DIPLOMADO DE PROFUNDIZACION CISCO

CARLOS ALDEMAR CAICEDO
HECTOR FABIO ESCOBAR
ALEXANDER GARCIA
LUIS HELMER MARTINEZ
JOSE RAMON VALENCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
PROGRAMA INGENIERÍA DE TELECOMUNICACIONES
PALMIRA
2016

DIPLOMADO DE PROFUNDIZACION CISCO

CARLOS ALDEMAR CAICEDO
HECTOR FABIO ESCOBAR
ALEXANDER GARCIA
LUIS HELMER MARTINEZ
JOSE RAMON VALENCIA

Diplomado de profundización CISCO (diseño e Implementación de soluciones integradas LAN/WAN)

Edgar Rodrigo Enríquez
Tutor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
PROGRAMA INGENIERÍA DE TELECOMUNICACIONES
PALMIRA
2016

_____

Firma del jurado

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del jurado

Santiago de Cali, 10 de agosto del 2021

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

RESUMEN

La sociedad necesita ir a la vanguardia de los avances tecnológicos e informáticos para facilitar ciertos aspectos de la vida, el trabajo, la educación y el entretenimiento; y es por esto por lo que las redes de datos se han convertido en un sistema de comunicación de gran importancia para mantener a millones de usuarios conectados de una forma confiable y segura.

Las redes de comunicaciones han beneficiado a un sin número de empresas permitiéndoles aprovechar sus recursos informáticos de una manera más rápida y fácil, ahorrando costes en hardware, software y espacio, obteniendo mayores velocidades de transmisión de datos y compartiendo eficientemente sus recursos informáticos.

PALABRAS CLAVES: CISCO, Datos, Hardware, Software, Velocidad.

ABSTRACT

Society needs to be at the forefront of technological and computing advances to facilitate certain aspects of life, work, education and entertainment; and that is why data networks have become a communication system of great importance to keep millions of users connected in a reliable and secure way.

Communication networks have benefited countless companies by allowing them to take advantage of their IT resources in a faster and easier way, saving costs in hardware, software and space, obtaining higher data transmission speeds and efficiently sharing their IT resources.

KEYWORDS: CISCO, Data, Hardware, Software, Speed.

INTRODUCCIÓN

En la mayoría de estas empresas se hace necesario tener personal capacitado en la instalación, configuración y administración de estas redes, y el curso CCNA II brinda las bases para lograrlo. En este trabajo se encuentra el desarrollo de la actividad colaborativa que comprende prácticas de los capítulos del 1 al 6 del CCNA II y en el cual se ha consignado los aportes de un equipo de trabajo.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Identificar y solucionar problemas propios de enrutamiento mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces.

2.2 OBJETIVOS ESPECÍFICOS

- Representar una red con el programa de simulación Packet Tracer.
- Comprender el funcionamiento de los diferentes dispositivos de una red.
- Aprender a conectar dispositivos de red a través de diferentes medios físicos.
- Aprender los comandos necesarios para la configuración de dispositivos de capa 2 y capa 3.
- Identificar los eventos que se generan en el envío de un paquete de datos.
- Desarrollar habilidades de Ruteo que permitan conectar dos redes remotas.

5.3 Desarrollo de la actividad

- **Numeral 1.2.4.4**

Paso 1: Acceder a las páginas de ayuda, a videos de tutoriales y a los recursos en línea de Packet Tracer

a. Acceda a las páginas de ayuda de Packet Tracer de dos maneras:

1) Haga clic en el ícono de signo de interrogación que está en la esquina superior derecha de la barra de herramientas del menú.

Figura 1.0

Fuente propia

2) Haga clic en el menú **Help** (Ayuda) y, a continuación, seleccione **Contents** (Contenido)

Figura 1.1

Fuente propia

b. Acceda a los videos de tutoriales de Packet Tracer haciendo clic en **Help** > **Tutorials** (Tutoriales). Estos videos son una demostración visual de la información que se encuentra en las páginas de **ayuda** y diversos aspectos del programa de software Packet Tracer. Antes de continuar con esta actividad, debe familiarizarse con la interfaz y el modo de simulación de Packet Tracer.

Figura 1.2

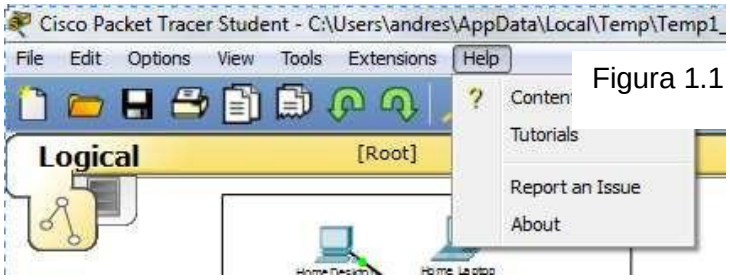


Figura 1.1

Fuente propia

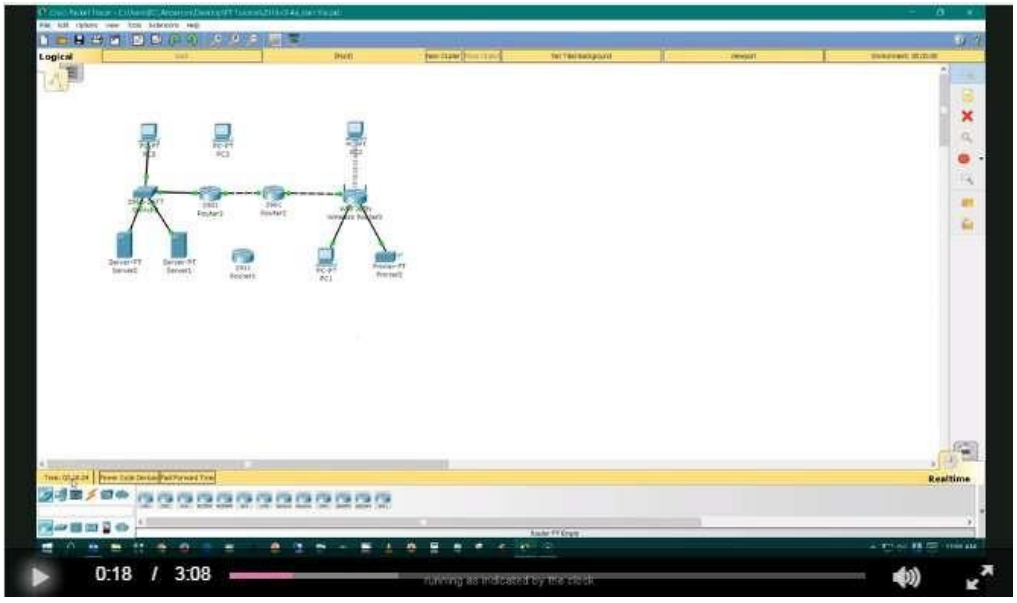
1) Vea el video **Interface Overview** (Descripción general de la interfaz) en la sección **Getting Started** (Introducción) de Tutorials.

Figura 1.3

Fuente propia

2) Vea el video **Simulation Environment** (Entorno de simulación) en la sección **Realtime and Simulation Modes** (Modos de tiempo real y de simulación) de **Tutorials**.

Figura 1.4



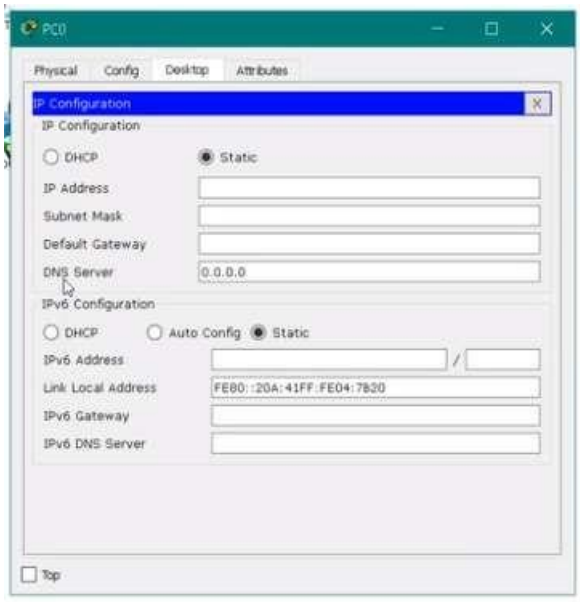
Fuente propia

c. Busque el tutorial “Configuring Devices Using the Desktop Tab” (Configuración de dispositivos mediante la ficha Desktop [Escritorio]). Mire la primera parte para responder la siguiente pregunta: ¿Qué información se puede configurar en la ventana IP Configuration (Configuración IP)?

R/ Se puede configurar los siguientes parámetros:

- El tipo de direccionamiento, es decir si la dirección es estática o dinámica por medio de servidor DHCP.
- La dirección IP
- La máscara de subred
- La puerta de Enlace
- El servidor DNS
- Parámetros para direccionamiento IPv6

Figura 1.5

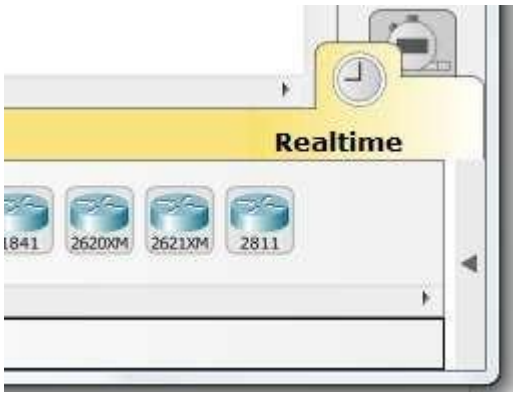


Fuente propia

Paso 2: Alternar entre los modos de tiempo real y de simulación

a. Busque la palabra **Realtime** (Tiempo real) en la esquina inferior derecha de la interfaz de Packet Tracer. En el modo de tiempo real, la red siempre funciona como una red real, ya sea que trabaje en la red o no. La configuración se realiza en tiempo real, y la red responde prácticamente en tiempo real.

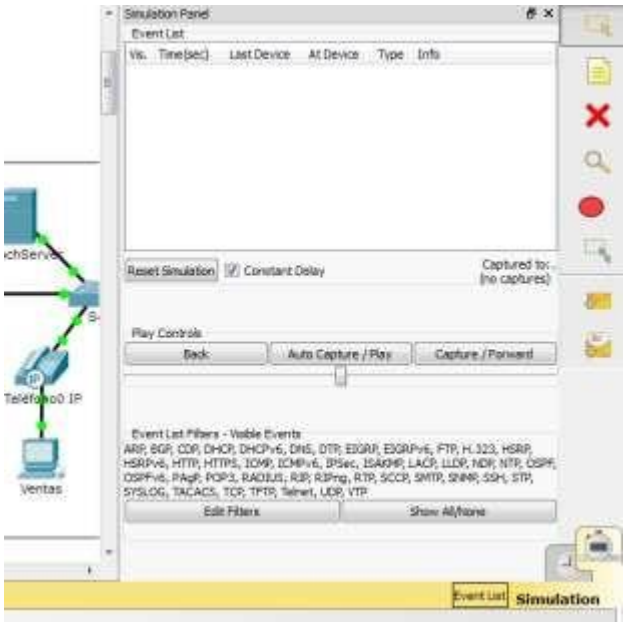
Figura 1.6



Fuente propia

b. Haga clic en la ficha que está justo detrás de la ficha **Realtime** para cambiar al modo **Simulation** (Simulación). En el modo de simulación, puede ver la red en funcionamiento a menor velocidad, lo que le permite observar las rutas por las que viajan los datos e inspeccionar los paquetes de datos en detalle.

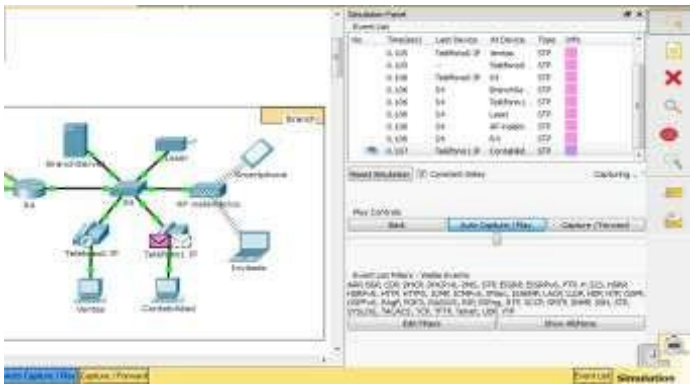
Figura 1.7



Fuente propia

c. En el panel de simulación, haga clic en **Auto Capture / Play** (Captura/reproducción automática). Ahora debería ver los paquetes de datos, que se representan con sobres de diversos colores, que viajan entre los dispositivos.

Figura 1.8

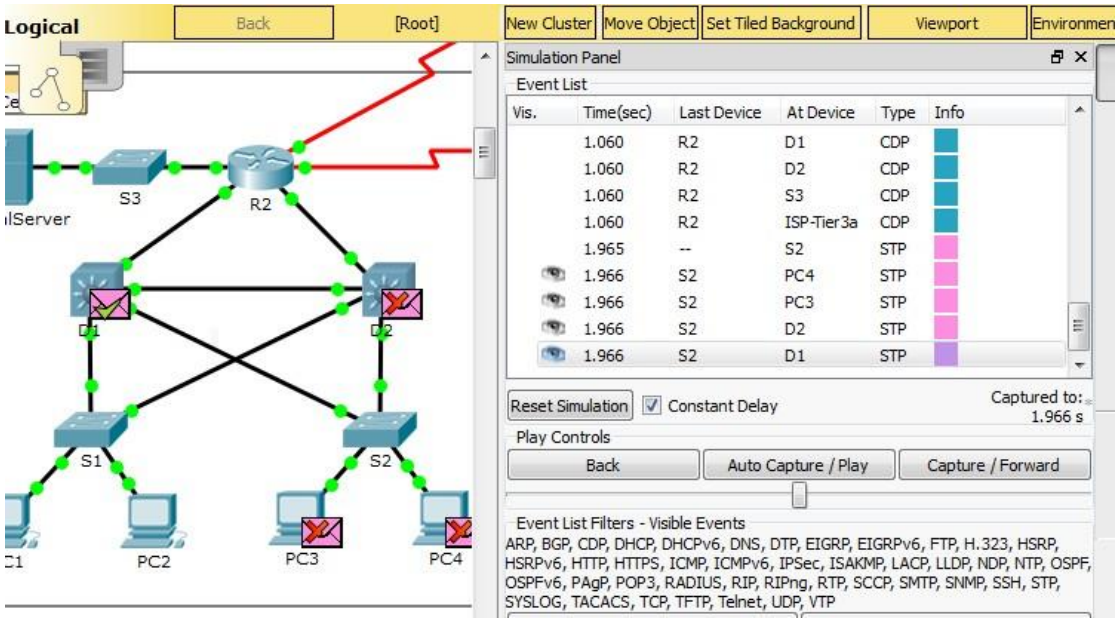


Fuente propia

d. Haga clic en **Auto Capture / Play** nuevamente para pausar la simulación.

e. Haga clic en **Capture / Forward** (Capturar/avanzar) para avanzar en la simulación. Haga clic en este botón algunas veces más para ver el efecto.

Figura 1.9

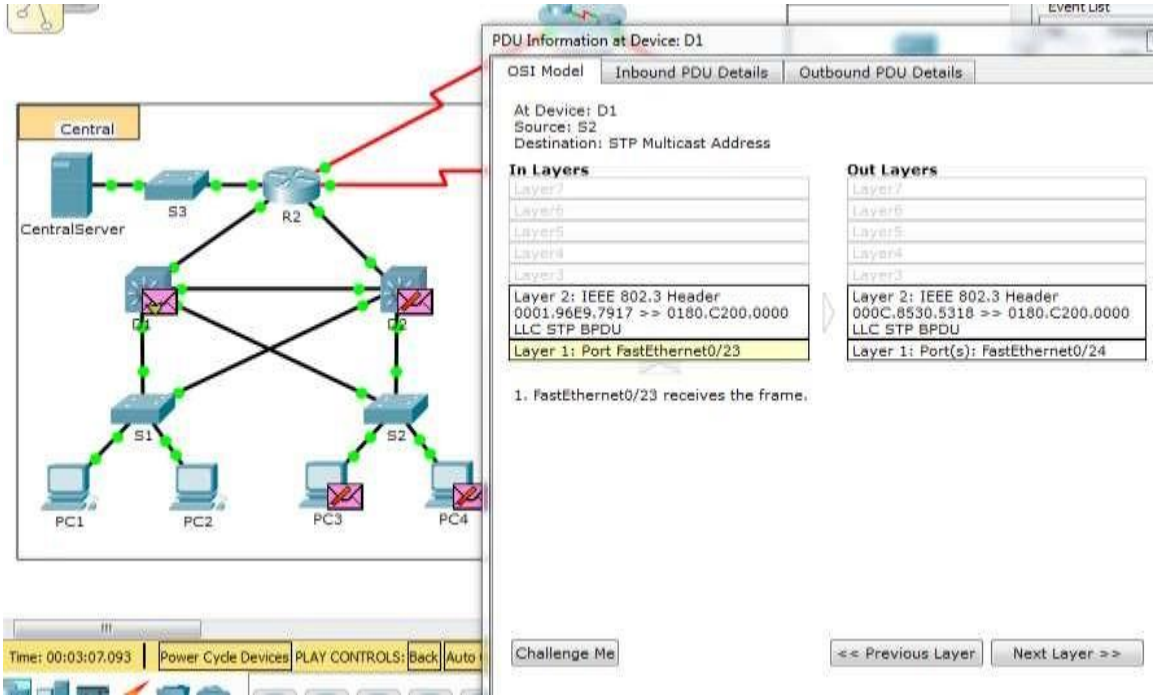


Fuente propia

f. En la topología de la red a la izquierda, haga clic en cualquiera de los sobres en un dispositivo intermediario e investigue qué hay dentro. En el curso de sus

estudios de CCNA, aprenderá el significado la mayor parte del contenido de estos sobres. Por el momento, intente responder las siguientes preguntas:

Figura 2.0



Fuente propia

En la **ficha OSI Model** (Modelo OSI), ¿cuántas **In Layers** (Capas de entrada) y **Out Layers** (Capas de salida) tienen información?

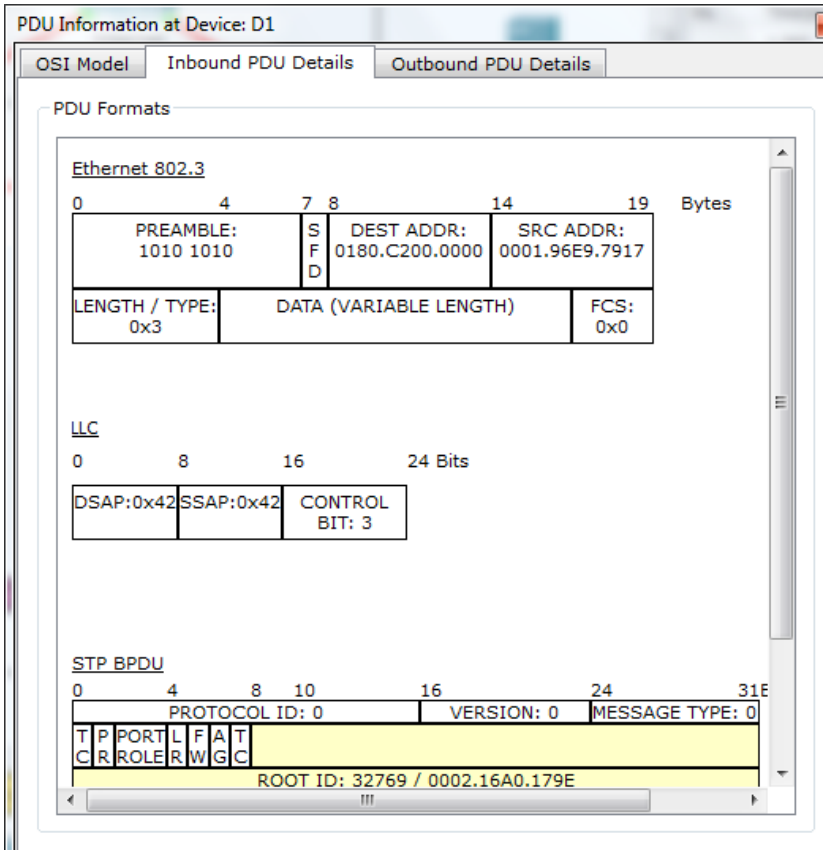
R/ En las capas de entrada, la capa 1 y 2 tienen información. En las capas de salida, la capa 1 y 2 tienen información.

En las fichas **Inbound PDU Details** (Detalles de la PDU de entrada) y **Outbound PDU Details** (Detalles de la PDU de salida), ¿cuáles son los encabezados de las secciones principales?

R/ Los encabezados son:

PREAMBLE, DEST ADDR, SRC ADDR, LENGTH/TYPE, DATA (VARIABLE LENGTH), FCS

Figura 2.



Fuente propia

Alterne entre las fichas **Inbound PDU Details** y **Outbound PDU Details**. ¿Observa cambios en la información? Si es así, ¿qué es lo que cambia?

R/ Cambian en la dirección de origen y el costo de la ruta

Paso 3: Alternar entre las vistas Logical y Physical

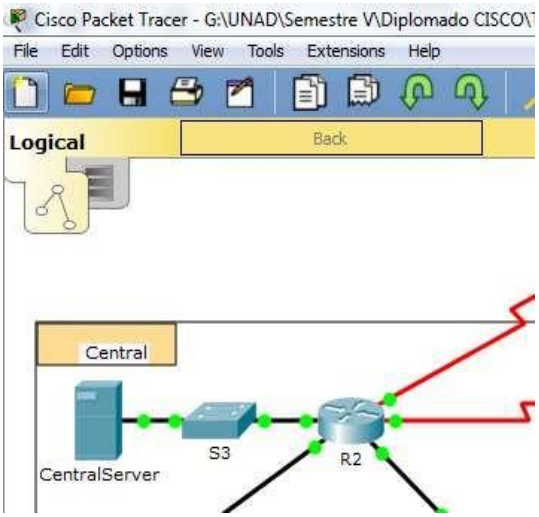
a. Busque la palabra **Logical** (Lógico) en la esquina superior izquierda de la interfaz de Packet Tracer. Actualmente se encuentra en el área de trabajo **Logical**, donde pasará la mayor parte del tiempo de creación, configuración, investigación y resolución de problemas de redes.

Figura 2.

Fuente propia

b. Haga clic en la ficha que está debajo **Logical** para pasar al área de trabajo **Physical** (Físico). El propósito del área de trabajo **Physical** es darle una dimensión física a la topología lógica de la red. Le da una idea de la escala y la ubicación (cómo se vería la red en un entorno real).

Figura 2.3

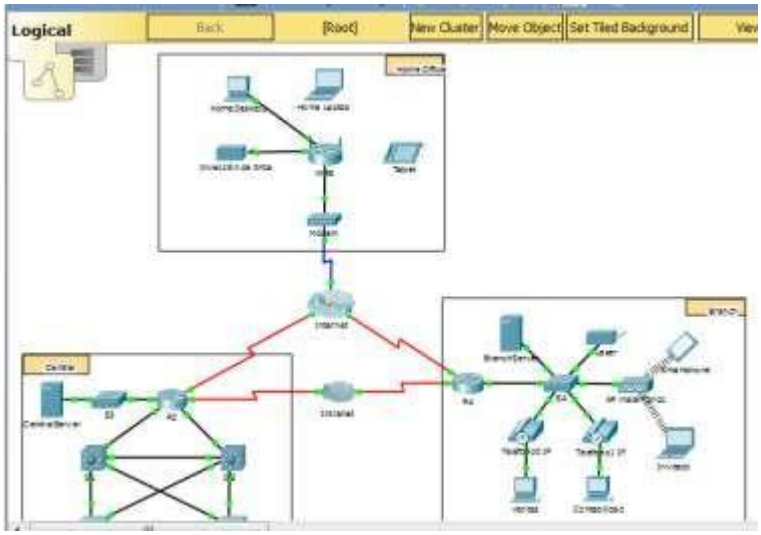


Fuente propia

c. Durante sus estudios en CCNA, utilizará esta área de trabajo de manera ocasional. Por el momento, solo debe saber que ese espacio está allí, disponible para que lo utilice. Para obtener más información sobre el área de trabajo Physical, consulte los archivos de ayuda y los videos de tutoriales.

d. Haga clic en el botón de alternancia ubicado debajo de **Physical** en la esquina superior derecha para volver al área de trabajo **Logical**.

Figura 2.4



Fuente propia

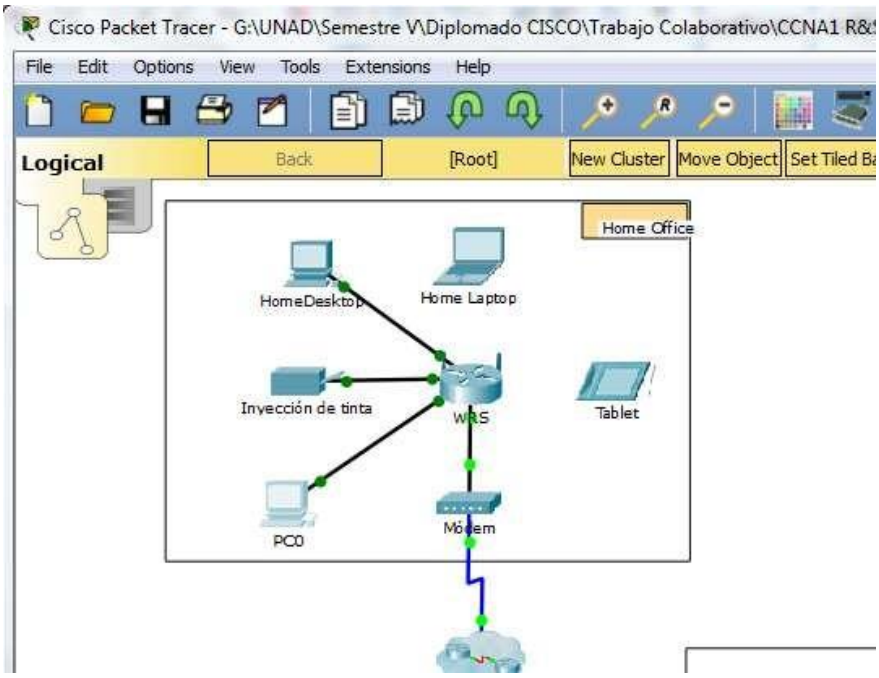
Desafío:

Ahora que tuvo la oportunidad de explorar la red representada en esta actividad de Packet Tracer, es posible que haya adquirido algunas habilidades que quiera poner en práctica o tal vez desee tener la oportunidad de analizar esta red en mayor detalle. Puede reconocer que la mayor parte de lo que ve y experimenta en Packet Tracer supera su nivel de habilidad en este momento. Sin embargo, los siguientes son algunos desafíos que tal vez quiera probar. No se preocupe si no puede completarlos todos. Muy pronto se convertirá en un usuario y diseñador de redes experto en Packet Tracer.

Agregue un dispositivo final a la topología y conéctelo a una de las LAN con una conexión de medios. ¿Qué otra cosa necesita este dispositivo para enviar datos a otros usuarios finales? ¿Puede proporcionar la información? ¿Hay alguna manera de verificar que conectó correctamente el dispositivo?

R/ Se agrega dispositivo final PC0 conectándolo al Router inalámbrico WRS con una interface Fast-Ethernet. Creo que la conexión se encuentra bien hecha por el color verde que muestra en los dos extremos del conector, aunque podría faltar una dirección IP y una puerta de enlace diferente a la que asigna por defecto.

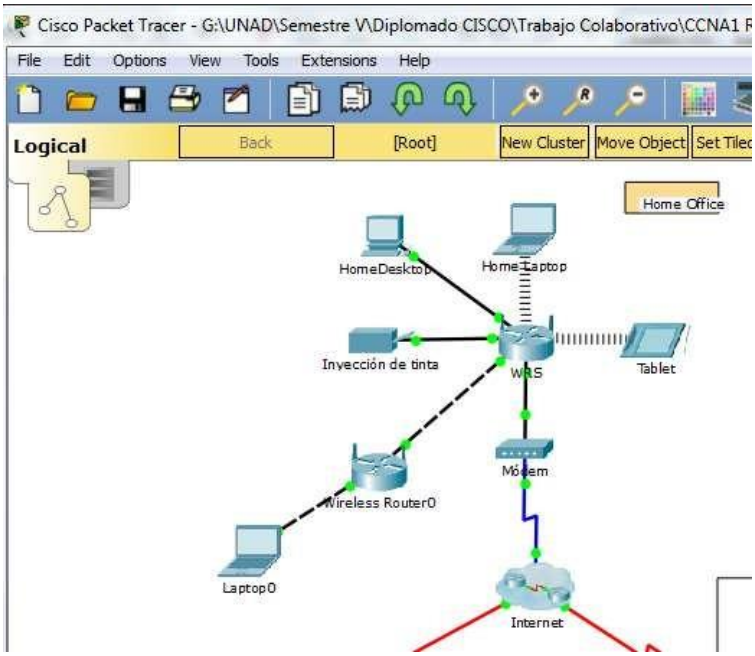
Figura 2.5



Fuente propia

Agregue un nuevo dispositivo intermediario a una de las redes y conéctelo a uno de las LAN o WAN con una conexión de medios. ¿Qué otra cosa necesita este dispositivo para funcionar como intermediario de otros dispositivos en la red?

Figura 2.6



Fuente propia

R/ Como se puede observar, se conectó un Router Inalámbrico (Router0) entre la Laptop0 y WRS.

Abra una nueva instancia de Packet Tracer. Cree una nueva red con, al menos, dos redes LAN conectadas mediante una WAN. Conecte todos los dispositivos. Investigue la actividad de Packet Tracer original para ver qué más necesita hacer para que la nueva red esté en condiciones de funcionamiento. Registre sus comentarios y guarde el archivo de Packet Tracer. Tal vez desee volver a acceder a la red cuando domine algunas habilidades más.

- **Numeral 2.1.4.8**

Parte 1: Conexiones básicas, acceso a la CLI y exploración de ayuda

En la parte 1 de esta actividad, conectará una PC a un switch mediante una conexión de consola e investigará diferentes modos de comando y características de ayuda.

Paso 1: La conexión de la PC1 a S1 requiere un cable de consola.

a. Haga clic en el ícono **Connections** (Conexiones), similar a un rayo, en la esquina inferior izquierda de la ventana de Packet Tracer.

Figura 2.7

Fuente propia

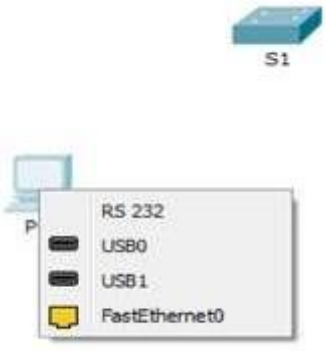
b. Haga clic en el cable de consola celeste para seleccionarlo. El puntero del mouse cambia a lo que parece ser un conector con un cable que cuelga de él.

Figura 2.8

Fuente propia

c. Haga clic en **PC1**. Aparece una ventana que muestra una opción para una conexión RS-232.

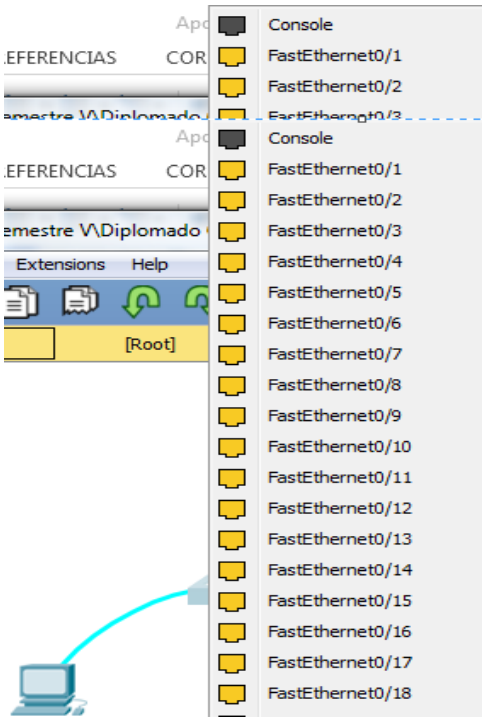
Figura 2.9



Fuente propia

d. Arrastre el otro extremo de la conexión de consola al switch S1 y haga clic en el switch para abrir la lista de conexiones.

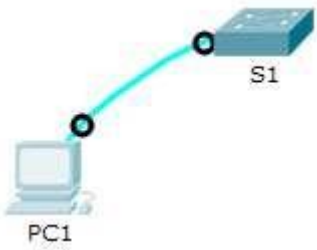
Figura 3.0



Fuente propia

e. Seleccione el puerto de consola para completar la conexión.

Figura 3.1

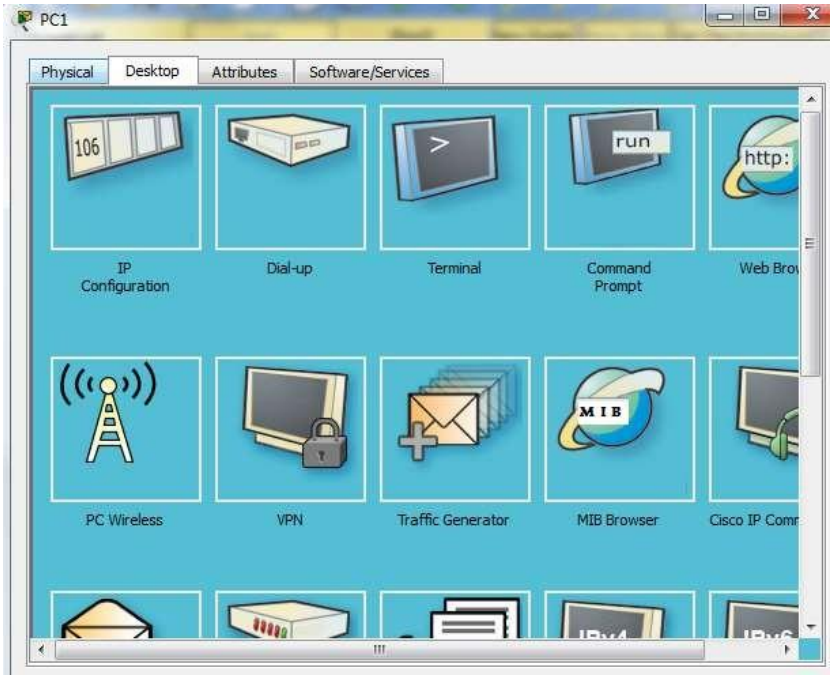


Fuente propia

Paso 2: Establezca una sesión terminal con S1.

a. Haga clic en **PC1** y después en la ficha **Desktop** (Escritorio).

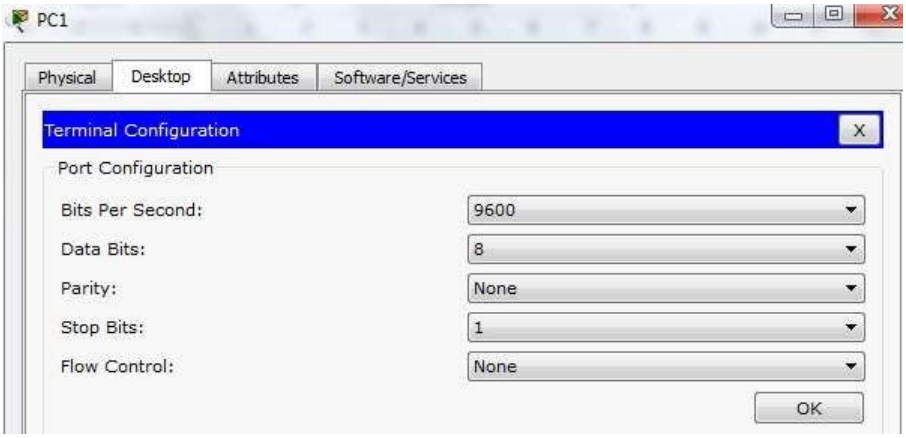
Figura 3.2



Fuente propia

b. Haga clic en el ícono de la aplicación **Terminal**. Verifique que la configuración predeterminada de Port Configuration (Configuración del puerto) sea la correcta.

Figura 3.3



Fuente propia

¿Cuál es el parámetro de bits por segundo?

R/ 9600 bits por segundo

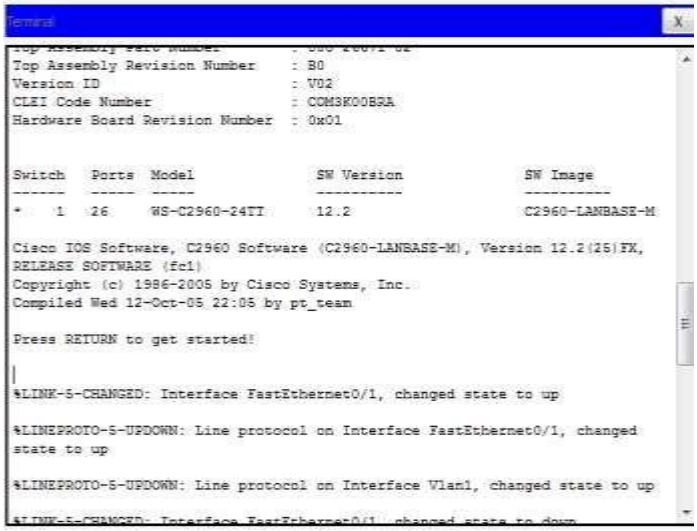
c. Haga clic en **OK** (Aceptar).

d. La pantalla que aparece puede mostrar varios mensajes. En alguna parte de la pantalla tiene que haber un mensaje que diga Press RETURN to get started! (Presione REGRESAR para comenzar) . Presione **Entrar**.

¿Cuál es la petición de entrada que aparece en la pantalla?

R/ S1>

Figura 3.4



Fuente propia

Paso 3: Explore la ayuda de IOS.

a. El IOS puede proporcionar ayuda para los comandos según el nivel al que se accede. La petición de entrada que se muestra actualmente se denomina **Modo EXEC del usuario** y el dispositivo está esperando un comando. La forma más básica de solicitar ayuda es escribir un signo de interrogación (?) en la petición de entrada para mostrar una lista de comandos.

S1> **?**

Figura 3.5

```
S1>?
Exec commands:
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
S1>
```

Fuente propia

¿Qué comando comienza con la letra “C”?

R/ el comando connect

b. En la petición de entrada, escriba **t**, seguido de un signo de interrogación (**?**).

S1> **t?**

Figura 3.6

```
S1>t?
telnet  terminal  traceroute
S1>t
```

Fuente propia

¿Qué comandos se muestran?

R/ Se muestran los comandos que empiezan con la letra ***“t”*** como ***telnet, terminal y traceroute***

c. En la petición de entrada, escriba **te**, seguido de un signo de interrogación (**?**).

S1> **te?**

Figura 3.7

```
S1>te?
telnet  terminal
S1>te
```

Fuente propia

¿Qué comandos se muestran?

R/ Se muestran los comandos que empiezan con ***"te"***

Este tipo de ayuda se conoce como **ayuda contextual**, ya que proporciona más información a medida que se amplían los comandos.

Parte 2: Exploración de los modos EXEC

En la parte 2 de esta actividad, debe cambiar al modo EXEC privilegiado y emitir comandos adicionales.

Paso 1: Entre al modo EXEC privilegiado.

a. En la petición de entrada, escriba el signo de interrogación (**?**).

S1> **?**

Figura 3.8

```
S1>?
Exec commands:
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
S1>
```

Fuente propia

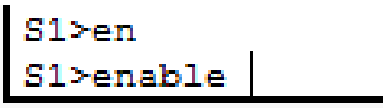
¿Qué información de la que se muestra describe el comando **enable**?

R/ El comando Enable habilita los comandos privilegiados

b. Escriba **en** y presione la tecla **Tabulación**.

S1> **en<Tabulación>**

Figura 47



Fuente propia

¿Qué se muestra después de presionar la tecla **Tabulación**?

R/Completa la palabra del comando Enable

Esto se denomina completar un comando o completar la tabulación. Cuando se escribe parte de un comando, la tecla **Tabulación** se puede utilizar para completar el comando parcial. Si los caracteres que se escriben son suficientes para formar un comando único, como en el caso del comando **enable**, se muestra la parte restante.

¿Qué ocurriría si escribiera **te<Tabulación>** en la petición de entrada?

R/ No aparece nada ya que hay dos comandos que empiezan con esas letras, los cuales son terminal y telnet

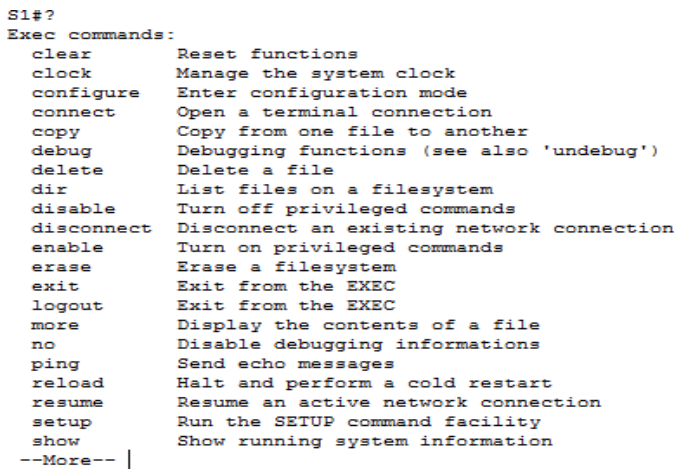
c. Introduzca el comando **enable** y presione tecla **Entrar**. ¿En qué cambia la petición de entrada?

