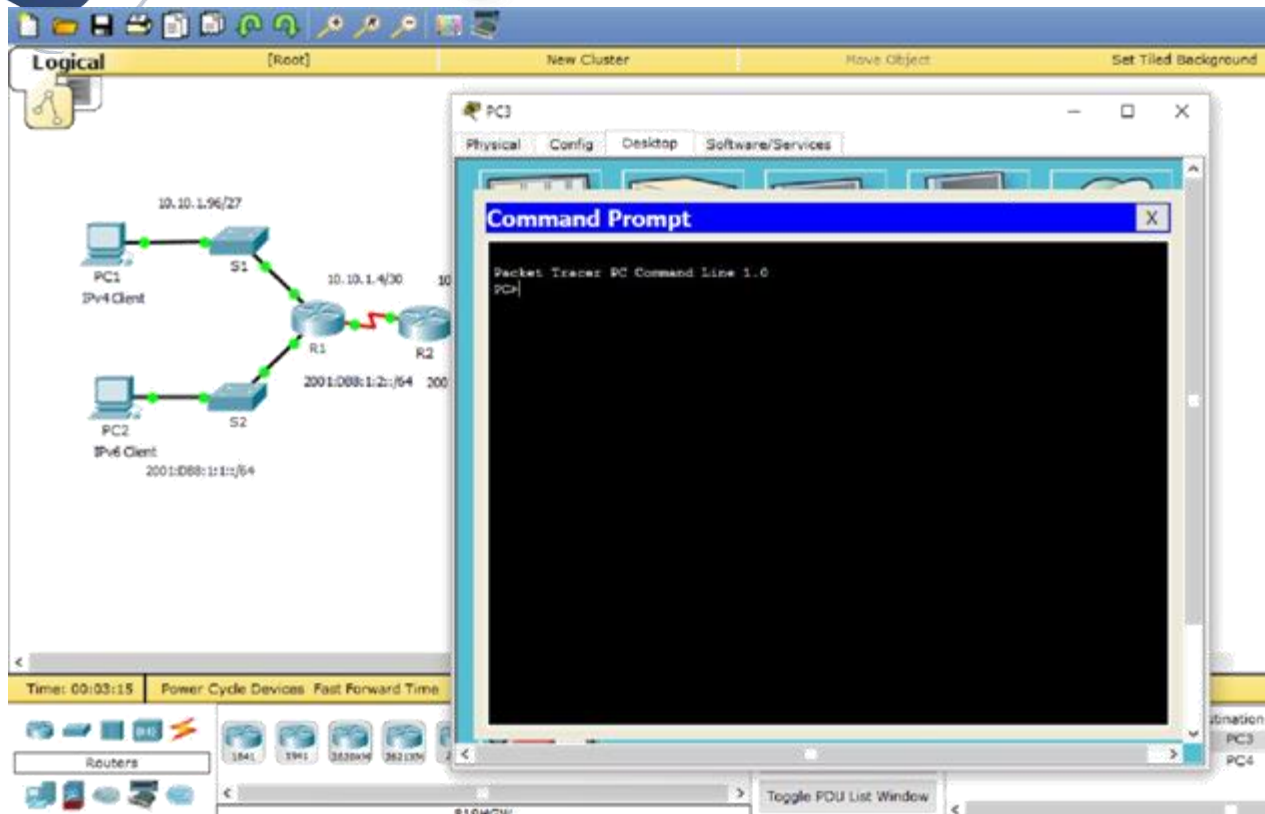
Destination	Type	Color	Time(sec)	Periodic	Num
PC3	ICMP		0.000	N	0
PC4	ICMP..		0.000	N	1

b. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

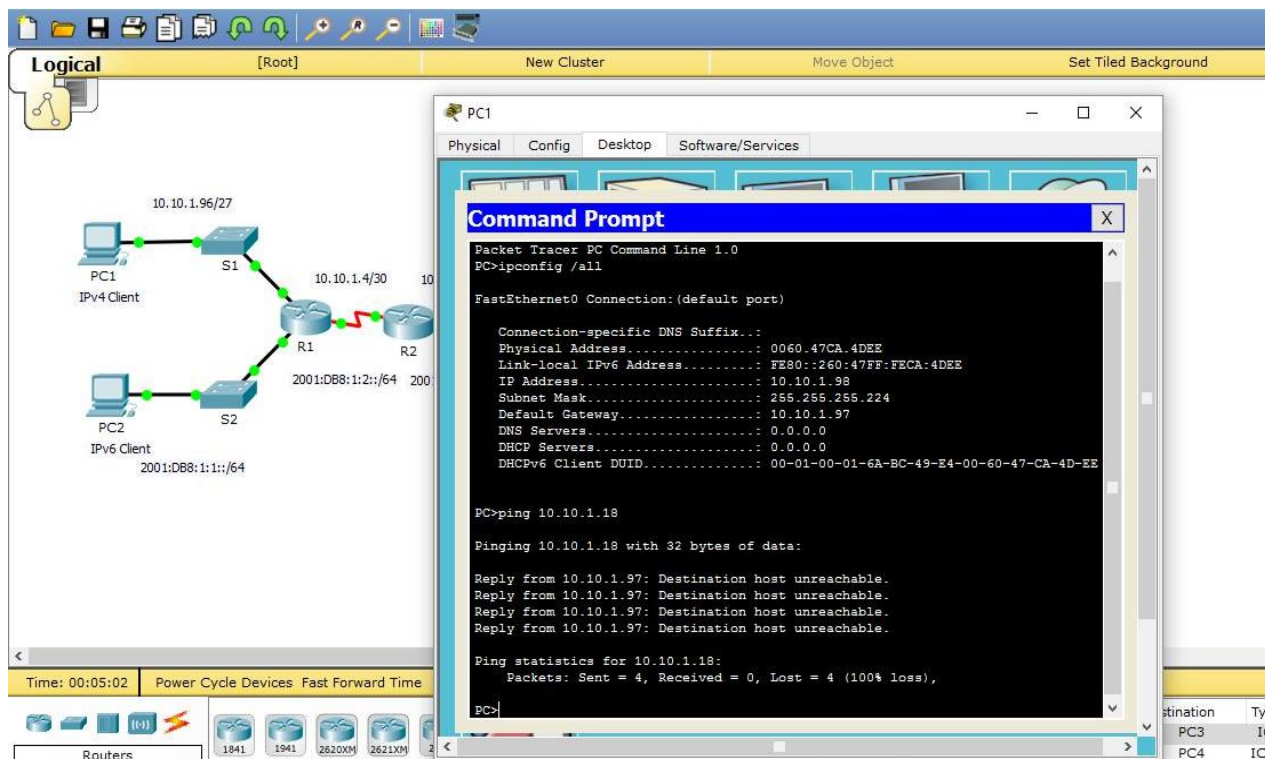
c. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop > Command Prompt**



d. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.



d. Pruebe la conectividad entre la **PC1** y la **PC3**. El ping debe fallar.



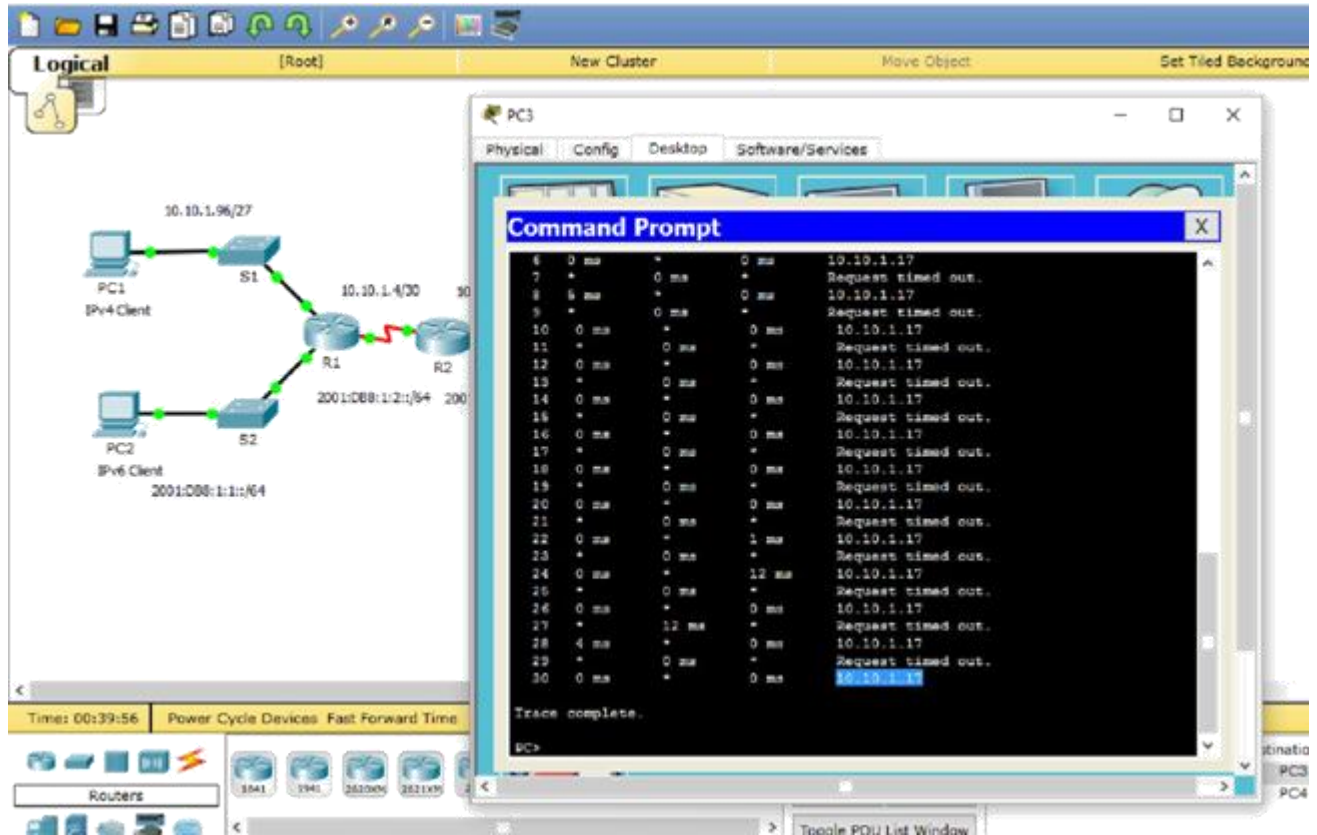
Paso 2: Localice el origen de la falla de conectividad.

- a. Desde la **PC1**, introduzca el comando necesario para rastrear la ruta a la **PC3**. ¿Cuál es la última dirección IPv4 correcta que alcanzó? 10.10.1.97

The screenshot shows a network simulation interface with a logical network diagram on the left and a command prompt window on the right. The diagram includes PC1 (IPv4 Client, 10.10.1.96/27), PC2 (IPv6 Client, 2001:DB8:1:1::/64), switches S1 and S2, and routers R1 and R2. A red line indicates a connectivity issue between R1 and R2. The command prompt window shows the output of a traceroute command from PC1 to 10.10.1.97.

```
Command Prompt
6 0 ms * 0 ms 10.10.1.97
7 + 0 ms * Request timed out.
8 0 ms * 0 ms 10.10.1.97
9 + 0 ms * Request timed out.
10 4 ms * 1 ms 10.10.1.97
11 + 0 ms * Request timed out.
12 0 ms * 0 ms 10.10.1.97
13 + 1 ms * Request timed out.
14 0 ms * 0 ms 10.10.1.97
15 + 0 ms * Request timed out.
16 0 ms * 0 ms 10.10.1.97
17 + 0 ms * Request timed out.
18 0 ms * 0 ms 10.10.1.97
19 + 0 ms * Request timed out.
20 2 ms * 0 ms 10.10.1.97
21 + 15 ms * Request timed out.
22 10 ms * 0 ms 10.10.1.97
23 + 1 ms * Request timed out.
24 0 ms * 0 ms 10.10.1.97
25 + 0 ms * Request timed out.
26 0 ms * 0 ms 10.10.1.97
27 + 0 ms * Request timed out.
28 2 ms * 0 ms 10.10.1.97
29 + 0 ms * Request timed out.
30 0 ms * 0 ms 10.10.1.97
Trace complete.
PC>
```

- b. El rastreo finalmente terminará después de 30 intentos. Introduzca **Ctrl+C** para detener el rastreo antes de los 30 intentos.



- c. Desde la **PC3**, introduzca el comando necesario para rastrear la ruta a la **PC1**.
¿Cuál es la última
- d. dirección IPv4 correcta que alcanzó? 10.10.1.17
- e. Introduzca **Ctrl+C** para detener el rastreo.
- f. Haga clic en **R1** y, a continuación, haga clic en la ficha **CLI**. Presione **ENTRAR** e inicie sesión en el router.
- g. Introduzca el comando **show ip interface brief** para obtener una lista de las interfaces y su estado. Hay dos direcciones IPv4 en el router. Una se debió haber registrado en el paso 2a.
¿Cuál es la otra? 10.10.1.6

The screenshot shows a network diagram on the left with routers R1 and R2, and PCs PC1 and PC2. R1 is connected to PC1 (10.10.1.96/27) and PC2 (2001:DB8:1:1::/64). R1 is also connected to R2 (2001:DB8:1:2::/64). The CLI window for R1 shows the following output for 'show ip interface brief':

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet0/1	10.10.1.97	YES	manual	up	up
Serial10/0/0	unassigned	YES	unset	administratively down	down
Serial10/0/1	10.10.1.6	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

g. Introduzca el comando **show ip route** para obtener una lista de las redes a las que está conectado el router. Observe que hay dos redes conectadas a la interfaz **Serial10/0/1**. ¿Cuáles son? 10.10.1.6/32, 10.10.1.4/30

The screenshot shows the same network diagram as above. The CLI window for R1 shows the output of 'show ip route':

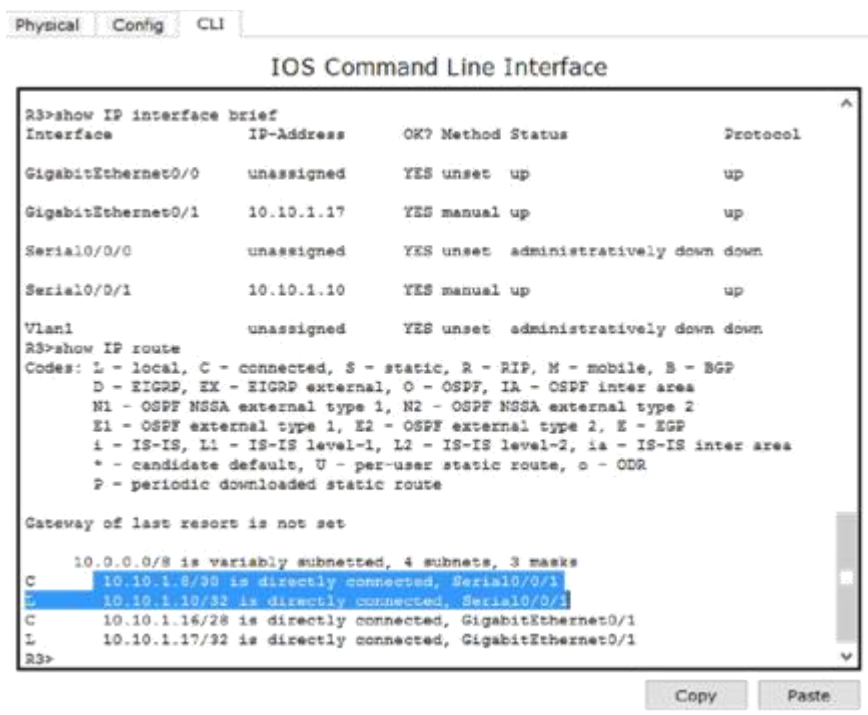
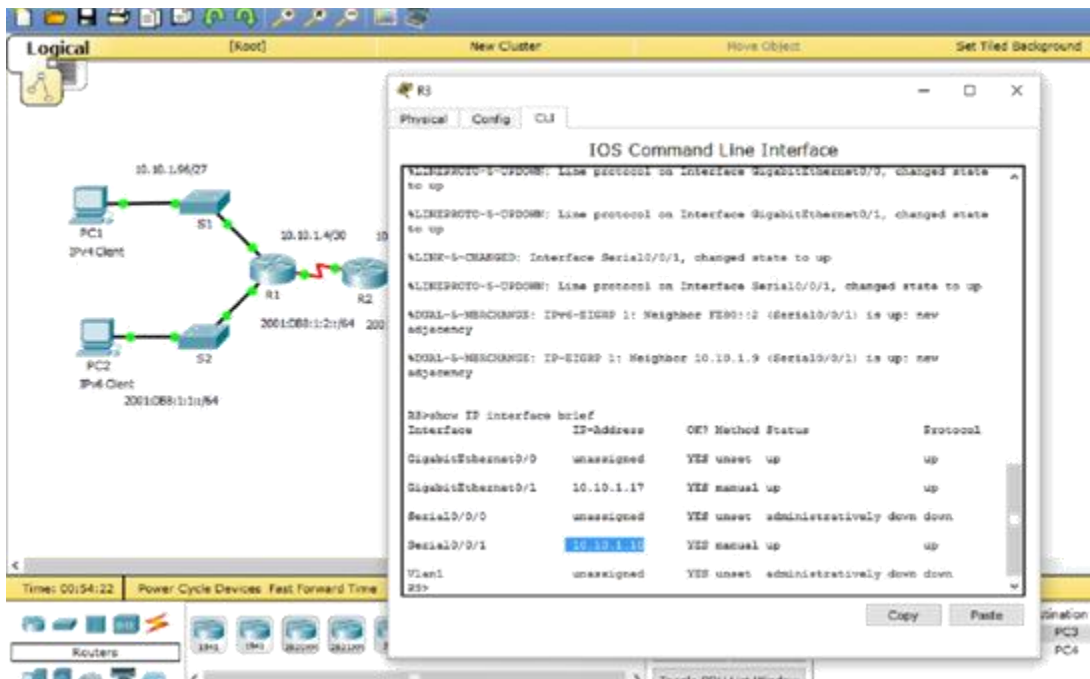
```

R1>show ip route
Codes: L - local, C - connected, S - static, 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 - SGP
       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

10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.10.1.4/30 is directly connected, Serial10/0/1
C       10.10.1.6/32 is directly connected, Serial10/0/1
C       10.10.1.96/27 is directly connected, GigabitEthernet0/1
L       10.10.1.97/32 is directly connected, GigabitEthernet0/1
R1>
    
```

h. Repita los pasos 2e a 2g con el R3 y escriba las respuestas aquí. 10.10.1.10, 10.10.1.8/30, 10.10.1.10/32



Observe cómo cambia la interfaz serial para el R3.

- h. Ejecute más pruebas si eso permite visualizar el problema. El modo de simulación está disponible.


The screenshot shows a network simulation environment. On the left, a topology diagram displays three routers: R1, R2, and R3. R1 is connected to R2 and R3. R1 has two GigabitEthernet interfaces (G0/0 and G0/1) and two Serial interfaces (S0/0 and S0/1). R2 has one GigabitEthernet interface (G0/0) and one Serial interface (S0/0). R3 has one GigabitEthernet interface (G0/0) and one Serial interface (S0/0). Two PCs, PC1 and PC2, are connected to R1. PC1 is labeled as an IPv4 Client with IP 10.10.1.56/27. PC2 is labeled as an IPv6 Client with address 2001:008:1:1::64. The interface S0/0/0 on R1 is highlighted in blue. On the right, a CLI window for R2 displays the output of the 'show IP interface brief' command. The output is as follows:

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	10.10.1.2	YES	manual	up	up
Serial0/0/1	10.10.1.3	YES	manual	up	up
T1ent1	unassigned	YES	unset	administratively down	down

Below the table, the CLI shows the output of 'show IP route' and 'show IP route' commands, indicating that the Serial0/0/0 interface is directly connected to 10.10.1.2/32 and 10.10.1.3/32.

Paso 3: Proponga una solución para resolver el problema. a. Compare sus respuestas del paso 2 con la documentación que tiene disponible para la red. ¿Cuál es el error?
La interfaz Serial 0/0/0 del R2 está configurada con una dirección IP incorrecta.

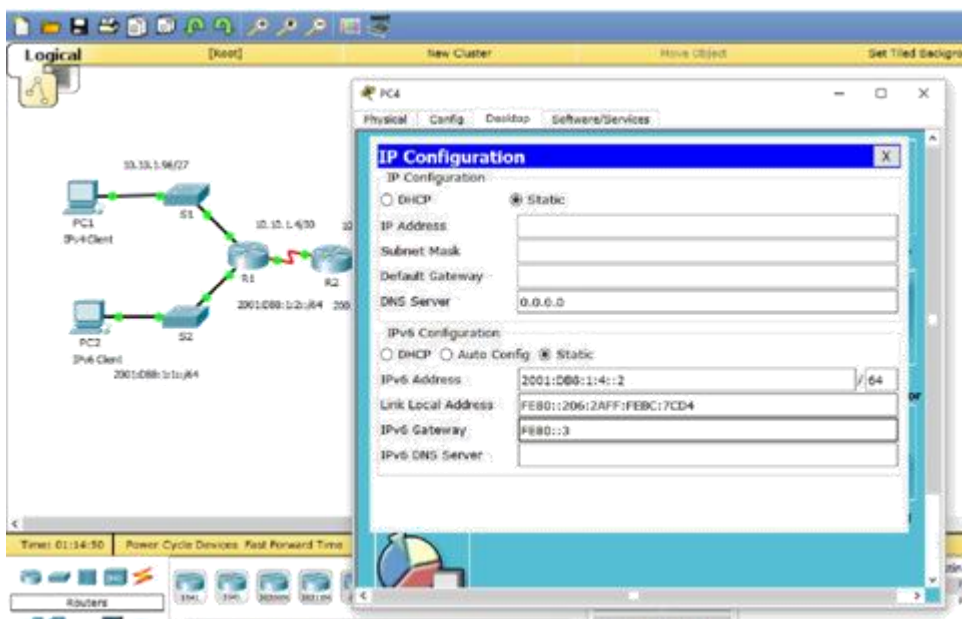
b. ¿Qué solución propondría para corregir el problema? Configurar la dirección IP correcta en la interfaz Serial 0/0/0 del R2 (10.10.1.5).



```
R2
-----
Physical  Config  CLI
IOS Command Line Interface

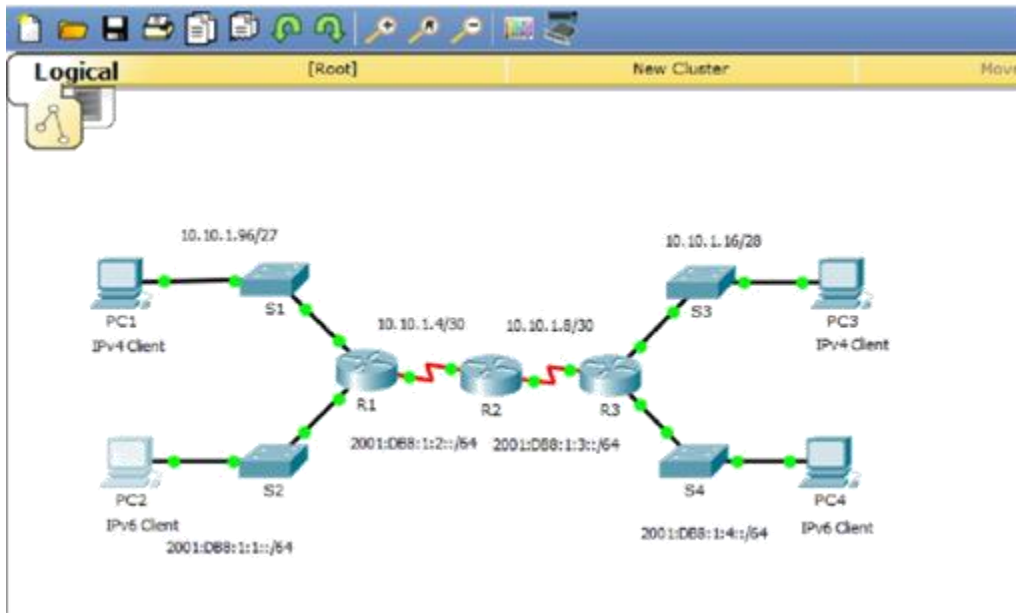
Press RETURN to get started.

R2>en
R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R2 (config)#interface s0/0/0
R2 (config-if)#ip address 10.10.1.5 255.255.255.252
R2 (config-if)#
%DUAL-5-DERCHANGE: IP-IGRP 1: Neighbor 10.10.1.6 (Serial0/0/0) is up: new
ad)acency
R2 (config-if)#exit
R2 (config)#
```



Paso 4: Implemente el plan.

Implemente la solución que propuso en el paso 3b.



Paso 5: Verifique que la conectividad esté restaurada. a. Desde la **PC1**, pruebe la conectividad a la **PC3**.

b. Desde la **PC3**, pruebe la conectividad a la **PC1**. ¿Se resolvió el problema? Sí

```
20 0 ms * 0 ms 10.10.1.17
21 * 0 ms * Request timed out.
22 0 ms * 1 ms 10.10.1.17
23 * 0 ms * Request timed out.
24 0 ms * 12 ms 10.10.1.17
25 * 0 ms * Request timed out.
26 0 ms * 0 ms 10.10.1.17
27 * 12 ms * Request timed out.
28 4 ms * 0 ms 10.10.1.17
29 * 0 ms * Request timed out.
30 0 ms * 0 ms 10.10.1.17

Trace complete.
PC>ping 10.10.1.98

Pinging 10.10.1.98 with 32 bytes of data:

Reply from 10.10.1.98: bytes=32 time=1ms TTL=128
Reply from 10.10.1.98: bytes=32 time=1ms TTL=128
Reply from 10.10.1.98: bytes=32 time=1ms TTL=128
Reply from 10.10.1.98: bytes=32 time=1ms TTL=128

Ping statistics for 10.10.1.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Paso 6: Documentar la solución.

Cisco Packet Tracer Student - C:\Users\Ladino\Desktop\DIPLOMADO CISCO\ACTIVIDAD 2\CCNA1 R&S UNIDAD 2\8.3.2.6 Packet Tracer - Pinging and Tracing to Test the Path.pka

Activity Results

Time Elapsed: 01:18:49

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Congratulations! You successfully completed the Packet Tracer - Pinging and Tracing to Test the Path activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.

Ejercicio 8.3.2.8: Resolución de problemas de direccionamiento IPv4 e IPv6

Topología

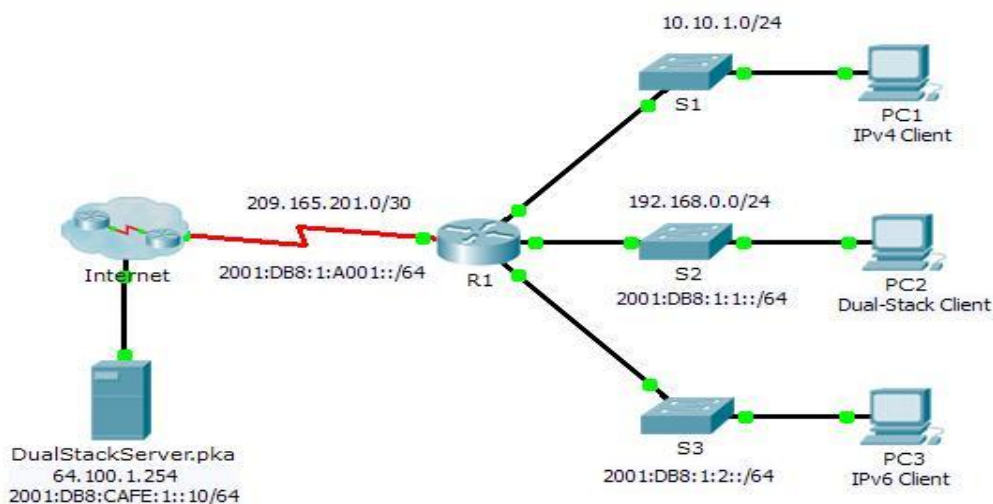


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	10.10.1.1	255.255.255.0	No aplicable
	Ga0/1	192.168.0.1	255.255.255.0	No aplicable
		2001:DB8:1:1::1/64		No aplicable
	G0/2	2001:DB8:1:2::1/64		No aplicable
	S0/0/0	209.165.201.2	255.255.255.252	No aplicable
		2001:DB8:1:A001::2/64		No aplicable
Link-local	FE80::1		No aplicable	
Servidor dual-stack	NIC	64.100.1.254	255.255.255.0	64.100.1.1
		2001:DB8:CAFE:1::10/64		FE80::A
PC1	NIC	10.10.1.2	255.255.255.0	10.10.1.1
PC2	NIC	192.168.0.2	255.255.255.0	192.168.0.1

		2001:DB8:1:1::2/64	FE80::1
PC3	NIC	2001:DB8:1:2::2/64	FE80::1

Objetivos

Parte 1: Resolver el primer problema

Parte 2: Resolver el segundo problema

Parte 3: Resolver el tercer problema

Situación

Usted es un técnico de red que trabaja para una compañía que decidió migrar de IPv4 a IPv6. Mientras tanto, debe admitir ambos protocolos (dual-stack). Tres compañeros de trabajo llamaron al soporte técnico para resolver algunos problemas, pero no recibieron suficiente asistencia. El soporte técnico le elevó el problema a usted, un técnico de soporte de nivel 2. Su trabajo es localizar el origen de los problemas e implementar las soluciones adecuadas.

Parte 1: Resolver el primer problema

Un cliente que usa la **PC1** se queja de que no puede acceder a la página Web **dualstackserver.pka**.

Paso 1: Verificar una solicitud detallada de soporte técnico.

El soporte técnico recopiló la siguiente información del cliente por vía telefónica. Verifique que sea correcto.

Solicitud de soporte técnico

Identificador de cliente: PC1

Problema: No puede acceder a la página Web dualstackserver.pka.

Información detallada sobre el problema

Prueba: ¿Tiene la PC una dirección IP cuando se utiliza ipconfig ?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el gateway usando ping ?	Sí
Prueba: ¿Puede la PC contactar al servidor utilizando tracert ?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el servidor mediante nslookup ?	No
Resolución: Elevar al soporte de nivel 2.	

Paso 2: Considerar las causas probables de la falla

- Observe las pruebas que se realizaron. De ser posible, analice con sus colegas técnicos de red (compañeros de curso) las situaciones que podrían ser la causa de este problema.
- Ejecute más pruebas si eso permite visualizar el problema. El modo de simulación está disponible.

Paso 3: Proponga una solución para resolver el problema.

Haga una lista de factores que se podrían cambiar para solucionar este problema. Comience con la solución que tenga más posibilidades de funcionar.

Paso 4: Implemente el plan.

Pruebe la solución más probable de la lista. Si ya se probó, pase a la siguiente solución.

Paso 5: Verificar que la solución haya resuelto el problema

- Repita las pruebas de la solicitud de soporte técnico. ¿Se solucionó el problema?
- Si el problema persiste, revierta el cambio en caso de no estar seguro de que sea correcto y vuelva al paso 4.

Paso 6: Documentar la solución.

Registre la solución al problema. Si alguna vez se vuelve a encontrar con el mismo problema, las notas serán muy valiosas.

La dirección DNS IPv4 de la PC1 es incorrecta.

Parte 2: Resolver el segundo el problema

Un cliente que usa la PC2 se queja de que no puede acceder a los archivos ubicados en **DualStackServer.pka** en 2001:DB8:CAFE:1::10.

Paso 1: Verificar una solicitud detallada de soporte técnico.

El soporte técnico recopiló la siguiente información del cliente por vía telefónica. Verifique que sea correcto.

Solicitud de soporte técnico

Identificador de cliente: PC2

Problema: No puede acceder al servicio FTP de 2001:DB8:CAFE:1:10.

Información detallada sobre el problema

Prueba: ¿Tiene la PC una dirección IPv6 cuando se utiliza ipv6config ?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el gateway usando ping ?	Sí
Prueba: ¿Puede la PC contactar al servidor utilizando tracert ?	No
Resolución: Elevar al soporte de nivel 2.	

Paso 2: Realizar los pasos 2 a 5 de la parte 1 para abordar este problema.

Paso 3: Documentar la solución.

Registre la solución al problema. Si alguna vez se vuelve a encontrar con el mismo problema, las notas serán muy valiosas.

La dirección de gateway IPv6 de DualStackServer.pka es incorrecta

Parte 3: Resolver el tercer problema

Un cliente que usa la **PC1** se queja de que no se puede comunicar con la **PC2**.

Paso 1: Verificar una solicitud detallada de soporte técnico.

El soporte técnico recopiló la siguiente información del usuario por vía telefónica. Verifique que sea correcto.

Solicitud de soporte técnico	
Identificador de cliente: PC3	
Problema: No se puede comunicar con la PC2.	
Información detallada sobre el problema	
Prueba: ¿Tiene la PC una dirección IP cuando se utiliza ipconfig ?	Sí
Prueba: ¿Tiene la PC una dirección IPv6 cuando se utiliza ipv6config ?	Sí
Prueba: ¿Puede la PC ponerse en contacto con su gateway IPv4 mediante ping ?	No
Prueba: ¿Puede la PC ponerse en contacto con su gateway IPv6 mediante ping ?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el cliente IPv4 mediante tracert ?	No
Prueba: ¿Puede la PC ponerse en contacto con el cliente IPv6 mediante tracert ?	Sí
Resolución: Elevar al soporte de nivel 2.	

Paso 2: Realizar los pasos 2 a 5 de la parte 1 para abordar este problema.

Paso 3: Documentar la solución.

Registre la solución al problema. Si alguna vez se vuelve a encontrar con el mismo problema, las notas serán muy valiosas.

La dirección de gateway IPv4 de la PC2 es incorrecta.

Ejercicio 8.4.1.2: Reto de habilidades de integración.

Topología

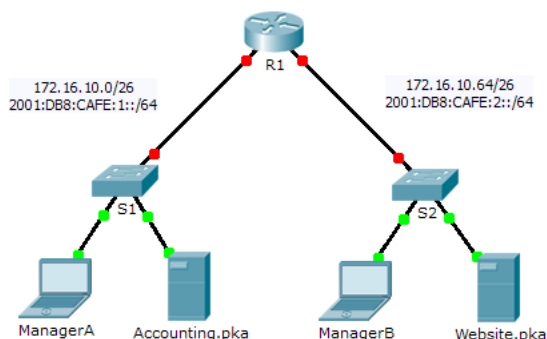


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de Dirección/Prefijo IPv6	Gateway predeterminado
R1	G0/0	172.16.10.1	255.255.255.192	No aplicable
		2001:DB8:CAFE:1::1/64		No aplicable
	G0/1	172.16.10.65	255.255.255.192	No aplicable
		2001:DB8:CAFE:2::1/64		No aplicable
	Link-local	FE80::1		No aplicable
S1	VLAN1	172.16.10.62	255.255.255.192	172.16.10.1
S2	VLAN1	172.16.10.126	255.255.255.192	172.16.10.65
ManagerA	NIC	172.16.10.3	255.255.255.192	172.16.10.1
		2001:DB8:CAFE:1::3/64		FE80::1
Accounting.pk	NIC	172.16.10.2	255.255.255.192	172.16.10.1
		2001:DB8:CAFE:1::2/64		FE80::1
ManagerB	NIC	172.16.10.67	255.255.255.192	172.16.10.65
		2001:DB8:CAFE:2::3/64		FE80::1
Website.pka	NIC	172.16.10.66	255.255.255.192	172.16.10.65
		2001:DB8:CAFE:2::2/64		FE80::1

Situación

Su compañía fue contratada para configurar una red pequeña para el propietario de un restaurante. Hay dos restaurantes cercanos entre sí y comparten una conexión. El equipo y el cableado están instalados, y el administrador de red diseñó el plan de implementación. Su trabajo consiste en implementar el resto del esquema de direccionamiento de acuerdo con la tabla de direccionamiento abreviada y verificar la conectividad.

Requisitos

- Complete el registro de la **tabla de direccionamiento**.
- Configure direccionamiento IPv4 e IPv6 en el **R1**.
- Configure direccionamiento IPv4 en el **S1**. El **S2** ya está configurado.
- Configure direccionamiento IPv4 e IPv6 en **ManagerA**. El resto de los clientes ya están configurados.
- Verifique la conectividad. Todos los clientes deben poder hacerse ping entre sí y acceder a los sitios
 Web en **Accounting.pka** y **Website.pka**.

Verificación de conectividad:

- Ping desde ManagerA hacia ManagerB (172.16.10.67), Accounting.pka (172.16.10.2) y Website.pka (172.16.10.66):

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

```

ManagerA
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.16.10.67

Pinging 172.16.10.67 with 32 bytes of data:

Reply from 172.16.10.67: bytes=32 time=1ms TTL=127
Reply from 172.16.10.67: bytes=32 time=25ms TTL=127
Reply from 172.16.10.67: bytes=32 time=19ms TTL=127
Reply from 172.16.10.67: bytes=32 time=15ms TTL=127

Ping statistics for 172.16.10.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 25ms, Average = 15ms

C:\>ping 172.16.10.2

Pinging 172.16.10.2 with 32 bytes of data:

Reply from 172.16.10.2: bytes=32 time<1ms TTL=128
Reply from 172.16.10.2: bytes=32 time=6ms TTL=128
Reply from 172.16.10.2: bytes=32 time=12ms TTL=128
Reply from 172.16.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 4ms

C:\>ping 172.16.10.66

Pinging 172.16.10.66 with 32 bytes of data:

Reply from 172.16.10.66: bytes=32 time=1ms TTL=127
Reply from 172.16.10.66: bytes=32 time=18ms TTL=127
Reply from 172.16.10.66: bytes=32 time=13ms TTL=127
Reply from 172.16.10.66: bytes=32 time=19ms TTL=127

Ping statistics for 172.16.10.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:

```

- Ping desde ManagerB hacia ManagerA (172.16.10.3), Accounting.pka (172.16.10.2) y Website.pka (172.16.10.66):

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

```

Physical Config Desktop Programming Attributes
Command Prompt
Pinging 172.16.10.3 with 32 bytes of data:

Reply from 172.16.10.3: bytes=32 time=1ms TTL=127
Reply from 172.16.10.3: bytes=32 time=20ms TTL=127
Reply from 172.16.10.3: bytes=32 time=16ms TTL=127
Reply from 172.16.10.3: bytes=32 time=17ms TTL=127

Ping statistics for 172.16.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 20ms, Average = 13ms

C:\>ping 172.16.10.2

Pinging 172.16.10.2 with 32 bytes of data:

Request timed out.
Reply from 172.16.10.2: bytes=32 time=25ms TTL=127
Reply from 172.16.10.2: bytes=32 time=15ms TTL=127
Reply from 172.16.10.2: bytes=32 time=14ms TTL=127

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 25ms, Average = 18ms

C:\>ping 172.16.10.66

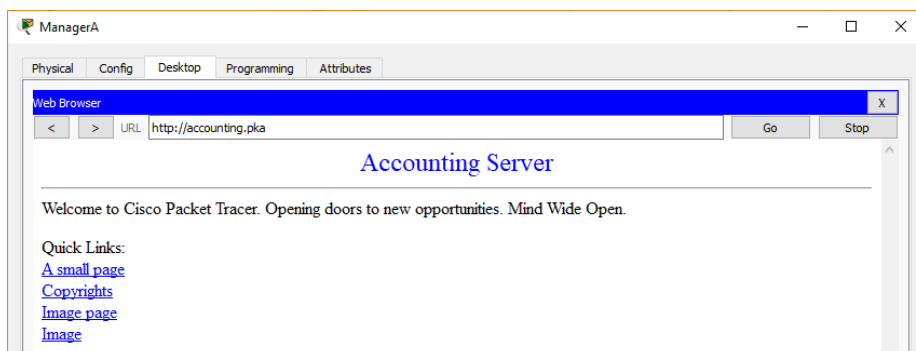
Pinging 172.16.10.66 with 32 bytes of data:

Reply from 172.16.10.66: bytes=32 time=1ms TTL=128
Reply from 172.16.10.66: bytes=32 time=13ms TTL=128
Reply from 172.16.10.66: bytes=32 time=12ms TTL=128
Reply from 172.16.10.66: bytes=32 time<1ms TTL=128