   R/ Cambia a ***S1#***

d. Cuando se le solicite, escriba el signo de interrogación (**?**).

   S1# **?**

Figura 48



Fuente propia

Antes había un comando que comenzaba con la letra “C” en el modo EXEC del usuario. ¿Cuántos comandos se muestran ahora que está activo el modo EXEC privilegiado? (**Sugerencia**: puede escribir c? para que aparezcan solo los comandos que comienzan con la letra “C”).

R/ Aparecen 20 comandos.

Paso 2: Entre al modo de configuración global.

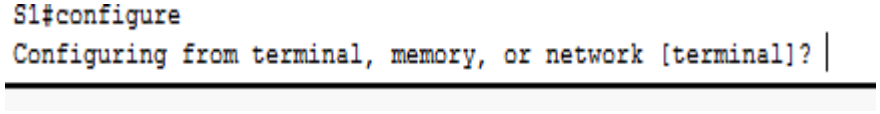
a. Cuando se está en el modo EXEC privilegiado, uno de los comandos que comienzan con la letra “C” es **configure**. Escriba el comando completo o la cantidad de caracteres suficiente para formar el comando único; presione la tecla <**Tabulación** para emitir el comando y, a continuación, **<Entrar>**.

   S1# **configure**

¿Cuál es el mensaje que se muestra?

R/

Figura 4.1



Fuente propia

b. Presione la tecla **<Entrar>** para aceptar el parámetro predeterminado **[terminal]** entre corchetes.

¿En qué cambia la petición de entrada?

R/

Figura 4.2

```
S1#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
```

c. Esto se denomina “modo de configuración global”. Este modo se analizará en más detalle en las próximas actividades y prácticas de laboratorio. Por el momento, escriba **end**, **exit** o **Ctrl-Z** para volver al modo EXEC privilegiado.

S1(config)# **exit**
S1#

Figura 4.3

```
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Parte 3: Configuración del comando clock

Paso 1: Utilizar el comando clock.

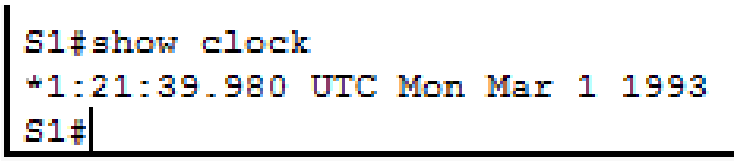
a. Utilice el comando **clock** para explorar en más detalle la ayuda y la sintaxis de comandos. Escriba **show clock** en la petición de entrada de EXEC privilegiado.

S1# **show clock**

¿Qué información aparece en pantalla? ¿Cuál es el año que se muestra?

R/

Figura 4.4



Fuente propia

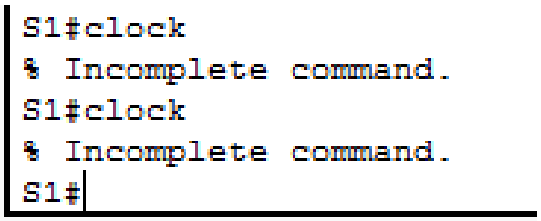
b. Utilice la ayuda contextual y el comando **clock** para establecer la hora del switch en la hora actual. Introduzca el comando **clock** y presione tecla **Entrar**.

S1# **clock<Entrar>**

¿Qué información aparece en pantalla?

R/

Figura 4.5



Fuente propia

c. El IOS devuelve el mensaje % Incomplete command (% comando incompleto), que indica que el comando **clock** necesita otros parámetros. Cuando se necesita más información, se puede proporcionar ayuda escribiendo un espacio después del comando y el signo de interrogación (?).

S1# **clock ?**

¿Qué información aparece en pantalla?

R/

Figura 4.6

```
S1#clock?
clock
```

Fuente propia

d. Configure el reloj con el comando **clock set**. Continúe utilizando este comando paso por paso.

S1# **clock set ?**

¿Qué información se solicita?

R/

Figura 4.7

```
S1#clock set?
set
```

Fuente propia

¿Qué información se habría mostrado si solo se hubiera ingresado el comando **clock set** y no se hubiera solicitado ayuda con el signo de interrogación?

R/ Saldría comando incompleto.

e. Según la información solicitada al emitir el comando **clock set ?**, introduzca la hora 3:00 p. m. con el formato de 24 horas, 15:00:00. Revise si se necesitan otros parámetros.

S1# **clock set 15:00:00 ?**

El resultado devuelve la solicitud de más información:

<1-31> Day of the month

MONTH Mes del año

Figura 4.8

```
S1#clock set 15:00:00?
hh:mm:ss
S1#clock set 15:00:00
```

Fuente propia

f. Intente establecer la fecha en 01/31/2035 con el formato solicitado. Es posible que para completar el proceso deba solicitar más ayuda mediante la ayuda contextual. Cuando termine, emita el comando **show clock** para mostrar la configuración del reloj. El resultado del comando debe mostrar lo siguiente:

S1# **show clock**

*15:0:4.869 UTC Fue Han 31 2035

Figura 4.9

```
S1#clock set 15:00:00 31 jan 2035
S1#show clock
15:0:6.113 UTC Wed Jan 31 2035
S1#
```

Fuente propia

g. Si no pudo lograrlo, pruebe con el siguiente comando para obtener el resultado anterior:

S1# **clock set 15:00:00 31 Jan 2035**

Paso 2: Explorar los mensajes adicionales del comando.

a. El IOS proporciona diversos resultados para los comandos incorrectos o incompletos, como se vio en secciones anteriores. Continúe utilizando el comando **clock** para explorar los mensajes adicionales con los que se puede encontrar mientras aprende a utilizar el IOS.

b. Emita el siguiente comando y registre los mensajes:

S1# **cl**

¿Qué información se devolvió?

Figura 5.0

```
S1#cl
% Ambiguous command: "cl"
S1#
```

Fuente propia

S1# **clock**

¿Qué información se devolvió?

Figura 5.1

```
S1#clock
% Incomplete command.
S1#
```

Fuente propia

S1# **clock set 25:00:00**

¿Qué información se devolvió?

Figura 5.2

```
S1#clock set 25:00:00
             ^
% Invalid input detected at '^' marker.
```

Fuente propia

S1# **clock set 15:00:00 32**

¿Qué información se devolvió?

Figura 5.3

```
S1#clock set 15:00:00 32
                      ^
% Invalid input detected at '^' marker.
```

Fuente propia

- **Numeral 2.2.3.3**

Parte 1: Verificar la configuración predeterminada del switch

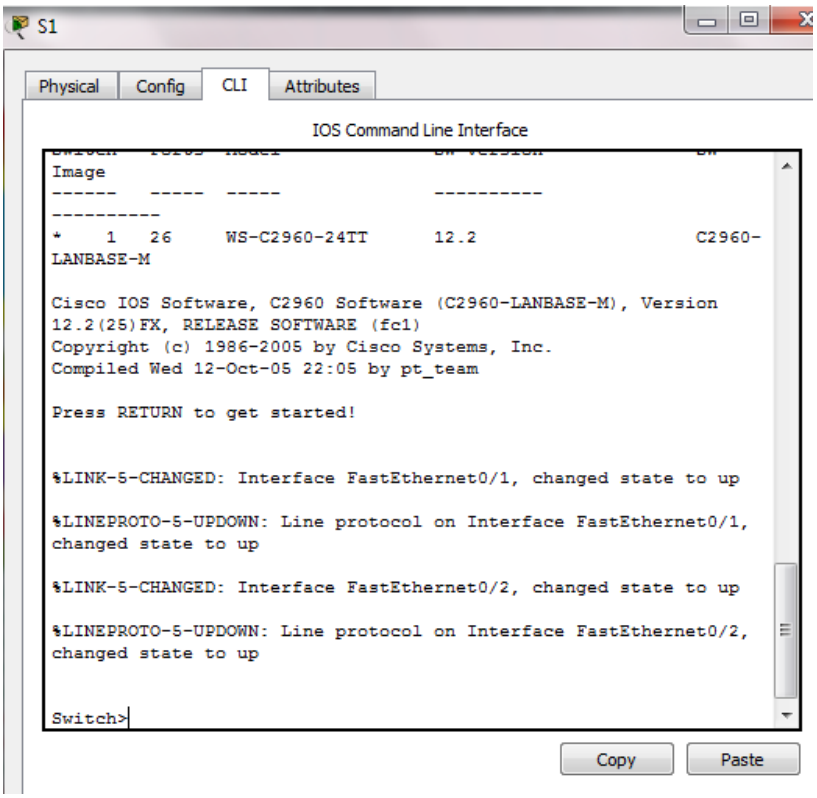
Paso 1: Ingrese al modo privilegiado.

Puede acceder a todos los comandos del switch en el modo privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado.

El conjunto de comandos EXEC privilegiados incluye aquellos comandos del modo EXEC del usuario, así como el comando **configure** a través del cual se obtiene el acceso a los modos de comando restantes.

a. Haga clic en **S1** y, a continuación, en la ficha **CLI**. Presione **<Entrar>**.

Figura 5.4



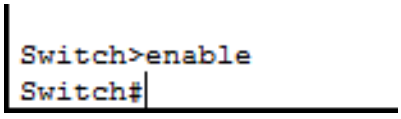
Fuente propia

b. Ingrese al modo EXEC privilegiado introduciendo el comando **enable:**

Switch> **enable**

Switch#

Figura 5.5



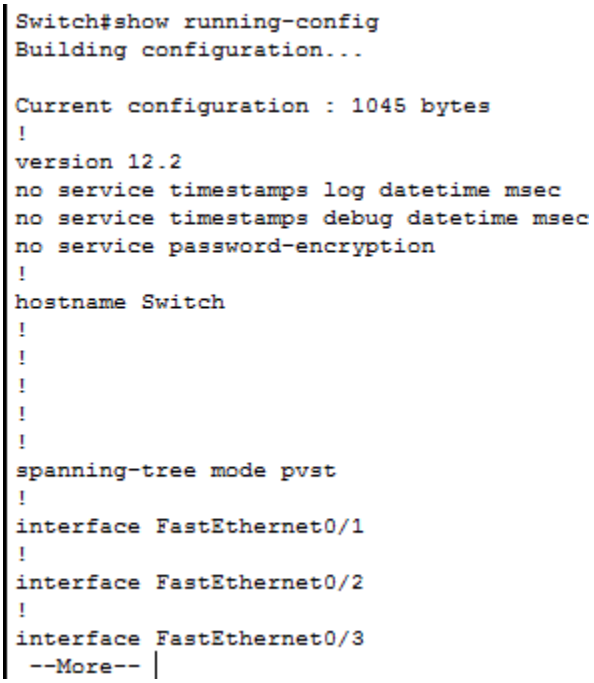
Fuente propia

Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

Paso 2: Examine la configuración actual del switch.

a. Ingrese el comando **show running-config**.

Figura 5.6



Fuente propia

Switch# **show running-config**

b. Responda las siguientes preguntas:

1. ¿Cuántas interfaces FastEthernet tiene el switch?

R/ Tiene 24 interafaces FastEthernet

2. ¿Cuántas interfaces Gigabit Ethernet tiene el switch?

R/ Tiene 2

3. ¿Cuál es el rango de valores que se muestra para las líneas vty?

R/0 a 4 y 5 a 15

4. ¿Qué comando muestra el contenido actual de la memoria de acceso aleatorio no volátil (NVRAM)?

Figura 5.6

```
Switch#show startup-config
startup-config is not present
```

Fuente propia

5. ¿Por qué el switch responde con startup-config is not present?

R/ Se debe a que el archivo de configuración se encuentra en la RAM y no en la NVRAM

Parte 2: Crear una configuración básica del switch

Paso 1: Asigne un nombre al switch.

Para configurar los parámetros de un switch, quizá deba pasar por diversos modos de configuración. Observe cómo cambia la petición de entrada mientras navega por el switch.

Switch# **configure terminal**

Switch(config)# **hostname S1**

S1(config)# **exit**

S1#

Figura 5.7

```
Switch#show startup-config
startup-config is not present
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Paso 2: Proporcionar un acceso seguro a la línea de consola.

Para proporcionar un acceso seguro a la línea de la consola, acceda al modo config-line y establezca la contraseña de consola en **letmein**.

S1# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# **line console 0**
S1(config-line)# **password letmein**
S1(config-line)# **login**
S1(config-line)# **exit**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

Figura 5.8

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#password letmein
S1(config-line)#login
S1(config-line)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

¿Por qué se requiere el comando **login**?

R/ Se necesitan los comandos login y password para realizar el proceso de control de contraseñas

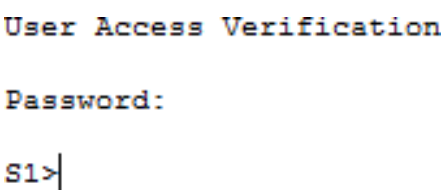
Paso 3: Verifique que el acceso a la consola sea seguro.

Salga del modo privilegiado para verificar que la contraseña del puerto de consola esté vigente.

S1# **exit**
Switch con0 is now available
Press RETURN to get started.
User Access Verification
Password:
S1>

Nota: si el switch no le pidió una contraseña, entonces no se configuró el parámetro **login** en el paso 2.

Figura 5.9



Fuente propia

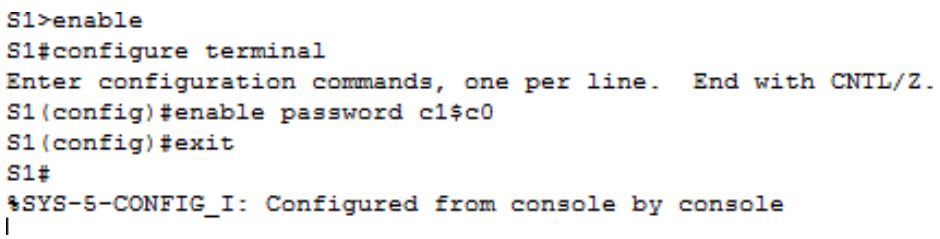
Paso 4: Proporcionar un acceso seguro al modo privilegiado.

Establezca la contraseña de **enable** en **c1$c0**. Esta contraseña protege el acceso al modo privilegiado.

Nota: el **0** en **c1$c0** es un cero, no una O mayúscula. Esta contraseña no calificará como correcta hasta que se la encripte tal como se indica en el paso 8.

S1> **enable**
S1# **configure terminal**
S1(config)# **enable password c1$c0**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

Figura 6.0



Fuente propia

Paso 5: Verificar que el acceso al modo privilegiado sea seguro

a. Introduzca el comando **exit** nuevamente para cerrar la sesión del switch.

b. Presione **<Entrar>**; a continuación, se le pedirá que introduzca una contraseña:

User Access Verification

Password:

c. La primera contraseña es la contraseña de consola que configuró para **line con 0**. Introduzca esta contraseña para volver al modo EXEC del usuario.

d. Introduzca el comando para acceder al modo privilegiado.

e. Introduzca la segunda contraseña que configuró para proteger el modo EXEC privilegiado.

f. Para verificar la configuración, examine el contenido del archivo de configuración en ejecución:

Figura 6.1

```
User Access Verification

Password:

S1>enable
Password:
S1#
```

Fuente propia

S1# **show running-configuration**

Figura 6.2

```
S1#show running-config
Building configuration...

Current configuration : 1090 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable password c1$c0
!
!
line con 0
 password letmein
 login
!
```

Fuente propia

Observe que las contraseñas de consola y de enable son de texto no cifrado. Esto podría presentar un riesgo para la seguridad si alguien está viendo lo que hace.

Paso 6: Configure una contraseña encriptada para proporcionar un acceso seguro al modo privilegiado.

La **contraseña de enable** se debe reemplazar por una nueva contraseña secreta encriptada mediante el comando **enable secret** . Establezca la contraseña secreta de enable en **itsasecret**.

S1# **config t**

S1(config)# **enable secret itsasecret**

S1(config)# **exit**

S1#

Figura 6.3

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable secret itsasecret
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Nota: la contraseña **secreta de enable** sobrescribe la contraseña de **enable**. Si ambas están configuradas en el switch, debe introducir la contraseña **secreta de enable** para ingresar al modo EXEC privilegiado.

Paso 7: Verificar si la contraseña secreta de enable se agregó al archivo de configuración

a. Introduzca el comando **show running-configuration** nuevamente para verificar si la nueva contraseña **secreta de enable** está configurada.

Nota: puede abreviar el comando **show running-configuration** de la siguiente manera:

S1# **show run**

Figura 6.4

```
S1$show run
Building configuration...

Current configuration : 1137 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password c1$c0
```

Fuente propia

b. ¿Qué se muestra como contraseña **secreta de enable**?

R/

Figura 6.5

```
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password c1$c0
```

Fuente propia

c. ¿Por qué la contraseña **secreta de enable** se ve diferente de lo que se configuró?

R/ Porque la contraseña esta encriptada.

Paso 8: Encriptar las contraseñas de consola y de enable.

Como pudo observar en el paso 7, la contraseña **secreta de enable** estaba encriptada, pero las contraseñas de **enable** y de **consola** aún estaban en texto no cifrado. Ahora encriptaremos estas contraseñas de texto no cifrado con el comando **service password-encryption**.

S1# **config t**
S1(config)# **service password-encryption**
S1(config)# **exit**

Figura 6.6

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#service password-encryption
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Si configura más contraseñas en el switch, ¿se mostrarán como texto no cifrado o en forma encriptada en el archivo de configuración? Explique por qué.

R/ El comando *service password-encryption* encripta las contraseñas actuales y futuras.

Parte 3: Configurar un título de MOTD

Paso 1: Configurar un mensaje del día (MOTD).

El conjunto de comandos IOS de Cisco incluye una característica que permite configurar los mensajes que cualquier persona puede ver cuando inicia sesión en el switch. Estos mensajes se denominan “mensajes del día” o “mensajes MOTD”. Encierre el texto del mensaje entre comillas o utilice un delimitador diferente de cualquier carácter que aparece en la cadena de MOTD.

S1# **config t**

S1(config)# **banner motd "This is a secure system. Authorized Access Only!"**

S1(config)# **exit**

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

S1#

Figura 6.7

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd "This is a secure system. Authorized
Access Only!"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

¿Cuándo se muestra este mensaje?

R/ El mensaje aparece cuando alguien intenta acceder al switch por el puerto consola

¿Por qué todos los switches deben tener un mensaje MOTD?

R/ Para servir de advertencia a usuarios que inician sesión en el switch.

Parte 4: Guardar los archivos de configuración en la NVRAM

Paso 1: Verificar que la configuración sea precisa mediante el comando show run

Paso 2: Guardar el archivo de configuración.

Usted ha completado la configuración básica del switch. Ahora realice una copia de seguridad del archivo de configuración en ejecución en la NVRAM para garantizar que no se pierdan los cambios realizados si el sistema se reinicia o se apaga.

S1# **copy running-config startup-config**
Destination filename [startup-config]?**[Enter]**
Building configuration...
[OK]

Figura 6.8

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Fuente propia

¿Cuál es la versión abreviada más corta del comando **copy running-config startup-config**?

R/ Figura 6.9

```
S1#cop run star
Destination filename [startup-config]?
```

Fuente propia

Paso 3: Examine el archivo de configuración de inicio.

¿Qué comando muestra el contenido de la NVRAM?

Figura 7.0

```
S1#show star
Using 1217 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 08221D0A0A49
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
 --More-- |
```

Fuente propia

¿Todos los cambios realizados están grabados en el archivo?

R/ Si, todos los datos fueron copiados a la NVRAM

Parte 5: Configurar el S2

Completó la configuración del S1. Ahora configurará el S2. Si no recuerda los comandos, consulte las partes 1 a 4 para obtener ayuda.

Configure el S2 con los siguientes parámetros:

a. Nombre del dispositivo: **S2**

Figura 7.1

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

b. Proteja el acceso a la consola con la contraseña **letmein**.

Figura 7.2

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#line console 0
S2(config-line)#password letmein
S2(config-line)#login
S2(config-line)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

c. Configure la contraseña **c1$c0** para enable y la contraseña secreta de enable, **itsasecret**.

Fuente propia

Figura 7.3

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#enable password c1$c0
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#enable secret itsasecret
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

d. Configure el siguiente mensaje para aquellas personas que inician sesión en el switch:

Acceso autorizado únicamente. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.

Figura 7.4

```
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#banner motd "Acceso Autorizado unicamente. Unathorized
access is prohibited and violators will be prosecuted to the full
extent of the law"
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

d. Encripte todas las contraseñas de texto no cifrado.

Figura 7.5

```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#service password-encryption
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

e. Asegúrese de que la configuración sea correcta.

Figura 7.6

```
S2#show run
Building configuration...

Current configuration : 1294 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S2
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 08221D0A0A49
!
```

Fuente propia

g. Guarde el archivo de configuración para evitar perderlo si el switch se apaga.

Figura 7.7

```
S2#show star
startup-config is not present
S2#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

Fuente propia

- **Numeral 2.3.2.5**

Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

Parte 1: Realizar una configuración básica en S1 y S2

Complete los siguientes pasos en el S1 y el S2.

Paso 1: Configurar un nombre de host en el S1.

a. Haga clic en **S1** y, a continuación, haga clic en la ficha **CLI**.

b. Introduzca el comando correcto para configurar el nombre de host **S1**.

Figura 7.8

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Paso 2: Configurar las contraseñas de consola y del modo EXEC privilegiado

a. Use **cisco** para la contraseña de consola.

Figura 7.9

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

b. Use **class** para la contraseña del modo EXEC privilegiado.

Figura 8.0

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable password class
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Paso 3: Verificar la configuración de contraseñas para el S1.

¿Cómo puede verificar que ambas contraseñas se hayan configurado correctamente?

R/ Con el comando ***show run***

Figura 8.1

```
S1#show run
Building configuration...

Current configuration : 1081 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable password class

!
!
!
line con 0
 password cisco
!
line vty 0 4
```

Fuente propia

Paso 4: Configurar un mensaje del día (MOTD).

Utilice un texto de aviso adecuado para advertir contra el acceso no autorizado. El siguiente texto es un ejemplo:

Acceso autorizado únicamente. Los infractores se procesarán en la medida en que lo permita la ley.

Figura 8.2

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd "Acceso Autorizado unicamente. Los
infractores se procesaran en la medida en qu elo permita la ley"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Paso 5: Guardar el archivo de configuración en la NVRAM.

¿Qué comando emite para realizar este paso?

Figura 8.3

```
S1#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Fuente propia

Paso 6: Repita los pasos 1 a 5 en S2.

Figura 8.4

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#exit
S2(config)#
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#enable password class
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Figura 8.5

```
S2#show run
Building configuration...

Current configuration : 1081 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
enable password class
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 --More--

!
!
line con 0
 password cisco
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
end
```

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#banner motd "Acceso Autorizado Unicamente. Entendido
Huey"
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
S2#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

Fuente propia

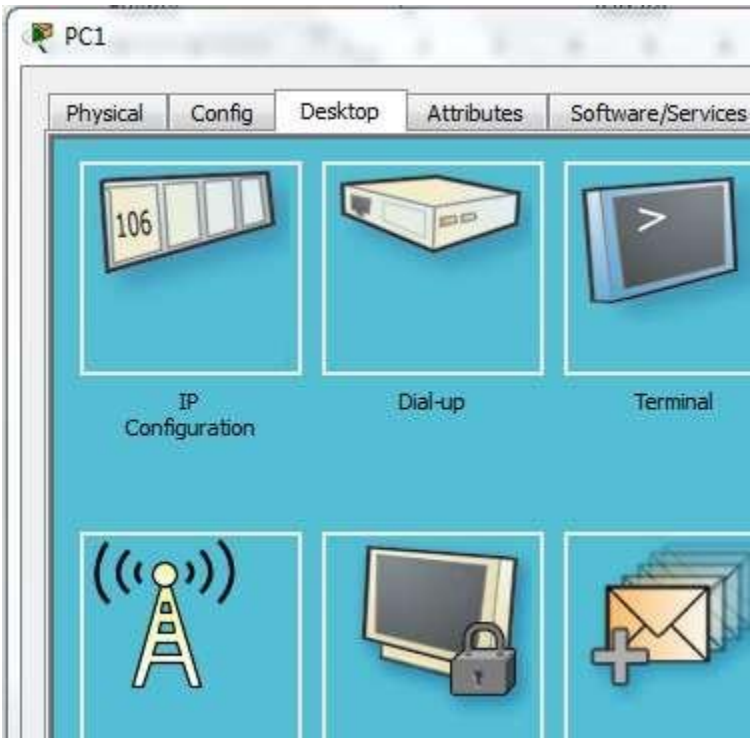
Paso 2: Configurar la PC

Configure la PC1 y la PC2 con direcciones IP.

Paso 1: Configurar ambas PC con direcciones IP.

a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** (Escritorio).

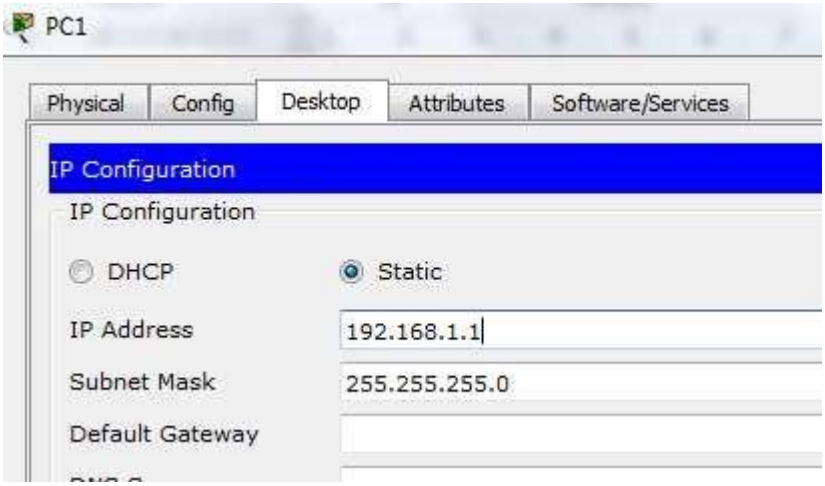
Figura 8.6



Fuente propia

b. Haga clic en **IP Configuration** (Configuración de IP). En la **tabla de direccionamiento** anterior, puede ver que la dirección IP para la PC1 es 192.168.1.1 y la máscara de subred es 255.255.255.0. Introduzca esta información para la PC1 en la ventana **IP Configuration**.

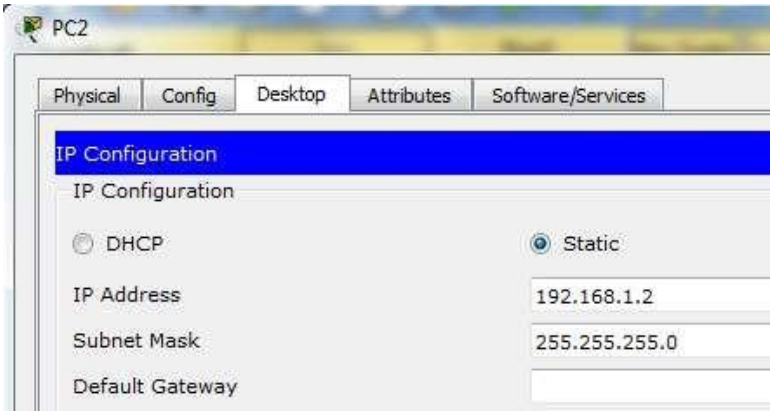
Figura 8.7



Fuente propia

c. Repita los pasos 1a y 1b para la PC2.

Figura 8.8

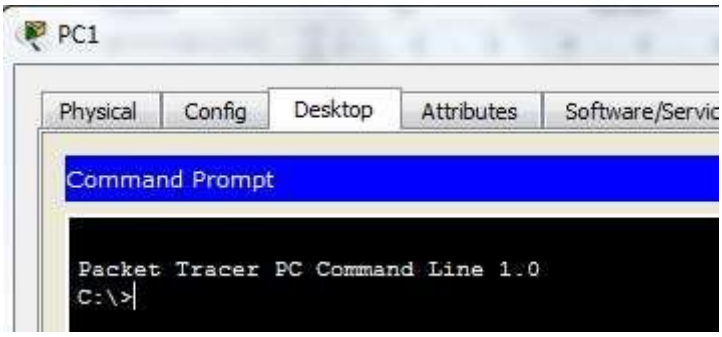


Fuente propia

Paso 2: Probar la conectividad a los switches.

a. Haga clic en **PC1**. Cierre la ventana **IP Configuration** si todavía está abierta. En la ficha **Desktop** , haga clic en **Command Prompt** (Símbolo del sistema).

Figura 8.9



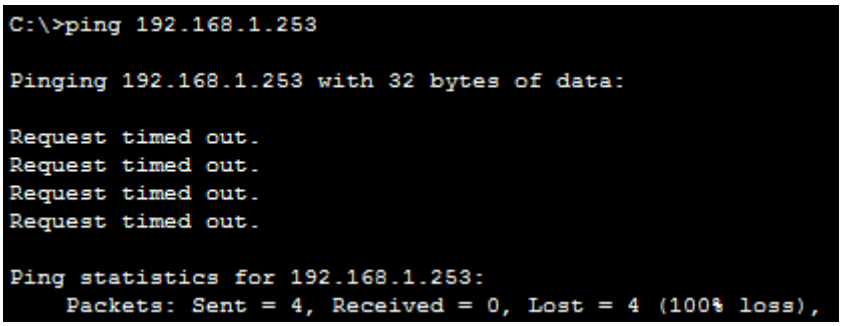
Fuente propia

b. Escriba el comando **ping** y la dirección IP para el S1 y presione **Entrar**.

Packet Tracer PC Command Line 1.0

PC> **ping 192.168.1.253**

Figura 9.0



Fuente propia

¿Tuvo éxito? ¿Por qué o por qué no?

R/ No Tuve éxito porque me conecté a una IP que no esta configurada en la red de S1.

Parte 3: Configurar la interfaz de administración de switches

Configure el S1 y el S2 con una dirección IP.

Paso 1: Configurar S1 con una dirección IP.

Los switches se pueden usar como dispositivos Plug and Play, lo que significa que no es necesario configurarlos para que funcionen. Los switches reenvían información desde un

puerto hacia otro sobre la base de direcciones de control de acceso al medio (MAC). Por lo tanto, ¿para qué lo configuraríamos con una dirección IP?

Use los siguientes comandos para configurar el S1 con una dirección IP.

S1 #**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# **interface vlan 1**
S1(config-if)# **ip address 192.168.1.253 255.255.255.0**
S1(config-if)# **no shutdown**
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# **exit**
S1#

Figura 9.1

```
S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.253 255.255.255.0
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

Fuente propia

¿Por qué debe introducir el comando **no shutdown**?

R/ Por que este es el comando que habilita una interfaz. Es importante tener presente que todas las interfaces de los routers Cisco están inhabilitadas por defecto, y se requiere la habilitación manual de cada una de ellas. Paralelamente no hay que olvidar que este comando no aparece en el archivo de configuración. En cambio, los switches Cisco tienen por defecto todas sus interfaces habilitadas y se deben deshabilitar manualmente aquellas que no serán utilizadas.

Paso 2: Configurar el S2 con una dirección IP.

Use la información de la tabla de direccionamiento para configurar el S2 con una dirección IP.

Figura 9.2

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.1.254 255.255.255.0
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
```

Fuente propia

Paso 3: Verificar la configuración de direcciones IP en el S1 y el S2

Use el comando **show ip interface brief** para ver la dirección IP y el estado de todos los puertos y las interfaces del switch. También puede utilizar el comando **show running-config**.

Figura 9.3

```
S2#show run
Building configuration...

Current configuration : 1239 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
enable password class
```

```
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.254 255.255.255.0
!
interface Vlan2
 mac-address 0030.a36d.6a01
 ip address 192.168.1.2 255.255.255.0
!
banner motd ^CAcceso Autorizado Unicamente. Entendido Huey^C
'
```

Fuente propia

S2#
S2#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual up up
FastEthernet0/2 unassigned YES manual up up
FastEthernet0/3 unassigned YES manual down down
FastEthernet0/4 unassigned YES manual down down
FastEthernet0/5 unassigned YES manual down down
FastEthernet0/6 unassigned YES manual down down
FastEthernet0/7 unassigned YES manual down down
FastEthernet0/8 unassigned YES manual down down
FastEthernet0/9 unassigned YES manual down down
FastEthernet0/10 unassigned YES manual down down
FastEthernet0/11 unassigned YES manual down down
FastEthernet0/12 unassigned YES manual down down
FastEthernet0/13 unassigned YES manual down down
FastEthernet0/14 unassigned YES manual down down
FastEthernet0/15 unassigned YES manual down down
FastEthernet0/16 unassigned YES manual down down
FastEthernet0/17 unassigned YES manual down down
FastEthernet0/18 unassigned YES manual down down
FastEthernet0/19 unassigned YES manual down down
FastEthernet0/20 unassigned YES manual down down
FastEthernet0/21 unassigned YES manual down down
FastEthernet0/22 unassigned YES manual down down
FastEthernet0/23 unassigned YES manual down down
FastEthernet0/24 unassigned YES manual down down
GigabitEthernet0/1 unassigned YES manual down down
GigabitEthernet0/2 unassigned YES manual down down
Vlan1 192.168.1.254 YES manual up up
Vlan2 192.168.1.2 YES manual down down

Paso 4: Guardar la configuración para el S1 y el S2 en la NVRAM

¿Qué comando se utiliza para guardar en la NVRAM el archivo de configuración que se encuentra en la RAM?

R/ copy run star

Figura 9.4

```
S2#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
S2#

S1#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Fuente propia

Paso 5. Verificar la conectividad de red.

La conectividad de red se puede verificar mediante el comando **ping**. Es muy importante que haya conectividad en toda la red. Se deben tomar medidas correctivas si se produce una falla. Haga ping a la dirección IP del S1 y el S2 desde la PC1 y la PC2.

a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** (Escritorio).

b. Haga clic en **Indicador del sistema**.

c. Haga ping a la dirección IP de la PC2.

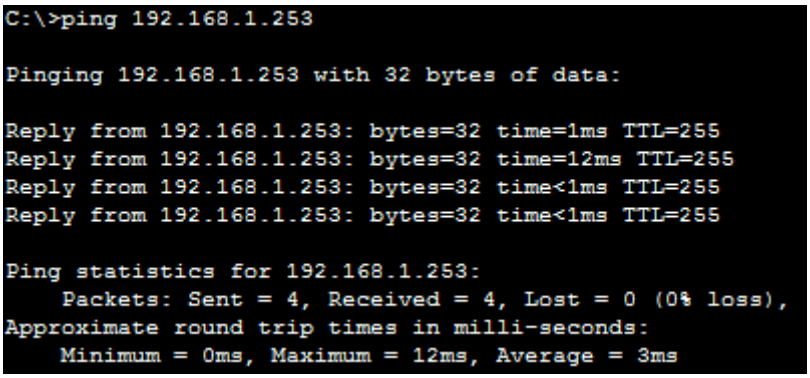
Figura 9.5

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=22ms TTL=128
Reply from 192.168.1.2: bytes=32 time=10ms TTL=128
Reply from 192.168.1.2: bytes=32 time=14ms TTL=128
Reply from 192.168.1.2: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 22ms, Average = 14ms
```

Fuente propia

d. Haga ping a la dirección IP del S1.

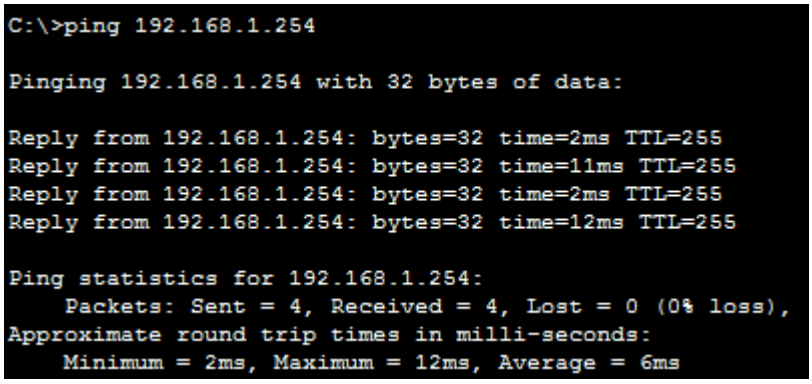
Figura 9.6



Fuente propia

e. Haga ping a la dirección IP del S2.

Figura 9.7



Fuente propia

Nota: también puede usar el mismo comando **ping** en la CLI del switch y en la PC2.

Todos los ping deben tener éxito. Si el resultado del primer ping es 80%, vuelva a intentarlo; ahora debería ser 100%. Más adelante, aprenderá por qué es posible que un ping falle la primera vez. Si no puede hacer ping a ninguno de los dispositivos, vuelva a revisar la configuración para detectar errores.

- **Numeral 2.4.1.2**

Tabla 1.1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
Room-145	VLAN 1	172.16.5.35	255.255.255.0
Room-146	VLAN 1	172.16.5.40	255.255.255.0
Manager	NIC	172.16.5.50	255.255.255.0
Reception	NIC	172.16.5.60	255.255.255.0

Objetivos:

- Configurar los nombres de host y las direcciones IP en dos switches que utilizan el Sistema operativo Internetwork (IOS) de Cisco mediante la interfaz de línea de comandos (CLI).
- Usar los comandos de Cisco IOS para especificar o limitar el acceso a las configuraciones de los dispositivos.
- Utilizar los comandos de IOS para guardar la configuración en ejecución.
- Configurar dos dispositivos host con direcciones IP.
- Verificar la conectividad entre los dos dispositivos finales de PC.

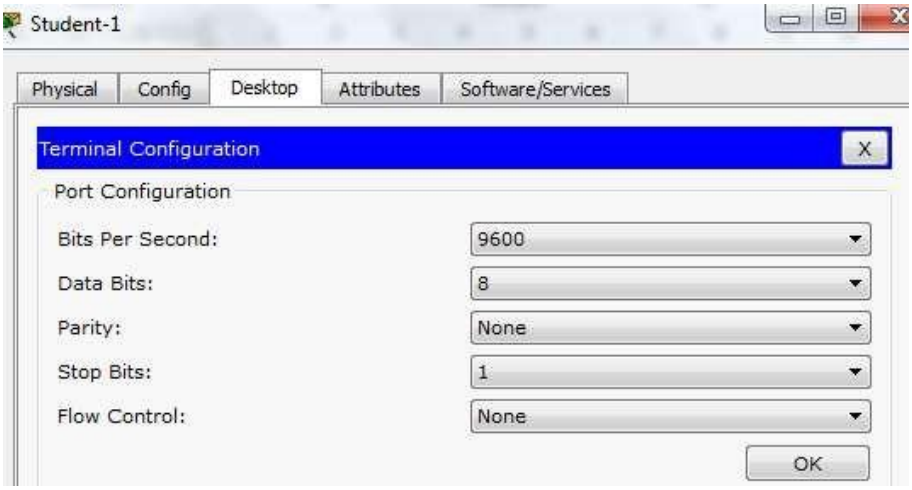
Situación:

Como técnico de LAN contratado recientemente, el administrador de red le solicitó que demuestre su habilidad para configurar una LAN pequeña. Sus tareas incluyen la configuración de parámetros iniciales en dos switches mediante Cisco IOS y la configuración de parámetros de dirección IP en dispositivos host para proporcionar conectividad de extremo a extremo. Debe utilizar dos switches y dos hosts/PC en una red conectada por cable y con alimentación.

Figura 9.8

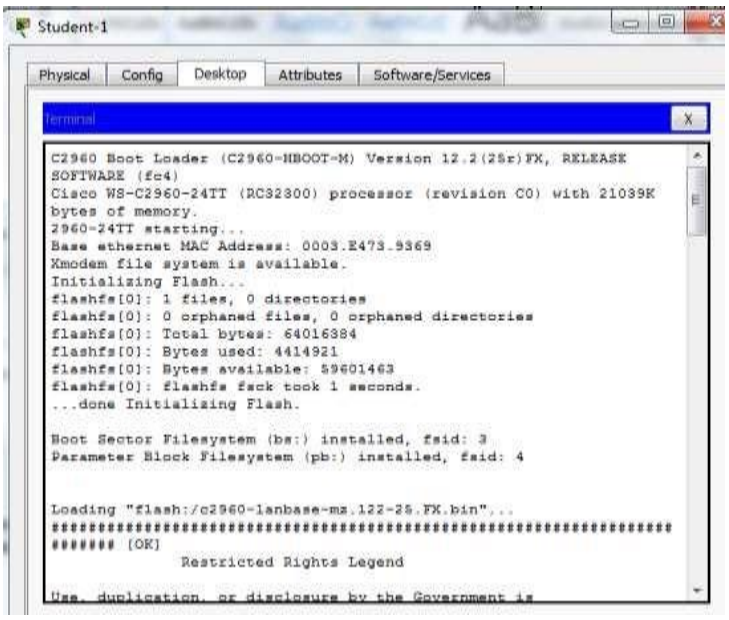
Fuente propia

Figura 9.9



Fuente propia

Figura 10.0



Fuente propia

Configuracion del Switch Class-A:

Al acceder por una conexión de consola desde el PC Student-1 y configurando la velocidad del puerto RS-232, ya podemos configurar el Switch que denominaremos Class-A

Figura 10.1

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Class-A
Class-A(config)#exit
Class-A#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Creamos contraseñas:

Figura 10.2

```
Class-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Class-A(config)#line console 0
Class-A(config-line)#password R4Xe3
Class-A(config-line)#enable password R4Xe3
Class-A(config)#exit
Class-A#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Habilitamos clave secreta:

Figura 10.3

```
Class-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Class-A(config)#enable secret C4AJA
Class-A(config)#exit
Class-A#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Encriptamos contraseñas

Figura 10.4

```
Class-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Class-A(config)#service password-encryption
Class-A(config)#exit
Class-A#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente propia

Colocamos mensaje de advertencia

Figura 10.5

```
Class-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Class-A(config)#banner motd "Advertencia"
Class-A(config)#exit
Class-A#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuramos dirección IP

Fuente propia

Figura 10.6

```
Class-A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Class-A(config)#interface vlan 1
Class-A(config-if)#ip address 10.10.10.100 255.255.255.0
Class-A(config-if)#no shutdown

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

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

Fuente propia

Guardamos en la NVRAM

Figura 10.7

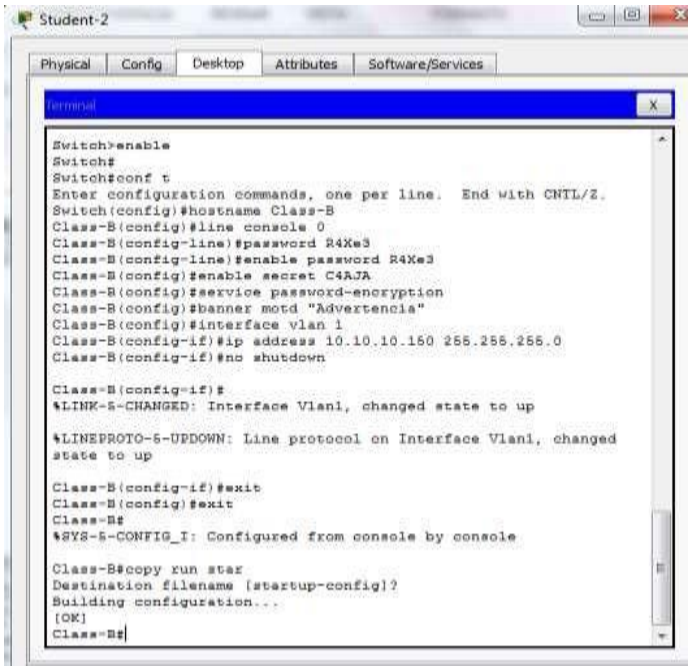
```
Class-A#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
```

Fuente propia

Configuracion Switch Class-B:

Al acceder por una conexión de consola desde el PC Student-2 y configurando la velocidad del puerto RS-232, ya podemos configurar el Switch que denominaremos Class-B

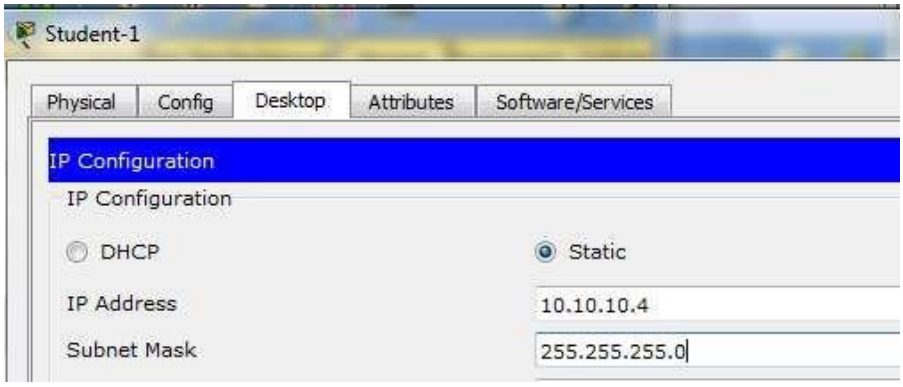
Figura 10.8



Fuente propia

Configuración de Dispositivos Student-1 y Student-2

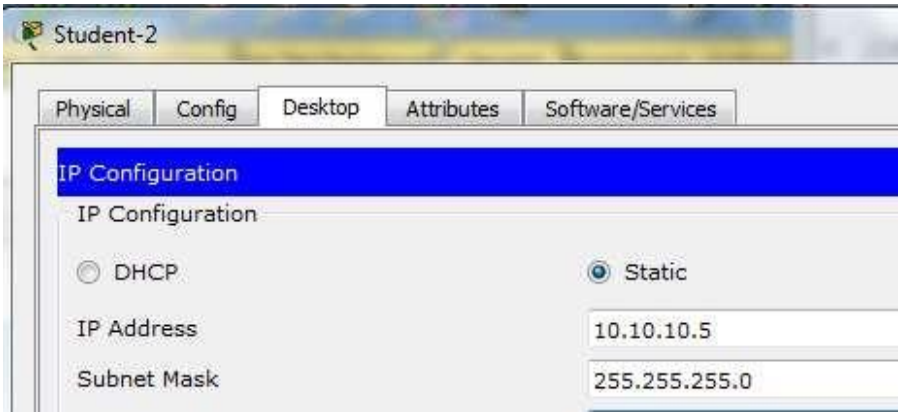
Figura 10.9



Fuente propia

Figura 11.0

Verificación de conectividad entre dispositivos:



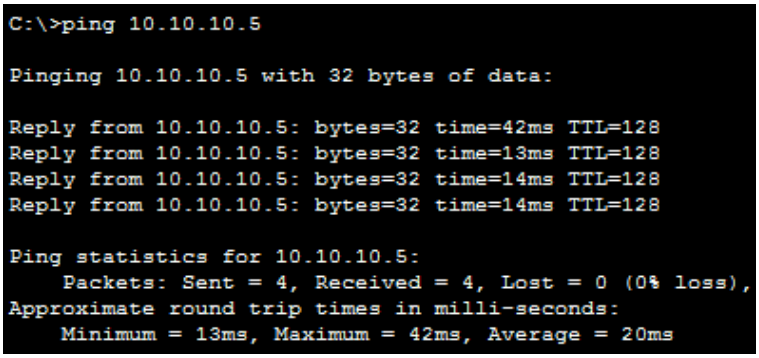
Fuente propia

Figura 11.1

```
C:\>ping 10.10.10.100

Pinging 10.10.10.100 with 32 bytes of data:

Reply from 10.10.10.100: bytes=32 time=2ms TTL=255
Reply from 10.10.10.100: bytes=32 time=1ms TTL=255
Reply from 10.10.10.100: bytes=32 time<1ms TTL=255
Reply from 10.10.10.100: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

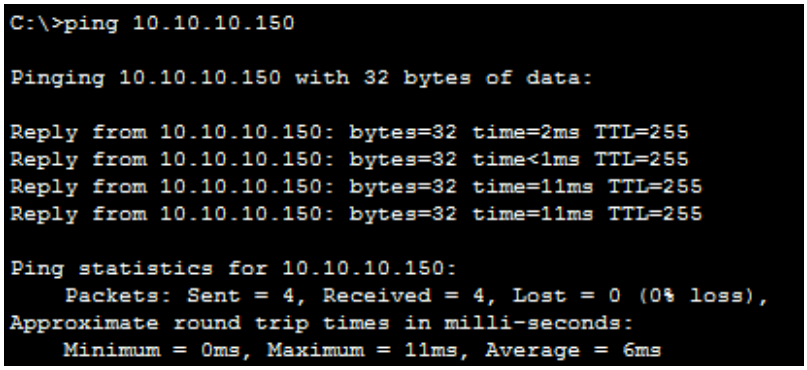
Fuente propia

Figura 11.2



Fuente propia

Figura 11.3



Fuente propia

Requisitos:

- Use una conexión de consola para acceder a cada switch.
- Nombre los switches **Class-A** y **Class-B**.
- Use la contraseña **R4Xe3** para todas las líneas.
- Use la contraseña secreta **C4aJa**.
- Encripte todas las contraseñas de texto no cifrado.
- Incluya la palabra **warning** (advertencia) en el mensaje del día (MOTD).
- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
- Guarde las configuraciones.
- Verifique la conectividad entre todos los dispositivos.

Nota: haga clic en **Check Results** (Verificar resultados) para ver su progreso. Haga clic en **Reset Activity** (Restablecer actividad) para generar un nuevo conjunto de requisitos. Si hace clic en esto antes de completar la actividad, se perderán todas las configuraciones.

- **Numeral 3.2.4.6**

Parte 1: Examinar el tráfico Web HTTP

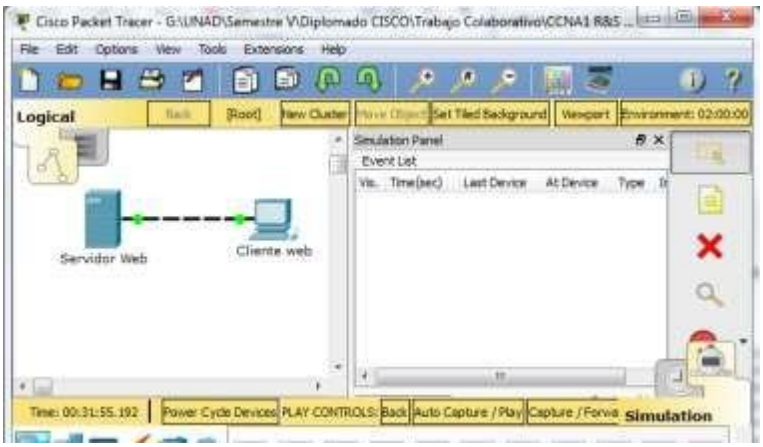
En la parte 1 de esta actividad, utilizará el modo de simulación de Packet Tracer (PT) para generar tráfico Web y examinar HTTP.

Paso 1: Cambie del modo de tiempo real al modo de simulación.

En la esquina inferior derecha de la interfaz de Packet Tracer, hay fichas que permiten alternar entre el modo **Realtime** (Tiempo real) y **Simulation** (Simulación). PT siempre se inicia en el modo **Realtime**, en el que los protocolos de red operan con intervalos realistas. Sin embargo, una excelente característica de Packet Tracer permite que el usuario “detenga el tiempo” al cambiar al modo de simulación. En el modo de simulación, los paquetes se muestran como sobres animados, el tiempo se desencadena por eventos y el usuario puede avanzar por eventos de red.

a. Haga clic en el ícono del modo **Simulation** (Simulación) para cambiar del modo **Realtime** (Tiempo real) al modo **Simulation**.

Figura 11.4

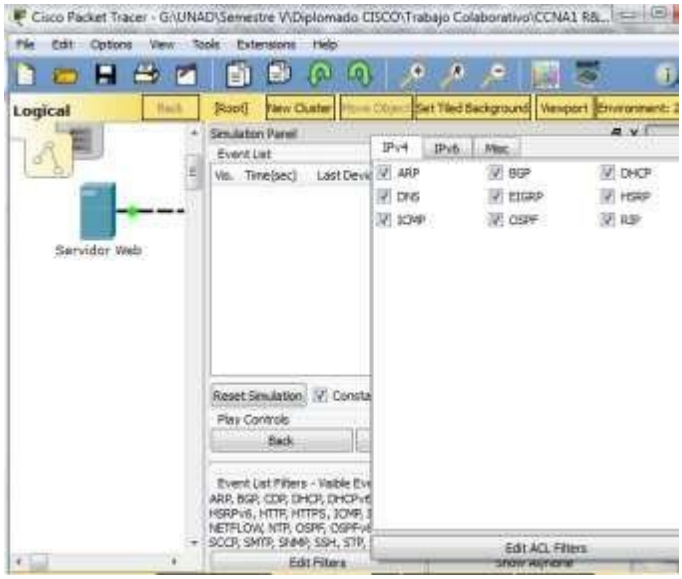


Fuente propia

b. Seleccione **HTTP** de **Event List Filters** (Filtros de lista de eventos).

1) Es posible que HTTP ya sea el único evento visible. Haga clic en **Edit Filters** (Editar filtros) para mostrar los eventos visibles disponibles. Alterne la casilla de verificación **Show All/None** (Mostrar todo/ninguno) y observe cómo las casillas de verificación se desactivan y se activan, o viceversa, según el estado actual.

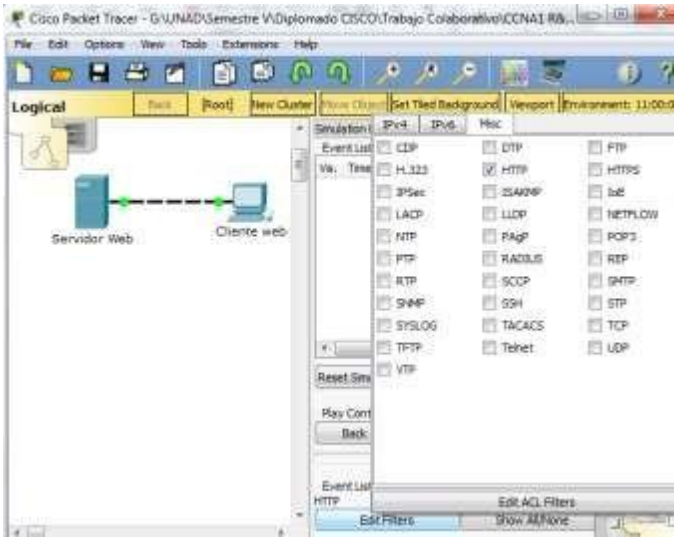
Figura 11.5



Fuente propia

2) Haga clic en la casilla de verificación **Show all/None** (Mostrar todo/ninguno) hasta que se desactiven todas las casillas y luego seleccione **HTTP**. Haga clic en cualquier lugar fuera del cuadro **Edit Filters**(Editar filtros) para ocultarlo. Los eventos visibles ahora deben mostrar solo HTTP.

Figura 11.



Fuente propia

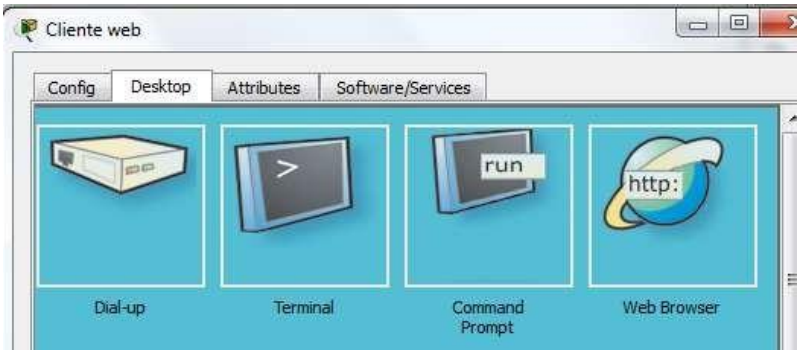
Paso 2: Genere tráfico web (HTTP).

El panel de simulación actualmente está vacío. En la parte superior de Event List (Lista de eventos) dentro del panel de simulación, se indican seis columnas. A medida que se genera y se revisa el tráfico, aparecen los eventos en la lista. La columna **Info** (Información) se utiliza para examinar el contenido de un evento determinado.

Nota: el servidor Web y el cliente Web se muestran en el panel de la izquierda. Se puede ajustar el tamaño de los paneles manteniendo el mouse junto a la barra de desplazamiento y arrastrando a la izquierda o a la derecha cuando aparece la flecha de dos puntas.

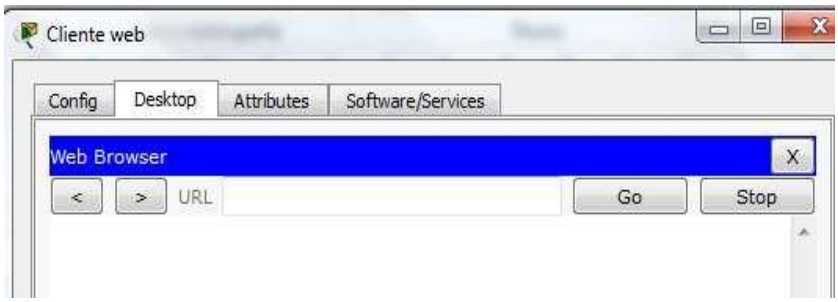
a. Haga clic en **Web Client** (Cliente Web) en el panel del extremo izquierdo.
b. Haga clic en la ficha **Desktop** (Escritorio) y luego en el ícono **Web Browser** (Explorador Web) para abrirlo.

Figura 11.



Fuente propia

Figura 11.8



Fuente propia

c. En el campo de dirección URL, introduzca **www.osi.local** y haga clic en **Go** (Ir).

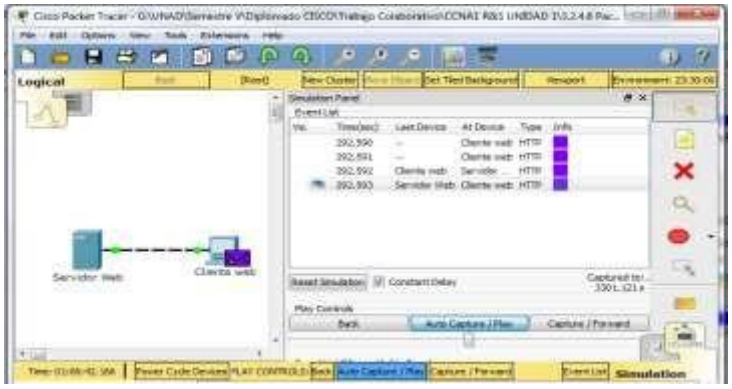
Debido a que el tiempo en el modo de simulación se desencadena por eventos, debe usar el botón **Capture/Forward** (Capturar/avanzar) para mostrar los eventos de red.

Figura 11.9

Fuente propia

c. Haga clic en **Capture/Forward** cuatro veces. Debe haber cuatro eventos en la lista de eventos.

Figura 12.0



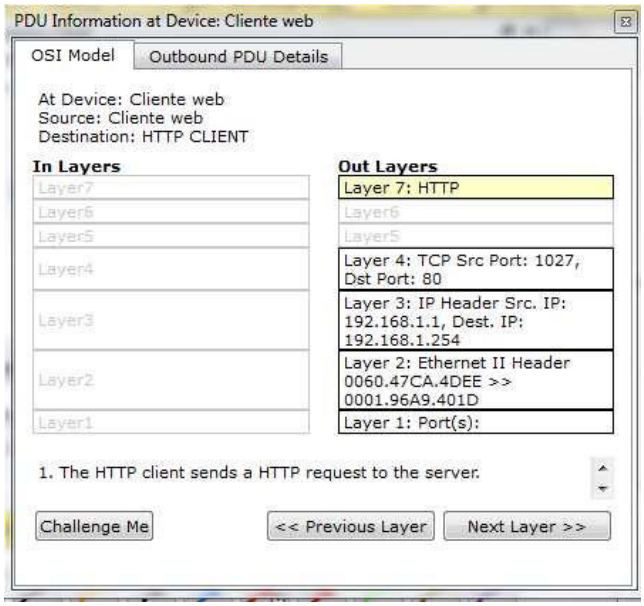
Fuente propia

Observe la página del explorador Web del cliente Web. ¿Cambió algo?

Paso 3: Explorar el contenido del paquete HTTP

a. Haga clic en el primer cuadro coloreado debajo de la columna **Event List** > **Info** (Lista de eventos > Información). Quizá sea necesario expandir el **panel de simulación** o usar la barra de desplazamiento que se encuentra directamente debajo de la **lista de eventos**.

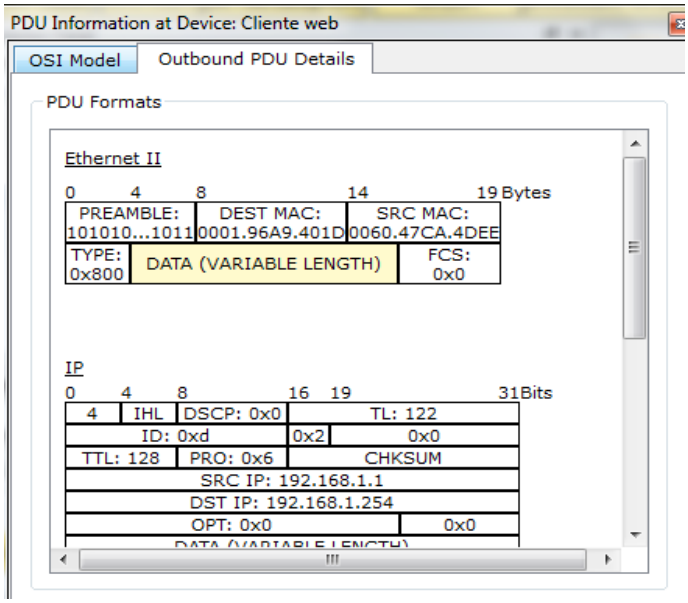
Figura 12.1



Fuente propia

Se muestra la ventana **PDU Information at Device: Web Client** (Información de PDU en dispositivo: cliente Web). En esta ventana, solo hay dos fichas, **OSI Model** (Modelo OSI) y **Outbound PDU Details**(Detalles de PDU saliente), debido a que este es el inicio de la transmisión. A medida que se analizan más eventos, se muestran tres fichas, ya que se agrega la ficha **Inbound PDU Details** (Detalles de PDU entrante). Cuando un evento es el último evento del stream de tráfico, solo se muestran las fichas **OSI Model** e **Inbound PDU Details**.

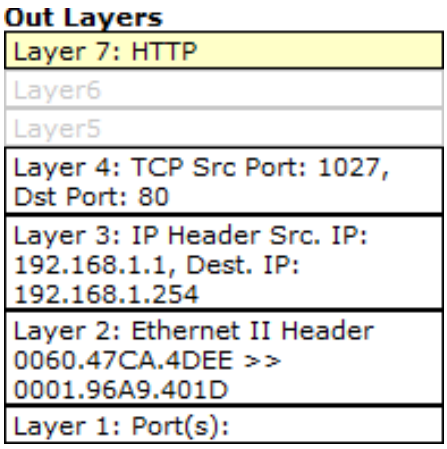
Figura 12.2



Fuente propia

b. Asegúrese de que esté seleccionada la ficha **OSI Model**. En la columna **Out Layers** (Capas de salida), asegúrese de que el cuadro **Layer 7** (Capa 7) esté resaltado.

Figura12.3



Fuente propia

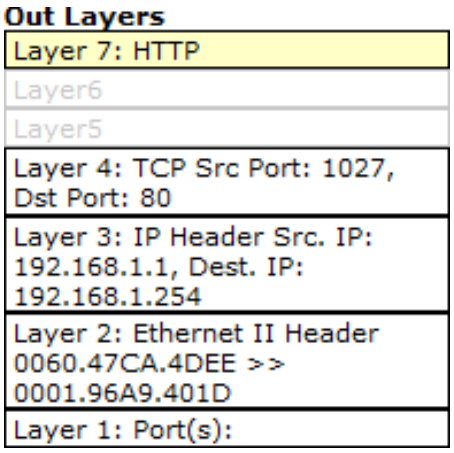
¿Cuál es el texto que se muestra junto a la etiqueta **Layer 7**?

R/ HTTP

¿Qué información se indica en los pasos numerados directamente debajo de los cuadros In Layers (Capas de entrada) y Out Layers (Capas de salida)?

R/ En In Layers se indica los Layers del 1 al 7. En Out Layers se indica lo siguiente:

Figura 12.4

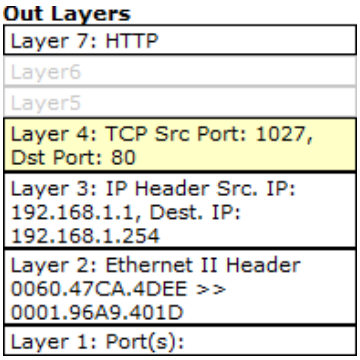


Fuente propia

c. Haga clic en **Next Layer** (Capa siguiente). Layer 4 (Capa 4) debe estar resaltado.

¿Cuál es el valor de **Dst Port** (Puerto de dest.)?
R/ 80

Figura 12.5



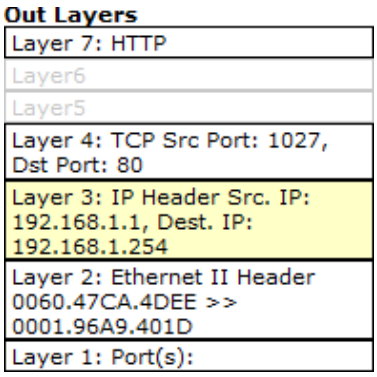
Fuente propia

d. Haga clic en **Next Layer** (Capa siguiente). Layer 3 (Capa 3) debe estar resaltado.

¿Cuál es valor de **Dest. IP** (IP de dest.)?

R/ 192.168.1.254

Figura 12.6



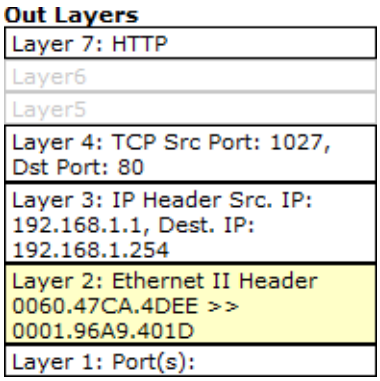
Fuente propia

e. Haga clic en **Next Layer** (Capa siguiente).

¿Qué información se muestra en esta capa?

R/ La información de la capa 2 (Layer 2) que se muestra a continuación:

Figura 12.7



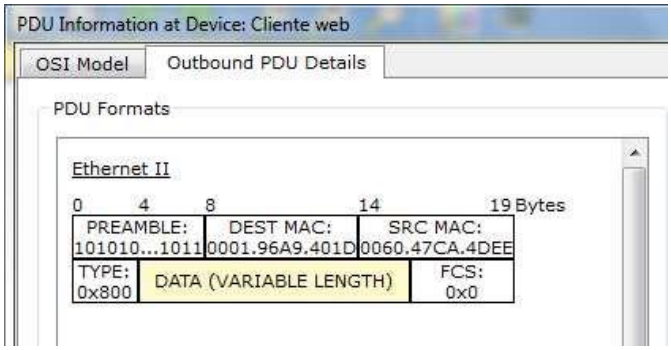
Fuente propia

f. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente).

La información que se indica debajo de **PDU Details** (Detalles de PDU) refleja las capas dentro del modelo TCP/IP.

Nota: la información que se indica en la sección **Ethernet II** proporciona información aun más detallada que la que se indica en Layer 2 (Capa 2) en la ficha **OSI Model**. **Outbound PDU Details** (Detalles de PDU saliente) proporciona información más descriptiva y detallada. Los valores de **DEST MAC** (MAC DE DEST.) y de **SRC MAC** (MAC DE ORIGEN) en la sección **Ethernet II** de **PDU Details** (Detalles de PDU) aparecen en la ficha **OSI Model**, en Layer 2, pero no se los identifica como tales.

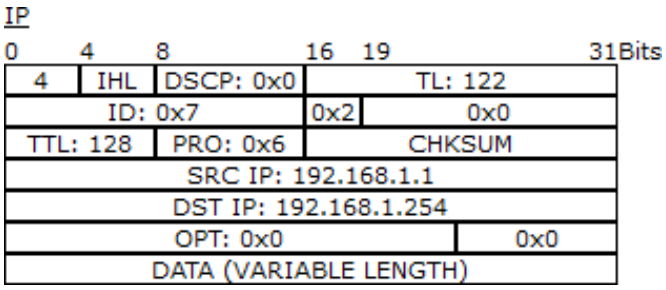
Figura 12.8



Fuente propia

¿Cuál es la información frecuente que se indica en la sección **IP** de **PDU Details** comparada con la información que se indica en la ficha **OSI Model** ? ¿Con qué capa se relaciona?

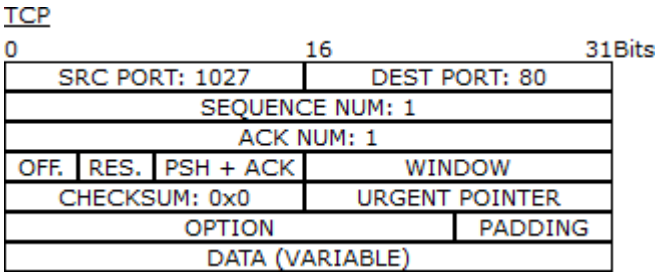
Figura 12.9



Fuente propia

¿Cuál es la información frecuente que se indica en la sección **TCP** de **PDU Details** comparada con la información que se indica en la ficha **OSI Model** , y con qué capa se relaciona?

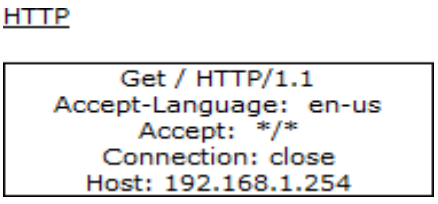
Figura 13.0



Fuente propia

¿Cuál es el **host** que se indica en la sección **HTTP** de **PDU Details**? ¿Con qué capa se relacionaría esta información en la ficha **OSI Model** ?

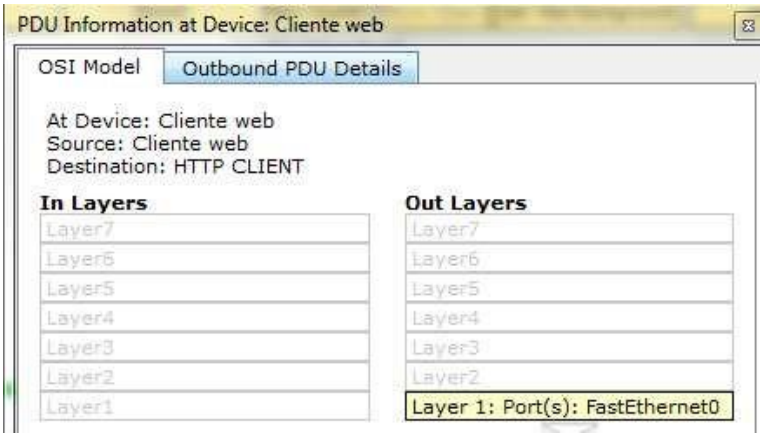
Figura 13.1



Fuente propia

f. Haga clic en el siguiente cuadro coloreado en la columna **Event List** > **Info** (Lista de eventos > Información). Solo la capa 1 está activa (sin atenuar). El dispositivo mueve la trama desde el búfer y la coloca en la red.

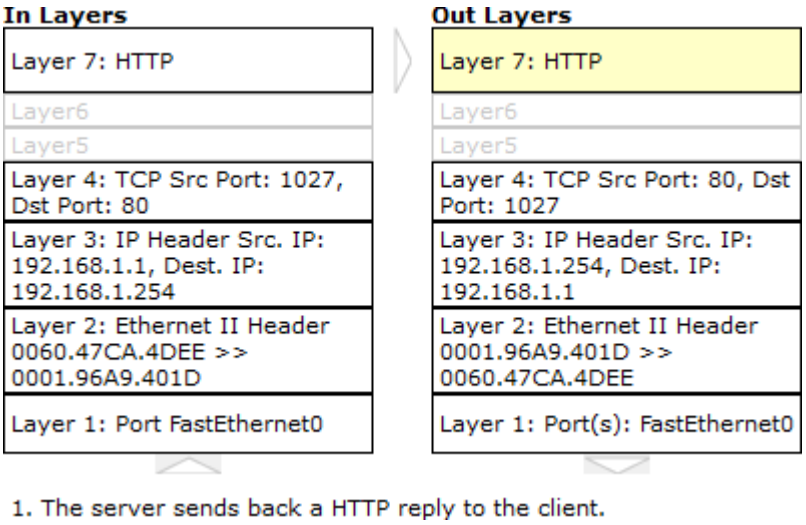
Figura 13.2



Fuente propia

g. Avance al siguiente cuadro **Info** (Información) de HTTP dentro de la **lista de eventos** y haga clic en el cuadro coloreado. Esta ventana contiene las columnas **In Layers** (Capas de entrada) y **Out Layers**(Capas de salida). Observe la dirección de la flecha que está directamente debajo de la columna **In Layers**; esta apunta hacia arriba, lo que indica la dirección en la que se transfiere la información. Desplácese por estas capas y tome nota de los elementos vistos anteriormente. En la parte superior de la columna, la flecha apunta hacia la derecha. Esto indica que el servidor ahora envía la información de regreso al cliente.

Figura 13.3



Fuente propia

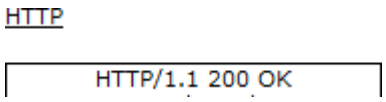
Compare la información que se muestra en la columna **In Layers** con la de la columna **Out Layers**: ¿cuáles son las diferencias principales?

R/ Las principales diferencias se encuentran en el puerto de origen y destino, en la IP de origen y destino, y en el encabezado (Header).

h. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). Desplácese hasta la sección **HTTP**.

Pregunta: ¿Cuál es la primera línea del mensaje HTTP que se muestra?

Figura13.4

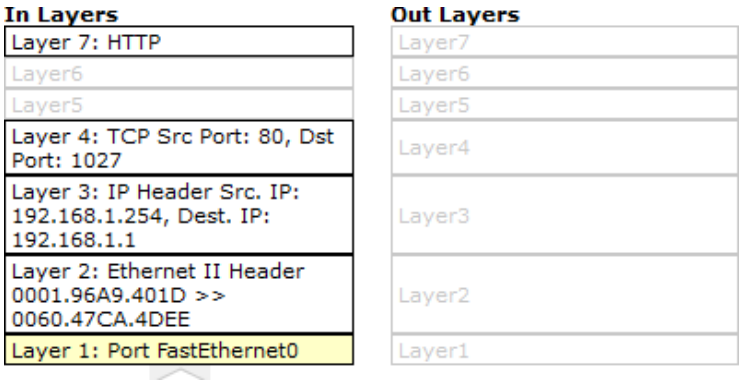


Fuente propia

i. Haga clic en el último cuadro coloreado de la columna **Info**. ¿Cuántas fichas se muestran con este evento y por qué?

R/ Solo se muestra habilitado ***In Layers***

Figuras 13.5



Fuente propia

Parte 2: Mostrar elementos de la suite de protocolos TCP/IP

En la parte 2 de esta actividad, utilizará el modo de simulación de Packet Tracer para ver y examinar algunos de los otros protocolos que componen la suite TCP/IP.

Paso 1: Ver eventos adicionales

a. Cierre todas las ventanas de información de PDU abiertas.

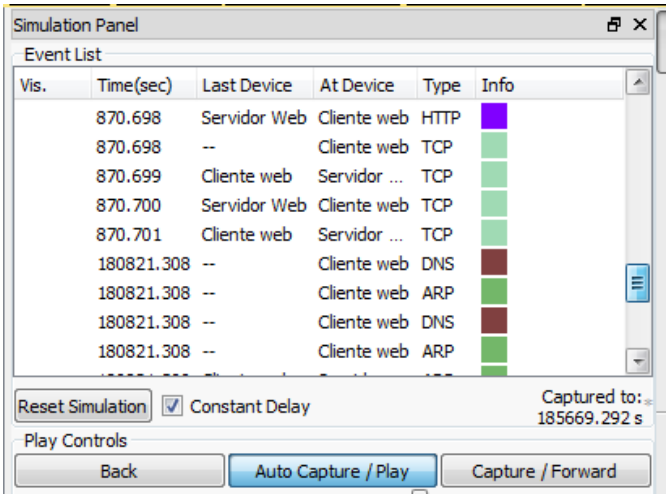
b. En la sección Event List Filters > Visible Events (Filtros de lista de eventos > Eventos visibles), haga clic en **Show All** (Mostrar todo).

¿Qué tipos de eventos adicionales se muestran?

R/ Eventos DNS, TCP y ARP

Estas entradas adicionales cumplen diversas funciones dentro de la suite TCP/IP. Si el protocolo de resolución de direcciones (ARP) está incluido, busca direcciones MAC. El protocolo DNS es responsable de convertir un nombre (por ejemplo, **www.osi.local**) a una dirección IP. Los eventos de TCP adicionales son responsables de la conexión, del acuerdo de los parámetros de comunicación y de la desconexión de las sesiones de comunicación entre los dispositivos. Estos protocolos se mencionaron anteriormente y se analizarán en más detalle a medida que avance el curso. Actualmente, hay más de 35 protocolos (tipos de evento) posibles para capturar en Packet Tracer.

Figura 13.6

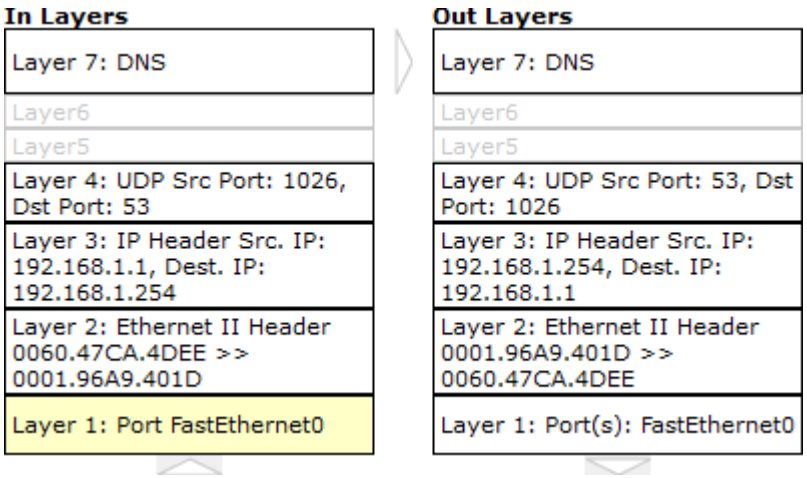


Fuente propia

d. Haga clic en el primer evento de DNS en la columna **Info**. Examine las fichas **OSI Model** y **PDU Detail**, y observe el proceso de encapsulación. Al observar la

ficha **OSI Model** con el cuadro **Layer 7** resaltado, se incluye una descripción de lo que ocurre, inmediatamente debajo de **In Layers** y **Out Layers**: (“1. The DNS client sends a DNS query to the DNS server.” [“El cliente DNS envía una consulta DNS al servidor DNS”]). Esta información es muy útil para ayudarlo a comprender qué ocurre durante el proceso de comunicación.

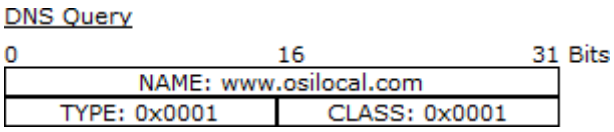
Figura 13.7



Fuente propia

e. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿Qué información se indica en **NAME**: (NOMBRE:) en la sección DNS QUERY (CONSULTA DNS)?

Figura 13.8



Fuente propia

e. Haga clic en el último cuadro coloreado **Info** de DNS en la lista de eventos. ¿Qué dispositivo se muestra?

¿Cuál es el valor que se indica junto a **ADDRESS**: (DIRECCIÓN:) en la sección DNS ANSWER (RESPUESTA DE DNS) de **Inbound PDU Details**?

f. Busque el primer evento de **HTTP** en la lista y haga clic en el cuadro coloreado del evento de **TCP** que le sigue inmediatamente a este evento. Resalte **Layer 4** (Capa

4) en la ficha **OSI Model** (Modelo OSI). En la lista numerada que está directamente debajo de **In Layers** y **Out Layers**, ¿cuál es la información que se muestra en los elementos 4 y 5?

R/4. La conexión TCP se realizó correctamente. 5. El dispositivo establece el estado de la conexión en ESTABLISHED (ESTABLECIDA).

El protocolo TCP administra la conexión y la desconexión del canal de comunicación, además de tener otras responsabilidades. Este evento específico muestra que SE ESTABLECIÓ el canal de comunicación.

g. Haga clic en el último evento de TCP. Resalte Layer 4 (Capa 4) en la ficha **OSI Model** (Modelo OSI). Examine los pasos que se indican directamente a continuación de **In Layers** y **Out Layers**. ¿Cuál es el propósito de este evento, según la información proporcionada en el último elemento de la lista (debe ser el elemento 4)? R/ ***Cerrar la conexión***

Desafío:

En esta simulación, se proporcionó un ejemplo de una sesión Web entre un cliente y un servidor en una red de área local (LAN). El cliente realiza solicitudes de servicios específicos que se ejecutan en el servidor. Se debe configurar el servidor para que escuche puertos específicos y detecte una solicitud de cliente. (Sugerencia: observe Layer 4 [Capa 4] en la ficha **OSI Model** para obtener información del puerto).

Sobre la base de la información que se analizó durante la captura de Packet Tracer, ¿qué número de puerto escucha el **servidor Web** para detectar la solicitud Web?