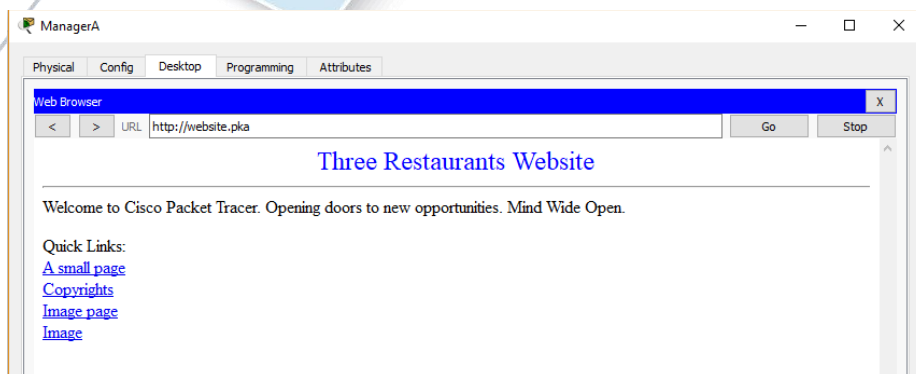
Ping statistics for 172.16.10.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 6ms
  
```

Accediendo a los sitios Web:

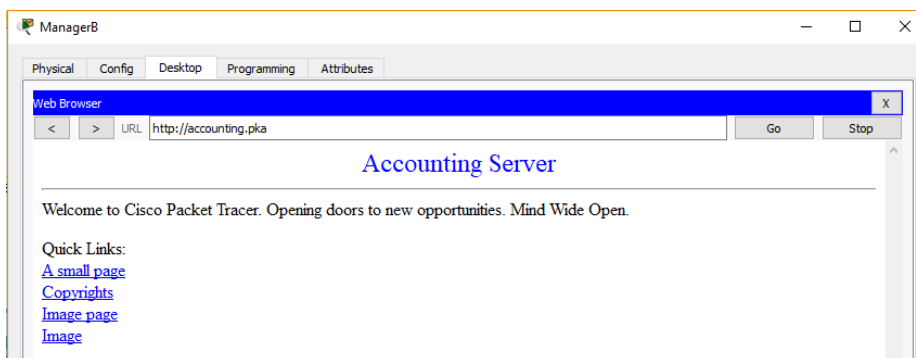
- Desde ManagerA



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



- Desde ManagerB



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Resultados:

PT Activity: 00:50:16

s1	VLAN1	172.16.10.62	255.255.255.192	172.16.10.1
s2	VLAN1	172.16.10.126	255.255.255.192	172.16.10.65
managerA	NIC	172.16.10.3	255.255.255.192	
		2001:DB8:CAFE:1::3/64		
ccounting.pka	NIC	172.16.10.2	255.255.255.192	
		2001:DB8:CAFE:1::2/64		
managerB	NIC	172.16.10.67	255.255.255.192	
		2001:DB8:CAFE:2::3/64		
Website.pka	NIC	172.16.10.66	255.255.255.192	
		2001:DB8:CAFE:2::2/64		

Situación

Su compañía fue contratada para configurar una red pequeña para el propietario de un restaurante. Hay dos restaurantes cercanos entre sí y comparten una conexión. El equipo y el cableado están instalados, y el administrador de red diseñó el plan de implementación. Su trabajo consiste en implementar el resto del esquema de direccionamiento de acuerdo con la tabla de direccionamiento abreviada y verificar la conectividad.

Requisitos

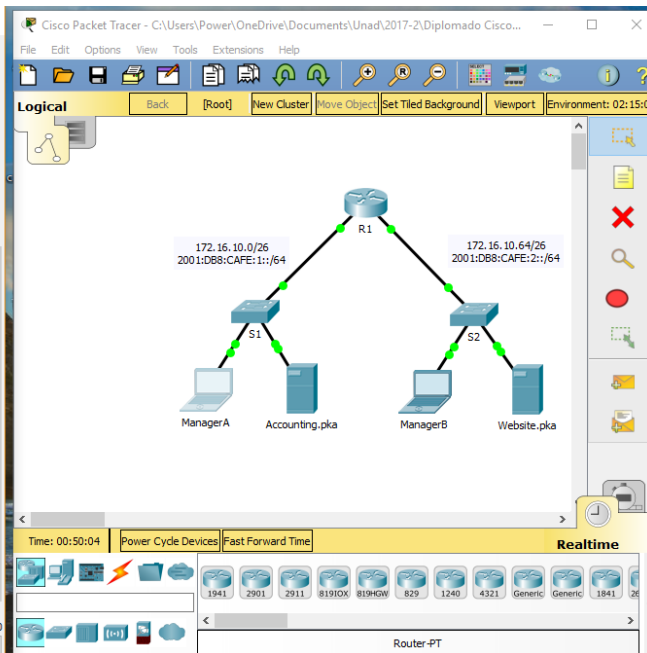
- Complete el registro de la tabla de direccionamiento.
- Configure direccionamiento IPv4 e IPv6 en el R1.
- Configure direccionamiento IPv4 en el S1. El S2 ya está configurado.
- Configure direccionamiento IPv4 e IPv6 en ManagerA. El resto de los clientes ya están configurados.
- Verifique la conectividad. Todos los clientes deben poder hacerse ping entre sí y acceder a los sitios Web en Accounting.pka y Website.pka.

Tabla de calificación sugerida

Packet Tracer tienen una puntuación de 80 puntos. Completar la tabla de direccionamiento vale 20 puntos.

Time Elapsed: 00:50:16 Completion: 80/80

Top Check Results Reset Activity



Cisco Packet Tracer - C:\Users\Power\OneDrive\Documents\Unad\2017-2\Diplomado Cisco...

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:51:37

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Score : 80/80
Item Count : 24/24

Component	Items/Total	Score
Default Gateway Configuration	3/3	15/15
Device Interface Configuration	12/12	35/35
IPv4 Host Address Configuration	6/6	19/19
IPv6 Host Address Configuration	3/3	11/11

Assessment Items

- Network
 - ManagerA
 - Default Gateway
 - Default Gateway IPv6
 - DNS Server IP
 - DNS Server IPv6
 - Ports
 - FastEthernet0
 - IP Address
 - IPv6 Addresses
 - 2001:DB8:CAFE...
 - IP Address
 - Prefix Le...
 - Subnet Mask
 - R1
 - Ports
 - GigabitEthernet0/0
 - IP Address
 - IPv6 Addresses
 - 2001:DB8:CAFE...
 - IP Address
 - Prefix Le...
 - Link Local
 - Port Status
 - Subnet Mask
 - GigabitEthernet0/1
 - IP Address
 - IPv6 Addresses
 - 2001:DB8:CAFE...
 - IP Address
 - Prefix Le...
 - Link Local
 - Port Status

Ejercicio 9.4.1.6: Situación de división en subredes 1.

Topología

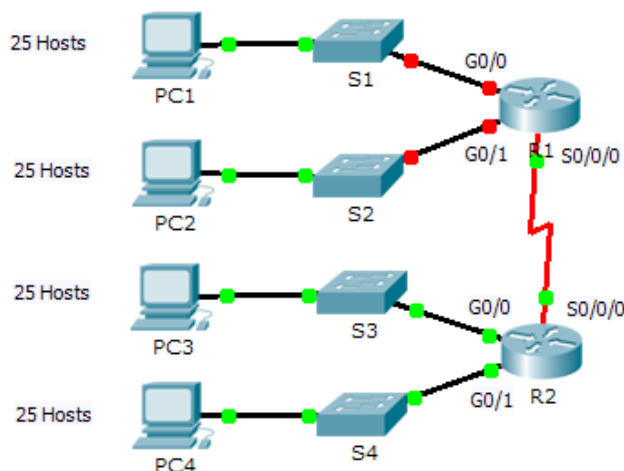


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de	Gateway predeterminad
R1	G0/0	192.168.100.1	255.255.255.22	No aplicable
	G0/1	192.168.100.33	255.255.255.22	No aplicable
	S0/0/0	192.168.100.129	255.255.255.22	No aplicable
R2	G0/0	192.168.100.65	255.255.255.22	No aplicable
	G0/1	192.168.100.97	255.255.255.22	No aplicable
	S0/0/0	192.168.100.158	255.255.255.22	No aplicable
S1	VLAN 1	192.168.100.2	255.255.255.22	192.168.100.1
S2	VLAN 1	192.168.100.34	255.255.255.22	192.168.100.33
S3	VLAN 1	192.168.100.66	255.255.255.22	192.168.100.65
S4	VLAN 1	192.168.100.98	255.255.255.22	192.168.100.97
PC1	NIC	192.168.100.30	255.255.255.22	192.168.100.1
PC2	NIC	192.168.100.62	255.255.255.22	192.168.100.33
PC3	NIC	192.168.100.94	255.255.255.22	192.168.100.65
PC4	NIC	192.168.100.126	255.255.255.22	192.168.100.97

Objetivos

Parte 1: Diseñar un esquema de direccionamiento IP

Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

Situación

En esta actividad, se le asigna la dirección de red 192.168.100.0/24 para que cree una subred y proporcione el direccionamiento IP para la red que se muestra en la topología. Cada LAN de la red necesita espacio suficiente para alojar, como mínimo, 25 direcciones para dispositivos finales, el switch y el router. La conexión entre las redes R1 y R2 requiere una dirección IP para cada extremo del enlace.

Parte 1: Diseñar un esquema de direccionamiento IP

Paso 1: Divida en subredes la red 192.168.100.0/24 en la cantidad adecuada de subredes.

- a. Según la topología, ¿cuántas subredes se necesitan?
5 subredes
- b. ¿Cuántos bits se deben tomar prestados para admitir la cantidad de subredes en la tabla de topología?
3 bit
- c. ¿Cuántas subredes se crean?
8 subredes
- e. ¿Cuántos hosts utilizables se crean por subred?
30 host

Nota: si su respuesta es menor que los 25 hosts requeridos, tomó prestados demasiados bits. e. Calcule el valor binario para las primeras cinco subredes. La primera subred ya se muestra.

Net 0: 192. 168. 100. 0 0 0 0 0 0 0 0

Net 1: 192. 168. 100. _____

Net 1: 192. 168. 100. 0 0 1 0 0 0 0 0

Net 2: 192. 168. 100. _____

Net 2: 192. 168. 100. 0 1 0 0 0 0 0 0

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Net 3: 192. 168. 100.
 Net 3: 192. 168. 100. 0 1 1 0 0 0 0 0

Net 4: 192. 168. 100.
 Net 4: 192. 168. 100. 1 0 0 0 0 0 0 0

f. Calcule el valor binario y el valor decimal de la nueva máscara de subred.

11111111.11111111.11111111.
 11111111.11111111.11111111. 1 1 1 0 0 0 0 0
 255. 255. 255.
 255. 255. 255. 224

g. Complete la **tabla de subredes** con el valor decimal de todas las subredes disponibles, la primera y la última dirección de host utilizable y la dirección de broadcast. Repita hasta que todas las direcciones estén en la lista.

Nota: es posible que no necesite utilizar todas las filas.

Tabla de subredes

Número de	Dirección de	Primera dirección de host	Última dirección de host utilizable	Dirección de
0	192.168.100.0	192.168.100.1	192.168.100.30	192.168.100.31
1	192.168.100.32	192.168.100.33	192.168.100.62	192.168.100.63
2	192.168.100.64	192.168.100.65	192.168.100.94	192.168.100.95
3	192.168.100.96	192.168.100.97	192.168.100.126	192.168.100.127
4	192.168.100.128	192.168.100.129	192.168.100.158	192.168.100.159
5	192.168.100.160	192.168.100.161	192.168.100.190	192.168.100.191
6	192.168.100.192	192.168.100.193	192.168.100.222	192.168.100.223
7	192.168.100.224	192.168.100.225	192.168.100.254	192.168.100.255
8				
9				
10				

Paso 2: Asigne las subredes a la red que se muestra en la topología.

a. Asigne la subred 0 a la LAN conectada a la interfaz GigabitEthernet 0/0 del R1:
 192.168.100.0 /27

```
R1>enable
R1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#ip address 192.168.100.1 255.255.255.224
R1(config-if)#no shut
```

b. Asigne la subred 1 a la LAN conectada a la interfaz GigabitEthernet 0/1 del R1:
 192.168.100.32 /27

```
R1(config-if)#int g0/1
R1(config-if)#ip address 192.168.100.33 255.255.255.224
R1(config-if)#no shut
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up
```

```
R1(config-if)#int s0/0/0
R1(config-if)#ip address 192.168.100.129 255.255.255.252
R1(config-if)#
```

```
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.100.158 (Serial0/0/0) is down: interface
down
```

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

c. Asigne la subred 2 a la LAN conectada a la interfaz GigabitEthernet 0/0 del R2:
 192.168.100.64 /27

d. Asigne la subred 3 a la LAN conectada a la interfaz GigabitEthernet 0/1 del R2:
 192.168.100.96 /27

e. Asigne la subred 4 al enlace WAN entre el R1 y el R2:
 192.168.100.128 /27

Paso 3: Documente el esquema de direccionamiento.

Complete la **tabla de direccionamiento** con las siguientes pautas:

- a. Asigne las primeras direcciones IP utilizables al R1 para los dos enlaces LAN y el enlace WAN.
ok

b. Asigne las primeras direcciones IP utilizables al R2 para los enlaces LAN. Asigne la última dirección IP

— utilizable para el enlace WAN.

ok

d. Asigne las segundas direcciones IP utilizables a los switches.

Al switch 3

S3>enable

S3#configure t

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

S3(config)#int vlan 1

S3(config-if)#ip address 192.168.100.66 255.255.255.224

S3(config-if)#no shut

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

e. Asigne las últimas direcciones IP utilizables a los hosts.

Ok

Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para realizar la configuración de direccionamiento.

Paso 1: Configurar el direccionamiento IP en las interfaces LAN del R1

Ok

Paso 2: Configure el direccionamiento IP en S3, incluido el gateway predeterminado.

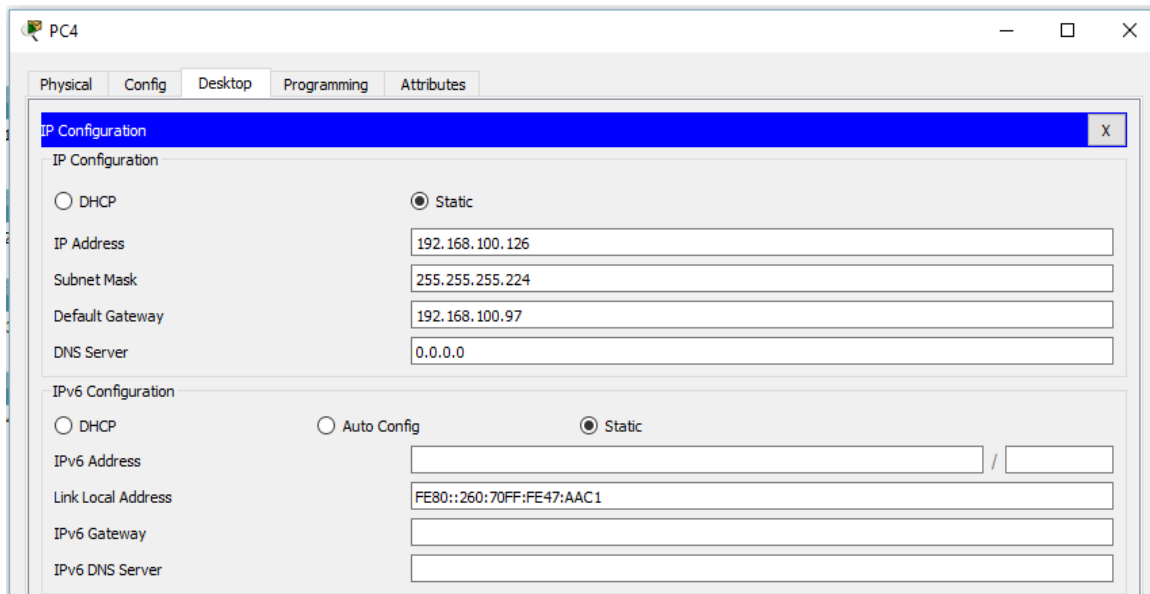
S3(config)#ip default-gateway

% Incomplete command.

S3(config)#ip default-gateway 192.168.100.65

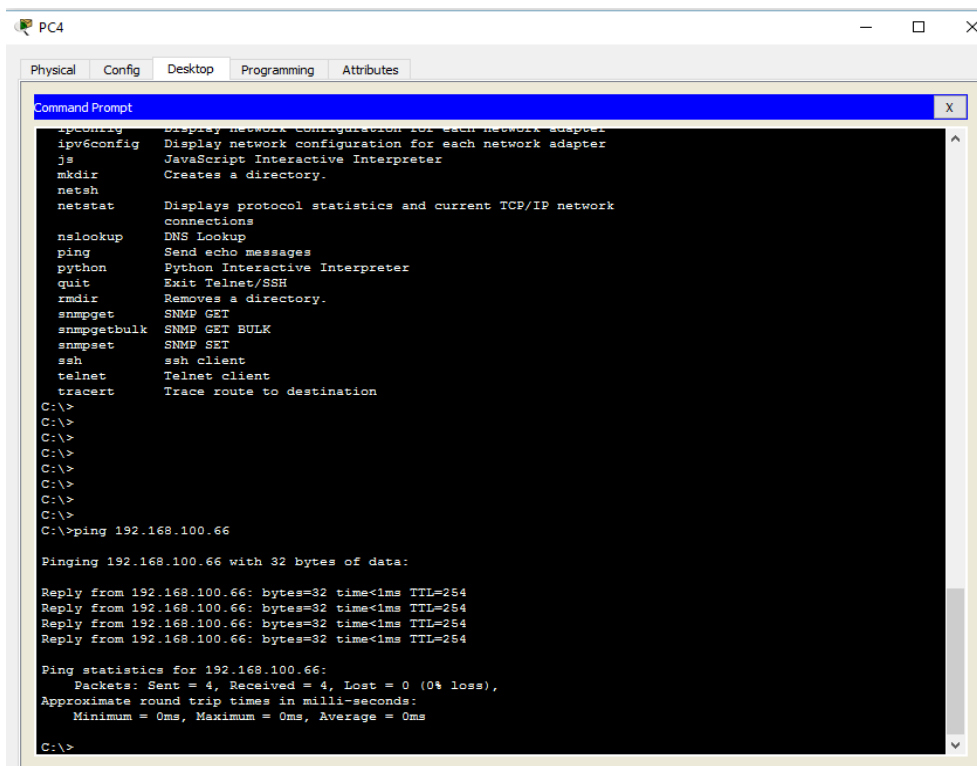
S3(config)#

Paso 3: Configure el direccionamiento IP en PC4, incluido el gateway predeterminado.



Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde el R1, el S3 y la PC4. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.



Ejercicio 9.1.4.7: Situación de división en subredes 2.

Topología

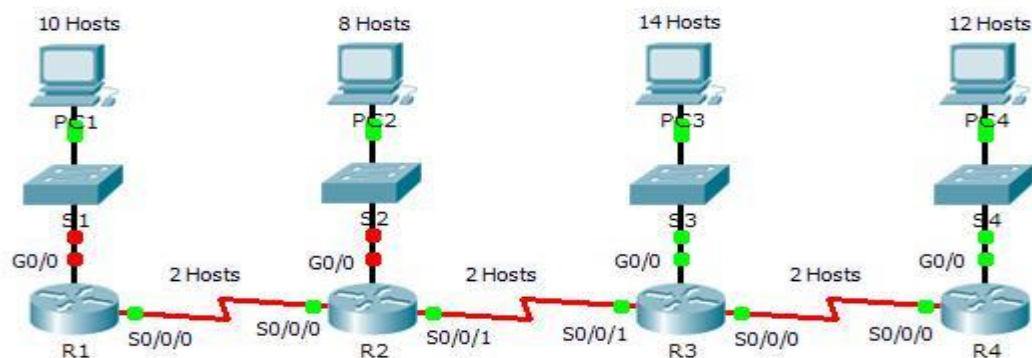


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.31.1.1	255.255.255.240	No aplicable
	S0/0/0	172.31.1.65	255.255.255.240	No aplicable
R2	G0/0	172.31.1.17	255.255.255.240	No aplicable
	S0/0/0	172.31.1.78	255.255.255.240	No aplicable
	S0/0/1	172.31.1.81	255.255.255.240	No aplicable
R3	G0/0	172.31.1.33	255.255.255.240	No aplicable
	S0/0/0	172.31.1.97	255.255.255.240	No aplicable
	S0/0/1	172.31.1.94	255.255.255.240	No aplicable
R4	G0/0	172.31.1.49	255.255.255.240	No aplicable
	S0/0/0	172.31.1.110	255.255.255.240	No aplicable
S1	VLAN 1	172.31.1.2	255.255.255.240	172.31.1.1
S2	VLAN 1	172.31.1.18	255.255.255.240	172.31.1.17
S3	VLAN 1	172.31.1.34	255.255.255.240	172.31.1.33
S4	VLAN 1	172.31.1.50	255.255.255.240	172.31.1.49
PC1	NIC	172.31.1.14	255.255.255.240	172.31.1.1

		172.31.1.30	255.255.255.240	172.31.1.17
PC3	NIC	172.31.1.46	255.255.255.240	172.31.1.33
PC4	NIC	172.31.1.62	255.255.255.240	172.31.1.49

Objetivos

Parte 1: Diseñar un esquema de direccionamiento IP

Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

Situación

En esta actividad, se le asigna la dirección de red 172.31.1.0 /24 para que la divida en subredes y proporcione direccionamiento IP para la red que se muestra en la topología. Las direcciones de host requeridas para cada enlace WAN y LAN se muestran en la topología.

Parte 1: Diseñar un esquema de direccionamiento IP

Paso 1: Divida la red 172.31.1.0/24 en subredes de acuerdo con la cantidad máxima de hosts que requiere la subred más extensa.

- Según la topología, ¿cuántas subredes se necesitan?
R: 7
- ¿Cuántos bits se deben tomar prestados para admitir la cantidad de subredes en la tabla de topología?
R: 4
- ¿Cuántas subredes se crean?
R: 16
- ¿Cuántas direcciones de host utilizables se crean por subred?
R: 14
- Nota:** si su respuesta es menor que el máximo de 14 hosts que requiere la LAN del R3, tomó prestados demasiados bits.
- Calcule el valor binario para las primeras cinco subredes. La subred cero ya se muestra.

Net 0: 172 . 31 . 1 . 0 0 0 0 0 0 0 0

Net 1: 172 . 31 . 1 . _____

Net 1: 172 . 31 . 1 . 0 0 0 1 0 0 0 0

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Net 2: 172 . 31 . 1 . _____
 Net 2: 172 . 31 . 1 . 0 0 1 0 0 0 0 0

Net 3: 172 . 31 . 1 . _____
 Net 3: 172 . 31 . 1 . 0 0 1 1 0 0 0 0

Net 4: 172 . 31 . 1 . _____
 Net 4: 172 . 31 . 1 . 0 1 0 0 0 0 0 0

k. Calcule el valor binario y el valor decimal de la nueva máscara de subred.

11111111.11111111.11111111. _____
 11111111.11111111.11111111. 1 1 1 1 0 0 0 0
 255 . 255 . 255 . _____
 255 . 255 . 255 . 240

g. Complete la **tabla de subredes** con todas las subredes disponibles, la primera y la última dirección de host utilizable y la dirección de broadcast. La primera subred ya se completó. Repita hasta que todas las direcciones estén en la lista.

Nota: es posible que no necesite utilizar todas las filas

Tabla de subredes

Número de subred	IP de subred	Primera IP de host utilizable	Última IP de host utilizable	Dirección de broadcast
0	172.31.1.0	172.31.1.1	172.31.1.14	172.16.1.15
1	172.31.1.16	172.31.1.17	172.31.1.30	172.31.1.31
2	172.31.1.32	172.31.1.33	172.31.1.46	172.31.1.47
3	172.31.1.48	172.31.1.49	172.31.1.62	172.31.1.63
4	172.31.1.64	172.31.1.65	172.31.1.78	172.31.1.79
5	172.31.1.80	172.31.1.81	172.31.1.94	172.31.1.95
6	172.31.1.96	172.31.1.97	172.31.1.110	172.31.1.111
7	172.31.1.112	172.31.1.113	172.31.1.126	172.31.1.127
8	172.31.1.128	172.31.1.129	172.31.1.142	172.31.1.143
9	172.31.1.144	172.31.1.145	172.31.1.158	172.31.1.159

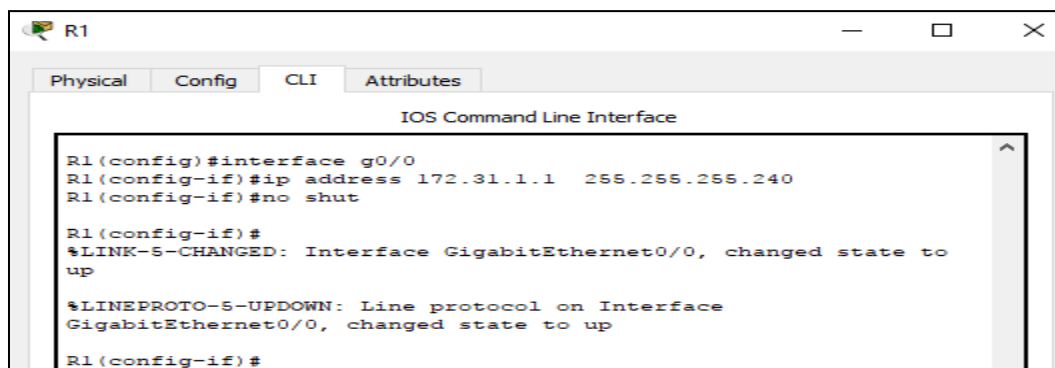
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

10	172.31.1.160	172.31.1.161	172.31.1.174	172.31.1.175
11	172.31.1.176	172.31.1.177	172.31.1.190	172.31.1.191
12	172.31.1.192	172.31.1.193	172.31.1.206	172.31.1.207
13	172.31.1.208	172.31.1.209	172.31.1.222	172.31.1.223
14	172.31.1.224	172.31.1.225	172.31.1.238	172.31.1.239
15	172.31.1.240	172.31.1.241	172.31.1.254	172.31.1.255

Paso 2: Asigne las subredes a la red que se muestra en la topología.

Cuando asigne las subredes, tenga en cuenta que es necesario el enrutamiento para permitir que la información se envíe a través de la red.

f. Asigne la subred 0 a la LAN del R1:



```

R1
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

R1(config)#interface g0/0
R1(config-if)#ip address 172.31.1.1 255.255.255.240
R1(config-if)#no shut

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

g. Asigne la subred 1 a la LAN del R2:

```

R2>enable
R2#configure termi
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface g0/0
R2(config-if)#ip address 172.31.1.17 255.255.255.240
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to
up
R2(config-if)#
  
```

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
 Código del curso 203092 – Diplomado de Profundización Cisco
 Paso 3 – Actividad Colaborativa 2

h. Asigne la subred 2 a la LAN del R3
 Ya ha sido asignada

i. Asigne la subred 3 a la LAN del R4:
 Ya ha sido asignada

j. Asigne la subred 4 al enlace entre el R1 y el R2:
 Ya ha sido asignada

```
R1>enable
R1#show run
Building configuration...

hostname R1
!
interface Serial0/0/0
ip address 172.31.1.65 255.255.255.240
clock rate 64000
!
end
```

R1#

k. Asigne la subred 5 al enlace entre el R2 y el R3:
 Ya ha sido asignada

```
R2>enable
R2#show run
Building configuration...
interface Serial0/0/1
ip address 172.31.1.81 255.255.255.240
clock rate 2000000
!
end
```

R2#

l. Asigne la subred 6 al enlace entre el R3 y el R4:
 Ya ha sido asignada

Paso 3: Documente el esquema de direccionamiento.

Complete la **tabla de direccionamiento** con las siguientes pautas:

- f. Asigne las primeras direcciones IP utilizables a los routers para cada uno de los enlaces LAN.
- g. Utilice el siguiente método para asignar las direcciones IP de los enlaces WAN:

Para el enlace WAN entre el R1 y el R2, asigne la primera dirección IP utilizable al R1 y la última dirección IP utilizable al R2.

Ya ha sido asignada

Para el enlace WAN entre el R2 y el R3, asigne la primera dirección IP utilizable al R2 y la última dirección IP utilizable al R3.

Ya ha sido asignada

Para el enlace WAN entre el R3 y el R4, asigne la primera dirección IP utilizable al R3 y la última dirección IP utilizable al R4.

Ya ha sido asignada

- g. Asigne las segundas direcciones IP utilizables a los switches.

```
S3>enable
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface vlan 1
S3(config-if)#ip address 172.31.1.34 255.255.255.240
S3(config-if)#no shut

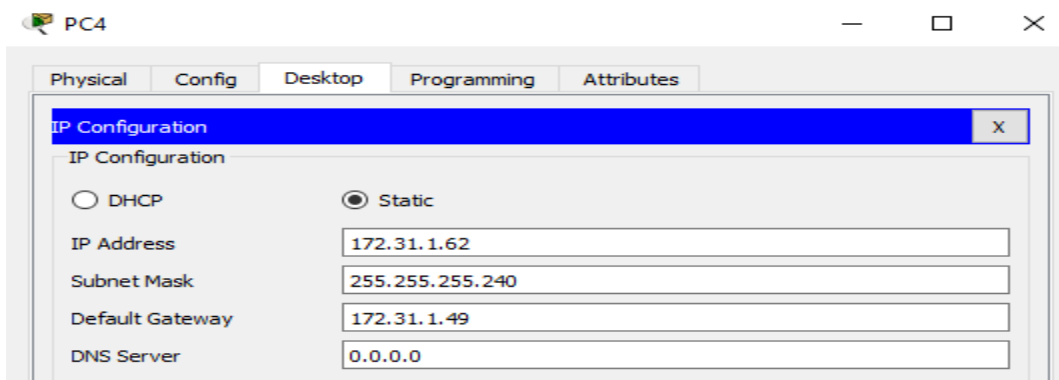
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

S3(config-if)#

Los demás switches ya han sido configurados

h. Asigne las últimas direcciones IP utilizables a los hosts.



Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para realizar la configuración de direccionamiento.

Paso 1: Configurar el direccionamiento IP en las interfaces LAN del R1 y el R2

```
R1#show run
Building configuration...

Current configuration : 797 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
interface GigabitEthernet0/0
ip address 172.31.1.1 255.255.255.240
duplex auto
speed auto
!
interface Serial0/0/0
ip address 172.31.1.65 255.255.255.240
clock rate 64000
!
end
```

R1#

```
R2>enable
R2#show run
Building configuration...

Current configuration : 805 bytes
!
!
interface GigabitEthernet0/0
ip address 172.31.1.17 255.255.255.240
duplex auto
speed auto
!
interface Serial0/0/0
ip address 172.31.1.78 255.255.255.240
!
interface Serial0/0/1
ip address 172.31.1.81 255.255.255.240
clock rate 2000000
!
!
end
```

R2#

Paso 2: Configure el direccionamiento IP en S3, incluido el gateway predeterminado.

```
S3#show run
Building configuration...

Current configuration : 1120 bytes
!
hostname S3
!
!
interface Vlan1
ip address 172.31.1.34 255.255.255.240
!
```

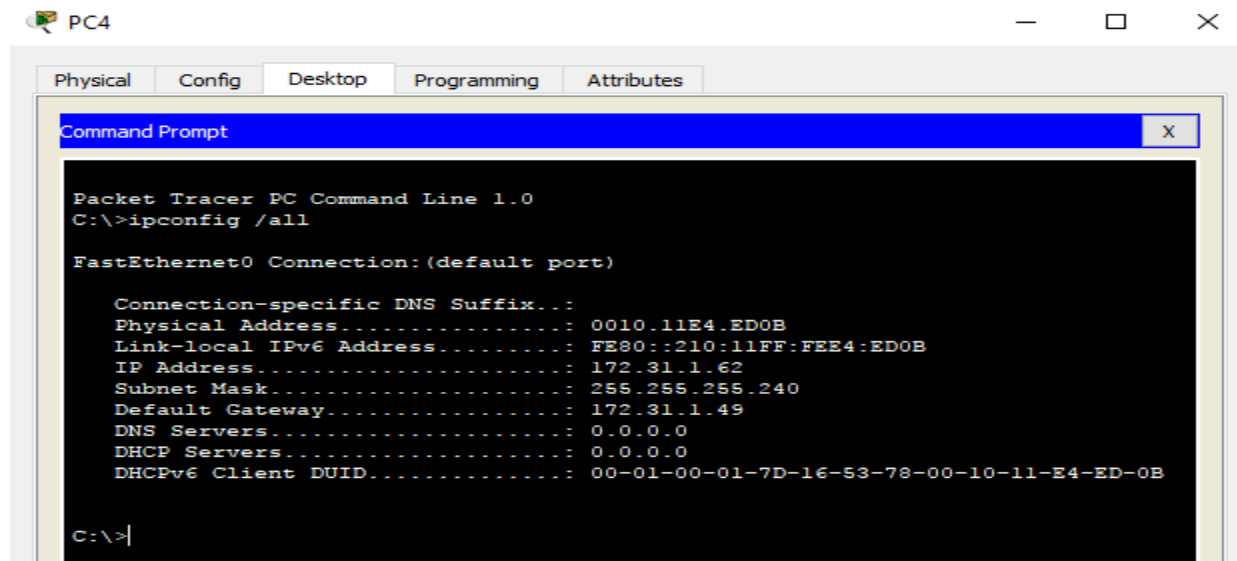
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

```
ip default-gateway 172.31.1.33
!
```

```
end
```

```
S3#
```

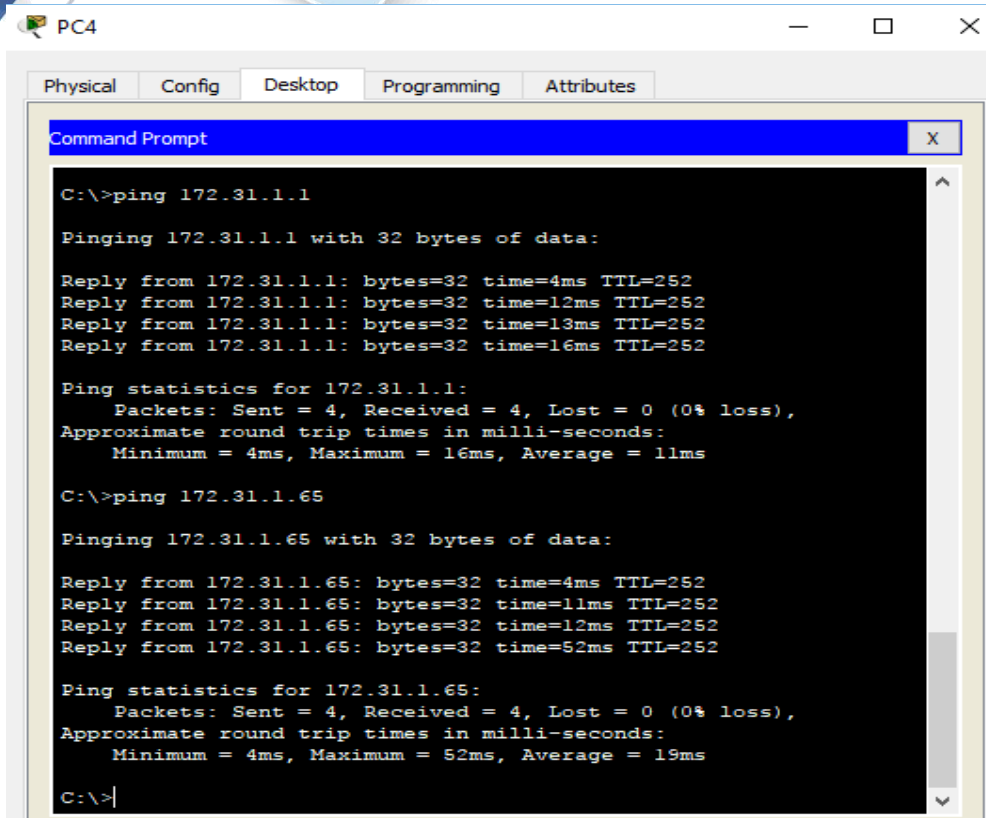
Paso 3: Configure el direccionamiento IP en PC4, incluido el gateway predeterminado.



Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde el R1, el R2, el S3 y la PC4. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.

Ping desde el PC4 a R1



```

PC4
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.31.1.1

Pinging 172.31.1.1 with 32 bytes of data:

Reply from 172.31.1.1: bytes=32 time=4ms TTL=252
Reply from 172.31.1.1: bytes=32 time=12ms TTL=252
Reply from 172.31.1.1: bytes=32 time=13ms TTL=252
Reply from 172.31.1.1: bytes=32 time=16ms TTL=252

Ping statistics for 172.31.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 16ms, Average = 11ms

C:\>ping 172.31.1.65

Pinging 172.31.1.65 with 32 bytes of data:

Reply from 172.31.1.65: bytes=32 time=4ms TTL=252
Reply from 172.31.1.65: bytes=32 time=11ms TTL=252
Reply from 172.31.1.65: bytes=32 time=12ms TTL=252
Reply from 172.31.1.65: bytes=32 time=52ms TTL=252

Ping statistics for 172.31.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 52ms, Average = 19ms

C:\>|
  
```

Ping desde el PC4 a R2

```

C:\>ping 172.31.1.17

Pinging 172.31.1.17 with 32 bytes of data:

Reply from 172.31.1.17: bytes=32 time=2ms TTL=253
Reply from 172.31.1.17: bytes=32 time=12ms TTL=253
Reply from 172.31.1.17: bytes=32 time=10ms TTL=253
Reply from 172.31.1.17: bytes=32 time=13ms TTL=253

Ping statistics for 172.31.1.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 13ms, Average = 9ms

C:\>ping 172.31.1.78

Pinging 172.31.1.78 with 32 bytes of data:

Reply from 172.31.1.78: bytes=32 time=3ms TTL=253
  
```

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

```
Reply from 172.31.1.78: bytes=32 time=19ms TTL=253
Reply from 172.31.1.78: bytes=32 time=11ms TTL=253
Reply from 172.31.1.78: bytes=32 time=13ms TTL=253
```

Ping statistics for 172.31.1.78:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 19ms, Average = 11ms

```
C:\>ping 172.31.1.81
```

Pinging 172.31.1.81 with 32 bytes of data:

```
Reply from 172.31.1.81: bytes=32 time=3ms TTL=253
Reply from 172.31.1.81: bytes=32 time=12ms TTL=253
Reply from 172.31.1.81: bytes=32 time=13ms TTL=253
Reply from 172.31.1.81: bytes=32 time=12ms TTL=253
```

Ping statistics for 172.31.1.81:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 13ms, Average = 10ms

```
C:\>
```

Ping desde el PC4 a R2

```
C:\>ping 172.31.1.33
```

Pinging 172.31.1.33 with 32 bytes of data:

```
Reply from 172.31.1.33: bytes=32 time=2ms TTL=254
Reply from 172.31.1.33: bytes=32 time=1ms TTL=254
Reply from 172.31.1.33: bytes=32 time=10ms TTL=254
Reply from 172.31.1.33: bytes=32 time=1ms TTL=254
```

Ping statistics for 172.31.1.33:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 10ms, Average = 3ms

```
C:\>ping 172.31.1.97
```

Pinging 172.31.1.97 with 32 bytes of data:

```
Reply from 172.31.1.97: bytes=32 time=1ms TTL=254
Reply from 172.31.1.97: bytes=32 time=1ms TTL=254
Reply from 172.31.1.97: bytes=32 time=1ms TTL=254
Reply from 172.31.1.97: bytes=32 time=1ms TTL=254
```

Ping statistics for 172.31.1.97:

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

C:\>ping 172.31.1.94

Pinging 172.31.1.94 with 32 bytes of data:

```
Reply from 172.31.1.94: bytes=32 time=1ms TTL=254
Reply from 172.31.1.94: bytes=32 time=4ms TTL=254
Reply from 172.31.1.94: bytes=32 time=2ms TTL=254
Reply from 172.31.1.94: bytes=32 time=2ms TTL=254
```

Ping statistics for 172.31.1.94:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\>

Ping PC4 a S1

C:\>ping 172.31.1.2

Pinging 172.31.1.2 with 32 bytes of data:

```
Reply from 172.31.1.2: bytes=32 time=3ms TTL=251
Reply from 172.31.1.2: bytes=32 time=16ms TTL=251
Reply from 172.31.1.2: bytes=32 time=14ms TTL=251
Reply from 172.31.1.2: bytes=32 time=15ms TTL=251
```

Ping statistics for 172.31.1.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 3ms, Maximum = 16ms, Average = 12ms

C:\>

Ping PC4 a S2

```
C:\>ping 172.31.1.18

Pinging 172.31.1.18 with 32 bytes of data:

Reply from 172.31.1.18: bytes=32 time=3ms TTL=252
Reply from 172.31.1.18: bytes=32 time=13ms TTL=252
Reply from 172.31.1.18: bytes=32 time=16ms TTL=252
Reply from 172.31.1.18: bytes=32 time=13ms TTL=252

Ping statistics for 172.31.1.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 16ms, Average = 11ms
C:\>
```

Ping PC4 a S3

```
C:\>ping 172.31.1.34

Pinging 172.31.1.34 with 32 bytes of data:

Reply from 172.31.1.34: bytes=32 time=2ms TTL=253
Reply from 172.31.1.34: bytes=32 time=13ms TTL=253
Reply from 172.31.1.34: bytes=32 time=10ms TTL=253
Reply from 172.31.1.34: bytes=32 time=13ms TTL=253

Ping statistics for 172.31.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 13ms, Average = 9ms
C:\>
```

Ping PC4 a PC1, PC2 y PC3

```
C:\>ping 172.31.1.14

Pinging 172.31.1.14 with 32 bytes of data:

Reply from 172.31.1.14: bytes=32 time=4ms TTL=124
Reply from 172.31.1.14: bytes=32 time=15ms TTL=124
Reply from 172.31.1.14: bytes=32 time=22ms TTL=124
```


ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Reply from 172.31.1.14: bytes=32 time=17ms TTL=124

Ping statistics for 172.31.1.14:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 4ms, Maximum = 22ms, Average = 14ms

C:\>ping 172.31.1.30

Pinging 172.31.1.30 with 32 bytes of data:

Reply from 172.31.1.30: bytes=32 time=2ms TTL=125

Reply from 172.31.1.30: bytes=32 time=13ms TTL=125

Reply from 172.31.1.30: bytes=32 time=12ms TTL=125

Reply from 172.31.1.30: bytes=32 time=12ms TTL=125

Ping statistics for 172.31.1.30:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 13ms, Average = 9ms

C:\>ping 172.31.1.46

Pinging 172.31.1.46 with 32 bytes of data:

Reply from 172.31.1.46: bytes=32 time=2ms TTL=126

Reply from 172.31.1.46: bytes=32 time=11ms TTL=126

Reply from 172.31.1.46: bytes=32 time=14ms TTL=126

Reply from 172.31.1.46: bytes=32 time=21ms TTL=126

Ping statistics for 172.31.1.46:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 21ms, Average = 12ms

C:\>

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Ítems Resueltos

Cisco Packet Tracer - D:\UNAD\CISCO\Trabajo Colaborativo No 2\CCNA1 R&S UNIDAD 2\9.1.4.7 Packet Tracer - Subnetting Scenario 2.pka

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 02:25:39

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
PC4				
Default Gateway	Correct	2	Default Gatew...	
Ports				
FastEthernet0				
IP Addre...	Correct	2	IPv4 Host Add...	
Subnet ...	Correct	2	IPv4 Subnet M...	
R1				
Ports				
GigabitEthernet...				
IP Addre...	Correct	3	IPv4 Host Add...	
Port Stat...	Correct	1	Device Interfa...	
Subnet ...	Correct	3	IPv4 Subnet M...	
R2				
Ports				
GigabitEthernet...				
IP Addre...	Correct	3	IPv4 Host Add...	
Port Stat...	Correct	1	Device Interfa...	
Subnet ...	Correct	3	IPv4 Subnet M...	
S3				
Default Gateway	Correct	3	Default Gatew...	
Ports				
Vlan1				
IP Addre...	Correct	3	IPv4 Host Add...	
Port Stat...	Correct	1	Device Interfa...	
Subnet ...	Correct	3	IPv4 Subnet M...	

Score : 30/30
Item Count : 13/13

Component	Items/Total	Score
Default Gateway Configuration	2/2	5/5
Device Interface Configuration	3/3	3/3
IPv4 Host Address Calculation	4/4	11/11
IPv4 Subnet Mask Calculation	4/4	11/11

Ejercicio 9.2.1.5: Diseño e implementación de un esquema de direccionamiento VSLM

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
[[R1Name]]	G0/0	[[R1G0Add]]	[[R1G0Sub]]	No aplicable
	G0/1	[[R1G1Add]]	[[R1G1Sub]]	No aplicable
	S0/0/0	[[R1S0Add]]	[[R1S0Sub]]	No aplicable
[[R2Name]]	G0/0	[[R2G0Add]]	[[R2G0Sub]]	No aplicable
	G0/1	[[R2G1Add]]	[[R2G1Sub]]	No aplicable
	S0/0/0	[[R2S0Add]]	[[R2S0Sub]]	No aplicable
[[S1Name]]	VLAN 1	[[S1Add]]	[[S1Sub]]	[[R1G0Add]]
[[S2Name]]	VLAN 1	[[S2Add]]	[[S2Sub]]	[[R1G1Add]]
[[S3Name]]	VLAN 1	[[S3Add]]	[[S3Sub]]	[[R2G0Add]]
[[S4Name]]	VLAN 1	[[S4Add]]	[[S4Sub]]	[[R2G1Add]]
[[PC1Name]]	NIC	[[PC1Add]]	[[PC1Sub]]	[[R1G0Add]]
[[PC2Name]]	NIC	[[PC2Add]]	[[PC2Sub]]	[[R1G1Add]]
[[PC3Name]]	NIC	[[PC3Add]]	[[PC3Sub]]	[[R2G0Add]]
[[PC4Name]]	NIC	[[PC4Add]]	[[PC4Sub]]	[[R2G1Add]]

Objetivos

Parte 1: Examinar los requisitos de la red

Parte 2: Diseñar el esquema de direccionamiento VLSM

Parte 3: Asignar direcciones IP a los dispositivos y verificar la conectividad

Información básica

En esta actividad, se le proporciona una dirección de red /24 para diseñar un esquema de direccionamiento VLSM. Sobre la base de un conjunto de requisitos, asignará subredes y direccionamiento, configurará los dispositivos y verificará la conectividad.

Parte 1: Examinar los requisitos de la red

Paso 1: Determinar la cantidad de subredes necesarias

Dividirá la dirección de red `[[DisplayNet]]` en subredes. La red tiene los siguientes requisitos:

- La LAN de **Room-114** requerirá **27** direcciones IP de host.
- La LAN de **Room-279** requerirá **25** direcciones IP de host.
- La LAN de **Room-312** requerirá **14** direcciones IP de host.
- La LAN de **Room-407** requerirá **8** direcciones IP de host.

¿Cuántas subredes se necesitan en la topología de la red?

R: 5

Paso 2: Determinar la información de máscara de subred para cada subred a. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **Room-114**?

¿Cuántas direcciones de host utilizables admitirá esta subred?

b. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **Room-279**?

¿Cuántas direcciones de host utilizables admitirá esta subred?

c. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **Room-312**?

¿Cuántas direcciones de host utilizables admitirá esta subred?

d. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **Room-407**?

¿Cuántas direcciones de host utilizables admitirá esta subred?

e. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para la conexión entre **Branch1** y **Branch2**?

Parte 2: Diseñar el esquema de direccionamiento VLSM

Paso 1: Dividir la red `172.31.103.0/24` según la cantidad de hosts por subred

- a. Use la primera subred para la LAN más extensa.
- b. Use la segunda subred para la segunda LAN más extensa.
- c. Use la tercera subred para la tercera LAN más extensa.
- d. Use la cuarta subred para la cuarta LAN más extensa.
- e. Use la quinta subred para admitir la conexión entre **Branch1** y **Branch2**.

Paso 2: Registrar las subredes VLSM

Complete la **tabla de subredes** con las descripciones de las subred (p. ej., LAN de Room-114), la cantidad de hosts necesarios, la dirección de red para la subred, la primera dirección de host utilizable y la dirección de broadcast. Repita hasta que todas las direcciones estén en la lista.

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Dirección de broadcast

Paso 3: Documente el esquema de direccionamiento.

- Asigne las primeras direcciones IP utilizables a **Branch1** para los dos enlaces LAN y el enlace WAN.
- Asigne las primeras direcciones IP utilizables a **Branch2** para los dos enlaces LAN. Asigne la última dirección IP utilizable para el enlace WAN.
- Asigne las segundas direcciones IP utilizables a los switches.
- Asigne las últimas direcciones IP utilizables a los hosts.

Parte 3: Asignar direcciones IP a los dispositivos y verificar la conectividad

La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para realizar la configuración de direccionamiento.

Paso 1: Configurar el direccionamiento IP en las interfaces LAN de [[R1Name]]

The screenshot shows a network diagram in Packet Tracer with two routers, Branch1 and Branch2. Branch1 is connected to PC-A (Room-101, 27 Hosts) and PC-B (Room-279, 25 Hosts). Branch2 is connected to PC-C (Room-302, 14 Hosts) and PC-D (Room-407, 8 Hosts). A WAN link connects Branch1 and Branch2. The network address 172.31.103.0/24 is shown. Overlaid on the diagram is the CLI window for Branch1, showing the following configuration commands:

```

Branch1#enable
Branch1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Branch1(config)#int g0/0
Branch1(config-if)#172.31.103.1 255.255.255.224
Branch1(config-if)#no sh

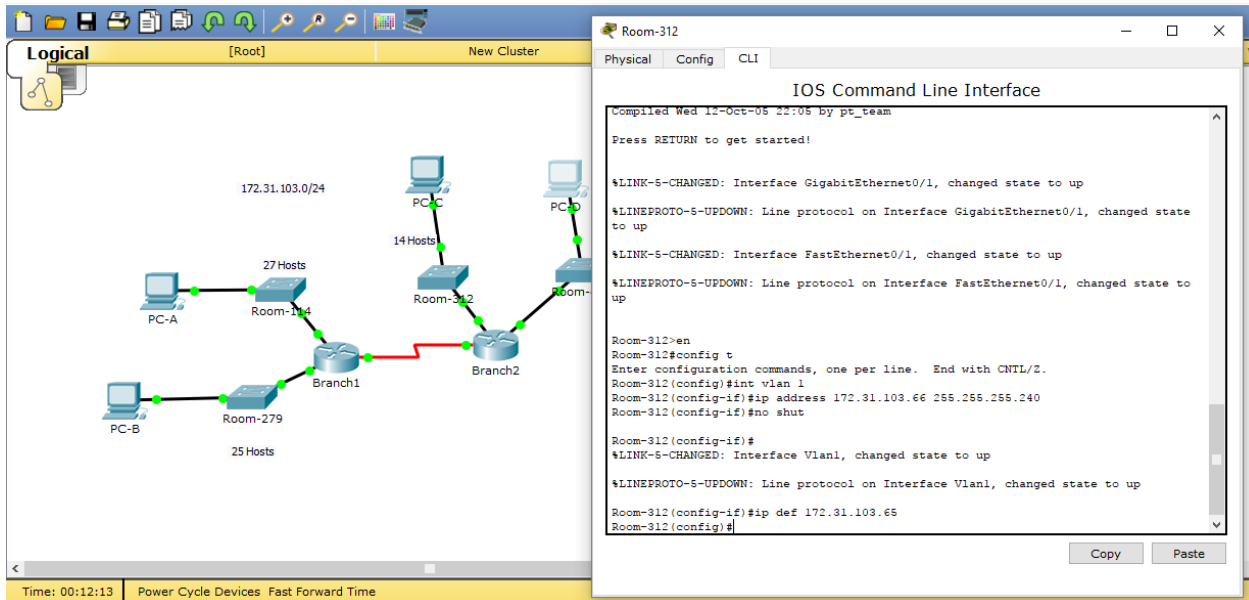
Branch1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Branch1(config-if)#int g0/1
Branch1(config-if)#ip address 172.31.103.33 255.255.255.224
Branch1(config-if)#no sh