R/La primera PDU HTTP que solicita el cliente Web muestra el puerto 80 en el puerto DST (DESTINO) de capa 4.

¿Qué puerto escucha el **servidor Web** para detectar una solicitud de DNS?

R/ La primera PDU DNS que solicita el cliente Web muestra que el puerto de destino de capa 4 es el puerto 53.

- **Numeral 3.3.3.3**

Parte 1: Examinar el tráfico de internetwork en la sucursal

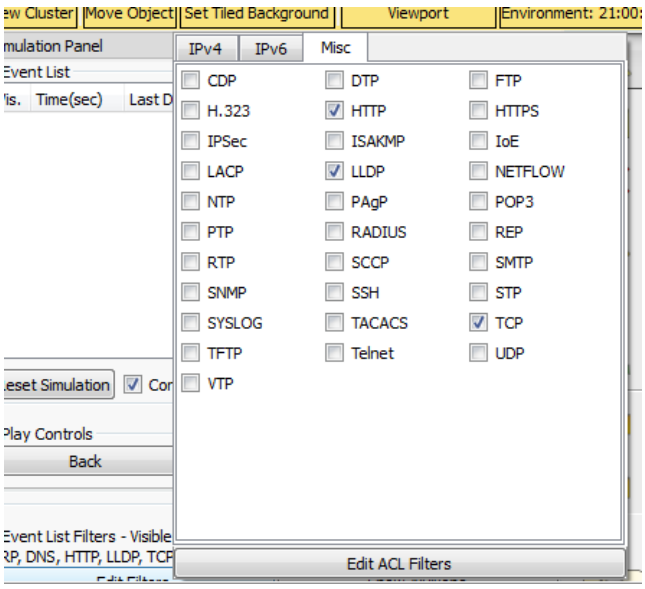
En la parte 1 de esta actividad, utilizará el modo de simulación para generar tráfico Web y examinar el protocolo HTTP junto con otros protocolos necesarios para las comunicaciones.

Paso 1: Cambiar del modo de tiempo real al modo de simulación.

a. Haga clic en el ícono del modo **Simulation** (Simulación) para cambiar del modo **Realtime** (Tiempo real) al modo **Simulation**.

b. Verifique que **ARP, DNS, HTTP** y **TCP** estén seleccionados en **Event List Filters** (Filtros de lista de eventos).

Figura 13.9



Fuente propia

c. Mueva completamente hacia la derecha la barra deslizable que se encuentra debajo de los botones **Play Controls** (Controles de reproducción), **Back**, **Auto Capture/Play**, **Capture/Forward** (Retroceder, Captura/Reproducción automática, Capturar/avanzar).

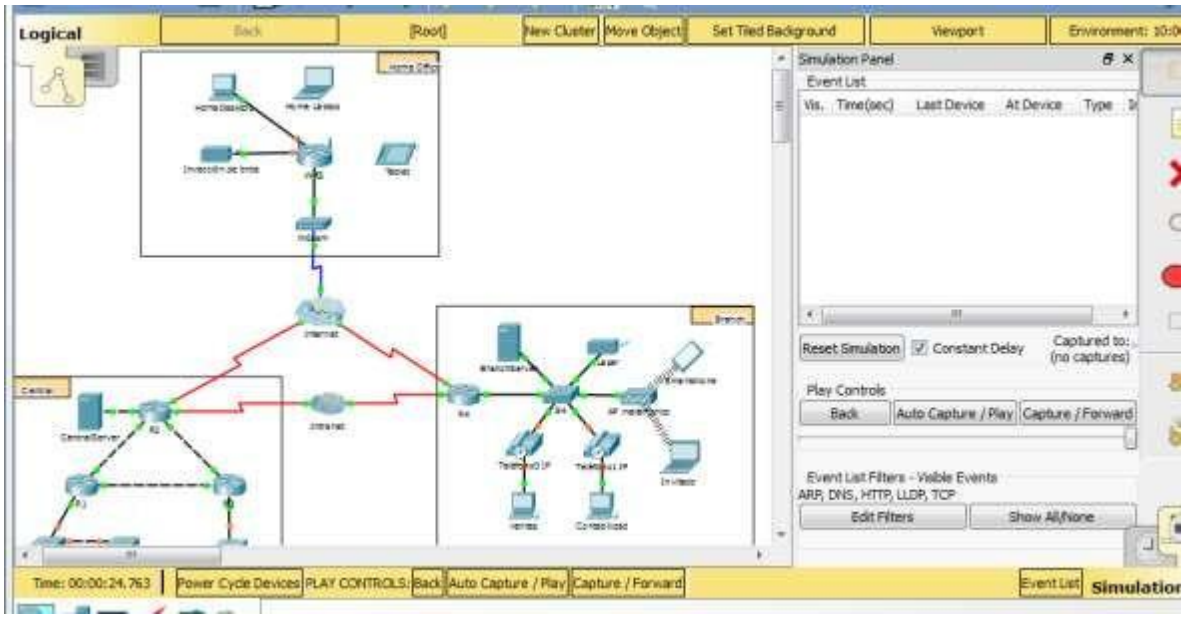
Paso 2: Generar tráfico mediante un explorador Web.

El panel de simulación actualmente está vacío. En Event List (Lista de eventos), en la parte superior del panel de simulación, hay seis columnas en el encabezado. A medida

que se genera y se revisa el tráfico, aparecen los eventos en la lista. La columna **Info** (Información) se utiliza para examinar el contenido de un evento determinado.

Nota: la topología se muestra en el panel de la izquierda del panel de simulación. Utilice las barras de desplazamiento para incorporar la ubicación Branch al panel, en caso necesario. Se puede ajustar el tamaño de los paneles manteniendo el mouse junto a la barra de desplazamiento y arrastrando a la izquierda o a la derecha.

Figura 14.0



Fuente propia

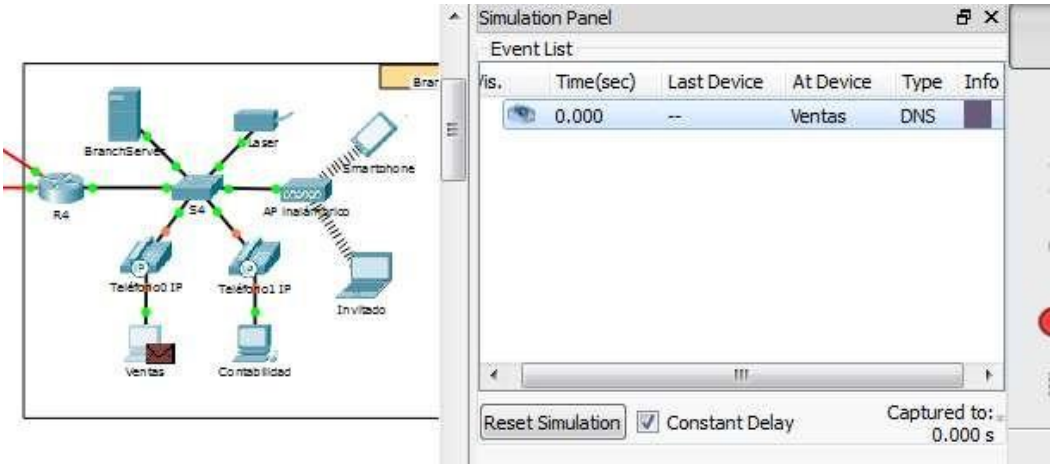
a. Haga clic en **Sales PC** (PC de ventas) en el panel del extremo izquierdo.

b. Haga clic en la ficha **Desktop** (Escritorio) y luego en el ícono **Web Browser** (Explorador Web) para abrirlo.

c. En el campo de dirección URL, introduzca **http://branchserver.pt.pta** y haga clic en **Go** (Ir). Observe la lista de eventos en el panel de simulación. ¿Cuál es el primer tipo de evento que se indica?

R/ Un evento DNS

Figura 14.1

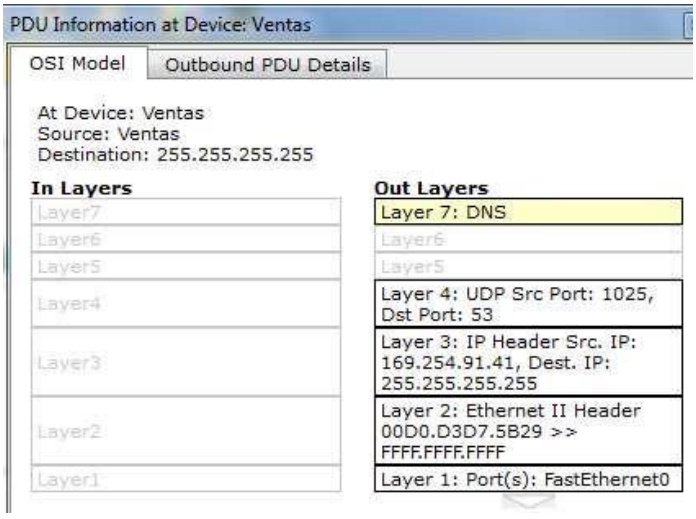


Fuente propia

d. Haga clic en el cuadro de información de **DNS** . En **Out Layers** (Capas de salida), se indica DNS para la capa 7. La capa 4 utiliza UDP para comunicarse con el servidor DNS en el puerto 53 (**Dst Port:** [Pto. de destino:]). Se indica tanto la dirección IP de origen como la de destino. ¿Qué información falta para comunicarse con el servidor DNS?

R/ La dirección MAC de destino

Figura 14.2



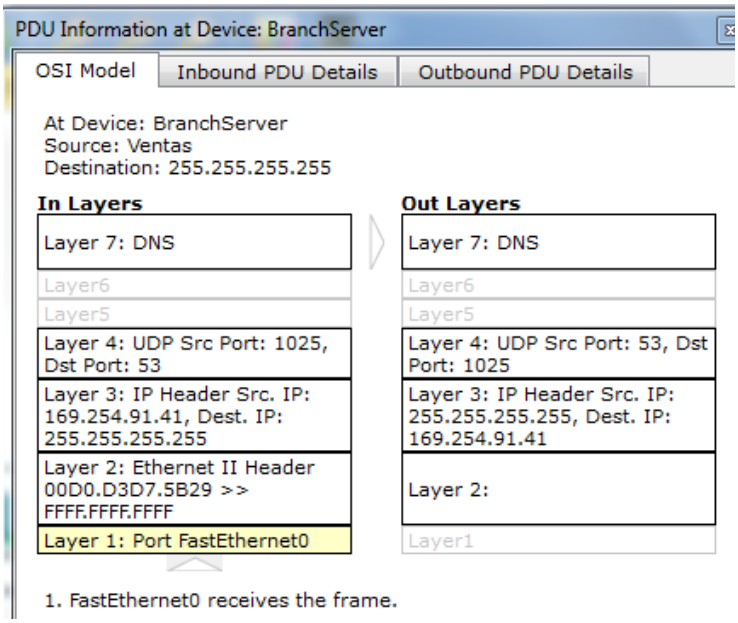
Fuente propia

e. Haga clic en **Auto Capture/Play**. En aproximadamente 45 segundos, aparece una ventana en la que se indica la finalización de la simulación actual. Haga clic en el botón **View Previous Events** (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista y observe la cantidad de eventos de **ARP**. Observe la columna Device (Dispositivo) en la lista de eventos: ¿cuántos de los dispositivos en la ubicación Branch atraviesa la solicitud de **ARP** ?

R/ Todos los dispositivos recibieron la solicitud ARP, es decir, 11 dispositivos de la ubicación Branch

f. Seleccione el evento de **DNS** para el que se indica **BranchServer** en At Device (En el dispositivo). Haga clic en el cuadro de la columna **Info**. ¿Qué se puede determinar seleccionando la capa 7 en **OSI Model** (Modelo OSI)? (Consulte los resultados que se muestran directamente debajo de **In Layers** [Capas de entrada]).

Figura 14.3

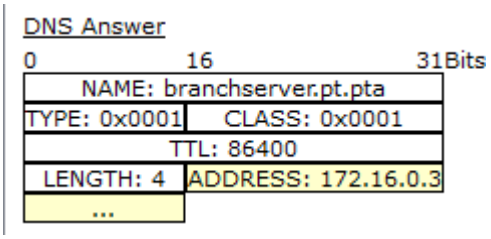


Fuente propia

g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). Desplácese hasta la parte inferior de la ventana y ubique la sección DNS Answer (Respuesta de DNS). ¿Cuál es la dirección que se muestra?

R/ 172.17.0.3

Figura 14.4

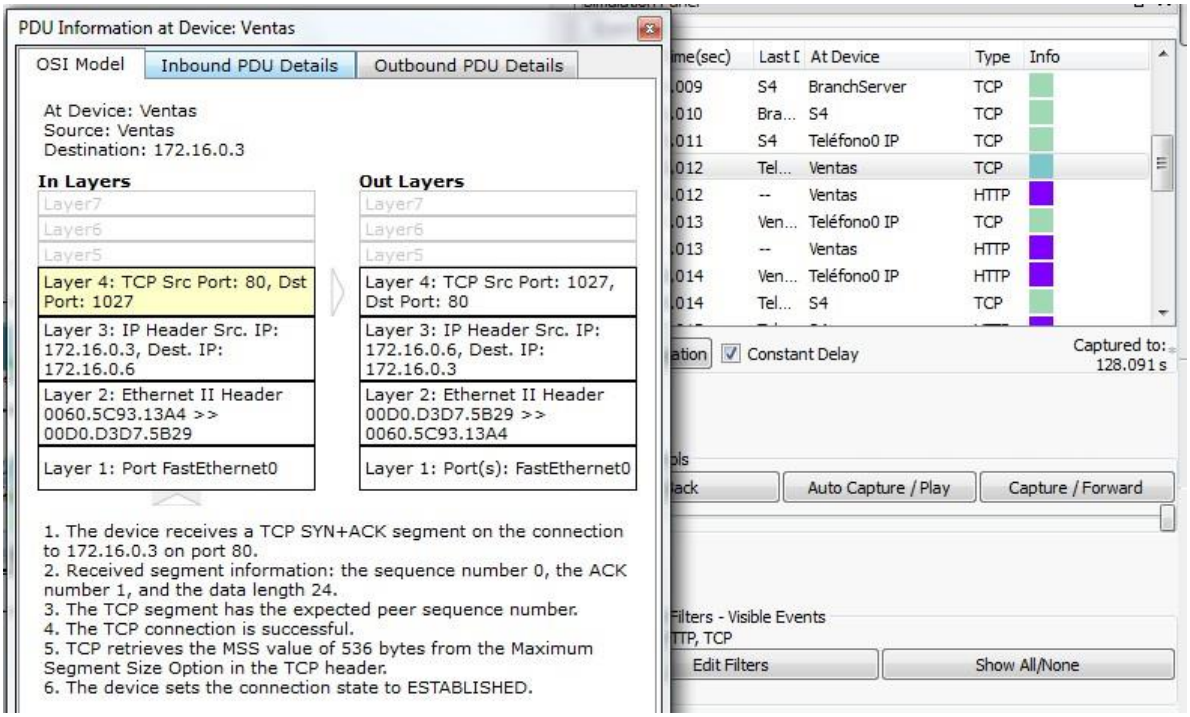


Fuente propia

h. Los eventos siguientes son eventos de **TCP** que permiten que se establezca un canal de comunicación. En el dispositivo **Sales**, seleccione el último evento de **TCP** anterior al evento de **HTTP** . Haga clic en el cuadro coloreado Info para ver la información de PDU. Resalte Layer 4 (Capa 4) en la columna **In Layers**. Observe el elemento 6 en la lista que se encuentra directamente debajo de la columna **In Layers**: ¿cuál es el estado de la conexión?

   R/ Conexión Establecida

Figura 14.5

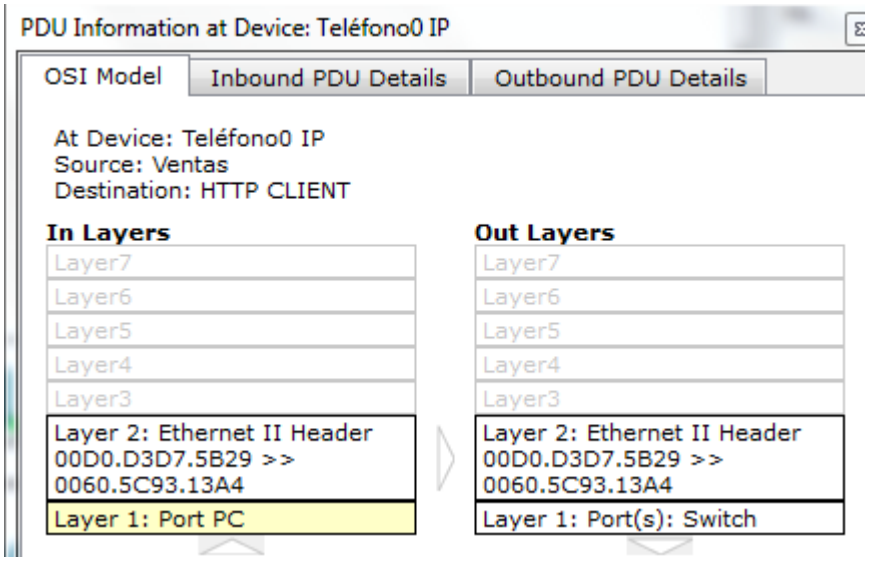


Fuente propia

i. Los eventos siguientes son eventos de **HTTP**. Seleccione cualquiera de los eventos de **HTTP** en un dispositivo intermediario (teléfono IP o switch). ¿Cuántas capas están activas en uno de estos dispositivos y por qué?

R/ Hay solo dos capas activas, la capa 1 y 2

Figura 14.6

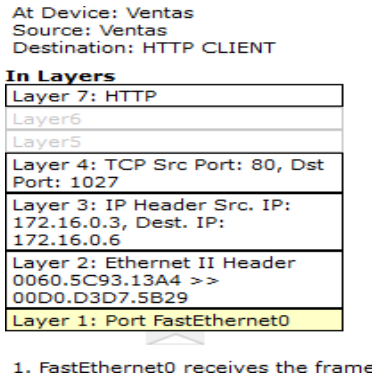


Fuente propia

j. Seleccione el último evento de **HTTP** en Sales PC. Seleccione la capa superior en la ficha **OSI Model**. ¿Cuál es el resultado que se indica debajo de la columna **In Layers**?

R/ FastEthernet0 recibe el frame

Figura 14.7



Parte 2: Examinar el tráfico de internetwork a la central

En la parte 2 de esta actividad, utilizará el modo de simulación de Packet Tracer (PT) para ver y examinar cómo se administra el tráfico que sale de la red local.

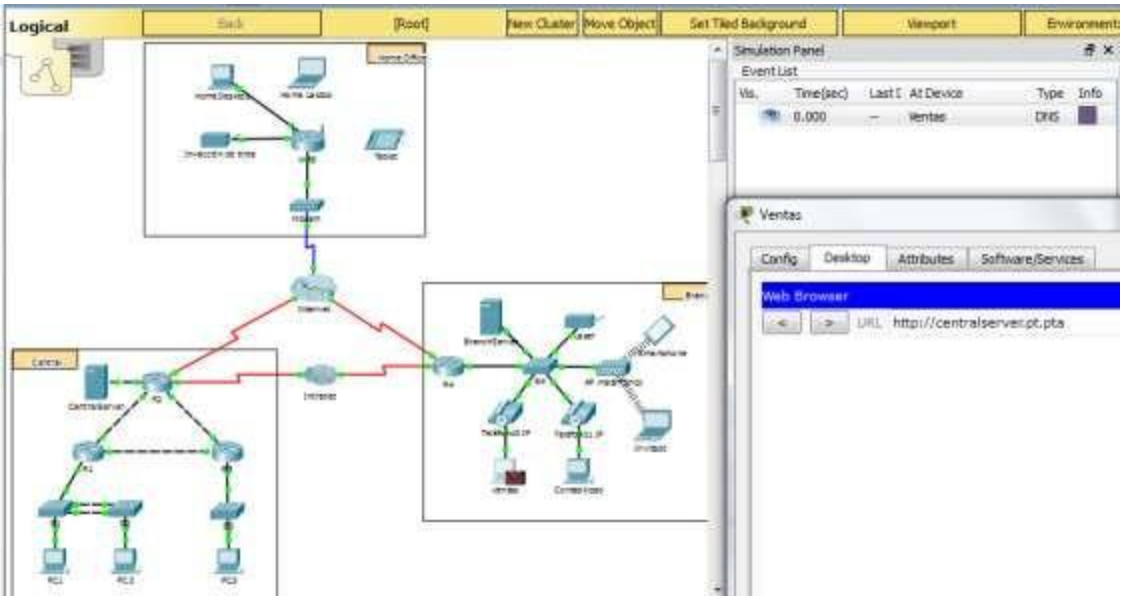
Paso 1: Configurar la captura de tráfico hacia el servidor Web de la central

a. Cierre todas las ventanas de información de PDU abiertas.

b. Haga clic en la opción **Reset Simulation** (Restablecer simulación), que se encuentra cerca del centro del panel de simulación.

c. Escriba **http://centralserver.pt.pta** en el explorador Web de Sales PC.

Figura 14.8

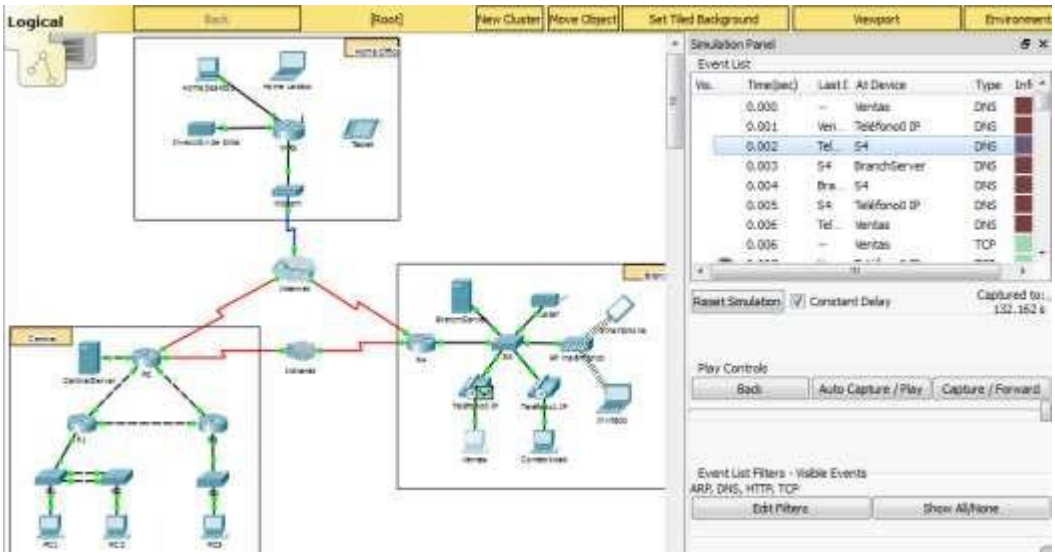


Fuente propia

d. Haga clic en **Auto Capture/Play** (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en **View Previous Events** (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe que la primera serie de eventos es **DNS** y que no hay entradas de **ARP** antes de comunicarse con**Branchserver**. Según lo aprendido hasta ahora, ¿a qué se debe esto?

R/ Se debe a que el equipo Ventas solicita al servidor DNS BranchServer una resolución de dirección de la pagina web y este a su vez le envía una respuesta con la dirección resuelta.

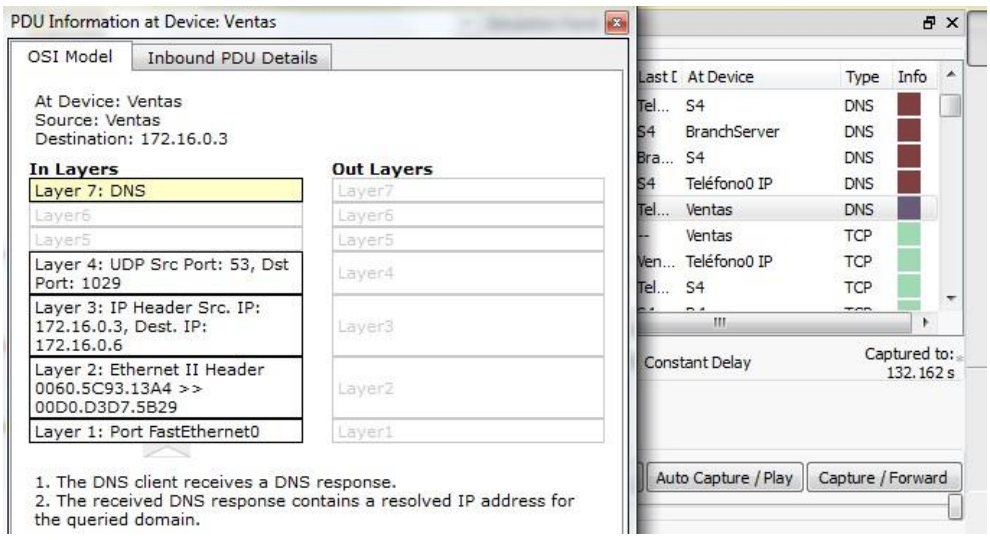
Figura 14.9



Fuente propia

e. Haga clic en el último evento de DNS en la columna **Info**. Seleccione **Layer 7** (Capa 7) en la ficha **OSI Model**.

Figura 15.0



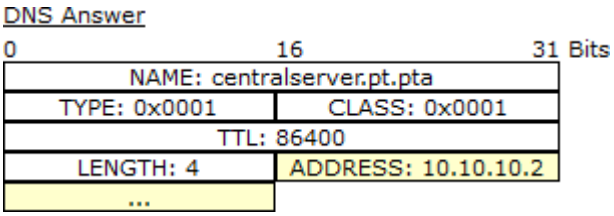
Fuente propia

Al observar la información proporcionada, ¿qué se puede determinar sobre los resultados de DNS?
R/ BranchServer realiza la resolución de la dirección para el dominio requerido y envía una respuesta al equipo Ventas, la cual la recibe exitosamente.

f. Haga clic en la ficha Inbound PDU Details (Detalles de PDU entrante). Desplácese hasta la sección DNS ANSWER (RESPUESTA DE DNS). ¿Cuál es la dirección que se indica para centralserver.pt.pta?

R/ 10.10.10.2

Figura 15.1



Fuente propia

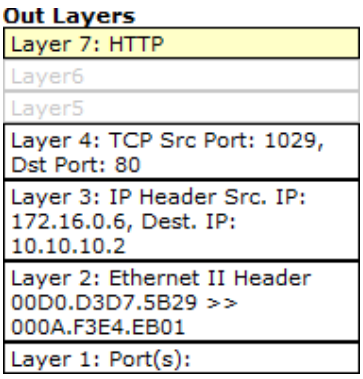
g. Los eventos siguientes son eventos de **ARP**. Haga clic en el cuadro coloreado Info del último evento de **ARP** . Haga clic en la ficha **Inbound PDU Details** y observe la dirección MAC. Sobre la base de la información en la sección de ARP, ¿qué dispositivo proporciona la respuesta de ARP?

R/ El servidor R4

h. Los eventos siguientes son eventos de **TCP** , que nuevamente se preparan para establecer un canal de comunicación. Busque el primer evento de **HTTP** en Event List. Haga clic en el cuadro coloreado del evento de **HTTP**. Resalte Layer 2 (Capa 2) en la ficha **OSI Model**. ¿Qué se puede determinar sobre la dirección MAC de destino?

R/ La dirección corresponde al servidor CentralServer

Figura 15.2

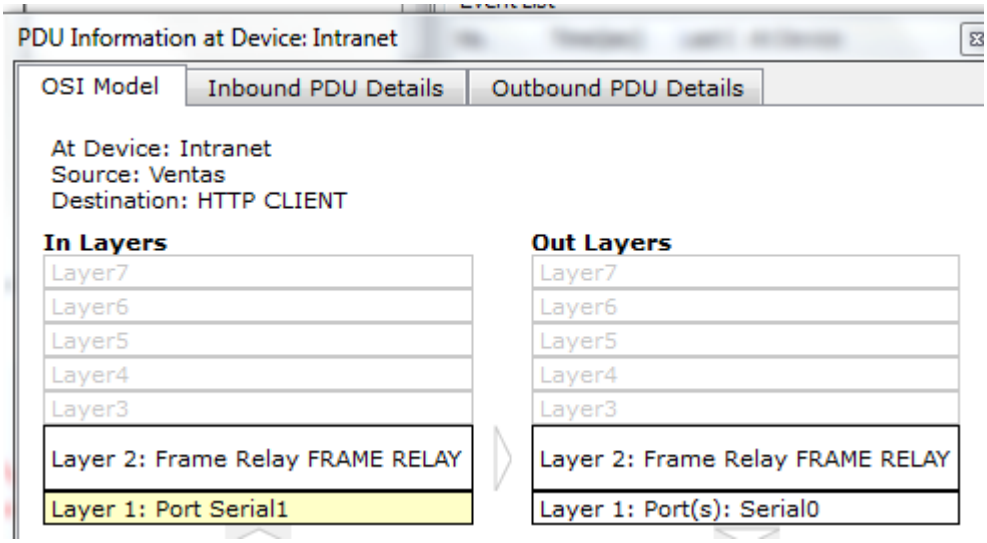


Fuente propia

i. Haga clic en el evento de **HTTP** en el dispositivo **R4**. Observe que la capa 2 contiene un encabezado de Ethernet II. Haga clic en el evento de **HTTP** en el dispositivo **Intranet**. ¿Cuál es la capa 2 que se indica en este dispositivo?

R/ La capa 2 indica una tecnología basada en Frame Relay

Figura 15.3



Fuente propia

Observe que solo hay dos capas activas, en oposición a lo que sucede cuando se atraviesa el router. Esta es una conexión WAN, y se analizará en otro curso.

Parte 3: Examinar el tráfico de Internet desde la sucursal

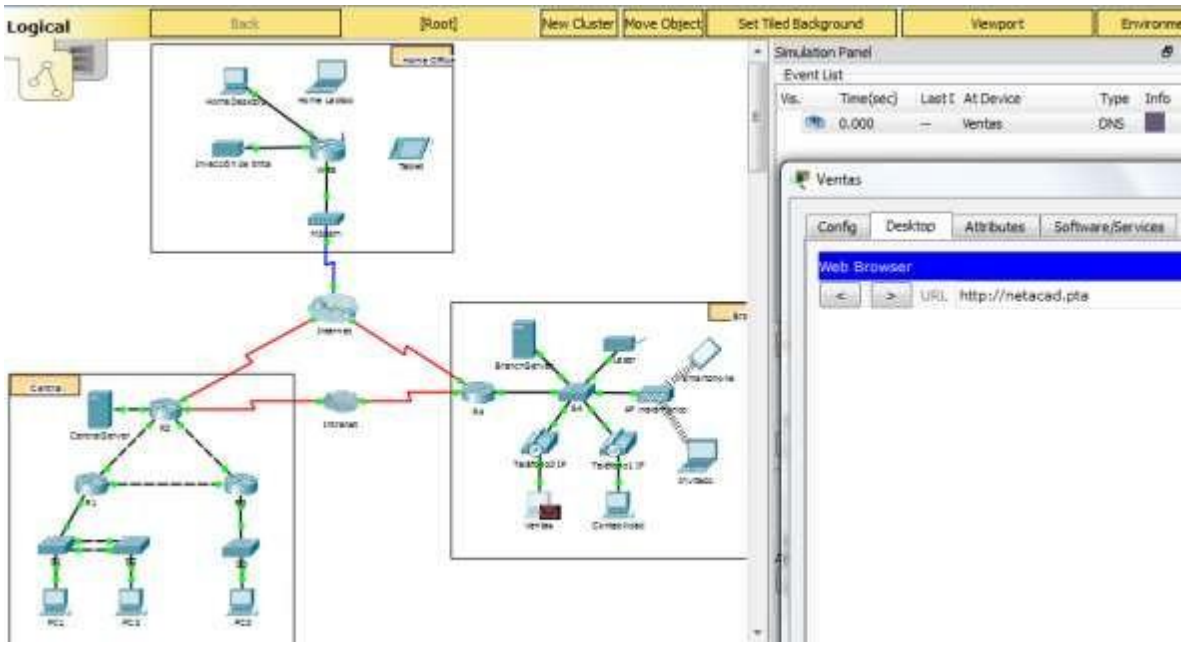
En la parte 3 de esta actividad, borrará los eventos y comenzará una nueva solicitud Web que usará Internet.

Paso 1: Configurar la captura de tráfico hacia un servidor Web de Internet

a. Cierre todas las ventanas de información de PDU abiertas.

b. Haga clic en la opción **Reset Simulation**, que se encuentra cerca del centro del panel de simulación. Escriba **http://www.netacad.pta** en el explorador Web de Sales PC.

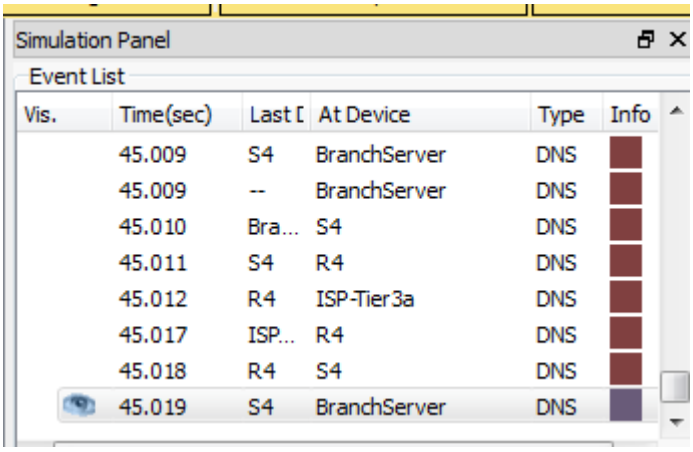
Figura 15.4



Fuente propia

c. Haga clic en **Auto Capture/Play** (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en **View Previous Events** (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe que la primera serie de eventos es **DNS**. ¿Qué advierte sobre la cantidad de eventos de **DNS**?

Figura 15.5



Fuente propia

d. Observe algunos de los dispositivos a través de los que se transfieren los eventos de DNS en el camino hacia un servidor DNS. ¿Dónde se encuentran estos dispositivos?

R/ Se encuentran en la red Branch

e. Haga clic en el último evento de DNS . Haga clic en la ficha Inbound PDU Details y desplácese hasta la última sección DNS Answer. ¿Cuál es la dirección que se indica para www.netacad.pta?

R/ 216.146.46.11

f. Cuando los routers mueven el evento de HTTP a través de la red, hay tres capas activas en In Layers y Out Layers en la ficha OSI Model. Sobre la base de esa información, ¿cuántos routers se atraviesan?

R/ Un solo Router S4 interactua con la nube

g. Haga clic en el evento de TCP anterior al último evento de HTTP . Según la información que se muestra, ¿cuál es el propósito de este evento?

R/ Cerrar la conexión con el servidor 216.146.46.11

h. Se indican varios eventos más de TCP . Ubique el evento de TCP donde se indique IP Phone (Teléfono IP) para Last Device (Último dispositivo) y Sales para At Device. Haga clic en el cuadro coloreado Info y seleccione Layer 4 en la ficha OSI Model. Según la información del resultado, ¿cómo se configuró el estado de la conexión?

- **Numeral 4.2.4.5**

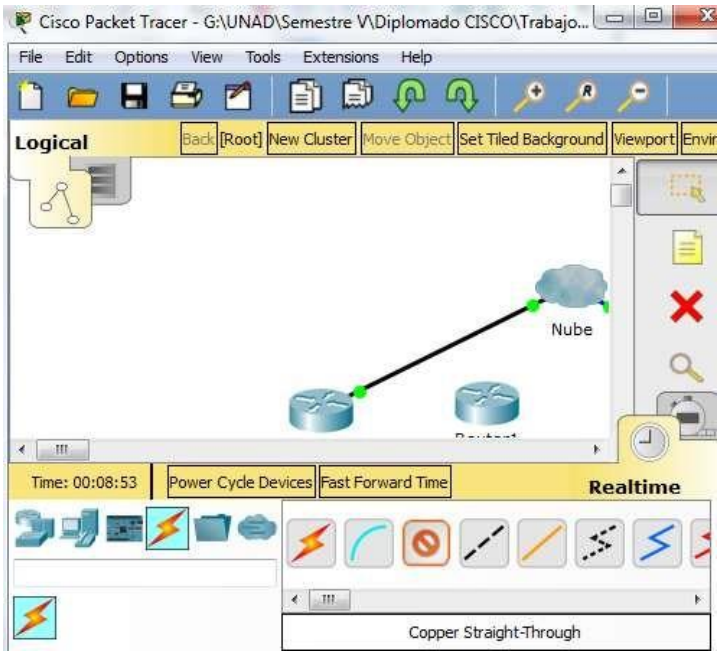
Parte 1: Conectarse a la nube

Paso 1: Conectar la nube al Router0.

a. En la esquina inferior izquierda, haga clic en el ícono de rayo anaranjado para abrir las **conexiones** disponibles.

b. Elija el cable adecuado para conectar la **interfaz Fa0/0 del Router0** a la **interfaz Eth6 de la nube**. La **nube** es un tipo de switch, de modo que debe usar una conexión por **cable de cobre de conexión directa**. Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Figura 15.6



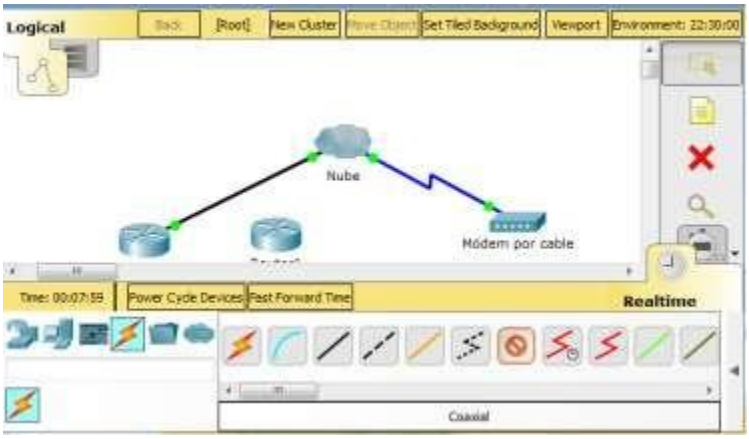
Fuente propia

Paso 2: Conectar la nube al módem por cable.

Elija el cable adecuado para conectar la **interfaz Coax7 de la nube** al **Puerto0 del módem**.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Figura 15.7



Fuente propia

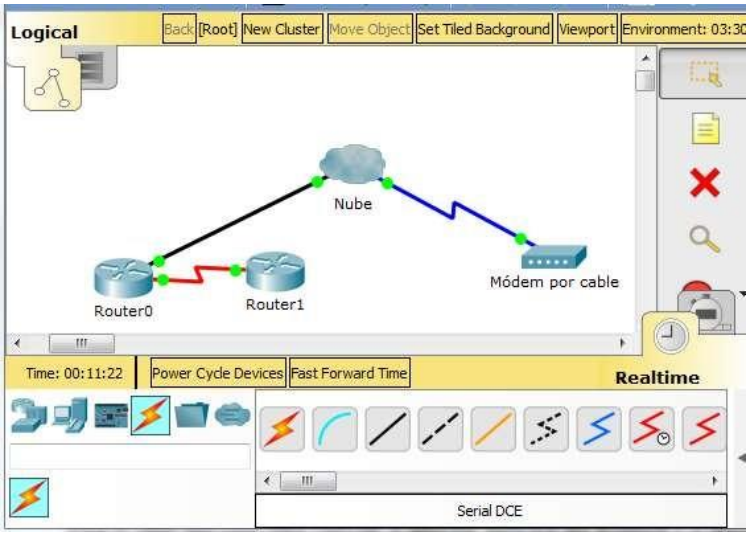
Parte 2: Conectar el Router0

Paso 1: Conecte el Router0 al Router1.