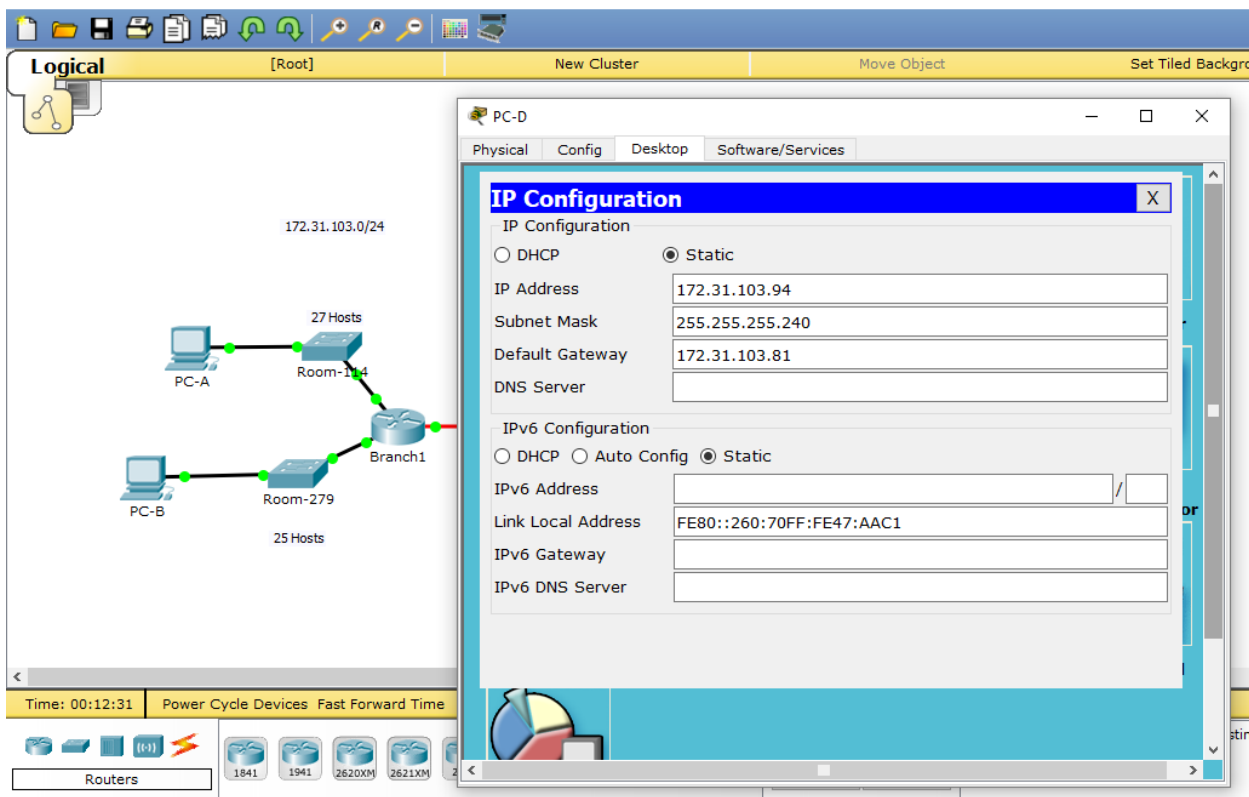
Branch1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Branch1(config-if)#
  
```

Paso 2: Configurar el direccionamiento IP en [[S3Name]], incluido el gateway predeterminado

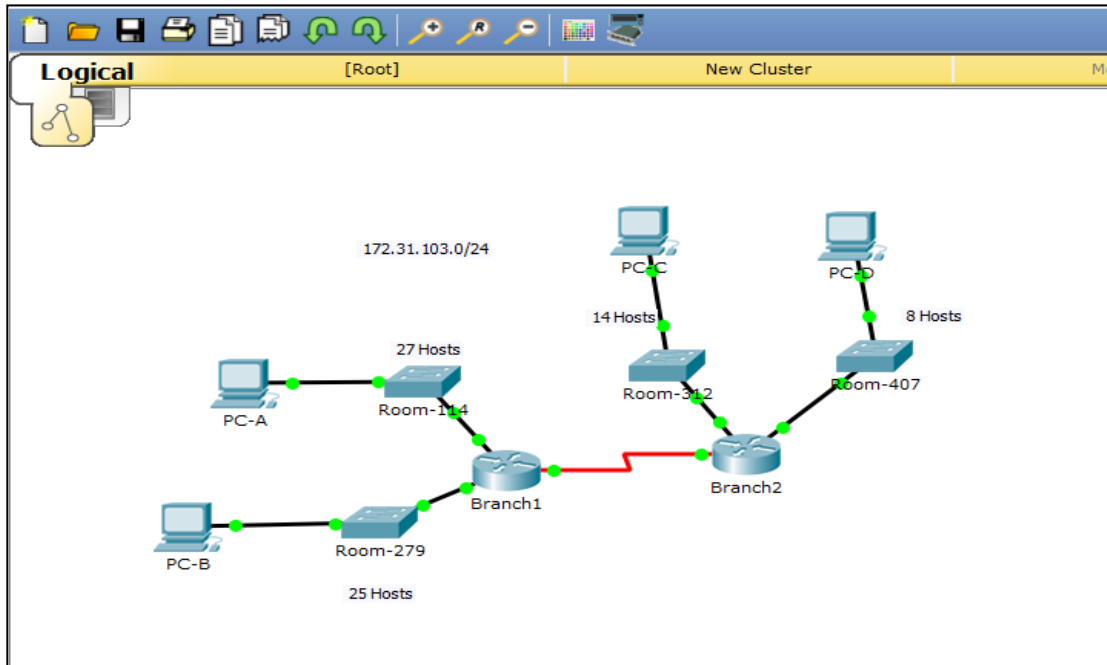


Paso 3: Configurar el direccionamiento IP en [[PC4Name]], incluido el gateway predeterminado



Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde [[R1Name]], [[S3Name]] y [[PC4Name]]. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.



Cisco Packet Tracer Student - C:\Users\Ladino\Desktop\DIPLOMADO CISCO\ACTIVIDAD 2\CCNA1 R&S UNIDAD 2\9.2.1.5 Packet Tracer - Designing and Implementing a VLSM Addressing Scheme.pka

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 00:13:09

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Congratulations! You successfully completed the **Packet Tracer - Designing and Implementing a VLSM Addressing Scheme** activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.

Click **Reset Activity** to generate a new scenario.

Close

Ejercicio 9.3.1.4: Implementación de un esquema de direccionamiento IPv6 dividido en subredes

Topología

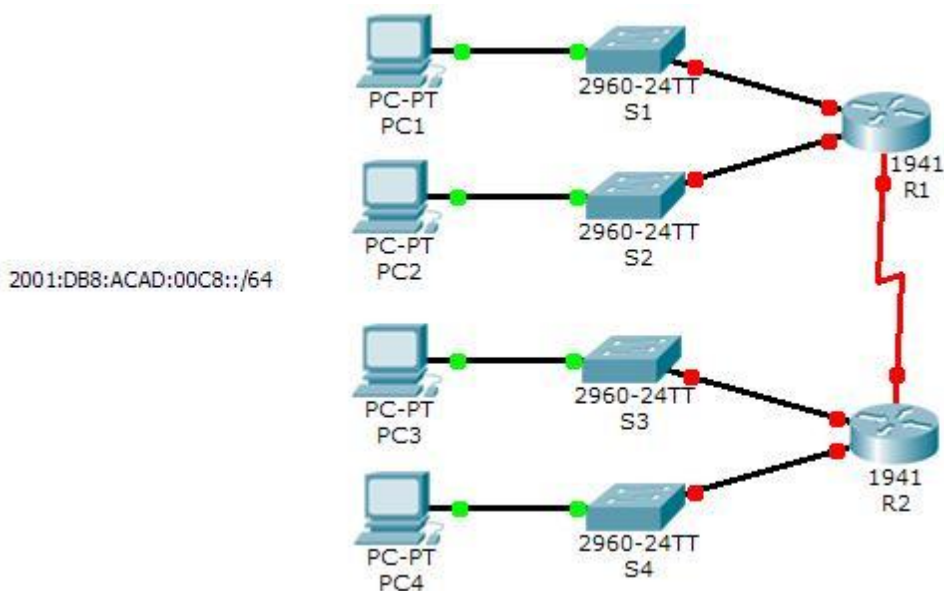


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Link-Local
R1	G0/0	2001:DB:ACAD:00C8::1/64	FE80::1
	G0/1	2001:DB:ACAD:00C9::1/64	FE80::1
	S0/0/0	2001:DB:ACAD:00CC::1/64	FE80::1
R2	G0/0	2001:DB:ACAD:00CA::1/64	FE80::2
	G0/1	2001:DB:ACAD:00CB::1/64	FE80::2
	S0/0/0	2001:DB:ACAD:00CC::2/64	FE80::2
PC1	NIC	Configuración automática	
PC2	NIC	Configuración automática	
PC3	NIC	Configuración automática	
PC4	NIC	Configuración automática	

Objetivos

Parte 1: Determinar las subredes y el esquema de direccionamiento IPv6

Parte 2: Configurar el direccionamiento IPv6 en los routers y las PC, y verificar la conectividad

Situación

El administrador de red desea que asigne cinco subredes IPv6 /64 a la red que se muestra en la topología. Su tarea consiste determinar las subredes IPv6, asignar direcciones IPv6 a los routers y configurar las PC para que reciban automáticamente el direccionamiento IPv6. El último paso es verificar la conectividad entre los hosts IPv6.

Parte 1: Determinar las subredes y el esquema de direccionamiento IPv6

Paso 1: Determinar la cantidad de subredes necesarias

Comience con la subred IPv6 2001:DB:ACAD:00C8::/64 y asígnela a la LAN del R1 conectada

a GigabitEthernet 0/0, como se muestra en la **tabla de subredes**. Para el resto de las subredes IPv6, incremente la dirección de la subred 2001:DB:ACAD:00C8::/64 de a 1 y complete la **tabla de subredes** con las direcciones de la subred IPv6.

Tabla de subredes

Descripción de la subred	Dirección de subred
R1 G0/0 LAN	2001:DB:ACAD:00C8::0/64
R1 G0/1 LAN	2001:DB:ACAD:00C9::0/64
R2 G0/0 LAN	2001:DB:ACAD:00CA::0/64
R2 G0/1 LAN	2001:DB:ACAD:00CB::0/64
Enlace WAN	2001:DB:ACAD:00CC::0/64

Paso 2: Asignar el direccionamiento IPv6 a los routers

- Asigne las primeras direcciones IPv6 al R1 para los dos enlaces LAN y el enlace WAN.
- Asigne las primeras direcciones IPv6 al R2 para las dos LAN. Asigne la segunda dirección IPv6 para el enlace WAN.
- Registre el esquema de direccionamiento IPv6 en la **tabla de direccionamiento**.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

```
Press RETURN to get started!
```

```
R1>enable
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:00C8::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

R1(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
```

```
R1(config-if)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:00C9::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
```

```
R1(config-if)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:00CC::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

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

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface gigabitethernet 0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:00CA::1/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

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

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
 Código del curso 203092 – Diplomado de Profundización Cisco
 Paso 3 – Actividad Colaborativa 2

```
R2(config-if)#interface gigabitethernet 0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:00CB::1/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
```

```
R2(config-if)#interface serial 0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:00CC::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

Parte 2: Configurar el direccionamiento IPv6 en los routers y las PC, y verificar la conectividad

Paso 1: Configurar el direccionamiento IPv6 en los routers

Nota: esta red ya está configurada con algunos comandos de IPv6 que se abordan en un curso posterior. En este punto de sus estudios, solo necesita saber cómo configurar la dirección IPv6 en una interfaz. Configure el R1 y el R2 con las direcciones IPv6 que especificó en la **tabla de direccionamiento** y active las interfaces.

```
Router(config-if)# ipv6 address ipv6-address/prefix
```

```
Router(config-if)# ipv6 address ipv6-link-local link-local
```

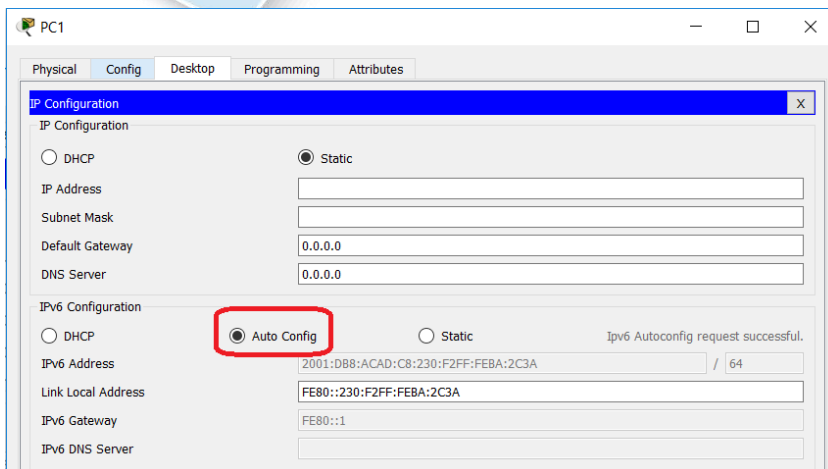
Paso 2: Configurar las PC para que reciban el direccionamiento IPv6 automáticamente

Configure las cuatro PC para que tengan configuración automática. Luego, cada una debe recibir automáticamente las direcciones IPv6 completas de los routers.

Paso 3: Verificar la conectividad entre las PC

Cada PC debe ser capaz de hacer ping a las otras PC y a los routers.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



Ejercicio 9.4.1.2: Reto de habilidades de integración

Topología

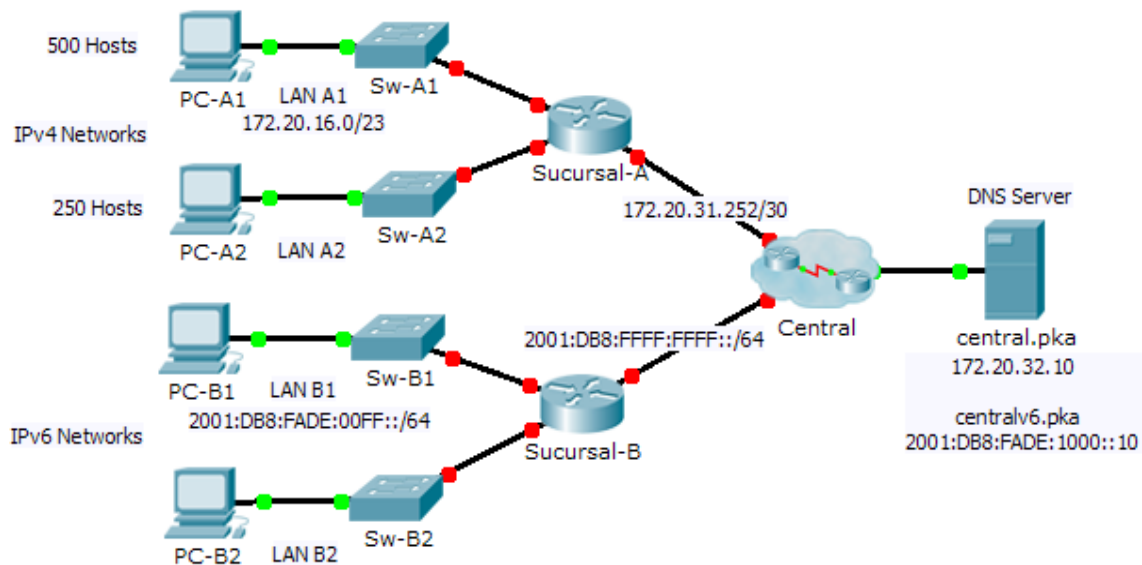


Tabla de direccionamiento: Resaltado en Amarillo se muestra las direcciones IP configuradas

Dispositivo	Interfaz	Dirección Dirección/Prefijo IPv6	Máscara de	Gateway predeterminado
Sucursal-A	G0/0	172.20.16.1	255.255.254.0	No aplicable
	G0/1	172.20.18.1	255.255.255.0	No aplicable
	G0/2	172.20.31.25	255.255.255.25	No aplicable
Sucursal-B	G0/0	2001:DB8:FADE:00FF::1/64		No aplicable
	G0/1	2001:DB8:FADE:0100::1/64		No aplicable
	G0/2	2001:DB8:FFFF:FFFF::2/64		No aplicable
PC-A1	NIC	172.20.17.25	255.255.254.0	172.20.16.1
PC-A2	NIC	172.20.18.25	255.255.255.0	172.20.18.1
PC-B1	NIC	2001:DB8:FADE:00FF::10/64		FE80::B
PC-B2	NIC	2001:DB8:FADE:0100::10/64		FE80::B

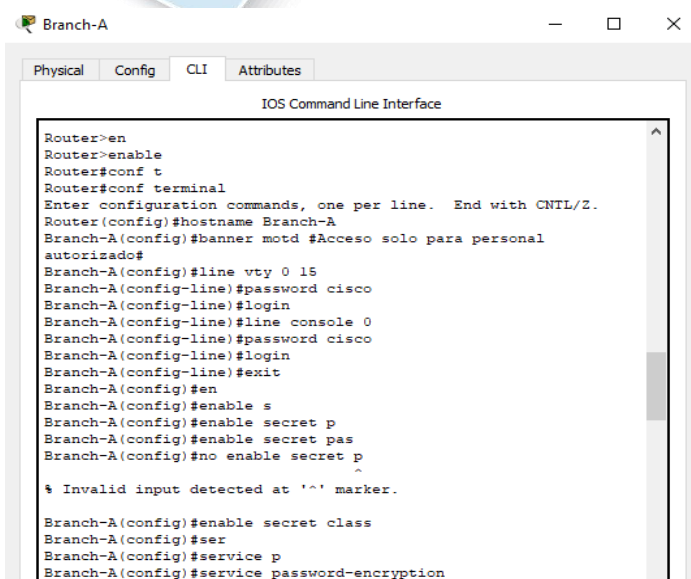
Situación

Como técnico de redes familiarizado con implementaciones de direccionamiento IPv4 e IPv6, ya está preparado para tomar una infraestructura de red existente y aplicar sus conocimientos y habilidades a finalizar la configuración. En esta actividad, el administrador de red ya configuró algunos comandos en los routers. **No borre ni modifique esas configuraciones.** Su tarea consiste en completar el esquema de direccionamiento IPv4 e IPv6, implementar el direccionamiento IPv4 e IPv6 y verificar la conectividad.

Requisitos

- Configure los parámetros iniciales en **Sucursal-A** y **Sucursal-B**, incluidos el nombre de host, el aviso, las líneas y las contraseñas. Utilice **cisco** como contraseña de EXEC del usuario y **class** como contraseña de EXEC privilegiado. Encripte todas las contraseñas.

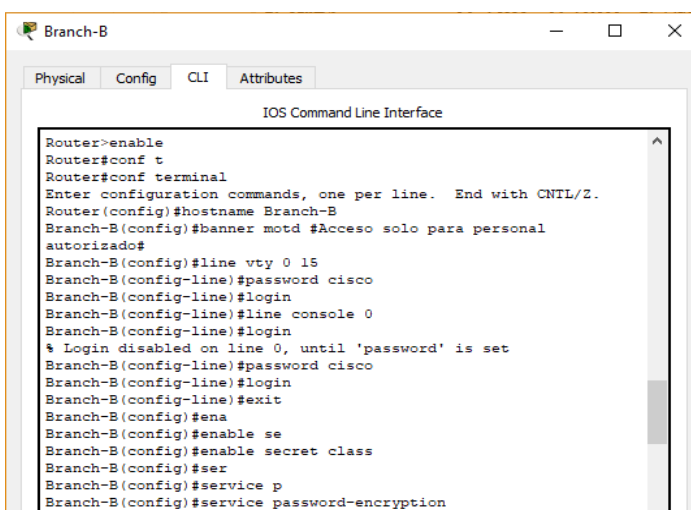
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



```

Branch-A
Physical Config CLI Attributes
IOS Command Line Interface
Router>en
Router>enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)#hostname Branch-A
Branch-A (config)#banner motd #Acceso solo para personal
autorizado#
Branch-A (config)#line vty 0 15
Branch-A (config-line)#password cisco
Branch-A (config-line)#login
Branch-A (config-line)#line console 0
Branch-A (config-line)#password cisco
Branch-A (config-line)#login
Branch-A (config-line)#exit
Branch-A (config)#en
Branch-A (config)#enable s
Branch-A (config)#enable secret p
Branch-A (config)#enable secret pas
Branch-A (config)#no enable secret p
^
% Invalid input detected at '^' marker.

Branch-A (config)#enable secret class
Branch-A (config)#ser
Branch-A (config)#service p
Branch-A (config)#service password-encryption
  
```



```

Branch-B
Physical Config CLI Attributes
IOS Command Line Interface
Router>enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)#hostname Branch-B
Branch-B (config)#banner motd #Acceso solo para personal
autorizado#
Branch-B (config)#line vty 0 15
Branch-B (config-line)#password cisco
Branch-B (config-line)#login
Branch-B (config-line)#line console 0
Branch-B (config-line)#login
% Login disabled on line 0, until 'password' is set
Branch-B (config-line)#password cisco
Branch-B (config-line)#login
Branch-B (config-line)#exit
Branch-B (config)#ena
Branch-B (config)#enable se
Branch-B (config)#enable secret class
Branch-B (config)#ser
Branch-B (config)#service p
Branch-B (config)#service password-encryption
  
```

- LAN A1 utiliza la subred 172.20.16.0/23. Asigne la siguiente subred disponible a LAN A2 para admitir un máximo de 250 hosts.
- LAN B1 utiliza la subred 2001:DB8:FADE:00FF::/64. Asigne la siguiente subred disponible a la B2 de LAN.
- Termine de registrar el esquema de direccionamiento en la **tabla de direccionamiento** con las siguientes pautas:
 - Asigne la primera dirección IP a la interfaz del router para LAN A1, LAN A2, LAN B1 y LAN B2.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

```

Branch-A
Physical Config CLI Attributes
IOS Command Line Interface
Branch-A(config)#service password-encryption
Branch-A(config)#int g0/0
Branch-A(config-if)#ip address 172.20.16.1 255.255.254.0
Branch-A(config-if)#no sh
Branch-A(config-if)#no shutdown

Branch-A(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

Branch-A(config-if)#int g0/1
Branch-A(config-if)#ip address 172.20.18.1 255.255.255.0
Branch-A(config-if)#no shutdown

Branch-A(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

Branch-A(config-if)#int g0/2
Branch-A(config-if)#ip address 172.20.31.254 255.255.255.252
Branch-A(config-if)#no shutdown

Branch-A(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/2, changed state to up

```

```

Branch-B
Physical Config CLI Attributes
IOS Command Line Interface
Branch-B(config)#int g0/0
Branch-B(config-if)#ipv6 address 2001:DB8:FADE:00FF::1/64
Branch-B(config-if)#ipv6 address FE80::1 link-local
Branch-B(config-if)#no shutdown

Branch-B(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

Branch-B(config-if)#int g0/1
Branch-B(config-if)#ipv6 address 2001:DB8:FADE:0100::1/64
Branch-B(config-if)#ipv6 address FE80::1 link-local
Branch-B(config-if)#no shutdown

Branch-B(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

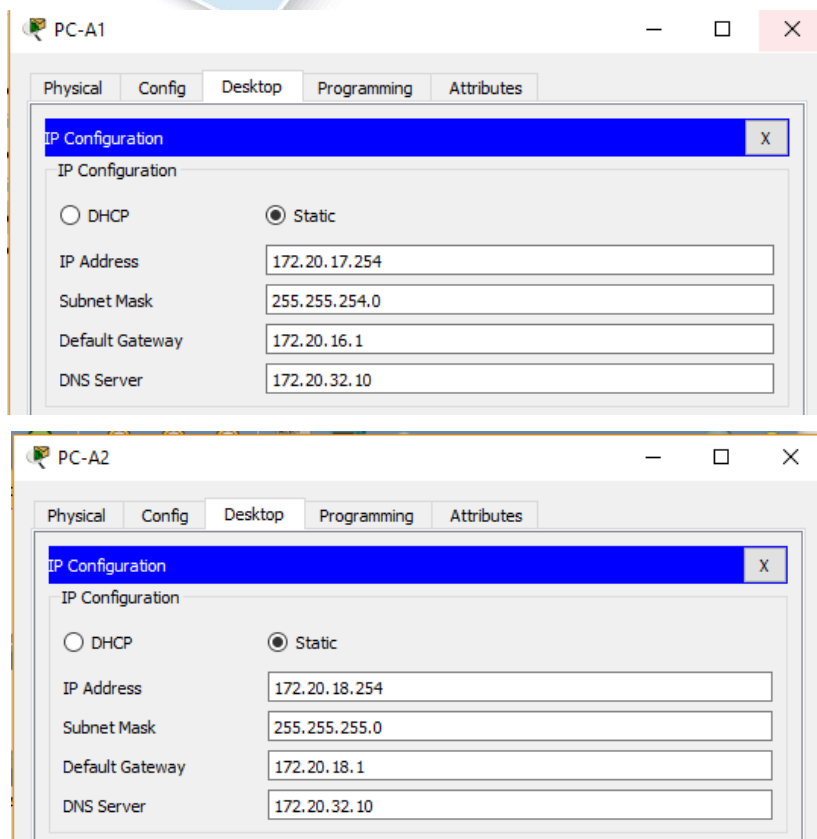
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

Branch-B(config-if)#int g0/2
Branch-B(config-if)#ipv6 address 2001:DB8:FFFF:FFFF::2/64
Branch-B(config-if)#ipv6 address FE80::1 link-local
Branch-B(config-if)#no shutdown

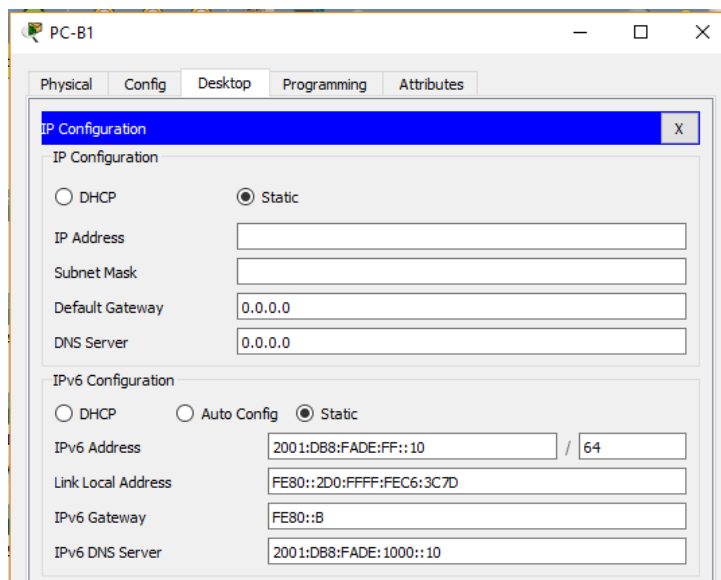
```

- Para las redes IPv4, asigne la última dirección IPv4 a las PC.

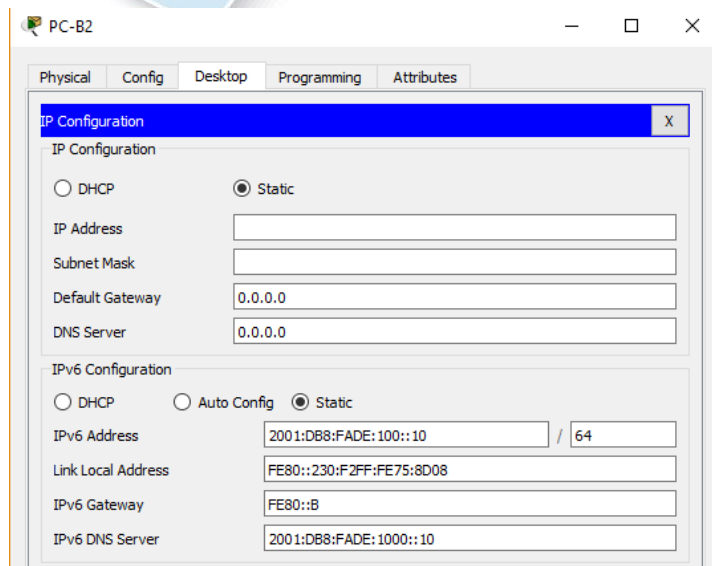
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



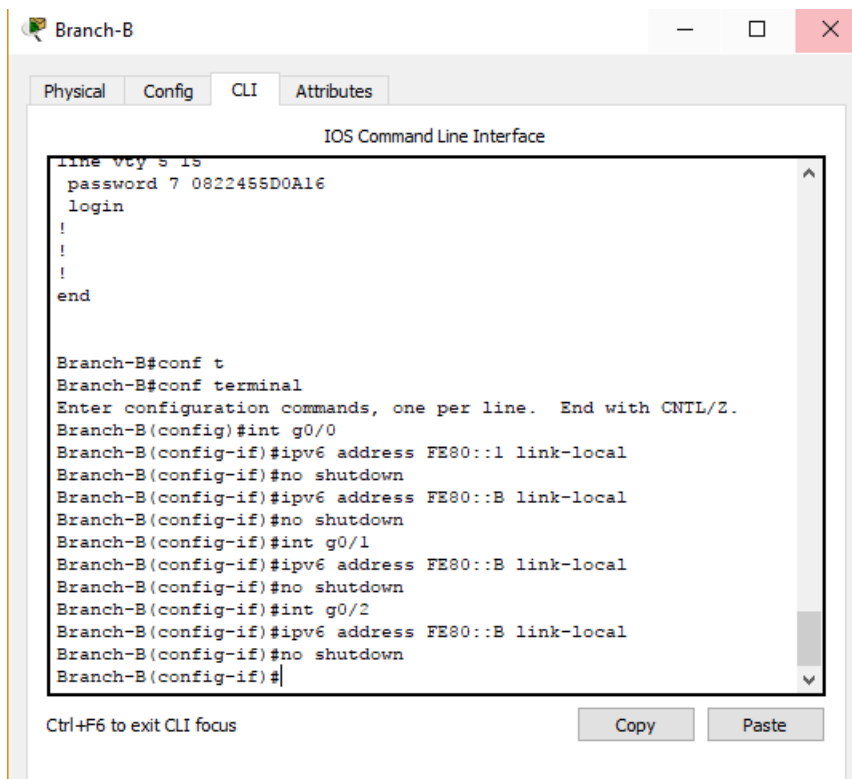
- Para las redes IPv6, asigne la 16.^a dirección IPv6 a las PC.



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



- Configure el direccionamiento de los routers según los registros. Incluya una descripción adecuada para cada interfaz del router. **Sucursal-B** utiliza FE80::B como dirección link-local.



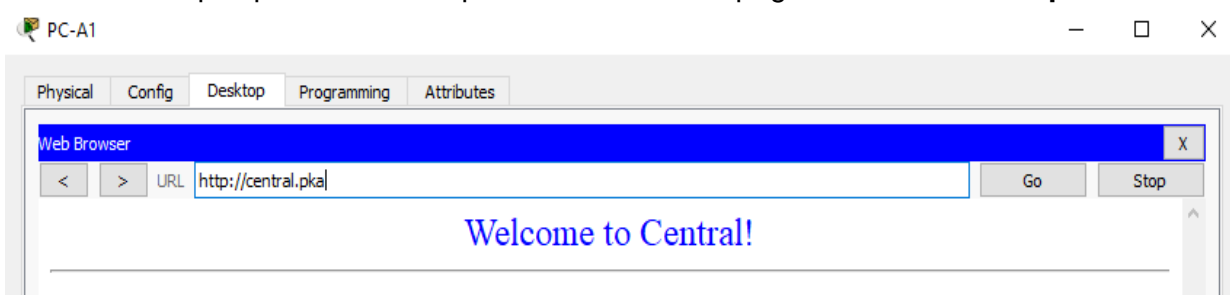
- Configure el direccionamiento de las PC según los registros. Las direcciones del servidor DNS para IPv4 e IPv6 se muestran en la topología.
- Verifique la conectividad entre las PC IPv4 y entre las PC IPv6.

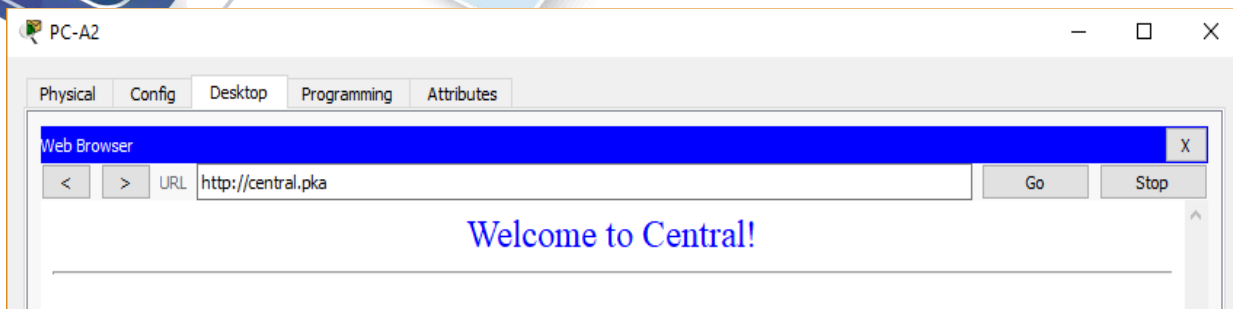
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

```
PC-A1  
Physical Config Desktop Programming Attributes  
Command Prompt  
Packet Tracer PC Command Line 1.0  
C:\>ping 172.20.18.254  
  
Pinging 172.20.18.254 with 32 bytes of data:  
  
Reply from 172.20.18.254: bytes=32 time=1ms TTL=127  
Reply from 172.20.18.254: bytes=32 time=17ms TTL=127  
Reply from 172.20.18.254: bytes=32 time=26ms TTL=127  
Reply from 172.20.18.254: bytes=32 time=17ms TTL=127  
  
Ping statistics for 172.20.18.254:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 26ms, Average = 15ms  
  
C:\>
```

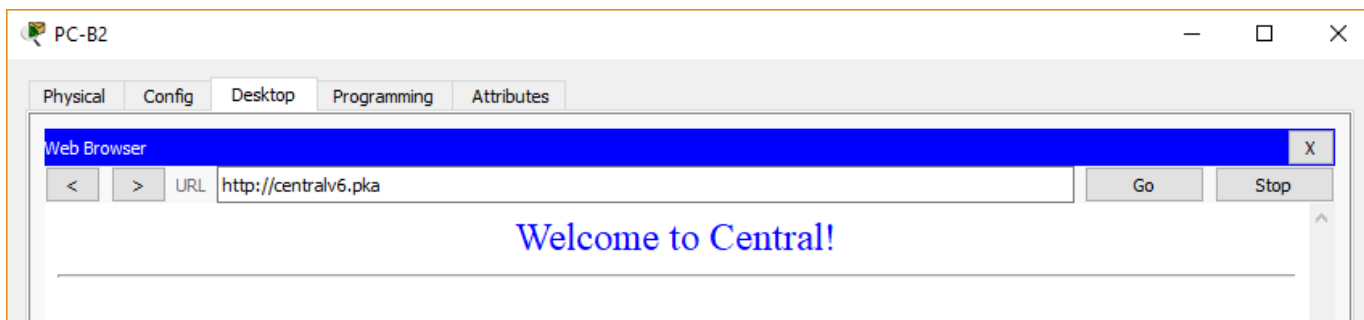
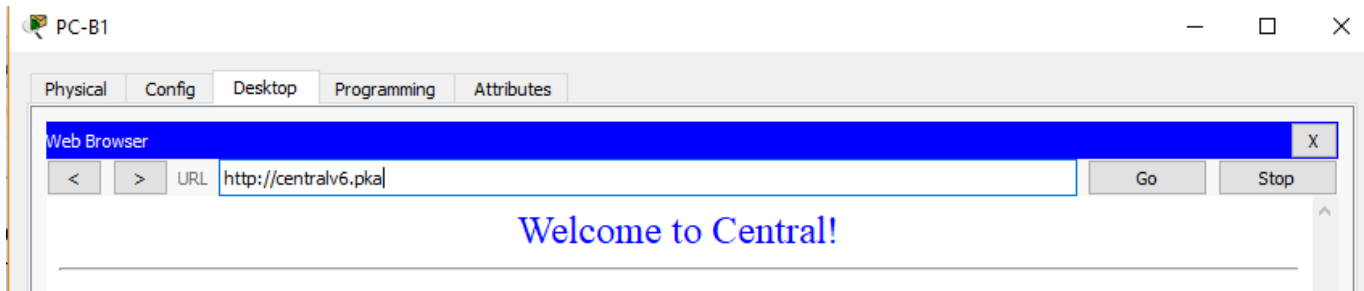
```
PC-B1  
Physical Config Desktop Programming Attributes  
Command Prompt  
Packet Tracer PC Command Line 1.0  
C:\>ping 2001:DB8:FADE:100::10  
  
Pinging 2001:DB8:FADE:100::10 with 32 bytes of data:  
  
Reply from 2001:DB8:FADE:100::10: bytes=32 time=1ms TTL=127  
Reply from 2001:DB8:FADE:100::10: bytes=32 time=13ms TTL=127  
Reply from 2001:DB8:FADE:100::10: bytes=32 time=1ms TTL=127  
Reply from 2001:DB8:FADE:100::10: bytes=32 time=25ms TTL=127  
  
Ping statistics for 2001:DB8:FADE:100::10:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 25ms, Average = 10ms  
  