Elija el cable adecuado para conectar la **interfaz Ser0/0/0 del Router0** a la **interfaz Ser0/0 del Router1**. Use uno de los cables **seriales** disponibles.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Figura 15.8



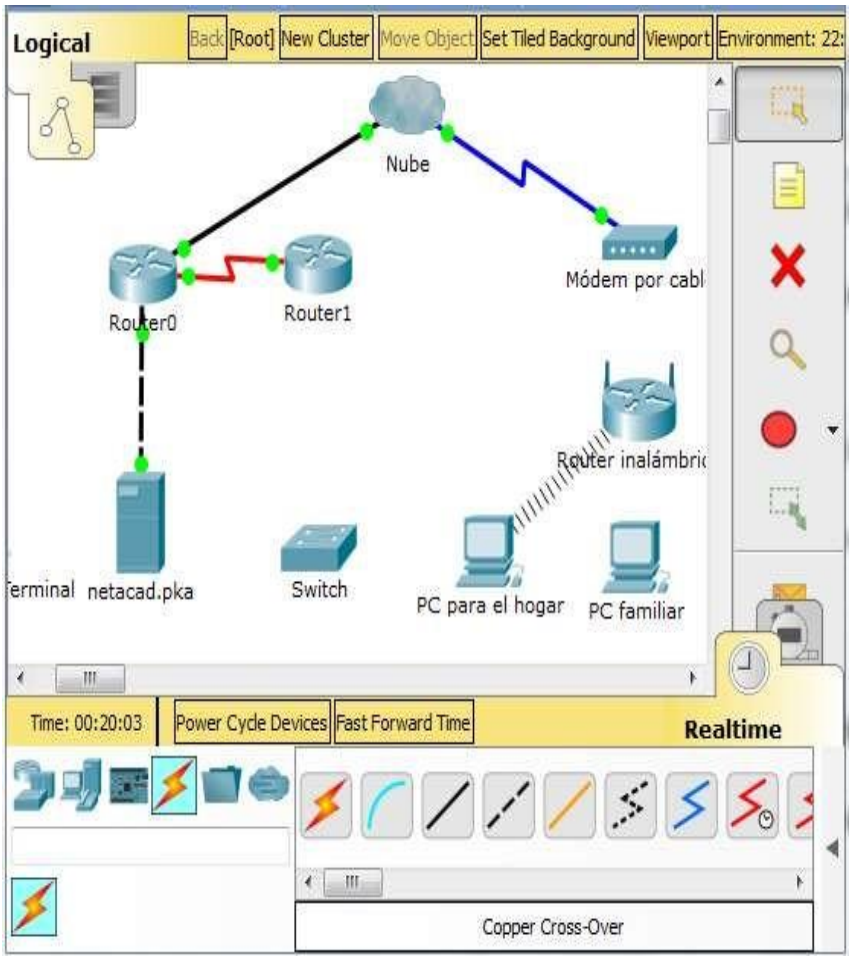
Fuente propia

Paso 2: Conectar el Router0 a netacad.pka.

Elija el cable adecuado para conectar la **interfaz Fa0/1 del Router0** a la **interfaz Fa0 de netacad.pka**. Los routers y las PC tradicionalmente utilizan los mismos cables para transmitir (1 y 2) y recibir (3 y 6). El cable adecuado que se debe elegir consta de cables cruzados. Si bien muchas NIC ahora pueden detectar automáticamente qué par se utiliza para transmitir y recibir, el **Router0** y **netacad.pka** no tienen NIC con detección automática.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Figura 119



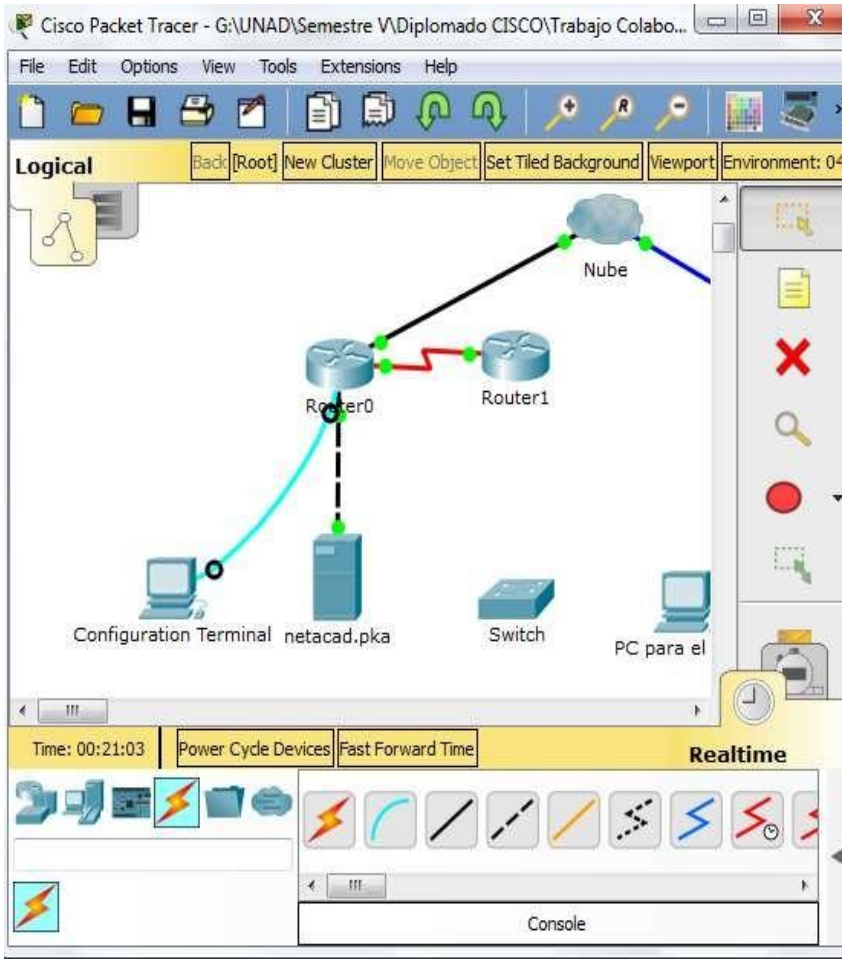
Fuente propia

Paso 3: Conectar el Router0 a la terminal de configuración.

Elija el cable adecuado para conectar la **consola** del **Router0** a la **terminal de configuración RS232**. Este cable no proporciona acceso a la red a la **terminal de configuración**, pero le permite configurar el**Router0** a través de su terminal.

Si conectó el cable correcto, las luces de enlace del cable cambian a color negro.

Figura 120



Fuente propia

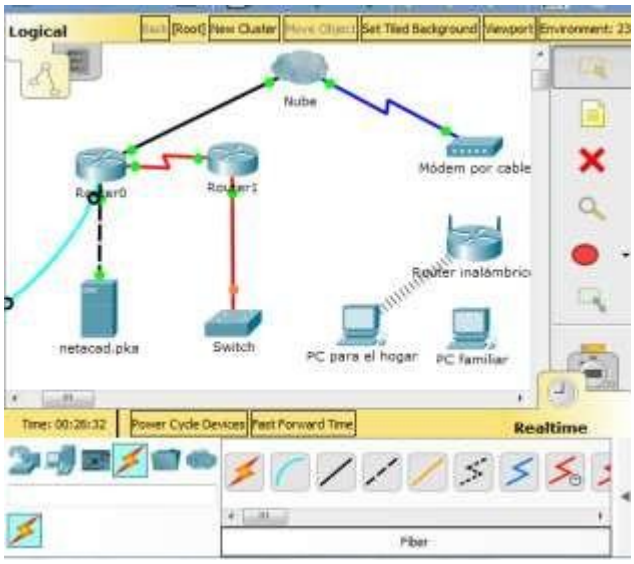
Parte 3: Conectar los dispositivos restantes

Paso 1: Conectar el Router1 al switch.

Elija el cable adecuado para conectar la **interfaz Fa1/0 del Router1** a la **interfaz Fa0/1 del switch**.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde. Deje que transcurran unos segundos para que la luz cambie de color ámbar a verde.

Figura 16.1



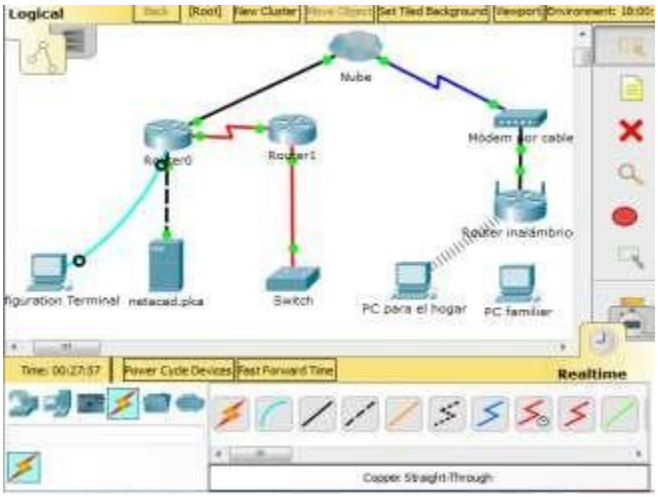
Fuente propia

Paso 2: Conectar el módem por cable al router inalámbrico.

Elija el cable adecuado para conectar el **Puerto1** del **módem** al puerto de **Internet del router inalámbrico**.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Figura 16.2



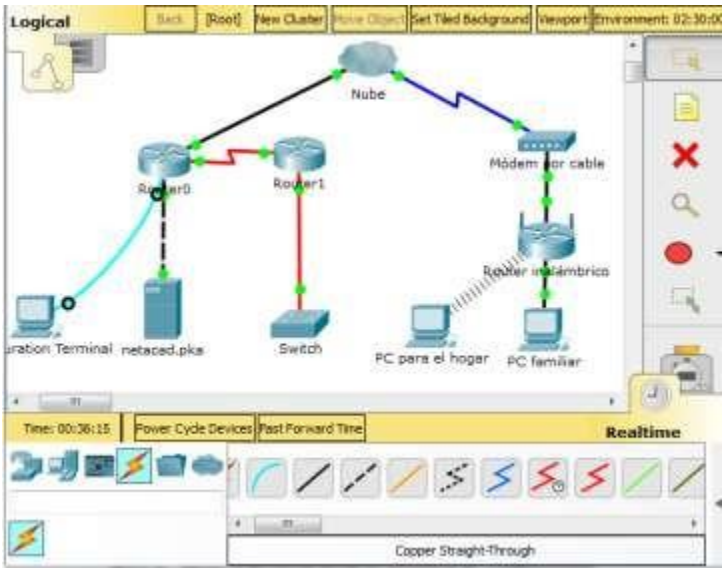
Fuente propia

Paso 3: Conectar el router inalámbrico a la PC familiar.

Elija el cable adecuado para conectar la **interfaz Ethernet 1 del router inalámbrico** a la **PC familiar**.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Figura 16.4



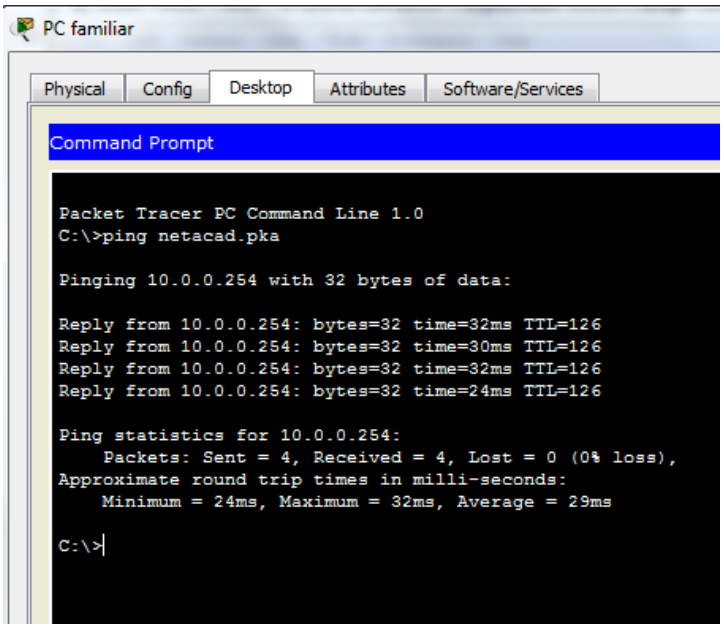
Fuente propia

Parte 4: Verificar las conexiones

Paso 1: Probar la conexión de la PC familiar a netacad.pka

a. Abra el símbolo del sistema de la **PC familiar** y haga ping a **netacad.pka**.

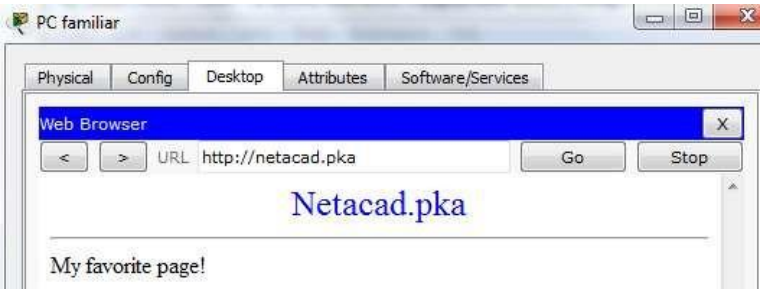
Figura 16.5



Fuente propia

b. Abra el **explorador Web** e introduzca dirección Web **http://netacad.pka**.

Figura 16.6

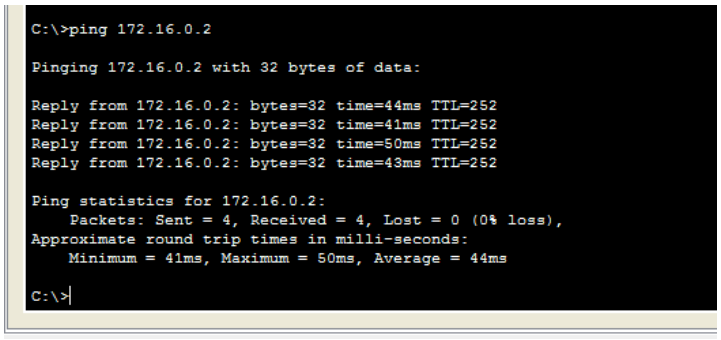


Fuente propia

Paso 2: Hacer ping al switch desde la PC doméstica.

Abra el símbolo del sistema de la **PC doméstica** y haga ping a la dirección IP del **switch** para verificar la conexión.

Figura 16.7



Fuente propia

Paso 3: Abrir el Router0 desde la terminal de configuración.

a. Abra la **terminal** de la **terminal de configuración** y acepte la configuración predeterminada.

b. Presione **Entrar** para ver el símbolo del sistema del **Router0** .

c. Escriba **show ip interface brief** para ver el estado de las interfaces.

Figura 16.8

```
Router0>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.2.1     YES manual up                    up
FastEthernet0/1        10.0.0.1        YES manual up                    up
Serial0/0/0            172.31.0.1      YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router0>
```

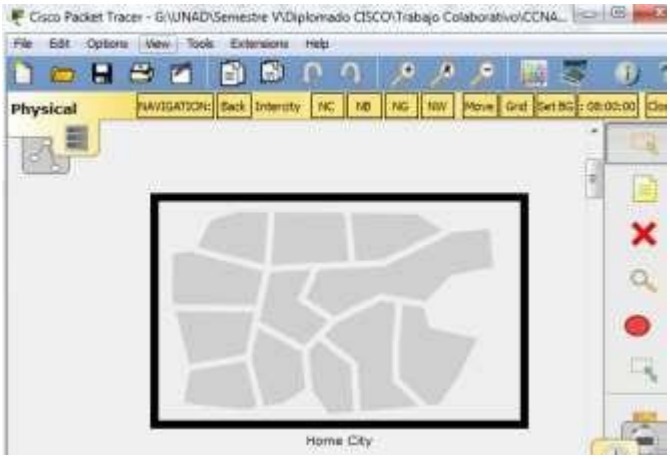
Fuente propia

Parte 5: Examinar la topología física

Paso 1: Examinar la nube.

a. Haga clic en la ficha **Physical Workspace** (Área de trabajo física) o presione **Mayús** + **P** y **Mayús** + **L** para alternar entre las áreas de trabajo lógicas y físicas.

Figura 16.9



Fuente propia

b. Haga clic en el ícono **Home City** (Ciudad de residencia).

c. Haga clic en el ícono **Cloud** (Nube). ¿Cuántos cables están conectados al switch en el bastidor azul?

Figura 17.0

Fuente propia

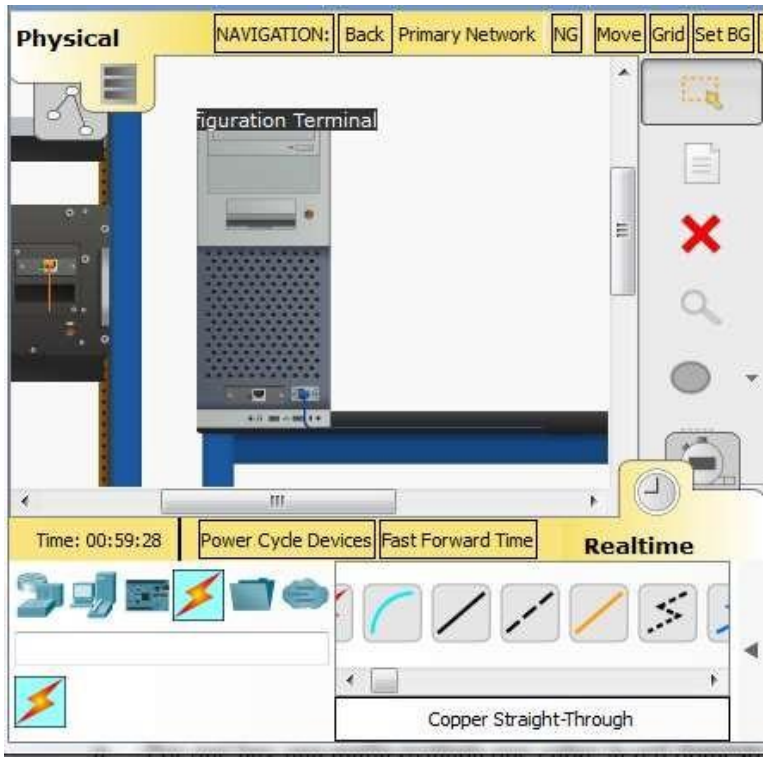
d. Haga clic en Back (Atrás) para volver a Home City (Ciudad de residencia).

Paso 2: Examinar la red principal.

a. Haga clic en el ícono Primary Network (Red principal). Mantenga el puntero del mouse sobre los distintos cables. ¿Qué se encuentra sobre la mesa a la derecha del bastidor azul?

R/ Se encuentra la CPU de la Terminal de configuración.

Figura 17.1



Fuente propia

b. Haga clic en Back (Atrás) para volver a Home City (Ciudad de residencia).

Paso 3: Examinar la red secundaria.

a. Haga clic en el ícono Secondary Network (Red secundaria). Mantenga el puntero del mouse sobre los distintos cables. ¿Por qué hay dos cables anaranjados conectados a cada dispositivo?
R/ Porque se necesita un cable para la transmisión y otro para recepción.

b. Haga clic en Back (Atrás) para volver a Home City (Ciudad de residencia).

Paso 4: Examinar la red doméstica.

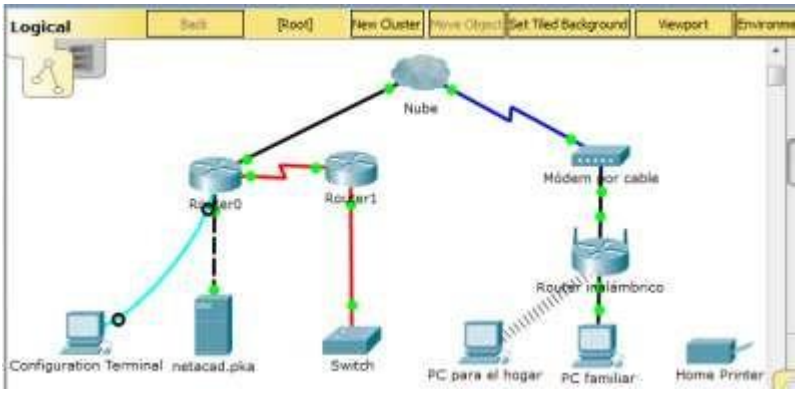
a. ¿Por qué hay una malla ovalada que cubre la red doméstica?

R/ Quiere decir que existe una conexión inalámbrica entre el PC Domestico y el Router Inalámbrico.

b. Haga clic en el ícono Home Network (Red doméstica). ¿Por qué no hay ningún bastidor para contener el equipo?
R/ Los dispositivos de una red domestica casi nunca tienen bastidores, esto se cumple regularmente a nivel empresarial.

c. Haga clic en la ficha Logical Workspace (Área de trabajo lógica) para volver a la topología lógica.

Figura 17.2

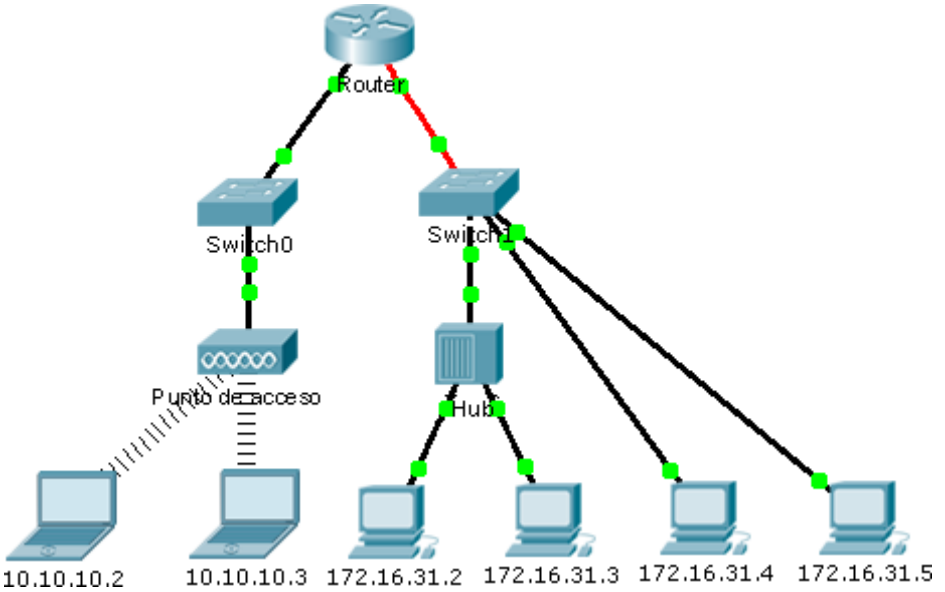


Fuente propia

Packet Tracer: Identificación de direcciones MAC y direcciones IP

5. 4 Topología

Figura 17.3



Fuente propia

Información básica:

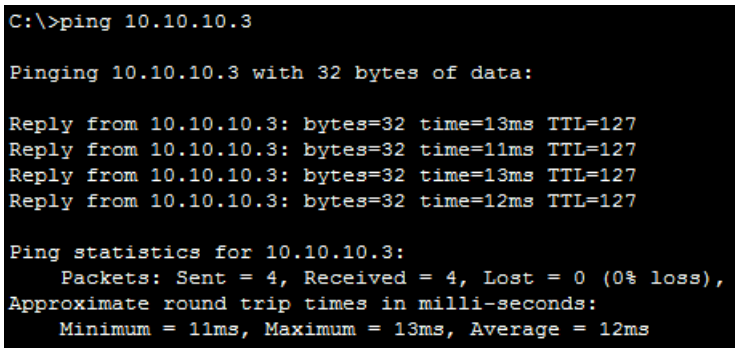
Esta actividad está optimizada para la visualización de PDU. Los dispositivos ya están configurados. Recopilará información de PDU en el modo de simulación y responderá una serie de preguntas sobre los datos que obtenga.

Parte 1: Recopilar información de la PDU
Nota: revise las preguntas de reflexión de la parte 2 antes de continuar con la parte 1. Le darán una idea de los tipos de información que debe recopilar.

Paso 1: Recopilar información de la PDU mientras un paquete se transfiere de 172.16.31.2 a 10.10.10.3

a. Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.
b. Introduzca el comando **ping 10.10.10.3**.

Figura 17.4

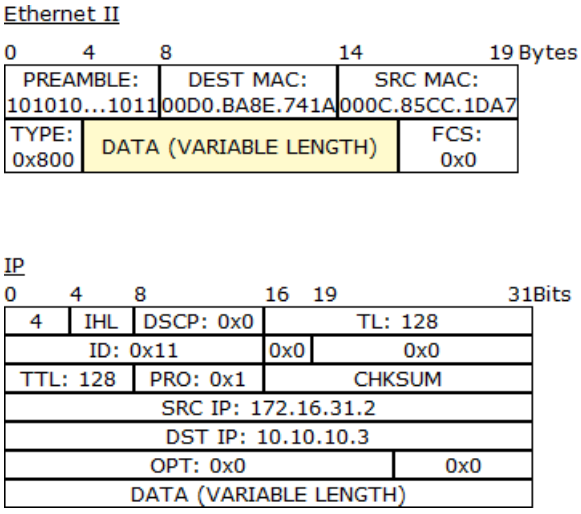


Fuente propia

c. Cambie al modo de simulación y repita el comando **ping 10.10.10.3**. Aparece una PDU junto a **172.16.31.2**.
d. Haga clic en la PDU y observe la siguiente información en la ficha **Outbound PDU Layer** (Capa de PDU saliente):

- Dirección MAC de destino: 00D0:BA8E:741A
- Dirección MAC de origen: 000C:85CC:1DA7
- Dirección IP de origen: 172.16.31.2
- Dirección IP de destino: 10.10.10.3
- En el dispositivo: PC

Figura 17.5



Fuente propia

e. Haga **clic en Capture/Forward (Capturar/reenviar)** para mover la PDU al siguiente dispositivo. Recopile la misma información del paso 1d. Repita este proceso hasta que la PDU llegue al destino. Registre la información que recopiló de la PDU en una hoja de cálculo con un formato como el de la tabla que se muestra a continuación:

Tabla 1.2. Formato de hoja de cálculo de ejemplo

Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.2 a 10.10.10.3	172.16.31.2	00D0:BA8E:741A	000C:85CC:1DA7	172.16.31.2	10.10.10.3
	Hub	--	--	--	--
	Switch1	00D0:BA8E:741A	000C:85CC:1DA7	--	--
	Router	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3
	Switch0	0060:4706:572B	00D0:588C:2401	--	--
	Punto de acceso	--	--	--	--
	10.10.10.3	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3

Paso 2: Recopilar información adicional de la PDU de otros ping

Repita el proceso del paso 1 y recopile información para las pruebas siguientes:

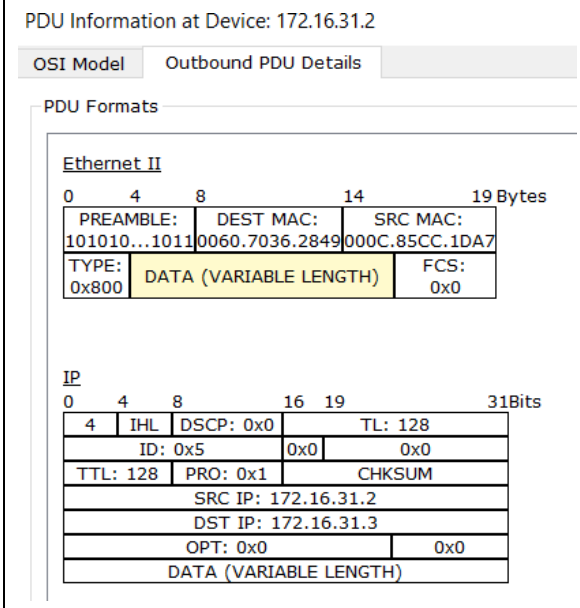
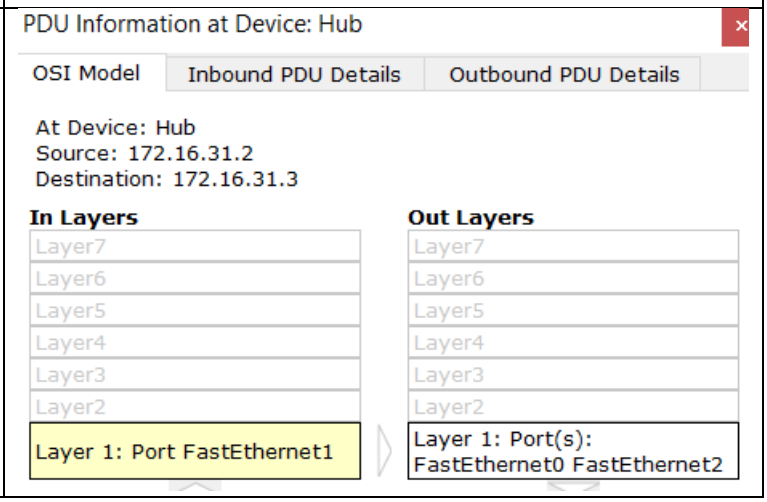
Ping de 10.10.10.2 a 10.10.10.3

Tabla 1.3

Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 10.10.10.2 a 10.10.10.3	10.10.10.2	0050.0FAB.6C82	0060.2FB4.4AB6	10.10.10.2	10.10.10.3
	Access point	--	--	--	--
	10.10.10.3	0060.4706.572B	0050.0FAB.6C82	10.10.10.2	10.10.10.3

Ping de 172.16.31.2 a 172.16.31.3

Tabla 1.4

PDU	
172.16.31.2	
Hub	

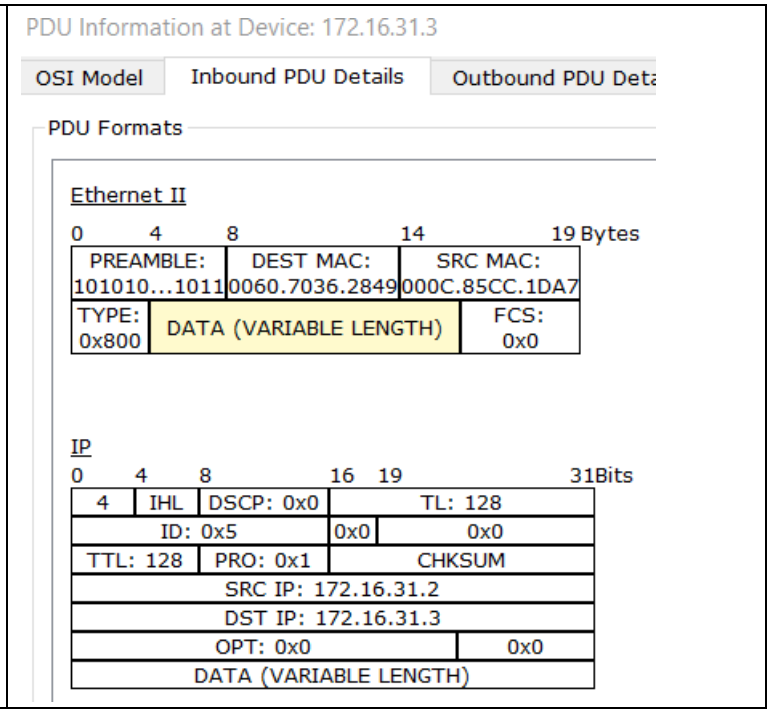
172.16.31.3	

Tabla 1.5

Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.2 a 172.16.31.3	172.16.31.2	0060.7036.2849	000C.85CC.1DA	172.16.31.2	172.16.31.3
	Hub	--	--	--	--
	172.16.31.3	0060.7036.2849	000C.85CC.1DA7	172.16.31.2	172.16.31.3

Ping de 172.16.31.4 a 172.16.31.5

Tabla 1.

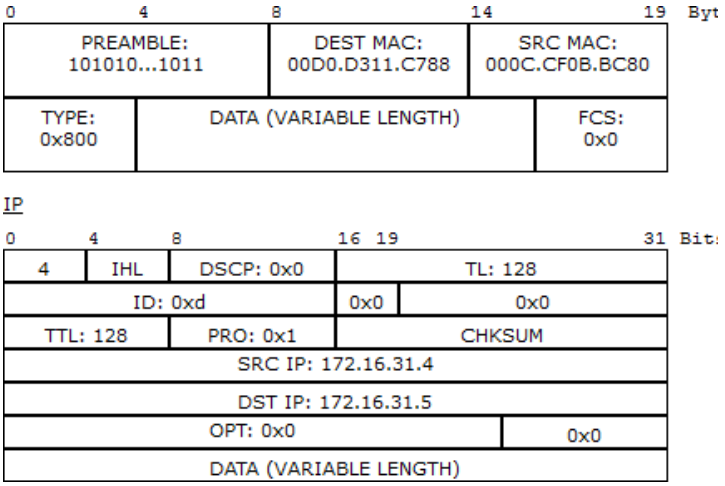
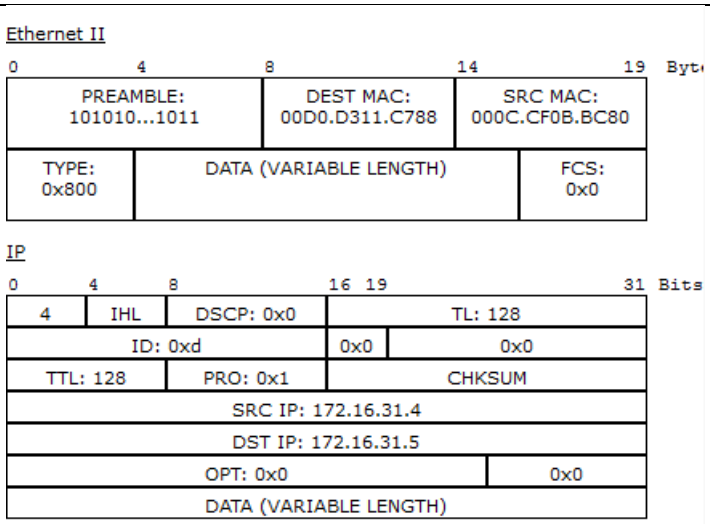
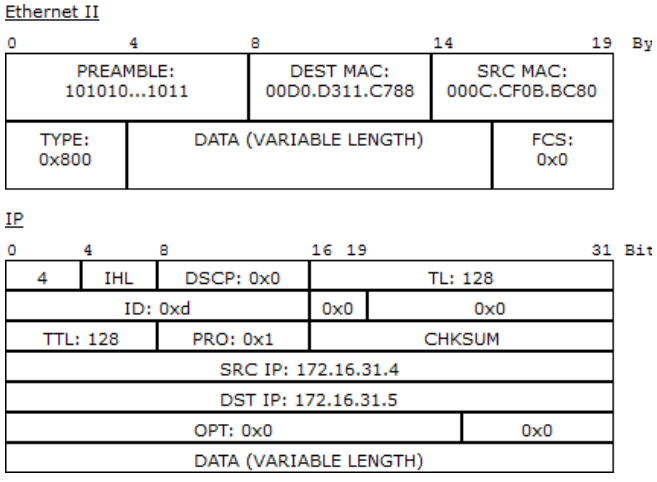
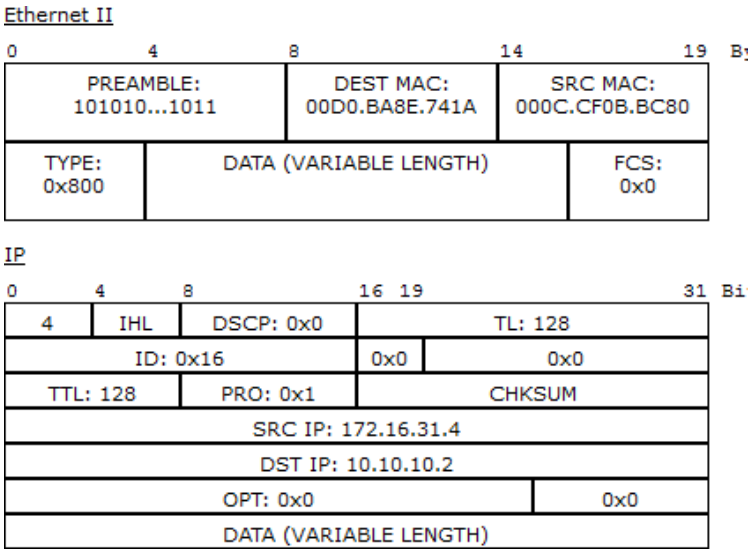
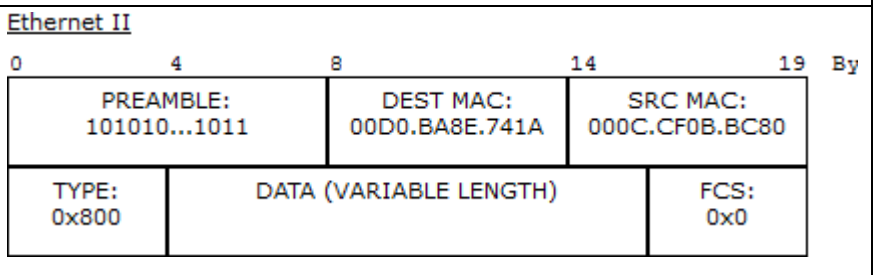
En 172.16.31.4	
Switch	
172.16.31.5	

Tabla 1.