C:\>
```

- Verifique que las PC IPv4 puedan acceder a la página Web en **central.pka**.





- Verifique que las PC IPv6 puedan acceder a la página Web en **centralv6.pka**.



Resultados

The screenshot shows the 'Activity Results' window in Cisco Packet Tracer. It displays a list of assessment items and a table of connectivity test results.

Assessment Items

- Network
 - Branch-A
 - Banner MOTD
 - Console Line
 - Login
 - Password
 - Enable Secret
 - Host Name
 - Ports
 - GigabitEthernet0/0
 - Description
 - IP Address
 - Port Status
 - Subnet Mask
 - GigabitEthernet0/1
 - Description
 - IP Address
 - Port Status
 - Subnet Mask
 - GigabitEthernet0/2
 - Description
 - IP Address
 - Port Status
 - Subnet Mask
 - Service Password En
 - VTY Lines
 - VTY Line 0
 - Password

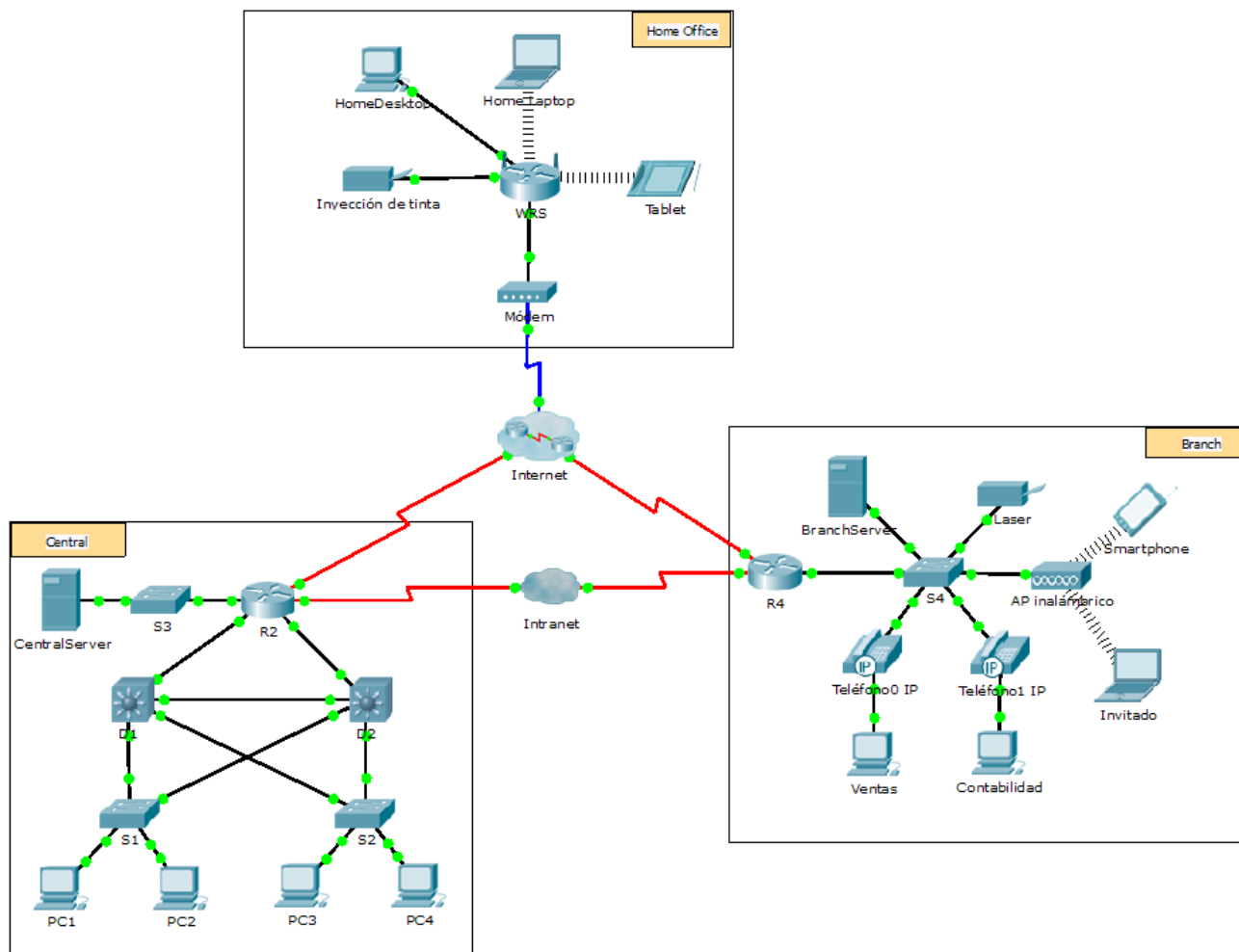
Connectivity Tests

Component	Items/Total	Score
Basic Security Configuration	12/12	12/12
DNS Server Address Configuration	4/4	4/4
Default Gateway Configuration	4/4	4/4
Device Interface Configuration	12/12	12/12
Hostname Configuration	2/2	2/2
IPv4 Host Address Calculation	5/5	11/11
IPv4 Subnet Mask Calculation	5/5	8/8
IPv6 Host Address Calculation	5/5	14/14
IPv6 Prefix Calculation	5/5	5/5
Ip	3/3	3/3

Overall Feedback: Score: 75/75, Item Count: 57/57

Ejercicio 10.2.1.8: Servidores Web y de correo electrónico

Topología



Objetivos

Parte 1: Configurar y verificar los servicios Web

Parte 2: Configurar y verificar los servicios de correo electrónico

Información básica

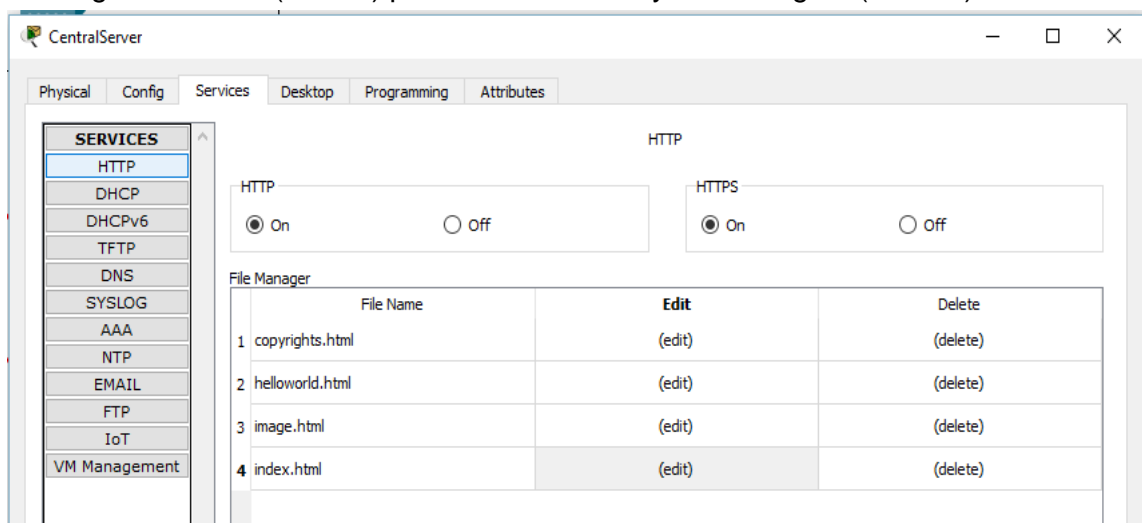
En esta actividad, configurará los servicios HTTP y de correo electrónico mediante el servidor simulado de Packet Tracer. Luego, configurará clientes para que accedan a los servicios HTTP y de correo electrónico.

Nota: Packet Tracer simula solamente el proceso para configurar estos servicios. Cada paquete de software de HTTP y de correo electrónico tiene sus propias instrucciones exclusivas de configuración e instalación.

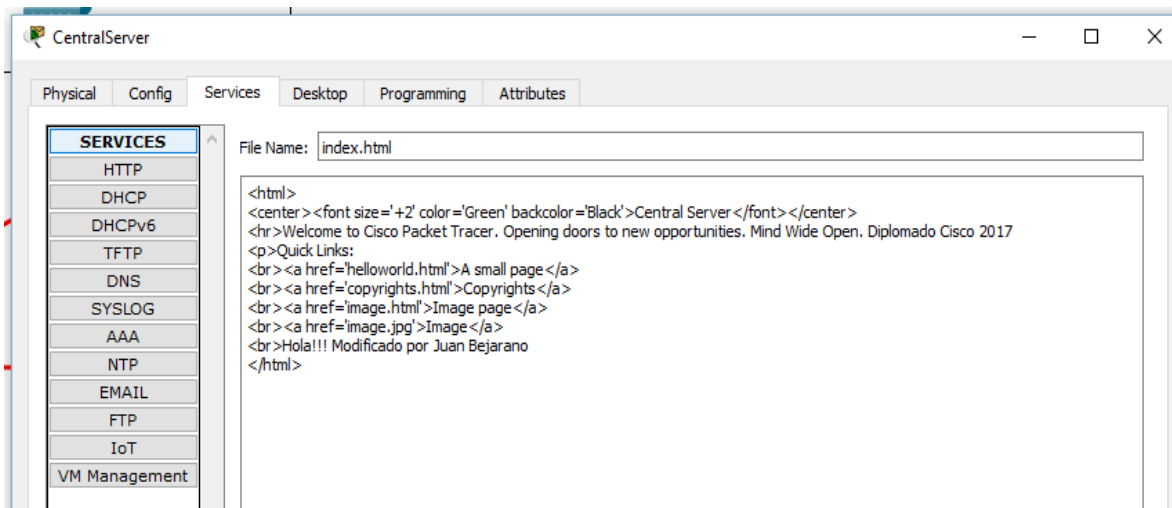
Parte 1: Configurar y verificar los servicios Web

Paso 1: Configurar servicios Web en CentralServer y BranchServer

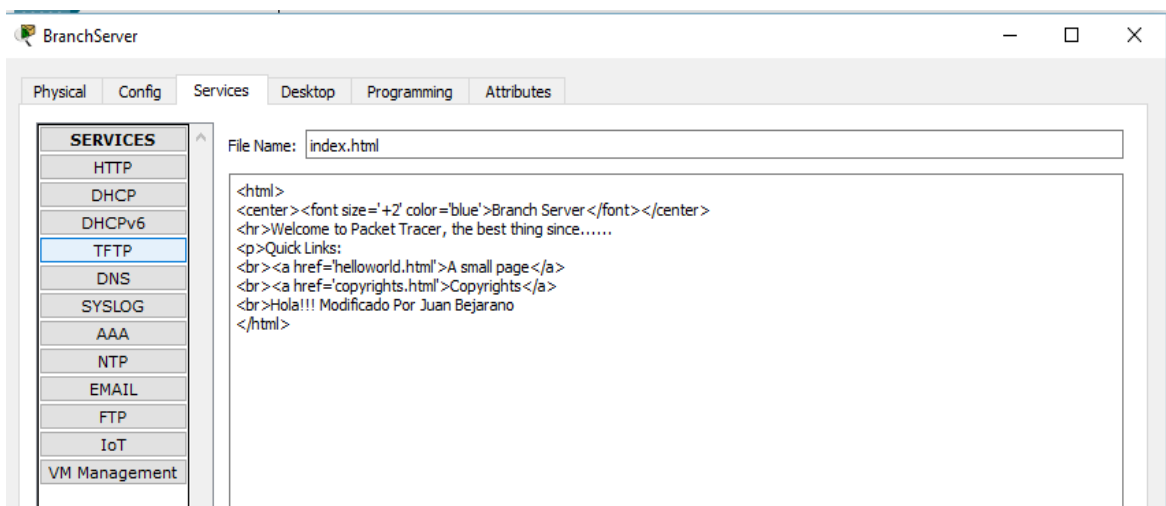
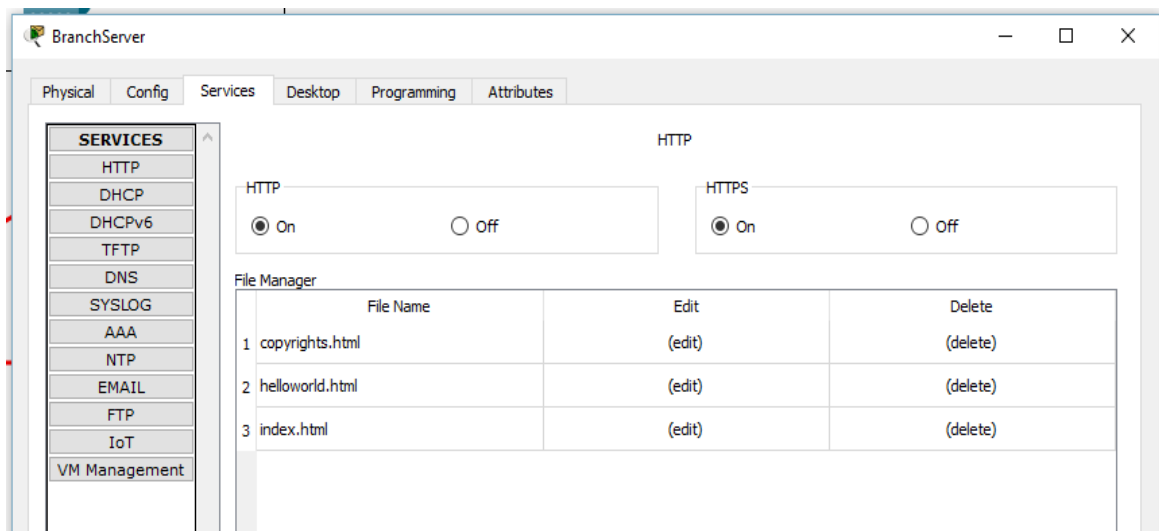
- Haga clic en **CentralServer** y, a continuación, haga clic en la ficha **Config > HTTP**.
- Haga clic en **On** (Activar) para habilitar HTTP y HTTP seguro (HTTPS).



- Optativo: personalice el código HTML.



d. Repita desde el paso 1a hasta el paso 1c en **BranchServer**.

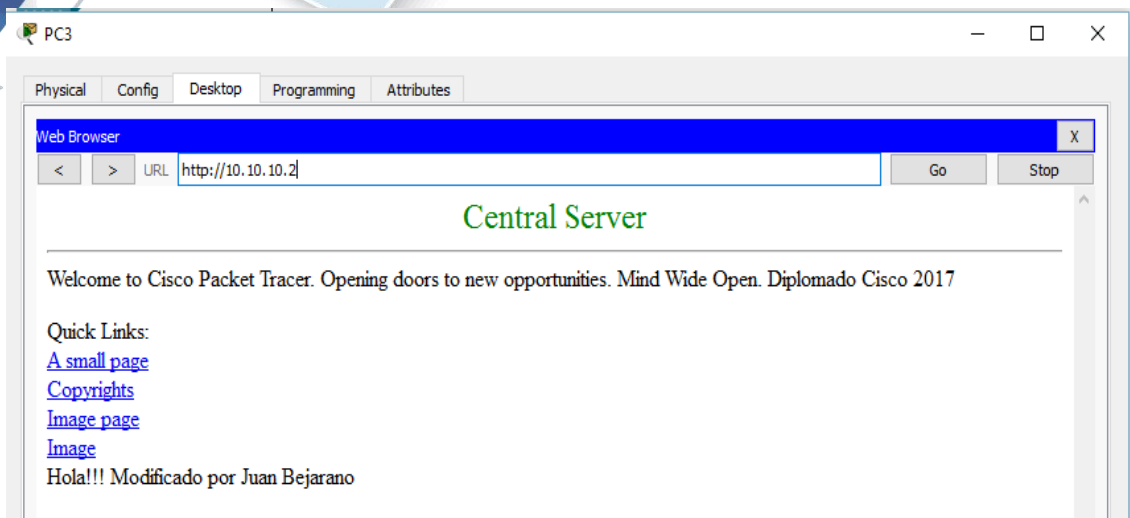


Paso 2: Verificar los servidores Web mediante el acceso a las páginas Web

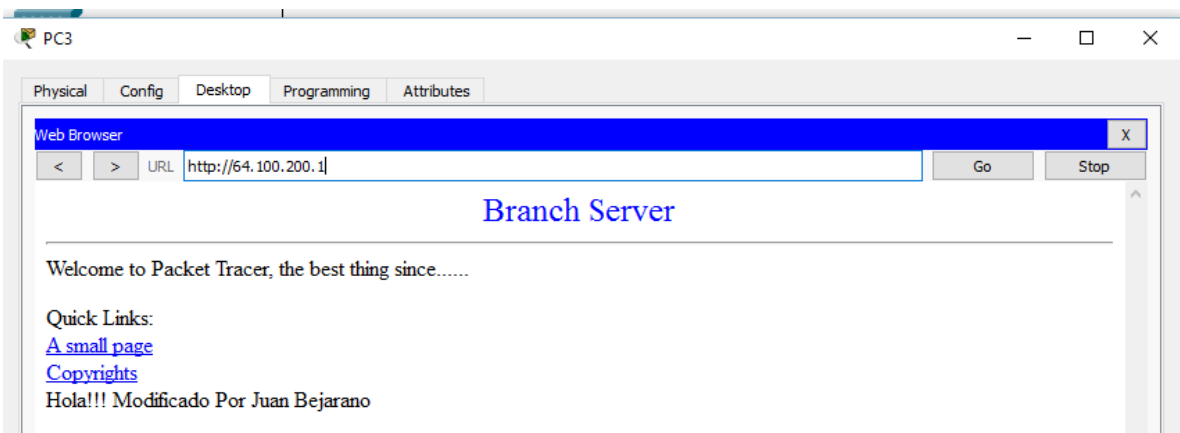
Existen muchos dispositivos terminales en esta red, pero para este paso, use **PC3**.

- Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop > Web Browser** (Escritorio > Explorador Web).
- En el cuadro de dirección URL, introduzca **10.10.10.2** como dirección IP y haga clic en **Go** (Ir). Aparece el sitio Web de **CentralServer**.

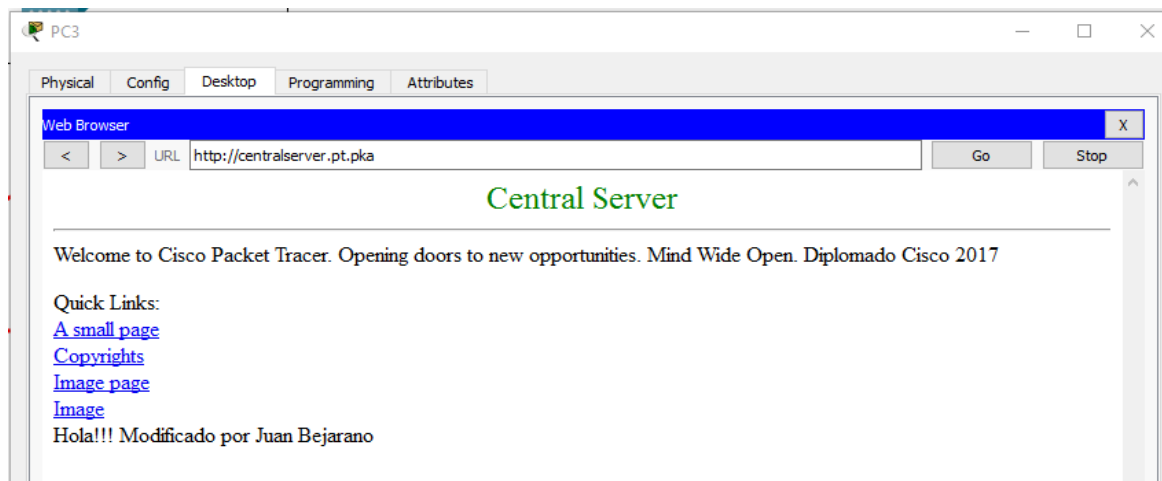
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



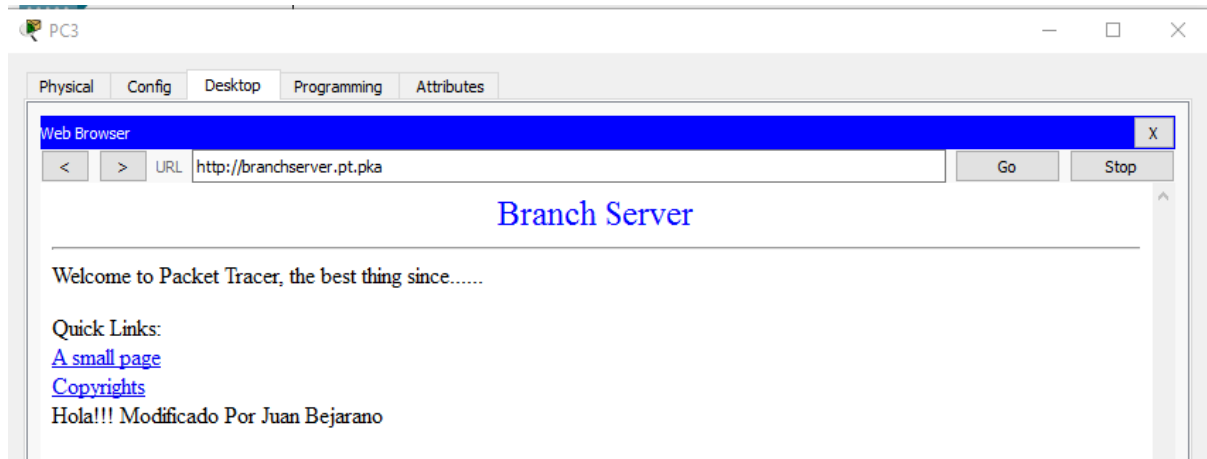
- c. En el cuadro de dirección URL, introduzca **64.100.200.1** como dirección IP y haga clic en **Go**. Aparece el sitio Web de **BranchServer**.



- d. En el cuadro de dirección URL, introduzca **centralserver.pt.pka** y haga clic en **Go**. Aparece el sitio Web de **CentralServer**.



- e. En el cuadro de dirección URL, introduzca **branchserver.pt.pka** y haga clic en **Go**. Aparece el sitio Web de **BranchServer**.



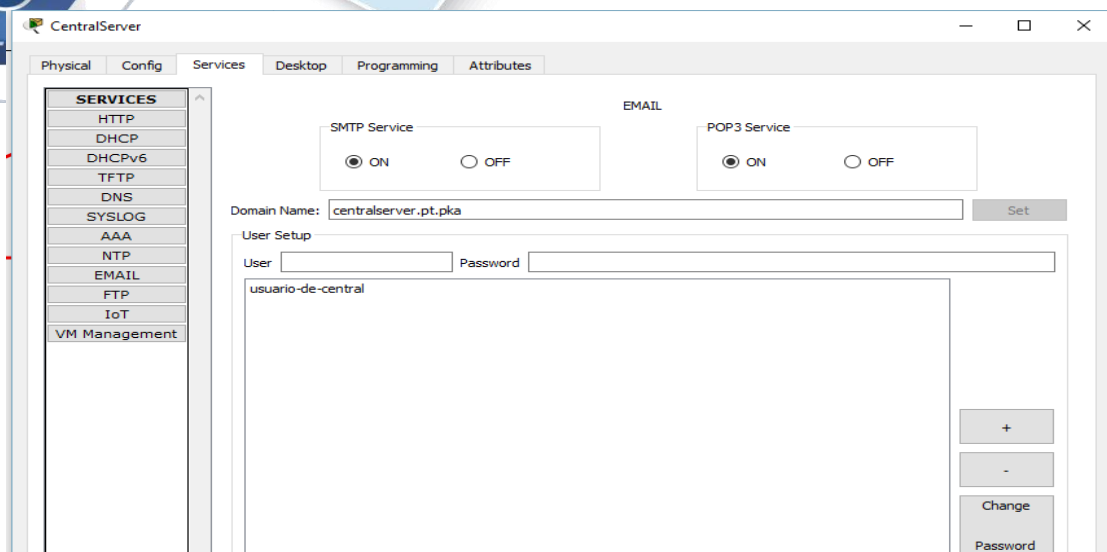
- ¿Qué protocolo traduce los nombres **centralserver.pt.pka** y **branchserver.pt.pka** por direcciones IP?
 Servicio de nombres de dominios (DNS, Domain Name Service)

Parte 2: Configurar y verificar los servicios de correo electrónico en los servidores

Paso 1: Configurar CentralServer para enviar (SMTP) y recibir (POP3) correo electrónico

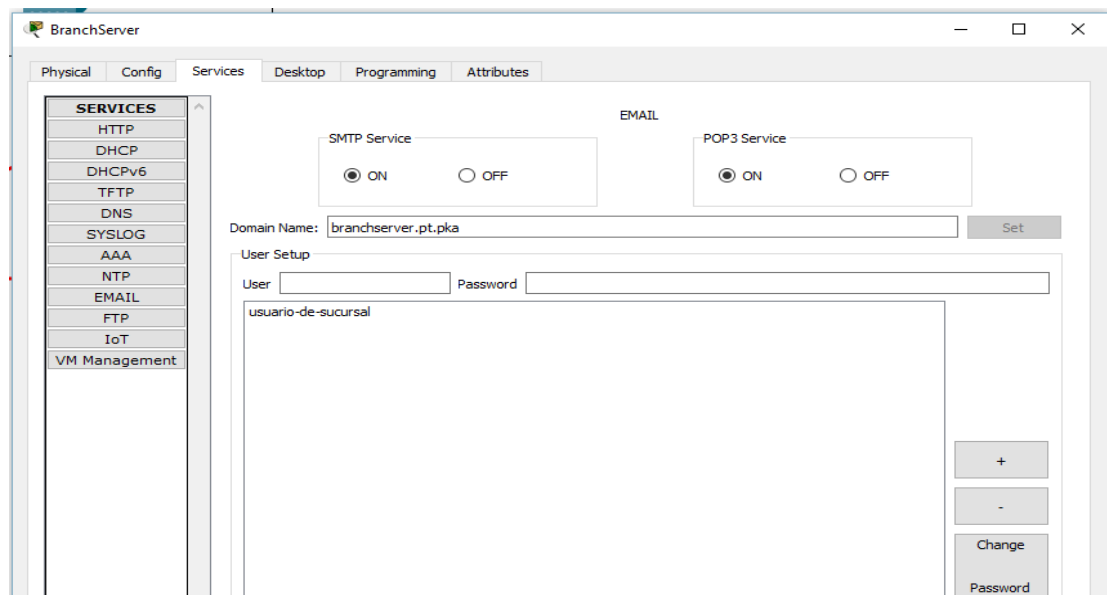
- a. Haga clic en **CentralServer** y, a continuación, seleccione la ficha **Config**, seguida del botón **EMAIL** (Correo electrónico).
- b. Haga clic en **On** para habilitar SMTP y POP3.
- c. Establezca el nombre de dominio **centralserver.pt.pka** y haga clic en **Set** (Establecer).
- d. Cree un usuario denominado **usuario-de-central** con la contraseña **cisco**. Haga clic en **+** para agregar el usuario

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



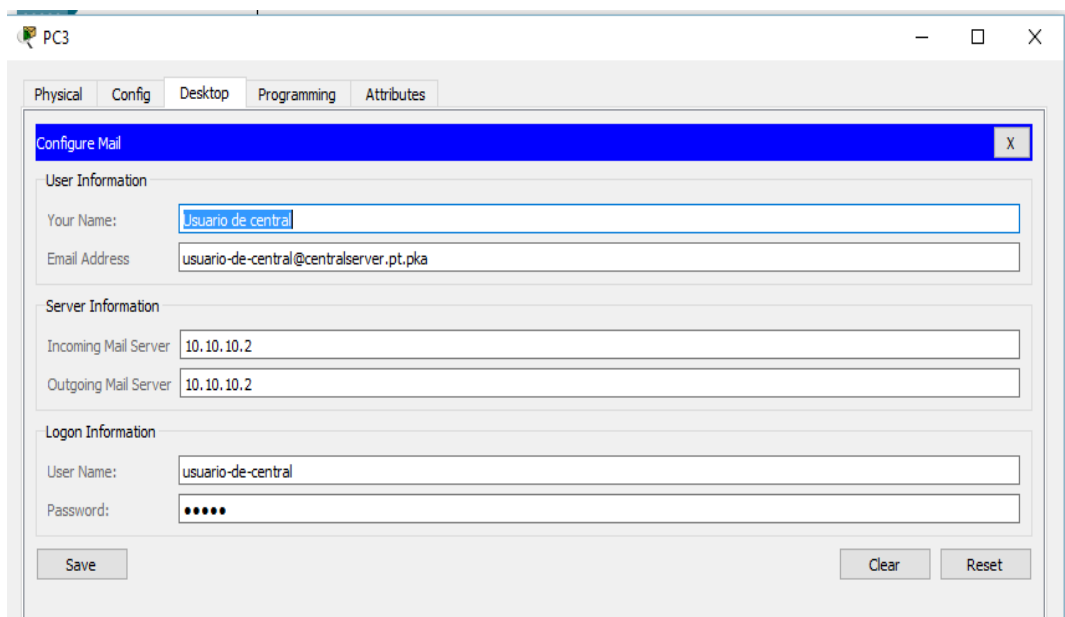
Paso 2: Configurar BranchServer para enviar (SMTP) y recibir (POP3) correo electrónico

- Haga clic en **BranchServer** y, a continuación, haga clic en la ficha **Config > EMAIL**.
- Haga clic en **On** para habilitar SMTP y POP3.
- Establezca el nombre de dominio **branchserver.pt.pka** y haga clic en **Set**.
- Cree un usuario denominado **usuario-de-sucursal** con la contraseña **cisco**. Haga clic en **+** para agregar el usuario.

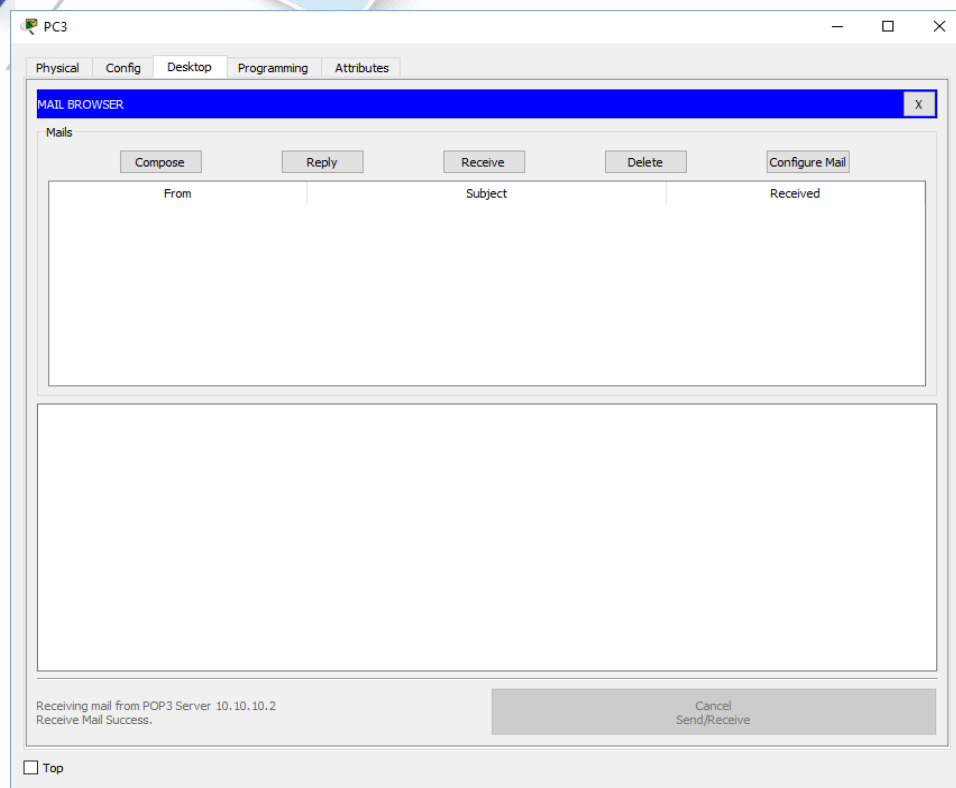


Paso 3: Configurar la PC3 para que use el servicio de correo electrónico de CentralServer

- a. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop > E Mail** (Correo electrónico).
- b. Introduzca los siguientes valores en los campos correspondientes:
 - 1) Your Name (Su nombre): **Usuario de central**
 - 2) Email Address (Dirección de correo electrónico): **usuario-de-central@centralserver.pt.pka**
 - 3) Incoming Mail Server (Servidor de correo entrante): **10.10.10.2**
 - 4) Outgoing Mail Server (Servidor de correo saliente): **10.10.10.2**
 - 5) User Name (Nombre de usuario): **usuario-de-central**
 - 6) Password (Contraseña): **cisco**
- c. Haga clic en **Save** (Guardar). Aparece la ventana del explorador de correo.
- d. Haga clic en **Receive** (Recibir). Si todo se configuró correctamente tanto en el cliente como en el servidor, la ventana del explorador de correo muestra la confirmación de mensaje **Receive Mail Success** (La función Recibir correo se realizó correctamente).



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

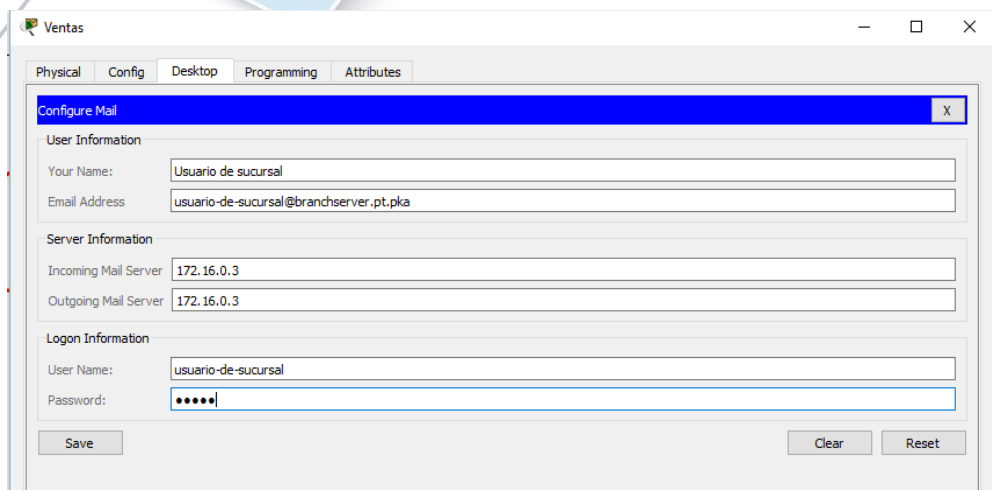


Paso 4: Configurar Sales para que use el servicio de correo electrónico de BranchServer

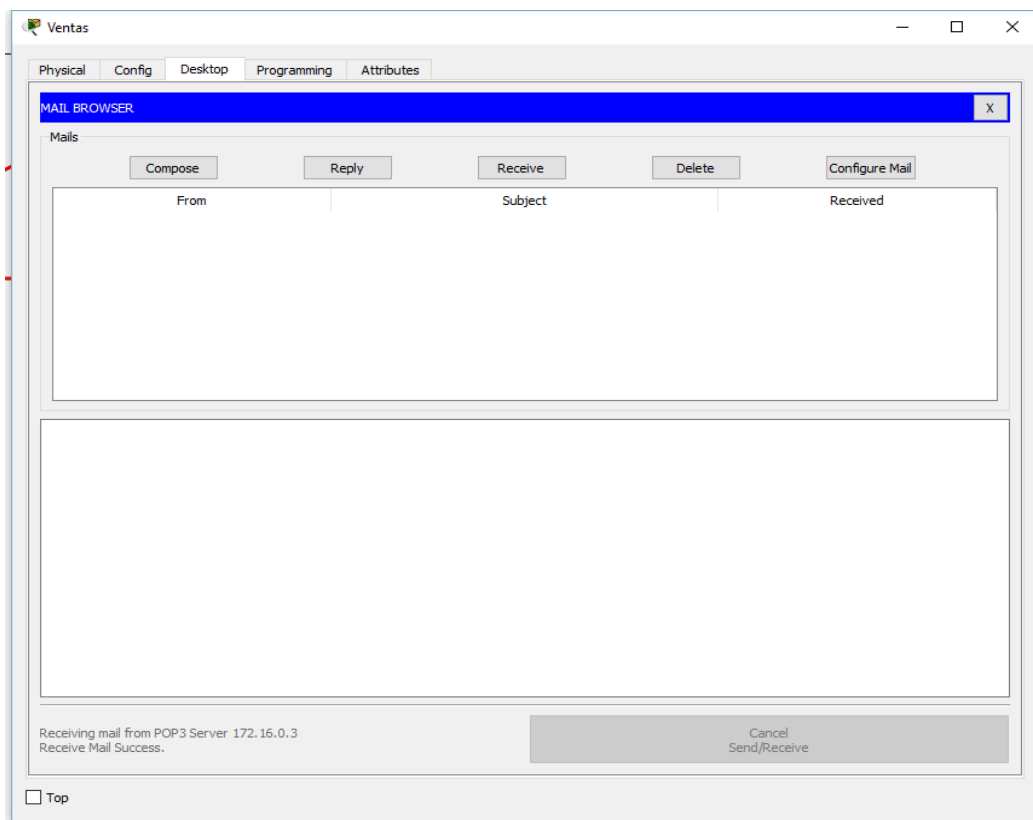
a. Haga clic en **Sales** (Ventas) y, a continuación, haga clic en la ficha **Desktop** > **E Mail**. b. Introduzca los siguientes valores en los campos correspondientes:

- 1) Your Name (Su nombre): **Usuario de sucursal**
 - 2) Email Address (Dirección de correo electrónico): **usuario-de-sucursal@branchserver.pt.pka**
 - 3) Incoming Mail Server (Servidor de correo entrante): **172.16.0.3**
 - 4) Outgoing Mail Server (Servidor de correo saliente): **172.16.0.3**
 - 5) User Name (Nombre de usuario): **usuario-de-sucursal**
 - 6) Password (Contraseña): **cisco**
- c. Haga clic en **Save** (Guardar). Aparece la ventana del explorador de correo.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



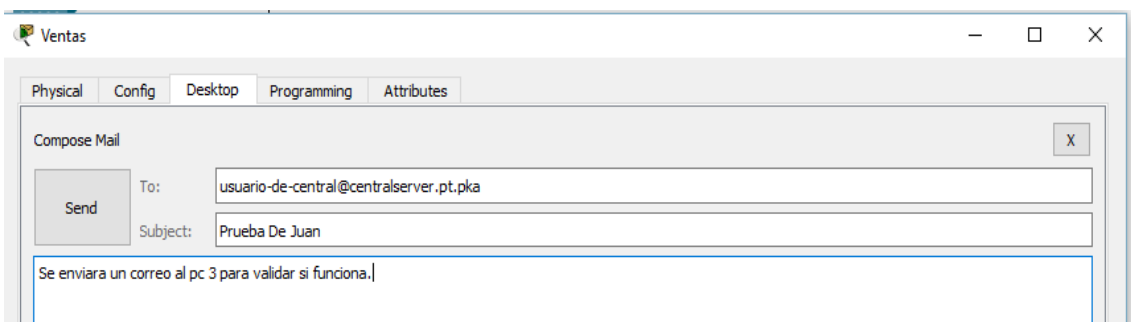
d. Haga clic en **Receive** (Recibir). Si todo se configuró correctamente tanto en el cliente como en el servidor, la ventana del explorador de correo muestra la confirmación de mensaje **Receive Mail Success** (La función Recibir correo se realizó correctamente).



e. Esta actividad debe completarse en un 100%. No cierre la ventana de configuración de Sales ni la ventana del explorador de correo.

Paso 5: Envíe un correo electrónico desde el cliente Sales y el cliente PC3.

- a. Desde la ventana del **explorador de correo** de **Sales**, haga clic en **Compose** (Redactar).
- b. Introduzca los siguientes valores en los campos correspondientes:
 - 1) To (Para): **usuario-de-central@centralserver.pt.pka**
 - 2) Subject (Asunto): *Personalice el asunto.*
 - 3) **Email** body (Cuerpo del correo electrónico): *Personalice el correo electrónico.*
- c. Haga clic en **Send** (Enviar).

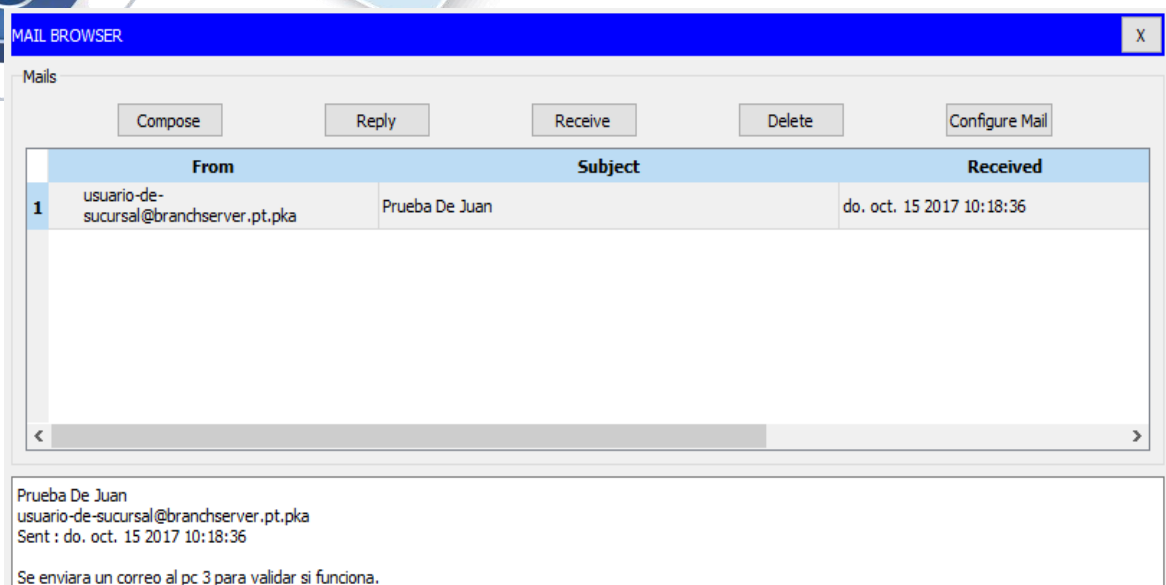


Sending mail to usuario-de-central@centralserver.pt.pka , with subject : Prueba De Juan .. Mail Server: 172.16.0.3
Send Success.

Verifique que la **PC3** haya recibido el correo electrónico. Haga clic en **PC3**. Si la ventana del explorador de correo está cerrada, haga clic en **E Mail**.

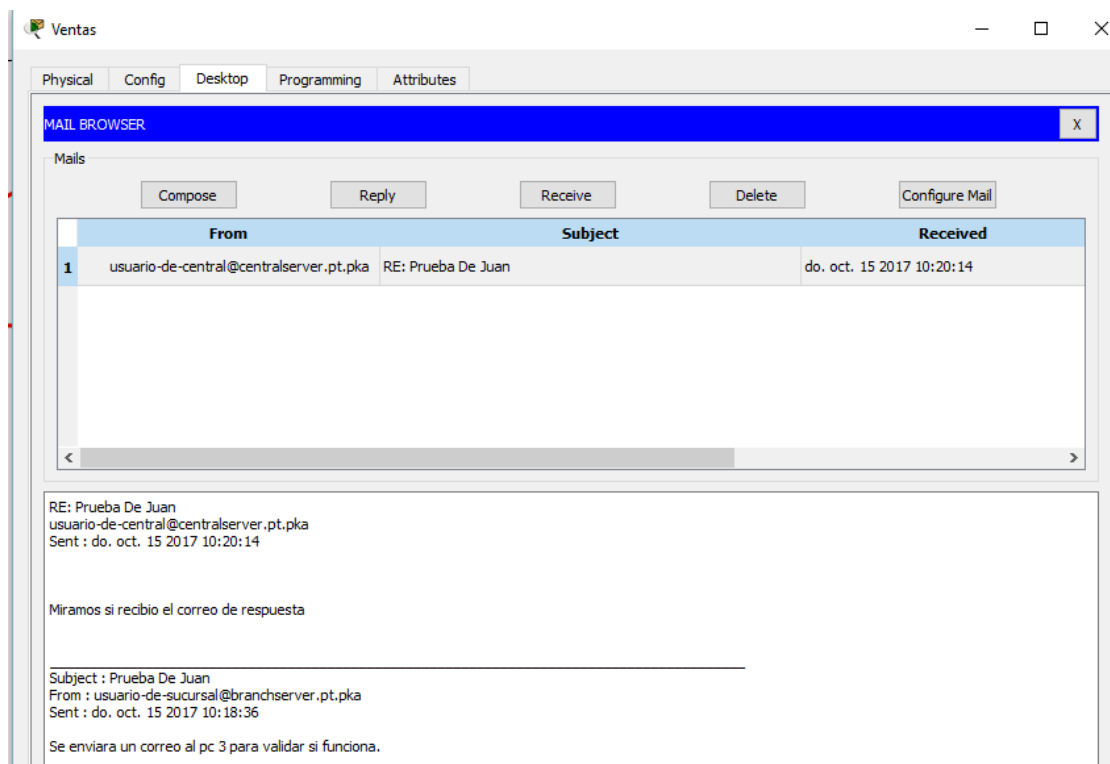
Haga clic en **Receive** (Recibir). Aparece un correo electrónico proveniente de Sales. Haga doble clic en el correo electrónico.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



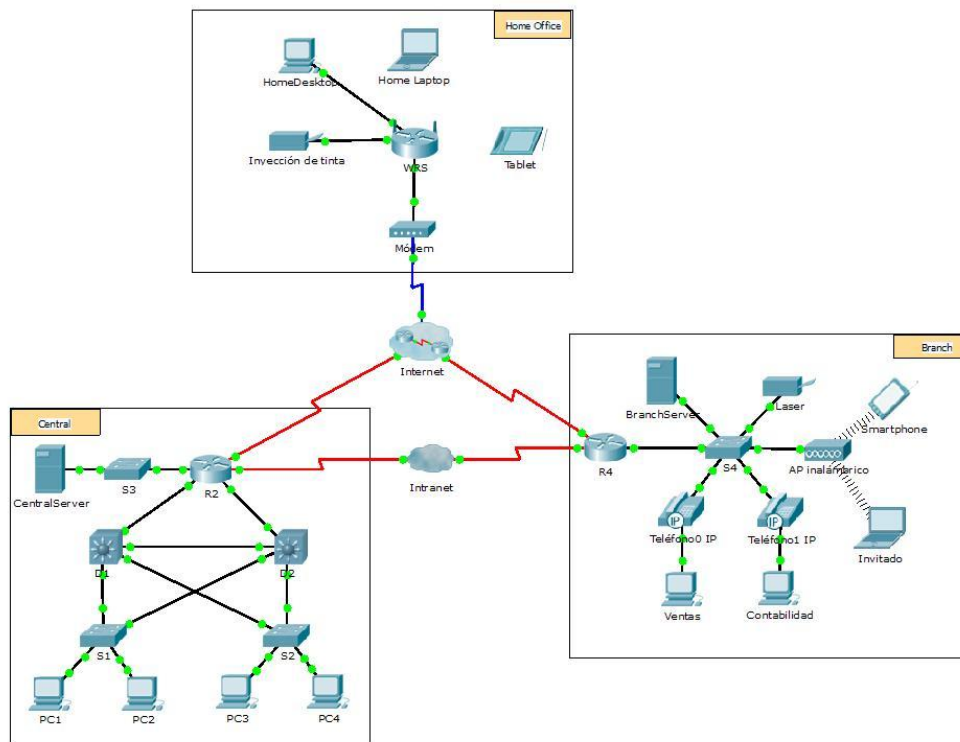
f. Haga clic en **Reply** (Responder), personalice una respuesta y haga clic en **Send**.

g. Verifique que **Sales** haya recibido la respuesta.



Ejercicio 10.2.2.8: Servidores de DHCP y servidores DNS

Topología



Objetivos

Parte 1: Configurar el direccionamiento IPv4 estático

Parte 2: Configurar y verificar los registros DNS

Información básica

En esta actividad, configurará y verificará el direccionamiento IP estático y el direccionamiento DHCP. A continuación, configurará un servidor DNS para que asigne direcciones IP a los nombres de sitios Web.

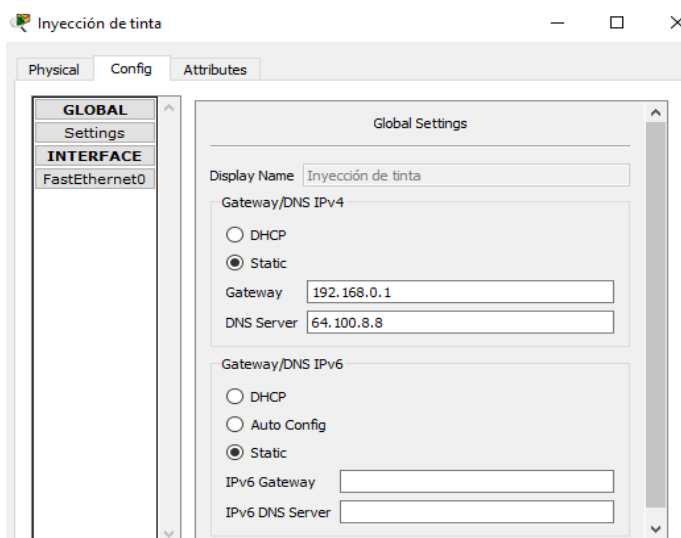
Nota: Packet Tracer simula solamente el proceso para configurar estos servicios. Cada paquete de software de DHCP y DNS tiene sus propias instrucciones exclusivas de configuración e instalación.

Parte 1: Configurar el direccionamiento IPv4 estático

Paso 1: Configurar la impresora de inyección de tinta con direccionamiento IPv4 estático

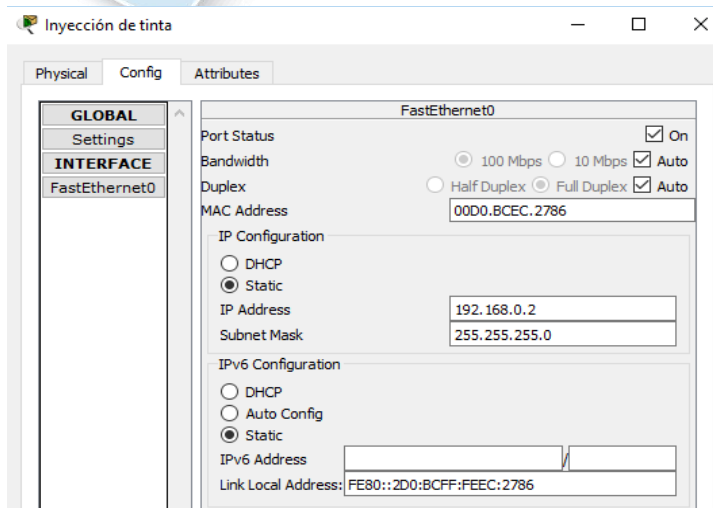
Las PC de oficinas domésticas necesitan conocer la dirección IPv4 de una impresora para enviarle información. Por lo tanto, la impresora debe utilizar una dirección IPv4 estática (invariable).

- Haga clic en **Inkjet** (Inyección de tinta) y, a continuación, haga clic en la ficha **Config**, en la que se muestran los parámetros de Global Settings (Configuración global).
- Asigne de manera estática la dirección de gateway **192.168.0.1** y la dirección de servidor DNS **64.100.8.8**.



Haga clic en **FastEthernet0** y asigne de manera estática la dirección IP **192.168.0.2** y la dirección de máscara de subred **255.255.255.0**.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



- Cierre la ventana Inkjet.

Paso 2: Configurar WRS para que proporcione servicios de DHCP

- I. Haga clic en **WRS** y, a continuación, haga clic en la ficha **GUI** y maximice la ventana.
- m. Se muestra la ventana Basic Setup (Configuración básica) de manera predeterminada. Configure los siguientes parámetros en la sección Network Setup (Configuración de red):

Cambie la Dirección IP a **192.168.0.1**.

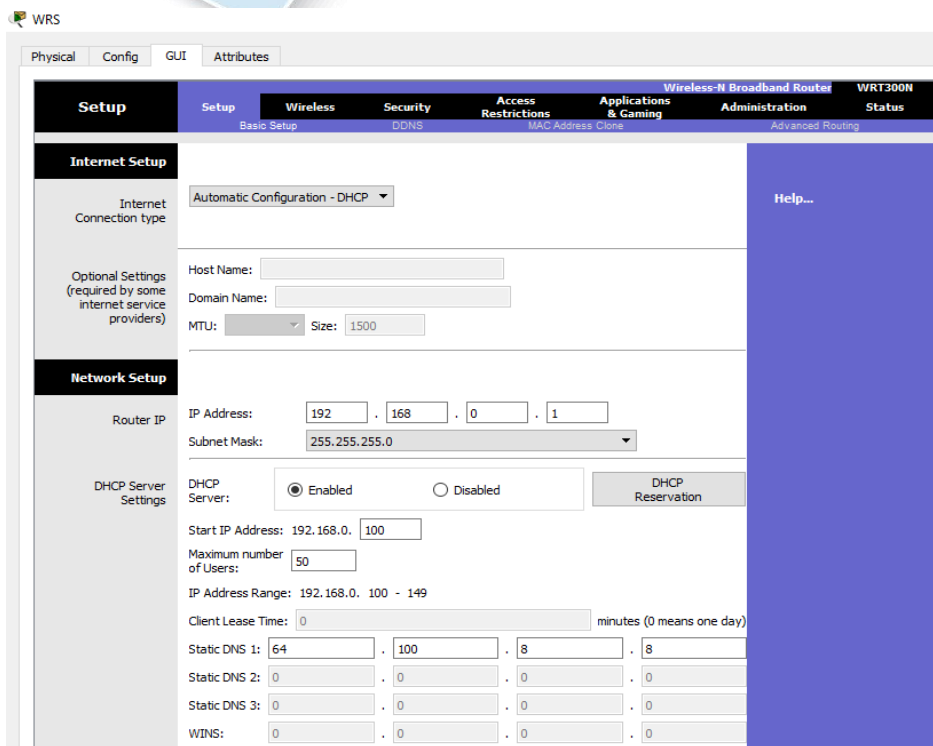
Establezca la máscara de subred **255.255.255.0**.

Habilite el servidor de DHCP.

Establezca la dirección DNS estática 1 **64.100.8.8**.

Desplácese hasta la parte inferior y haga clic en **Save** (Guardar).

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



Physical Config GUI Attributes

Wireless-N Broadband Router WRT300N

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers):

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP: IP Address: 192 . 168 . 0 . 1
Subnet Mask: 255.255.255.0

DHCP Server Settings:

DHCP Server: Enabled Disabled

Start IP Address: 192.168.0.

Maximum number of Users:

IP Address Range: 192.168.0. 100 - 149

Client Lease Time: minutes (0 means one day)

Static DNS 1: . . .

Static DNS 2: . . .

Static DNS 3: . . .

WINS: . . .

Help...

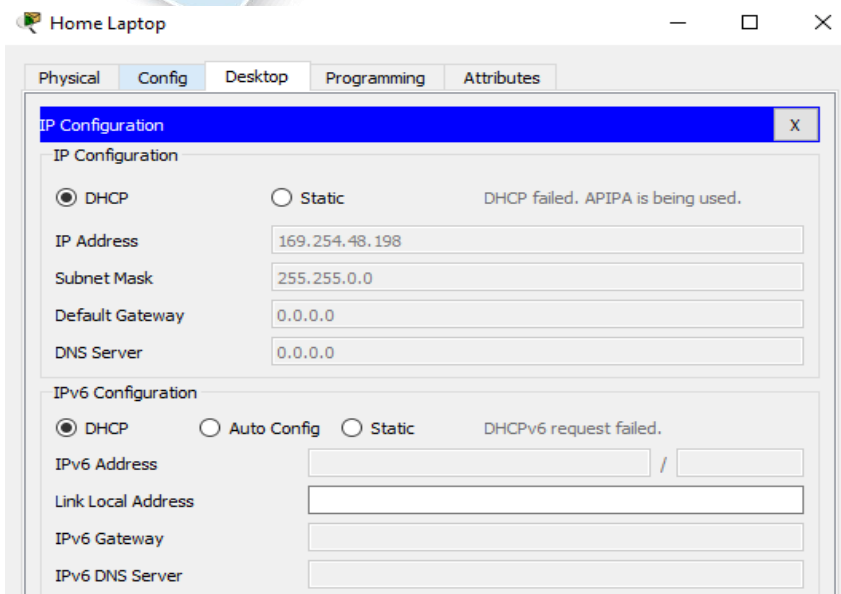
n. Cierre la ventana **WRS**.

Paso 3: Solicitar direccionamiento DHCP para la computadora portátil doméstica

Esta actividad se centra en la oficina doméstica. Los clientes que configurará con DHCP son **Home Laptop** (Computadora portátil doméstica) y **Tablet PC**.

- Haga clic en **Home Laptop** y, a continuación, haga clic en la ficha **Desktop > IP Configuration** (Escritorio > Configuración de IP).
- Haga clic en **DHCP** y espere hasta que la solicitud de DHCP sea correcta.

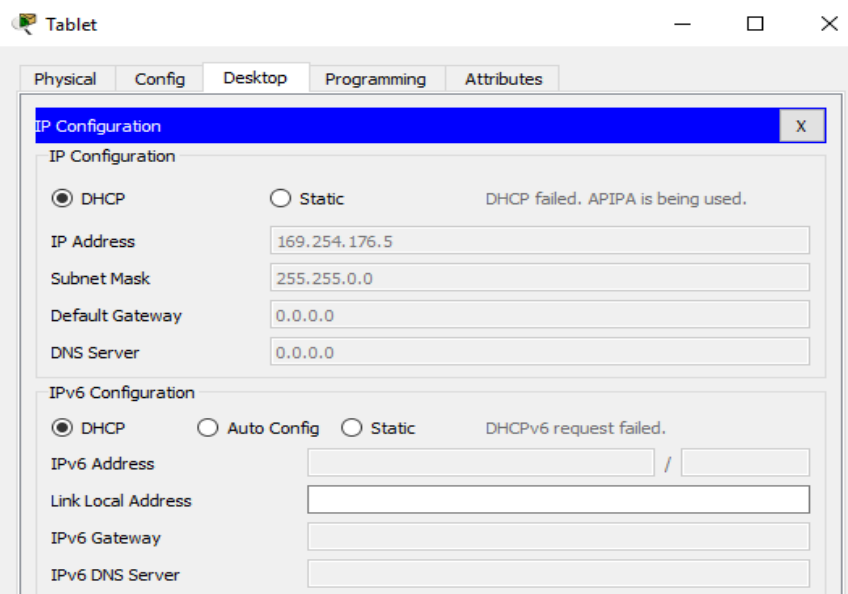
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



- c. Ahora, **Home Laptop** debe tener una configuración IP completa. De no ser así, vuelva al paso 2 y verifique las configuraciones en la **WRS**.
- d. Cierre la ventana IP Configuration y, a continuación, cierre la ventana **Home Laptop**.

Paso 4: Solicitar direccionamiento DHCP para la tablet PC

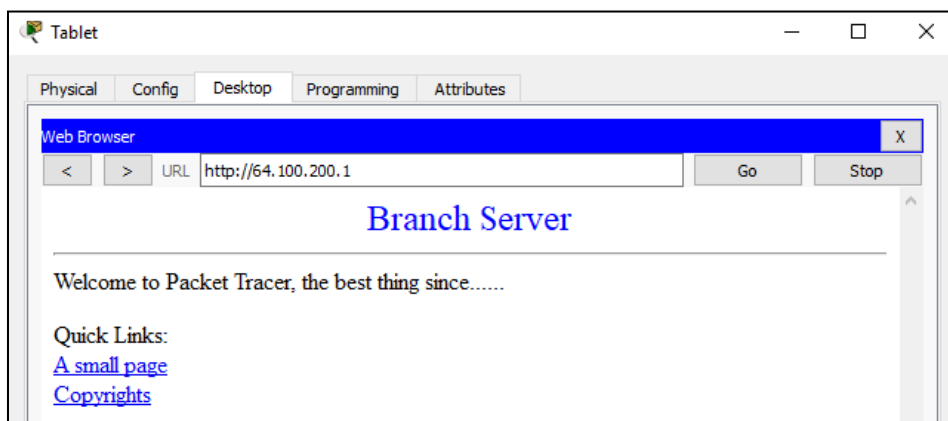
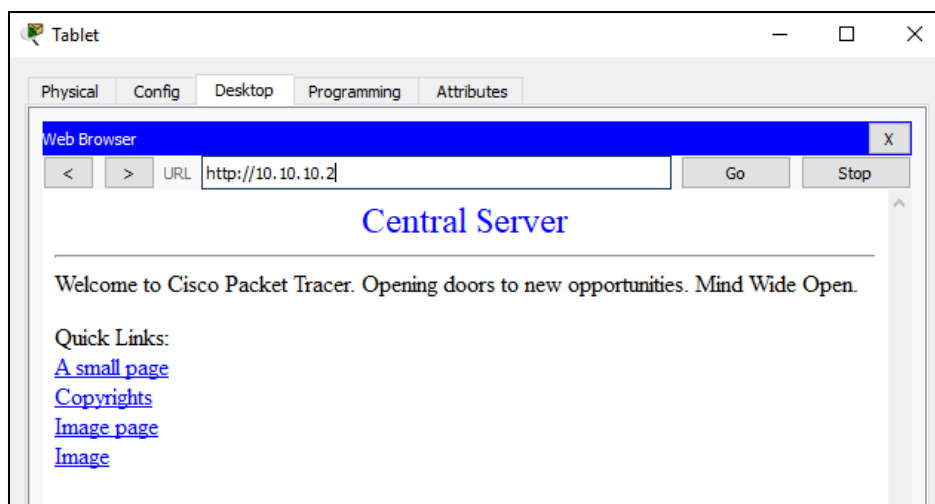
- a. Haga clic en **Tablet** y, a continuación, haga clic en la ficha **Desktop > IP Configuration**.
- b. Haga clic en **DHCP** y espere hasta que la solicitud de DHCP sea correcta.



- c. Ahora, **Tablet** debe tener una configuración IP completa. De no ser así, vuelva al paso 2 y verifique las configuraciones en la **WRS**.

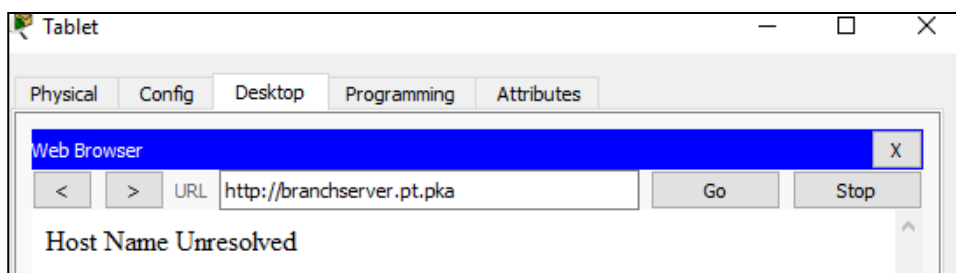
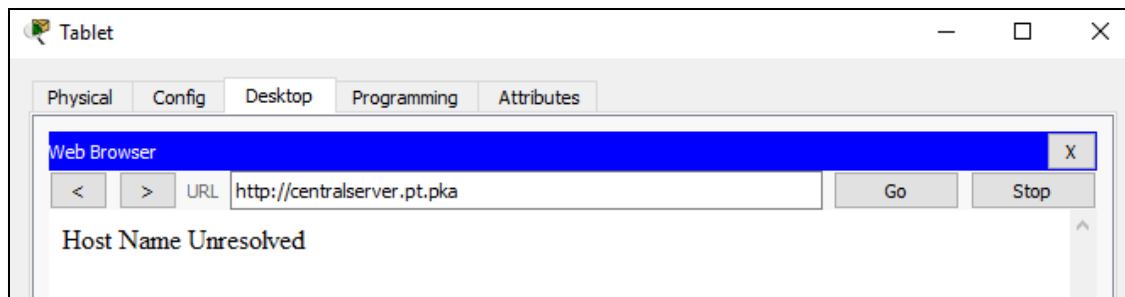
Paso 5: Probar el acceso a sitios Web

- a. Cierre la ventana **IP Configuration** y, a continuación, haga clic en Web Browser (Explorador Web).
- b. En el cuadro de dirección URL, escriba **10.10.10.2** (para el sitio Web de **CentralServer**) o **64.100.200.1** (para el sitio web de **BranchServer**) y haga clic en **Go** (Ir). Deben aparecer ambos sitios Web.



- c. Vuelva a abrir el explorador Web. Pruebe los nombres para esos mismos sitios Web mediante la introducción de **centralserver.pt.pka** y **branchserver.pt.pka**. Haga clic en **Fast Forward Time** (Adelantar el tiempo) en la barra amarilla que se encuentra debajo de la topología, a fin de acelerar el proceso.

Con los nombres no genera conexión al sitio.

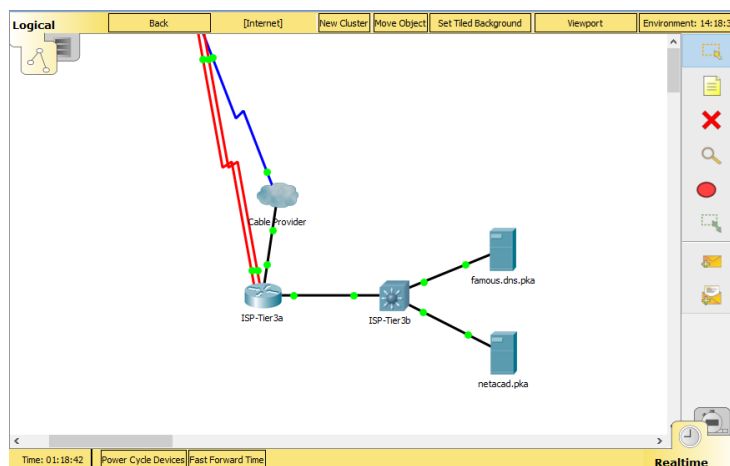


Parte 2: Configurar los registros en el servidor DNS

Paso 1: Configurar famous.dns.pka con registros para CentralServer y BranchServer.

En general, los registros DNS se realizan ante compañías, pero en esta actividad, usted controla el servidor **famous.dns.pka** en Internet.

- a. Haga clic en la nube de **Internet**. Se muestra una nueva red.

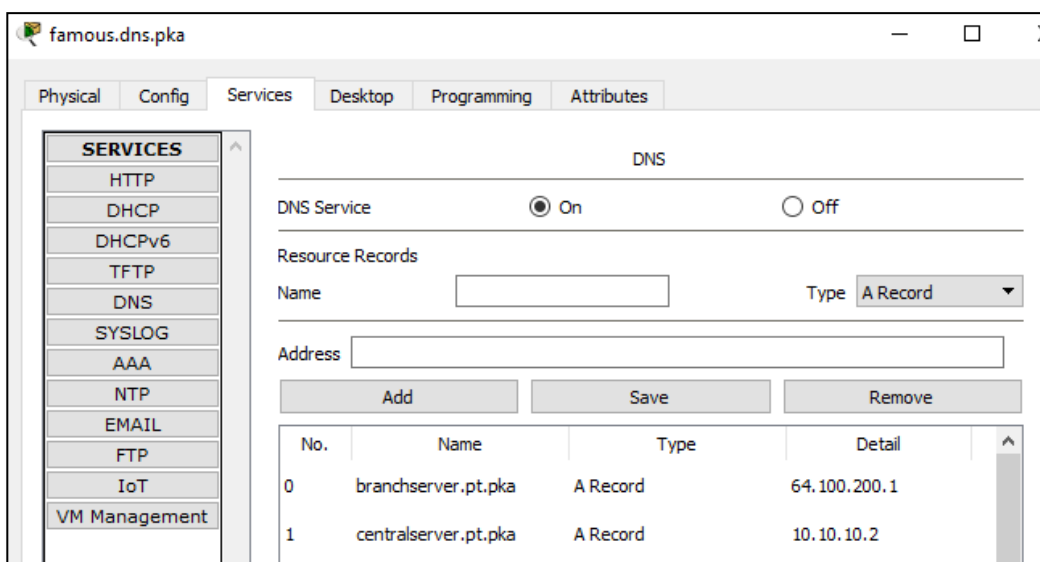


ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- b. Haga clic en **famous.dns.pka** y, a continuación, haga clic en la ficha **Config > DNS**. c. Agregue los siguientes registros del recurso:

Nombre de registro del recurso	Dirección
centralserver.pt.pka	10.10.10.2.
branchserver.pt.pka	64.100.200.1

- d. Cierre la ventana famous.dns.pka.



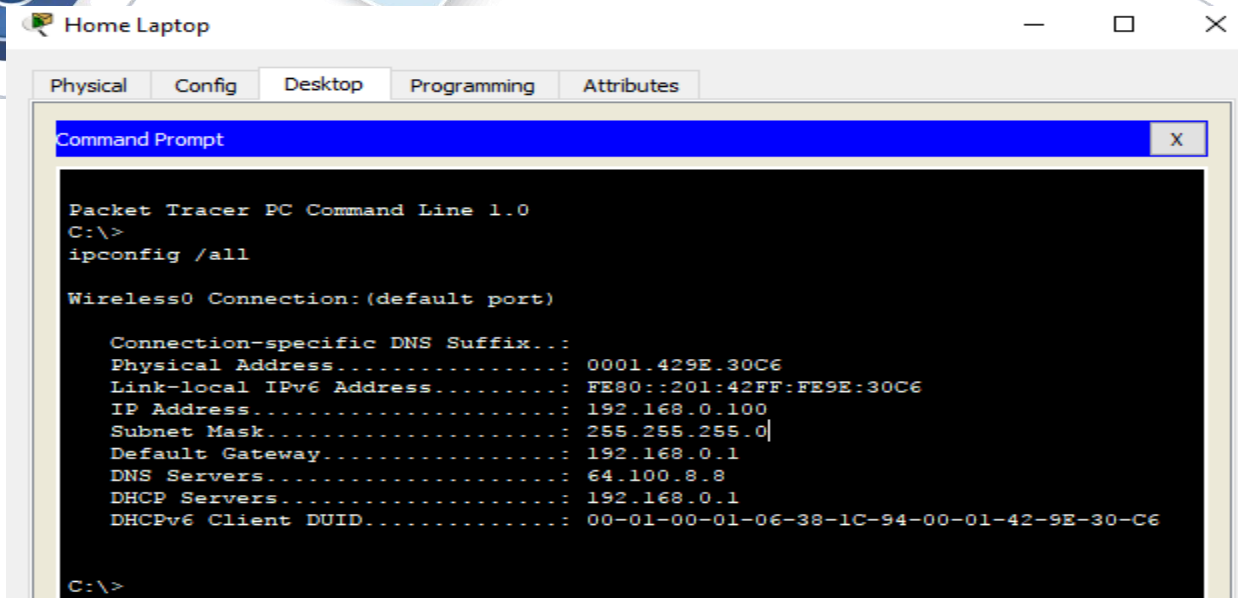
- e. Haga clic en **Back** (Atrás) para salir de la nube de **Internet**.

Paso 2: Verificar la capacidad de los equipos cliente para usar DNS

Ahora que configuró los registros DNS, **Home Laptop** y **Tablet** deben ser capaces de acceder a los sitios Web mediante los nombres en lugar de las direcciones IP. Primero, compruebe que el cliente DNS funcione correctamente y, a continuación, verifique el acceso al sitio Web.

- Haga clic en **Home Laptop** o **Tablet**.
- Si el explorador Web está abierto, ciérralo y seleccione **Command Prompt** (Símbolo del sistema).
- Verifique el direccionamiento IPv4 mediante la introducción del comando `ipconfig /all`. Debe ver la dirección IP del servidor DNS.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