Prueba	En dispositivo	Direccion MAC	Src MAC	Src IPV4	Dest IPV4
Ping de 172.16.31.4 a 172.16.31.5	172.16.31.4	00D0.D311.C788	000C.CF0B.BC80	172.16.31.4	172.16.31.5
	Switch	00D0.D311.C788	000C.CF0B.BC80		
	172.16.31.5	00D0.D311.C788	000C.CF0B.BC80	172.16.31.4	172.16.31.5

Ping de 172.16.31.4 a 10.10.10.2

Tabla 1.8

172.16.31.4	
Switch1	

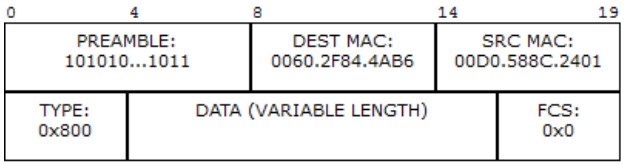
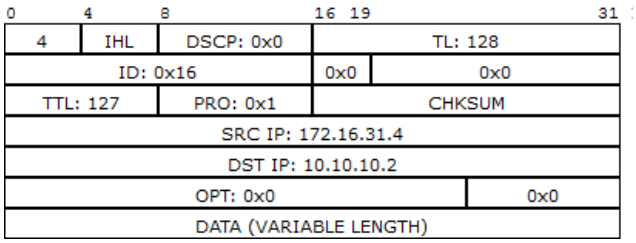
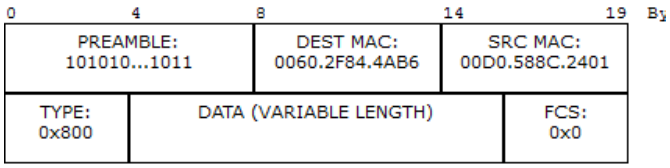
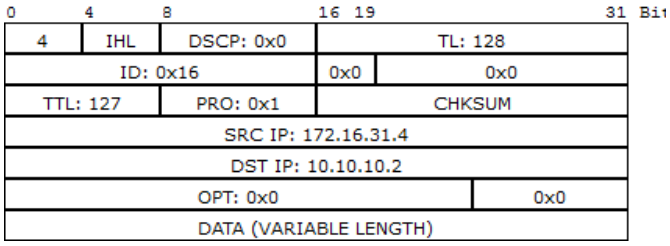
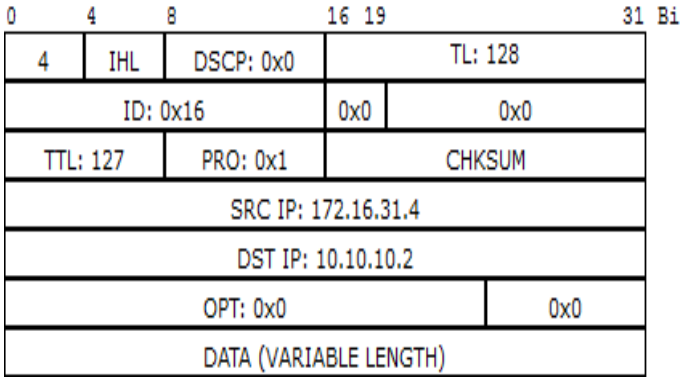
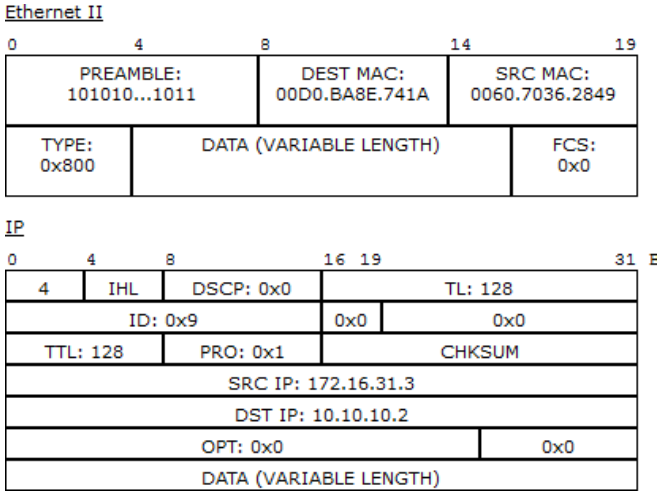
Router	Ethernet II  IP 
Switch0	Ethernet II  IP 
10.10.10.2	IP 

Tabla 1.9

Prueba	En dispositivo	Direccion MAC	Src MAC	Src IPV4	Dest IPV4
Ping de 172.16.31.4 a 10.10.10.2	172.16.31.4	00D0.BA8E.741A	000C.CF0B.BC80	172.16.31.4	10.10.10.2
	Switch1	00D0.BA8E.741A	000C.CF0B.BC80	--	--
	Router	0060.2F84.4AB6	00D0.588C.2401	172.16.31.4	10.10.10.2
	Switch0	0060.2F84.4AB6	00D0.588C.2401	--	--
	Access point	--	--	--	--
	10.10.10.2	0060.2F84.4AB6	00D0.588C.2401	172.16.31.4	10.10.10.2

Ping de 172.16.31.3 a 10.10.10.2

Tabla 2.0

172.16.31.3	

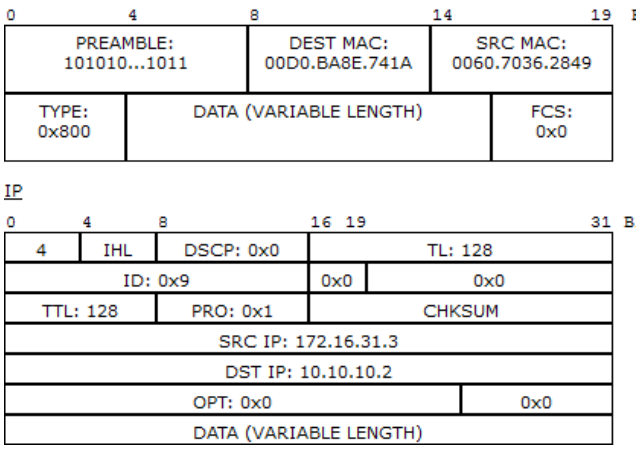
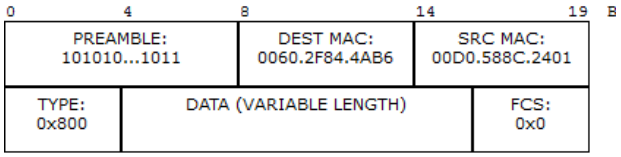
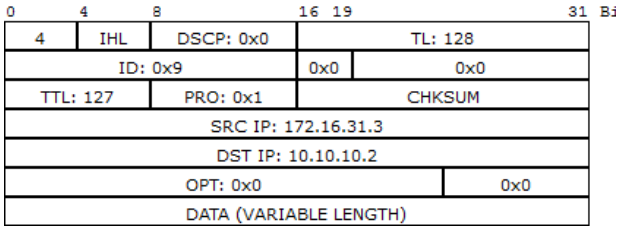
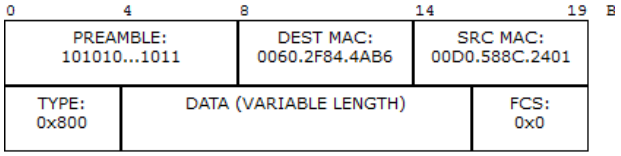
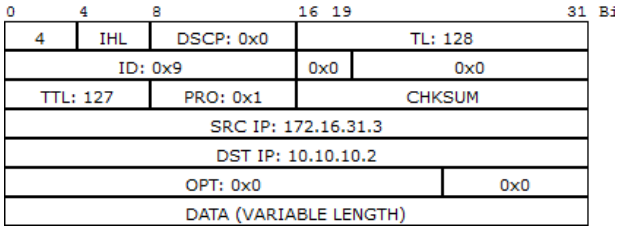
Switch1	Ethernet II  IP
Router	Ethernet II  IP 
10.10.10.2	Ethernet II  IP 

Tabla 2.1

Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPV4	Dest IPV4
Ping de 172.16.31.3 a 10.10.10.2	172.16.31.3	00D0.BA8E.741A	0060.7036.2849	172.16.31.3	10.10.10.2
	Hub	--	--	--	--
	Switch1	00D0.BA8E.741A	0060.7036.2849	--	--
	Router	0060.2F84.4AB6	00D0.588C.2401	172.16.31.3	10.10.10.2
	Switch0	0060.2F84.4AB6	00D0.588C.2401	--	--
	Access point	--	--	--	--
	10.10.10.2	0060.2F84.4AB6	00D0.588C.2401	172.16.31.3	10.10.10.2

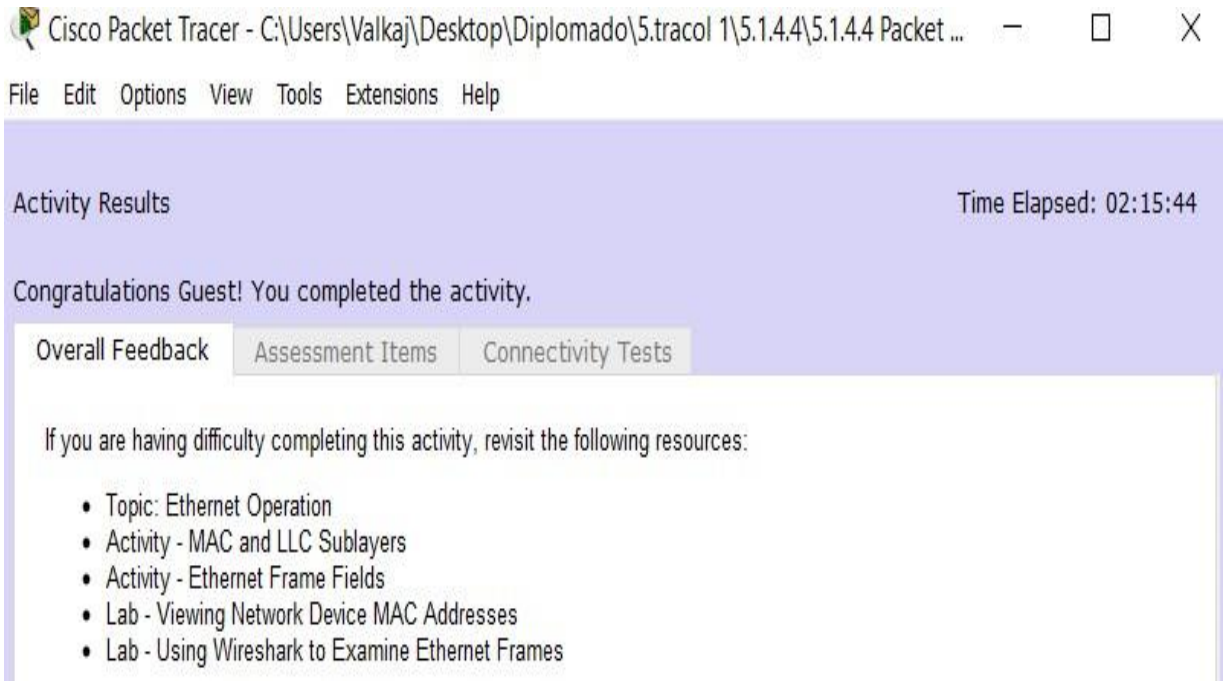
Parte 2: Preguntas de reflexión

Responda las siguientes preguntas relacionadas con la información reunida:

1. ¿Se utilizaron diferentes tipos de cables para conectar los dispositivos? Sí, de cobre y de fibra.
2. ¿Los cables cambiaron el manejo de la PDU de alguna forma? No
3. ¿El **hub** perdió la información que se le entregó? No
4. ¿Qué hace el **hub** con las direcciones MAC y las direcciones IP? Nada.
5. ¿El **punto de acceso inalámbrico** hizo algo con la información que se le entregó? Sí. La volvió a empaquetar según el estándar inalámbrico 802.11.
6. ¿Se perdió alguna dirección MAC o IP durante la transferencia inalámbrica? No
7. ¿Cuál fue la capa OSI más alta que utilizaron el **hub** y el **punto de acceso**? Capa 1
8. ¿El **hub** o el **punto de acceso** reprodujeron en algún momento una PDU rechazada con una “X” de color rojo? Sí
9. Al examinar la ficha **PDU Details** (Detalles de PDU), ¿qué dirección MAC aparecía primero, la de origen o la de destino? Destino
10. ¿Por qué las direcciones MAC aparecen en este orden? Si el destino aparece primero en la lista, un switch puede comenzar a reenviar una trama a una dirección MAC conocida más rápidamente.
11. ¿Había un patrón para el direccionamiento MAC en la simulación? No

12. ¿Los switches reprodujeron en algún momento una PDU rechazada con una “X” de color rojo? No
13. Cada vez que se enviaba la PDU entre las redes 10 y 172, había un punto donde las direcciones MAC cambiaban repentinamente. ¿Dónde ocurrió eso? En el router.
14. ¿Qué dispositivo utiliza las direcciones MAC que comienzan con 00D0? El router.
15. ¿A qué dispositivos pertenecen las otras direcciones MAC? Al emisor y al receptor.
16. ¿Las direcciones IPv4 de envío y recepción cambian en alguna de las PDU? No
17. Si sigue la respuesta a un ping, a veces denominado *pong*, ¿las direcciones IPv4 de envío y recepción cambian? Sí
18. ¿Cuál es el patrón para el direccionamiento IPv4 en esta simulación? Cada puerto de router requiere un conjunto de direcciones que no se superpongan.
19. ¿Por qué es necesario asignar diferentes redes IP a los diferentes puertos de un router? La función de un router es interconectar diferentes redes IP.
20. Si esta simulación fuera configurada con IPv6 en vez de IPv4, ¿cuál sería la diferencia? Las direcciones IPv4 se reemplazarían con direcciones IPv6, pero todo lo demás sería igual.

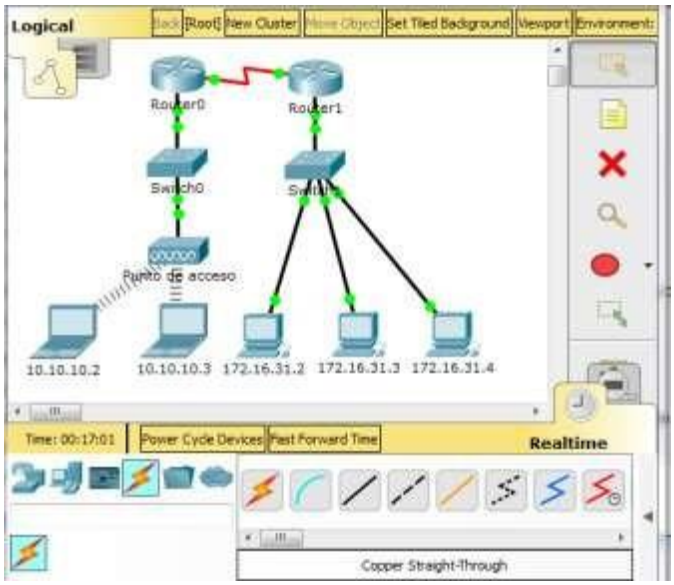
Figura 17.6



Fuente propia

- **Numeral 5.2.1.7**

Figura 17.7



Fuente propia

Tabla 2.2

Dispositivo	Interfaz	Dirección MAC	Interfaz del switch
Router0	Gig0/0	0001.6458.2501	Gig0/1
	Se0/0/0	No aplicable	No aplicable
Router1	Gig0/0	00E0.F7B1.8901	Gig0/1
	Se0/0/0	No aplicable	No aplicable
10.10.10.2.	Inalámbrico	0060.2F84.4AB6	Fa0/2
10.10.10.3	Inalámbrico	0060.4706.572B	Fa0/2
172.16.31.2	Fa0	000C.85CC.1DA7	Fa0/1
172.16.31.3	Fa0	0060.7036.2849	Fa0/2
172.16.31.4	Gig0	0002.1640.8D75	Fa0/3

Parte 1: Examinar una solicitud de ARP

Paso 1: Generar solicitudes de ARP haciendo ping a 172.16.31.3 desde 172.16.31.2

a. Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.

b. Introduzca el comando **arp -d** para borrar la tabla ARP.

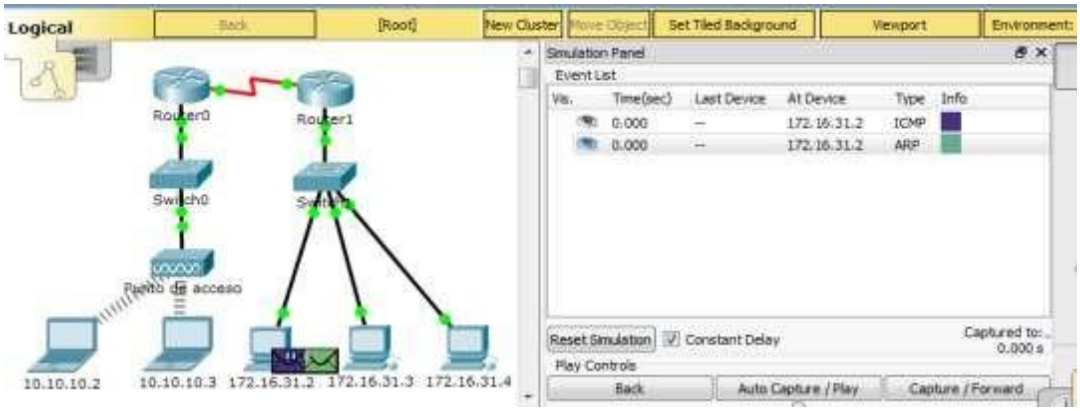
Figura 17.8

```
C:\>arp -d
C:\>ping 172.16.31.3

Pinging 172.16.31.3 with 32 bytes of data:

Reply from 172.16.31.3: bytes=32 time=30ms TTL=128
Reply from 172.16.31.3: bytes=32 time=13ms TTL=128
Reply from 172.16.31.3: bytes=32 time=15ms TTL=128
Reply from 172.16.31.3: bytes=32 time=1ms TTL=128

Ping statistics for 172.16.31.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 30ms, Average = 14ms
```

Fuente propia

c. Ingrese al modo **Simulation** (Simulación) e introduzca el comando **ping 172.16.31.3**. Se generan dos PDU. El comando **ping** no puede completar el paquete ICMP sin conocer la dirección MAC del destino. Por lo tanto, la PC envía una trama de broadcast de ARP para hallar la dirección MAC del destino.

Figura 17.9

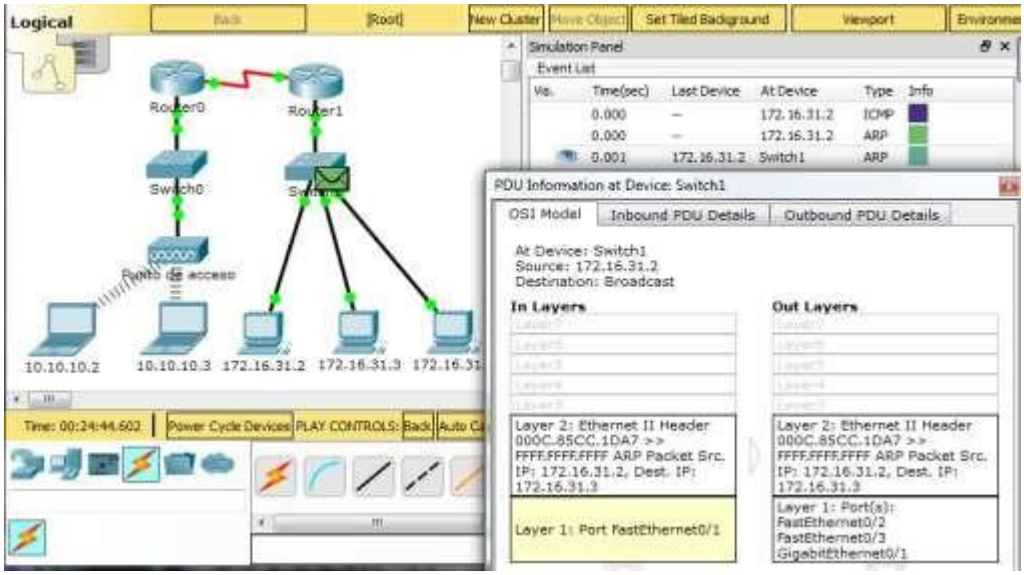


Fuente propia

d. Haga clic en Capture/Forward (Capturar/avanzar) una vez. La PDU ARP mueve el Switch1, mientras que la PDU ICMP desaparece y espera la respuesta de ARP. Abra la PDU y registre la dirección MAC de destino. ¿Esta dirección se indica en la tabla anterior?

R/ Indica la dirección de destino 176.16.31.3 que se encuentra en la tabla anterior

Figura 18.0



Fuente propia

e. Haga clic en **Capture/Forward** (Capturar/avanzar) para mover la PDU al siguiente dispositivo. ¿Cuántas copias de la PDU realizó el **Switch1**?

R/ 3 copias

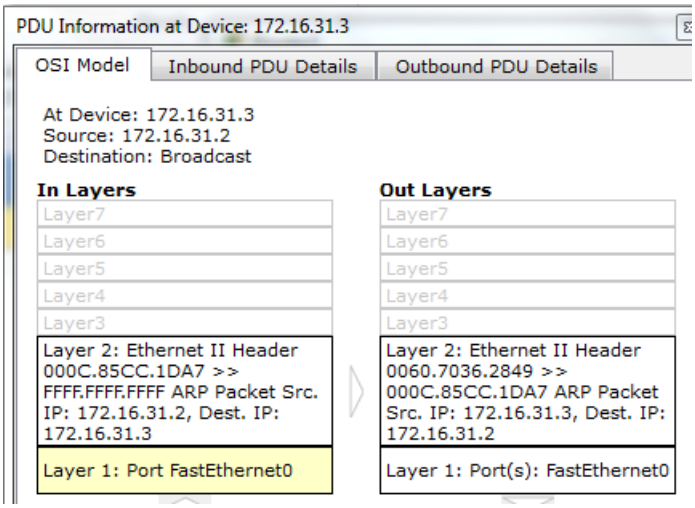
f. ¿Cuál es la dirección IP del dispositivo que aceptó la PDU?

R/ 172.16.31.3

g. Abra la PDU y examine la capa 2. ¿Qué sucedió con las direcciones MAC de origen y destino?

R/ Se intercambiaron las dos MAC debido a que ya se identifico la MAC de destino, ahora la PC 176.16.31.3 responderà el mensaje enviando una PDU a 176.16.31.2.

Figura 18.1



Fuente propia

h. Haga clic en **Capture/Forward** hasta que la PDU regrese a **172.16.31.2**. ¿Cuántas copias de la PDU realizó el switch durante la respuesta de ARP?

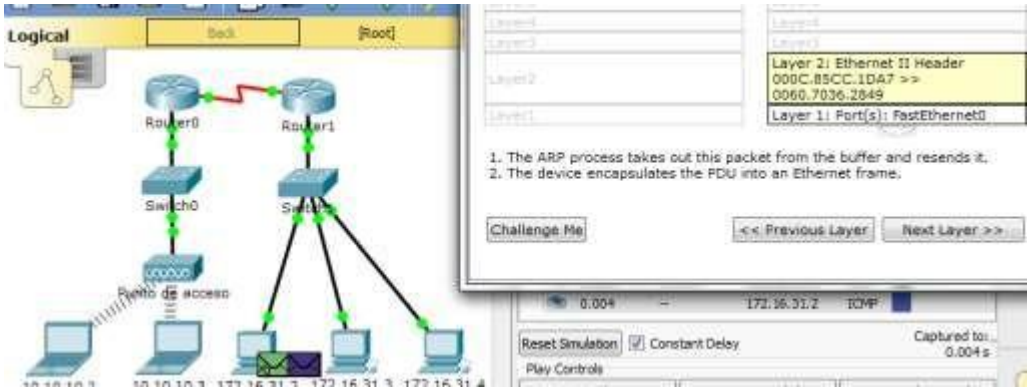
R/ Realizo 1 copia hacia 172.16.31.2

Paso 2: Revisar la tabla ARP

a. Observe que vuelve a aparecer el paquete ICMP. Abra la PDU y revise las direcciones MAC. ¿Las direcciones MAC de origen y destino coinciden con sus direcciones IP?

R/ Si coinciden

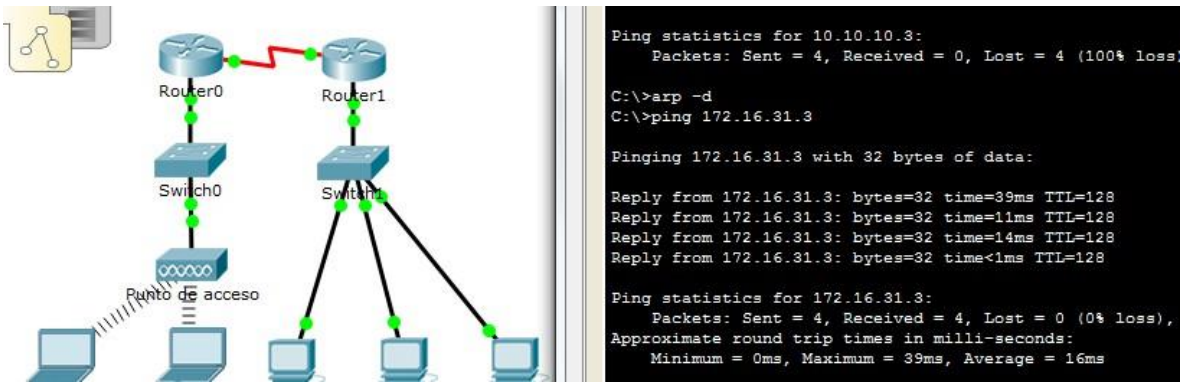
Figura 18.2



Fuente propia

b. Vuelva a cambiar al modo **Realtime** (Tiempo real), y el ping se completa.

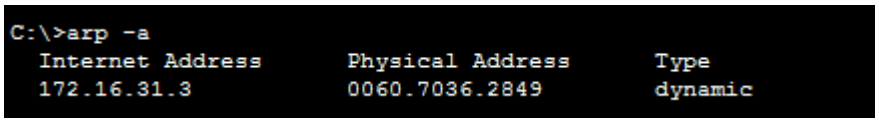
Figura 18.3



Fuente propia

c. Haga clic en **172.16.31.2** e introduzca el comando **arp -a**. ¿A qué dirección IP corresponde la entrada de la dirección MAC?

Figura 18.4



Fuente propia

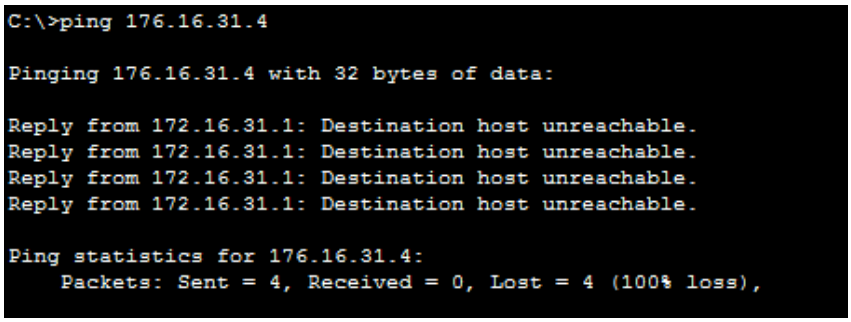
d. En general, ¿cuándo emite un dispositivo final una solicitud de ARP?
R/ Cuando no conoce la direccion MAC de la dirección IP de destino.

Parte 2:Examinar una tabla de direcciones MAC del switch

Paso 1: Generar tráfico adicional para completar la tabla de direcciones MAC del switch

a. En **172.16.31.2**, introduzca el comando **ping 172.16.31.4**.

Figura 18.5



Fuente propia

b. Haga clic en **10.10.10.2** y abra el **símbolo del sistema**.

c. Introduzca el comando **ping 10.10.10.3**. ¿Cuántas respuestas se enviaron y se recibieron?

Paso 2: Examinar la tabla de direcciones MAC en los switches

a. Haga clic en **Switch1** y, a continuación, en la ficha **CLI**. Introduzca el comando **show mac-address-table**. ¿Las entradas corresponden a las de la tabla anterior?

R/ SI

b. Haga clic en **Switch0** y, a continuación, en la ficha **CLI**. Introduzca el comando **show mac-address-table**. ¿Las entradas corresponden a las de la tabla anterior?

R/ Si

Figura 18.6

```
Switch0>show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.6458.2501    DYNAMIC     Gig0/1
   1    0060.2f84.4ab6    DYNAMIC     Fa0/1
   1    0060.4706.572b    DYNAMIC     Fa0/1
```

Fuente propia

c. ¿Por qué hay dos direcciones MAC asociadas a un puerto?

R/ Porque ambas MAC hicieron uso del mismo puerto para enviarse mensajes.

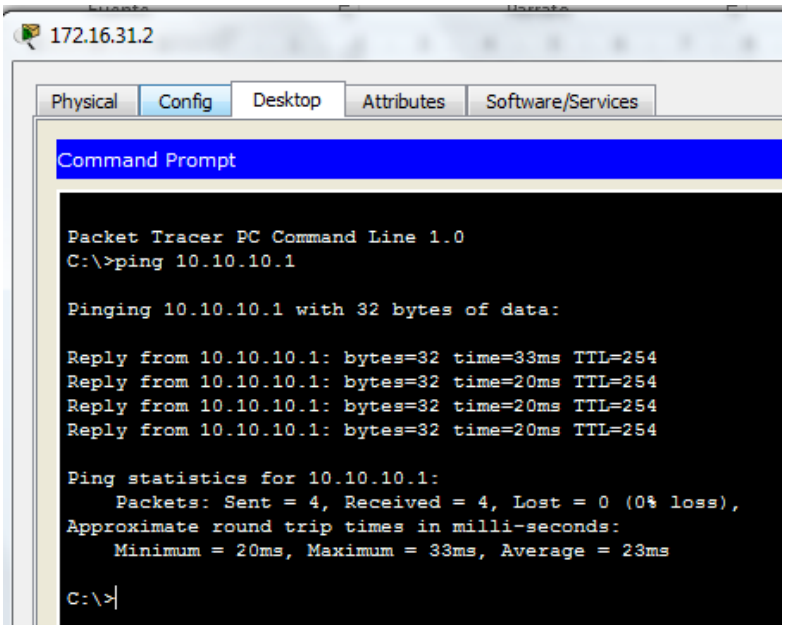
Parte 3:Examinar el proceso de ARP en comunicaciones remotas

Paso 1: Generar tráfico para producir tráfico ARP

a. Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.

b. Introduzca el comando **ping 10.10.10.1**.

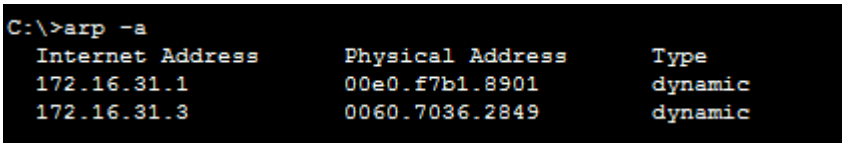
Figura 18.7



Fuente propia

c. Escriba **arp -a**. ¿Cuál es la dirección IP de la nueva entrada de la tabla ARP?

Figura 18.8



Fuente propia

d. Introduzca el comando **arp -d** para borrar la tabla ARP y volver a cambiar al modo de **simulación**.

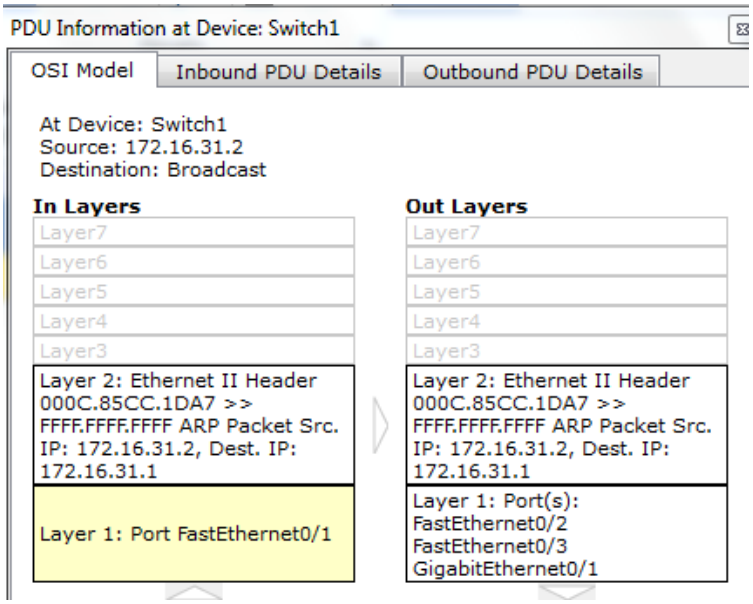
e. Repita el ping a 10.10.10.1. ¿Cuántas PDU aparecen?

R/ Aparecen dos PDU

f. Haga clic en **Capture/Forward** (Capturar/avanzar). Haga clic en la PDU que ahora se encuentra en el **Switch1**. ¿Cuál es la dirección IP de destino de la solicitud de ARP?

R/ IP de destino es 172.16.31.1

Figura 18.9



Fuente propia

g. La dirección IP de destino no es 10.10.10.1. ¿Por qué?

R/ Porque trata de buscar el destino 10.10.10.1 a traves de un Broadcast en su red local, pero como este no se encuentra entonces procede con un evento ICMP a traves de las demás redes externas.}

Paso 2: Examinar la tabla ARP en el Router1

a. Cambie al modo **Realtime**. Haga clic en **Router1** y, a continuación, en la ficha **CLI**.

b. Ingrese al modo EXEC privilegiado y, a continuación, introduzca el comando **show mac-address-table**. ¿Cuántas direcciones MAC figuran en la tabla? ¿Por qué?

R/ El comando es invalido.

Figura 19.0

```
Router>enable
Router#show mac address-table
                ^
% Invalid input detected at '^' marker.
```

Fuente propia

c. Introduzca el comando **show arp**. ¿Figura una entrada para **172.16.31.2**?

R/ Si figura

Figura 19.1

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type
Interface
Internet  172.16.31.1             -   00E0.F7B1.8901  ARPA
GigabitEthernet0/0
Internet  172.16.31.2            46   000C.85CC.1DA7  ARPA
GigabitEthernet0/0
Internet  172.16.31.3             5   0060.7036.2849  ARPA
GigabitEthernet0/0
```

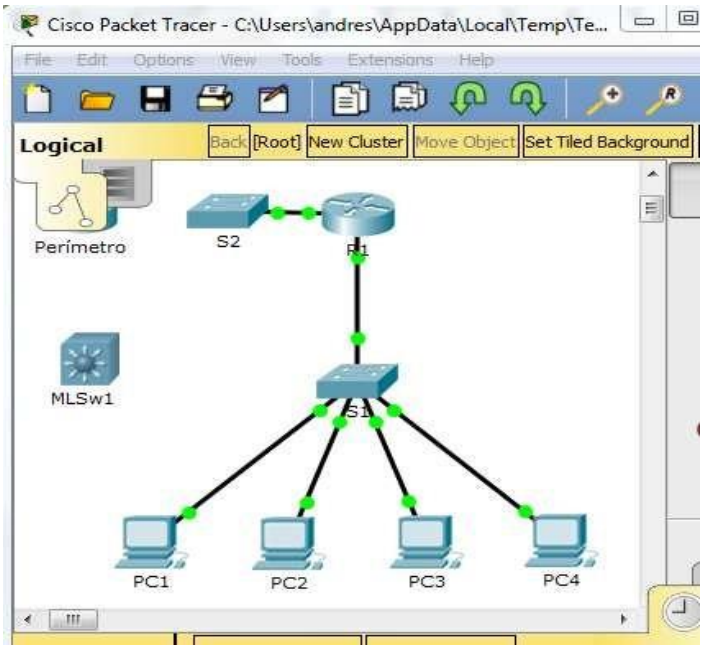
Fuente propia

d. ¿Qué sucede con el primer ping en una situación en la que el router responde a la solicitud de ARP?

R/ Excede el tiempo de espera.

- **Numeral 5.3.3.5**

Figura 19.



Fuente propia

Situación:

El administrador de red reemplaza el router y el switch actuales por un nuevo switch de capa 3. Como técnico de red, su trabajo consiste en configurar el switch y ponerlo en funcionamiento. Trabajará después del horario laboral para minimizar los inconvenientes para la empresa.

Nota: esta actividad comienza con una puntuación de 8/100, debido a que ya se calificaron las conexiones de los dispositivos para las PC. En la parte 2, eliminará y restaurará estas conexiones. La puntuación se incluye para verificar que haya restaurado correctamente las conexiones.

Parte 1: Documentar la configuración actual de la red

Nota: por lo general, un router de producción tendría muchas más configuraciones que simplemente el direccionamiento IP de las interfaces. Sin embargo, para agilizar esta actividad, se configuró solo el direccionamiento IP de interfaces en **R1**.

a. Haga clic en **R1** y, a continuación, haga clic en la ficha **CLI**.

b. Utilice los comandos disponibles para recopilar información sobre el direccionamiento de interfaces.

Figura 19.

```
Router#show star
Using 1109 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Alice
!
!
!
!
!
ipv6 unicast-routing
    .
    license udi pid CISCO2911/K9 sn FTX152422VM
    !
    !
    !
    !
    !
    spanning-tree mode pvst
    !
    !
    !
    !
    interface GigabitEthernet0/0
     ip address 172.16.31.1 255.255.255.0
     duplex auto
     speed auto
     ipv6 address 2001:BA5:1C:ADD::1/64
     ipv6 eigrp 1
     ipv6 address autoconfig
    !
    interface GigabitEthernet0/1
     ip address 192.168.0.2 255.255.255.0
     duplex auto
     speed auto
     ipv6 address 2001:FED:E7E:BC::2/64
     ipv6 eigrp 1
    .
```

```
router eigrp 1
 passive-interface GigabitEthernet0/0
 network 172.16.31.0 0.0.0.255
 network 192.168.0.0
 auto-summary
!
ipv6 router eigrp 1
 router-id 192.168.0.2
 no shutdown
!
ip classless
!
!
!
no cdp run
```

Fuente propia

c. Registre la información en la **tabla de direccionamiento**.

Tabla 2.3

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/0	172.16.31.1	255.255.255.0
	G0/1	192.168.0.2	255.255.255.0
MLSw1	G0/1	192.168.0.2	255.255.255.0
	VLAN 1	172.16.31.1	255.255.255.0

Figura 19.4

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type
Interface
Internet  172.16.31.1            -   00E0.F7B1.8901  ARPA
GigabitEthernet0/0
Internet  192.168.0.2            -   00E0.F7B1.8902  ARPA
GigabitEthernet0/1
Router#
```

Fuente propia

Parte 2: Configurar, implementar y probar el nuevo switch multicapa

Paso 1: Configurar MLSw1 para utilizar el esquema de direccionamiento de R1

a. Haga clic en **MLSw1** y, a continuación, en la ficha **CLI**.

b. Ingrese al modo de configuración de interfaz para **GigabitEthernet 0/1**.

c. Cambie el puerto al modo de enrutamiento introduciendo el comando **no switchport**.

Figura 19.5

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#no switchport
Switch(config-if)#
```

Fuente propia

d. Configure la dirección IP para que sea la misma que la dirección de **R1 GigabitEthernet 0/1** y active el puerto.

Figura 19.6

```
Switch(config-if)#ip address 192.168.0.2 255.255.255.0
Switch(config-if)#no shutdown

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

Fuente propia

e. Ingrese al modo de configuración de interfaz para **interface VLAN1**.

f. Configure la dirección IP para que sea la misma que la dirección de **R1 GigabitEthernet 0/0** y active el puerto.

Figura 19.7

```
Switch#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 172.16.31.1 255.255.255.0
Switch(config-if)#no shutdown

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

Fuente propia

g. Guarde la configuración.

Figura19.8

```
Switch#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Fuente propia

Paso 2: Implementar el nuevo switch multicapa y verificar que la conectividad esté restaurada

Nota: por lo general, los siguientes pasos se llevarían a cabo después del horario laboral o cuando el tráfico en la red de producción está en su volumen más bajo. Para minimizar el tiempo de inactividad, el nuevo equipo debe estar totalmente configurado y listo para implementar.

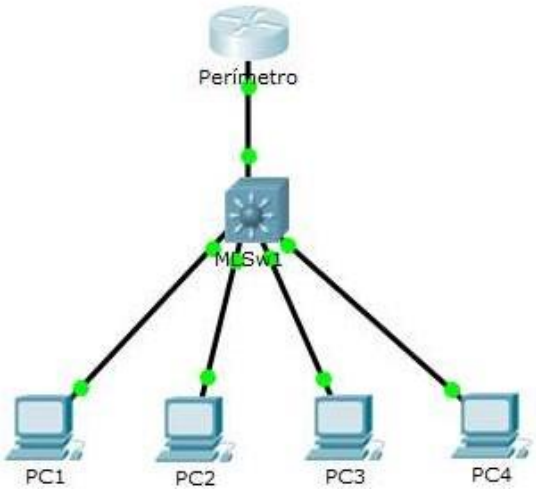
a. Haga clic en un área vacía de la pantalla para anular la selección de todos los dispositivos.

b. Use la herramienta **Delete** (Eliminar) para eliminar todas las conexiones o simplemente elimine **R1**, **S1** y **S2**.

c. Seleccione los cables adecuados para completar lo siguiente:

- Conectar **MLSw1 GigabitEthernet 0/1** a **Edge GigabitEthernet 0/0**.
- Conectar las PC a los puertos Fast Ethernet en **MLSw1**.

Figura 155

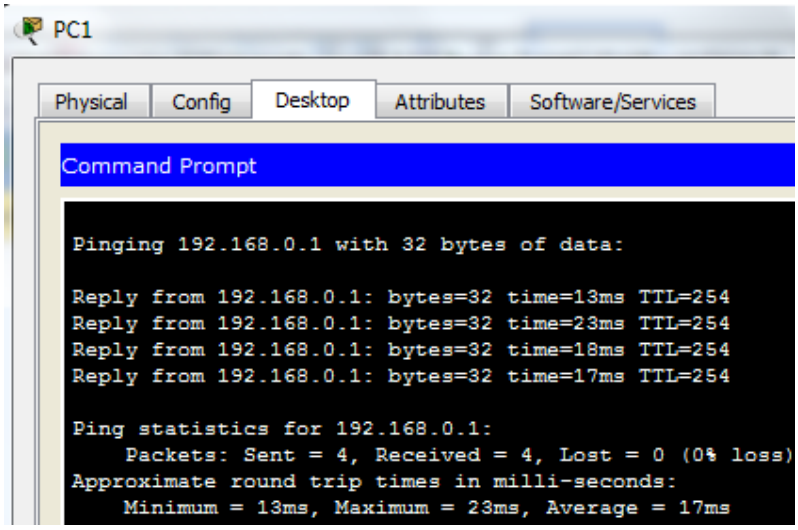


Fuente propia

d. Verifique que todas las PC puedan hacer ping a **Edge** en 192.168.0.1.

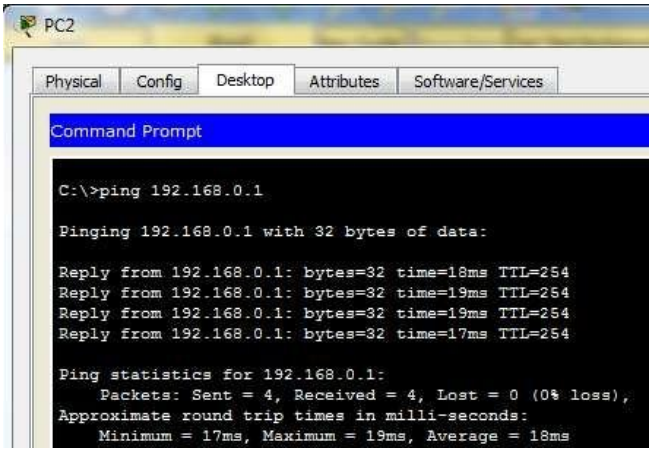
Nota: espere hasta que las luces de enlace anaranjadas cambien a color verde.

Figura 20.0



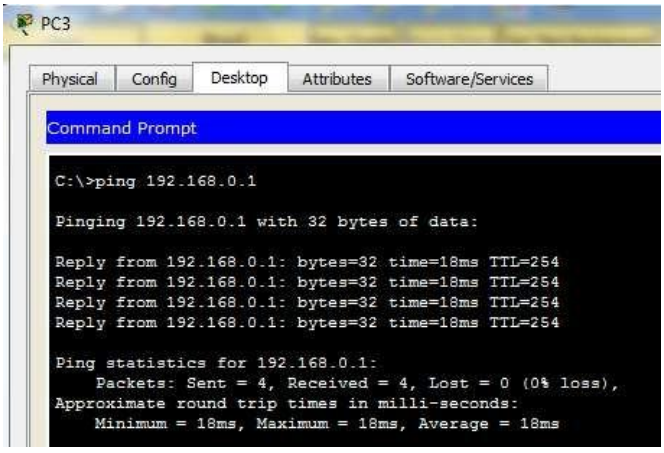
Fuente propia

Figura 156



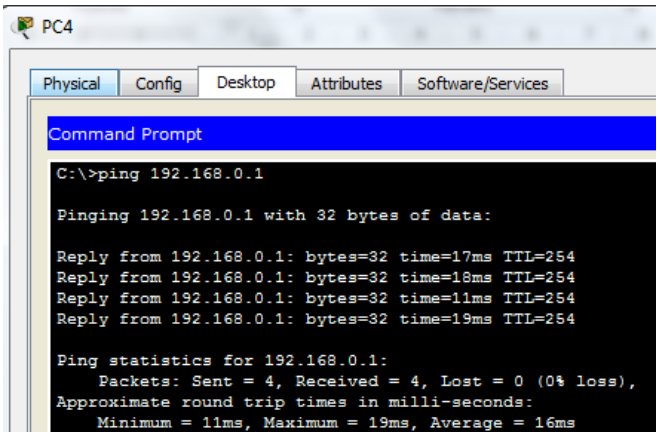
Fuente propia

Figura 20.2



Fuente propia

Figura 20.3



Fuente propia

- **Numeral 6.3.1.10**

Parte 1:Identificar las características físicas de los dispositivos de internetworking

Paso 1: Identificar los puertos de administración de un router Cisco

a. Haga clic en el router **East** (Este). La ficha **Physical** (Capa física) debe estar activa.

b. Acerque el elemento y expanda la ventana para ver todo el router.

c. ¿Qué puertos de administración se encuentran disponibles?

R/ Dos puertos, el auxilar y el de consola.

Figura 20.4

Fuente propia

Paso 2: Identificar las interfaces LAN y WAN de un router Cisco

a. ¿Qué interfaces LAN y WAN se encuentran disponibles en el router **East** y cuántas hay?

R/ Dos interfaces WAN GigabitEthernet y una interface LAN

Figura 20.5

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
```

Fuente propia

b. Haga clic en la ficha **CLI** e introduzca los siguientes comandos:

East> **show ip interface brief**

Figura 20.6

```
East#show ip interface bri
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            unassigned      YES unset  down
down
Serial0/0/1            unassigned      YES unset  down
down
Vlan1                  unassigned      YES unset
administratively down down
```

Fuente propia

El resultado verifica la cantidad correcta de interfaces y su designación. La interfaz vlan1 es una interfaz virtual que solo existe en el software. ¿Cuántas interfaces físicas se indican?

R/ 5 interfaces

c. Introduzca los siguientes comandos:

East> **show interface gigabitethernet 0/0**

Pregunta: ¿Cuál es el ancho de banda predeterminado de esta interfaz?

R/ El ancho de banda es de 1 Gigabit por segundo (Gbps)

East> **show interface serial 0/0/0**

Pregunta:¿Cuál es el ancho de banda predeterminado de esta interfaz?

R/ El ancho de banda es de 1544 kilobit por segundo (Kbps)

Nota: los procesos de enrutamiento usan el ancho de banda en las interfaces seriales para determinar el mejor camino hacia un destino. Esto no indica el ancho de banda real de la interfaz. El ancho de banda real se negocia con un proveedor de servicios.

Paso 3: Identificar las ranuras de expansión de módulos en los switches

a. ¿Cuántas ranuras de expansión se encuentran disponibles para agregar más módulos al router **East**?
R/Hay dos ranuras de expansión

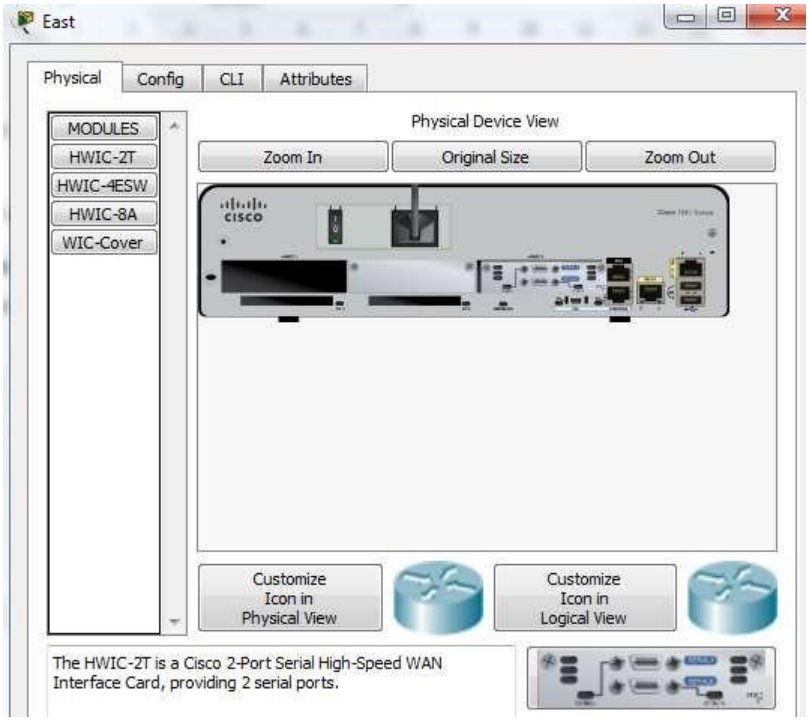
b. Haga clic en **Switch2** o **Switch3** .¿Cuántas ranuras de expansión están disponibles?
R/ Hay 5 ranuras de expansión

Parte 2: Seleccionar los módulos correctos para la conectividad

Paso 1: Determinar qué módulos proporcionan la conectividad requerida

a. Haga clic en **East** y, a continuación, haga clic en la ficha **Physical**. En el lado izquierdo, debajo de la etiqueta **Modules** (Módulos), se ven las opciones disponibles para expandir las capacidades del router. Haga clic en cada módulo. Se muestra una imagen y una descripción en la parte inferior. Familiarícese con estas opciones.

Figura 20.7



Fuente propia

Figura 161

The HWIC-4ESW provides four switching ports.

Fuente propia

Figura 20.9

The HWIC-8A provides up to eight asynchronous EIA-232 connections to console ports.

Fuente propia

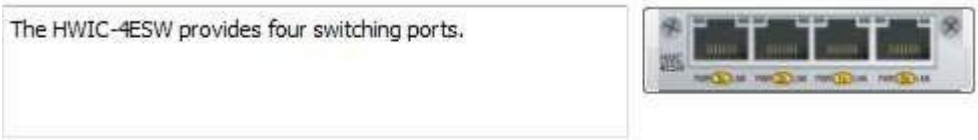
Figura 21.0

The WIC cover plate provides protection for the internal electronic components. It also helps maintain adequate cooling by normalizing airflow.

Fuente propia

1) Debe conectar las PC 1, 2 y 3 al router **East**, pero no cuenta con los fondos necesarios para adquirir un nuevo switch. ¿Qué módulo puede usar para conectar las tres PC al router **East**?
R/ El modulo HWIC-4ESW el cual expande a 4 puertos Ethernet

Figura 162



Fuente propia

Figura 21.2

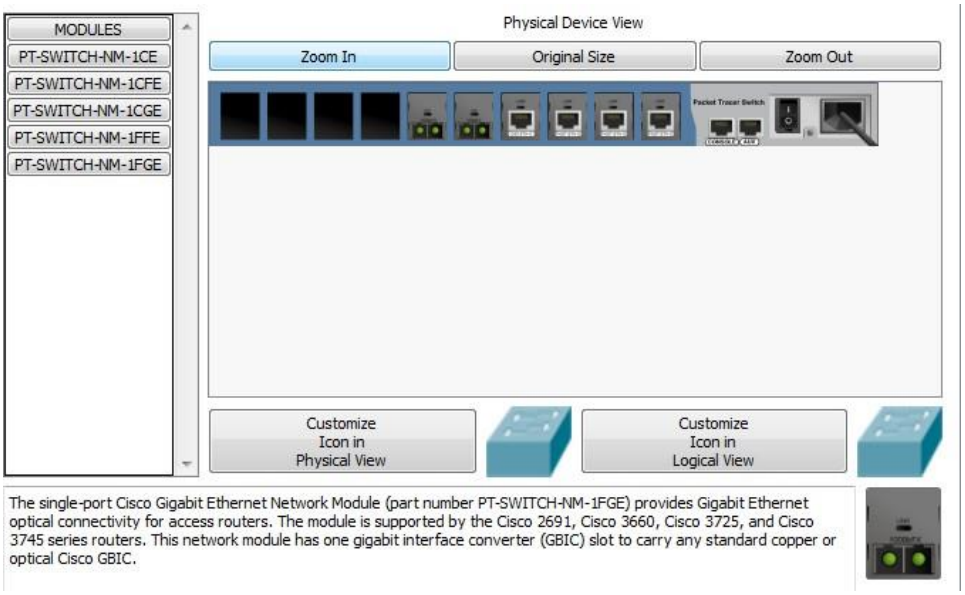
Fuente propia

2) ¿Cuántos hosts puede conectar al router mediante este módulo?

R/ 4 hosts

b. Haga clic en **Switch2**. ¿Qué módulo puede insertar para proporcionar una conexión óptica Gigabit al **Switch3**?

Figura 21.



Fuente propia

Paso 2: Agregar los módulos correctos y encender los dispositivos

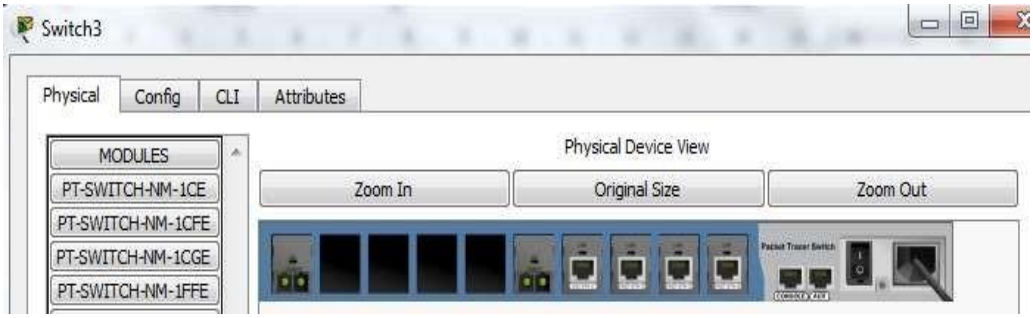
a. Haga clic en **East** e intente insertar el módulo adecuado del paso 1a.

b. Debe aparecer el mensaje Cannot add a module when the power is on (No se puede agregar un módulo cuando el dispositivo está encendido). Las interfaces para este modelo de router no son intercambiables en caliente. Se debe apagar el dispositivo. Haga clic en el interruptor de alimentación que se encuentra a la derecha del logotipo de Cisco para apagar **East**. Inserte el módulo adecuado del paso 1a. Cuando haya terminado, haga clic en el interruptor de alimentación para encender **East**.

   Nota: si inserta el módulo incorrecto y debe quitarlo, arrastre el módulo hasta su imagen en la esquina inferior derecha y suelte el botón del mouse.

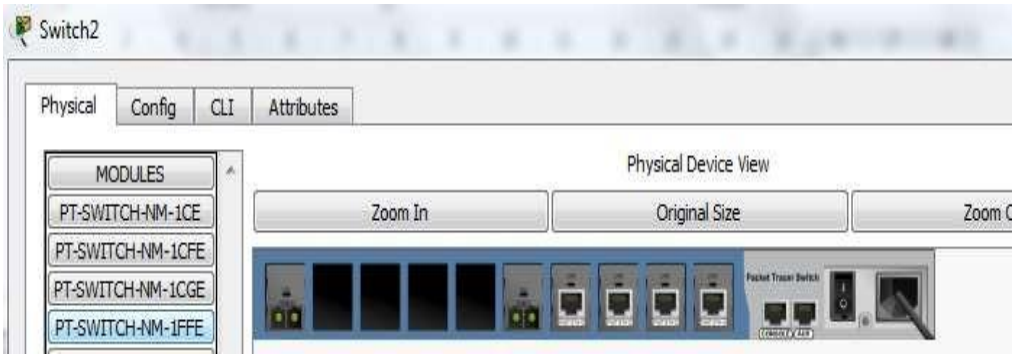
c. Mediante el mismo procedimiento, inserte los módulos correctos del paso 1b en la ranura vacía más alejada que se encuentra a la derecha en el **Switch2** y el **Switch3**.

Figura 21.



Fuente propia

Figura 21.5



Fuente propia

d. Use el comando **show ip interface brief** para identificar la ranura en la que se colocó el módulo.

¿En qué ranura se insertó?

R/ En la ranura 9/1

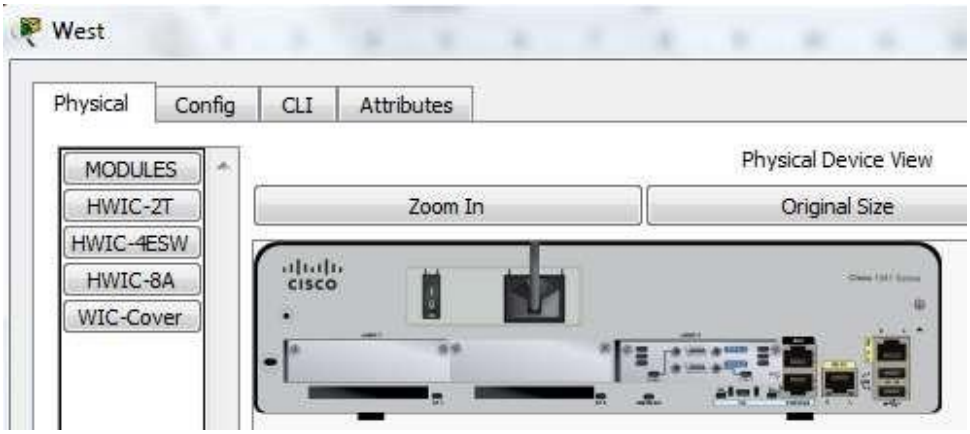
Figura 21.6

```
Switch>enable
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual down                  down
FastEthernet1/1        unassigned      YES manual down                  down
FastEthernet2/1        unassigned      YES manual down                  down
GigabitEthernet3/1     unassigned      YES manual down                  down
FastEthernet4/1        unassigned      YES manual down                  down
GigabitEthernet9/1     unassigned      YES manual down                  down
Vlan1                  unassigned      YES manual administratively down down
```

Fuente propia

d. Haga clic en el router **West** (Oeste). La ficha **Physical** (Capa física) debe estar activa. Instale el módulo adecuado que agregará una interfaz serial a la ranura para tarjetas de interfaz WAN de alta velocidad mejoradas (**EHWIC 0**) de la derecha. Puede cubrir las ranuras sin utilizar para evitar que ingrese polvo al router (optativo).

Figura 21.7



Fuente propia

e. Use el comando adecuado para verificar que se hayan instalado las nuevas interfaces seriales.

Figura 21.8

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

Fuente propia

Parte 3: Conectar los dispositivos

Esta puede ser la primera actividad que realiza en la que se le solicita conectar dispositivos. Si bien es posible que no conozca el propósito de los distintos tipos de cables, use la tabla que se encuentra a continuación y siga estas pautas para conectar correctamente todos los dispositivos:

a. Seleccione el tipo de cable adecuado.

b. Haga clic en el primer dispositivo y seleccione la interfaz especificada.

c. Haga clic en el segundo dispositivo y seleccione la interfaz especificada.

d. Si conectó correctamente los dos dispositivos, verá que su puntuación aumenta.

Ejemplo: para conectar **East** al **Switch1**, seleccione el tipo de cable de **cobre de conexión directa**. Haga clic en **East** y elija **GigabitEthernet0/0**. Luego, haga clic en **Switch1** y elija **GigabitEthernet0/1**. Su puntuación ahora debe ser de 4/52.

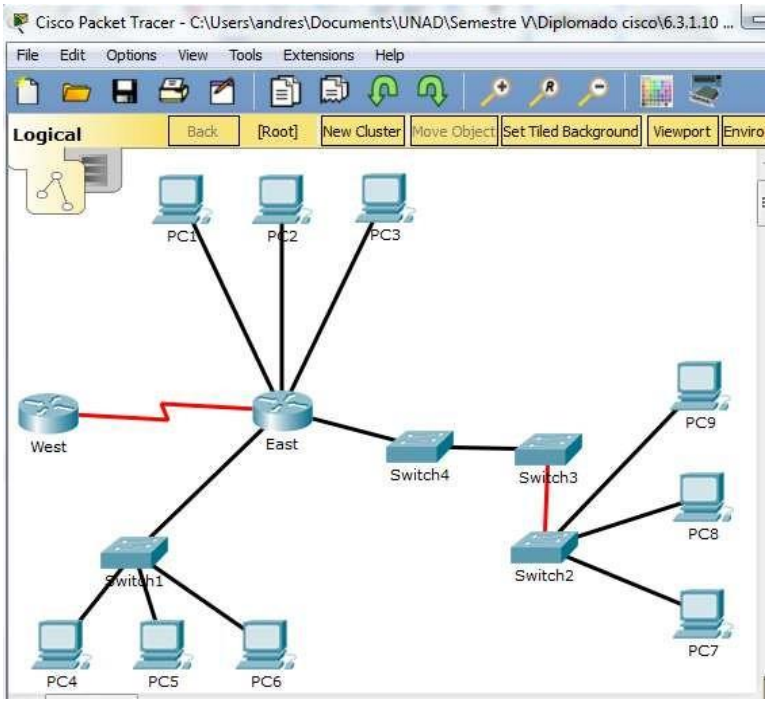
Nota: a los efectos de esta actividad, se deshabilitaron las luces de enlace. Los dispositivos no están configurados con ningún direccionamiento IP, de modo que no puede probar la conectividad.

Tabla 2.4

Dispositivo	Interfaz	Tipo de cable	Dispositivo	Interfaz
East	GigabitEthernet0/0	Cable de cobre de conexión directa	Switch1	GigabitEthernet0/1
East	GigabitEthernet0/1	Cable de cobre de conexión directa	Switch4	GigabitEthernet0/1
East	FastEthernet0/1/0	Cable de cobre de conexión directa	PC1	FastEthernet0
East	FastEthernet0/1/1	Cable de cobre de conexión directa	PC2	FastEthernet0
East	FastEthernet0/1/2	Cable de cobre de conexión directa	PC3	FastEthernet0
Switch1	FastEthernet0/1	Cable de cobre de conexión directa	PC4	FastEthernet0
Switch1	FastEthernet0/2	Cable de cobre de conexión directa	PC5	FastEthernet0
Switch1	FastEthernet0/3	Cable de cobre de conexión directa	PC6	FastEthernet0

Switch4	GigabitEthernet0/2	Cross-Over de cobre	Switch3	GigabitEthernet3/1
Switch3	GigabitEthernet5/1	Fibra	Switch2	GigabitEthernet5/1
Switch2	FastEthernet0/1	Cable de cobre de conexión directa	PC7	FastEthernet0
Switch2	FastEthernet1/1	Cable de cobre de conexión directa	PC8	FastEthernet0
Switch2	FastEthernet2/1	Cable de cobre de conexión directa	PC9	FastEthernet0
East	Serial0/0/0	DCE serial (conectar primero a East)	West	Serial0/0/0

Figura 169



Fuente propia

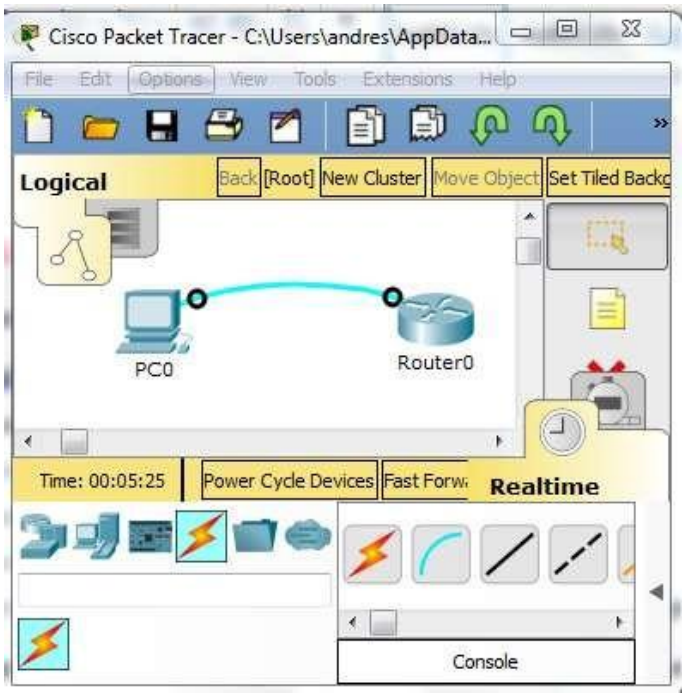
- **Numeral 6.4.1.2**

Parte 1: Verificar la configuración predeterminada del router

Paso 1: Establecer una conexión de consola al R1.

a. Elija un cable de **consola** de las conexiones disponibles.
b. Haga clic en **PCA** y seleccione **RS 232**.
c. Haga clic en **R1** y seleccione **Console** (Consola).

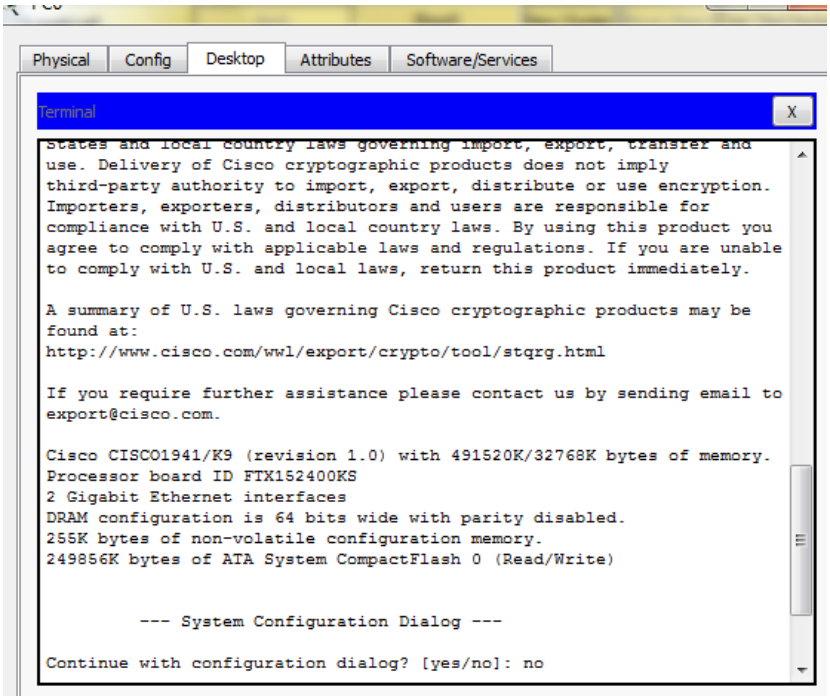
Figura 170



Fuente propia

d. Haga clic en **PCA** > ficha **Desktop** (Escritorio) > **Terminal**.
e. Haga clic en **OK** (Aceptar) y presione **Entrar**. Ahora puede configurar **R1**.

Figura 22.



Fuente propia

Paso 2: Ingresar al modo privilegiado y examinar la configuración actual

Puede acceder a todos los comandos del router en el modo EXEC privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado.

a. Ingrese al modo EXEC privilegiado introduciendo el comando **enable** .

Router> **enable**

Router#

Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

b. Introduzca el comando **show running-config**:

Router# **show running-config**

Figura 22.

```
Router>enable
Router#show running-config
Building configuration...

Current configuration : 607 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX15243989
!
         spanning-tree mode pvst
         !
```

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet0/1/0
 switchport mode access
!
interface FastEthernet0/1/1
 switchport mode access
!
interface FastEthernet0/1/2
 switchport mode access
!
interface FastEthernet0/1/3
 switchport mode access
!
      line con 0
      !
      line aux 0
      !
      line vty 0 4
       login
      !
      !
      !
      end
```

Fuente propia

c. Responda las siguientes preguntas:

¿Cuál es el nombre de host del router?

R/ Router

¿Cuántas interfaces Fast Ethernet tiene el router?

R/ 4 interface

¿Cuántas interfaces Gigabit Ethernet tiene el router?

R/ 2 interfaces

¿Cuántas interfaces seriales tiene el router?

R/ 2 interfaces

¿Cuál es el rango de valores que se muestra para las líneas vty?

R/ 0 a 4

d. Muestre el contenido actual de la NVRAM.

Router# **show startup-config**
startup-config is not present

Figura 22.3

```
Router#
Router#
Router#show startup-config
startup-config is not present
Router#
```

Fuente propia

Pregunta: ¿Por qué el router responde con el mensaje startup-config is not present?

R/Por que no hay una configuración guardada en la memoria ram volatil

Parte 2: Configurar y verificar la configuración inicial del router

Para configurar los parámetros de un router, quizá deba pasar por diversos modos de configuración. Observe cómo cambia la petición de entrada mientras navega por el router.

Paso 1: Configurar los parámetros iniciales de R1.

Nota: si tiene dificultad para recordar los comandos, consulte el contenido de este tema. Los comandos son los mismos que configuró en un switch.

a. Establezca **R1** como nombre de host.

Figura 22.4

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

Fuente propia

b. Utilice las siguientes contraseñas:

1) Consola: **letmein**

Figura 22.5

```
R1(config)#line console 0
R1(config-line)#password letmein
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Fuente propia

2) EXEC privilegiado, sin encriptar: **cisco**

Figura 22.6

```
R1(config)#enable password cisco
```

Fuente propia

3) EXEC privilegiado, encriptado: **itsasecret**

Figura 176

```
R1(config)#enable secret itsasecret
```

Fuente propia

b. Encripte todas las contraseñas de texto no cifrado.

Figura 22.8

```
R1(config)#service password-encryption
```

Fuente propia

c. Texto del mensaje del día: Unauthorized access is strictly prohibited (El acceso no autorizado queda terminantemente prohibido).

Figura 22.9

```
R1(config)#banner motd "Unathorized access is strictly prohibited (El acceso no autorizado queda
terminantemente prohibido"
```

Fuente propia

Paso 2: Verificar los parámetros iniciales de R1.

a. Para verificar los parámetros iniciales, observe la configuración de R1. ¿Qué comando utiliza?

Figura 177

```
R1#show star
Using 1186 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 0822455D0A16
```

Fuente propia

b. Salga de la sesión de consola actual hasta que vea el siguiente mensaje:

R1 con0 is now available
Press RETURN to get started.

Figura 23.1

```
Unathorized access is strictly prohibited (El acceso no autorizado queda terminantemente prohibido

User Access Verification

Password:
```

Fuente propia

c. Presione **Entrar**; debería ver el siguiente mensaje:

Unauthorized access is strictly prohibited.
User Access Verification
Password:

¿Por qué todos los routers deben tener un mensaje del día (MOTD)?

R/ Para informar a los usuarios sobre las restricciones del sistema. Tambien podría servir para dar consejos o informar sobre las novedades.

Si no se le pide una contraseña, ¿qué comando de la línea de consola se olvidó de configurar?

Figura 23.2

```
R1(config)#line console 0
R1(config-line)#password letmein
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Fuente propia

d. Introduzca las contraseñas necesarias para regresar al modo EXEC privilegiado.

Figura 23.3

```
R1>enable
Password:
Password:
Password:
R1#
```

Fuente propia

¿Por qué la contraseña **secreta de enable** permitiría el acceso al modo EXEC privilegiado y **la contraseña de enable** dejaría de ser válida?

R/ Si configura más contraseñas en el router, ¿se muestran como texto no cifrado o en forma encriptada en el archivo de configuración? Explique.

Parte 3: Guardar el archivo de configuración en ejecución

Paso 1: Guarde el archivo de configuración en la NVRAM.

a. Configuró los parámetros iniciales de **R1**. Ahora realice una copia de seguridad del archivo de configuración en ejecución en la NVRAM para garantizar que no se pierdan los cambios realizados si el sistema se reinicia o se apaga.

¿Qué comando introdujo para guardar la configuración en la NVRAM?

R/ copy running-config startup-config

Pregunta: ¿Cuál es la versión más corta e inequívoca de este comando?

R/copy run star

¿Qué comando muestra el contenido de la NVRAM?

Figura 23.4

```
R1#show startup-config
Using 1186 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 0822455D0A16
!
no ip cef
no ipv6 cef
!
license udi pid CISCO1941/K9 sn FTX15243989
!
spanning-tree mode pvst
```

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet0/1/0
 switchport mode access
!
interface FastEthernet0/1/1
 switchport mode access
!
interface FastEthernet0/1/2
 switchport mode access
!
interface FastEthernet0/1/3
 switchport mode access
!
interface Vlan1
 no ip address

 ip classless
 !
 ip flow-export version 9
 !
```

```
banner motd ^CUnathorized access is strictly prohibited (El acceso
prohibido^C
!
!
!
!
line con 0
 password 7 082D495A041C0C19
 login
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Fuente propia

b. Verifique que todos los parámetros configurados estén registrados. Si no fuera así, analice el resultado y determine qué comandos no se introdujeron o se introdujeron incorrectamente. También puede hacer clic en **Check Results** (Verificar resultados) en la ventana de instrucción.

Paso 2: Puntos extra optativos: guarde el archivo de configuración de inicio en la memoria flash.

Aunque aprenderá más sobre la administración del almacenamiento flash de un router en los siguientes capítulos, le puede interesar saber ahora que puede guardar el archivo de configuración de inicio en la memoria flash como procedimiento de respaldo adicional. De manera predeterminada, el router seguirá cargando la configuración de inicio desde la NVRAM, pero si esta se daña, puede restablecer la configuración de inicio copiándola de la memoria flash.

Complete los siguientes pasos para guardar la configuración de inicio en la memoria flash.

a. Examine el contenido de la memoria flash mediante el comando **show flash**:

R1# **show flash**

Figura 23.5

```
R1#show flash

System flash directory:
File  Length   Name/status
  3   33591768 c1900-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)
```

Fuente propia

¿Cuántos archivos hay almacenados actualmente en la memoria flash?

R/ 3 archivos

¿Cuál de estos archivos cree que es la imagen de IOS?

Figura 23.6

```
3   33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
```

Fuente propia

¿Por qué cree que este archivo es la imagen de IOS?

R/ Porque es el archivo de mas peso.

b. Utilice los siguientes comandos para guardar el archivo de configuración de inicio en la memoria flash:

R1# **copy startup-config flash**

Destination filename [startup-config]

Figura 23.7

```
R1#copy startup-config flash
Destination filename [startup-config]?

1186 bytes copied in 0.416 secs (2850 bytes/sec)
R1#
```

Fuente propia

El router le pide que almacene el archivo en la memoria flash con el nombre entre corchetes. Si la respuesta es afirmativa, presione **Entrar**; de lo contrario, escriba un nombre adecuado y presione la tecla**Entrar**.

b. Utilice el comando **show flash** para verificar que el archivo de configuración de inicio esté almacenado en la memoria flash.

Figura 23.8

```
R1#show flash

System flash directory:
File  Length   Name/status
  3   33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
  4   1186     startup-config
[33848773 bytes used, 221895227 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

Fuente propia

- **Numeral 6.4.3.3**

Parte 1: Mostrar la información del router

Paso 1: Mostrar la información de la interfaz en el R1.

Nota: haga clic en un dispositivo y, a continuación, en la ficha **CLI** para acceder a la línea de comandos directamente. La contraseña de consola es **cisco**. La contraseña de EXEC privilegiado es **class**.

a. ¿Qué comando muestra las estadísticas para todas las interfaces configuradas en el router?

Figura 23.9

```
R1>enable
Password:
R1#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     unassigned      YES unset
administratively down down
GigabitEthernet0/1     unassigned      YES unset
administratively down down
Serial0/0/0            209.165.200.225 YES manual up
up
Serial0/0/1            unassigned      YES unset
administratively down down
FastEthernet0/1/0      unassigned      YES unset  up
down
FastEthernet0/1/1      unassigned      YES unset  up
down
FastEthernet0/1/2      unassigned      YES unset  up
down
FastEthernet0/1/3      unassigned      YES unset  up
down
Vlan1                  unassigned      YES unset
administratively down down
```

Fuente propia

b. ¿Qué comando muestra solo la información de la interfaz Serial 0/0/0?

Figura 24.0

```
R1#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 209.165.200.225/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 104 bits/sec, 0 packets/sec
  5 minute output rate 106 bits/sec, 0 packets/sec
     172 packets input, 10280 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
     175 packets output, 10436 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Fuente propia

c. Introduzca el comando para visualizar las estadísticas de la interfaz Serial 0/0/0 en el R1 y responda las siguientes preguntas:

   1) ¿Cuál es la dirección IP configurada en el **R1**?

Figura 24.1

R/ `Internet address is 209.165.200.225/30`

Fuente propia

2) ¿Cuál es el ancho de banda en la interfaz Serial 0/0/0?

Figura 24.2

R/ BW 1544 Kbit,

Fuente propia

d. Introduzca el comando para visualizar las estadísticas de la interfaz GigabitEthernet 0/0 y responda las siguientespreguntas:

1) ¿Cuál es la dirección IP en el **R1**?

R/ No muestra la dirección IP

2) ¿Cuál es la dirección MAC de la interfaz GigabitEthernet 0/0?

Figura 24.3

R/ Hardware is CN Gigabit Ethernet, address is 000d.bd6c.7d01 (bia 000d.bd6c.7d01)

Fuente propia

3) ¿Cuál es el ancho de banda en la interfaz GigabitEthernet 0/0?

Figura 24.4

R/ BW 1000000 Kbit

Fuente propia

Paso 2: Mostrar una lista de resumen de las interfaces en el R1

a. ¿Qué comando muestra un breve resumen de las interfaces, los estados y las direcciones IP actualmente asignadas a ellas?

Figura 24.

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     unassigned      YES unset
administratively down down
GigabitEthernet0/1     unassigned      YES unset
administratively down down
Serial0/0/0            209.165.200.225 YES manual up
up
Serial0/0/1            unassigned      YES unset
administratively down down
FastEthernet0/1/0      unassigned      YES unset  up
down
FastEthernet0/1/1      unassigned      YES unset  up
down
FastEthernet0/1/2      unassigned      YES unset  up
down
FastEthernet0/1/3      unassigned      YES unset  up
down
Vlan1                  unassigned      YES unset
administratively down down
```

Fuente propia

b. Introduzca el comando en cada router y responda las siguientes preguntas:

1) ¿Cuántas interfaces seriales hay en **R1** y **R2**?

R/ En R1 hay una interface serial y en R2 hay 2

2) ¿Cuántas interfaces Ethernet hay en **R1** y **R2**?

R/En R1 hay 4 interfaces Ethernet y en R2 no hay interfaces Ethernet.

3) ¿Son iguales todas las interfaces Ethernet en el **R1**? Si no es así, explique las ***diferencias.***

R/ No lo son. Hay dos interfaces Gigabit Ethernet y cuatro interfaces Fast Ethernet. Las interfaces Gigabit Ethernet admiten velocidades de hasta 1 000 000 000 bits, y las interfaces Fast Ethernet admiten velocidades de hasta 1 000 000 bits.

Paso 3: Mostrar la tabla de enrutamiento en el R1.

a. ¿Qué comando muestra el contenido de la tabla de enrutamiento?

b. Introduzca el comando en el **R1** y responda las siguientes preguntas:

Figura 24.

```
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 -
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       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
```

Fuente propia

1) ¿Cuántas rutas conectadas hay (utilizan el código C)?
R/ Hay una sola ruta conectada en la interfaz serial 0/0
2) ¿Qué ruta se indica?

Figura 24.7

R/ `C       209.165.200.224/30 is directly connected, Serial0/0/0`

Fuente propia

1) ¿Cómo administra el router un paquete destinado a una red que no se incluye en la tabla de enrutamiento?

R/ Cuando el router no tiene ruta para el destino de un paquete, directamente lo va a descartar

Parte2: Configurar las interfaces del router

Paso 1: Configurar la interfaz GigabitEthernet 0/0 en el R1

a. Introduzca los siguientes comandos direccionar y activar la interfaz GigabitEthernet 0/0 en el **R1**:

R1(config)# **interface gigabitethernet 0/0**

R1(config-if)# **ip address 192.168.10.1 255.255.255.0**

R1(config-if)# **no shutdown**

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

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

Figura 24.8

```
R1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
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
```

Fuente propia

b. Es aconsejable configurar una descripción en cada interfaz para ayudar a registrar la información de la red. Configure una descripción de la interfaz que indique a qué dispositivo está conectada.

R1(config-if)# **description LAN connection to S1**

c. Ahora, el **R1** debe poder hacer ping a la PC1.

R1(config-if)# **end**

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

R1# **ping 192.168.10.10**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms

Figura 24.9

```
R1#ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/7/11
ms
```

Fuente propia

Paso 2: Configure las interfaces Gigabit Ethernet restantes en R1 y R2.

Tabla 2.5

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No aplicable
	G0/1	192.168.11.1	255.255.255.0	No aplicable
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	No aplicable
R2	G0/0	10.1.1.1	255.255.255.0	No aplicable
	G0/1	10.1.2.1	255.255.255.0	No aplicable
	S0/0/0	209.165.200.226	255.255.255.252	No aplicable
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1

a. Utilice la información en la tabla de direccionamiento para finalizar la configuración de **R1** y **R2**. Para cada interfaz, realice lo siguiente:

1) Introduzca la dirección IP y active la interfaz.
2) Configure una descripción apropiada.

Configuracion R1

Figura 25.0

```
R1#config termi
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/1
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)#no shutdown

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

R1(config-if)#description LAN conection to S2
R1(config-if)#exit

   R1(config-if)#ip address 209.165.200.225 255.255.255.252
   R1(config-if)#description LAN conection to R2
   R1(config-if)#no shutdown
   R1(config-if)#exit
```

Fuente propia

Configuracion R2

Figura 25.1

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.252
R2(config-if)#description LAN conection to R1
R2(config-if)#exit

  R2(config-if)#interface serial 0/0/0
  R2(config-if)#no shutdown
  R2(config-if)#exit
```

```
R2(config)#interface g0/0
R2(config-if)#ip address  10.1.1.1 255.255.255.0
R2(config-if)#description LAN conection to S3
R2(config-if)#no shutdown

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

 R2(config)#interface g0/1
 R2(config-if)#ip address 10.1.2.1 255.255.255.0
 R2(config-if)#description LAN conection to S4
 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
```

Fuente propia

b. Verifique las configuraciones de las interfaces.

Figura 25.2

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     192.168.10.1    YES manual up
up
GigabitEthernet0/1     192.168.11.1    YES manual up
up
Serial0/0/0            209.165.200.225 YES manual up
up
```

Fuente propia

Figura 25.3

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     10.1.1.1        YES manual up
up
GigabitEthernet0/1     10.1.2.1        YES manual up
up
Serial0/0/0            209.165.200.226 YES manual up
up
```

Fuente propia

Paso 3: Realizar una copia de seguridad de las configuraciones en la NVRAM.

Guarde los archivos de configuración de ambos routers en la NVRAM. ¿Qué comando utilizó?