```

Home Laptop
Physical Config Desktop Programming Attributes
Command Prompt X
Packet Tracer PC Command Line 1.0
C:\>
ipconfig /all

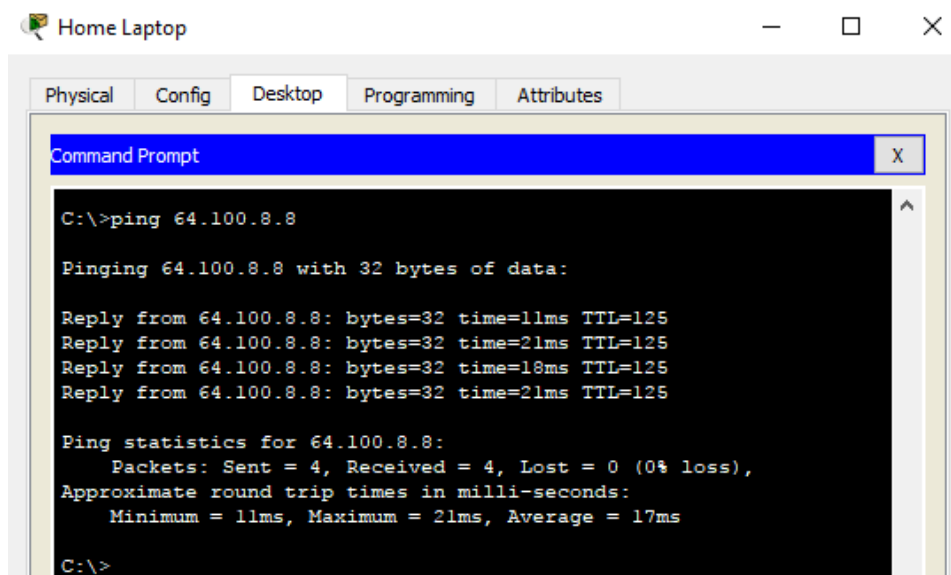
Wireless0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0001.429E.30C6
Link-local IPv6 Address.....: FE80::201:42FF:FE9E:30C6
IP Address.....: 192.168.0.100
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.0.1
DNS Servers.....: 64.100.8.8
DHCP Servers.....: 192.168.0.1
DHCPv6 Client DUID.....: 00-01-00-01-06-38-1C-94-00-01-42-9E-30-C6

C:\>

```

- d. Haga ping al servidor DNS en **64.100.8.8** para verificar la conectividad.



```

Home Laptop
Physical Config Desktop Programming Attributes
Command Prompt X
C:\>ping 64.100.8.8

Pinging 64.100.8.8 with 32 bytes of data:

Reply from 64.100.8.8: bytes=32 time=11ms TTL=125
Reply from 64.100.8.8: bytes=32 time=21ms TTL=125
Reply from 64.100.8.8: bytes=32 time=18ms TTL=125
Reply from 64.100.8.8: bytes=32 time=21ms TTL=125

Ping statistics for 64.100.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 21ms, Average = 17ms

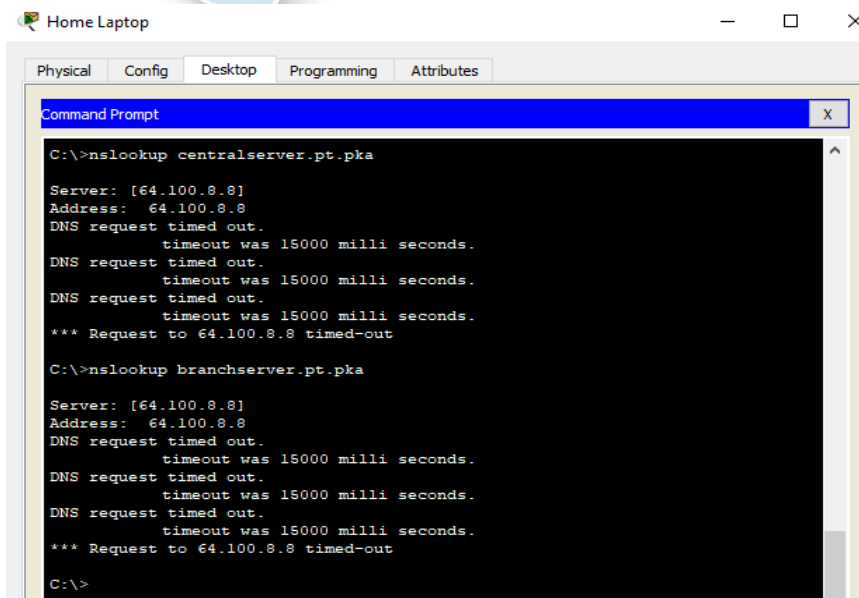
C:\>

```

Nota: es posible que los primeros dos o tres pings fallen, ya que Packet Tracer simula los distintos procesos que deben ocurrir para que la conectividad a un recurso remoto sea correcta.

- e. Pruebe la funcionalidad del servidor DNS mediante la introducción de los comandos `nslookup centralserver.pt.pka` y `nslookup branchserver.pt.pka`. Debe obtener una resolución de nombre que muestre la dirección IP de cada uno.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



```

C:\>nslookup centralserver.pt.pka

Server: [64.100.8.8]
Address: 64.100.8.8
DNS request timed out.
        timeout was 15000 milli seconds.
DNS request timed out.
        timeout was 15000 milli seconds.
DNS request timed out.
        timeout was 15000 milli seconds.
*** Request to 64.100.8.8 timed-out

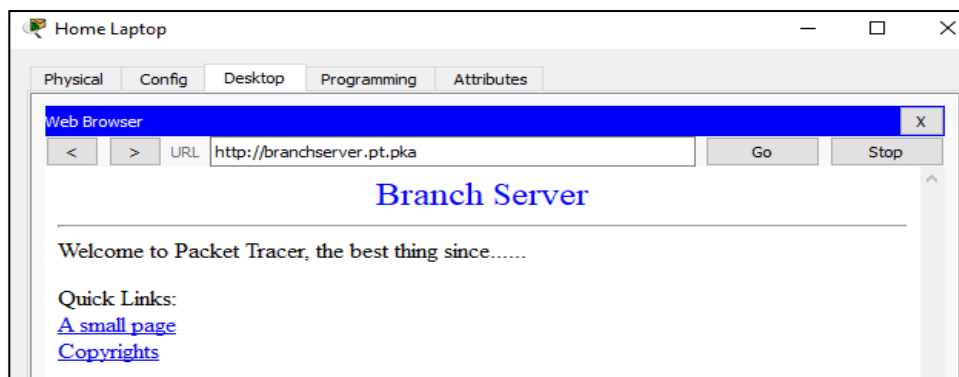
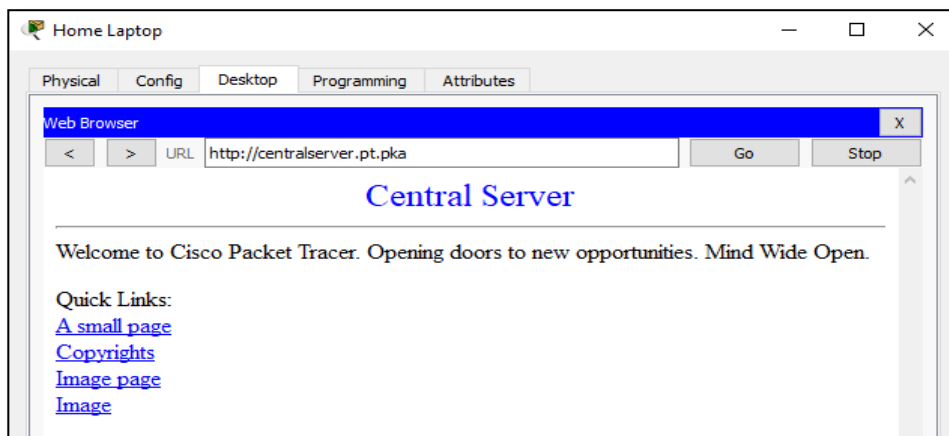
C:\>nslookup branchserver.pt.pka

Server: [64.100.8.8]
Address: 64.100.8.8
DNS request timed out.
        timeout was 15000 milli seconds.
DNS request timed out.
        timeout was 15000 milli seconds.
DNS request timed out.
        timeout was 15000 milli seconds.
*** Request to 64.100.8.8 timed-out

C:\>

```

- f. Cierre la ventana Command Prompt y haga clic en **Web Browser**. Verifique que **Home Laptop** o **Tablet** puedan acceder ahora a las páginas Web de **CentralServer** y **BranchServer**.



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Cisco Packet Tracer - D:\UNAD\CISCO\Trabajo Colaborativo No 2\CCNA1 R&S UNIDAD 2\10.2.2.8 Packet Tracer - DNS and DHCP.pka

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 02:11:39

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

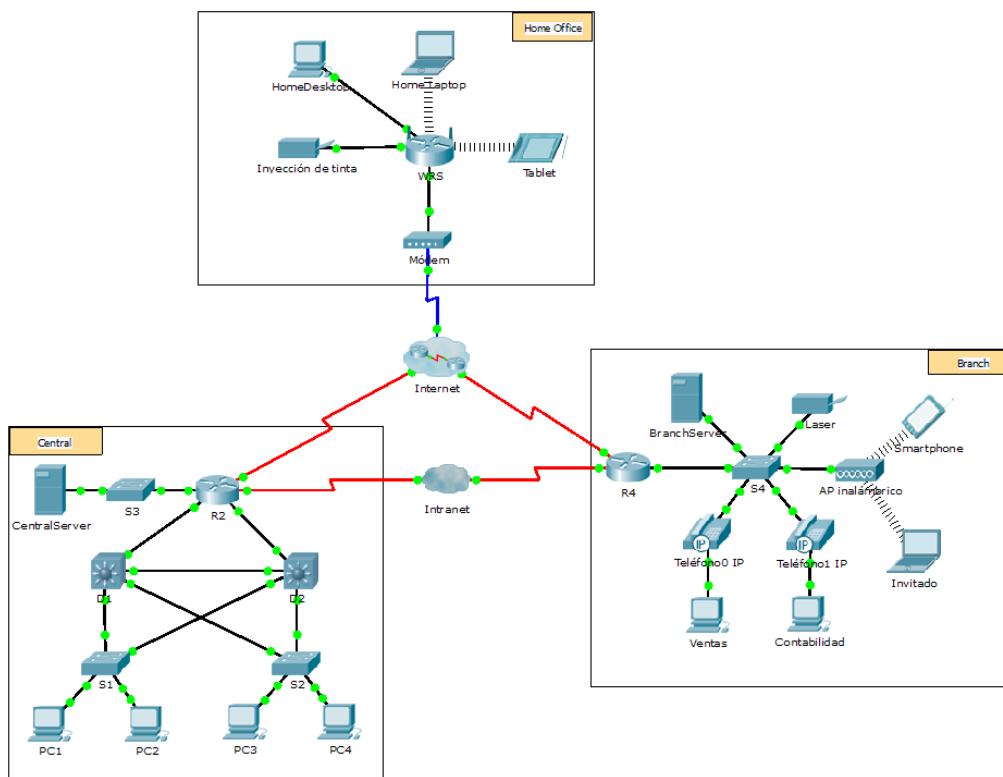
Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
famous.dns.pka				
DNS Server				
Resource Records				
branchserver.pt.pka		0	PT Server Configuration	
A Records		0	IP	
Address	Correct	12	PT Server Configuration	
centralserver.pt.pka		0	PT Server Configuration	
A Records		0	IP	
Address	Correct	12	PT Server Configuration	
Home Laptop				
Default Gateway	Correct	2	Client DHCP Configuration	
DNS Server IP	Correct	2	Client DHCP Configuration	
Ports				
Wireless0				
IP Address	Correct	2	Client DHCP Configuration	
Subnet Mask	Correct	2	Client DHCP Configuration	
Tablet				
Default Gateway	Correct	2	Client DHCP Configuration	
DNS Server IP	Correct	2	Client DHCP Configuration	
Ports				
Wireless0				
IP Address	Correct	2	Client DHCP Configuration	
Subnet Mask	Correct	2	Client DHCP Configuration	
WRS				
DHCP Server				
DHCP Enable	Correct	8	Linksys DHCP Configuration	
Pools				
Pool linksysPool				
Default Gat...	Correct	8	Linksys DHCP Configuration	
DNS server ...	Correct	8	Linksys DHCP Configuration	
Start IP add...	Correct	8	Linksys DHCP Configuration	
Subnet mask	Correct	8	Linksys DHCP Configuration	

Component	Items/Total	Score
Client DHCP Configuration	8/8	16/16
Linksys DHCP Configuration	5/5	40/40
PT Server Configuration	2/2	24/24

Score : 80/80
Item Count : 15/15

Ejercicio 10.2.3.2: Servidores FTP



Objetivos

Parte 1: Configurar servicios FTP en los servidores

Parte 2: Subir un archivo al servidor FTP

Parte 3: Descargar un archivo del servidor FTP

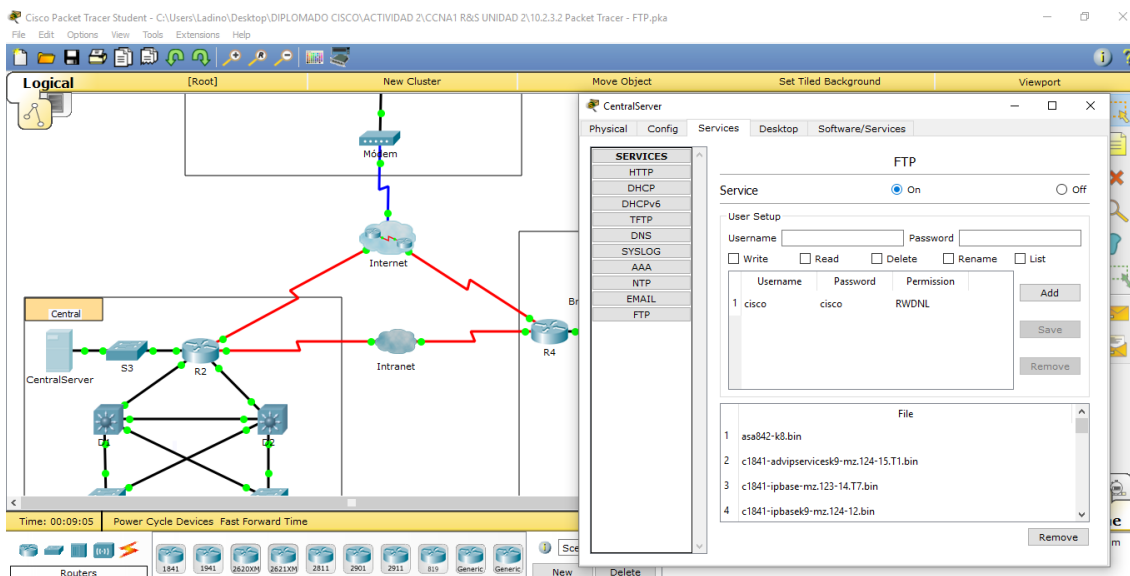
Información básica

En esta actividad, configurará servicios FTP. Luego, utilizará los servicios FTP para transferir archivos entre los clientes y el servidor.

Nota: Packet Tracer simula solamente el proceso para configurar estos servicios. Cada paquete de software de servidor y cliente FTP tiene sus propias instrucciones exclusivas de configuración e instalación. La primera vez que intente conectarse a una dirección Web, Packet Tracer tardará varios

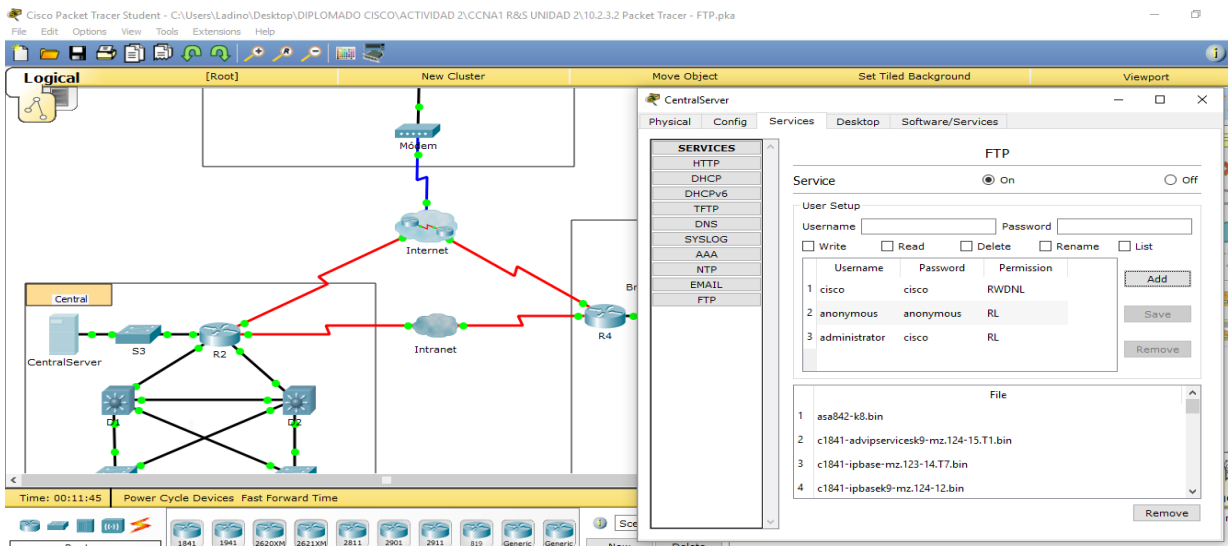
Parte 1: Configurar servicios FTP en los servidores
Paso 1: Configurar el servicio FTP en CentralServer

- a. Haga clic en **CentralServer** > ficha **Config** > **FTP**.
- b. Haga clic en **On** (Activar) para habilitar el servicio FTP.



c. En **User Setup** (Configuración de usuario), cree las siguientes cuentas de usuario. Haga clic en el botón **+** para agregar la cuenta:

Nombre de usuario	Contraseña	Permisos
anonymous	anonymous	limitado a Read (Lectura) y List (Lista)
administrator	cisco	permiso total



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- e. Haga clic en la cuenta de usuario **cisco** predeterminada y, a continuación, haga clic en el botón - para eliminarla. Cierre la ventana de configuración de la CentralServer.

The screenshot shows the Cisco Packet Tracer interface with the 'CentralServer' configuration window open. The 'Services' tab is selected, and the 'FTP' service is configured. The 'User Setup' table is as follows:

Username	Password	Permission
1 anonymous	anonymous	RL
2 administrator	cisco	RWDNL

The 'File' list contains the following items:

- 1 asa842-k8.bin
- 2 c1841-advipservicesk9-mz.124-15.T1.bin
- 3 c1841-ipbase-mz.123-14.T7.bin
- 4 c1841-ipbasek9-mz.124-12.bin

Paso 2: Configurar el servicio FTP en BranchServer
Repita el paso 1 en **BranchServer**

The screenshot shows the Cisco Packet Tracer interface with the 'BranchServer' configuration window open. The 'Services' tab is selected, and the 'FTP' service is configured. The 'User Setup' table is as follows:

Username	Password	Permission
1 anonymous	anonymous	RL
2 administrator	cisco	RWDNL

The 'File' list contains the following items:

- 1 asa842-k8.bin
- 2 c1841-advipservicesk9-mz.124-15.T1.bin
- 3 c1841-ipbase-mz.123-14.T7.bin
- 4 c1841-ipbasek9-mz.124-12.bin

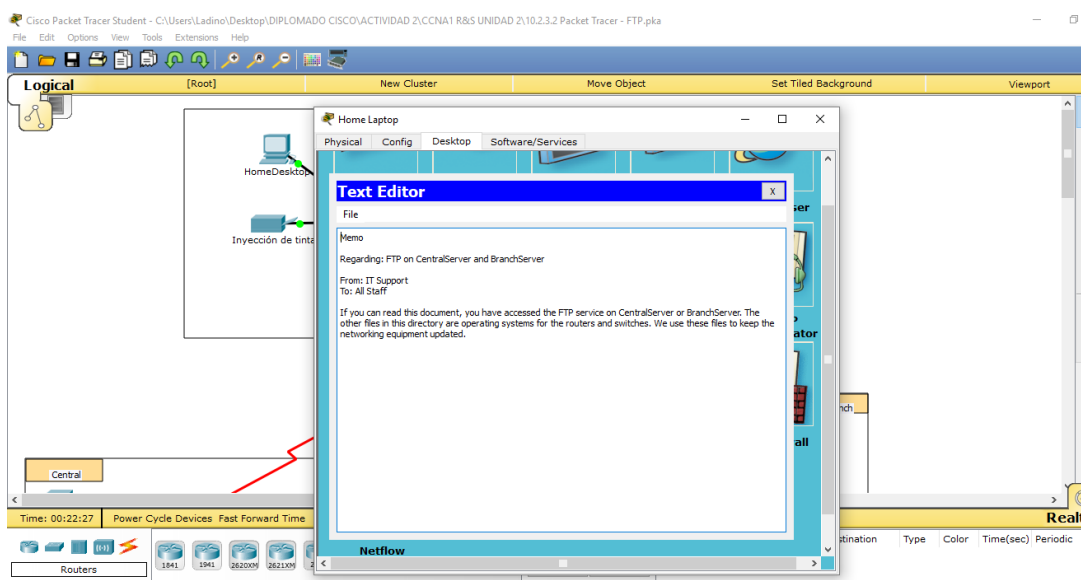
Parte 2: Subir un archivo al servidor FTP

Paso 1: Transferir el archivo README.txt de la computadora portátil doméstica a CentralServer

Como administrador de red, debe colocar un aviso en los servidores FTP. El documento se creó en la computadora portátil doméstica y se debe subir a los servidores FTP.

- Haga clic en **Home Laptop** (Computadora portátil doméstica) y, a continuación, haga clic en la ficha **Desktop > Text Editor** (Escritorio > Editor de texto).
- Abra el archivo **README.txt** y revíselo. Cierre **Text Editor** cuando haya terminado.

Nota: no modifique el archivo porque esto afecta la puntuación.



- En la ficha **Desktop**, abra la ventana del símbolo del sistema y siga estos pasos: 1) Escriba `ftp centralserver.pt.pka`. Espere algunos segundos mientras se conecta el cliente.

Nota: dado que Packet Tracer es una simulación, FTP puede tardar hasta 30 segundos en conectarse la primera vez.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

The screenshot shows the Cisco Packet Tracer interface. On the left, a network topology is visible with a central router connected to an Internet cloud. A 'Home Office' cluster contains a Home Desktop, Home Laptop, Inyección de tinta, and Tablet, all connected to a central switch (W/S). A Modem is connected to the switch and the Internet. On the right, a 'Home Laptop' window is open, displaying a Command Prompt with the following text:

```
Packet Tracer PC Command Line 1.0
PC>ftp centralserver.pt.pka
Trying to connect...centralserver.pt.pka
```

The interface also shows a 'Logical' view at the top, a 'Central' view at the bottom, and a 'Scenario 0' dropdown menu.

This screenshot is similar to the one above, but the Command Prompt window now displays an error message:

```
Packet Tracer PC Command Line 1.0
PC>ftp centralserver.pt.pka
Trying to connect...centralserver.pt.pka
Could not open connection to the host, on port 21: Connect failed
PC>
```

The network topology and interface elements are identical to the previous screenshot.

2) El servidor pide un nombre de usuario y una contraseña. Utilice las credenciales de la cuenta **administrator** (administrador).

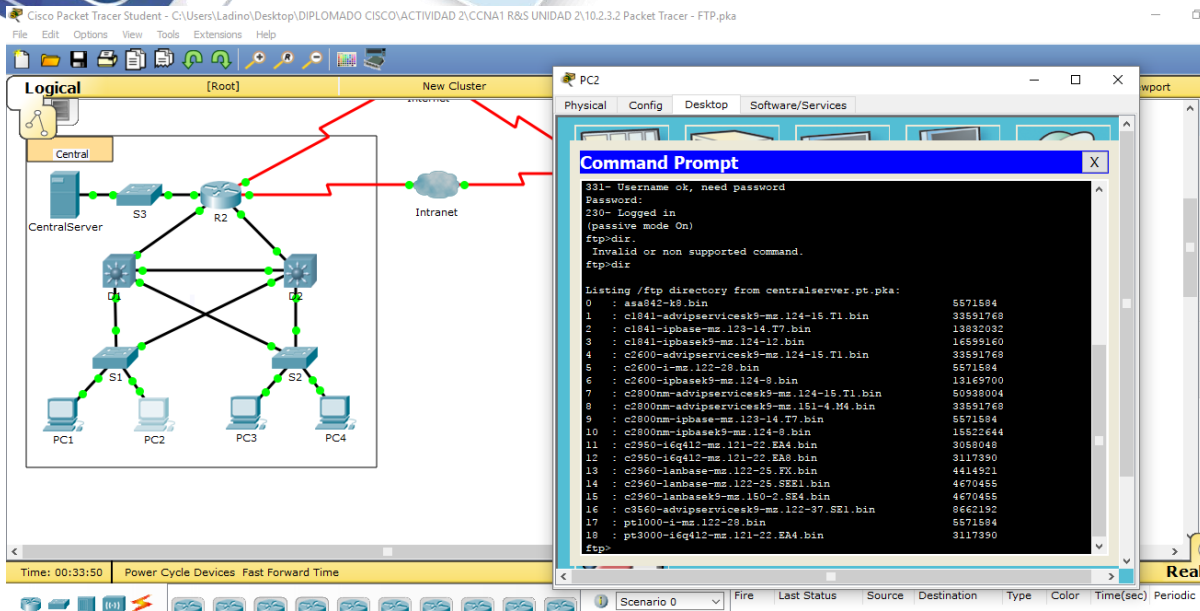
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Time: 00:29:54 Power Cycle Devices Fast Forward Time

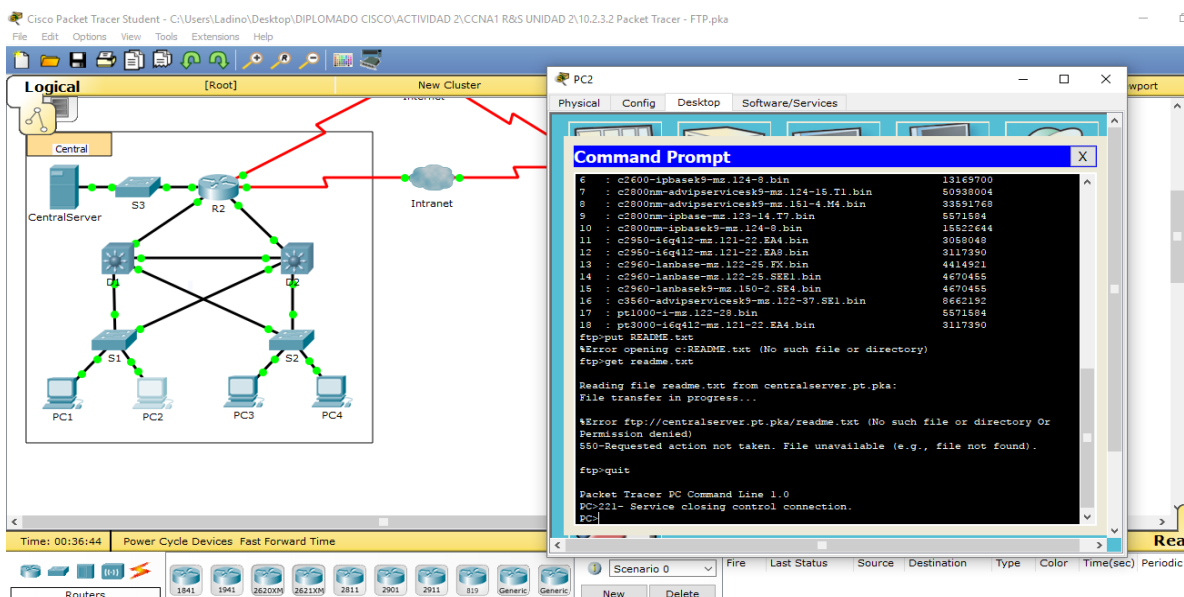
Time: 00:32:43 Power Cycle Devices Fast Forward Time

3) La petición de entrada cambia a ftp>. Enumere el contenido del directorio escribiendo dir. Se muestra el directorio de archivos en **CentralServer**.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



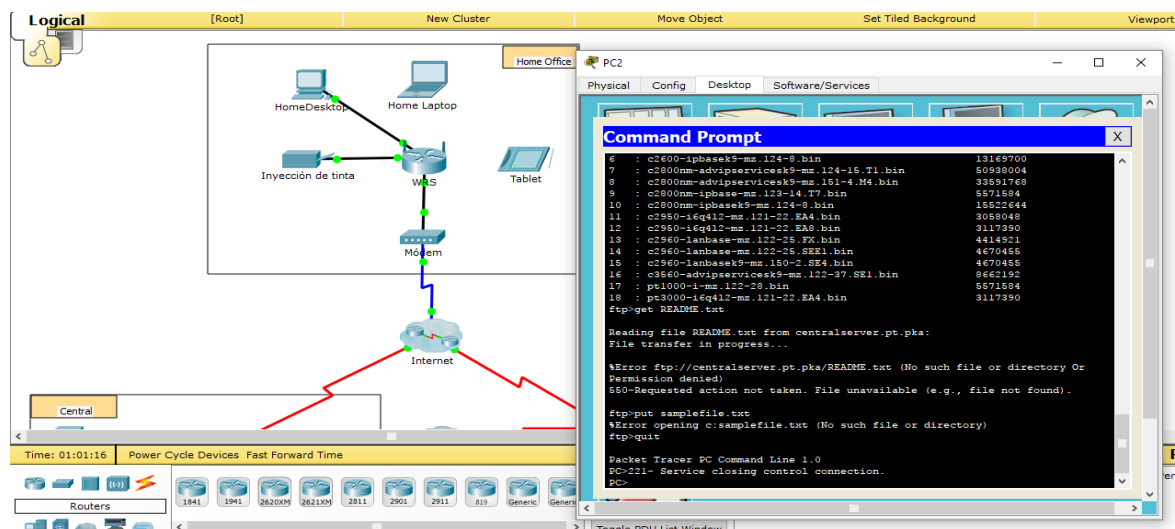
- 4) Transfiera el archivo README.txt: en la petición de entrada ftp>, escriba **put README.txt**. El archivo README.txt se transfiere de la computadora portátil doméstica a **CentralServer**.
- 5) Para verificar la transferencia del archivo, escriba **dir**. El archivo README.txt ahora figura en el directorio de archivos.
- 6) Cierre el cliente FTP escribiendo **quit**. La petición de entrada se revierte a PC>.



- Paso 2: Transferir el archivo README.txt de la computadora portátil doméstica a BranchServer**
- a. Repita el paso 1c para transferir el archivo README.txt a branchserver.pt.pka.
 - b. Cierre las ventanas Command Prompt (Símbolo del sistema) y Home Laptop.
- Parte 3: Descargar un archivo del servidor FTP**
- Paso 1: Transferir README.txt de CentralServer a la PC2**
- a. Haga clic en PC2 y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**. 1) Escriba **ftp centralserver.pt.pka**.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- 2) El servidor pide un nombre de usuario y una contraseña. Utilice las credenciales de la cuenta **anonymous** (anónimo)
- 3) La petición de entrada cambia a `ftp>`. Enumere el contenido del directorio escribiendo `dir`. El archivo `README.txt` figura en la parte superior de la lista del directorio.
- 4) Descargue el archivo `README.txt`: en la petición de entrada `ftp>`, escriba `get README.txt`. El archivo `README.txt` se transfiere a la **PC2**.
- 5) Verifique que la cuenta **anonymous** no tenga permiso para escribir archivos en **CentralServer** escribiendo `put sampleFile.txt`. Se muestra el siguiente mensaje de error:



```
Writing file sampleFile.txt to centralserver.pt.pka:
File transfer in progress...
%Error ftp://centralserver.pt.pka/sampleFile.txt (No such file or directory Or
Permission denied)
550-Requested action not taken. permission denied).
```

- 6) Cierre el cliente FTP escribiendo `quit`. La petición de entrada se revierte a `PC>`.
- 7) Para verificar la transferencia del archivo a la PC2, escriba `dir`. El archivo `README.txt` figura en el directorio.
- 8) Cierre la ventana de línea de comandos.
 - b. En la ficha **Desktop**, abra **Text Editor** y, a continuación, el archivo **README.txt** para verificar la integridad del archivo.
 - c. Cierre **Text Editor** y, luego, cierre la ventana de configuración de la PC2.

Paso 2: Transferir el archivo README.txt de BranchServer al smartphone

Repita el paso 1 para **Smart Phone**, excepto la descarga del archivo `README.txt` desde **branchserver.pt.pka**.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Cisco Packet Tracer Student - C:\Users\Ladino\Desktop\DIPLOMADO CISCO\ACTIVIDAD 2\CCNA1 R&S UNIDAD 2\10.2.3.2 Packet Tracer - FTP.pka

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 01:07:25

You did not complete the activity. Please close this window and try again.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
BranchServer				
FTP Server				
FTP Enable	Correct	4	PT Server Con...	
Server Files	0	0	Ip	
README.txt	Incorrect	5	FTP File Transe...	
User Accounts				
Account administrator				
User Name	Correct	6	PT Server Con...	
User Password	Correct	6	PT Server Con...	
User Permis...	Correct	6	PT Server Con...	
Account anonymous				
User Name	Correct	6	PT Server Con...	
User Password	Correct	6	PT Server Con...	
User Permis...	Correct	6	PT Server Con...	
CentralServer				
FTP Server				
FTP Enable	Correct	4	PT Server Con...	
Server Files	0	0	Ip	
README.txt	Incorrect	5	FTP File Transe...	
User Accounts				
Account administrator				
User Name	Correct	6	PT Server Con...	
User Password	Correct	6	PT Server Con...	
User Permis...	Correct	6	PT Server Con...	
Account anonymous				
User Name	Correct	6	PT Server Con...	
User Password	Correct	6	PT Server Con...	
User Permis...	Correct	6	PT Server Con...	
PC2				
Files				
C Directory				
README.txt	Incorrect	5	FTP File Transe...	

Score : 80/95
Item Count : 14/17

Component	Items/Total	Score
FTP File Transfer	0/3	0/15
PT Server Configuration	14/14	80/80

Close

Ejercicio 10.4.1.2: Función Multiusuario de Packet Tracer: Tutorial

Topología

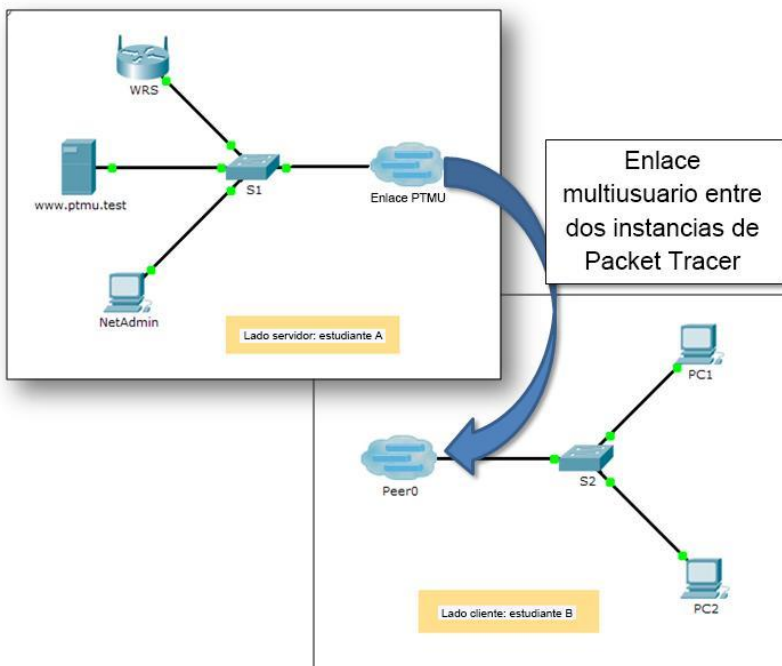


Tabla de direccionamiento

Dispositivo	Dirección IP	Máscara de subred	Servidor DNS
www.ptmu.test	10.10.10.1	255.0.0.0	10.10.10.1
PC	10.10.10.10	255.0.0.0	10.10.10.1

Objetivos

Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

Parte 2: Verificar la conectividad a través de una conexión multiusuario local

Información básica

La característica Multiusuario de Packet Tracer permite varias conexiones punto a punto entre diversas instancias de Packet Tracer. Esta primera actividad de la función Multiusuario de Packet Tracer (PTMU, Packet Tracer Multiuser) es un tutorial rápido que muestra los pasos para establecer y verificar una conexión multiusuario a otra instancia de Packet Tracer dentro de la misma LAN. Idealmente, esta actividad está pensada para dos estudiantes. Sin embargo, también se puede realizar como actividad individual abriendo los dos archivos independientes para crear dos instancias distintas de Packet Tracer en su máquina local.

Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

Paso 1: Seleccionar un compañero y determinar el rol para cada estudiante

- Busque un compañero de clase con el que cooperará para realizar esta actividad. Ambas PC deben estar conectadas a la misma LAN.
- Determinen quién desempeñará la función del lado servidor y quién desempeñará la función del lado cliente en esta actividad.

El jugador del lado servidor abre el archivo **Packet Tracer Multiuser - Tutorial - Server Side.pka**.

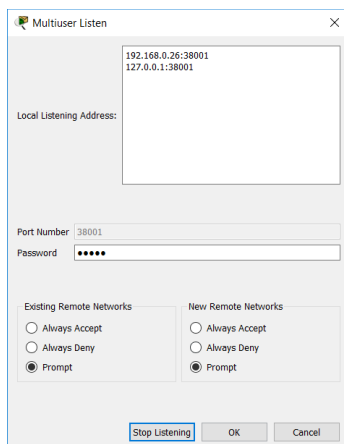
El jugador del lado cliente abre el archivo **Packet Tracer Multiuser - Tutorial - Client Side.pka**.

Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

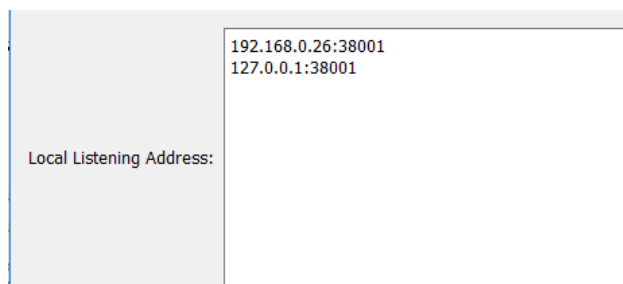
Paso 2: Jugador del lado servidor: configurar el lado servidor del enlace PTMU

El jugador del lado cliente debe contar con la dirección IP, el número de puerto y la contraseña utilizados por el jugador del lado servidor para poder crear una conexión con el jugador del lado servidor.

- a. Siga estos pasos para configurar Packet Tracer de manera de que esté preparado para recibir una conexión entrante:
 - 1) Haga clic en el menú **Extensions** (Extensiones), después en **Multiuser** (Multiusuario) y, finalmente, en **Listen** (Escuchar).



- 2) Tiene dos Local Listening Addresses (Direcciones de escucha locales). Si se indican más de dos direcciones, utilice solo las primeras dos. La primera es la dirección IP real de la máquina local del jugador del lado servidor. Es la dirección IP que utiliza su PC para enviar y recibir datos. La otra dirección IP (127.0.0.1) solamente se puede utilizar para comunicaciones dentro del entorno de su propia PC.



- 3) El número de puerto se indica junto a las direcciones IP y en el campo Port Number (Número de puerto). Si esta es la primera instancia de Packet Tracer que abrió en la PC, el número de puerto será 38000. Sin embargo, si hay varias instancias abiertas, el número aumenta de a uno por cada instancia (38001, 38002, etcétera). El número de puerto es necesario para que el jugador del lado cliente configure la conexión multiusuario.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Port Number 38001

- 4) La contraseña está establecida en **cisco** de manera predeterminada. Puede cambiarla, pero no es necesario hacerlo para esta actividad.

Password ●●●●●

- 5) Comuníquese al jugador del lado cliente su dirección IP, número de puerto y contraseña. El jugador del lado cliente necesitará estos tres datos para conectarse a su instancia de Packet Tracer en el paso 3.
- 6) En la sección **Existing Remote Networks** (Redes remotas existentes), debe hacer clic en el botón de opción **Always Accept** (Aceptar siempre) o **Prompt** (Preguntar) para que el jugador del lado cliente se conecte de forma correcta.

Existing Remote Networks

Always Accept

Always Deny

Prompt

- 7) En la sección **New Remote Networks** (Nuevas redes remotas), confirme que el botón de opción **Always Deny** (Denegar siempre) esté habilitado. Esto evitará que el jugador del lado cliente cree un nuevo enlace no especificado en esta actividad.

New Remote Networks

Always Accept

Always Deny

Prompt

- 8) Haga clic en **OK** (Aceptar).

- b. Haga clic en el ícono **Multiuser Connection** (Conexión multiusuario, representado con una nube con tres líneas). Luego haga clic en el ícono **Remote Network** (Red remota) y agregue una **red remota** a la topología.

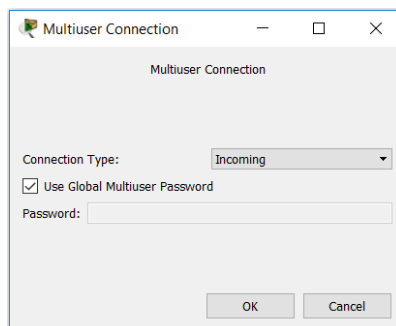


Server Side - Student A

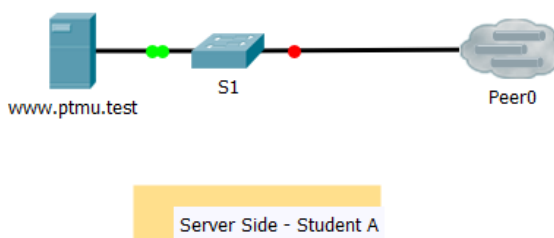
- c. Haga clic en el nombre **Peer0** y cámbielo por **Enlace PTMU** (distingue mayúsculas de minúsculas).

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- d. Haga clic en la nube del **Enlace PTMU** y verifique que en Connection Type (Tipo de conexión) diga **Incoming** (Entrante) y que la casilla de verificación **Use Global Multiuser Password** (Utilizar contraseña de multiusuario global) esté habilitada.



- e. Haga clic en el ícono **Connections** (Conexiones) y elija la conexión negro sólido **Copper Straight-Through** (cable de cobre de conexión directa).
- f. Haga clic en el **S1** y elija la conexión GigabitEthernet0/1. A continuación, haga clic en **Enlace PTMU > Create New Link** (Crear nuevo enlace).



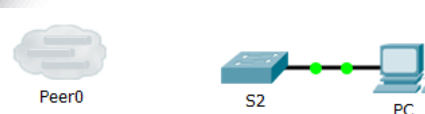
Paso 3: Jugador del lado cliente: configurar el lado cliente del enlace PTMU

- a. Registre la siguiente información que le suministró el jugador del lado servidor:
Dirección IP: **192.168.90.26**

Número de puerto: **38001**

Contraseña (**cisco**, de manera predeterminada): **cisco**
- b. El jugador del lado cliente debe agregar una **red remota** a la topología mediante las siguientes instrucciones: haga clic en el ícono **Multiuser Connection** (representado con una nube con tres líneas). Luego haga clic en el ícono **Remote Network** (Red remota) y agregue una **red remota** a la topología.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

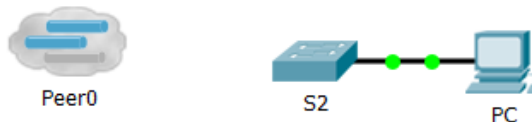


Client Side - Student B

- c. Haga clic en la nube de **Peer0** y cambie Connection Type por **Outgoing** (Saliente).
- 1) En el campo Peer Address (Dirección del punto), introduzca la dirección IP del lado servidor que registró en el paso 3a.
 - 2) En el campo Peer Port Number (Número de puerto del punto), introduzca el número de puerto del lado servidor que registró en el paso 3a.
 - 3) En el campo Peer Network Name (Nombre de red del punto), introduzca **Enlace PTMU**. Este campo distingue mayúsculas de minúsculas.
 - 4) En el campo Password (Contraseña), introduzca **cisco** o la contraseña que haya configurado el jugador del lado servidor.

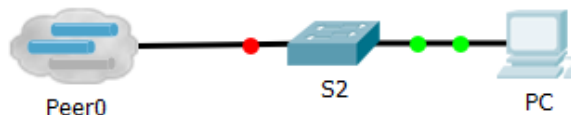
- 5) Haga clic en **Connect** (Conectar).
- d. La nube de **Peer0** ahora debería ser amarilla, lo que indica que las dos instancias de Packet Tracer están conectadas.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



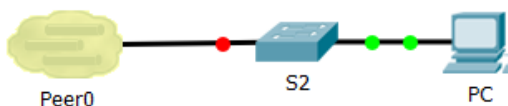
Client Side - Student B

- e. Haga clic en el ícono **Connections** (Conexiones) y elija la conexión negro sólido **Copper Straight-Through** (cable de cobre de conexión directa).
- f. Haga clic en el **S2** y elija la conexión **GigabitEthernet0/1**. A continuación, haga clic en **Peer0 > Link 0 (S1 GigabitEthernet 0/1)**.

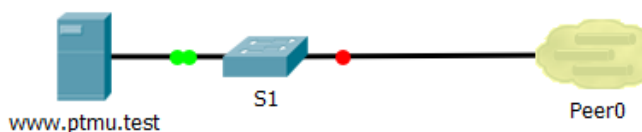


Client Side - Student B

Tanto la nube de **Peer0** del jugador del lado cliente como la nube de **Enlace PTMU** del jugador del lado servidor ahora deben ser azules. Después de un período breve, la luz de enlace entre el switch y la nube pasa de color ámbar a verde.



Client Side - Student B



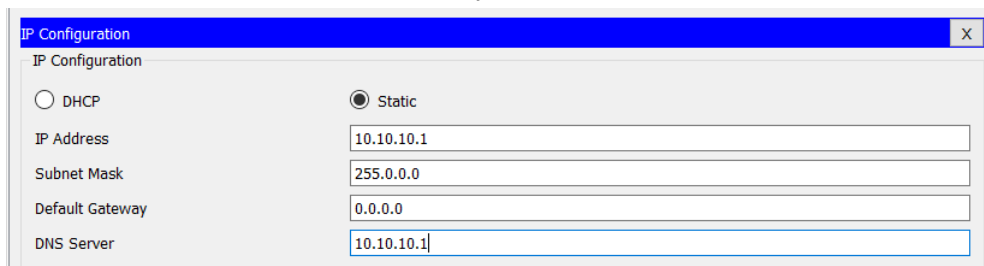
Server Side - Student A

El enlace de multiusuario está establecido y listo para probar.

Parte 2: Verificar la conectividad a través de una conexión multiusuario local

Paso 1: Configurar el direccionamiento IP

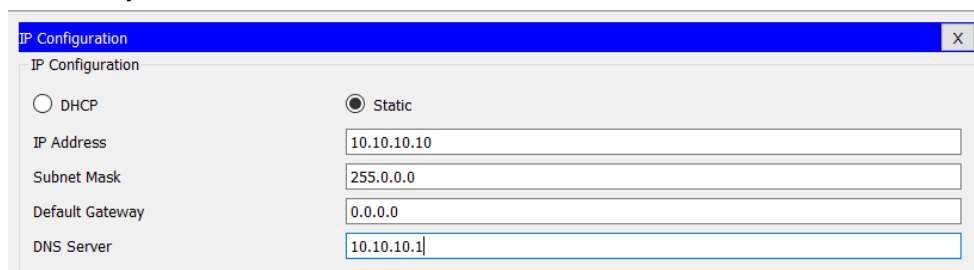
- i. El jugador del lado servidor configura el servidor de **www.ptmu.test** con la dirección IP **10.10.10.1**, la máscara de subred **255.0.0.0** y la dirección de servidor DNS **10.10.10.1**.



The screenshot shows the 'IP Configuration' window with the following settings:

Field	Value
IP Configuration	Static
IP Address	10.10.10.1
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
DNS Server	10.10.10.1

- j. El jugador del lado cliente configura la PC con la dirección IP **10.10.10.10**, la máscara de subred **255.0.0.0** y la dirección de servidor DNS **10.10.10.1**.



The screenshot shows the 'IP Configuration' window with the following settings:

Field	Value
IP Configuration	Static
IP Address	10.10.10.10
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
DNS Server	10.10.10.1

Paso 2: Verificar la conectividad y acceder a una página Web desde el lado servidor

- a. El jugador del lado servidor ahora debe poder hacer ping a la PC en la instancia de Packet Tracer del jugador del lado cliente.
- b. El jugador del lado cliente ahora debe poder hacer ping al servidor de **www.ptmu.test**.
- c. El jugador del lado cliente también debe poder abrir el explorador Web y acceder a la página Web en **www.ptmu.test**. ¿Qué se muestra en la página Web?

Congratulations! You successfully verified a Packet Tracer multiuser connection (Felicidades. Verificó correctamente una conexión multiusuario de Packet Trac.

Ejercicio 10.4.1.3 Función Multiusuario de Packet Tracer: Implementación de servicios

Topología

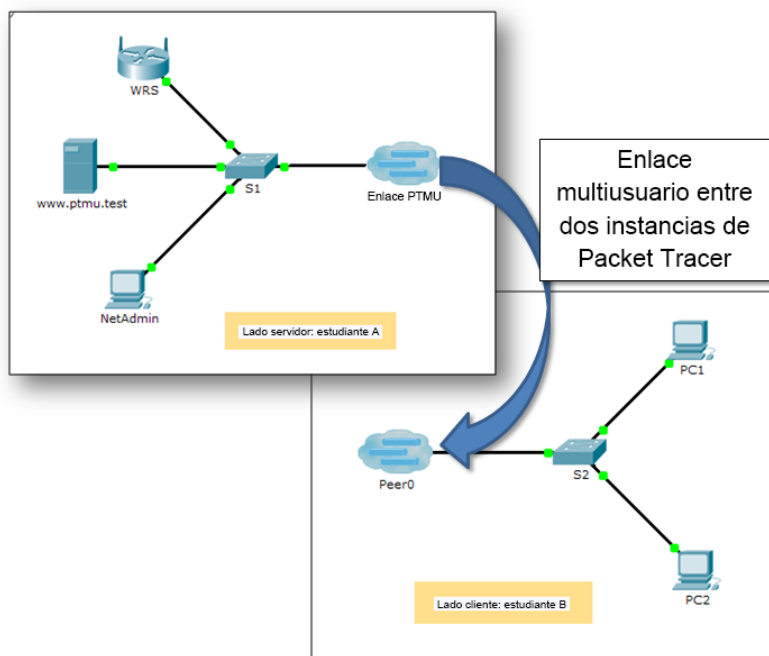


Tabla de direccionamiento

Dispositivo	Dirección IP	Máscara	de
Jugador del lado servidor			
WRS	172.16.1.254	255.255.255.0	
S1	172.16.1.1	255.255.255.0	
www.ptmu.test	172.16.1.5	255.255.255.0	
NetAdmin	DHCP asignado	DHCP asignado	
Jugador del lado cliente			
S2	172.16.1.2	255.255.255.0	
PC1	DHCP asignado	DHCP asignado	
PC2	DHCP asignado	DHCP asignado	

Objetivos

Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

Parte 2: Jugador del lado servidor: Implementar y verificar servicios

Parte 3: Jugador del lado cliente: Configurar y verificar el acceso a los servicios

Información básica

Nota: completar las actividades previas de este capítulo, incluida la actividad **Función Multiusuario de Packet Tracer: Tutorial**, constituye un requisito previo.

En esta actividad para varios usuarios, dos estudiantes (jugadores) cooperan para implementar y verificar servicios, incluso DHCP, HTTP, correo electrónico, DNS y FTP. El jugador del lado servidor implementará y verificará servicios en un servidor. El jugador del lado cliente configurará dos clientes y verificará el acceso a los servicios.

Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

Paso 1: Seleccionar un compañero y determinar el rol para cada estudiante

- a. Busque un compañero de clase con el que cooperará para realizar esta actividad. Ambas PC deben estar conectadas a la misma LAN.
- b. Determinen quién desempeñará la función del lado servidor y quién desempeñará la función del lado cliente en esta actividad.
 - El jugador del lado servidor abre el archivo **Packet Tracer Multiuser - Implement Services - Server Side.pka**.
 - El jugador del lado cliente abre el archivo **Packet Tracer Multiuser - Implement Services - Client Side.pka**.

Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

Paso 2: Configurar los parámetros iniciales de los switches

Cada jugador: configure su respectivo switch con los siguientes parámetros:

- Nombre de host que utilice el nombre para mostrar (**S1** o **S2**)
- Mensaje del día (MOTD) adecuado
- Contraseñas de modo EXEC privilegiado y de línea
- Direccionamiento IP correcto, según Tabla de direccionamiento

S1

```

Switch>en
Switch>enable
Switch>conf t
Enter configuration commands, one per line. End with CNIL/Z.
Switch(config)#hostname S1
S1(config)#enable password cisco
S1(config)#enable secret class
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#line console 0
S1(config-line)#password cisco
S1(config-line)#exit
S1(config)#service pa
S1(config)#service password-encryption
S1(config)#banner motd #Acceso solo para personal autorizado#
S1(config)#int vlan 1
S1(config-if)#ip address 172.16.1.1 255.255.255.0
S1(config-if)#no sh
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)#
    
```

S2

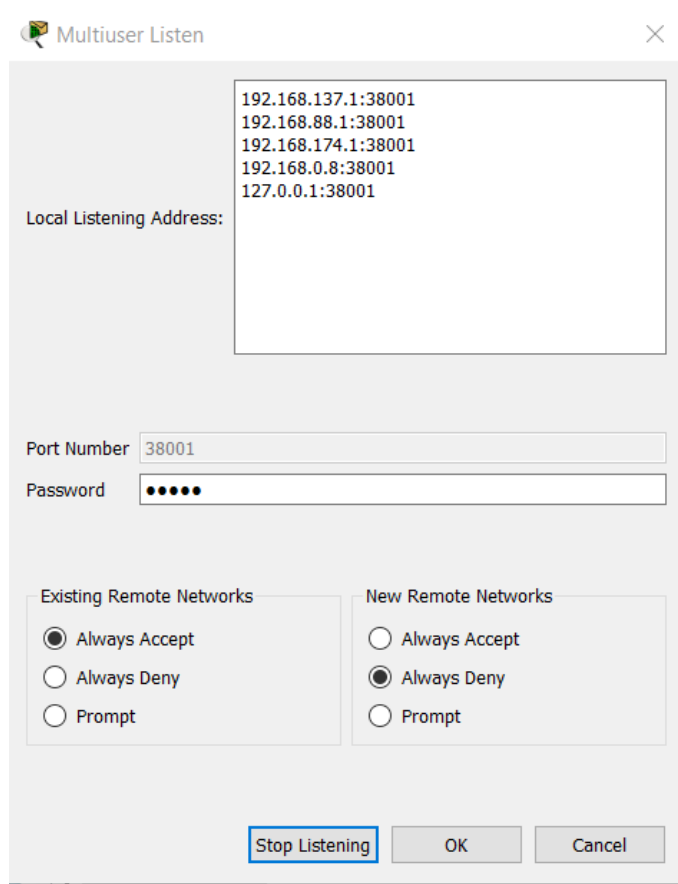
```

Switch>en
Switch>enable
Switch>conf t
Switch>conf terminal
Enter configuration commands, one per line. End with CNIL/Z.
Switch(config)#hostname S2
S2(config)#banner motd #Acceso solo para personal autorizado#
S2(config)#enable password cisco
S2(config)#enable secret class
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#line console 0
S2(config-line)#password cisco
S2(config-line)#exit
S2(config)#service pass
S2(config)#service password-encryption
S2(config)#int vlan 1
S2(config-if)#ip address 172.16.1.2 255.255.255.0
S2(config-if)#no sh
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
S2(config-if)#
    
```

Paso 3: Jugador del lado servidor: Configurar el enlace PTMU y comunicar el direccionamiento

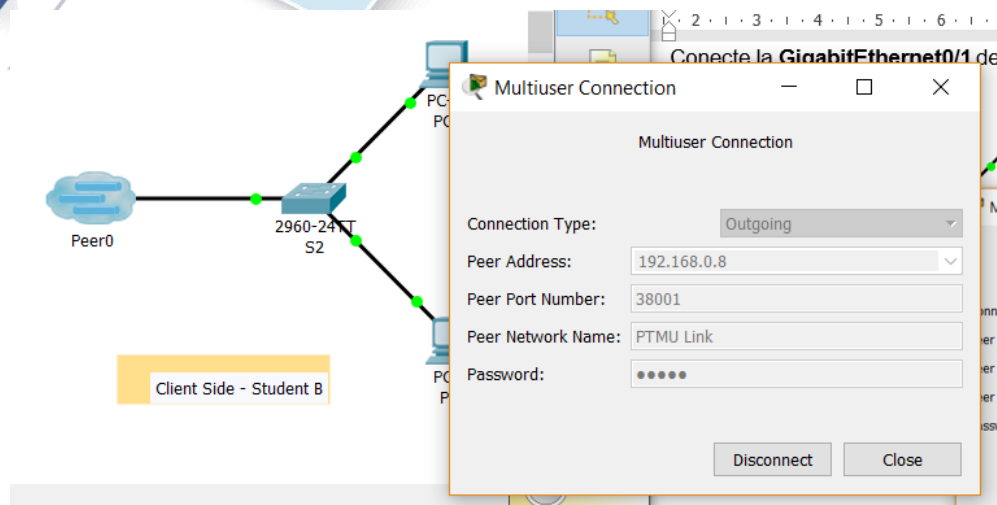
- a. Complete los pasos necesarios para verificar que el **enlace PTMU** esté listo para recibir una conexión entrante.
- b. Comunique la información de configuración necesaria al jugador del lado cliente.



Paso 4: Jugador del lado cliente: Configurar la conexión multiusuario saliente

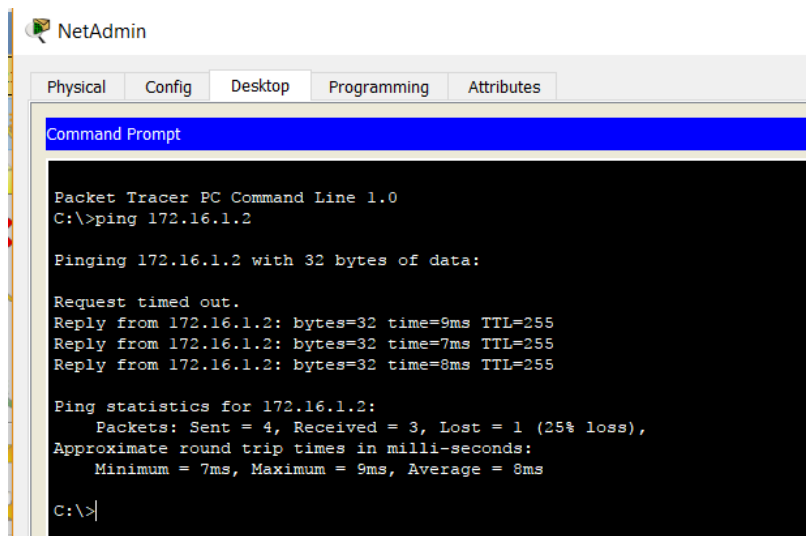
- a. Jugador del lado cliente: registre la siguiente información que le proporcionó el jugador del lado servidor: Dirección IP: 192.168.0.8
 Número de puerto: 38001
 Contraseña (**cisco**, de manera predeterminada): cisco
- b. Configure **Peer0** para conectarse al **enlace PTMU** del jugador del lado servidor. c. Conecte la **GigabitEthernet0/1** de **S2** al **Link0** en **Peer0**.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



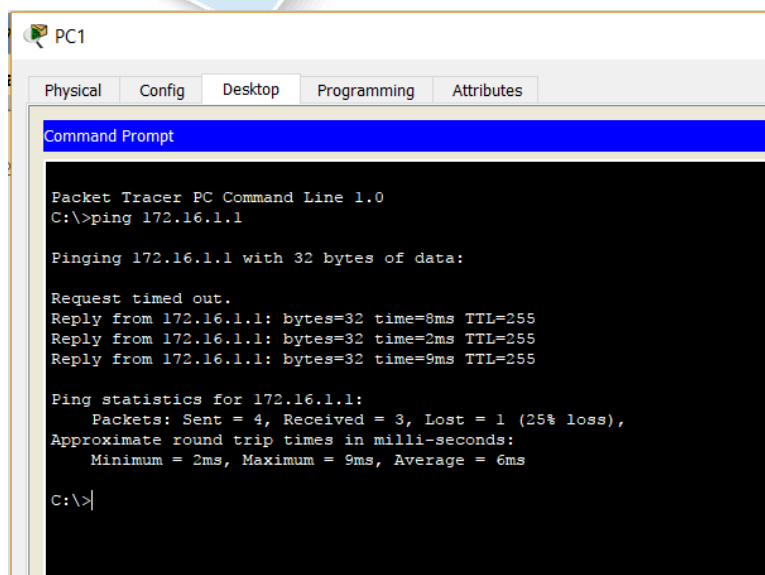
Paso 5: Verificar la conectividad a través de una conexión multiusuario local

- a. El jugador del lado servidor debe poder hacer ping al S2 en la instancia de Packet Tracer del jugador del lado cliente.



- b. El jugador del lado cliente debe poder hacer ping al S1 en la instancia de Packet Tracer del jugador del lado servidor.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



```

PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Request timed out.
Reply from 172.16.1.1: bytes=32 time=8ms TTL=255
Reply from 172.16.1.1: bytes=32 time=2ms TTL=255
Reply from 172.16.1.1: bytes=32 time=9ms TTL=255

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 9ms, Average = 6ms

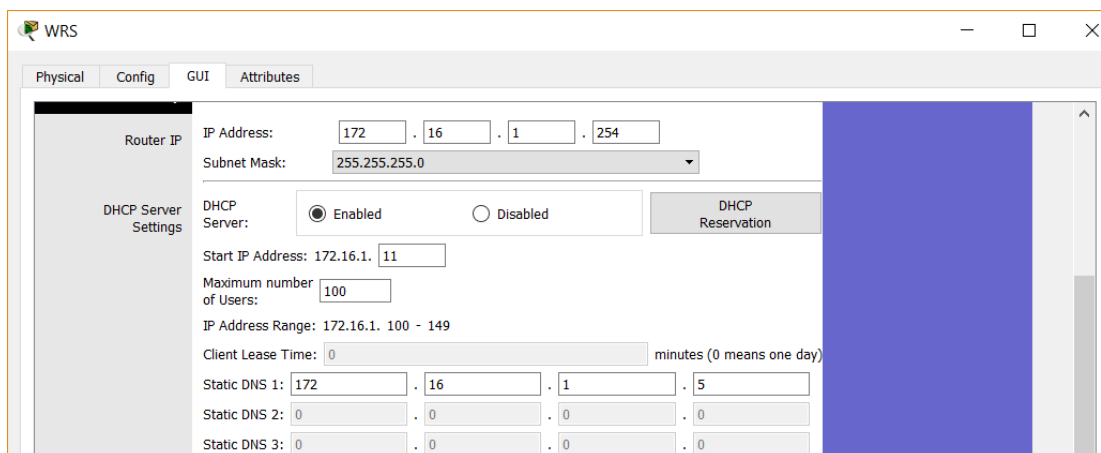
C:\>|
  
```

Parte 2: Jugador del lado servidor: Implementar y verificar servicios

Paso 1: Configurar WRS como servidor de DHCP

WRS proporciona servicios de DHCP. Establezca los siguientes parámetros para la configuración del servidor de DHCP:

- La dirección IP de inicio es **172.16.1.11**.
- La cantidad máxima de usuarios es **100**.
- El **DNS 1 estático** es **172.16.1.5**.



WRS

Physical Config GUI Attributes

Router IP
IP Address: 172 . 16 . 1 . 254
Subnet Mask: 255.255.255.0

DHCP Server Settings
DHCP Server: Enabled Disabled DHCP Reservation

Start IP Address: 172.16.1. 11

Maximum number of Users: 100

IP Address Range: 172.16.1. 100 - 149

Client Lease Time: 0 minutes (0 means one day)

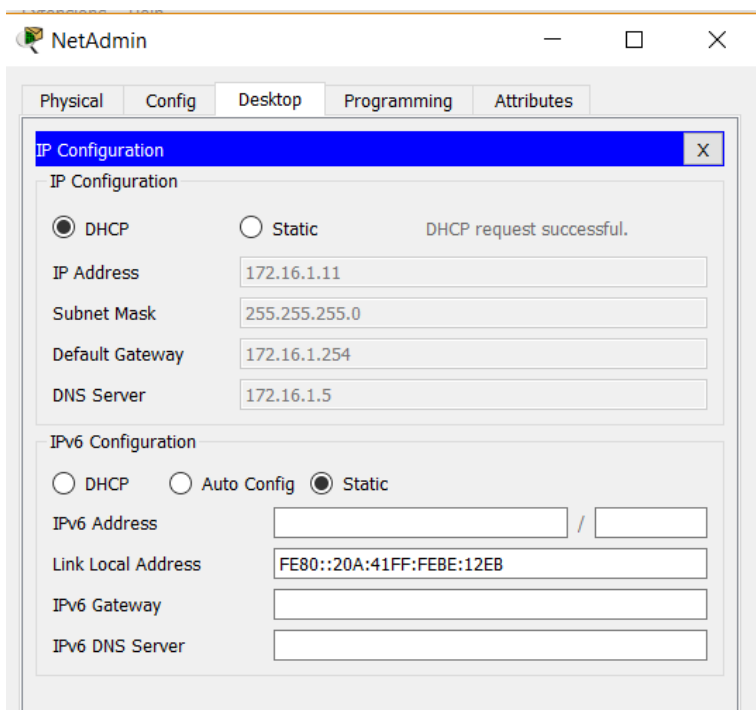
Static DNS 1: 172 . 16 . 1 . 5

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

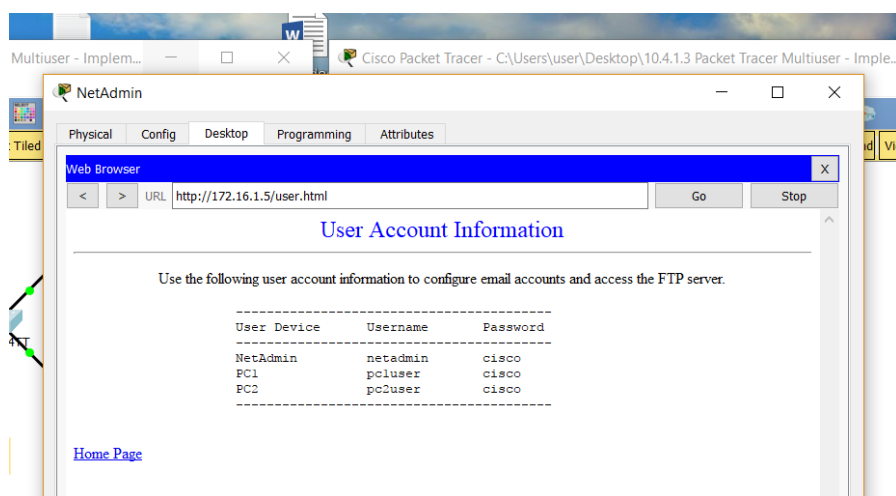
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Verifique si **NetAdmin** recibió el direccionamiento IP mediante DHCP.



En **NetAdmin**, acceda a la página Web User Account Information (Información de cuenta de usuario) en

172.16.1.5. Utilizará esta información para configurar las cuentas de usuario en el paso 2.

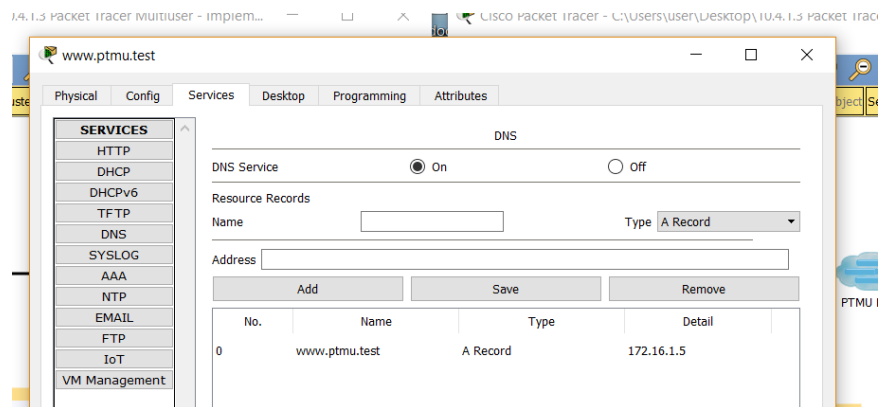


ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

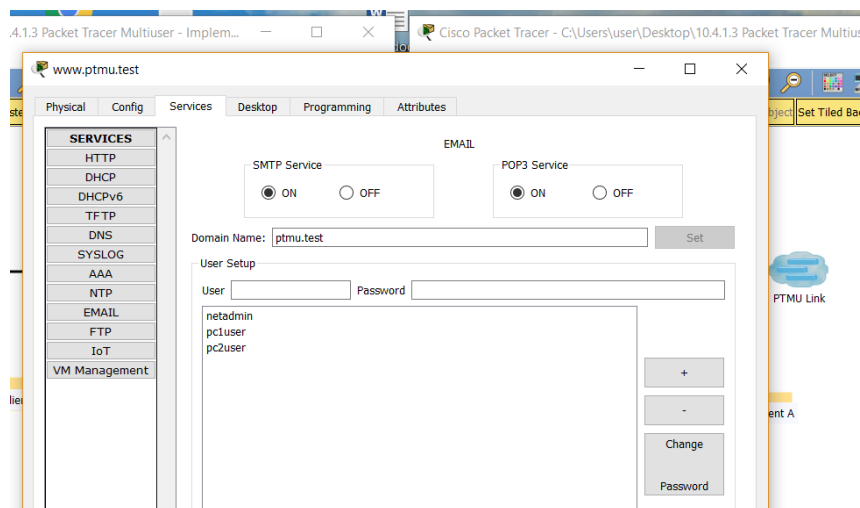
Paso 2: Configurar servicios en www.ptmu.test

El servidor **www.ptmu.test** proporciona el resto de los servicios y se debe configurar con lo siguiente:

Un registro DNS que asocie la dirección IP del servidor **www.ptmu.test** al nombre **www.ptmu.test**.

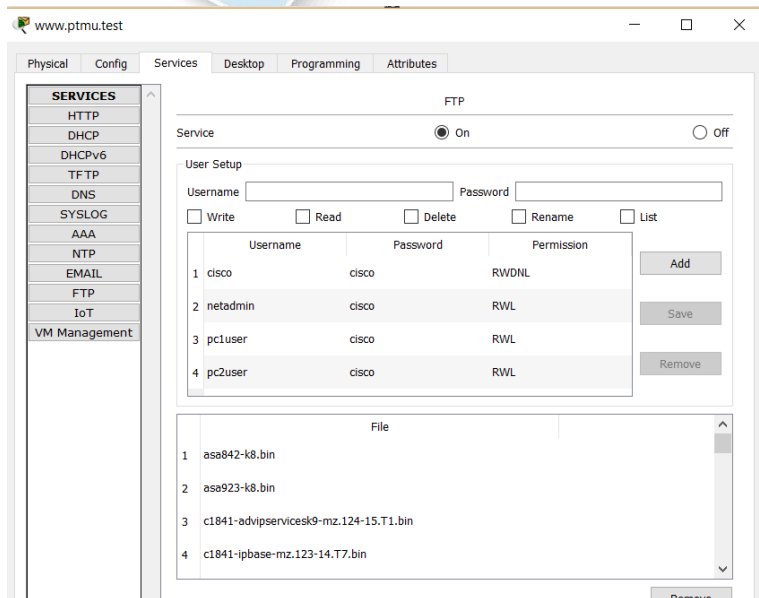


Cuentas de usuario y servicios de correo electrónico según la lista de usuarios. El nombre de dominio es **ptmu.test**.



Cuentas de usuario y servicios FTP según la lista de usuarios. Otorgue permiso a cada usuario para escribir, leer y enumerar.

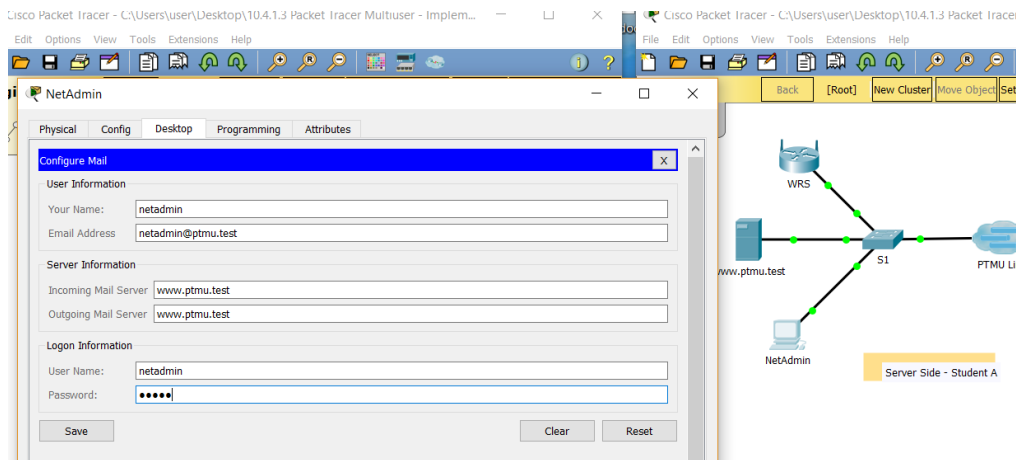
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



Paso 3: Verificar que todos los servicios estén implementados de acuerdo con los requisitos

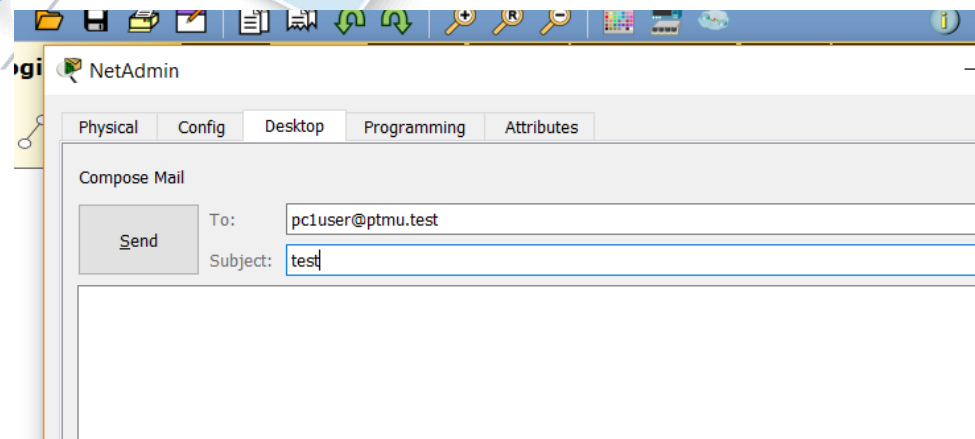
En **NetAdmin**, realice lo siguiente:

Configure el cliente de correo electrónico para la cuenta de usuario de NetAdmin.

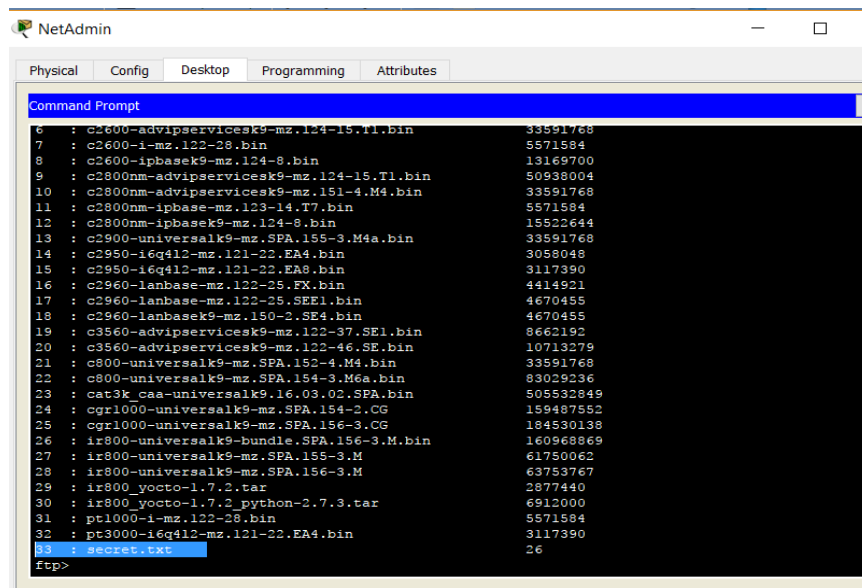
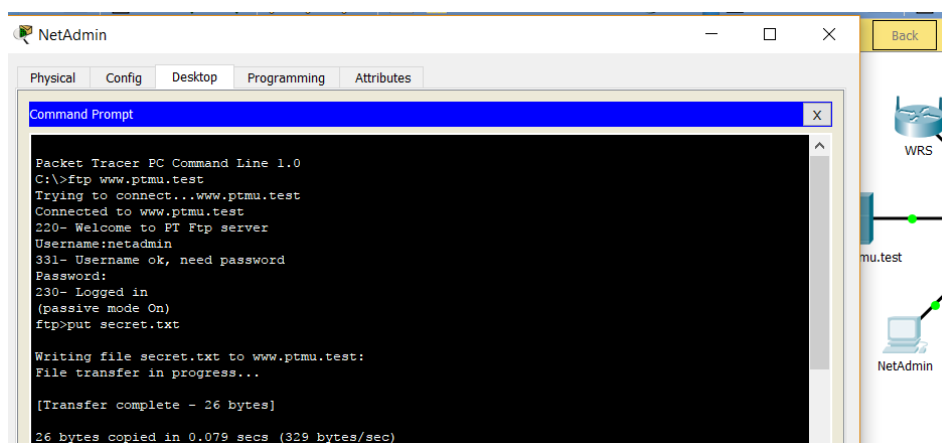


Envíe un correo electrónico al usuario de la **PC1**.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



Suba el archivo **secret.txt** al servidor FTP. No modifique el archivo.



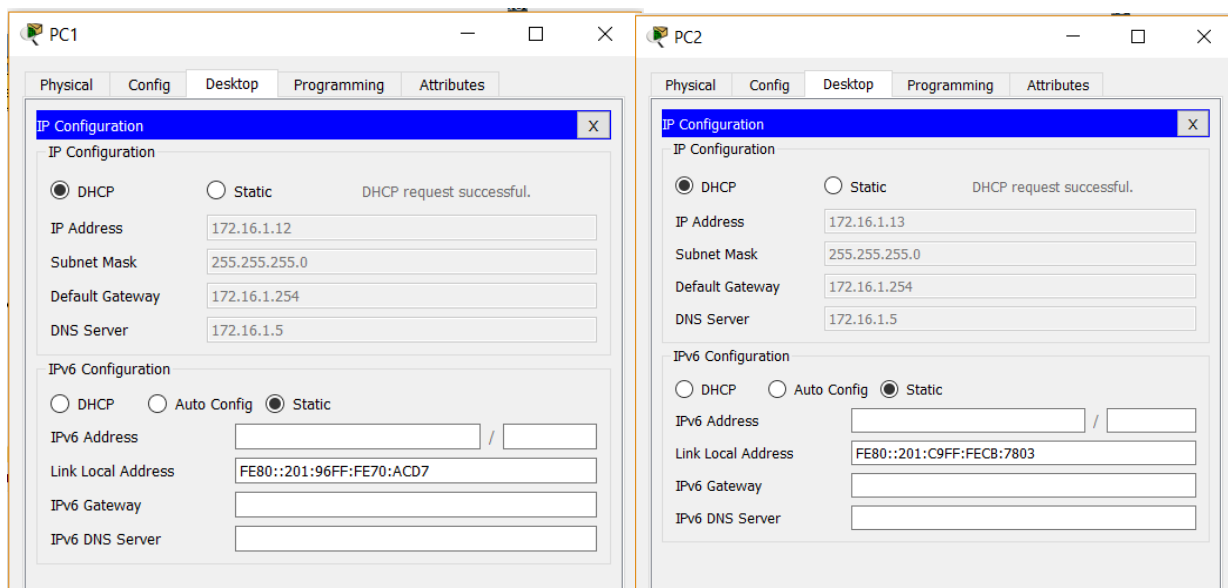
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Nota: la puntuación para el jugador del lado servidor será de **43/44** hasta que el jugador del lado cliente descargue correctamente el archivo **secret.txt**, lo modifique y lo suba al servidor FTP **www.ptmu.test**.

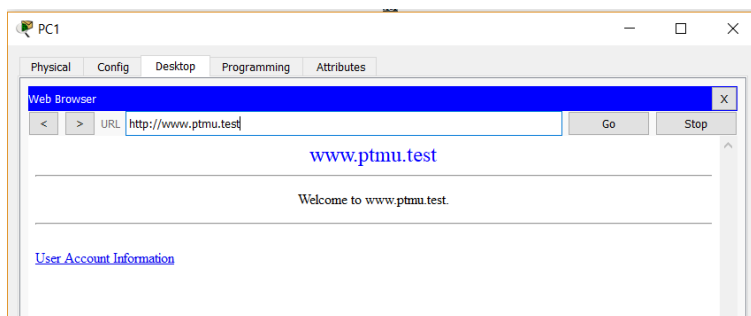
Parte 3: Jugador del lado cliente: Configurar y verificar el acceso a los servicios

Paso 1: Configurar y verificar el direccionamiento de las PC

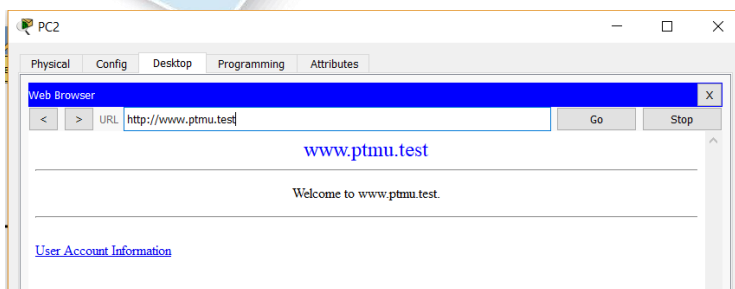
- a. Configure la **PC1** y la **PC2** para obtener el direccionamiento automáticamente.



- b. Las PC1 y PC2 deben poder acceder a la página Web **http://www.ptmu.test**.

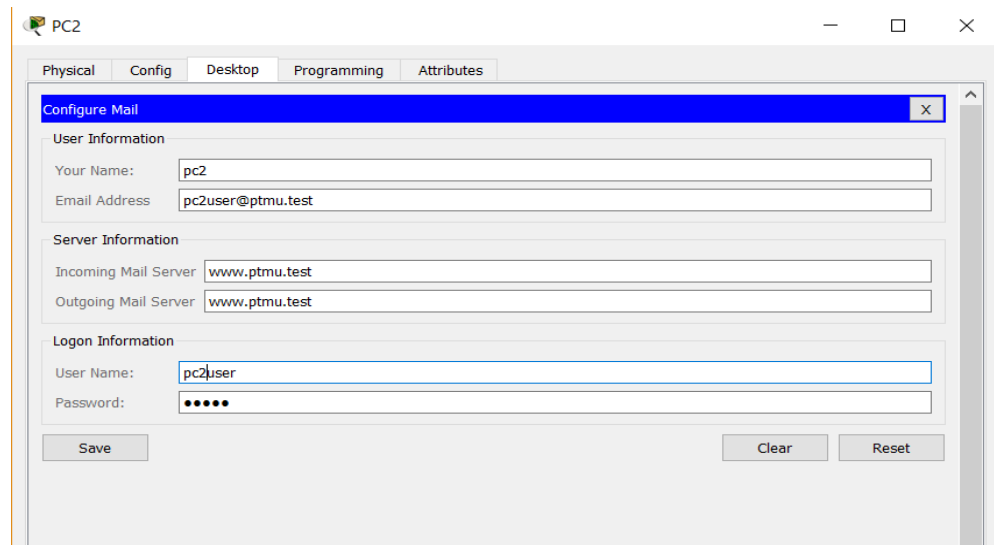
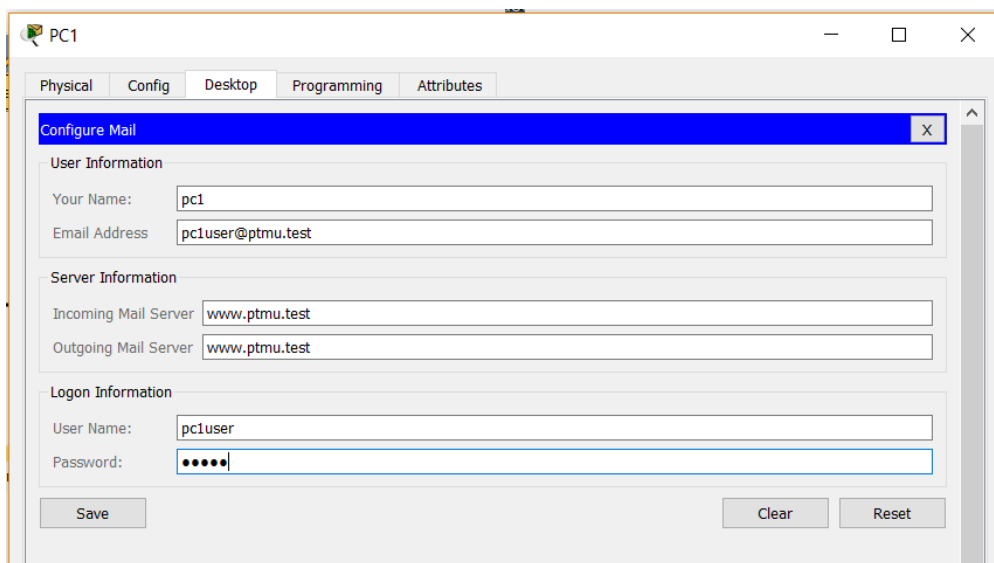


ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



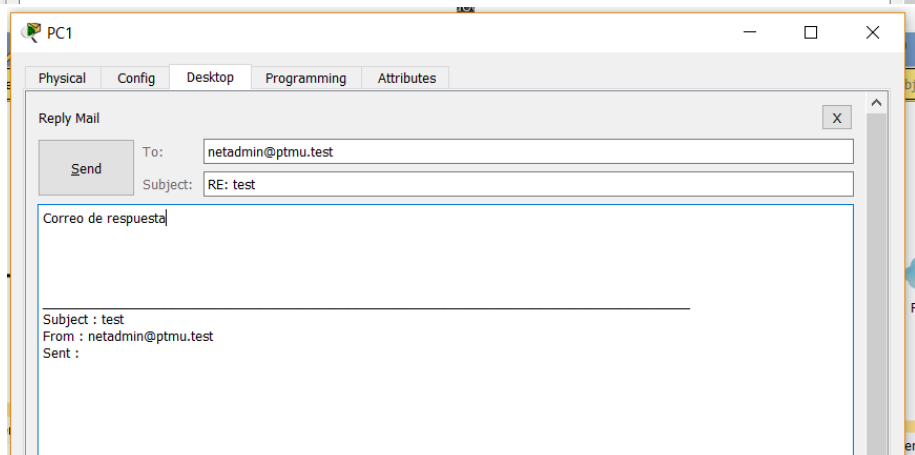
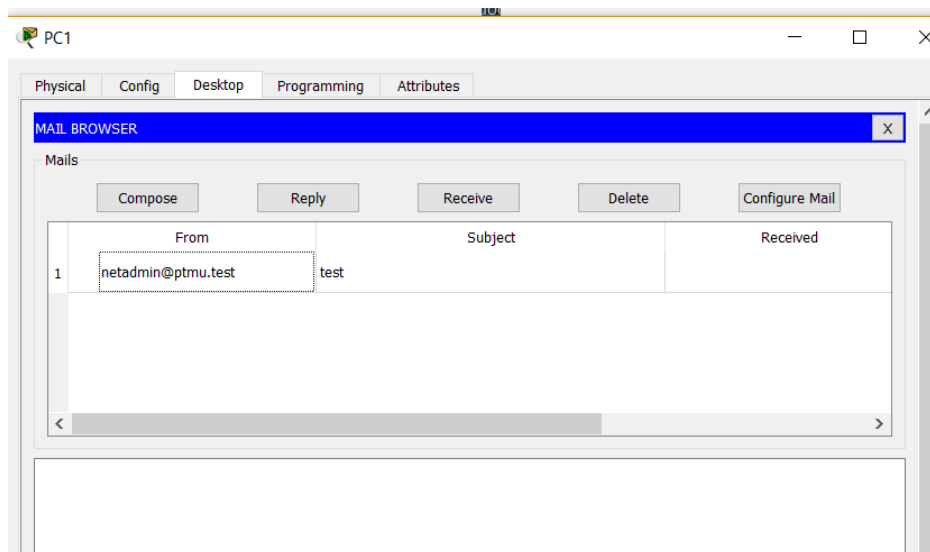
Paso 2: Configurar y verificar las cuentas de correo electrónico de las PC

- a. Configure las cuentas de correo electrónico según los requisitos que se indican en www.ptmu.test/user.html

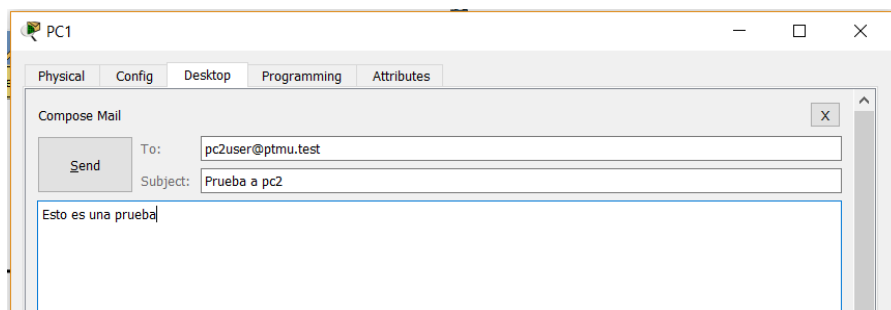


ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

b. Verifique si la PC1 recibió un correo electrónico de NetAdmin y envíe una respuesta.

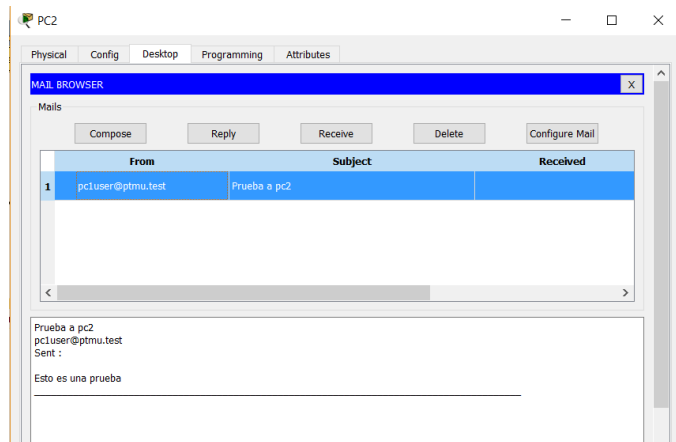


c. Envíe un correo electrónico de la PC1 a la PC2. **Nota:** la puntuación no cambiará.



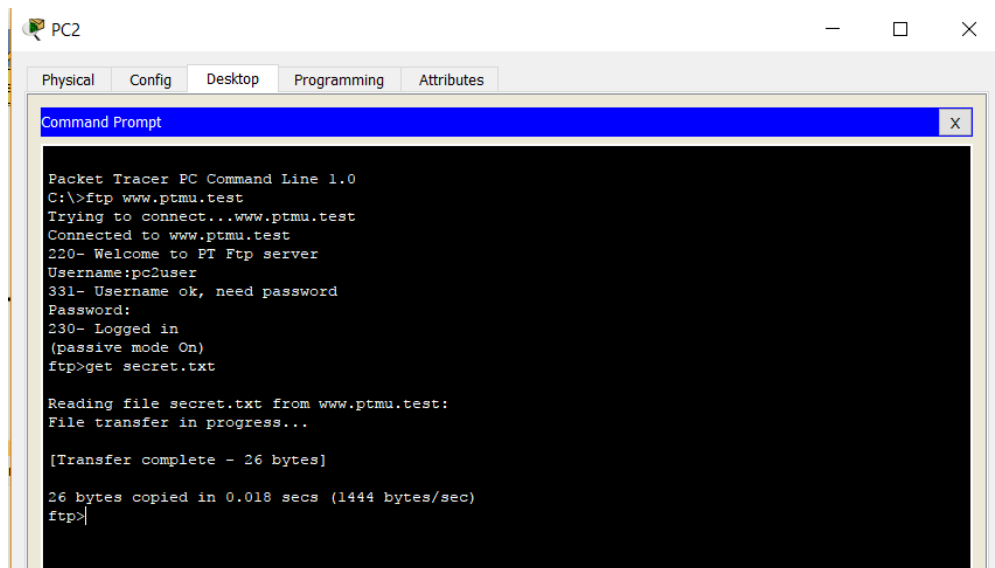
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- d. Verifique si la PC2 recibió un correo electrónico de la PC1.



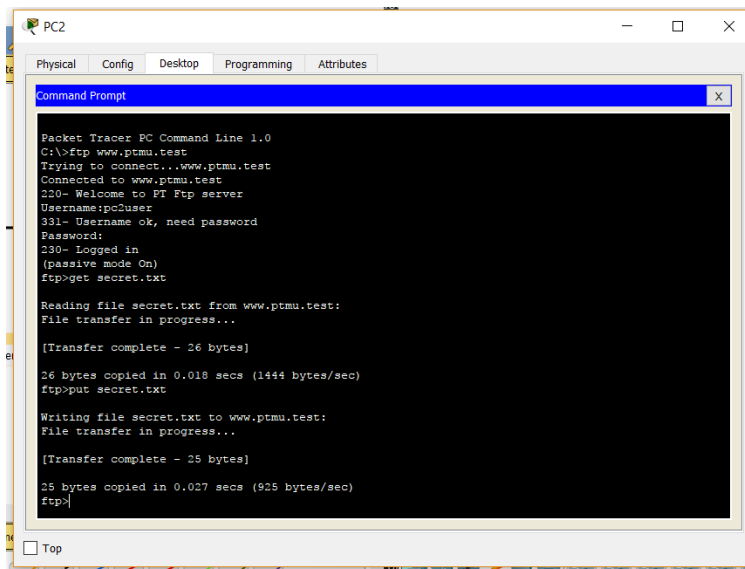
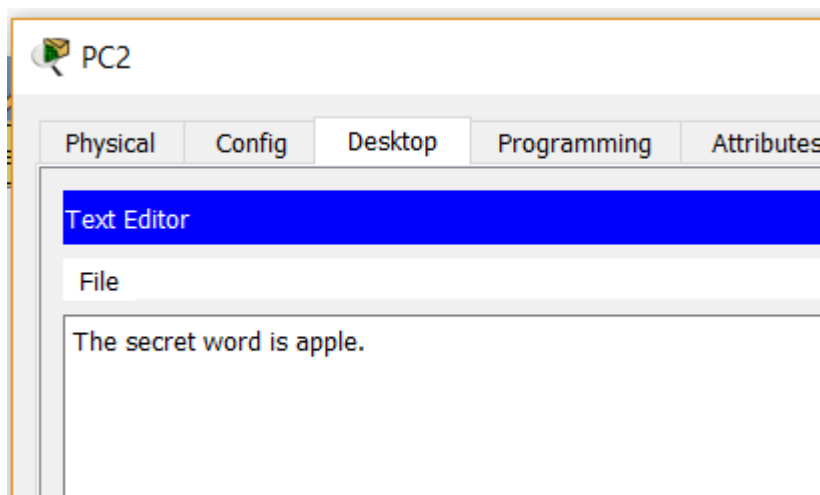
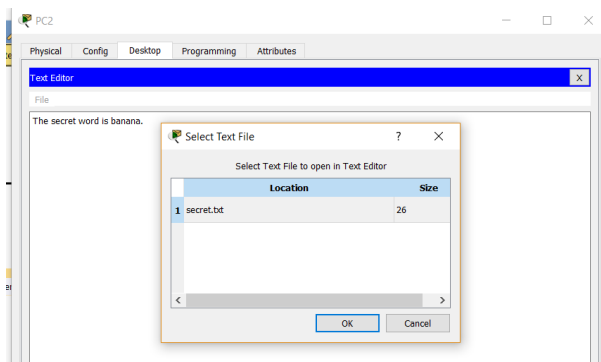
Paso 3: Subir un archivo al servidor FTP y descargarlo de dicho servidor

- a. En la PC2, acceda al servidor FTP y descargue el archivo **secret.txt**.



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

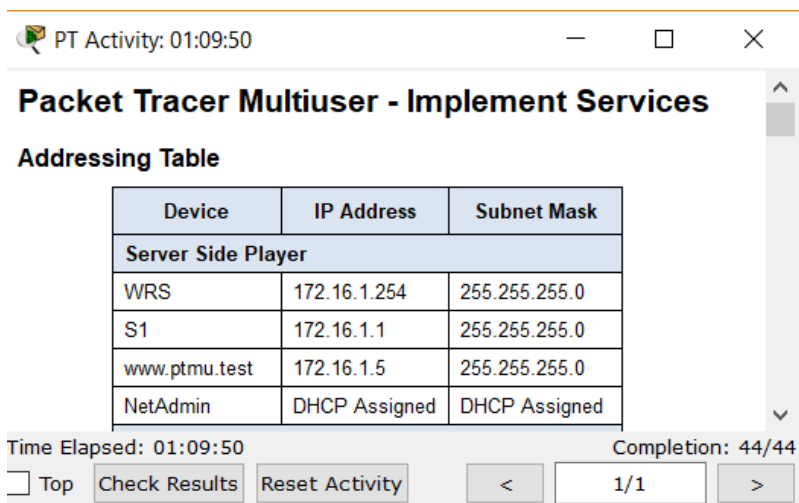
b. Abra el archivo **secret.txt**, solo cambie la palabra secreta por **apple** y suba el archivo.



- c. La puntuación del jugador del lado servidor debería ser **44/44** y la del jugador del lado cliente debería ser **33/33**.

RESULTADOS:

Lado del servidor:



PT Activity: 01:09:50

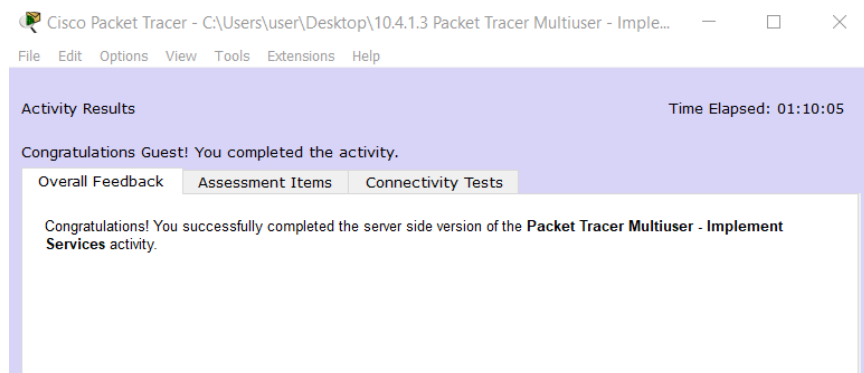
Packet Tracer Multiuser - Implement Services

Addressing Table

Device	IP Address	Subnet Mask
Server Side Player		
WRS	172.16.1.254	255.255.255.0
S1	172.16.1.1	255.255.255.0
www.ptmu.test	172.16.1.5	255.255.255.0
NetAdmin	DHCP Assigned	DHCP Assigned

Time Elapsed: 01:09:50 Completion: 44/44

Top



Cisco Packet Tracer - C:\Users\user\Desktop\10.4.1.3 Packet Tracer Multiuser - Imple...

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 01:10:05

Congratulations Guest! You completed the activity.

Overall Feedback **Assessment Items** Connectivity Tests

Congratulations! You successfully completed the server side version of the **Packet Tracer Multiuser - Implement Services** activity.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Cisco Packet Tracer - C:\Users\user\OneDrive\Documents\Unad\2017-2\Diplomado Cisco...

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 01:42:35

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status
Network	
NetAdmin	
Default Gateway	Correct
DNS Server IP	Correct
Email Client	
Email User	
Email	Correct
Incoming Mail S...	Correct
Outgoing Mail S...	Correct
User Name	Correct
User Password	Correct
Ports	
FastEthernet0	
DHCP client ena...	Correct
IP Address	Correct
Subnet Mask	Correct
PTMU Link	
Connected	Correct
S1	
Banner MOTD	Correct
Console Line	

Component	Items/Total	Score
Basic Security Configuration	5/5	5/5
Client DHCP Configuration	5/5	5/5
IPv4 Host Configuration	3/3	3/3
PT Client Configuration	5/5	5/5
PT Server Configuration	25/25	25/25
PTMU Configuration	1/1	1/1

Score : 44/44
Item Count : 44/44

Close

Lado del cliente:

PT Activity: 01:13:27

Packet Tracer Multiuser - Implement Services

Addressing Table

Device	IP Address	Subnet Mask
Server Side Player		
WRS	172.16.1.254	255.255.255.0
S1	172.16.1.1	255.255.255.0
www.ptmu.test	172.16.1.5	255.255.255.0
NetAdmin	DHCP Assigned	DHCP Assigned

Time Elapsed: 01:13:27 Completion: 33/33

Top

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

Código del curso 203092 – Diplomado de Profundización Cisco

Paso 3 – Actividad Colaborativa 2

Cisco Packet Tracer - C:\Users\user\Desktop\10.4.1.3 Packet Tracer Multiuser - Implem... - □ ×

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 01:13:51

Congratulations Guest! You completed the activity.

Overall Feedback **Assessment Items** Connectivity Tests

Congratulations! You successfully completed the client side version of the Packet Tracer Multiuser - Implement Services activity.

Cisco Packet Tracer - C:\Users\user\Desktop\10.4.1.3 Packet Tracer Multiuser - Implem... - □ ×

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 01:14:06

Congratulations Guest! You completed the activity.

Overall Feedback **Assessment Items** Connectivity Tests

Expand/Collapse All

Assessment Items	Status
Network	
PC1	
Default Gateway	Correct
DNS Server IP	Correct
Email Client	
Email User	
Email	Correct
Incoming Mail S...	Correct
Outgoing Mail S...	Correct
User Name	Correct
User Password	Correct
Ports	
FastEthernet0	
DHCP client ena...	Correct
IP Address	Correct
Subnet Mask	Correct
PC2	
Default Gateway	Correct
DNS Server IP	Correct
Email Client	
Email User	
Email	Correct
Incoming Mail S...	Correct
Outgoing Mail S...	Correct
User Name	Correct
User Password	Correct
Files	

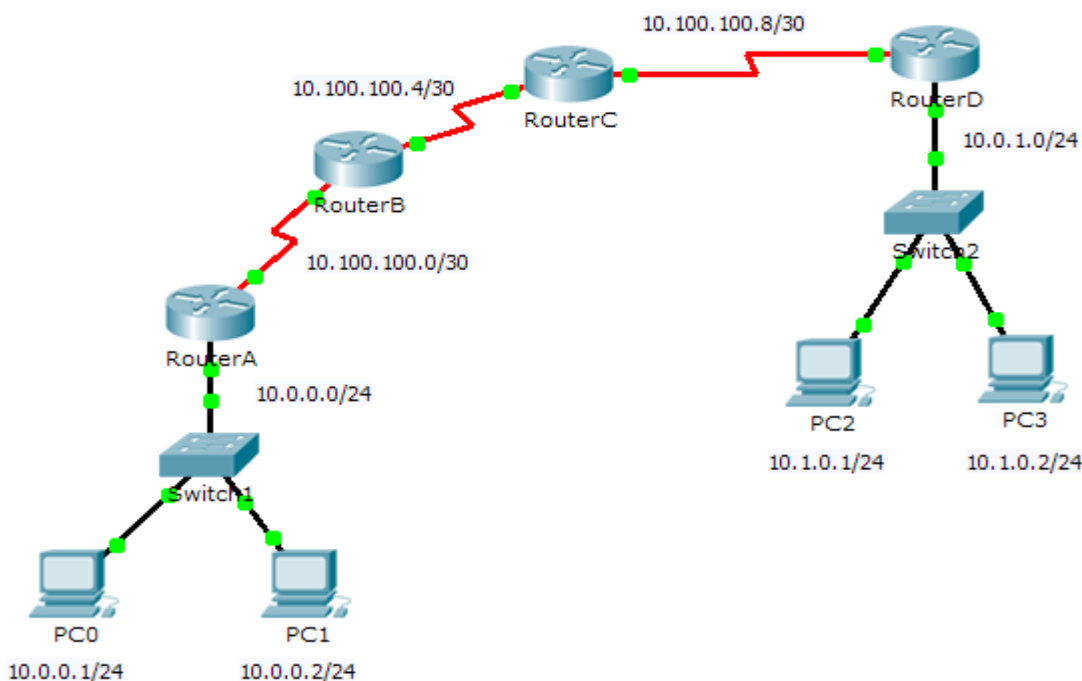
Component	Items/Total	Score
Basic Security Configuration	5/5	5/5
Client DHCP Configuration	10/10	10/10
Email Client Configuration	5/5	5/5
FTP File Transfer	2/2	2/2
IPv4 Host Configuration	3/3	3/3
PT Client Configuration	5/5	5/5
PTMU Configuration	3/3	3/3

Score : 33/33
Item Count : 33/33

Close

Ejercicio 11.3.2.2 Prueba de la conectividad con traceroute

Topología



Objetivos

Parte 1: Probar la conectividad de extremo a extremo con el comando tracert

Parte 2: Comparar con el comando traceroute en un router

Información básica

Esta actividad está diseñada para ayudarlo a llevar a cabo la resolución de problemas de conectividad de red utilizando comandos para rastrear la ruta de origen a destino. Debe examinar el resultado de **tracert** (el comando de Windows) y **traceroute** (el comando de IOS) mientras los paquetes atraviesan la red y determinar la causa de un problema de red. Una vez que se corrija el problema, utilice los comandos **tracert** y **traceroute** para verificar la finalización.

Parte 1: Probar la conectividad de extremo a extremo con el comando tracert

Paso 1: Enviar un ping de un extremo al otro de la red

Haga clic en **PC1** y abra el **símbolo del sistema**. Haga ping a **PC3** en **10.1.0.2**. ¿Qué mensaje se muestra como resultado del ping?

Host de destino inalcanzable.

```

PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.1.0.2

Pinging 10.1.0.2 with 32 bytes of data:

Reply from 10.100.100.6: Destination host unreachable.
Reply from 10.100.100.6: Destination host unreachable.
Reply from 10.100.100.6: Destination host unreachable.
Reply from 10.100.100.6: Destination host unreachable.

Ping statistics for 10.1.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
  
```

- c. Observe los resultados del comando **tracert**. ¿Cuál es la última dirección que se alcanzó con el comando **tracert**?

10.100.100.6

Paso 3: Corregir el problema de red

- a. Compare la última dirección que se alcanzó con el comando **tracert** con las direcciones de red indicadas en la topología. El dispositivo más alejado del host 10.0.0.2 con una dirección en el rango de la red que se encontró es el punto de falla. ¿Qué dispositivos tienen direcciones configuradas para la red donde ocurrió la falla?

El RouterB y el RouterC.

- b. Haga clic en **RouterC** y, a continuación, haga clic en la ficha **CLI**. c. ¿Cuál es el estado de las interfaces?

Parecen estar activas.

- d. Compare las direcciones IP en las interfaces con las direcciones de red en la topología. ¿Hay algo que parezca fuera de lo común?

La interfaz serial 0/0/0 tiene una dirección IP incorrecta según la topología.

- e. Realice los cambios necesarios para restaurar la conectividad, pero no modifique las subredes. ¿Cuál es la solución?

Cambiar la dirección IP de la S0/0/0 a 10.100.100.9/30.

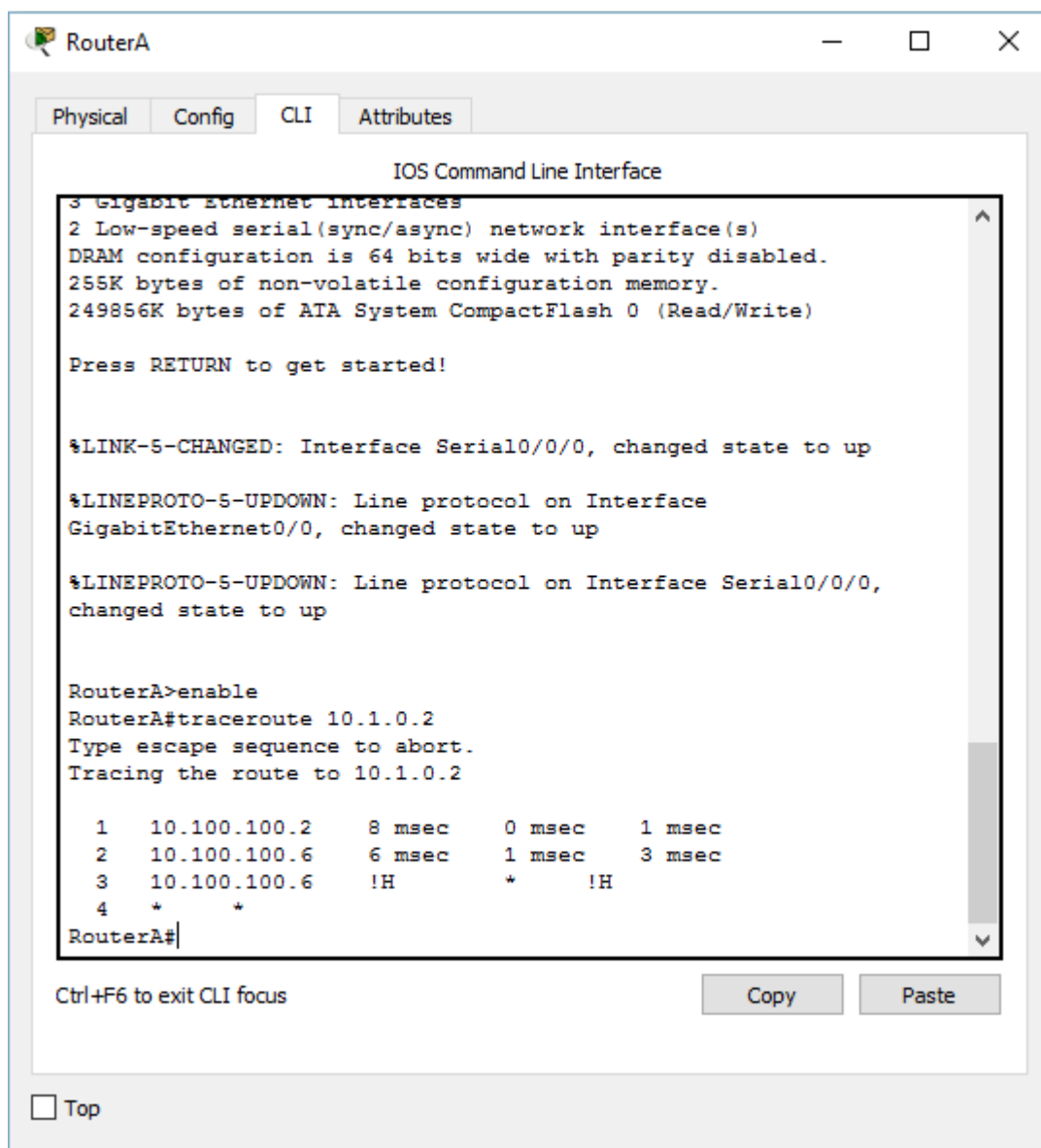
Paso 4: Verificar que la conectividad de extremo a extremo esté establecida

- a. En el **símbolo del sistema de la PC1**, introduzca el comando **tracert 10.1.0.2**.
c. Observe el resultado del comando **tracert**. ¿El comando funcionó correctamente?

Sí

Parte 2: Comparar con el comando traceroute en un router

- a. Haga clic en **RouterA** y, a continuación, haga clic en la ficha **CLI**.
- d. Introduzca el comando **traceroute 10.1.0.2**. ¿El comando se completó correctamente? Sí



The screenshot shows the RouterA CLI interface with the following text:

```

IOS Command Line Interface

3 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

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

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

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

RouterA>enable
RouterA#traceroute 10.1.0.2
Type escape sequence to abort.
Tracing the route to 10.1.0.2

 1  10.100.100.2    8 msec    0 msec    1 msec
 2  10.100.100.6    6 msec    1 msec    3 msec
 3  10.100.100.6    !H        *        !H
 4  *              *

RouterA#

```

Below the terminal output, there are buttons for "Copy" and "Paste", and a "Top" button with a checkbox.

- c. Compare el resultado del comando **traceroute** del router con el del comando **tracert** de la PC.
¿Cuál es la diferencia más notable de la lista de direcciones que se devolvió?

El router tiene una dirección IP menos, porque el próximo dispositivo que utilizará en la ruta será el RouterB

Ejercicio 11.3.3.4 Uso de los comandos show

Objetivos

Parte 1: Analizar el resultado del comando show

Parte 2: Preguntas de reflexión

Información básica

Esta actividad está diseñada para reforzar el uso de los **show** del router. No debe comandos configuraciones, sino examinar el resultado de realizar **show**.
 diversos comandos

Parte 1: Analizar el resultado del comando show

Paso 1: Conectarse a ISPRouter

- Haga clic en **PC ISP** y, a continuación, en la ficha **Desktop** (Escritorio), seguida de **Terminal**.
- Ingrese al modo EXEC privilegiado.

```
ISPRouter>enable
ISPRouter#
```

- Use los siguientes comandos **show** para contestar las preguntas de reflexión en la parte 2:

show arp

```
ISPRouter#show arp
Protocol Address          Age (min)  Hardware Addr  Type   Interface
Internet 209.165.201.1      -         0030.F275.CE01 ARPA   GigabitEthernet0/0
ISPRouter#
```

show flash:

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

```
ISPRouter#show flash:

System flash directory:
File Length Name/status
  3 33591768 cl900-universalk9-mz.SPA.151-4.M4.bin
  2 28282 sigdef-category.xml
  1 227537 sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)

ISPRouter#
```

show ip route

```
ISPRouter#show ip route
Codes: L - local, C - connected, S - static, 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

    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Serial0/0/1
L       209.165.200.226/32 is directly connected, Serial0/0/1
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/27 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0

ISPRouter#
```

show interfaces

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

```
ISPRouter#
ISPRouter#show interfaces
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0030.f275.ce01 (bia
0030.f275.ce01)
  Internet address is 209.165.201.1/27
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 1017 multicast, 0 pause input
    0 input packets with dribble condition detected
--More--
```

show ip interface
brief

```
ISPRouter#
ISPRouter#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0 209.165.201.1  YES manual up             up
GigabitEthernet0/1 unassigned      YES unset   administratively down down
Serial0/0/0        unassigned      YES unset   administratively down down
Serial0/0/1        209.165.200.226 YES manual up             up
Vlan1              unassigned      YES unset   administratively down down
ISPRouter#
```

show protocols

```
ISPRouter#show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 209.165.201.1/27
GigabitEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is administratively down, line protocol is down
Serial0/0/1 is up, line protocol is up
  Internet address is 209.165.200.226/27
Vlan1 is administratively down, line protocol is down
ISPRouter#
```

show users

```
ISPRouter#show users
Line      User      Host(s)      Idle      Location
* 0 con 0      idle         00:00:00

Interface  User      Mode      Idle      Peer Address
ISPRouter#
```

show version

```
ISPRouter#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 20 minutes, 13 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
--More-- |
```

Parte 2: Preguntas de reflexión

o. ¿Qué comandos proporcionarían la dirección IP, el prefijo de red y la interfaz?

R: Los comandos son:

Show ip route

Show interfaces

Show protocols

p. ¿Qué comandos proporcionan la dirección IP y la asignación de interfaces, pero no el prefijo de red?

R: show ip interface brief

q. ¿Qué comandos proporcionan el estado de las interfaces?

R: Los comandos son:

Show interfaces

Show ip interface brief.

r. ¿Qué comandos proporcionan información sobre el IOS que se encuentra cargado en el router?

R: Los comandos son:

Show flash, show version.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

s. ¿Qué comandos proporcionan información sobre las direcciones de las interfaces del router?

R: Los comandos son:

Show arp

Show interfaces

t. ¿Qué comandos proporcionan información sobre la cantidad de memoria flash disponible?

R: show version

u. ¿Qué comandos proporcionan información sobre las líneas que se utilizan para propósitos de control de dispositivos o de configuración?

R: Show users

v. ¿Qué comandos proporcionan estadísticas de tráfico de las interfaces del router?

R: show interfaces

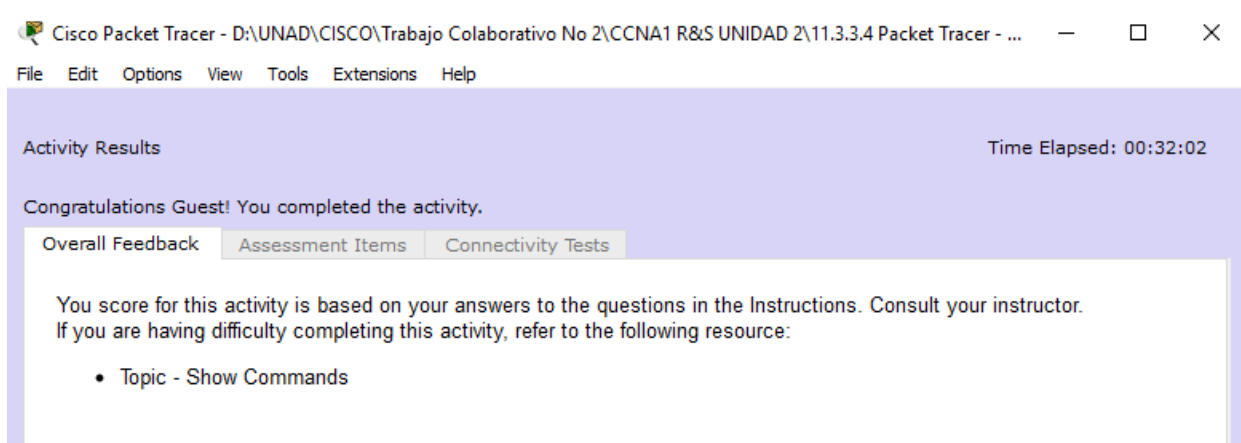
h. ¿Qué comandos proporcionan información sobre las rutas disponibles para el tráfico de la red?

R: show ip route

i. ¿Qué interfaces están activas actualmente en el router?

R: GigabitEthernet 0/0, Serial 0/0/1.

Ítems Resueltos



Cisco Packet Tracer - D:\UNAD\CISCO\Trabajo Colaborativo No 2\CCNA1 R&S UNIDAD 2\11.3.3.4 Packet Tracer - ...

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:32:02

Congratulations Guest! You completed the activity.

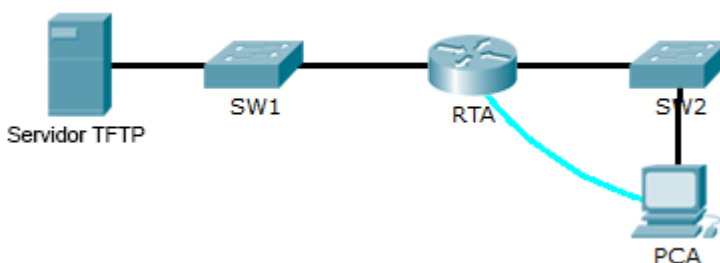
Overall Feedback Assessment Items Connectivity Tests

You score for this activity is based on your answers to the questions in the Instructions. Consult your instructor. If you are having difficulty completing this activity, refer to the following resource:

- Topic - Show Commands

Ejercicio 11.4.2.5 Realización de copias de seguridad de archivos de configuración

Topología



Objetivos

Parte 1: Establecer la conectividad al servidor TFTP

Parte 2: Transferir la configuración del servidor TFTP

Parte 3: Realizar copias de seguridad de la configuración y del IOS en el servidor TFTP

Información básica/Situación

Esta actividad está diseñada para mostrar cómo restaurar una configuración a partir de una copia de seguridad y, luego, realizar una nueva copia de seguridad. Debido a una falla del equipo, se colocó un router nuevo. Afortunadamente, los archivos de configuración de respaldo se guardaron en un servidor de protocolo TFTP (Trivial File Transfer Protocol, protocolo trivial de transferencia de archivos). Debe restaurar los archivos del servidor TFTP para que el router vuelva a estar en línea con el menor tiempo de inactividad posible.

Parte 1: Establecer la conectividad al servidor TFTP

Nota: debido a que es un router nuevo, la configuración inicial se realizará mediante una conexión de consola al router.

- a. Haga clic en **PCA**, después en la ficha **Desktop** (Escritorio) y, a continuación, en **Terminal** para acceder a la línea de comandos **RTA**.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

The screenshot shows the Cisco Packet Tracer interface. On the left, a network diagram is visible with components: Servidor TFTP, SW1, RTA, and SW2. A PC labeled 'PCA' is connected to RTA. A 'Terminal Configuration' dialog box is open in the foreground, showing port settings: Bits Per Second: 9600, Data Bits: 8, Parity: None, Stop Bits: 1, Flow Control: None. The dialog also features icons for various tools like Command Prompt, Web Browser, MIB Browser, Cisco IP Communicator, Email, PPPoE Dialer, Text Editor, Firewall, and IPv6 Firewall.

The screenshot shows the Cisco Packet Tracer interface with the same network diagram as above. A 'Terminal' window is open, displaying the following configuration commands and their output:

```

Router>EN
Router#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip address 172.16.1.1 255.255.255.0
Router(config-if)#no sh

Router(config-if)#
%LINK-6-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up

Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

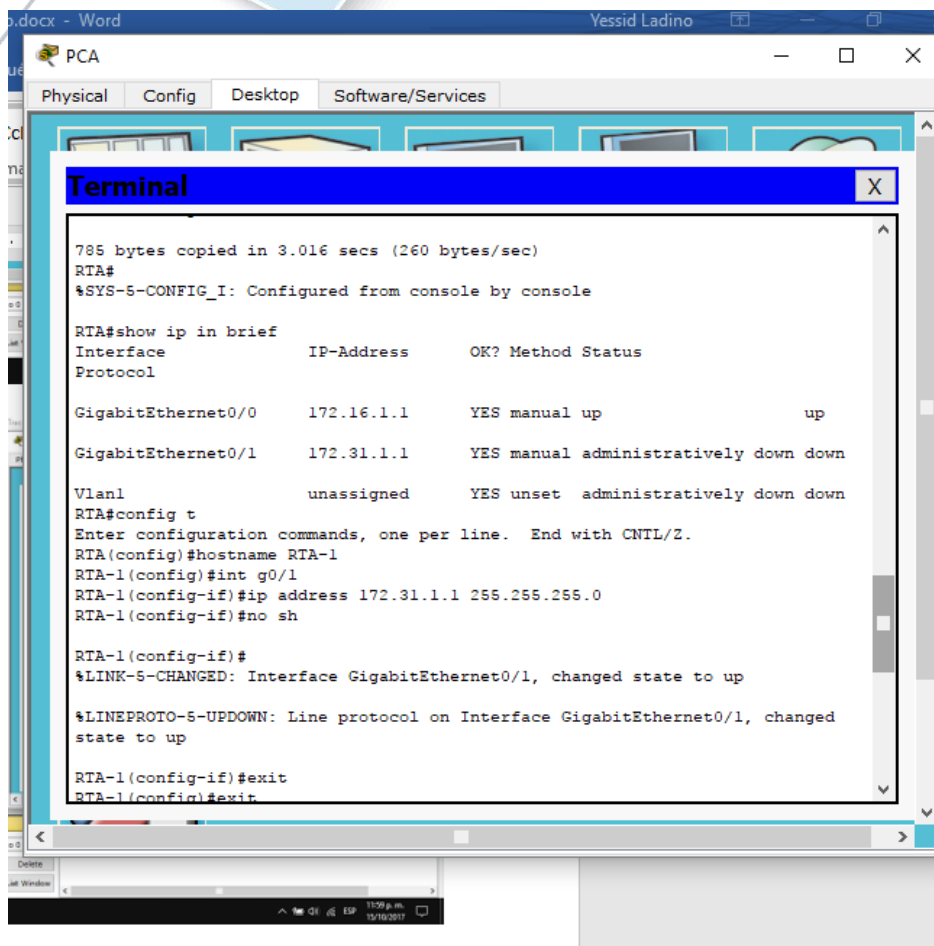
Router#copy tft running-config
Address or name of remote host []? 172.16.1.2
Source filename []? RTA-config
Destination filename [running-config]?

Accessing sftp://172.16.1.2/RTA-config....
Loading RTA-config from 172.16.1.2: 1
[OK - 785 bytes]

785 bytes copied in 3.016 secs (260 bytes/sec)
  
```

The status bar at the bottom indicates 'Time: 00:17:49' and 'Power Cycle Devices Fast Forward Time'. A 'Realtime' indicator is also present.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



- b. Configure y active la interfaz **Gigabit Ethernet 0/0**. La dirección IP debe coincidir con el gateway predeterminado para el **servidor TFTP**.
- c. Pruebe la conectividad al **servidor TFTP**. Si es necesario, lleve a cabo la resolución de problemas.

Parte 2: Transferir la configuración del servidor TFTP

- a. Emita el siguiente comando desde el modo EXEC privilegiado:

```
Router# copy tftp running-config
```

Address or name of remote host [?]: **172.16.1.2 Packet Tracer: Realización de copias de seguridad de archivos de configuración** © 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco. Página 2 de 2

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Cisco Packet Tracer Student - C:\Users\Ladino\Desktop\DIPLOMADO CISCO\ACTIVIDAD 2\CENA1 R&S UNIDAD 2\11.4.2.5 Packet Tracer - Backing Up Configuration Files.pka

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 00:22:04

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
RTA				
Host Name	Correct	1	Hostname Con...	
Ports				
GigabitEthernet0/0				
IP Address	Correct	1	Device Interfa...	
Port Status	Correct	1	Device Interfa...	
Subnet M...	Correct	1	Device Interfa...	
GigabitEthernet0/1		0	Other	
Port Status	Correct	1	Device Interfa...	
Startup Config	Correct	25	IOS Config Fil...	

Score	Item Count
: 30/30	: 6/6

Component	Items/Total	Score
Device Interface Configuration	4/4	4/4
Hostname Configuration	1/1	1/1
IOS Config File Management	1/1	25/25

Ejercicio 11.5.2.4: Configuración de un router Linksys

Topología



Objetivos

Parte 1: Conectar al router Linksys

Parte 2: Habilitar conectividad inalámbrica

Parte 3: Configurar y verificar el acceso al cliente inalámbrico

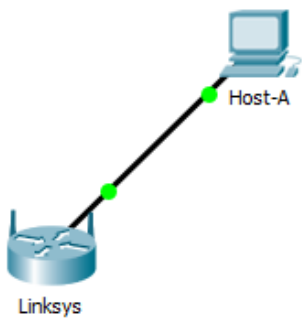
Información básica

En esta actividad, configurará un router inalámbrico Linksys, lo que permite el acceso remoto a los clientes inalámbricos así como conectividad con seguridad WPA.

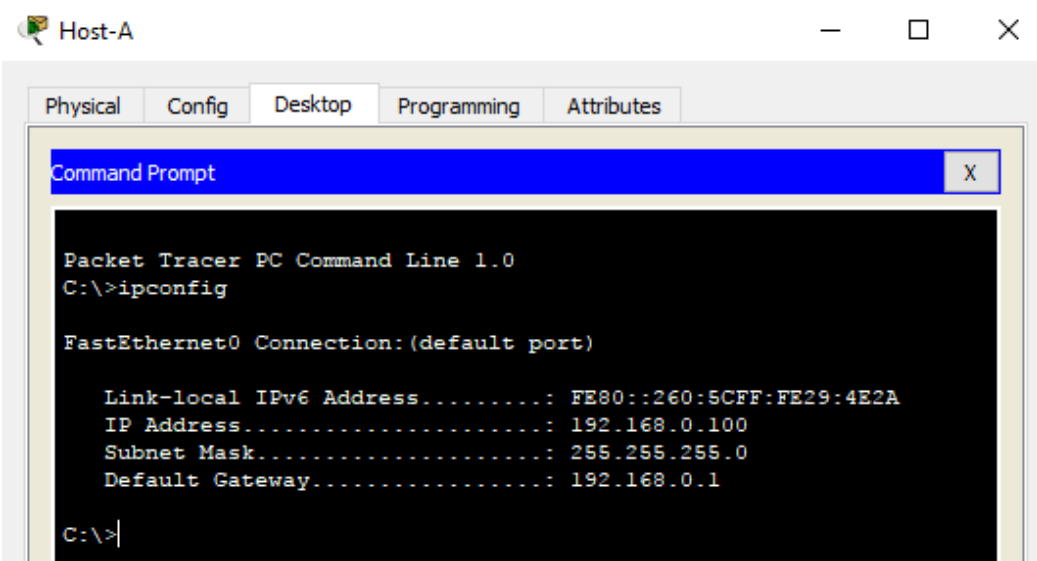
Parte 1: Conectar al router Linksys

Paso 1: Establecer y verificar la conectividad al router Linksys

- Conecte el cable adecuado del **Host-A** al puerto Ethernet 1 en **Linksys**.

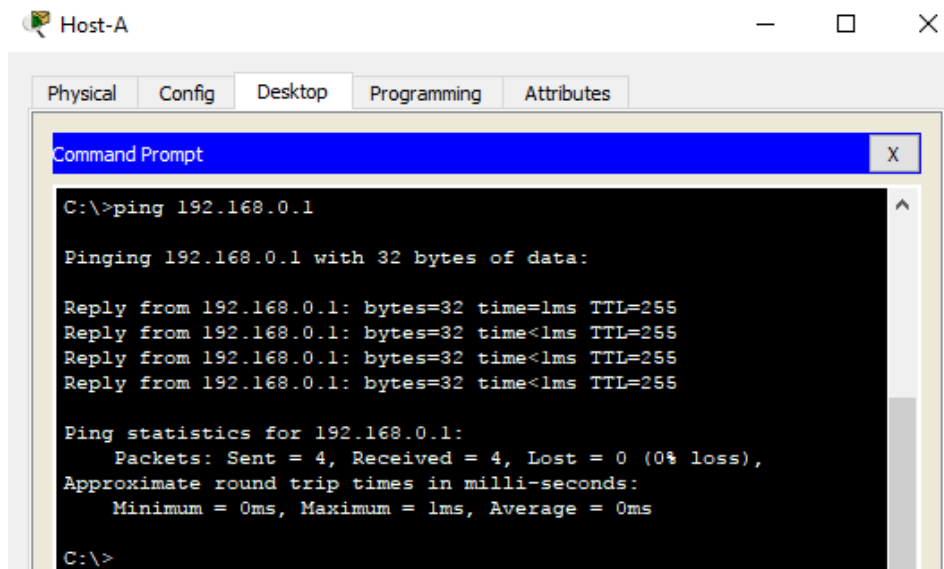


- Espere a que la luz de enlace se vuelva de color verde. A continuación, abra el símbolo del sistema para el **Host-A**. Utilice el comando **ipconfig** para verificar la información de direccionamiento IP del **Host recibido**.



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- Introduzca el comando **ping 192.168.0.1** para verificar que el **Host-A** pueda acceder al gateway predeterminado.



```

Host-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
  
```

Paso 2: Acceda a la interfaz gráfica de usuario (GUI) de Linksys mediante un explorador Web.

- w. Para configurar el router **Linksys** con la GUI, debe acceder a este mediante el explorador Web del **Host-A**. Abra el explorador Web y escriba la dirección de gateway predeterminado en el campo de dirección URL para acceder a **Linksys**.
- x. Introduzca **admin** como nombre de usuario y contraseña predeterminados para acceder al router **Linksys**.

Nota: no podrá ver el cambio en la puntuación al configurar el router **Linksys** hasta que haya hecho clic en **Save Settings** (Guardar configuración).

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

Host-A

Physical Config Desktop Programming Attributes

Web Browser

URL: http://192.168.0.1

Go Stop

Setup Wireless Security Access Restrictions Applications & Gaming Administration

Basic Setup DDNS MAC Address Clone AirView

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers):

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address: 192 168 0 1

Subnet Mask: 255.255.255.0

DHCP Server Settings

DHCP Server: Enabled Disabled

Start IP Address: 192.168.0. 100

Maximum number of Users: 50

IP Address Range: 192.168.0. 100 - 149

Client Lease Time: 0 minutes (0 means one day)

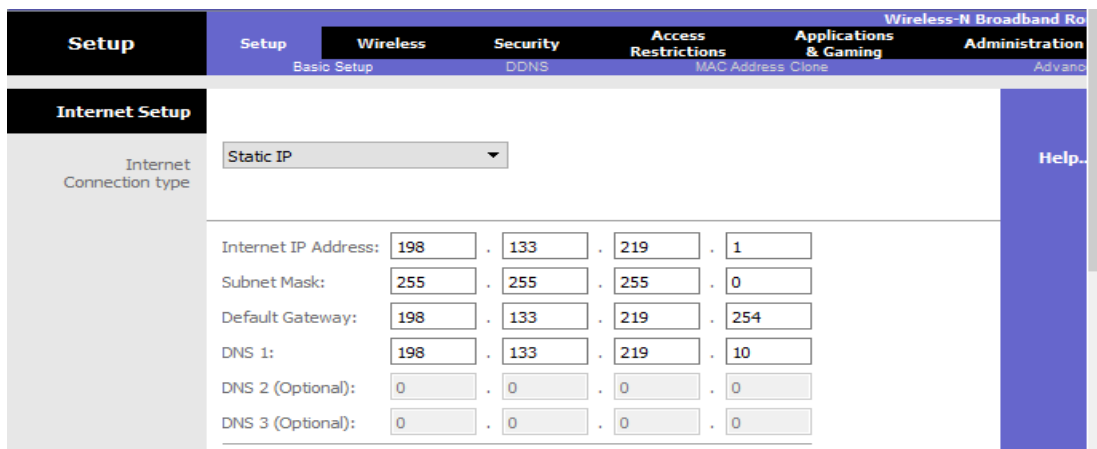
Static DNS 1: 0 0 0 0

Parte 2: Habilitar conectividad inalámbrica

Paso 1: Configure el router Linksys para que tenga conectividad a Internet.

En esta situación no hay conectividad a Internet, pero de todas formas configurará los parámetros para la interfaz con conexión a Internet. Para **Internet Connection Type** (Tipo de conexión a Internet), elija **Static IP** (IP estática) en la lista desplegable. A continuación, introduzca la siguiente información de IP estática:

- j. Dirección IP de Internet: **198.133.219.1**
- k. Máscara de subred: **255.255.255.0**
- l. Gateway predeterminado: **198.133.219.254**
- m. DNS 1: **198.133.219.10**

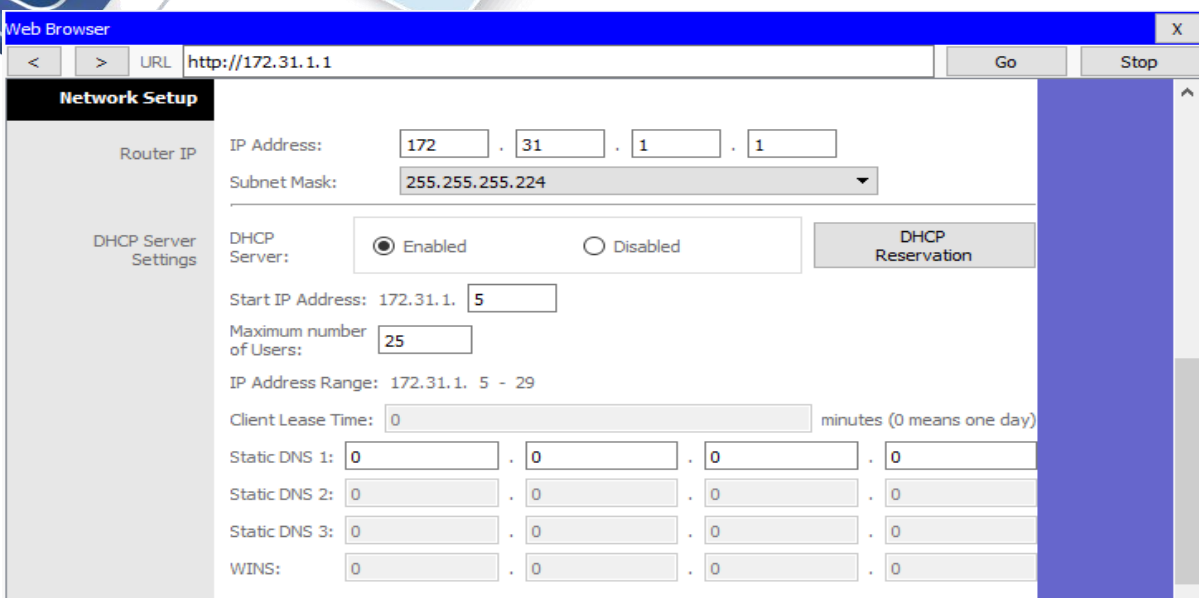


Setup	Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Administration
	Basic Setup		DDNS	MAC Address Clone		Advanced
Internet Setup						
Internet Connection type	Static IP					
Internet IP Address:	198	133	219	1		
Subnet Mask:	255	255	255	0		
Default Gateway:	198	133	219	254		
DNS 1:	198	133	219	10		
DNS 2 (Optional):	0	0	0	0		
DNS 3 (Optional):	0	0	0	0		

Paso 2: Configure los parámetros de red internos.

Desplácese hasta la sección **Network Setup** (Configuración de red) y configure la siguiente información:

- m. Dirección IP: **172.31.1.1**
- n. Máscara de subred: **255.255.255.224**
- o. Dirección IP de inicio: introduzca **5** para el último octeto.
- p. Cantidad máxima de usuarios: **25**



Nota: el rango de direcciones IP del pool de DHCP solo refleja los cambios una vez que hace clic en **Save Settings**.

Paso 3: Guardar la configuración y volver a conectarse al router Linksys

- h. Desplácese hasta la parte inferior de la página y haga clic en **Save Settings**. Si pasa de una ficha a otra sin guardar la configuración, esta se perderá.
- i. Cuando hace clic en **Save Settings**, se pierde la conexión. Esto ocurre porque cambió la dirección IP del router.
- j. Regrese al símbolo del sistema del **Host-A**. Introduzca el comando **ipconfig /renew** para renovar la dirección IP.

```
C:\>ipconfig /renew
```

```
IP Address.....: 172.31.1.5
Subnet Mask.....: 255.255.255.224
Default Gateway.....: 172.31.1.1
DNS Server.....: 198.133.219.10
```

```
C:\>
```

- k. Utilice el explorador Web del **Host-A** para volver a conectarse al router **Linksys**. Deberá utilizar la nueva dirección de gateway predeterminado. Verifique la configuración de **Internet**

Connection (Conexión)

- a Internet) en la ficha **Status** (Estado). La configuración debe coincidir con los valores que configuró en el paso 1 de la parte 2. Si no coinciden, repita los pasos 1 y 2 de la parte 2.

The screenshot shows the 'Status' page of a Wireless-N Broadband Router (WRT300N). The page is divided into two main sections: 'Router Information' and 'Internet Connection'. The 'Router Information' section displays the following details:

Firmware Version:	v0.93.3
Current Time:	Not Available
Internet MAC Address:	0001.C7BC.1601
Host Name:	
Domain Name:	

The 'Internet Connection' section displays the following details:

Connection Type:	Static IP
Internet IP Address:	198.133.219.1
Subnet Mask:	255.255.255.0
Default Gateway:	198.133.219.254
DNS1:	198.133.219.10
DNS2:	
DNS3:	
MTU:	1500
DHCP Lease Time:	

At the bottom of the 'Internet Connection' section, there are two buttons: 'IP Address Release' and 'IP Address Renew'. A 'Help...' link is visible on the right side of the page.

Paso 4: Configurar la conectividad inalámbrica de los dispositivos inalámbricos

- k. Haga clic en la ficha **Wireless** (Conexión inalámbrica) e investigue las opciones de la lista desplegable de **Network Mode** (Modo de red).

The screenshot shows the 'Wireless' settings page of a Wireless-N Broadband Router (WRT300N). The 'Basic Wireless Settings' section is visible, and the 'Network Mode' dropdown menu is open, showing the following options:

- Disabled
- Mixed
- BG-Mixed
- Wireless-G Only
- Wireless-B Only
- Wireless-N Only
- Disabled

Other settings visible include 'Network Name (SSID)', 'Radio Band', 'Wide Channel', 'Standard Channel' (set to 1 - 2.412GHz), and 'SSID Broadcast' (set to Enabled).

¿En qué caso elegiría la opción **Disable** (Deshabilitar)?

R: Cuando no haya dispositivos inalámbricos.

¿En qué caso elegiría la opción **Mixed** (Combinada)?

R: Cuando hay dispositivos inalámbricos que constan de B, G o N.

- l. Configure el modo de red en **Wireless-N Only** (Solo Wireless-N).

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
 Código del curso 203092 – Diplomado de Profundización Cisco
 Paso 3 – Actividad Colaborativa 2

Basic Wireless Settings	
Network Mode:	Wireless-N Only
Network Name (SSID):	Default
Radio Band:	Auto
Wide Channel:	Auto
Standard Channel:	1 - 2.412GHz
SSID Broadcast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

m. Cambie el SSID a **MiRedDoméstica**.

¿Cuáles son dos características de un SSID?

R: Distingue mayúsculas de minúsculas y el nombre no puede exceder los 32 caracteres.

d. Cuando un cliente inalámbrico busca redes inalámbricas en el área, este detecta cualquier transmisión del SSID. Las transmisiones del SSID están habilitadas de manera predeterminada.

Si no se transmite el SSID de un punto de acceso, ¿cómo se conectan los dispositivos a este?

R: El cliente debe estar configurado con el nombre, el cual debe estar escrito correctamente para que se lleve a cabo la conexión.

e. Para obtener el mejor rendimiento de una red que utiliza Wireless-N, configure la banda de radio en **Wide-40MHz** (40 MHz de ancho).

Basic Wireless Settings	
Network Mode:	Wireless-N Only
Network Name (SSID):	MyHomeNetwork
Radio Band:	Wide - 40MHz Channel
Wide Channel:	3
Standard Channel:	1 - 2.412GHz
SSID Broadcast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

f. Haga clic en **Save settings** (Guardar configuración) y, a continuación, haga clic en **Continue** (Continuar).

Paso 5: Configure la seguridad inalámbrica de modo que los clientes deban autenticarse para

poder conectarse a la red inalámbrica.

- Haga clic en la opción **Wireless Security** (Seguridad inalámbrica) en la ficha **Wireless**.
- Configure el **Security Mode** (Modo de seguridad) en **WPA2 Personal**.

The screenshot shows the 'Wireless Security' configuration page. The 'Security Mode' dropdown is set to 'WPA2 Personal'. The 'Encryption' dropdown is set to 'AES'. The 'Passphrase' field is empty. The 'Key Renewal' field is set to '3600' seconds. A 'Help...' button is visible on the right side of the page.

¿Cuál es la diferencia entre la opción Personal y la opción Enterprise (Empresa)?
R: La opción Enterprise utiliza un servidor Radius para autenticar a los usuarios, mientras que el modo Personal utiliza el router Linksys para autenticar los usuarios.

- Deje el modo de encriptación en AES y establezca la frase de contraseña **itsasecret**.

This screenshot is similar to the previous one, but the 'Passphrase' field now contains the text 'itsasecret'.

- Haga clic en **Save settings** (Guardar configuración) y, a continuación, haga clic en **Continue** (Continuar).

Paso 6: Cambie la contraseña predeterminada para acceder a la configuración del router Linksys.

- Siempre debe cambiar la contraseña predeterminada. Haga clic en la ficha **Administration** (Administración) y cambie la contraseña de **Router Access** (Acceso al router) por **letmein**.

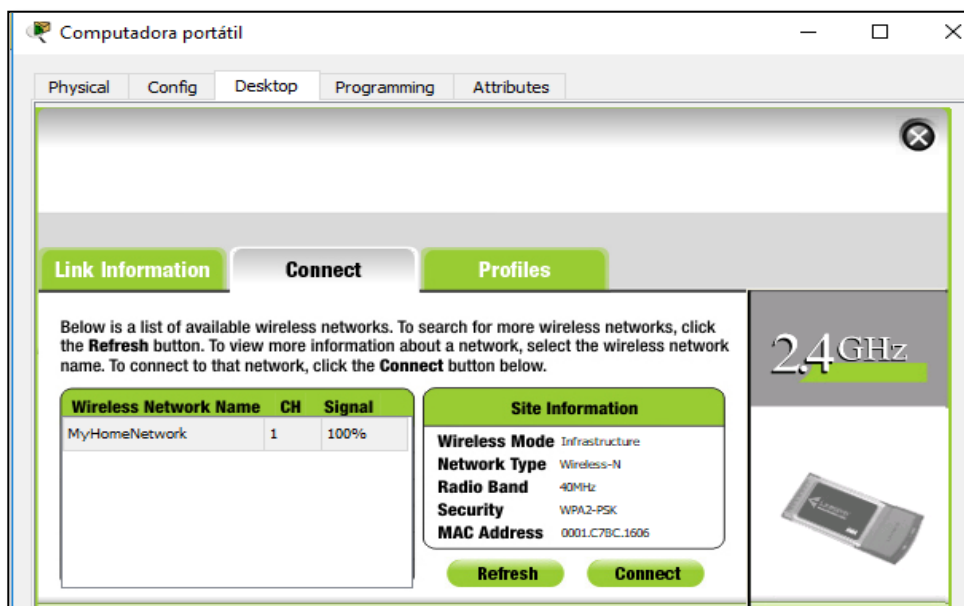
The screenshot shows the 'Router Access' configuration page. It has two input fields: 'Router Password:' and 'Re-enter to confirm:'. Both fields contain a series of black dots, indicating that a password has been entered and is being confirmed.

- b. Haga clic en **Save Settings**. Introduzca el nombre de usuario **admin** y la nueva contraseña.

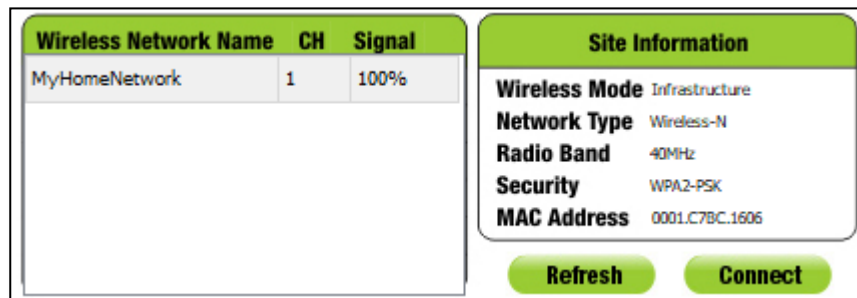
Parte 3: Configurar y verificar el acceso al cliente inalámbrico

Paso 1: Configurar la computadora portátil para acceder a la red inalámbrica

- a. Haga clic en **Laptop** (Computadora portátil) y después en **Desktop > PC Wireless** (PC inalámbrica). La ventana que se abre es la GUI de Linksys del cliente.
- b. Haga clic en la ficha **Connect** (Conectar) y después en **Refresh** (Actualizar), si es necesario. Debería ver la red **MiRedDoméstica** indicada en Wireless Network Name (Nombre de red inalámbrica).

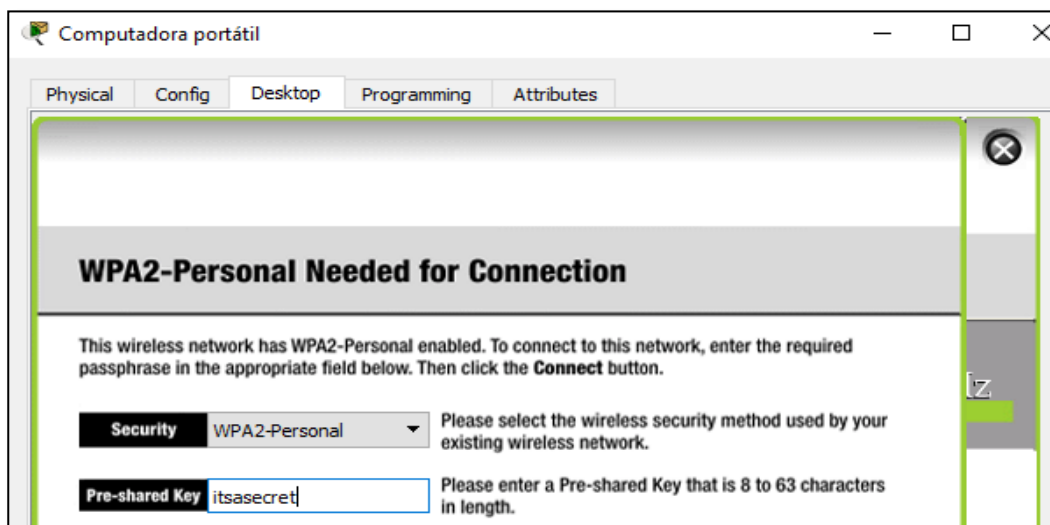


- c. Haga clic en **MiRedDoméstica** y después en **Connect**.

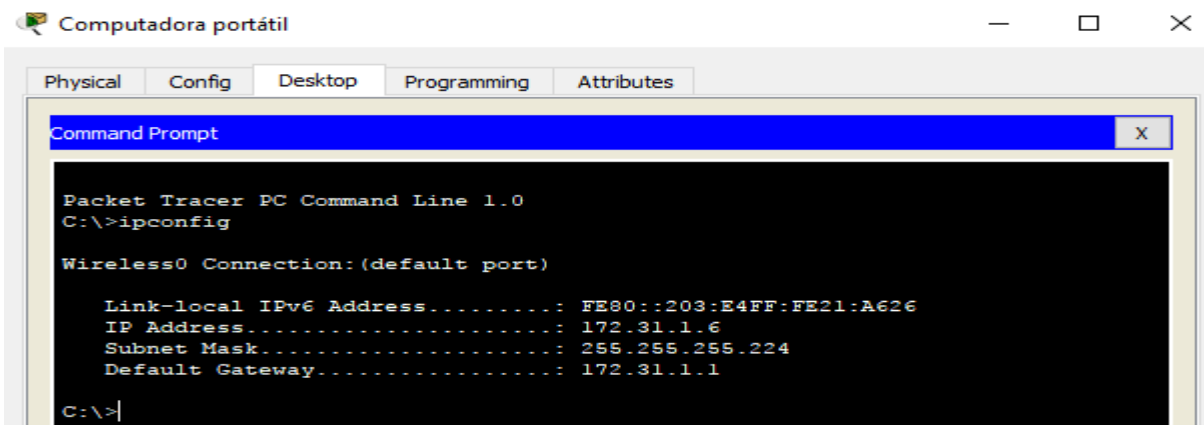


ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- d. Ahora debería ver la red **MiRedDoméstica**. Haga clic en esta y después en **Connect**.
- e. La **Pre-shared Key** (Clave previamente compartida) es la contraseña que configuró en el paso 5c de la parte 2. Introduzca la contraseña y haga clic en **Connect**.



- f. Cierre la GUI de Linksys y haga clic en **Command Prompt** (Símbolo del sistema). Introduzca el comando **ipconfig** para verificar si **Laptop** recibió el direccionamiento IP.



Paso 2: Verificar la conectividad entre la computadora portátil y el Host-A

- a. Haga ping al router **Linksys** desde la **computadora portátil**.

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

```

C:\>ping 172.31.1.1

Pinging 172.31.1.1 with 32 bytes of data:

Reply from 172.31.1.1: bytes=32 time=20ms TTL=255
Reply from 172.31.1.1: bytes=32 time=9ms TTL=255
Reply from 172.31.1.1: bytes=32 time=14ms TTL=255
Reply from 172.31.1.1: bytes=32 time=13ms TTL=255

Ping statistics for 172.31.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 20ms, Average = 14ms

C:\>
  
```

b. Haga ping desde el **Host-A** a la **computadora portátil**.

```

C:\>ping 172.31.1.6

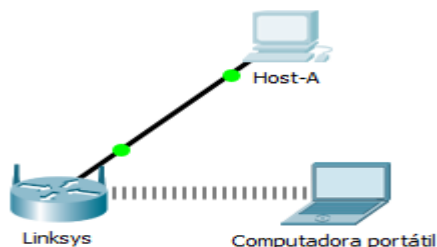
Pinging 172.31.1.6 with 32 bytes of data:

Reply from 172.31.1.6: bytes=32 time=13ms TTL=128
Reply from 172.31.1.6: bytes=32 time=9ms TTL=128
Reply from 172.31.1.6: bytes=32 time<1ms TTL=128
Reply from 172.31.1.6: bytes=32 time=1ms TTL=128

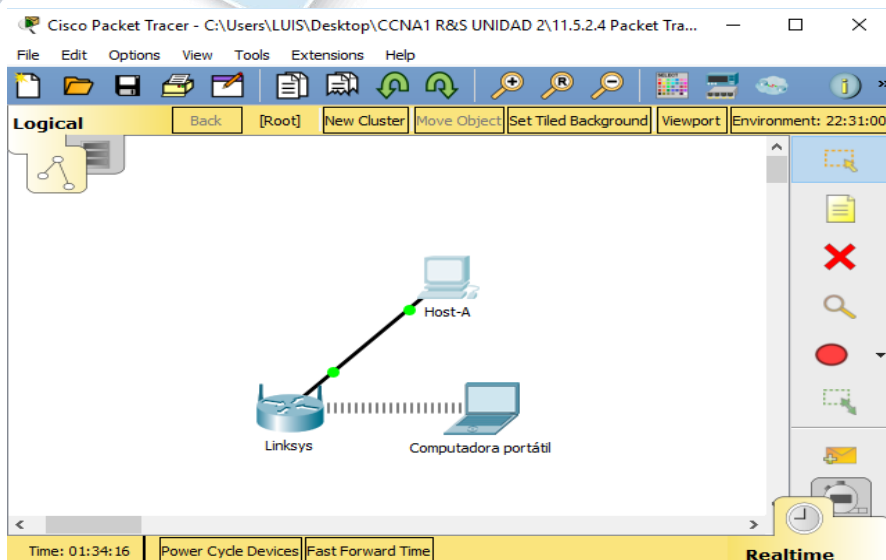
Ping statistics for 172.31.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 5ms

C:\>
  
```

Conexión Red final



ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2



Ejercicio 11.6.1.2: Reto de habilidades de integración

Topología

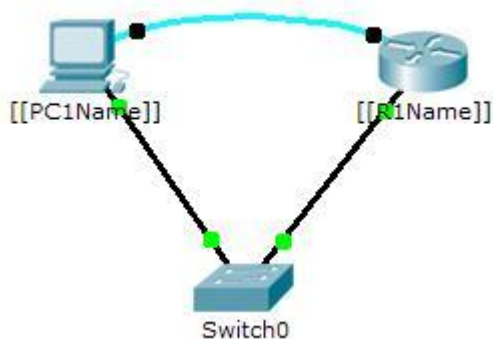


Tabla de direccionamiento

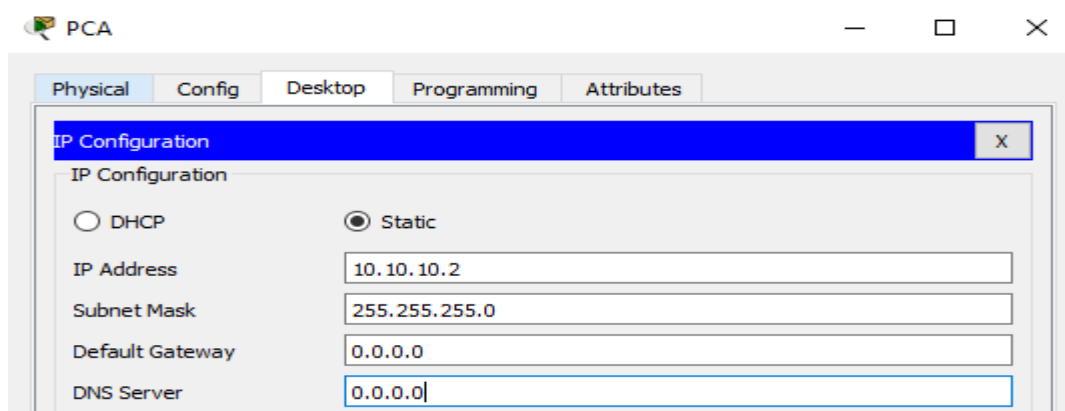
Dispositivo	Interfaz	Dirección IP	Máscara de subred
RTA	G0/0	10.10.10.1	255.255.255.0
PCA	NIC	10.10.10.2	255.255.255.0

Situación

El administrador de red le solicitó que prepare un router para la implementación. Antes de que pueda conectarse a la red, se deben habilitar las medidas de seguridad. En esta actividad, encriptará y configurará contraseñas seguras. A continuación, configurará SSH para obtener acceso remoto y demostrará que puede acceder al router desde una PC.

Requisitos

- Configure el direccionamiento IP en **PCA** y **RTA**.



```
Router>enable
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface g0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shut

Router(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
```

```
Router(config-if)#
```

- Configure el nombre de host como **RTA** y encripte todas las contraseñas de texto no cifrado.

```
Router(config-if)#exit
Router(config)#hostname RTA
RTA(config)#service password-encryption
RTA(config)#
```

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 3 – Actividad Colaborativa 2

- Establezca la contraseña secreta segura que desee.

```
RTA(config)#enable secret Ci$coLetmein
RTA(config)#
```

- Establezca el nombre de dominio en RTA (distinguir mayúsculas de minúsculas).

```
RTA(config)# ip domain-name RTA1
```

```
RTA(config)#ip domain-name RTA
RTA(config)#
```

- Cree un usuario de su elección con una contraseña segura.

```
RTA (config) # user Luis password Ci$co001
```

```
RTA(config)#user Luis password Ci$co001
RTA(config)#
```

- Genere claves RSA de 1024 bits.

Nota: en Packet Tracer, introduzca el comando **crypto key generate rsa** y presione tecla **Entrar** para continuar.

```
RTA(config)# crypto key generate rsa
```

```
RTA(config)#crypto key generate rsa
The name for the keys will be: RTA.RTA
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]

RTA(config)#
```

- y. Bloquee durante tres minutos a cualquier persona que no pueda iniciar sesión después de cuatro intentos en un período de dos minutos.

```
[[R1Name]](config)# login block-for 180 attempts 4 within 120
```


ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
 Código del curso 203092 – Diplomado de Profundización Cisco
 Paso 3 – Actividad Colaborativa 2

```
RTA(config)#login block-for 180 attempts 4 within 120
*mar. 1 1:18:40.588: %SSH-5-ENABLED: SSH 1.99 has been enabled
RTA(config)#
```

- z. Configure las líneas vty para el acceso por SSH y solicite los perfiles de usuarios locales.

```
RTA(config)#line vty 0 15
RTA(config-line)#transport input ssh
RTA(config-line)#login local
RTA(config-line)#
```

- aa. Guardar la configuración en la NVRAM.

```
RTA#copy running startup
Destination filename [startup-config]?
Building configuration...
[OK]
RTA#
```

- bb. Esté preparado para demostrar al instructor que estableció el acceso por SSH de **PCA a RTA**.

ID:10

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 1 – Actividad Colaborativa 1

The screenshot shows a Windows Command Prompt window titled 'Command Prompt' with a blue header bar. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The terminal output is as follows:

```
C:\>ssh
Packet Tracer PC SSH

Usage: SSH -l username target

C:\>ssh -l Luis 10.10.10.1
Open
Password:

RTA>enable
Password:
RTA#
```

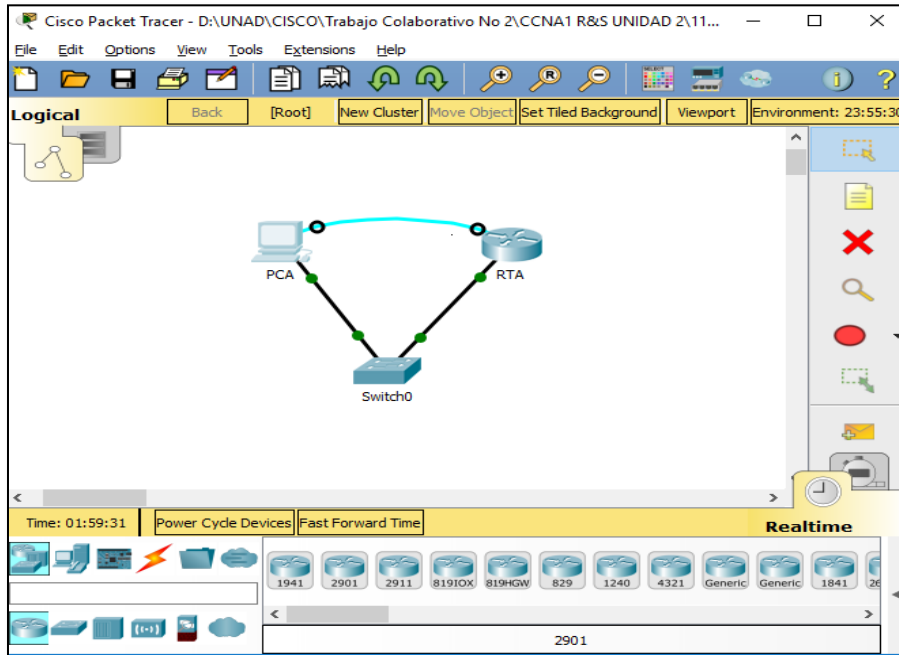
```
RTA#show running
Building configuration...

Current configuration : 1211 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname RTA
!
login block-for 180 attempts 4 within 120
!
enable secret 5 $1$mERr$oYgkCA110OcOAKSkOlk2D.
!
ip cef
no ipv6 cef
!
username Luis password 7 0802450A0A16554743
username any_Luis password 7 08204257363A0C5311044F547A7A
```

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Código del curso 203092 – Diplomado de Profundización Cisco
Paso 1 – Actividad Colaborativa 1

```
PCA  
Physical Config Desktop Programming Attributes  
Command Prompt  
deny tcp any any eq 22  
permit tcp any any eq 22  
!  
no cdp run  
!  
!  
!  
!  
!  
!  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
exec-timeout 15 0  
login local  
transport input ssh  
line vty 5 15  
login local  
transport input ssh  
!  
!  
!  
end  
RTA#  
 Top
```


Red final



CONCLUSIONES

Al haber concluido el desarrollo del presente trabajo se pudo establecer la importancia de los conocimientos adquiridos en los temas estudiados en la unidad dos, en total se desarrollaron 22 ejercicios utilizando el simulador de red Packet Tracer.

Se lograron identificarán y solucionar los problemas de las sub-redes y del direccionamiento IP mediante el uso adecuado de las estrategias basadas en comandos y estadísticas del IOS, con el cual se logró fortalecer el desarrollo de las competencias en el área de las redes orientadas al enrutamiento avanzado.



REFERENCIAS BIBLIOGRAFICAS

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de:
<https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking.
Recuperado de: <https://static-course-sssets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de:
<https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de:
<https://static-course-ssets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1>

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de:
<https://static-course-ssets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>

UNAD (2014). PING y TRACER como estrategia en procesos de Networking [OVA].
Recuperado de: <https://1drv.ms/u/s!AmIJYei-NT1lhgTCtKY-7F5KIRC3>