Figura 25.4

```
R1>enable
Password:
R1#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]

R2#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

Fuente propia

Parte3: Verificar la configuración

Paso 1: Utilizar los comandos de verificación para revisar la configuración de la interfaz

a. Utilice el comando **show ip interface brief** en **R1** y **R2** para verificar rápidamente que las interfaces estén configuradas con la dirección IP correcta y estén activas.

¿Cuántas interfaces en **R1** y **R2** están configuradas con direcciones IP y tienen el estado “up/up” (activa/activa)?

R/ Cada Router tiene 3 interfaces configuradas con direcciones IP y están activas.

¿Qué parte de la configuración de la interfaz NO se muestra en el resultado del comando?

R/ No se muestra la mascara de subred

¿Qué comandos puede utilizar para verificar esta parte de la configuración?

R/ show run, show interfaces, show ip protocols

c. Utilice el comando **show ip route** en **R1** y **R2** para ver las tablas de enrutamiento actuales y responda las siguientes preguntas:

Figura 25.5

```
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 -
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

D    10.0.0.0/8 [90/2170112] via 209.165.200.226, 00:24:16,
Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 3 subnets, 3 masks
D       209.165.200.0/24 is a summary, 01:04:07, Null0
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
```

```
R2#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

     10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D       10.0.0.0/8 is a summary, 00:25:36, Null0
C       10.1.1.0/24 is directly connected, GigabitEthernet0/0
L       10.1.1.1/32 is directly connected, GigabitEthernet0/0
C       10.1.2.0/24 is directly connected, GigabitEthernet0/1
L       10.1.2.1/32 is directly connected, GigabitEthernet0/1
D    192.168.10.0/24 [90/2170112] via 209.165.200.225, 01:05:20,
Serial0/0/0
D    192.168.11.0/24 [90/2170112] via 209.165.200.225, 00:53:17,
Serial0/0/0
     209.165.200.0/24 is variably subnetted, 3 subnets, 3 masks
D       209.165.200.0/24 is a summary, 00:25:36, Null0
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.226/32 is directly connected, Serial0/0/0
```

Fuente propia

1) ¿Cuántas rutas conectadas (utilizan el código **C**) ve en cada router?

R/ 3 rutas

2) ¿Cuántas rutas EIGRP (utilizan el código D) ve en cada router?

R/ 4 rutas

3) Si el router conoce todas las rutas en la red, la cantidad de rutas conectadas y de rutas descubiertas dinámicamente (EIGRP) debe ser igual a la cantidad total de LAN y WAN. ¿Cuántas LAN y WAN hay en la topología?

R/ 5 rutas en total por cada router.

4) ¿Esta cantidad coincide con la cantidad de rutas C y D que se muestran en la tabla de enrutamiento?

R/ Si coincide

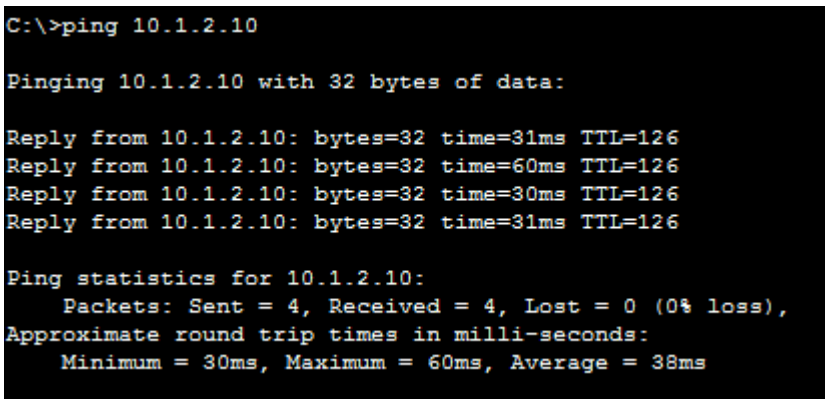
Nota: si su respuesta es “no”, falta una configuración necesaria. Revise los pasos de la parte 2.

Paso 2: Probar la conectividad de extremo a extremo a través de la red

Ahora debería poder hacer ping desde cualquier PC a cualquier otra PC en la red. Además, debería poder hacer ping a las interfaces activas de los routers. Por ejemplo, las siguientes pruebas deberían realizarse correctamente:

Desde la línea de comandos en la PC1, haga ping a la PC4.

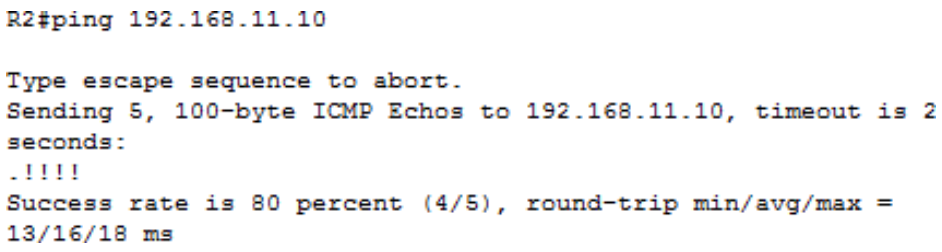
Figura 25.6



Fuente propia

Desde la línea de comandos en el R2, haga ping a la PC2.

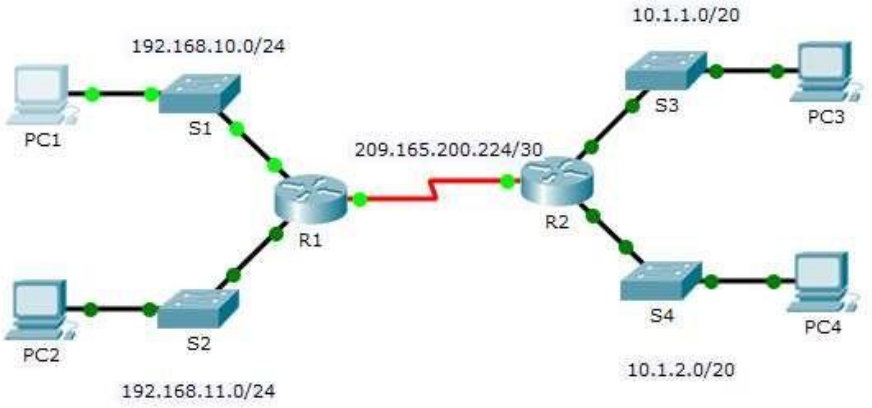
Figura 25.7



Fuente propia

Nota: para simplificar esta actividad, los switches no están configurados, por lo que podrá hacerles ping.

Figura 25.8



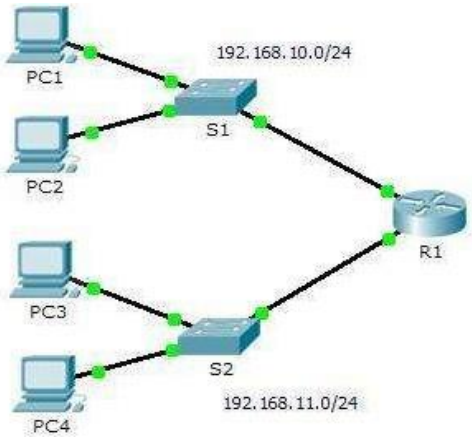
Fuente propia

- **Numeral 6.4.3.4**

Packet Tracer: Resolución de problemas del gateway predeterminado

Topología:

Figura 25.9



Fuente propia

Tabla 2.6. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No aplicable
	G0/1	192.168.11.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.10.2	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.11.2	255.255.255.0	192.168.11.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC3	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC4	NIC	192.168.11.11	255.255.255.0	192.168.11.1

Información básica:

Para que un dispositivo se comunique a través de varias redes, debe estar configurado con una dirección IP, una máscara de subred y un gateway predeterminado. El gateway predeterminado se utiliza cuando el host desea enviar un paquete a un dispositivo en otra red. Por lo general, la dirección de gateway predeterminado es la dirección de la interfaz del router asociada a la red local a la que el host está conectado. En esta actividad,

terminará de documentar la red. A continuación, verificará la documentación de la red mediante la puesta a prueba de la conectividad de extremo a extremo y la resolución de problemas. El método de resolución de problemas que utilizará consta de los siguientes pasos:

a. Verificar la documentación de la red y utilizar pruebas para descartar problemas.

b. Determinar cuál es la solución adecuada para un problema dado.

c. Implementar la solución.

d. Realizar pruebas para verificar que se haya resuelto el problema.

e. Documentar la solución.

A lo largo de sus estudios de CCNA, encontrará distintas descripciones del método de resolución de problemas, así como distintas formas de probar y documentar problemas y soluciones. Esto es intencional. No existe un estándar o una plantilla establecida para la resolución de problemas. Cada organización desarrolla procesos y estándares de documentación exclusivos (incluso si ese proceso consiste en no tener ninguno). No obstante, todas las metodologías de resolución de problemas eficaces generalmente incluyen los pasos anteriores.

Nota: si usted es experto en la configuración de gateway predeterminado, es posible que esta actividad parezca más compleja de lo debido. Lo más probable es que pueda descubrir y solucionar todos los problemas de conectividad más rápido que si siguiera estos procedimientos. No obstante, a medida que avance con sus estudios, las redes y los problemas que encuentre serán cada vez más complejos. En tales situaciones, la única forma eficaz de descartar y resolver problemas es aplicar un enfoque metódico como el que se usa en esta actividad.

Parte 1: Verificar el registro de la red y descartar problemas

En la parte 1 de esta actividad, completará la documentación y realizará pruebas de conectividad para detectar problemas. Además, determinará la solución adecuada y la implementará en la parte 2.

Paso 1: Verificar el registro de la red y descartar cualquier problema

a. Para que pueda probar una red con eficacia, debe contar con la documentación completa. Observe que falta determinada información en la **tabla de**

direccionamiento. Complete la **tabla de direccionamiento** con la información de gateway predeterminado que falta para los switches y las PC.

b. Pruebe la conectividad a los dispositivos en la misma red. Al descartar y corregir cualquier problema de acceso local, puede probar mejor la conectividad remota, con la seguridad de que la conectividad local está en funcionamiento.

Un plan de verificación puede ser tan simple como una lista de pruebas de conectividad. Use las siguientes pruebas para verificar la conectividad local y descartar cualquier problema de acceso.

El primer problema ya se documentó, pero debe implementar y verificar la solución durante la parte 2.

Tabla 2.7. Documentación de prueba y verificación

Prueba	¿Se realizó Correctamente?	Problemas	Solución	Verificado
PC1 a PC2	**No**	**Dirección IP en la PC1**	**Cambiar la dirección IP de la PC1**	ok
PC1 a S1	**No**	**Dirección IP en la PC1**	**Cambiar la dirección IP de la PC1**	**ok**
PC1 a R1	**No**	**Dirección IP en la PC1**	**Cambiar la dirección IP de la PC1**	**ok**
PC1 a S2	**No**	**Dirección IP en la PC1**	**Cambiar la dirección IP de la PC1**	**ok**
PC1 a PC3	**No**	**Dirección IP en la PC1**	**Cambiar la dirección IP de la PC1**	**ok**

PC1 a PC4	**No**	**Dirección IP en la PC1**	**Cambiar la dirección IP de la PC1**	**ok**
PC2 a S1	**Si**			
PC2 a R1	**Si**			
PC2 a S2	**No**	**Sin dirección IP en S2**	**Configurar dirección IP en S2**	**ok**
PC2 a PC3	**Si**			
PC2 a PC4	**No**	**PC4 con dirección Gateway errónea**	**Configurar Gateway en PC4**	**ok**
PC3 a S2	**No**	**Sin dirección IP en S2**	**Configurar dirección IP en S2**	**ok**
PC3 a R1	**Si**			
PC3 a S1	**No**	**S1 sin configurar Gateway**	**Configurar en S1 el Gateway**	**ok**
PC3 a PC1	**No**	**PC1 con dirección IP errada**	**Cambiar la dirección IP en PC1**	**ok**
PC3 a PC2	**Si**			
PC3 a PC4	**Si**			
PC4 a S2	**No**	**Sin dirección IP en S2**	**Configurar dirección IP en S2**	**ok**
PC4 a R1	**Si**			
PC4 a S1	**No**	**Configuración Gateway PC4 erroneo**	**Cambiar la dirección IP del Gateway en S4**	**ok**
PC4 a PC1	**No**	**PC1 con dirección IP errada**	**Cambiar la dirección IP en PC1**	**ok**
PC4 a PC2		**Configuración Gateway PC4 erroneo**	**Cambiar la dirección IP del Gateway en S4**	**ok**

Nota: esta tabla es un ejemplo; debe crear su propio documento. Puede usar lápiz y papel para dibujar una tabla, o puede utilizar un editor de texto o una hoja de cálculo. Consulte al instructor si necesita más orientación.

a. Pruebe la conectividad a los dispositivos remotos (p. ej., de la PC1 a la PC4) y documente cualquier problema. Esto se conoce frecuentemente como *conectividad de extremo a extremo*. Esto significa que la política de red permite que todos los todos los dispositivos en una red tengan conectividad total.

Nota: es posible que aún no se pueda realizar la prueba de conectividad remota, dado que primero debe resolver los problemas de conectividad local. Una vez que solucione dichos problemas, vuelva a este paso y pruebe la conectividad entre redes.

Paso 2: Determinar cuál es la solución adecuada para el problema

d. Con sus conocimientos sobre la forma en que operan las redes y sus aptitudes para configurar dispositivos, busque la causa del problema. Por ejemplo, el S1 no es la causa del problema de conectividad entre la PC1 y la PC2. Las luces de enlace son de color verde, y ninguna configuración en el S1 provocaría que no pase el tráfico entre la PC1 y la PC2. Por lo tanto, el problema debe de estar en la PC1, en la PC2 o en ambas.

e. Verifique el direccionamiento del dispositivo para asegurarse de que coincida con el registro de la red. Por ejemplo, la dirección IP para la PC1 es incorrecta, como se verificó con el comando **ipconfig**.

f. Sugiera una solución con la que usted crea que se resolverá el problema y documéntela. Por ejemplo, cambiar la dirección IP de la PC1 para que coincida con la documentación.

Nota: por lo general, hay más de una solución. Sin embargo, una práctica recomendada de resolución de problemas es implementar de a una solución por vez. Implementar más de una solución podría presentar problemas adicionales en una situación más compleja.

Parte 2: Implementar, verificar y documentar las soluciones

En la parte 2 de esta actividad, implementará las soluciones que identificó en la parte 1. Luego, verificará si la solución funcionó. Es posible que deba volver a la parte 1 para terminar de descartar todos los problemas.

Paso 1: Implementar soluciones para abordar los problemas de conectividad

Consulte la documentación en la parte 1. Elija el primer problema e implemente la solución que sugirió. Por ejemplo, corrija la dirección IP en la PC1.

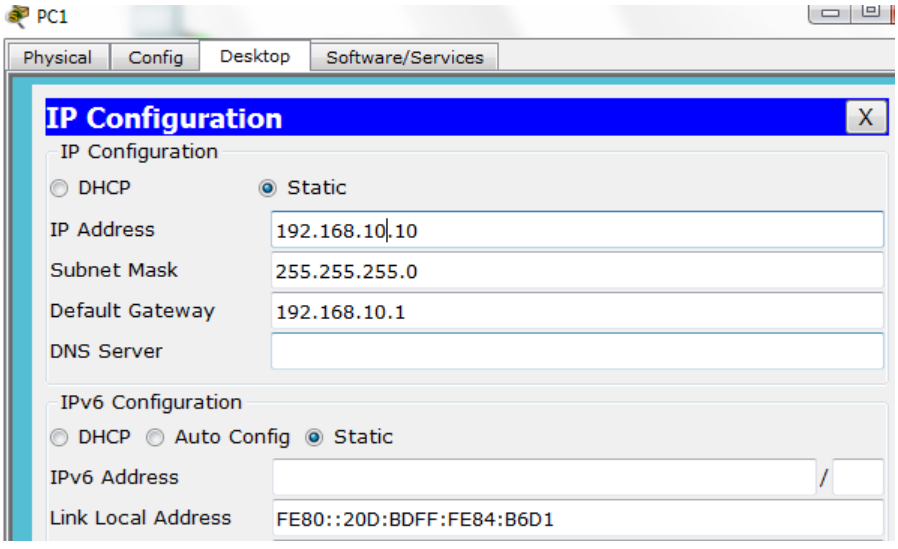
Dirección IP errada en PC1 según la tabla la dirección debe ser 192.168.10.10, se realiza cambio en la configuración de la PC1.

Figura 26.0

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::20D:BDFF:FE84:B6D1
   IP Address.....: 192.168.11.10
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.10.1
```

Fuente propia

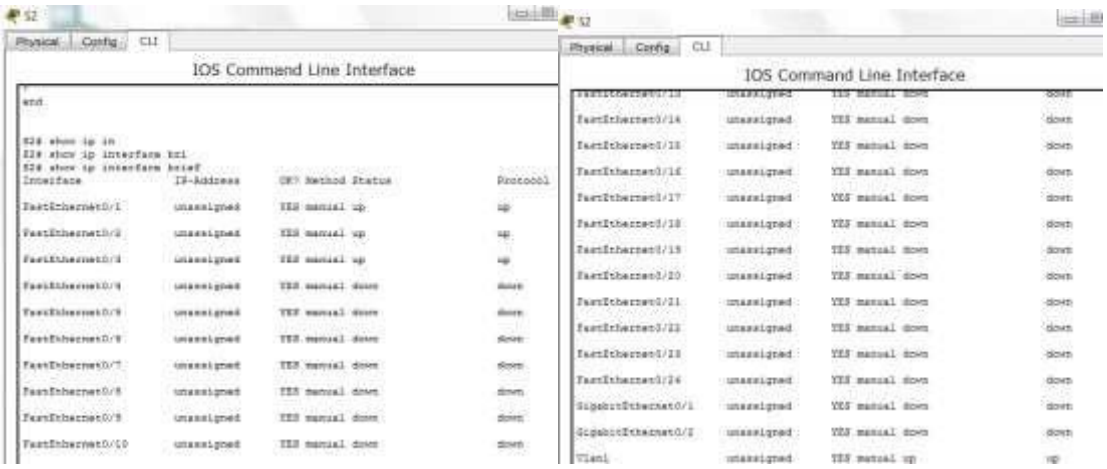
Figura 26.1



Fuente propia

Se revisa la configuración de S2 y se ajusta de acuerdo a la tabla de direcciones VLAN.

Figura 26.2



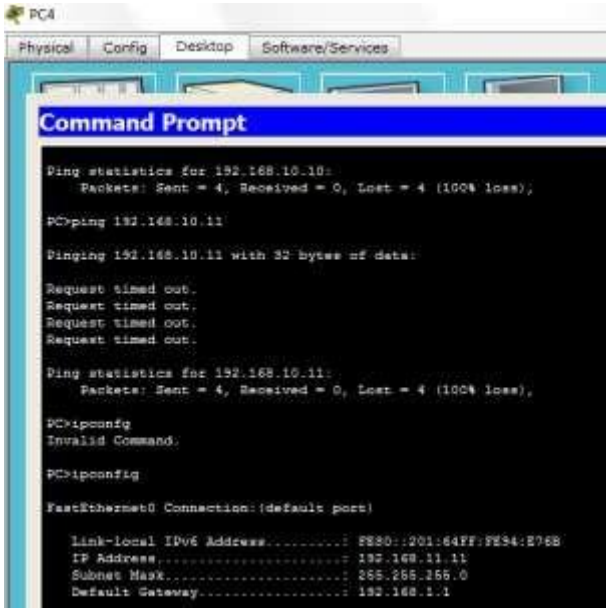
Fuente propia

Figura 26.3

Fuente propia

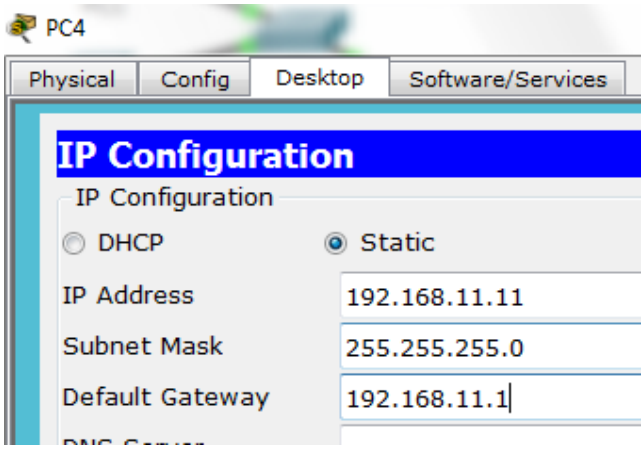
Se revisa el Gateway de la PC4 y se ajusta de acuerdo a la tabla de direcciones.

Figura 26.4



Fuente propia

Figura 26.5



Fuente propia

Se configura el Gateway de S1

Figura 26.6

Fuente propia

Paso 2: Verificar si ahora el problema está resuelto

h. Verifique si la solución que propuso solucionó el problema realizando la prueba que usó para identificarlo. Por ejemplo, ¿la PC1 puede ahora hacer ping a la PC2?

i. Si el problema se resolvió, indíquelo en la documentación. Por ejemplo, en la tabla anterior, con colocar una simple marca de verificación en la columna “Verificado” sería suficiente.

Paso 3: Verificar si se resolvieron todos los problemas

j. Si todavía tiene un problema pendiente con una solución que aún no se implementó, vuelva al paso 1 de la parte 2.

k. Si se solucionaron todos los problemas actuales, ¿también solucionó todos los problemas de conectividad remota (por ejemplo, que la PC1 pueda hacer ping a la PC4)? Si la respuesta es negativa, vuelva al paso 1c de la parte 1 para probar la conectividad remota.

Problemas:

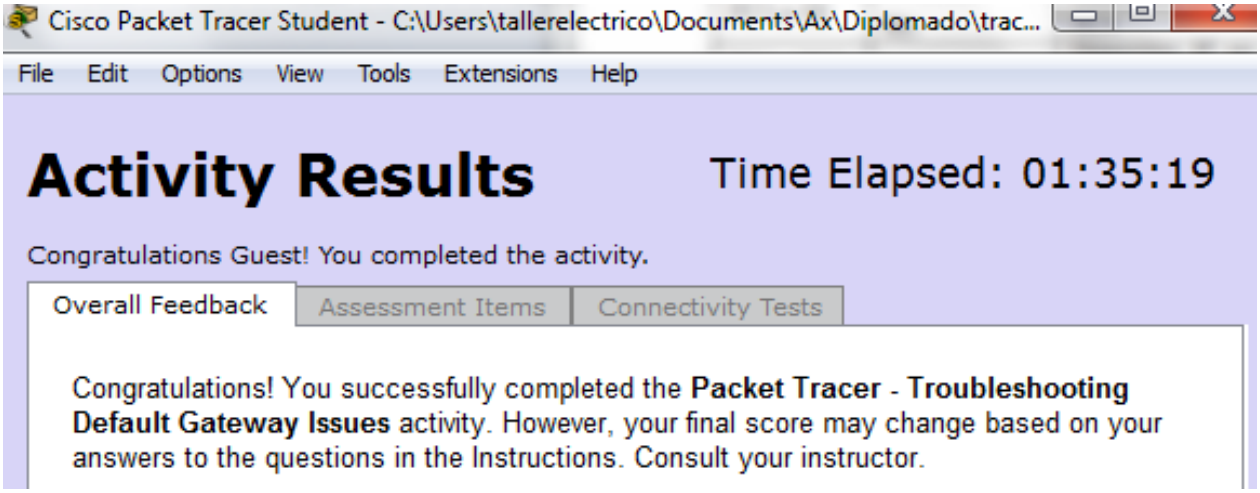
l. La PC1 no puede hacer ping a la PC2, porque la PC1 tiene una dirección IP que no pertenece a la red a la que está conectada.

m. Los dispositivos no pueden hacer ping al S2, y el S2 no puede hacer ping a ningún dispositivo porque le falta una dirección IP.

n. Los dispositivos remotos no pueden hacer ping a la PC4, porque la PC4 tiene configurado un gateway predeterminado incorrecto.

o. Los dispositivos remotos no pueden hacer ping al S1, porque le falta la configuración de gateway predeterminado.

Figura 26.7



Fuente propia

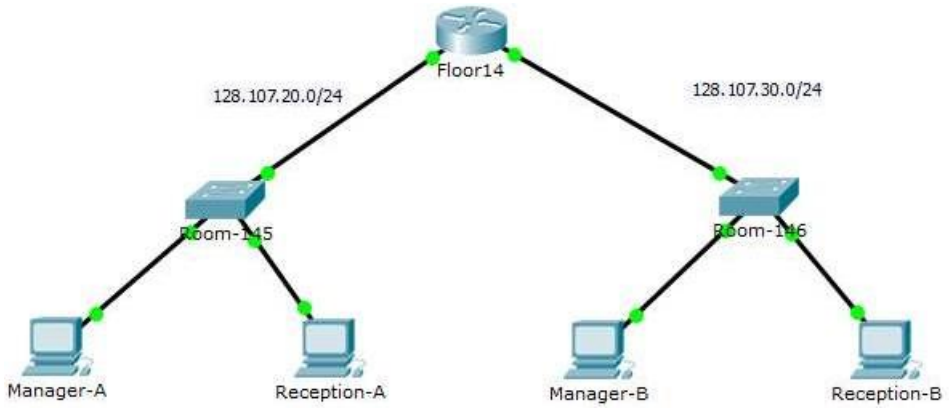
- **Numeral 6.5.1.2**

Packet Tracer: Reto de habilidades de integración

Topología:

Recibirá una de tres topologías posibles.

Figura 26.8



Fuente propia

Tabla 2.8. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Floor14	G0/0	128.107.20.1	255.255.255.0	No aplicable
	G0/1	128.107.30.1	255.255.255.0	No aplicable
Room-145	VLAN 1	128.107.20.10	255.255.255.0	128.107.20.1
Room-146	VLAN 1	128.107.30.15	255.255.255.0	128.107.30.1
Manager-A	NIC	128.107.20.25	255.255.255.0	128.107.20.1
Reception-A	NIC	128.107.20.30	255.255.255.0	128.107.20.1
Manager-B	NIC	128.107.30.25	255.255.255.0	128.107.30.1
Reception-B	NIC	128.107.30.30	255.255.255.0	128.107.30.1

Situación

La administradora de la red está muy conforme con su desempeño en el trabajo como técnico de LAN. Ahora, a ella le gustaría que demuestre su capacidad para configurar un router que conecta dos redes LAN. Las tareas incluyen la configuración básica de un router y un switch utilizando Cisco IOS. Luego, verificará la configuración realizada por usted, así como la configuración de los dispositivos existentes, probando la conectividad de extremo a extremo.

Nota: después de completar esta actividad, puede elegir hacer clic en el botón **Reset Activity** (Restablecer actividad) para generar un nuevo conjunto de requisitos. Entre los aspectos variables se incluyen los nombres de dispositivo, los esquemas de direccionamiento IP y la topología.

Requisitos:

- Proporcione la información que falta en la tabla de direccionamiento.
- Asigne el nombre **Floor14** al router y **Room-146** al segundo switch. No podrá acceder a **Room-145**.
- Utilice **cisco** como contraseña de EXEC del usuario para todas las líneas.
- Utilice **class** como contraseña de EXEC privilegiado.
- Encripte todas las contraseñas de texto no cifrado.
- Configure un aviso apropiado.
- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
- Registre las interfaces con descripciones, incluida la interfaz VLAN 1 de **Room-146**.
- Guarde las configuraciones.
- Verifique la conectividad entre todos los dispositivos. Todos los dispositivos deben poder hacerse ping entre sí.
- Resuelva cualquier problema y regístrelo.
- Implemente las soluciones necesarias para habilitar y verificar la completa conectividad de extremo a extremo.

Nota: haga clic en el botón **Check Results** (Revisar resultados) para ver su progreso. Haga clic en el botón clic en el botón **Reset Activity** para generar un nuevo conjunto de requisitos.

ID: 100

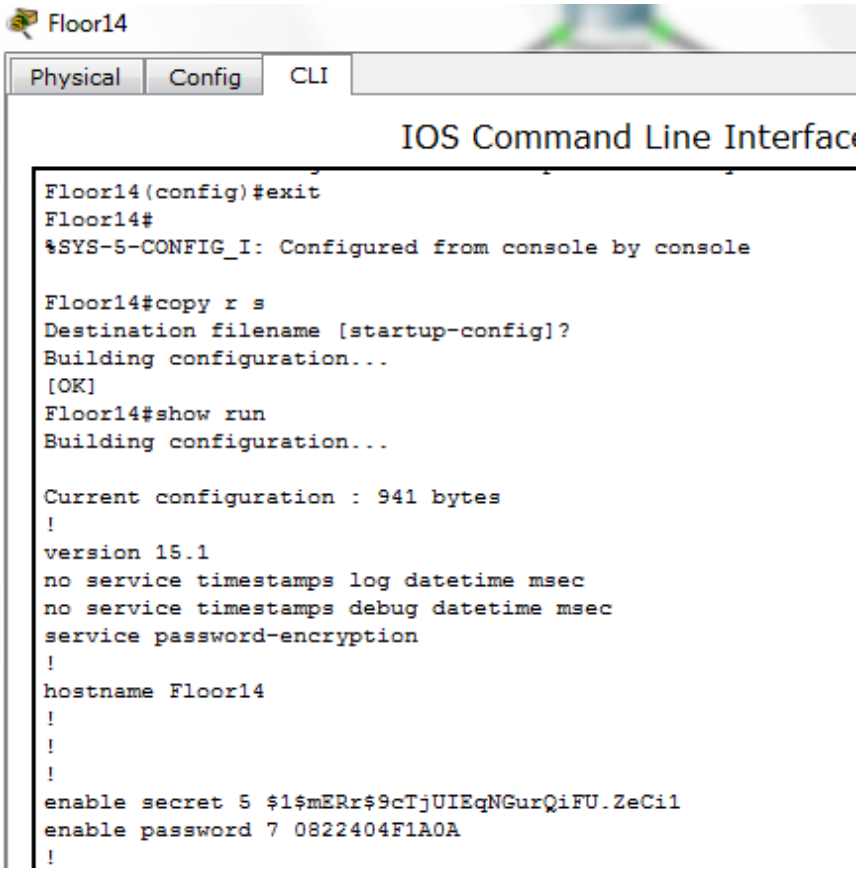
Configuración Floor14

Figura 210

```
Floor14#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     128.107.20.1    YES manual up                    up

GigabitEthernet0/1     128.107.30.1    YES manual up                    up

Vlan1                  unassigned      YES unset  administratively down down
```

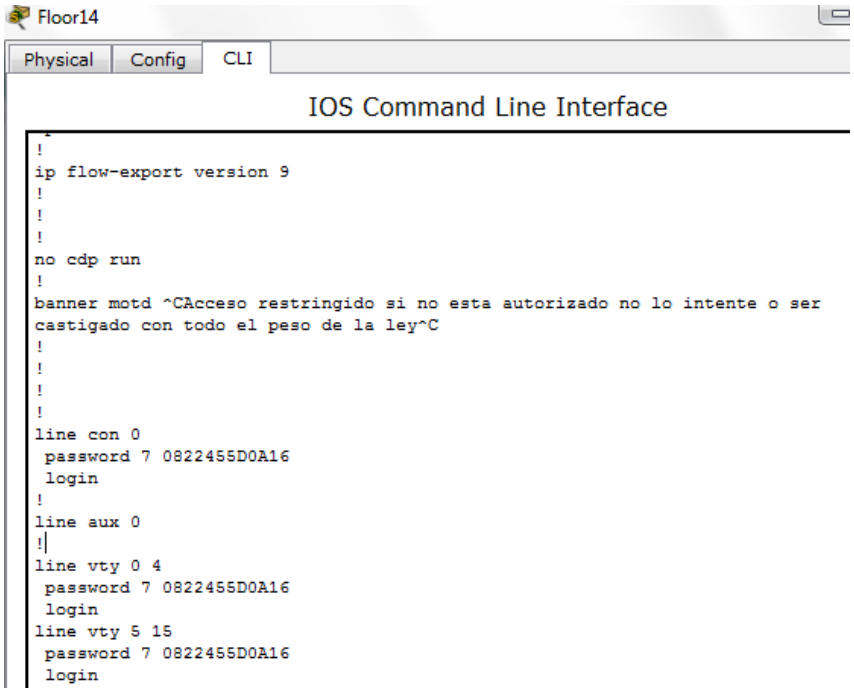
Fuente propia

Figura 27.0



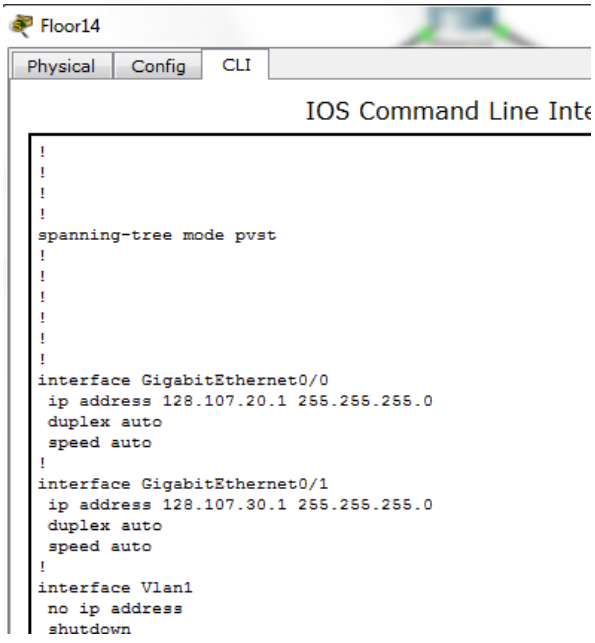
Fuente propia

Figura 211



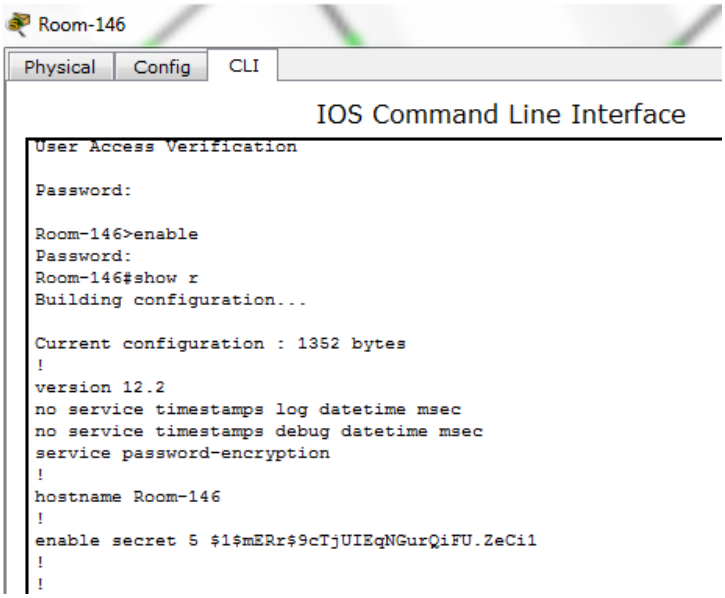
Fuente propia

Figura 27.2



Fuente propia

Configuración Room-146
Figura 27.3



Fuente propia

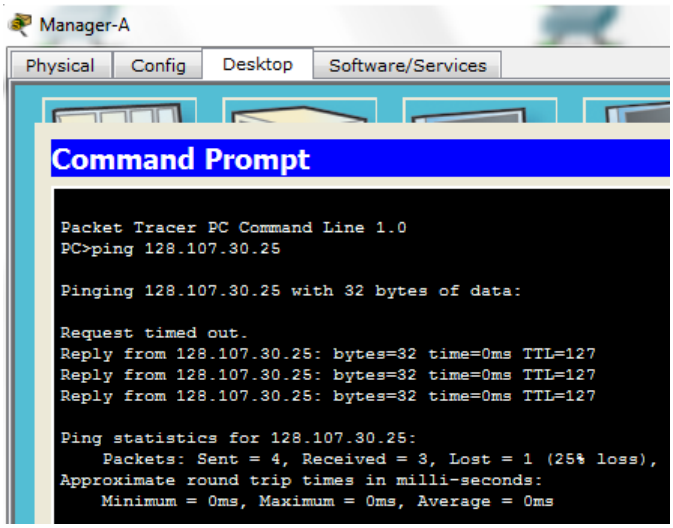
Figura 27.4

Fuente propia

Pruebas de conectividad

Ping Manager-A a Reception-B

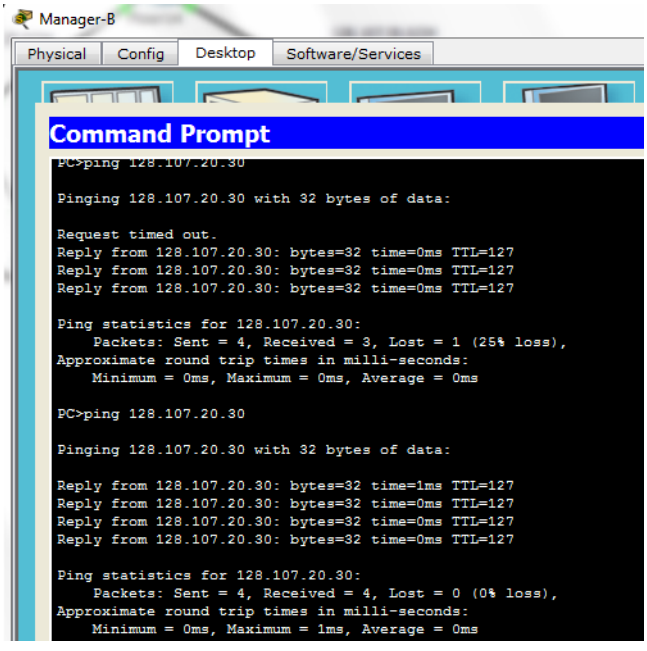
Figura 27.5



Fuente propia

Ping desde Manager-B a Reception-A

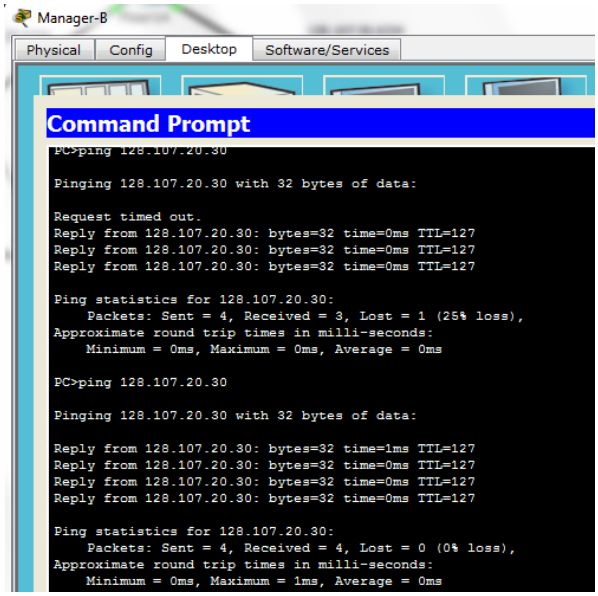
Figura 27.6



Fuente propia

Ping de Manager-A a Floor14

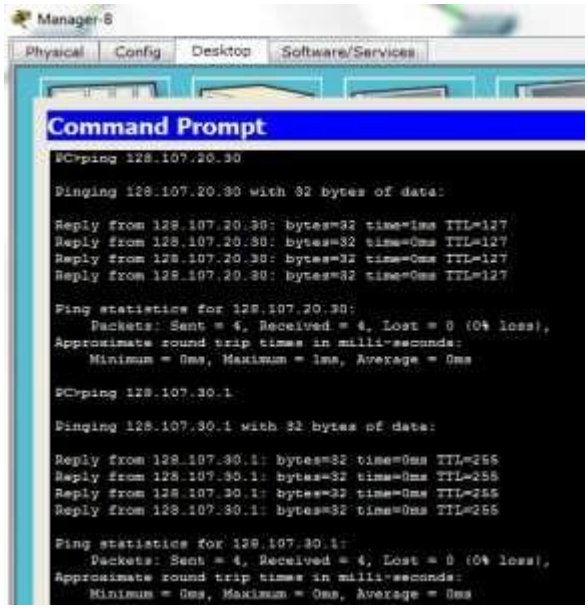
Figura 27.7



Fuente propia

Ping de Manager-B a Floor14

Figura 27.8



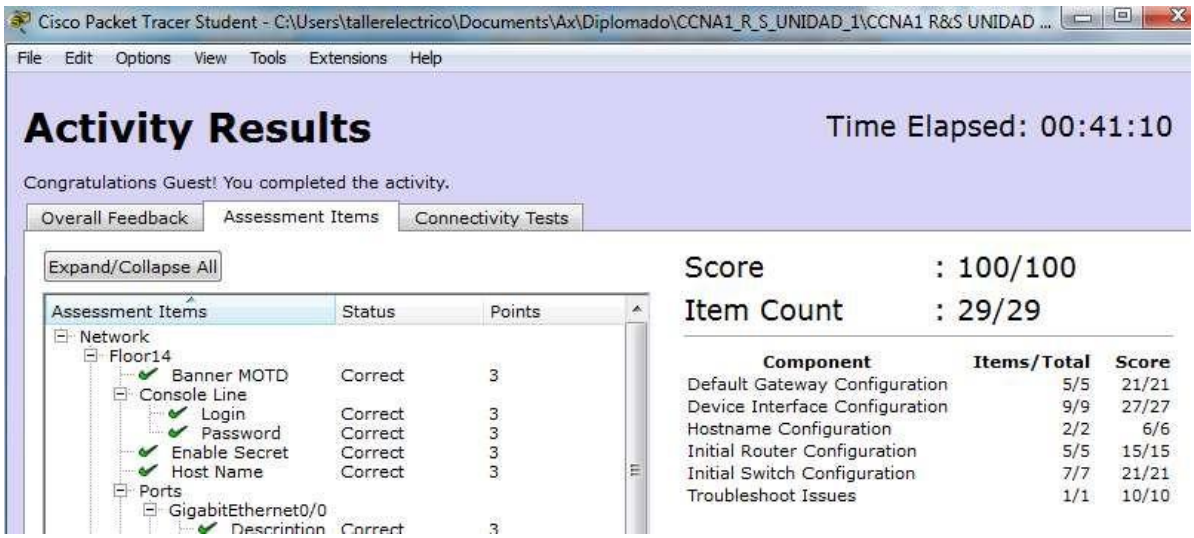
Fuente propia

Nota: haga clic en el botón **Check Results** (Revisar resultados) para ver su progreso. Haga clic en el botón clic en el botón **Reset Activity** para generar un nuevo conjunto de requisitos.

ID: [[indexNames]][[indexAdds]][[indexTopos]]

Esta actividad está configurada con un error que el estudiante deberá corregir para obtener la mayor puntuación. La dirección IP en [[PC4Name]] está en la subred incorrecta y no coincide con la dirección IP en la tabla de direccionamiento. Las respuestas correctas dependen de la situación que el alumno recibió para trabajar. La contraseña para acceder al asistente de la actividad es **PT_ccna5**.

Figura 27.9



Fuente propia

CONCLUSIONES

- Se realiza identificación de los dispositivos básicos LAN, con su respectiva configuración, se ejecuta la gestión de una red de datos con la utilización de la herramienta Packet Tracer.

- Con la elaboración de este trabajo podemos ver la importancia de las ACL que son las listas de control de acceso y que pueden ser aplicadas en un router para poder controlar el tráfico de información dentro de una red de un lugar a otro (permitir, denegar o bloquear un servicio) de acuerdo con los requerimientos del sistema.

- Con el protocolo DCHP se logra la configuración de los hots, además el servidor DHCPv4 tiene la facultad de asignar y administrar direcciones IPv4 vinculadas a VLAN específicas. Se puede realizar el swicheo con el modelo 2960 el cual funciona como dispositivo de capa 3 que permite trabajar el routing y rutas estáticas de igual forma únicas y múltiples esta última para permitir una comunicación constante entre los hosts de la red a trabajar.

- Se logra con la ejecución de las prácticas del trabajo comprender cómo se transmiten los datos a través de los medios físicos de transmisión como medios guiados y no guiados, identificando cuales se deben utilizar en un caso determinado, y aplicándolos gracias a la explicación de los manuales de Cisco.

BIBLIOGRAFÍA

CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de https://staticcourse-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course- assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de https://staticcourseassets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de: https://cdn2.hubspot.net/hub/280690/file270025813-pdf//ICND1.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf