

PRACTICAS DE LABORATORIOS INFORME FINAL DE LA UNIDAD 1
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN / WAN)

ELABORADO POR
EUNICE YULIETH PAEZ
NIRIO RAMON AMAYA
MARGARITA GUERRERO
LUZ AIDA FARELO
HENRY LANDINEZ

Grupo:
203092_26

TUTOR
NILSON ALBEIRO FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
INGENIERIA DE TELECOMUNICACIONES

INTRODUCCION

Dentro del desarrollo de la temática tratada en la unidad 1 y en cada uno de sus capítulos se evidencian y tratan diferentes técnicas de las cuales permitirán garantizar la conexión en los diferentes escenarios que puedan presentarse en el ambiente real dentro de la plataforma de redes de datos, dentro de los ejercicios realizados se afianzan conocimientos sobre: Exploración de la red, Configuración de un sistema operativo de red, Protocolos y comunicaciones de red, Acceso a la red, Ethernet y Capa de red.

Topología



Objetivos

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

Parte 2: Exploración de los modos EXEC

Parte 3: Configuración del comando clock

Información básica

En esta actividad, practicará las habilidades necesarias para navegar Cisco IOS, incluidos distintos modos de acceso de usuario, diversos modos de configuración y comandos comunes que utiliza habitualmente. También practicará el acceso a la ayuda contextual mediante la configuración del comando **clock**.

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.

- Haga clic en el ícono **Connections** (Conexiones), similar a un rayo, en la esquina inferior izquierda de la ventana de Packet Tracer.
- 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.
- Haga clic en **PC1**. Aparece una ventana que muestra una opción para una conexión RS-232.
- Arrastre el otro extremo de la conexión de consola al switch S1 y haga clic en el switch para abrir la lista de conexiones.
- Seleccione el puerto de consola para completar la conexión.



Paso 2: Establezca una sesión de terminal con el S1.

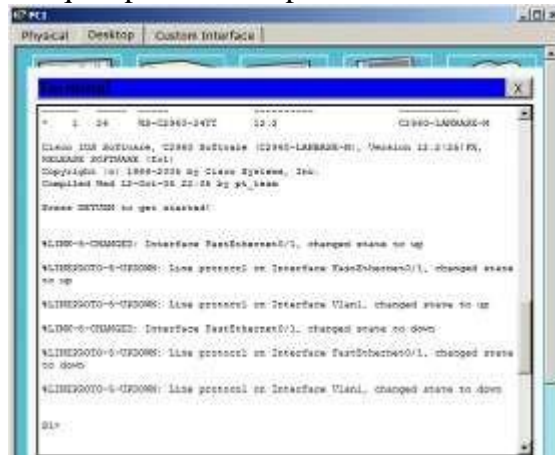
- a. Haga clic en **PC1** y después en la ficha **Desktop** (Escritorio).



- b. Haga clic en el ícono de la aplicación **Terminal**. Verifique que la configuración predeterminada de Port Configuration (Configuración del puerto) sea la correcta. ¿Cuál es el parámetro de bits por segundo? **9600**



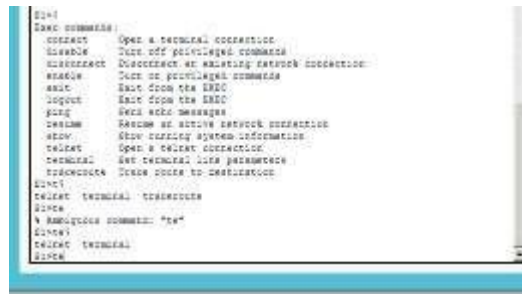
- c. Haga clic en **OK** (Aceptar).
- d. La pantalla que aparece puede mostrar varios mensajes. En alguna parte de la pantalla tiene que haber un mensaje que diga Press RETURN to get started! (Presione REGRESAR para comenzar). Presione **Entrar**.
¿Cuál es la petición de entrada que aparece en la pantalla? **S1**



Paso 3: Examine 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> ?

¿Qué comando comienza con la letra “C”? **CONECTAR**



- b. En la petición de entrada, escriba **t**, seguido de un signo de interrogación (?).
S1> t?

¿Qué comandos se muestran? **telnet terminal traceroute**

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

`“te”` no proporciona suficientes caracteres para formar un comando único; por lo tanto, los caracteres continuarán apareciendo, y se le solicitará al usuario que introduzca más caracteres para formar el comando único. Hay más de un comando que comienza con las letras `“te”`.

c. Introduzca el comando `enable` y presione tecla **Entrar**. ¿En qué cambia la petición de entrada? `Cambia de S1> a S1#, que indica el modo EXEC privilegiado.`

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

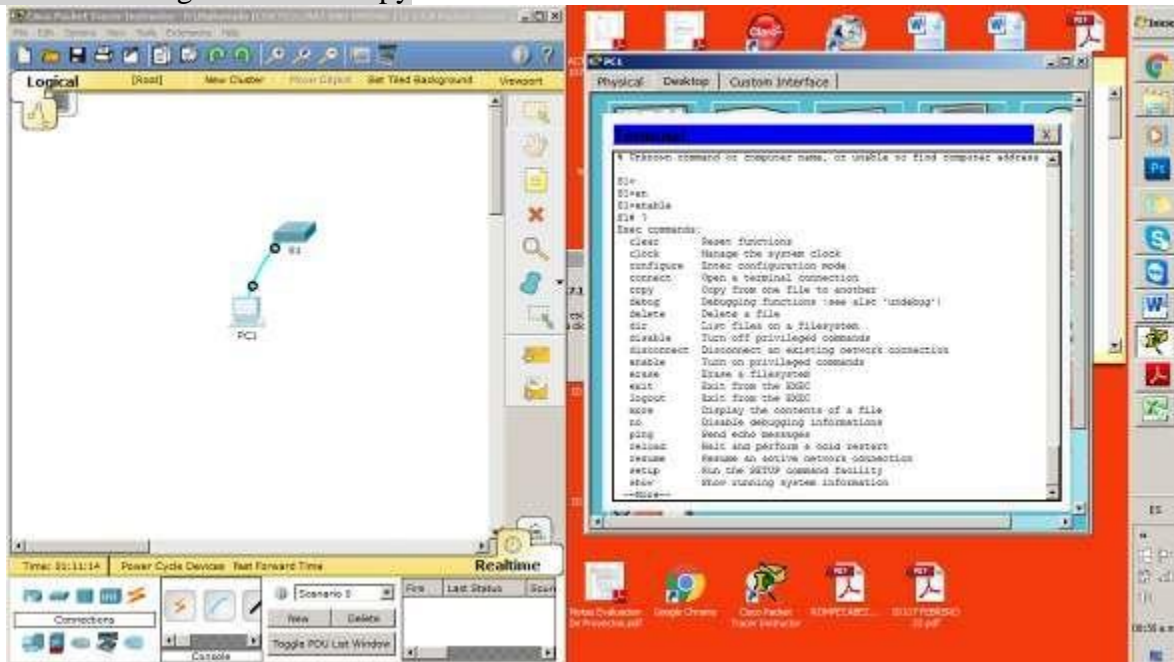
`S1# ?`

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”`).

5: clear clock configure connect copy



Paso 2: Ingresar en el modo de configuración global

- Quando 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, la tecla <Entrar>.

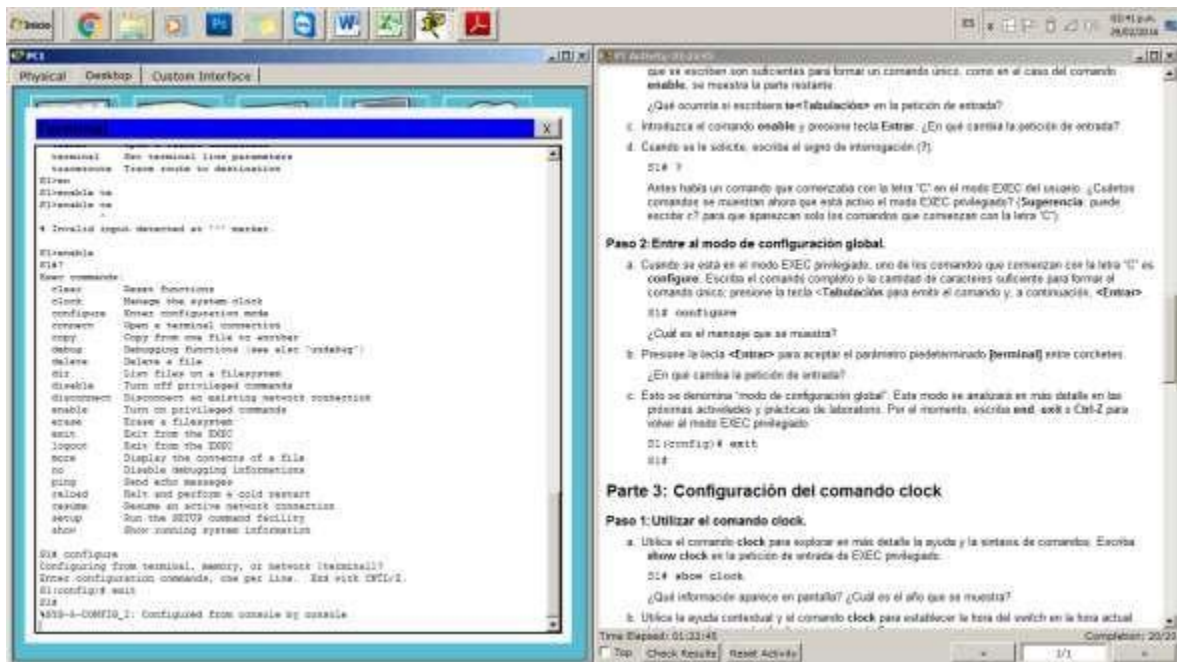
S1# **configure**

¿Cuál es el mensaje que se muestra?

Configuring from terminal, memory, or network [terminal]? (Configurando desde terminal, memoria o red [terminal]?)

- Presione la tecla <Entrar> para aceptar el parámetro predeterminado [**terminal**] entre corchetes. ¿En qué cambia la petición de entrada? S1(config)#
- 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#



Parte 3: Configuración del comando clock

Paso 1: Utilizar el comando clock

- 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?

UTC Mon Mar 1 1993 (UTC lun 1 de marzo de 1993), precedido por las horas, los minutos y segundos desde que el dispositivo se inició. El año es 1993.

- 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<ENTER>

¿Qué información aparece en pantalla? % Incomplete command.

- 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? set Configura la hora y la fecha

- d. Configure el reloj con el comando **clock set**. Continúe utilizando este comando paso por paso.
S1# clock set ?

¿Qué información se solicita? hh:mm:ss Hora actual

¿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? % Incomplete command

- 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 Month of the year

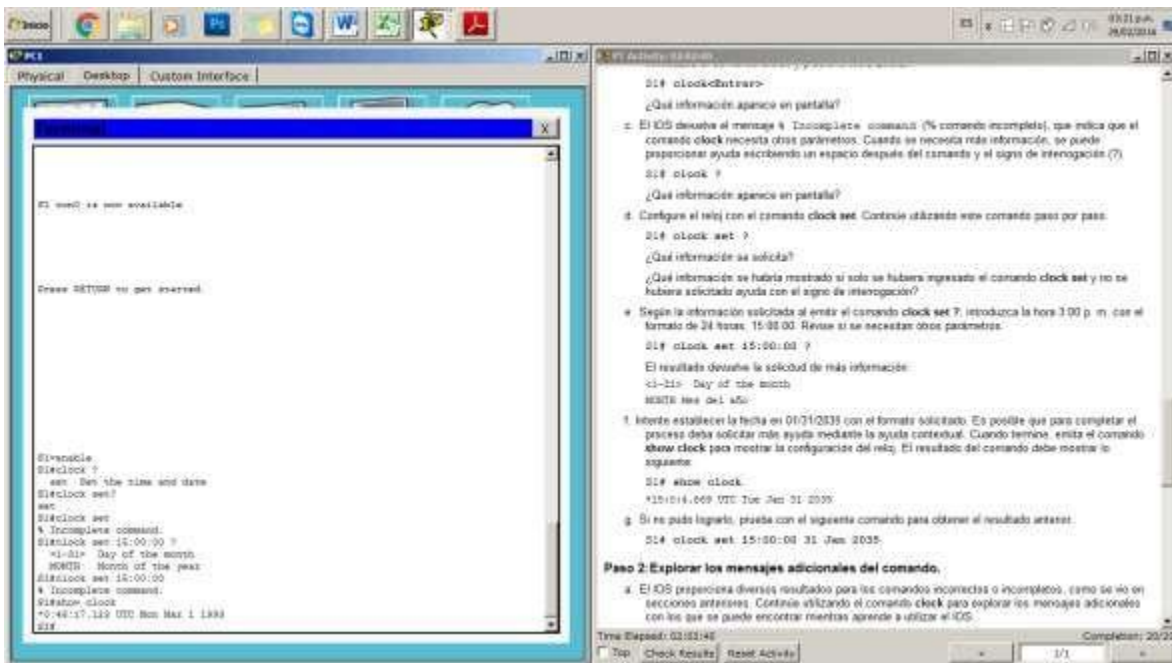
- f. Intente establecer la fecha en 01/31/2035 con el formato solicitado. Es posible que para completar el proceso deba solicitar más ayuda mediante la ayuda contextual. Cuando termine, emita el comando **show clock** para mostrar la configuración del reloj. El resultado del comando debe mostrar lo siguiente:

S1# show clock

*15:0:4.869 UTC Tue Jan 31 2035

- 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

- 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.
- Emita el siguiente comando y registre los mensajes:

S1# **cl**

¿Qué información se devolvió? % Ambiguous command: "cl"

S1# **clock**

¿Qué información se devolvió? % Incomplete command.

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

¿Qué información se devolvió?

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

^

% Invalid input detected at '^' marker.

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

¿Qué información se devolvió?

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

^

% Invalid input detected at '^' marker.

The screenshot shows a PC desktop with a Cisco IOS terminal window open. The terminal output displays the following commands and their results:

```
S1#enable
S1#clock ?
  sec  Set the time and date
S1#clock set ?
  sec
S1#clock set
  % Incomplete command.
S1#clock set 15:00:00 ?
  *1-31* Day of the month
  MONTH Month of the year
S1#clock set 15:00:00
  % Incomplete command.
S1#show clock
*0:40:17.122 UTC Mon Mar 1 1993
S1#cl
  % Ambiguous command: "cl"
S1# cl
  % Ambiguous command: " cl"
S1#clock
```

To the right of the terminal window is a document with the following text:

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? % Ambiguous command: "cl"

S1# **clock**

¿Qué información se devolvió? % Incomplete command.

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

¿Qué información se devolvió?

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

^

% Invalid input detected at '^' marker.

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

¿Qué información se devolvió?

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

^

% Invalid input detected at '^' marker.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Paso 1: Conocer las técnicas, acceso a la CLI y exploración de ayuda	Paso 2a	5	
	Paso 2c	5	
	Paso 3a	5	
	Paso 3b	5	
	Paso 3c	5	
Total de la parte 1		25	
Paso 2: Configuración de las redes EXEC	Paso 1a	5	
	Paso 1b	5	
	Paso 1c	5	
	Paso 1d	5	
	Paso 2a	5	
	Paso 2b	5	
Total de la parte 2		30	

Time Elapsed: 02:08:48 Total de la parte 1 Completion: 20/20

Top Check Results Reset Activity 1/1

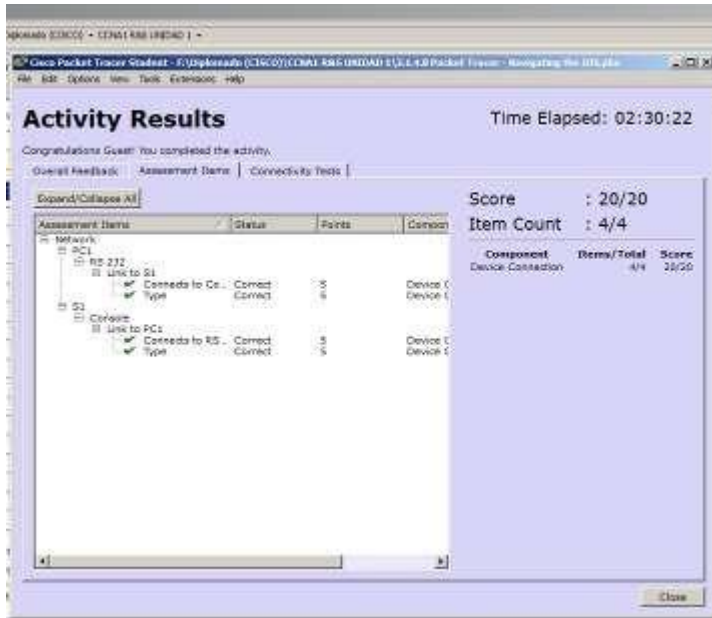


Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Conexiones básicas, acceso a la CLI y exploración de ayuda	Paso 2a	5	
	Paso 2c	5	
	Paso 3a	5	
	Paso 3b	5	
	Paso 3c	5	
Total de la parte 1		25	
Parte 2: Exploración de los modos EXEC	Paso 1a	5	
	Paso 1b	5	
	Paso 1c	5	

	Paso 1d	5	
	Paso 2a	5	
	Paso 2b	5	
Total de la parte 2		30	
Parte 3: Configuración del comando clock	Paso 1a	5	
	Paso 1b	5	
	Paso 1c	5	
	Paso 1d	5	
	Paso 2b	5	
Total de la parte 3		25	
Puntuación de Packet Tracer		20	
Puntuación total		100	

Packet Tracer: Configuración inicial del router

Topología



Objetivos

Parte 1: Verificar la configuración

predeterminada del router Parte 2: Configurar y verificar la configuración inicial del router Parte

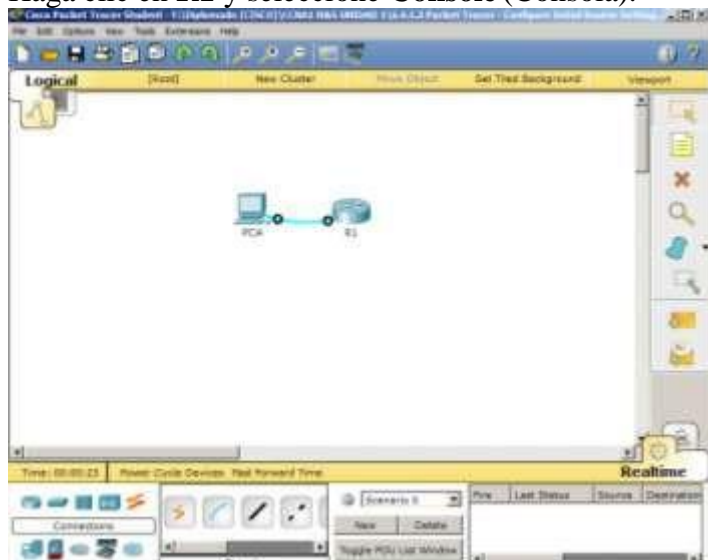
3: Guardar el archivo de configuración en ejecución

Información básica

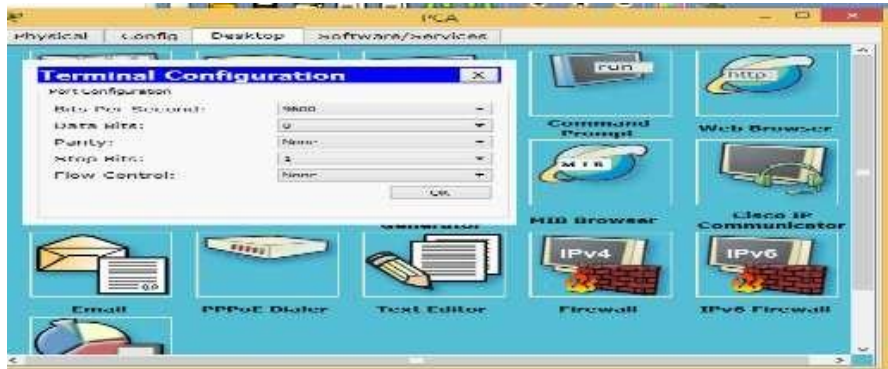
Parte 1: Verificar la configuración predeterminada del router

Paso 1: Establecer una conexión de consola al R1

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



d. Haga clic en **PCA** > ficha **Desktop** (Escritorio) > **Terminal**.



e. Haga clic en **OK** (Aceptar) y presione **Entrar**. Ahora puede configurar **R1**.

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

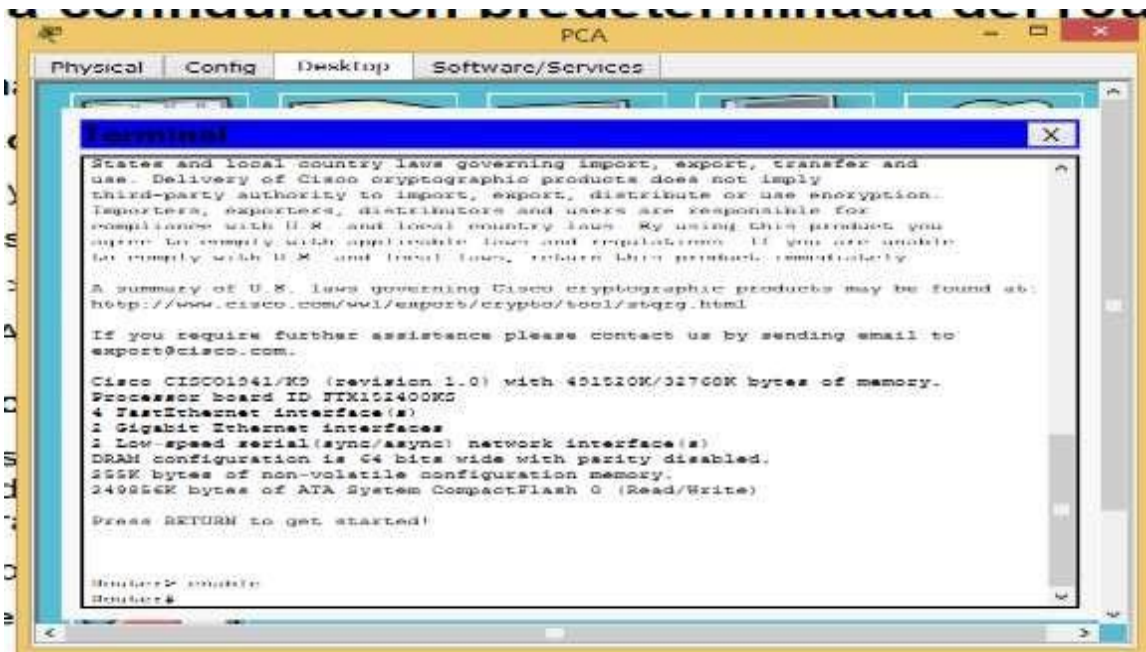
Puede acceder a todos los comandos del router en el modo EXEC privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado.

a. Introduzca el modo EXEC privilegiado introduciendo el comando **enable**.

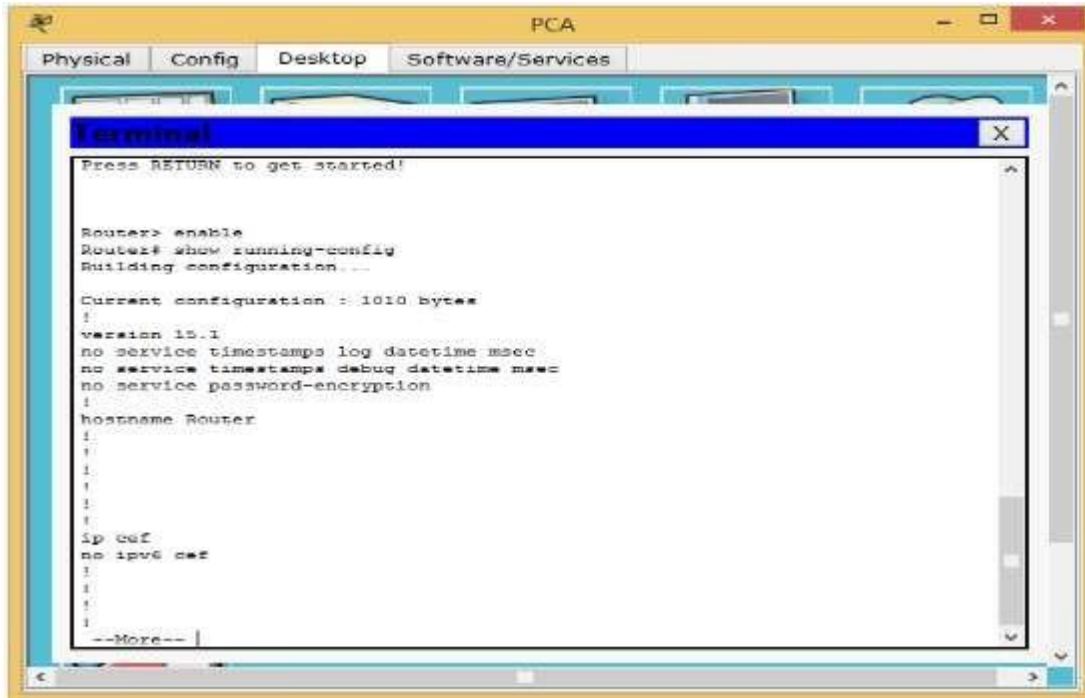
```
Router> enable
```

```
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**

c. Responda las siguientes preguntas:

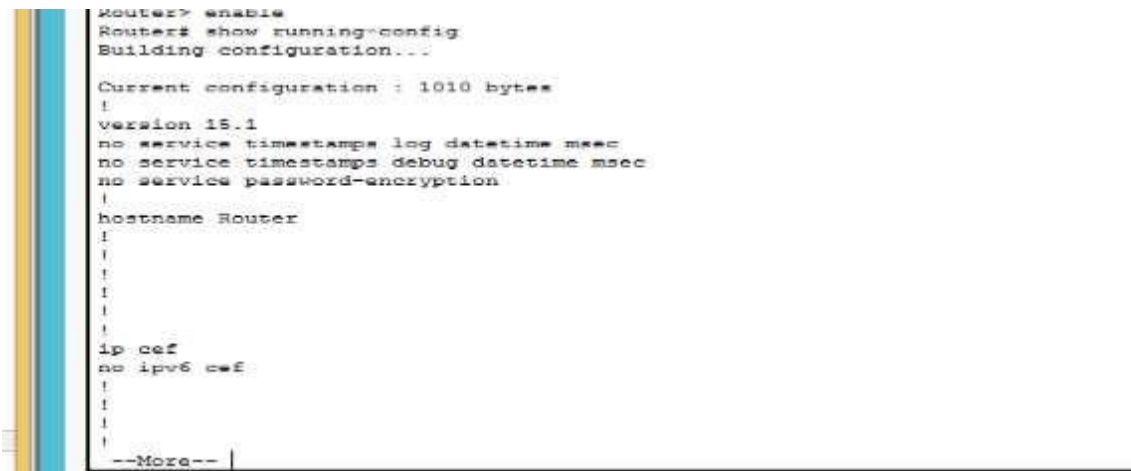
¿Cuál es el nombre de host del router? **Router**

¿Cuántas interfaces Fast Ethernet tiene el router? **4**

¿Cuántas interfaces Gigabit Ethernet tiene el router? **2**

¿Cuántas interfaces seriales tiene el router? **2**

¿Cuál es el rango de valores que se muestra para las líneas vty? **0 - 4**

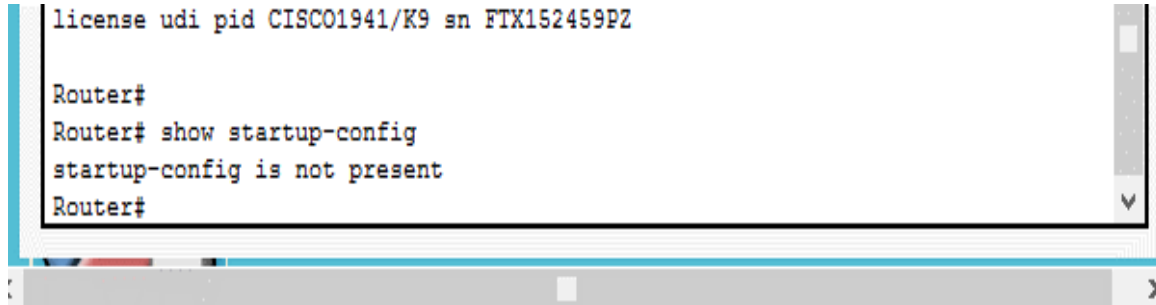


- d. Muestre el contenido actual de la NVRAM.

```
Router# show startup-config
```

```
startup-config is not present
```

¿Por qué el router responde con el mensaje startup-config is not present? Este mensaje se muestra porque el archivo de configuración no se guardó en la NVRAM. Actualmente se encuentra solo en RAM.



```
license udi pid CISCO1941/K9 sn FTX152459PZ
Router#
Router# show startup-config
startup-config is not present
Router#
```

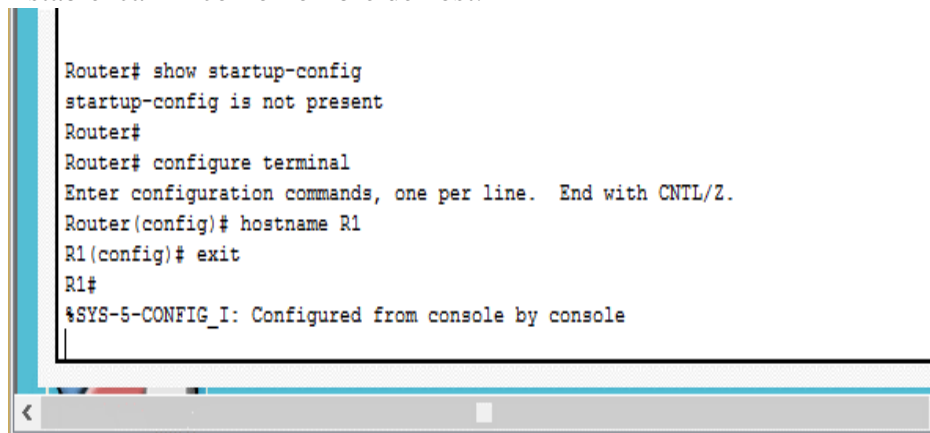
Parte 2: Configurar y verificar la configuración inicial del router

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.




```
Router# show startup-config
startup-config is not present
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- b. Utilice las siguientes contraseñas:
- 1) Consola: **letmein**
 - 2) EXEC privilegiado, sin encriptar: **cisco**
 - 3) EXEC privilegiado, encriptado: **itsasecret**

```
R1(config)#hostname R1
R1(config)#line console 0
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable password cisco
R1(config)#en
% Ambiguous command: "en"
R1(config)#enable
% Incomplete command.
R1(config)#enable secret itsasecret
R1(config)#service password-encryption
R1(config)#
R1(config)#
R1(config)#banner motd "Unauthorized access is strictly prohibited."
R1(config)#
```

- c. Encripte todas las contraseñas de texto no cifrado.
- d. Texto del mensaje del día: Unauthorized access is strictly prohibited(El acceso no autorizado queda terminantemente prohibido).



```

R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1# config t
Enter configuration commands, one per line. End with CTRL/Z.
R1(config)# service password-encryption
R1(config)# exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1# config t
Enter configuration commands, one per line. End with CTRL/Z.
R1(config)# banner motd "Unauthorized access is strictly prohibited"
R1(config)# exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 2: Verificar los parámetros iniciales de R1

- a. Para verificar los parámetros iniciales, observe la configuración de R1. ¿Qué comando utiliza?
`show running-config`



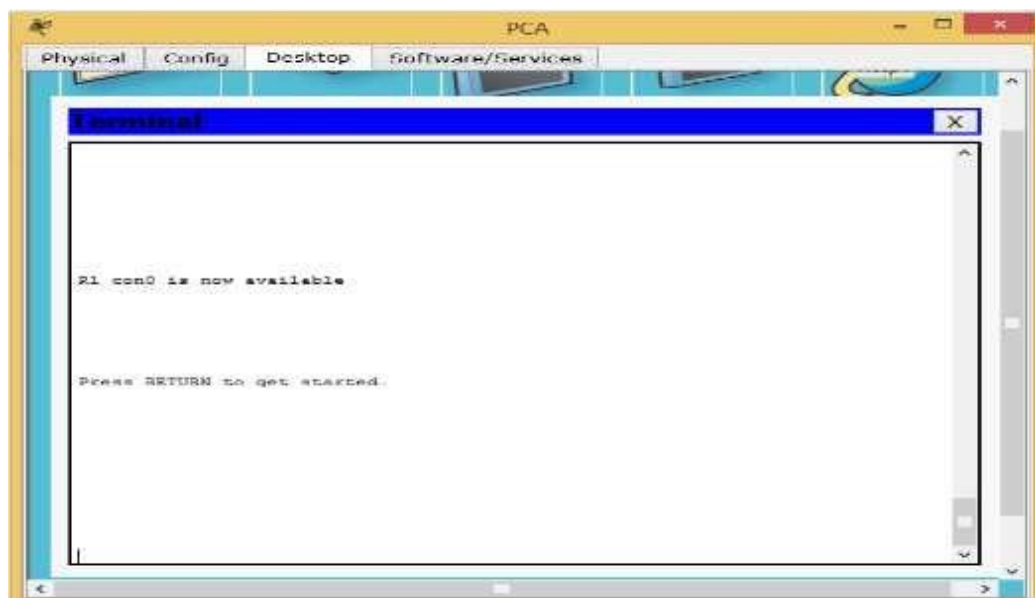
```
R1(config)# service password-encryption
R1(config)# exit
R1#
*SYS-8-CONFID_I: Configured from console by console

R1# show running-config
Building configuration...

Current configuration : 1119 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$m2Rz#11wq/b/kc.7K/ujA4Acsn0
enable password 7 0822458D0A16
!
!
!
ip def
no ipv6 def
!
--More--
```

- b. Salga de la sesión de consola actual hasta que vea el siguiente mensaje:
R1 con0 is now available Press

RETURN to get started.



- 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)? Cada router debe tener un mensaje para advertir a los usuarios no autorizados que el acceso está prohibido, pero también se puede utilizar para enviar mensajes al personal y a los técnicos de red (por ejemplo, sobre cierres inminentes del sistema o a quién contactar para obtener acceso).

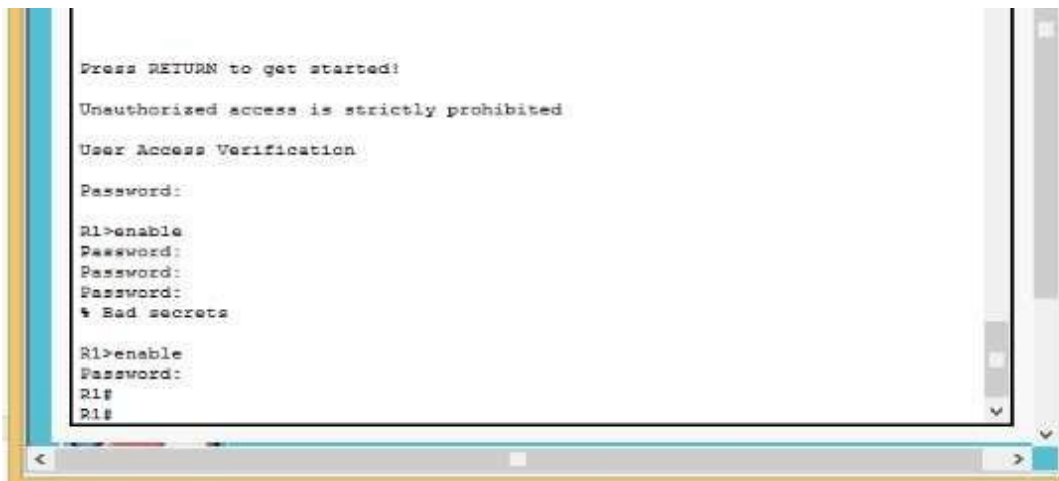
Si no se le pide una contraseña, ¿qué comando de la línea de consola se olvidó de configurar?

R1(config-line)# login

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

¿Por qué la contraseña **secreta de enable** permitiría el acceso al modo EXEC privilegiado y **la contraseña de enable** dejaría de ser válida? **La contraseña secreta de enable** sobrescribe la contraseña de enable. Si ambas están configuradas en el router, debe introducir la contraseña **secreta de enable** para ingresar al modo EXEC privilegiado.

Si configura más contraseñas en el router, ¿se muestran como texto no cifrado o en forma encriptada en el archivo de configuración? Explique. **El comando service password-encryption** encripta todas las contraseñas actuales y futuras.



```
Press RETURN to get started!  
Unauthorized access is strictly prohibited  
User Access Verification  
Password:  
R1>enable  
Password:  
Password:  
Password:  
% Bad secrets  
R1>enable  
Password:  
R1#  
R1#
```

Parte 3: Guardar el archivo de configuración en ejecución

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

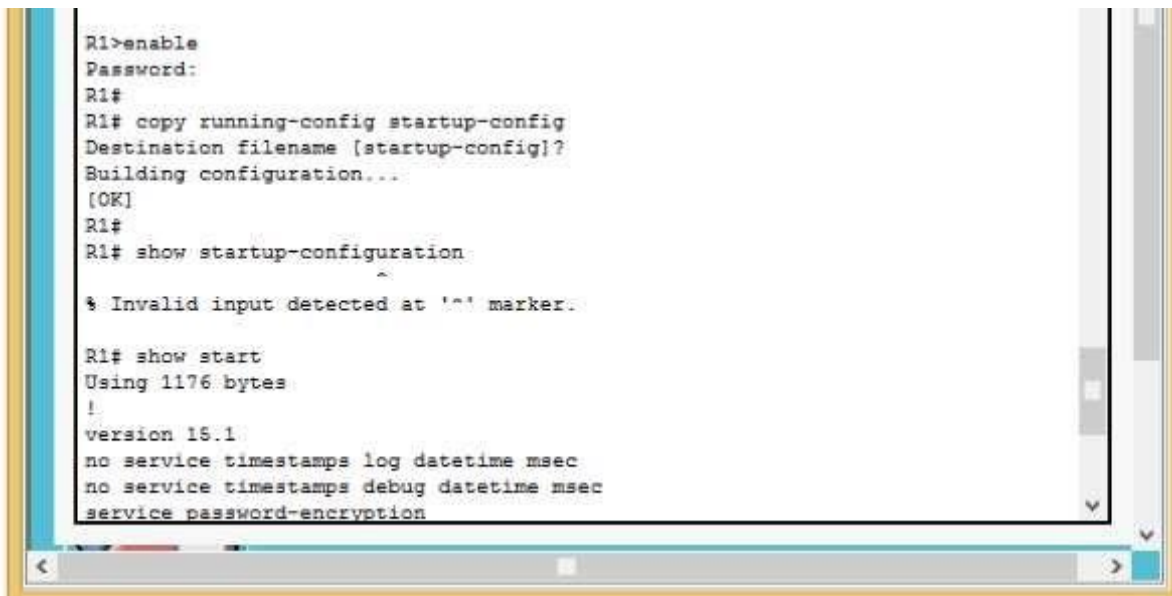
- a. Configuró los parámetros iniciales de **R1**. Ahora realice una copia de seguridad del archivo de configuración en ejecución en la NVRAM para garantizar que no se pierdan los cambios realizados si el sistema se reinicia o se apaga.

¿Qué comando introdujo para guardar la configuración en la NVRAM? `copy running-config startup-config`

¿Cuál es la versión más corta e inequívoca de este comando? `copy r s`

¿Qué comando muestra el contenido de la NVRAM? `show startup-configuration` or `show start`

- 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.



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

% Invalid input detected at '^' marker.

R1# show start
Using 1176 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
```

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**

¿Cuántos archivos hay almacenados actualmente en la memoria flash? **3**

¿Cuál de estos archivos cree que es la imagen de IOS? c1900-universalk9-mz.SPA.151-4.M4.bin

¿Por qué cree que este archivo es la imagen de IOS? Las respuestas pueden variar, pero hay dos pistas: la longitud del archivo en comparación con otros y la extensión .bin al final del nombre de archivo.

- 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]
```

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

```
249856K bytes of processor board System flash (Read/Write)
```

```
R1# copy startup-config flash
```

```
Destination filename [startup-config]?
```

```
1176 bytes copied in 0.416 secs (2826 bytes/sec)
```

```
R1#
```

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**.

```
1176 bytes copied in 0.416 secs (2826 bytes/sec)
```

```
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	1176	startup-config

```
[33848763 bytes used, 221895237 available, 255744000 total]
```

```
249856K bytes of processor board System flash (Read/Write)
```

```
R1#
```

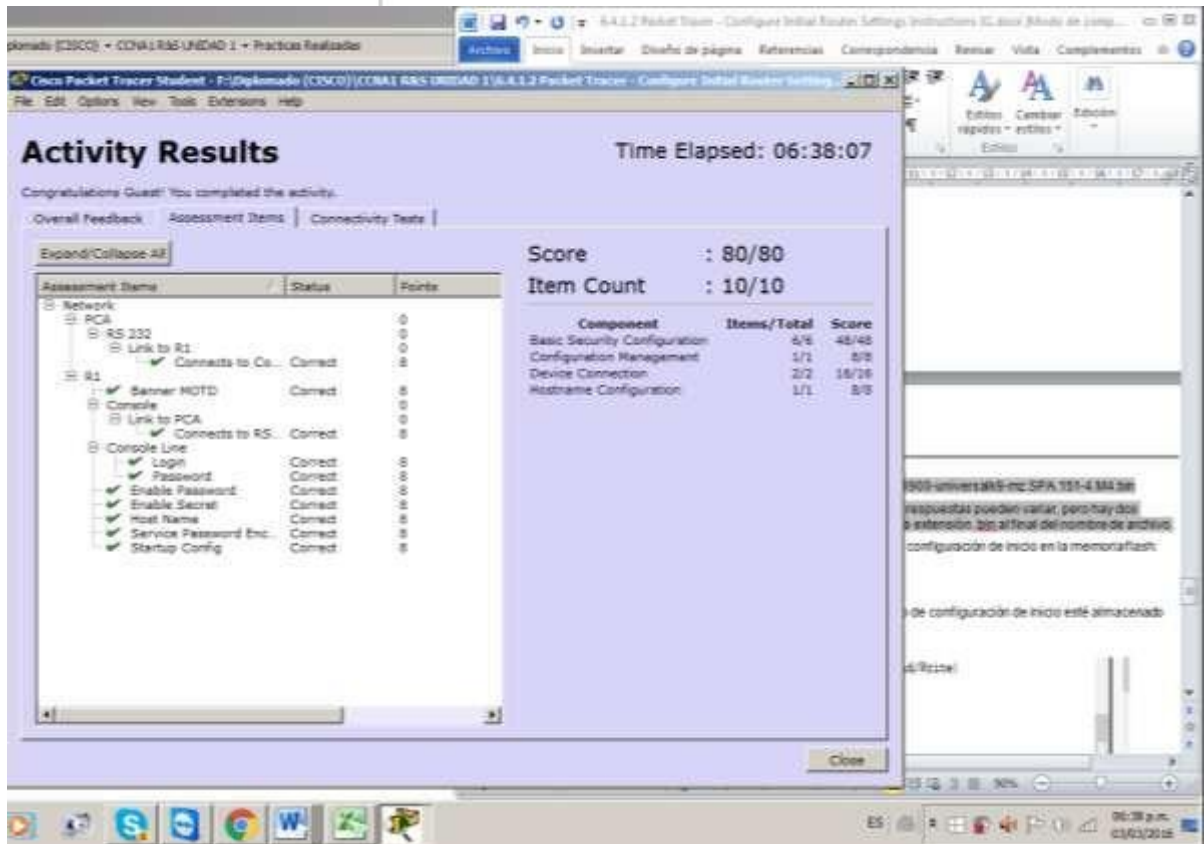


Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Verificar la configuración predeterminada del	Paso 2c	10	
	Paso 2d	2	
Total de la parte 1		12	
Parte 2: Configurar y verificar la configuración inicial del router	Paso 2a	2	
	Paso 2c	5	
	Paso 2d	6	
Total de la parte 2		13	
Parte 3: Guardar el archivo de configuración en	Paso 1a	5	
	Paso 2a (puntos	5	
Total de la parte 3		10	
Puntuación de Packet Tracer		80	
Puntuación total (con los puntos extra)		105	

Topología

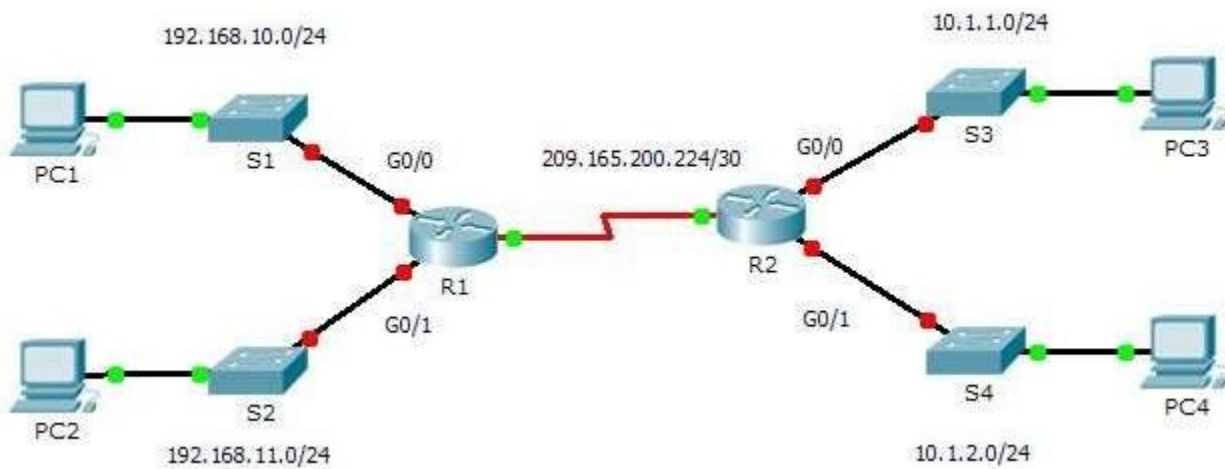


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección	Máscara de	Gatew ay
R1	G0/0	192.168.10.1	255.255.	No
	G0/1	192.168.11.1	255.255.	No
	S0/0/0	209.165.200.	255.255.25	No
R2	G0/0	10.1.1.1	255.255.	No
	G0/1	10.1.2.1	255.255.	No
	S0/0/0	209.165.200.	255.255.25	No
PC1	NIC	192.168.10.1	255.255.	192.168.10
PC2	NIC	192.168.11.1	255.255.	192.168.11
PC3	NIC	10.1.1.10	255.255.	10.1.1.1
PC4	NIC	10.1.2.10	255.255.	10.1.2.1

Objetivos

Parte 1: Mostrar la información del

router Paso 2: Configurar las interfaces

del router Paso 3: Verificar la


configuración

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? **showinterfaces**



```

R1
Physical | Config | CLI
IOS Command Line Interface

User Access Verification

Password:

R1#show interfaces
GigabitEthernet0/0 is administratively down, line protocol is down (disabled)
Hardware is CN Gigabit Ethernet, address is 000d.bd6c.7a01 (bia 000d.bd6c.7a01)
Internet address is 192.168.10.1/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 watchdog, 1017 multicast, 0 pause input
 0 input packets with dribble condition detected
--More--

```

- b. ¿Qué comando muestra solo la información de la interfaz Serial 0/0/0? `show interface serial 0/0/0`

```
R1>
R1>
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 0/0/255 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 40 bits/sec, 0 packets/sec
5 minute output rate 44 bits/sec, 0 packets/sec
28 packets input, 1640 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
28 packets output, 1720 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
--More--
```

- 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**? `209.165.200.225/30`

```
Hardware is HD64570
Internet address is 209.165.200.225/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
```

- 2) ¿Cuál es el ancho de banda en la interfaz Serial 0/0/0? `1544 kbits`

```
Physical | Config | CLI |
IOS Command Line Inter
R1>
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
```

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

- 1) ¿Cuál es la dirección IP en el **R1**? No hay dirección Ip.
NO HAY IP

- 2) ¿Cuál es la dirección MAC de la interfaz GigabitEthernet 0/0? `000d.bd6c.7d01`

```

--j -----, ----j -----, -----, -----,
address is 000d.bd6c.7d01 (bia 000d.bd6c.7d01)
OLY 10 usec,

```

3) ¿Cuál es el ancho de banda en la interfaz GigabitEthernet 0/0? 1 000 000kbits

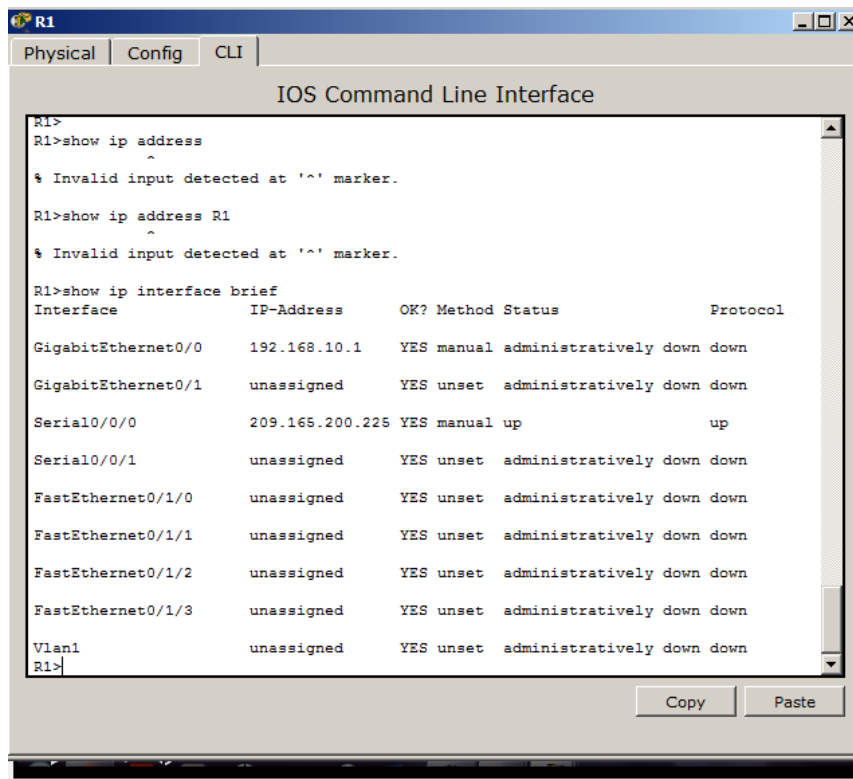
```

Gigabit Ethernet,
. BW 1000000 Kbit,
-----

```

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? `show ip interface brief`



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

1) ¿Cuántas interfaces seriales hay en **R1** y **R2**? Cada router tiene 2 interfaces seriales.

R1:

```
IOS Command Line Interface

!
!
interface GigabitEthernet0/0
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.11.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
ip address 209.165.200.225 255.255.255.252
clock rate 64000
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface FastEthernet0/1/0
switchport mode access
shutdown
!
interface FastEthernet0/1/1
switchport mode access
shutdown
--More--
```

R2:

```
R2
Physical Config CLI
IOS Command Line Interface

!
!
interface GigabitEthernet0/0
ip address 10.1.1.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 10.1.2.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
ip address 209.165.200.226 255.255.255.252
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 1
network 10.0.0.0
network 209.165.200.0
auto-summary
!
--More--

Copy Paste
```

- 2) ¿Cuántas interfaces Ethernet hay en **R1** y **R2**? **R1** tiene seis interfaces Ethernet y **R2** tiene dos interfaces Ethernet.

R2:



```
spanning-tree mode pvtst
!
!
!
interface GigabitEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.1.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 209.165.200.224 255.255.255.224
!
interface Serial0/0/1
 no ip address
 clock rate 1000000
 shutdown
!
interface Vlan1
```

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

```
Serial0/0/0      209.165.200.225 YES manual up      up
Serial0/0/1      unassigned      YES unset  administratively down down
Serial0/0/0      209.165.200.224 YES manual up      up
Serial0/0/1      unassigned      YES unset  administratively down down
```

En R1 vemos seis interfaces Ethernet como se aprecia en la siguiente imagen:

2) ¿Qué ruta se indica? 209.165.200.224/30

```
209.165.200.0/24 is variably subnetted, 4 subnets, 4 masks
C    209.165.200.224/30 is directly connected, Serial0/0/0
-    . . . . .
```

3) ¿Cómo administra el router un paquete destinado a una red que no se incluye en la tabla de enrutamiento? Un router solo envía paquetes a redes indicadas en la tabla de enrutamiento. Si una red no aparece en la lista, el paquete se descarta.

Parte 2: 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
```

```
R1#
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface GigabitEthernet 0/0
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
R1(config-if)#
```

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
```

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

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

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

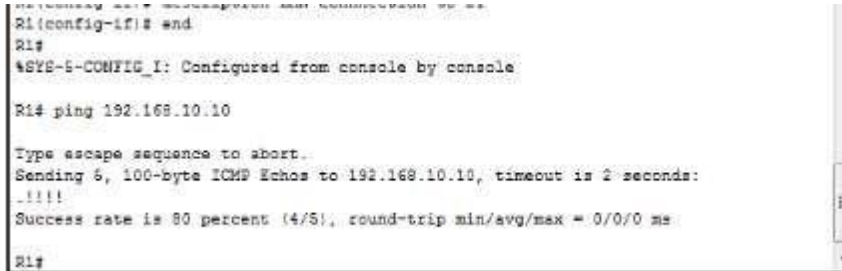
%SYS-5-CONFIG_I: Configured from console by console R1#
ping 192.168.10.10

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



```
R1(config-if)# end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1# ping 192.168.10.10

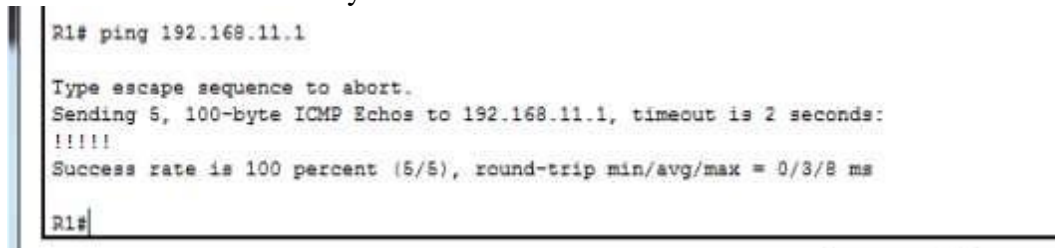
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

R1#
```

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

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

1) Introduzca la dirección IP y active la interfaz.



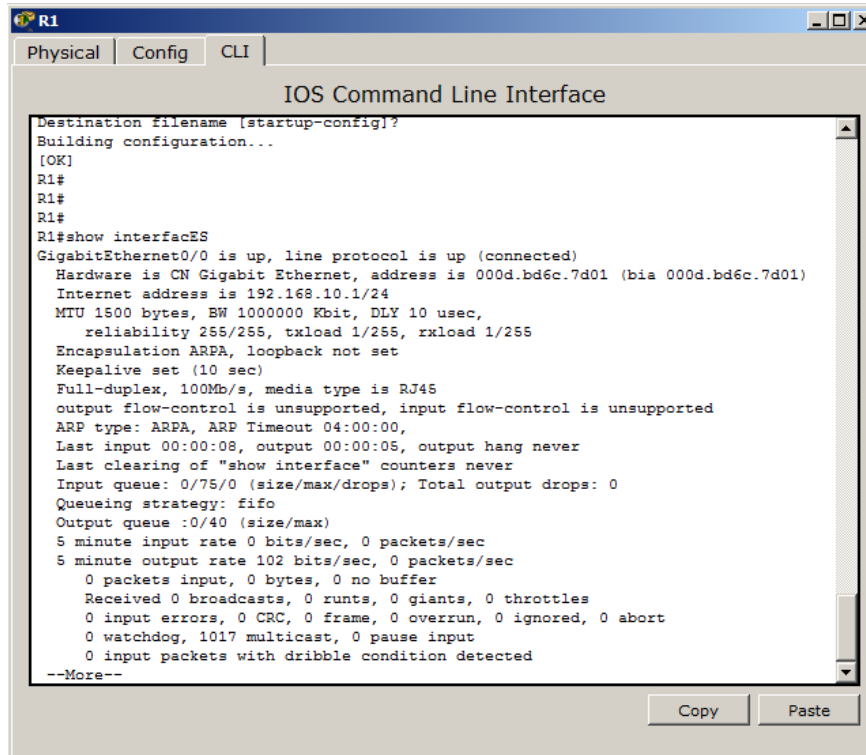
```
R1# ping 192.168.11.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/8 ms

R1#
```

2) Configure una descripción apropiada.

b. Verifique las configuraciones de las interfaces.



```
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
R1#
R1#
R1#show interfaceS
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 000d.bd6c.7d01 (bia 000d.bd6c.7d01)
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 102 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 1017 multicast, 0 pause input
    0 input packets with dribble condition detected
--More--
```

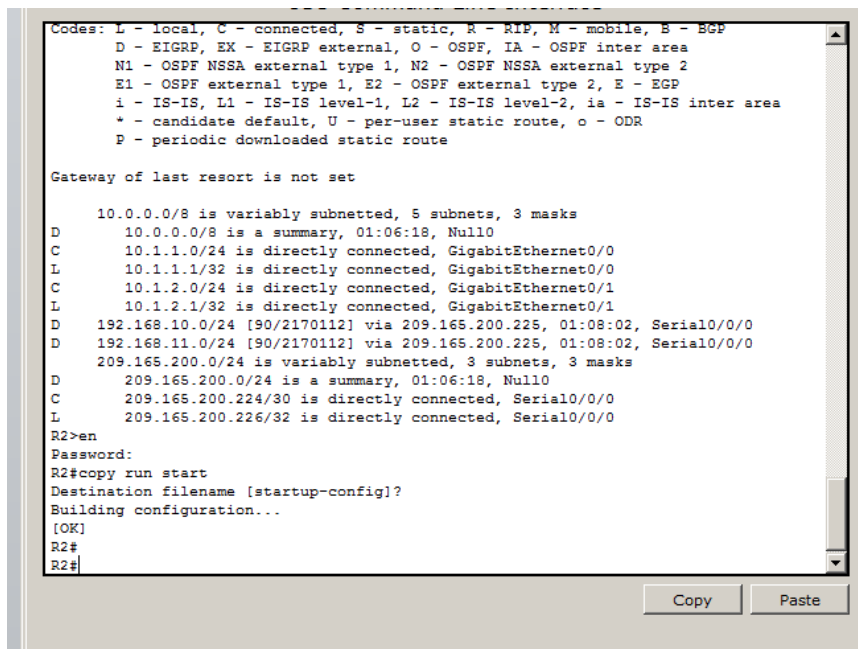
Paso 3: Realizar una copia de seguridad de las configuraciones en la NVRAM

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

R1:



R2:

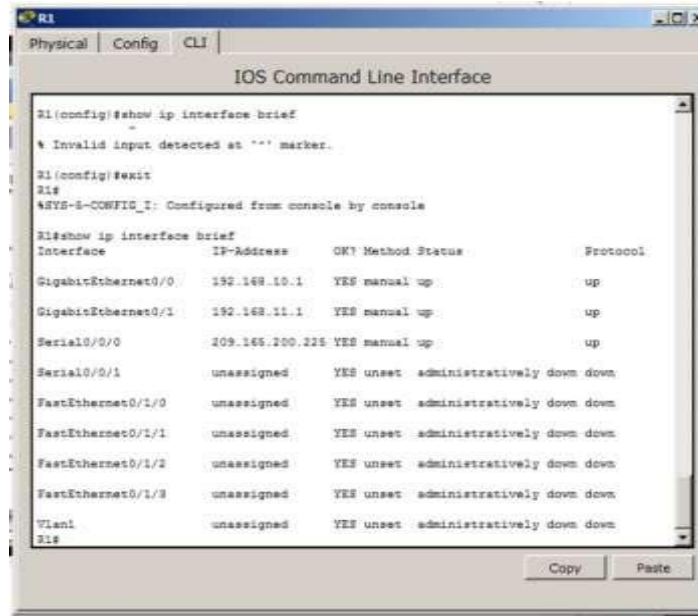


Parte 3: Verificar la configuración

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.

R1:



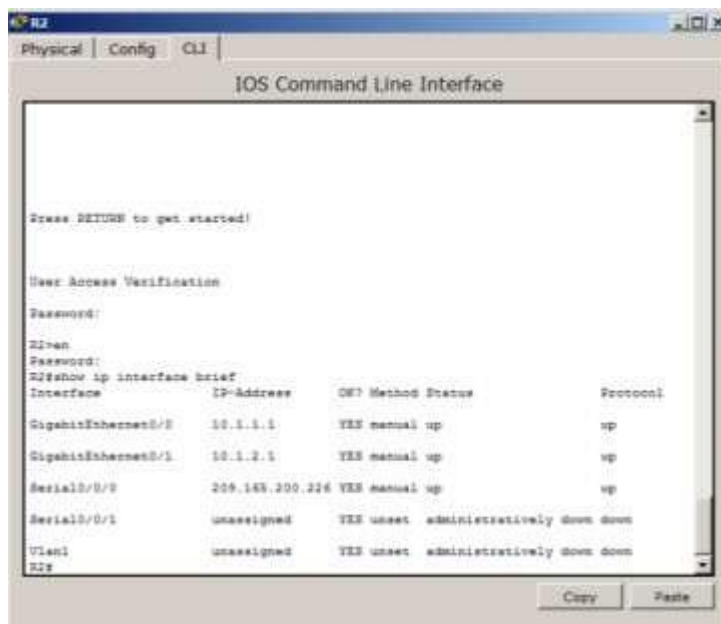
```
R1
Physical | Config | CLI
IOS Command Line Interface

R1(config)#show ip interface brief
% Invalid input detected at '' marker.

R1(config)#exit
R1#
%SYS-5-CFGIF_1: Configured from console by console

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
Serial0/0/1         unassigned      YES unset  administratively down down
FastEthernet0/1/0   unassigned      YES unset  administratively down down
FastEthernet0/1/1   unassigned      YES unset  administratively down down
FastEthernet0/1/2   unassigned      YES unset  administratively down down
FastEthernet0/1/3   unassigned      YES unset  administratively down down
Vlan1               unassigned      YES unset  administratively down down
R1#
```

R2:



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

Press RETURN to get started!

User Access Verification

Password:
R2>en
Password:
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         209.165.200.225 YES manual up          up
Serial0/0/1         unassigned      YES unset  administratively down down
Vlan1               unassigned      YES unset  administratively down down
R2#
```

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

```
R2#  
R2#  
R2#  
R2#show interfaces  
GigabitEthernet0/0 is up, line protocol is up (connected)  
Hardware is CN Gigabit Ethernet, address is 0002.16cb.1d01 (bia 0002.16cb.1d01)  
Internet address is 10.1.1.1/24  
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,  
reliability 255/255, txload 1/255, rxload 1/255
```

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

1) ¿Cuántas rutas conectadas (utilizan el código **C**) ve en cada router? **3**

R1:

```

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, 00:06:19, 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, 00:06:29, 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
R1#

```

Copy

Paste

R2:

The screenshot shows a terminal window titled 'R2' with tabs for 'Physical', 'Config', and 'CLI'. The main content is the 'IOS Command Line Interface' showing the output of the 'show ip route' command. The output is identical to the one shown for R1, but with a different timestamp for the summary route (00:07:43).

```

R2#
R2#
R2#
R2#
R2#
R2#
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, 00:07:43, 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, 00:07:43, Serial0/0/0
D    192.168.11.0/24 [90/2170112] via 209.165.200.225, 00:07:43, Serial0/0/0
    209.165.200.0/24 is variably subnetted, 3 subnets, 3 masks
D    209.165.200.0/24 is a summary, 00:07:43, 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
R2#

```

Copy

Paste

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

R1:

```
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, 00:06:19, 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, 00:06:29, 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
R1#
```

Copy

Paste

R2:

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

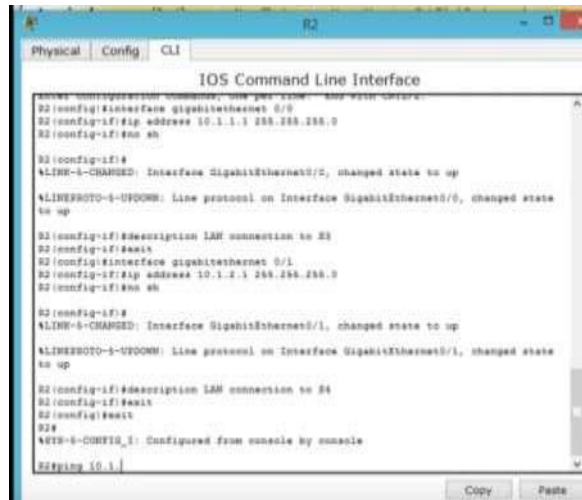
    10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D    10.0.0.0/8 is a summary, 00:07:43, Null0
C    10.1.1.0/24 is directly connected, GigabitEthernet0/0
L    10.1.1.1/32 is directly connected, GigabitEthernet0/0
C    10.1.2.0/24 is directly connected, GigabitEthernet0/1
L    10.1.2.1/32 is directly connected, GigabitEthernet0/1
D    192.168.10.0/24 [90/2170112] via 209.165.200.225, 00:07:43, Serial0/0/0
D    192.168.11.0/24 [90/2170112] via 209.165.200.225, 00:07:43, Serial0/0/0
    209.165.200.0/24 is variably subnetted, 3 subnets, 3 masks
D    209.165.200.0/24 is a summary, 00:07:43, 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
R2#
```

Copy

Paste

- 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? **5**
- 4) ¿Esta cantidad coincide con la cantidad de rutas C y D que se muestran en la tabla de enrutamiento? **¡sí!**

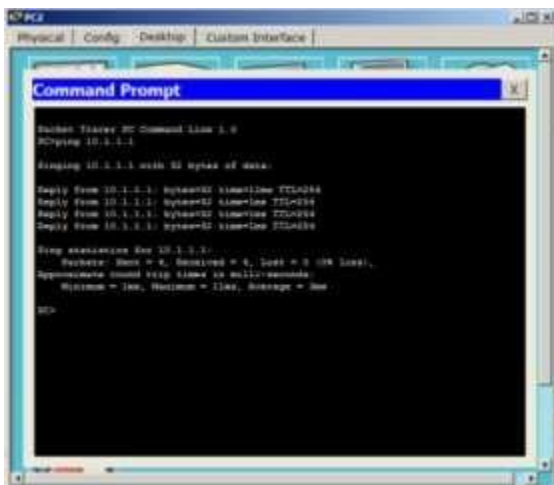
Nota: si su respuesta es “no”, falta una configuración necesaria. Revise los pasos de la parte 2.



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



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

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Mostrar la información del router	Paso	2	
	Paso	2	
	Paso	4	
	Paso	6	
	Paso	2	
	Paso	6	
	Paso	2	
	Paso	6	
Total de la parte 1		30	
Paso 2: Configurar las interfaces del	Pas	2	
Total de la parte 2		2	
Paso 3: Verificar la configuración	Paso	6	
	Paso	8	
Total de la parte 3		14	
Puntuación de Packet Tracer		54	
Puntuación total (con los puntos		100	

Packet Tracer: Resolución de problemas del gateway predeterminado

Topología

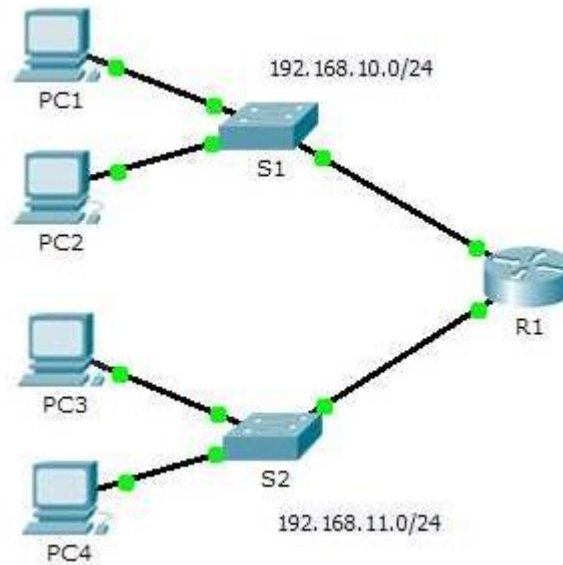


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.1 0.1	255.255.255.0	No aplicable
	G0/1	192.168.1 1.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.1 0.2	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.1 1.2	255.255.255.0	192.168.11.1
PC1	NIC	192.168.1 0.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.1 0.11	255.255.255.0	192.168.10.1
PC3	NIC	192.168.1 1.10	255.255.255.0	192.168.11.1
PC4	NIC	192.168.1 1.11	255.255.255.0	192.168.11.1

Objetivos

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

Parte 2: Implementar, verificar y documentar las soluciones

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:

- 1) Verificar la documentación de la red y utilizar pruebas para descartar problemas.
- 2) Determinar cuál es la solución adecuada para un problema dado.
- 3) Implementar la solución.
- 4) Realizar pruebas para verificar que se haya resuelto el problema.
- 5) 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. Al hacer una revisión de las configuraciones de cada dispositivo se encuentra que algunos de ellos tienen datos errados o no los tienen, con respecto a la tabla inicial dada. El resultado de la revisión inicial es:

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	
S2	VLAN 1		255.255.255.0	192.168.11.1
PC1	NIC	192.168.11.10	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	192.168.1.1

Para consultar los switch se puede obtener la información con el comando “show running-config” en la consola de línea de comandos CLI, habilitando previamente el modo “config” con el comando “enable”.

```

IOS Command Line Interface
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.10.2 255.255.255.0
!
!
line con 0
line vty 0 4
login
line vty 5 15
login
!
end
:~

```

```

IOS Command Line Interface
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface Vlan1
ip address 192.168.11.1 255.255.255.0
!
!
line con 0
line vty 0 4
login
line vty 5 15
login
!
end
:~

```

```

Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection: (default pc0)

Link-Local IPv6 Address.....: FE80::500:B0FF:FE84:B4D1
IP Address.....: 192.168.11.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.10.1

PC>

```

```

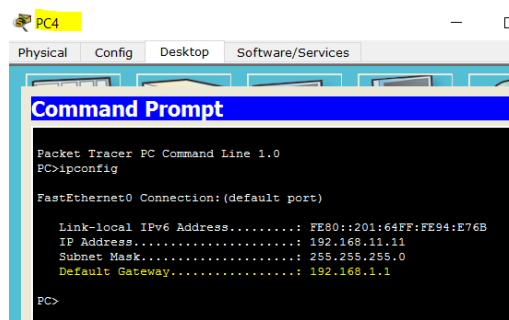
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection: (default pc0)

Link-Local IPv6 Address.....: FE80::201:43FF:FE80:4851
IP Address.....: 192.168.10.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.10.1

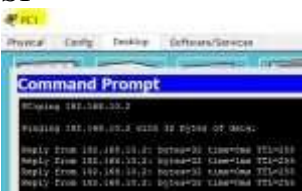
PC>

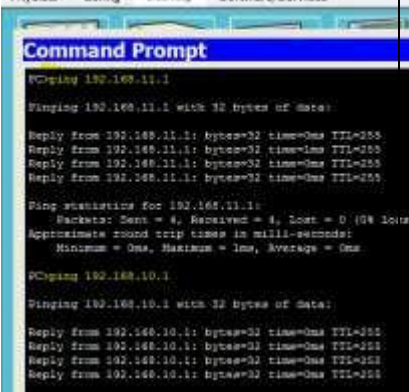
```

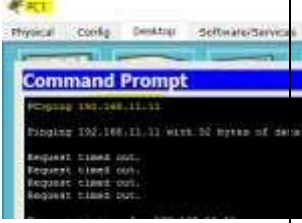



c. Pruebe la conectividad a los dispositivos en la misma red. Al descartar y corregir cualquier problema de acceso local, puede probar mejor la conectividad remota, con la seguridad de que la conectividad local está en funcionamiento.

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.

Prueba	¿Se realizó correctamente?	Problemas	Solución	Verificado
PC1 a PC2	No	Dirección IP en la PC1	Cambiar la dirección IP de la PC1	SI
PC1 a S1	SI 	NINGUNO		
PC1 a R1	SI	NINGUNO		

				
PC3 a PC4	SI 	NINGUNO		
PC3 a S2	NO	S2 no tiene asignada dirección IP	Asignar IP a S2	
PC3 a R1	SI 	NINGUNO		

Prueba	¿Se realizó correctamente?	Problemas	Solución	Verificado
PC1 a PC4	NO 	PC4 tiene mal configurado el Default Gateway	Configurar Correctamente el Default Gateway en PC4	SI
PC3 a S1	NO 	S1 no tiene configurado Default Gateway	Configurar Default Gateway en S1	SI

d. 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 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

Problema conectividad entre PC1 y PC2:

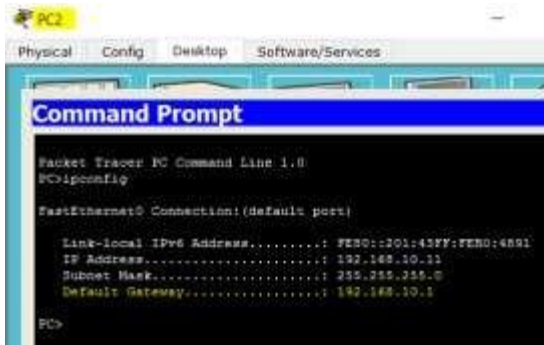
a. Causa del Problema

Una vez verificadas las IP de PC1 y PC2 se observa que la dirección de PC1 no corresponde a la que debería tener de acuerdo a la tabla de direccionamiento dada inicialmente.

IP de PC1: 192.168.11.10 Debería tener la IP: 192.168.10.10



IP de PC2: 192.168.10.11 está bien.



b. Solución sugerida-

Cambiar la dirección IP de PC1

Problema Conectividad entre PC3 y S2

a. Causa del problema

Al revisar la configuración ip del switch se observa que no tiene asignada dirección ip. Debería tener la 192.168.11.2

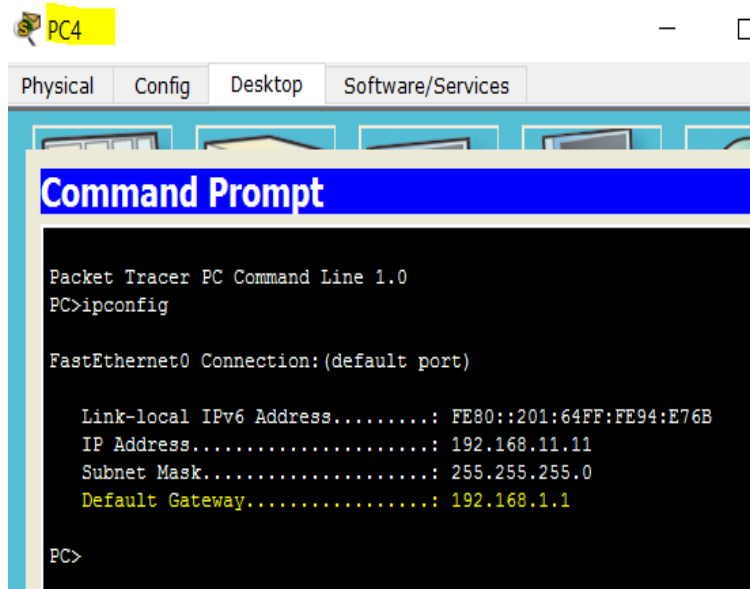


-
- b. Solución sugerida-
Asignar dirección IP al S2

Problema Conectividad entre PC1 y PC4

- a. Causa del problema

Al revisar la configuración de PC4 se observa que tiene mal configurado el default Gateway. Tiene configurado el 192.168.1.1 y el correcto es 192.168.11.1



```
PC4
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::201:64FF:FE94:E76B
IP Address.....: 192.168.11.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1

PC>
```

- b. Solución sugerida-
Corregir la dirección IP del Default Gateway en PC4

Problema conectividad entre PC3 y S1:

- a. Causa del Problema

Al revisar la configuración de S1 se observa que no tiene configurado Default Gateway y el mismo debería ser 192.168.10.1

```
Physical Config CLI
IOS Command Line Interface

!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.10.2 255.255.255.0
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
end
S1#
```

b. Solución Sugerida

Asignar el default Gateway al Switch NO. 2

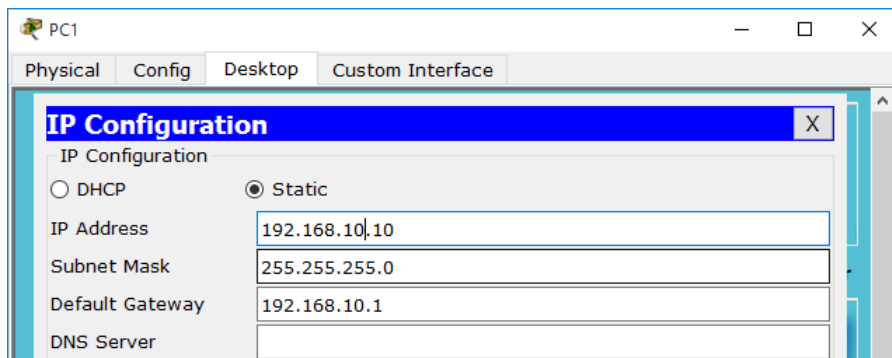
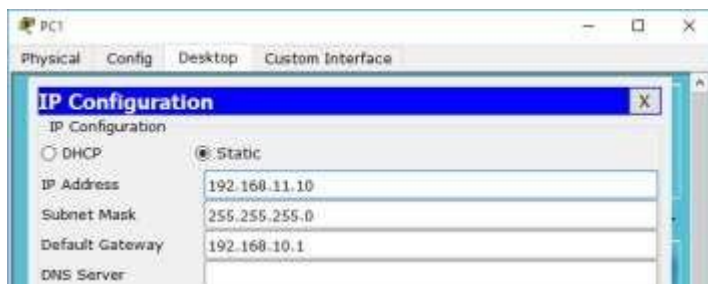
PARTE 2: Implementar, verificar y documentar las soluciones

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.

Problema conectividad PC1 a PC2

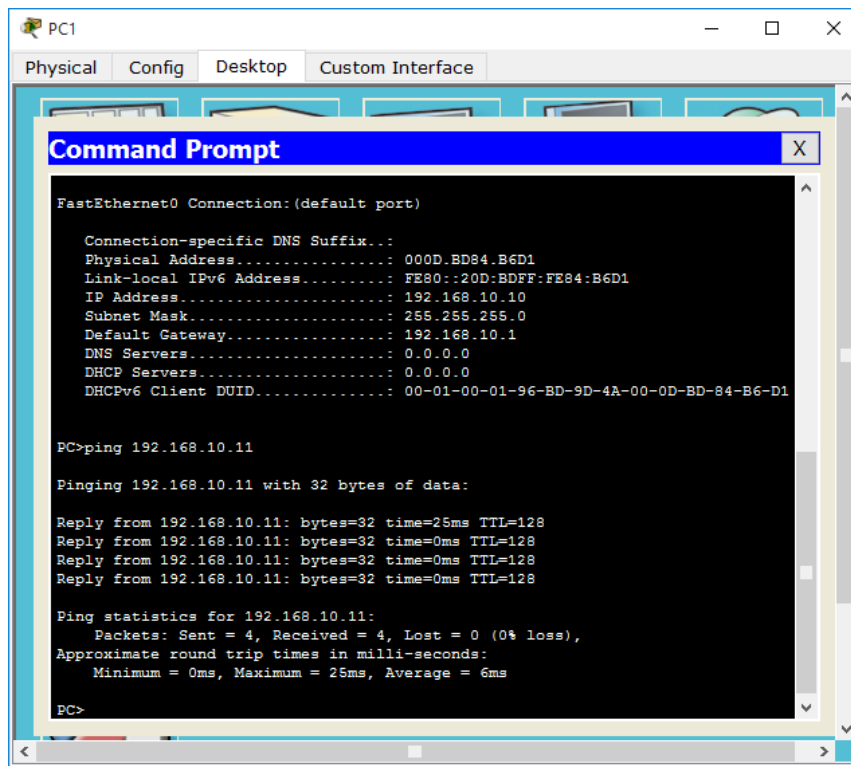
a. Implementar solución

Se cambia la IP en el PC1



b. Verificar solución.

Se verifica la IP del PC1 asegurándose que es correcta y se realiza ping desde el PC1 al PC2, siendo exitoso.



Problema Conectividad entre PC3 y S2

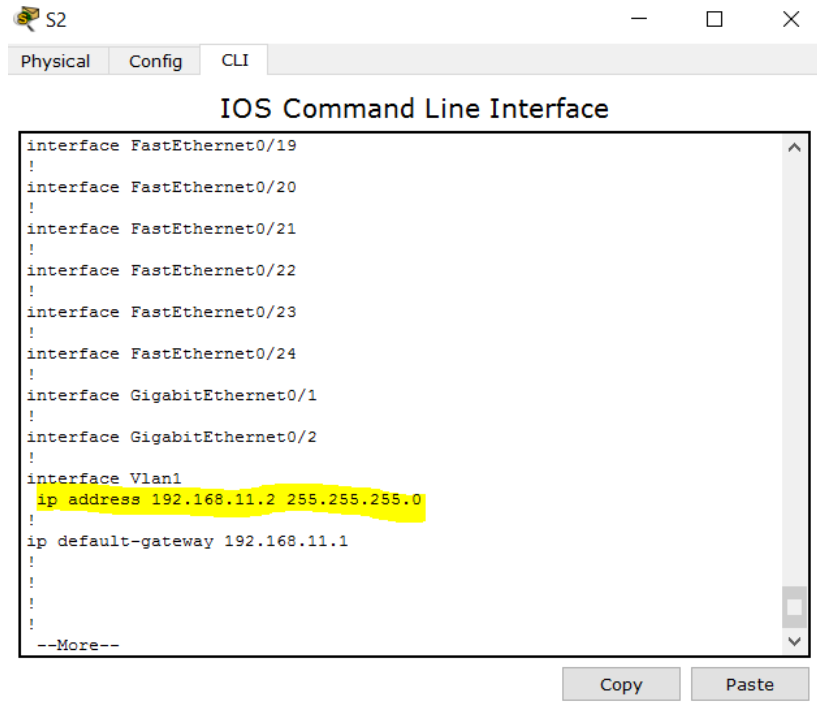
a. Implementar solución

Activando el modo de Config en la Consola de línea de comandos CLI, indicamos que vamos a configurar la interfase VLAN1 y con el comando "ip address" asignamos tanto la dirección IP como la máscara de red que se maneja.

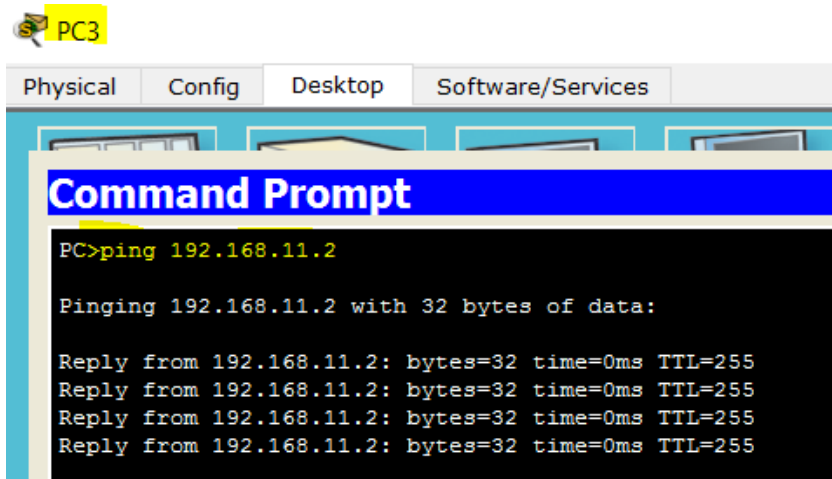


b. Verificar solución

Consultamos la dirección IP de S2 y nos aseguramos que sea correcta:



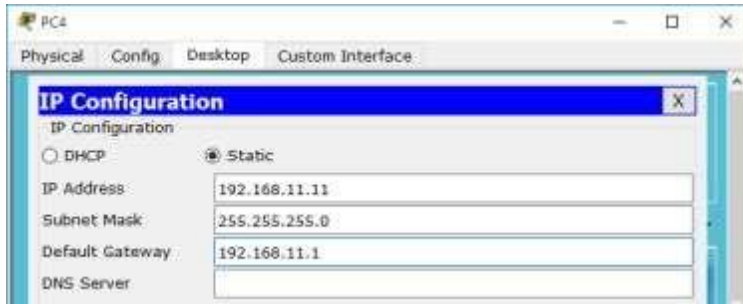
Verificamos la conectividad entre PC3 y S2



Problema Conectividad entre PC1 y PC4

a. Implementar Solución



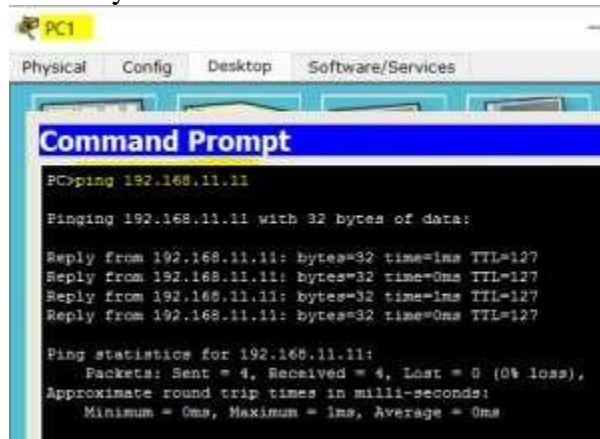


b. Verificar solución

Revisamos la configuración IP del PC4 para asegurarnos que haya quedado correcta



Probamos conectividad entre PC1 y PC4



Problema conectividad entre PC3 y S1:

a. Implementar solución

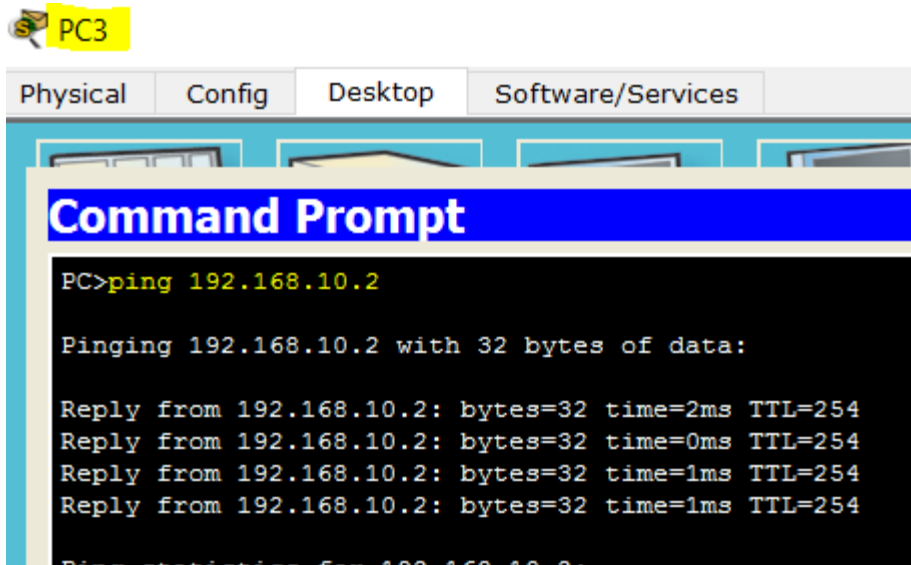
Activando el modo de Config en la Consola de línea de comandos CLI, indicamos que vamos a configurar la interfase VLAN1 y con el comando “configure terminal” y posteriormente con el comando “ip default-gateway” asignamos dirección IP del default Gateway

IOS Command Line Interface

```
Press RETURN to get started.  
  
S1>enable  
S1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
S1(config)#ip default-gateway 192.168.10.1  
S1(config)#exit  
S1#  
%SYS-5-CONFIG_I: Configured from console by console  
  
S1#
```

Copy Paste

c. Verificar solución



Paso 3: Verificar si se resolvieron todos los problemas

Una vez hechos todos los ajustes del caso, se encuentran resueltos todos los problemas de conectividad.

Una vez hechos todos los ajustes, la tabla de direccionamiento es:

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.1 0.1	255.255.255.0	No aplicable
	G0/1	192.168.1 1.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.1 0.2	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.1 1.2	255.255.255.0	192.168.11.1
PC1	NIC	192.168.1 0.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.1 0.11	255.255.255.0	192.168.10.1
PC3	NIC	192.168.1 1.10	255.255.255.0	192.168.11.1
PC4	NIC	192.168.1 1.11	255.255.255.0	192.168.11.1

Tabla de calificación sugerida

Tarea	Posibles puntos	P obt
Completar el registro de la red	20	
Documentar los problemas y las soluciones	45	
Puntuación de Packet Tracer (problemas resueltos)	35	
Puntuación total	100	

< >

Time Elapsed: 02:26:16 Completion: 35/35

Top >

Activity Results

Time Elapsed: 02:27:03

Congratulations Margarita Guerrero! You completed the activity.

[Overall Feedback](#) [Assessment Items](#) [Connectivity Tests](#)

Congratulations! You successfully completed the **Packet Tracer - Troubleshooting Default Gateway Issues** activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.

Close

COMENTARIOS

La utilidad del ping se hace evidente en la detección y solución de problema de conectividad al interior de las redes. Con esta herramienta fue posible identificar los problemas que planteaba el laboratorio y posteriormente verificar su solución.

Para la configuración tanto de routers como de switches se hace indispensable el dominio de IOS, en su interfaz de línea de comandos CLI.

Para que una red cumpla con su objetivo de intercomunicación entre terminales es indispensable que todos y cada uno de sus componentes se encuentre debidamente configurado.

Parte 2: Crear una configuración básica del switch

Paso 1: Asigne un nombre al switch

```
!
line vty 0 4
  login
line vty 5 15
  login
!
!
end

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

s1#
```

Cony Paste

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

Porque se requiere el comando login? = para que funcione el proceso de control para las contraseña

```
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

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

s1#
```

Cony Paste

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

```
s1#
%SYS-5-CONFIG_I: Configured from console by console
s1#exit

s1 con0 is now available

Press RETURN to get started.

Press RETURN to get started.

User Access Verification
Password:
s1>
```

Paso 4: Proporcionar un acceso seguro al modo privilegiado.

```
User Access Verification
Password:

s1>enable
s1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
s1(config)#enable password cisco
s1(config)#exit
s1#
%SYS-5-CONFIG_I: Configured from console by console
s1#
```

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

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

```
User Access Verification
```

```
Password: |
```

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

```
User Access Verification
```

```
Password:
```

```
s1>|
```

```
s1#show run
Building configuration...

Current configuration : 1088 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname s1
!
enable password cisco
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
```



```
.
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
!
!
!
line con 0
  password letmein
  login
!
line vty 0 4
  login
line vty 5 15
  login
!
!
end

s1#
```

Copy

Paste

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

```
!
line vty 0 4
  login
line vty 5 15
  login
!
!
end

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

s1#
```

Copy

Paste

Paso 7: Verificar si la contraseña secreta de enable se agregó al archivo de configuración. Que se muestra como contraseña secreta de enable = $\$1\$mERr\$ILwq/b7kc.7x/ejA4Aosn0$ Porque la contraseña secreta de enable se ve diferente de lo que se configuro = Enable secret esta encriptado, y la contraseña de enable aparece en texto no cifrado.

```

s1#show run
Building configuration...

Current configuration : 1135 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 cisco
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!

```

```

!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
!
!
!
line con 0
  password letmein
  login
!
line vty 0 4
  login
line vty 5 15
  login

```

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

Si configura mas contraseñas en el switch ¿se mostraran como texto no cifrado o en forma encriptada en el archivo de configuración ¿ porque ¿ =

Este comando service password-encryption es el encargado de encriptar todas las contraseñas inclusive las futuras

```

Current configuration : 1135 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 cisco
!
!

```

Parte 3: Configurar un título de MOTD

Paso 1: Configurar un mensaje del día (MOTD)

Cuando se muestra este mensaje configured from console by console = cuando se accede al switch por el puerto de consola.

Porque todos los switches deben tener un mensaje MOTD ? = Para advertir a los usuarios que el acceso esta prohibido no están autorizados y para enviar mensajes al personal y técnicos de red.

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

s1#
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

s1#
```

Conv

Paste

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

Cual es la versión abreviada mas corta del comando copy running-config startup-config? Cop r s

```
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
banner motd ~Cthis is a secure system. authorized access only~C
!
!
!
line con 0
  password letmein
  login
!
line vty 0 4
  login
line vty 5 15
  login
!
!
end

s1#
```

Paso 3 Examinar el archivo de configuración de inicio

Que comando muestra el contenido de la NVRAM ? = Show startup-configuration.

Todos los cambios realizados están gravados en el archivo ? = SI

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

s1#
s1#
s1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
s1#
```

Copy Paste

Parte 5: Configurar el S2

```
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
```

```
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

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

s2#
```

```
s2 con0 is now available
```

```
Press RETURN to get started.
```

```
User Access Verification
```

```
Password: |
```

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

```
User Access Verification
```

```
Password:
```

```
s2>enable
```

```
s2#configure terminal
```

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

```
s2(config)#enable password cisco
```

```
s2(config)#exit
```

```
s2#
```

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

```
s2#|
```

```
s2#show run
```

```
Building configuration...
```

```
Current configuration : 1088 bytes
```

```
!
```

```
version 12.2
```

```
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
```

```
no service password-encryption
```

```
!
```

```
hostname s2
```

```
!
```

```
enable password cisco
```

```
!
```

```
!
```

```
!
```

```
!
```

```
spanning-tree mode pvst
```

```
!
```

```
interface FastEthernet0/1
```

```
!
```

```
interface FastEthernet0/2
```

```
!
```

```
interface FastEthernet0/3
```

```
!
```

```
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

s2#show run
Building configuration...

Current configuration : 1135 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname s2
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password cisco
!
!
!
s2#
s2#config t
Enter configuration commands, one per line. End with CNTL/Z.
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)#banner motd "acceso autorizado unicamente . unauthorized 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

s2#
```

Press RETURN to get started.

```
acceso autorizado unicamente . unauthorized access is prohibited and violators
will be prosecuted to the full extent of the law
```

User Access Verification

Password:

PT Activity: 03:53:11

Packet Tracer: Configuración de los parámetros iniciales del switch

Objetivos

- Parte 1: Verificar la configuración predeterminada del switch
- Parte 2: Establecer una configuración básica del switch
- Parte 3: Configurar un título de MOTD
- Parte 4: Guardar los archivos de configuración en la NVRAM

Time Elapsed: 03:53:11 Completion: 72/72

Top

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points
[-] Network		
[-] S1		
✓ Banner MOTD	Correct	6
[-] Console Line		
✓ Login	Correct	4
✓ Password	Correct	4
✓ Enable Password	Correct	4
✓ Enable Secret	Correct	4
✓ Host Name	Correct	5
✓ Service Password Encry...	Correct	4
✓ Startup Config	Correct	5
[-] S2		
✓ Banner MOTD	Correct	6
[-] Console Line		
✓ Login	Correct	4
✓ Password	Correct	4
✓ Enable Password	Correct	4
✓ Enable Secret	Correct	4
✓ Host Name	Correct	5
✓ Service Password Encry...	Correct	4
✓ Startup Config	Correct	5

Score : 72/72
Item Count : 16/16

Component	Items/Total	Score
Basic Security Configuration	12/12	52/52
Configuration Management	2/2	10/10
Hostname Configuration	2/2	10/10

Implementación de conectividad básica

Realizar una configuración básica en S1 y S2

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

```
Cisco IOS Software, C2960 Software (C2960-LANBASE-K), Version 12.2(25)FX, RELEASE  
Copyright (c) 1986-2005 by Cisco Systems, Inc.  
Compiled Wed 12-Oct-05 17:05 by pt_team  
  
Press RETURN to get started!  
  
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up  
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up  
  
Switch>enable  
Switch#config ter  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#hostname S1  
S1(config)#
```



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

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed s  
up  
  
Switch>enable  
Switch#config ter  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#hostname S1  
S1(config)#line console 0  
S1(config-line)#password cisco  
S1(config-line)#login  
S1(config-line)#exit  
S1(config)#enable password class  
S1(config)#exit  
S1#  
%SYS-5-CONFIG_I: Configured from console by console  
  
S1#
```

Paso 3: Verificar S1.

¿Cómo pued
Time Elapsed: 00:
Top Check Re

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

Como puedo verificar que ambas contraseñas se hayan configurado correctamente?

Cuando salimos del modo EXEC del usuario el switch pide contraseña para entrar a la interfaz de consola y pide una contraseña por segunda vez para ingresar al modo EXEC privilegiado

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

Current configuration : 1086 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
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
--More-- |
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
!
!
!
line con 0
  password cisco
  login
!
line vty 0 4
  login
line vty 5 15
  login
!
!
end

S1#
```

Paso 4: Configurar un mensaje del día (MOTD)

```
S1(config)#banner motd " acceso autorizado unicamente. los infractores se
procesaran en la medida en que lo permita la ley"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Copy

Paste

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

Que comando emite para realizar este paso ?

S1 (config) # exit

S1 # copy run start

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

Copy

Paste

S1 con0 is now available

Press RETURN to get started.

acceso autorizado unicamente. los infractores se procesaran en la medida en que lo permita la ley

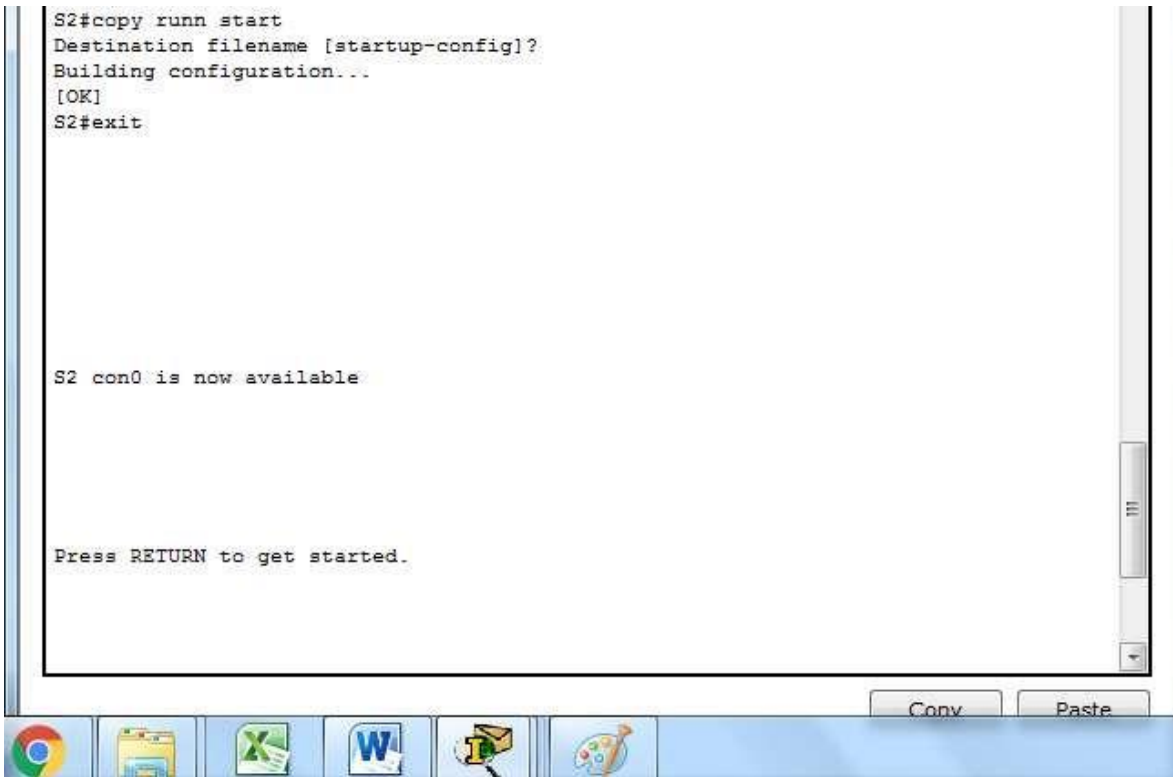
User Access Verification

Password:

S1>

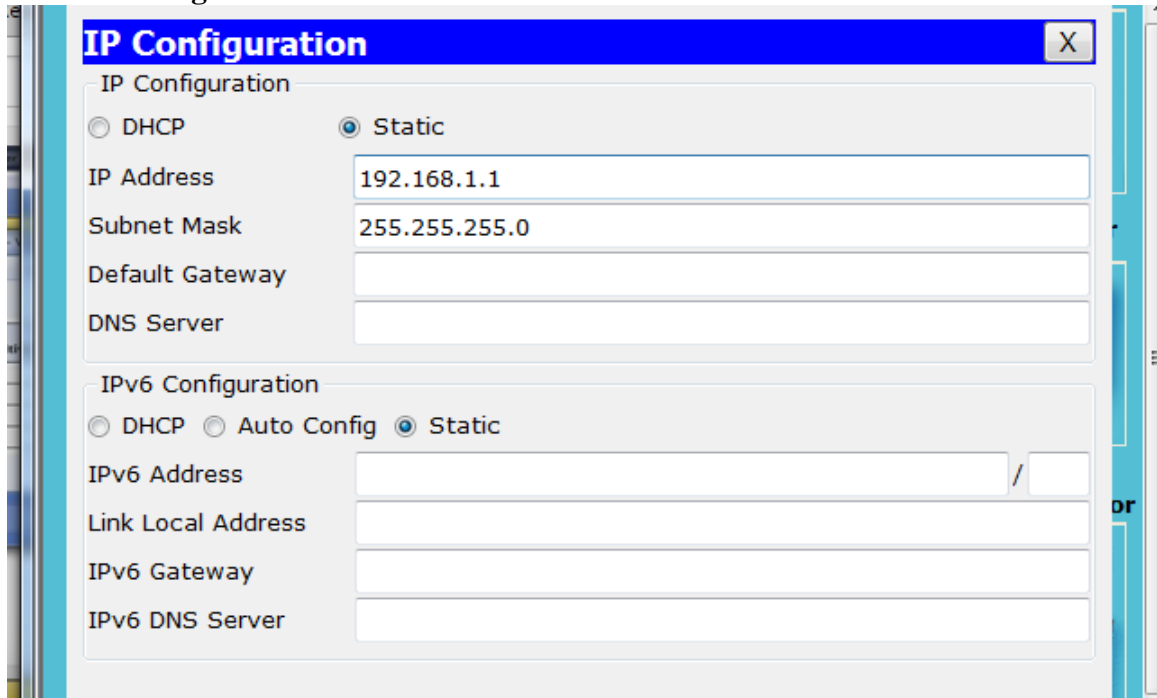
Paso 6: Repita los pasos 1 a 5 en S2.

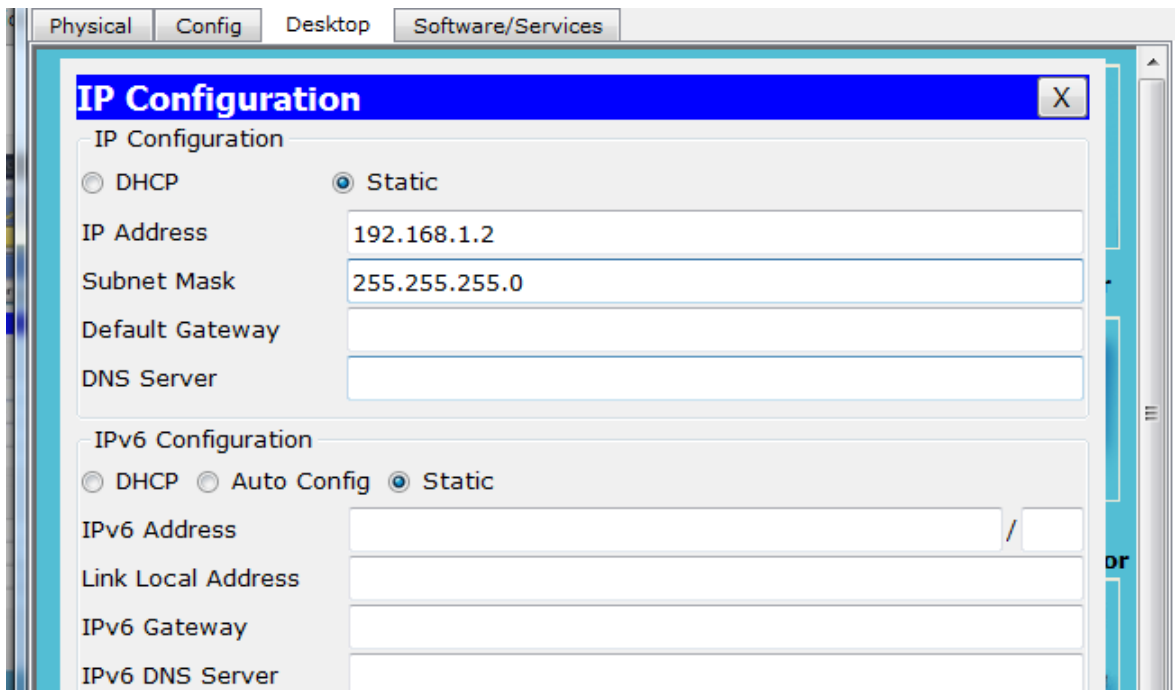
```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#enable password class
S2(config)#banner motd "acceso autorizado unicamente.los infractores se procesaran
en la medida en que lo permita la ley"
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```



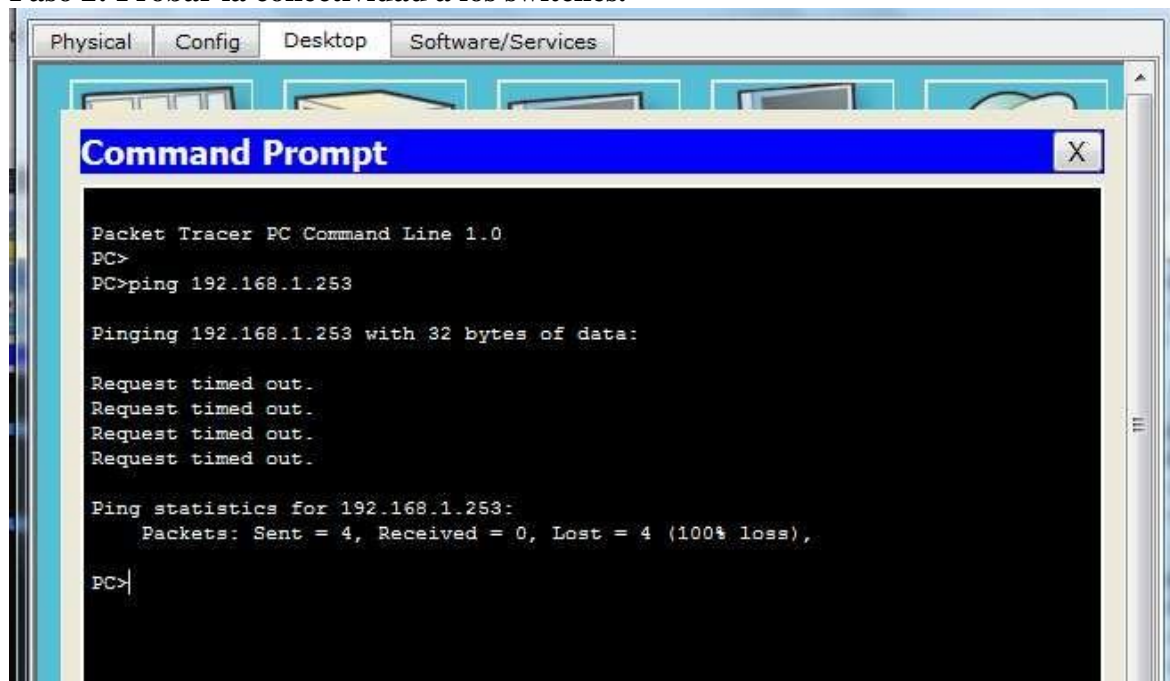
Paso 2: Configurar la PC

Paso 1: Configurar ambas PC con direcciones IP.





Paso 2: Probar la conectividad a los switches.



Tuvo éxito ? porque o porque no ?

Aún no están configurado los switches no se configuro una dirección IP

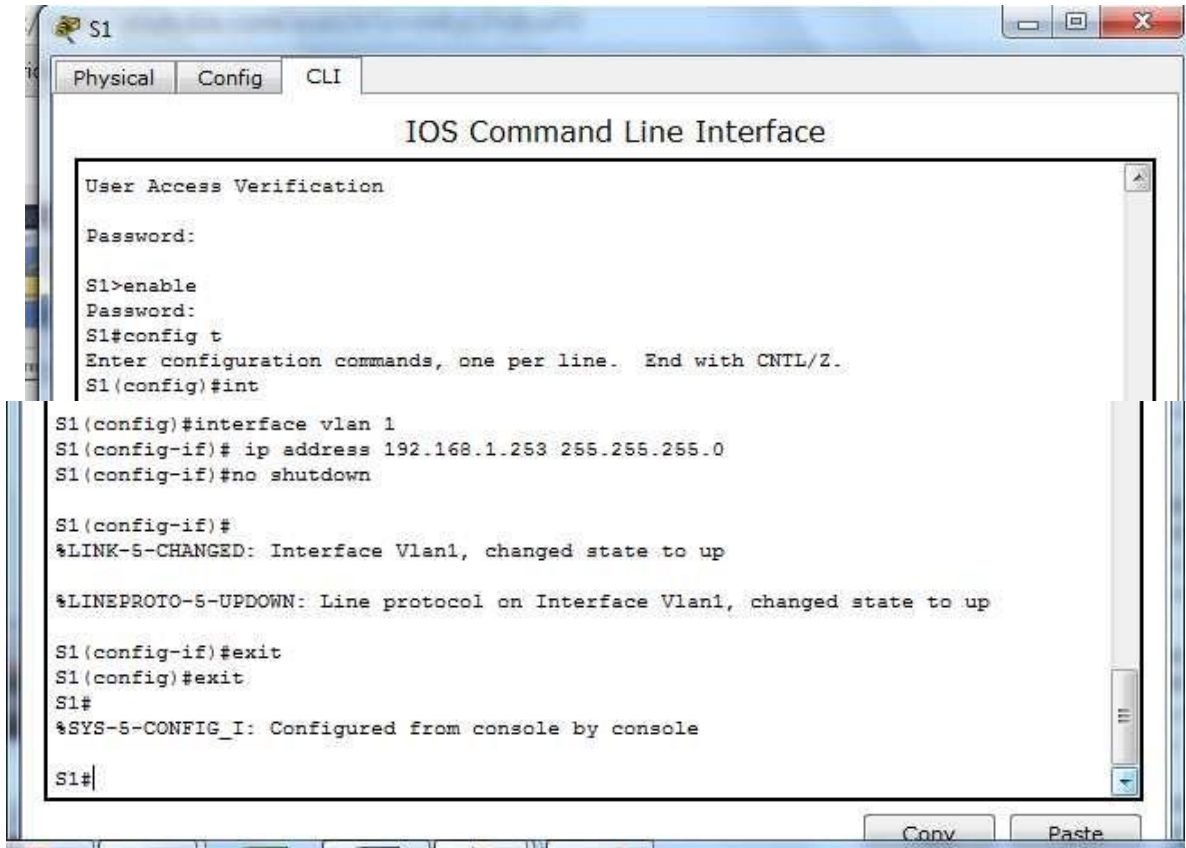
Parte 3: Configurar la interfaz de administración de switches

Paso 1: Configurar S1 con una dirección IP.

Para que lo configuramos con una dirección IP ?

Es indispensable asignar un dirección IP, para conectarse de forma remota , el switch esta configurado de manera predeterminada para su administración se realiza a través de VLAN 1. Porque debe introducir el comando no shutdown?

Habilita administrativamente el estado activo de la interfaz



```
S1
Physical Config CLI
IOS Command Line Interface
User Access Verification
Password:
S1>enable
Password:
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int
S1(config)#interface vlan 1
S1(config-if)# ip address 192.168.1.253 255.255.255.0
S1(config-if)#no shutdown

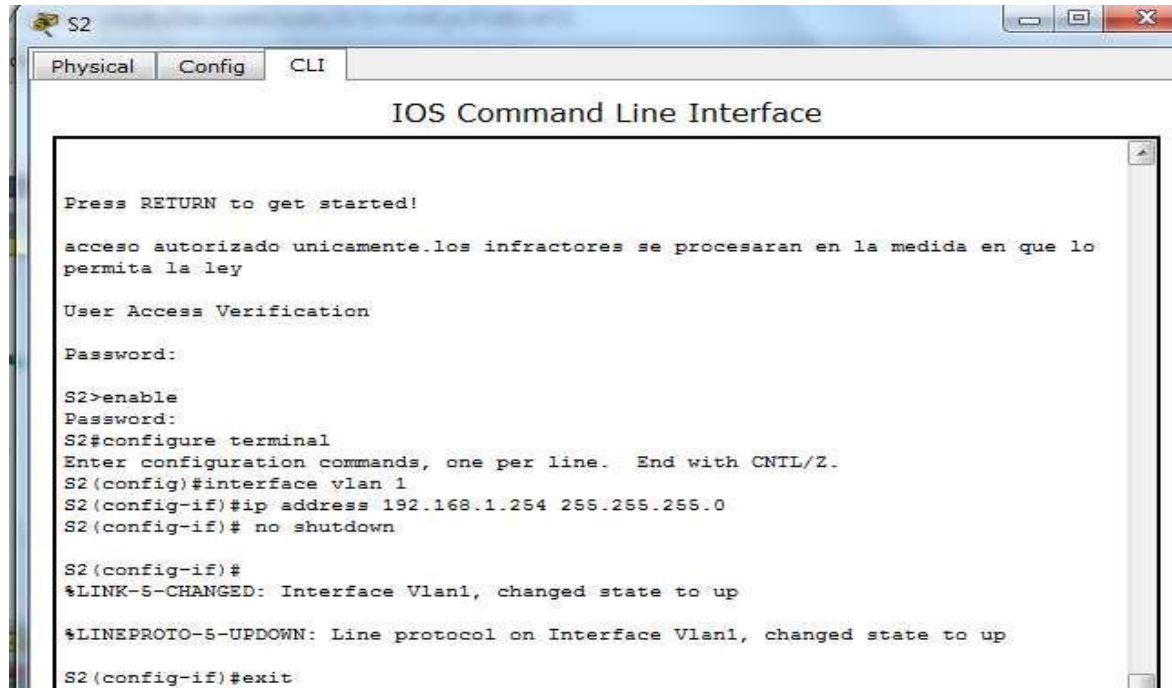
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

PASO 2 : CONFIGURAR EL S2 CON UNA DIRECCION IP



```
S2
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started!

acceso autorizado unicamente. los infractores se procesaran en la medida en que lo
permite la ley

User Access Verification

Password:

S2>enable
Password:
S2#configure terminal
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

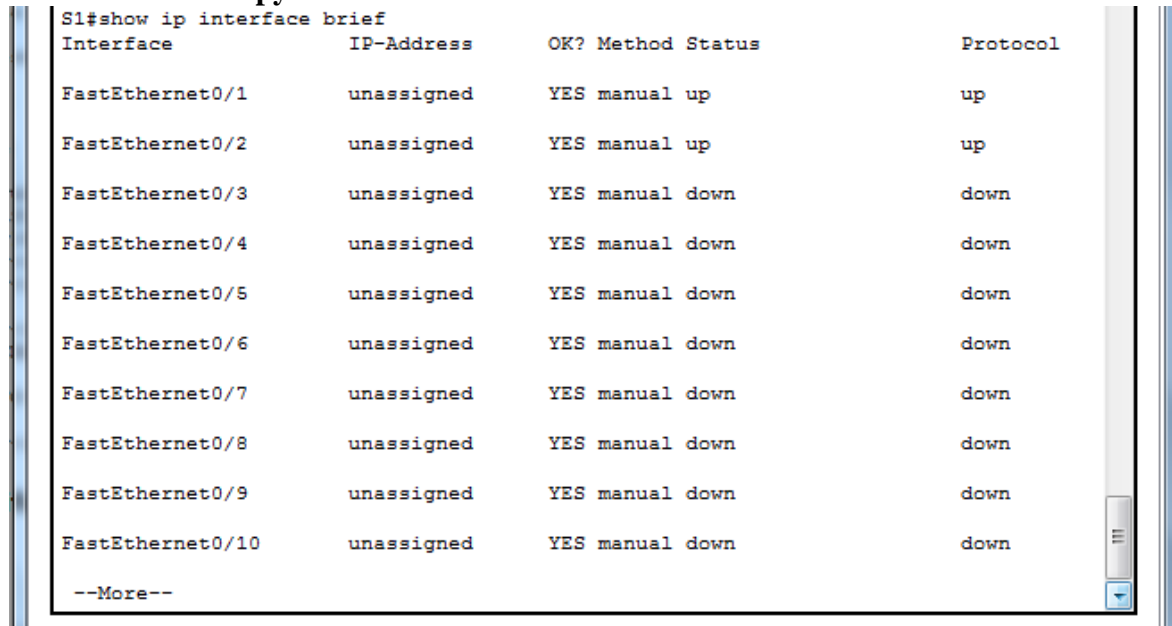
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#exit
```

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

Paso 4 : Guardar la configuración para el s1 y el s2 en la NVRAM

Que comando se utiliza para guardar en la NVRAM el archivo de configuración que se encuentra en la RAM ? = Copy run start



```
S1#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

--More--
```

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	192.168.1.253	YES manual	up	up

S1#

Paso 5. Verificar la conectividad de red.

```

PC>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.253: bytes=32 time=0ms TTL=255
Reply from 192.168.1.253: bytes=32 time=0ms TTL=255
Reply from 192.168.1.253: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>

```

```
Pinging 192.168.1.253 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.253: bytes=32 time=0ms TTL=255
Reply from 192.168.1.253: bytes=32 time=0ms TTL=255
Reply from 192.168.1.253: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

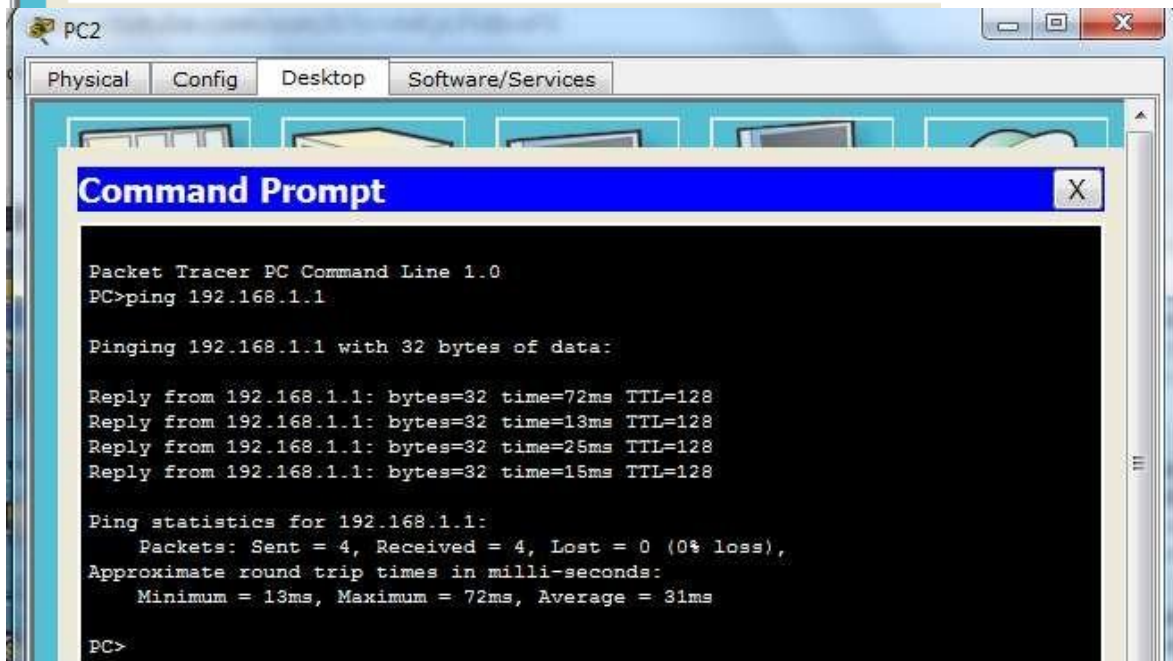
PC>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Reply from 192.168.1.253: bytes=32 time=3ms TTL=255
Reply from 192.168.1.253: bytes=32 time=11ms TTL=255
Reply from 192.168.1.253: bytes=32 time=13ms TTL=255
Reply from 192.168.1.253: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 6ms

PC>
```




```

Physical  Config  Desktop  Software/Services

Command Prompt
PC>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Reply from 192.168.1.253: bytes=32 time=3ms TTL=255
Reply from 192.168.1.253: bytes=32 time=11ms TTL=255
Reply from 192.168.1.253: bytes=32 time=13ms TTL=255
Reply from 192.168.1.253: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 6ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=26ms TTL=128
Reply from 192.168.1.2: bytes=32 time=13ms TTL=128
Reply from 192.168.1.2: bytes=32 time=14ms TTL=128
Reply from 192.168.1.2: bytes=32 time=13ms 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 = 13ms, Maximum = 26ms, Average = 16ms
  
```

Logical [Root] New Cluster Move Object Set Tied Background Viewport

PT Activity: 01:51:31

Packet Tracer: Implementación de conectividad básica

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

Time Elapsed: 01:51:31 Completion: 88/88

Top Check Results Reset Activity < 1/1 >

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

Assessment Item	Status	Points	Component(s)	Feedback
PC1				
Ports				
FastEthernet0				
IP Address	Correct	10	IPv4 Host Add.	
Subnet M.	Correct	2	IPv4 Host Add.	
PC2				
Ports				
FastEthernet0				
IP Address	Correct	10	IPv4 Host Add.	
Subnet M.	Correct	2	IPv4 Host Add.	
S1				
Banner MOTD	Correct	1	Basic Security	
Console Line				
Login	Correct	1	Basic Security	
Password	Correct	1	Basic Security	
Enable Secret	Correct	1	Basic Security	
Host Name	Correct	1	Hostname Conf.	
Ports				
Vlan1				
IP Address	Correct	5	IPv4 Host Add.	
Port Status	Correct	10	IPv4 Host Add.	

Score : 88/88
Item Count : 22/22

Component	Items/Total
Basic Security Configuration	8/8
Configuration Management	2/2
Hostname Configuration	2/2
IPv4 Host Address Configuration	10/10

PRACTICA 1

Packet Tracer: representación de la red

Objetivos

Parte 1: Descripción general del programa Packet Tracer

Parte 2: Exploración de LAN, WAN e Internet

Parte 1: Descripción general del programa Packet Tracer

El tamaño de la red es mayor que la mayoría de las redes con las que trabajará en este curso (si bien verá esta topología a menudo en sus estudios de Networking Academy). Es posible que deba ajustar el tamaño de la ventana de Packet Tracer para

ver la red completa. De ser necesario, puede utilizar las herramientas Acercar y Alejar para ajustar el tamaño de la ventana de Packet Tracer.

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)?

Se puede configurar la dirección IP, la máscara de subred, servidor DNS y la puerta por defecto (Gateway).

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:

- En la ficha OSI Model (Modelo OSI), ¿cuántas In Layers (Capas de entrada) y Out Layers (Capas de salida) 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?
- Alterne entre las fichas Inbound PDU Details y Outbound PDU Details. ¿Observa cambios en la información? Si es así, ¿qué es lo que cambia?.

Parte 2: Exploración de LAN, WAN e Internet

El modelo de red en esta actividad incluye muchas de las tecnologías que llegará a dominar en sus estudios en CCNA y representa una versión simplificada de la forma en que podría verse una red de pequeña o mediana empresa. Explore la red por su cuenta con libertad. Cuando esté listo, siga estos pasos y responda las preguntas.

Paso 1: Identificar los componentes comunes de una red según se los representa en Packet Tracer

- a. La barra de herramientas de íconos tiene diferentes categorías de componentes de red. Debería ver las categorías que corresponden a los dispositivos intermediarios, los dispositivos finales y los medios. La categoría **Connections** (Conexiones, cuyo ícono es un rayo) representa los medios de red que admite Packet Tracer. También hay una categoría llamada **End Devices** (Dispositivos finales) y dos categorías específicas de Packet Tracer: **Custom Made Devices** (Dispositivos personalizados) y **Multiuser Connection** (Conexión multiusuario).
- b. Enumere las categorías de los dispositivos intermediarios.

Los dispositivos intermediarios en la red son:

- Switches
- Routers
- Hubs
- Dispositivos inalámbricos
- Wan

- c. Sin ingresar en la nube de Internet o de intranet, ¿cuántos íconos de la topología representan dispositivos terminales (solo una conexión conduce a ellos)?

Son 13 dispositivos terminales.

- d. Sin contar las dos nubes, ¿cuántos íconos de la topología representan dispositivos intermediarios (varias conexiones conducen a ellos)?

Son 11 dispositivos intermedios.

- e. ¿Cuántos de esos dispositivos intermediarios son routers? Nota: el dispositivo Linksys es un router.

Son 5 router que están dentro de los dispositivos intermedios.

- f. ¿Cuántos dispositivos finales **no** son computadoras de escritorio?

Ochos dispositivos finales

- g. ¿Cuántos tipos diferentes de conexiones de medios se utilizan en esta topología de red?

Existen cuatro tipos de conexiones: coaxial, serial DTE, cable directo e inalámbrica.

- h. ¿Por qué no hay un ícono de conexión para la tecnología inalámbrica en la categoría Connections?

No se puede realizar una conexión física del inalámbrico de eso se encarga el dispositivo utilizado, pues activa el enlace físico.

Paso 2: Explicar la finalidad de los dispositivos.

a. En Packet Tracer, el dispositivo Server-PT puede funcionar como servidor. Las computadoras de escritorio y portátiles no pueden funcionar como servidores. ¿Esto sucede en el mundo real? Según lo que estudió hasta ahora, explique el modelo cliente-servidor.

Es una arquitectura que permite el acceso a usuarios finales. El proceso se inicia cuando el cliente envía un mensaje por un determinado servicio a un servidor el cual usa TCP/IP como transporte y este devuelve la respuesta.

b. Enumere, al menos, dos funciones de los dispositivos intermediarios.

- Volver a generar y transmitir las señales de datos.
- Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace.

c. Enumere, al menos, dos criterios para elegir un tipo de medio de red.

- La distancia por la que los medios pueden transportar una señal correctamente.
- El costo del medio y de la instalación
- La cantidad de datos y la velocidad a la que se deben transmitir
- El entorno en el que se instalan los medios.

Paso 3: Comparar redes LAN y WAN.

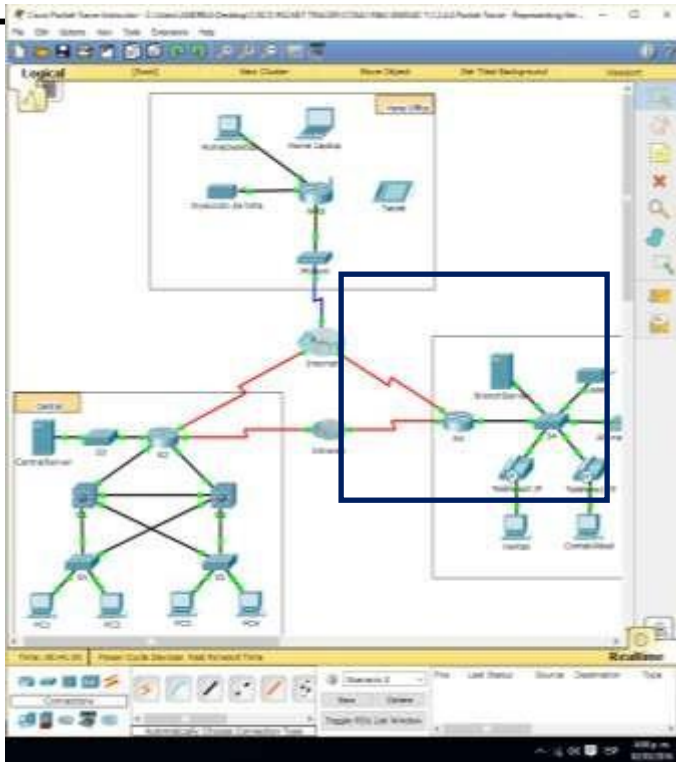
a. Explique la diferencia entre una LAN y una WAN, y dé ejemplos de cada una.

Se diferencia en que la LAN es una red de área local, es decir se usa en una única área geográfica a la cual se le conecta varios equipos y el alcance es limitado, en cambio la WAN son redes de área amplia, es decir para áreas más extensas geográficamente.

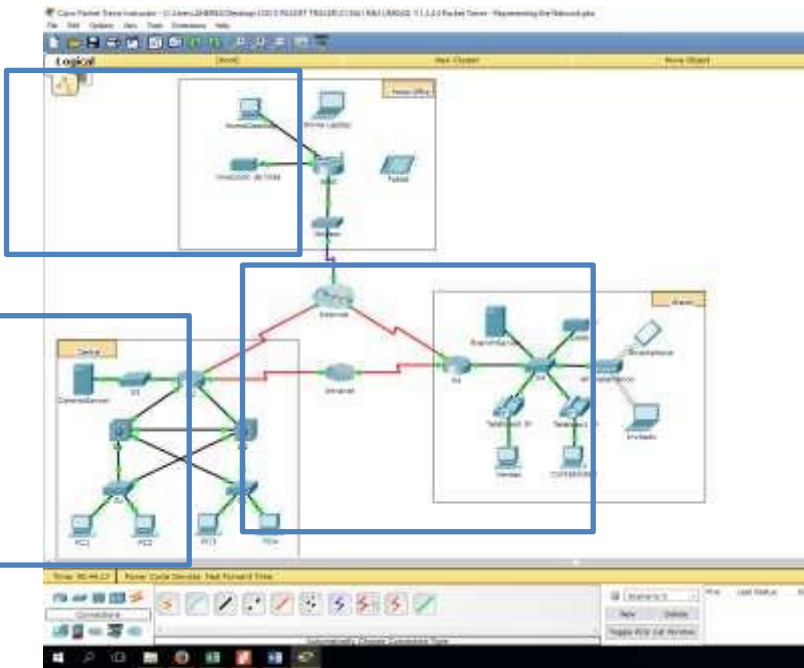
Un ejemplo de LAN es la red de una empresa y un ejemplo de WAN es la red de telefonía de un país.

b. ¿Cuántas WAN ve en la red de Packet Tracer?

Hay dos redes WAN una es la de internet y la de intranet.



c. ¿Cuántas LAN ve? Se ven tres redes LAN



d. En esta red de Packet Tracer, Internet está simplificada en gran medida y no representa ni la estructura ni la forma de Internet propiamente dicha. Describa Internet brevemente.

Internet es un conjunto de redes de comunicación que se encuentran conectadas mediante un grupo de protocolos.

e. ¿Cuáles son algunas de las formas más comunes que utiliza un usuario doméstico para conectarse a Internet?

Datos del celular, Dsl, wifi y por la red telefónica (Ethernet).

f. ¿Cuáles son algunas de las formas más comunes que utilizan las empresas para conectarse a Internet en su área?

Isp (empresa proveedora de servicios), red satelital, intranet y la Ethernet.

Revisión de la tabla ARP

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

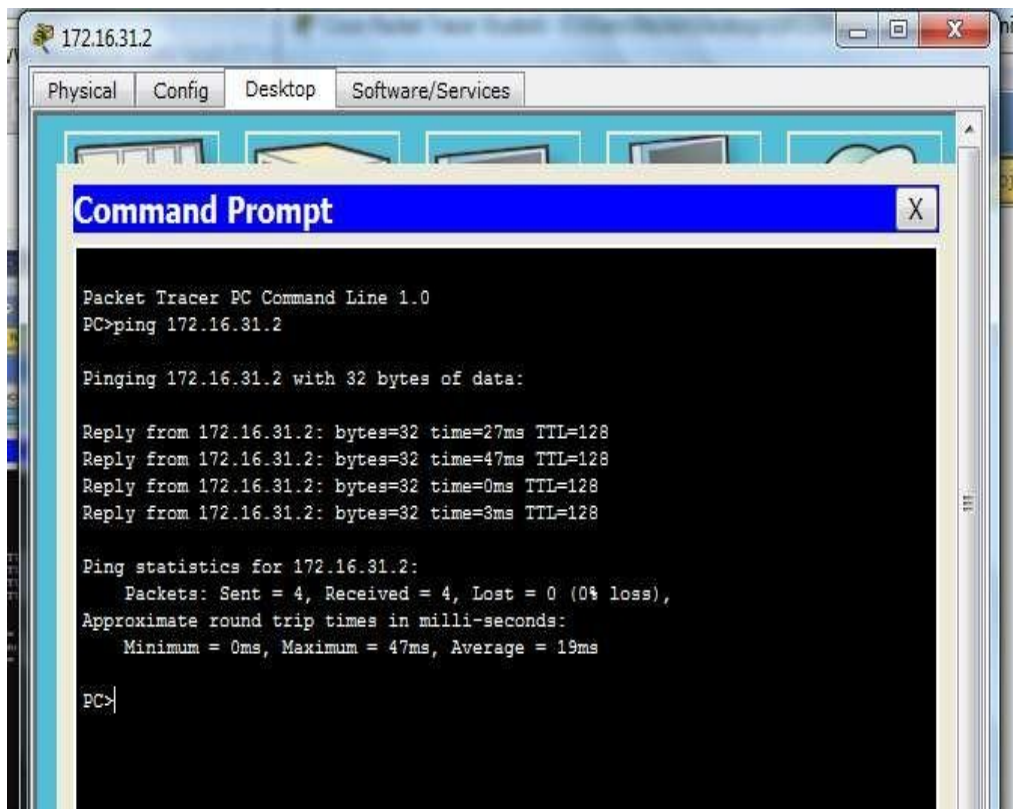
Haga clic en **Capture/Forward** (Capturar/avanzar) una vez. La PDU ARP mueve el **Switch1**, mientras que la PDU ICMP desaparece y espera la respuesta de ARP. Abra la PDU y registre la dirección MAC de destino. ¿Esta dirección se indica en la tabla anterior? NO

Haga clic en **Capture/Forward** (Capturar/avanzar) para mover la PDU al siguiente dispositivo. ¿Cuántas copias de la PDU realizó el **Switch1**? 3

¿Cuál es la dirección IP del dispositivo que aceptó la PDU? 172.16.31.3

Abra la PDU y examine la capa 2. ¿Qué sucedió con las direcciones MAC de origen y destino? El origen se transformó en el destino, FFFF.FFFF.FFFF se convirtió en la dirección MAC de 172.16.31.3

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? 1



```
172.16.31.2
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 172.16.31.2

Pinging 172.16.31.2 with 32 bytes of data:

Reply from 172.16.31.2: bytes=32 time=27ms TTL=128
Reply from 172.16.31.2: bytes=32 time=47ms TTL=128
Reply from 172.16.31.2: bytes=32 time=0ms TTL=128
Reply from 172.16.31.2: bytes=32 time=3ms TTL=128

Ping statistics for 172.16.31.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 47ms, Average = 19ms

PC>
```

Cisco Packet Tracer Student - C:\Users\Nestor\Desktop\DIPLOMADO\unidad uno\exercice\5.2.1.7 Packet Tracer - Examine the ARP Table.pka

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

Router0 Router1
Switch0 Switch1
Punto de acceso
10.10.10.2 10.10.10.3 172.16.31.2 172.16.31.3 172.16.31.4

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
<input checked="" type="checkbox"/>	0.000	--	172.16.31.2	ARP	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0.000	--	172.16.31.2	ICMP	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0.000	--	172.16.31.2	ARP	<input checked="" type="checkbox"/>

Reset Simulation Constant Delay Captured to: 0.000 s

Play Controls

Back Auto Capture / Play Capture / Forward

Event List Filters - Visible Events

Cisco Packet Tracer Student - C:\Users\Nestor\Desktop\DIPLOMADO\unidad uno\exercice\5.2.1.7 Packet Tracer - Examine the ARP Table.pka

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

Router0 Router1
Switch0 Switch1
Punto de acceso
10.10.10.2 10.10.10.3 172.16.31.2 172.16.31.3 172.16.31.4

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
<input type="checkbox"/>	0.000	--	172.16.31.2	ARP	<input checked="" type="checkbox"/>
<input type="checkbox"/>	0.000	--	172.16.31.2	ICMP	<input checked="" type="checkbox"/>
<input type="checkbox"/>	0.000	--	172.16.31.2	ARP	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0.001	172.16.31.2	Switch1	ARP	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0.001	--	172.16.31.2	ARP	<input checked="" type="checkbox"/>

Reset Simulation Constant Delay Captured to: 0.001 s

Play Controls

Back Auto Capture / Play Capture / Forward

Event List Filters - Visible Events

IF last event, capture then forward.

ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, FTP, H.323, HSRP, HSRPv6, HTTP

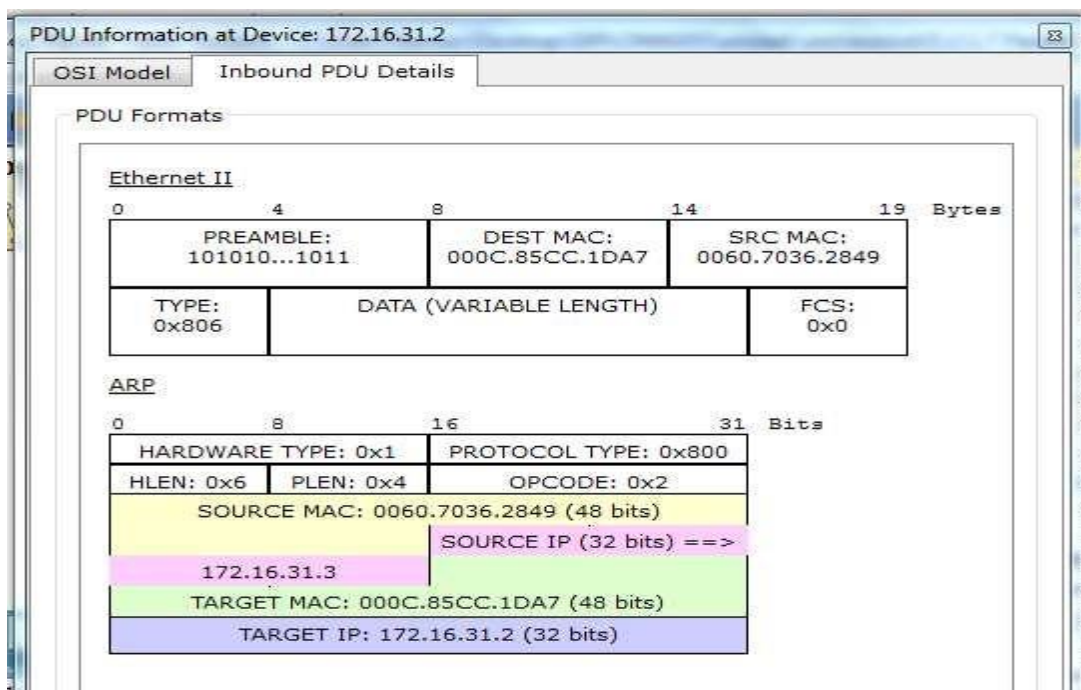
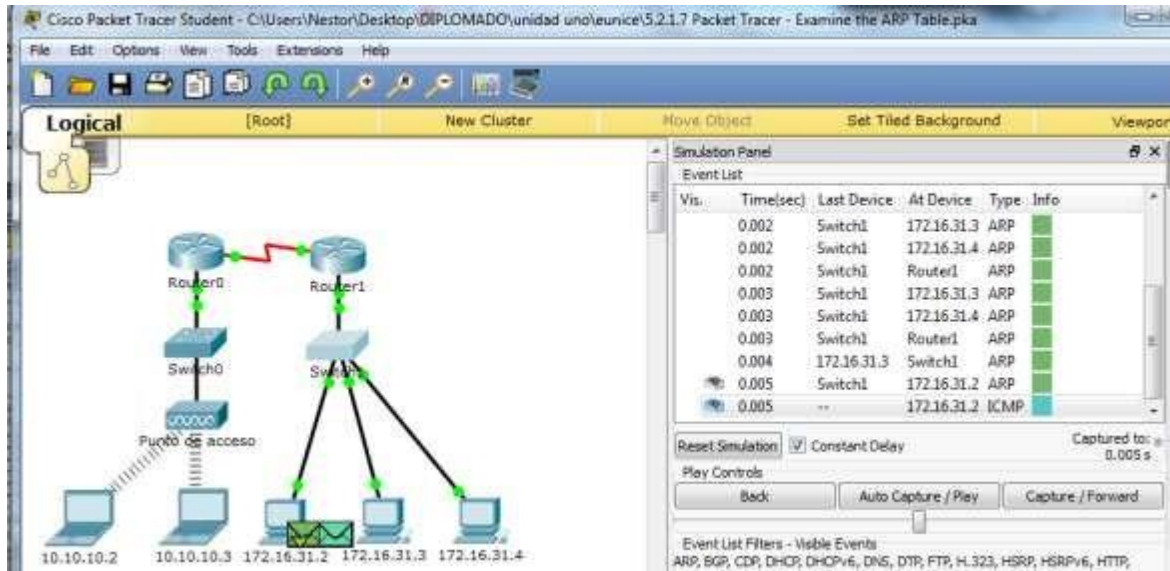
Paso 2: Revisar la tabla ARP

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? SI

Haga clic en **172.16.31.2** e introduzca el comando **arp -a**. ¿A qué dirección IP corresponde la entrada de la dirección MAC? 172.16.31.3

En general, ¿cuándo emite un dispositivo final una solicitud de ARP?

Cuando no conoce la dirección MAC del receptor



PDU Information at Device: 172.16.31.2

OSI Model Outbound PDU Details

PDU Formats

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0060.7036.2849		SRC MAC: 000C.85CC.1DA7	
TYPE: 0x800	DATA (VARIABLE LENGTH)			FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0		TL: 128		
ID: 0x9			0x0	0x0		
TTL: 128		PRO: 0x1	CHKSUM			
SRC IP: 172.16.31.2						
DST IP: 172.16.31.3						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

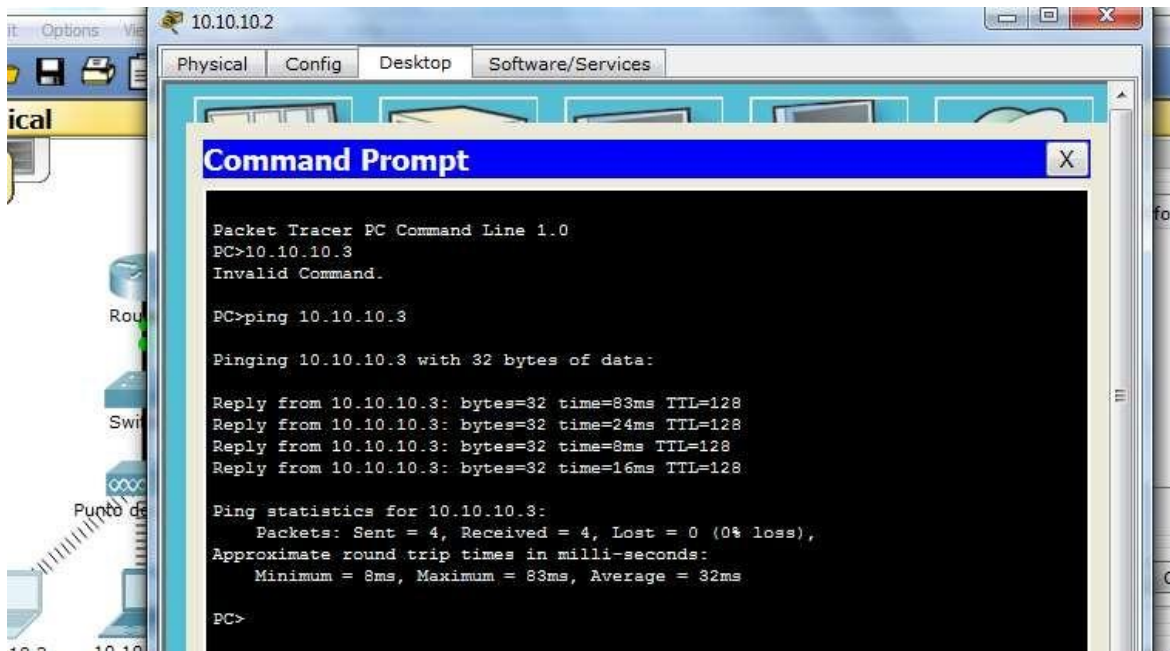
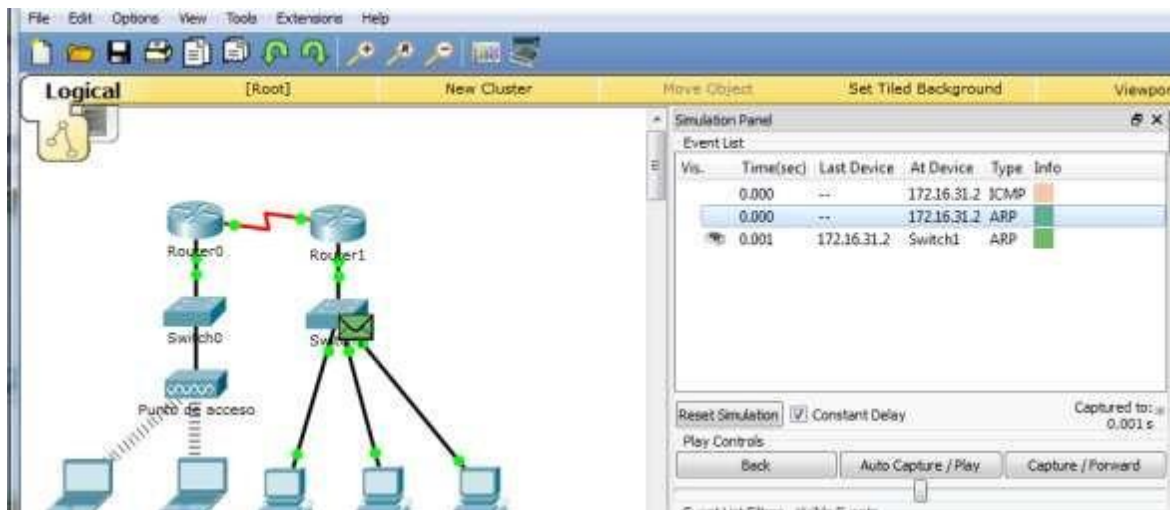
ICMP

0	8	16	31	Bits
---	---	----	----	------

Parte 2: Examinar una tabla de direcciones MAC del switch

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

Introduzca el comando **ping 10.10.10.3**. ¿Cuántas respuestas se enviaron y se recibieron? Se enviaron 4 se recibieron 4

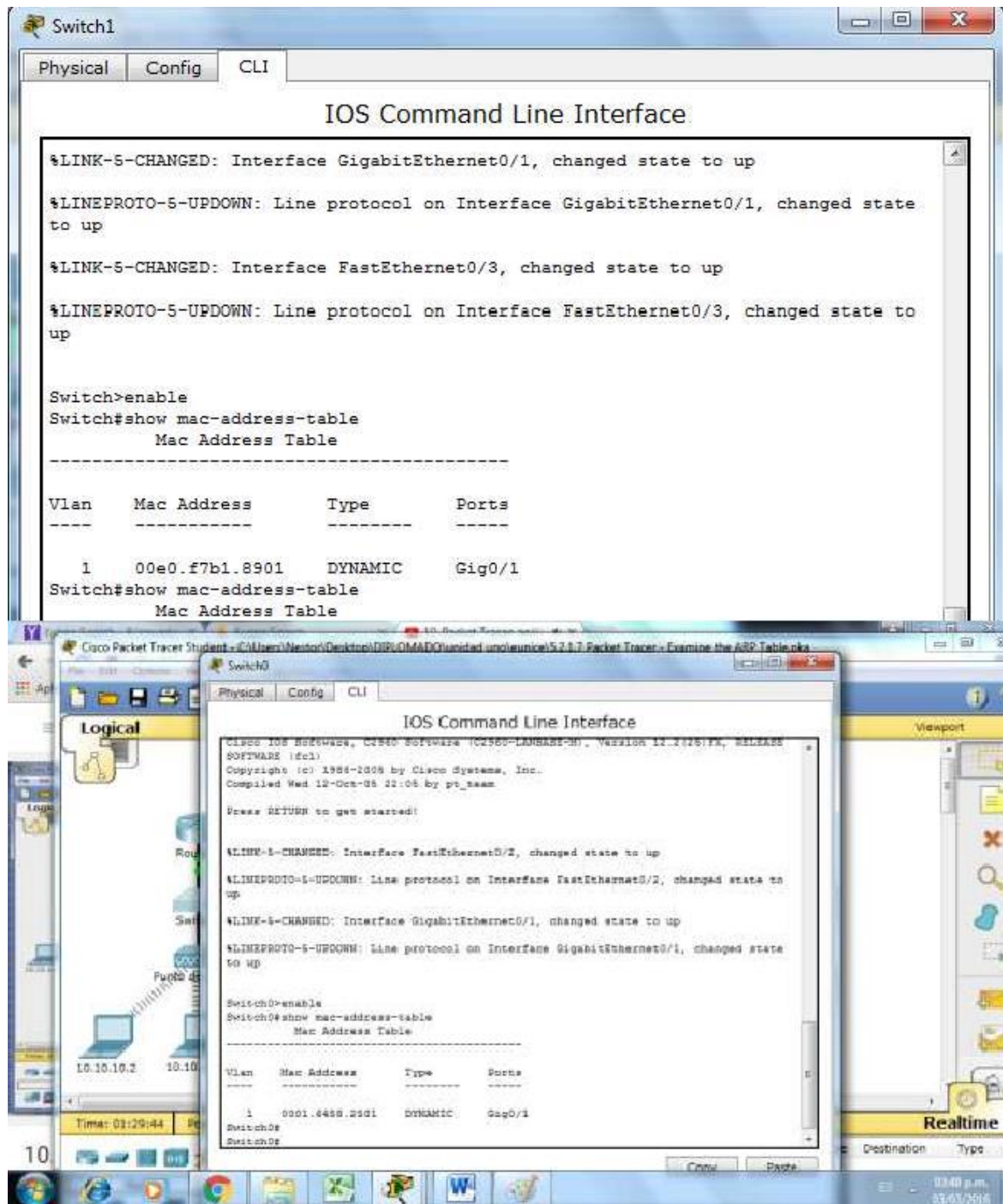


Paso 2: Examinar la tabla de direcciones MAC en los switches

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? SI

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? SI

¿Por qué hay dos direcciones MAC asociadas a un puerto? Ambos dispositivos se conectan a un puerto a través del punto de acceso.



Parte 3: Examinar el proceso de ARP en comunicaciones remotas

Paso 1: Generar tráfico para producir tráfico ARP

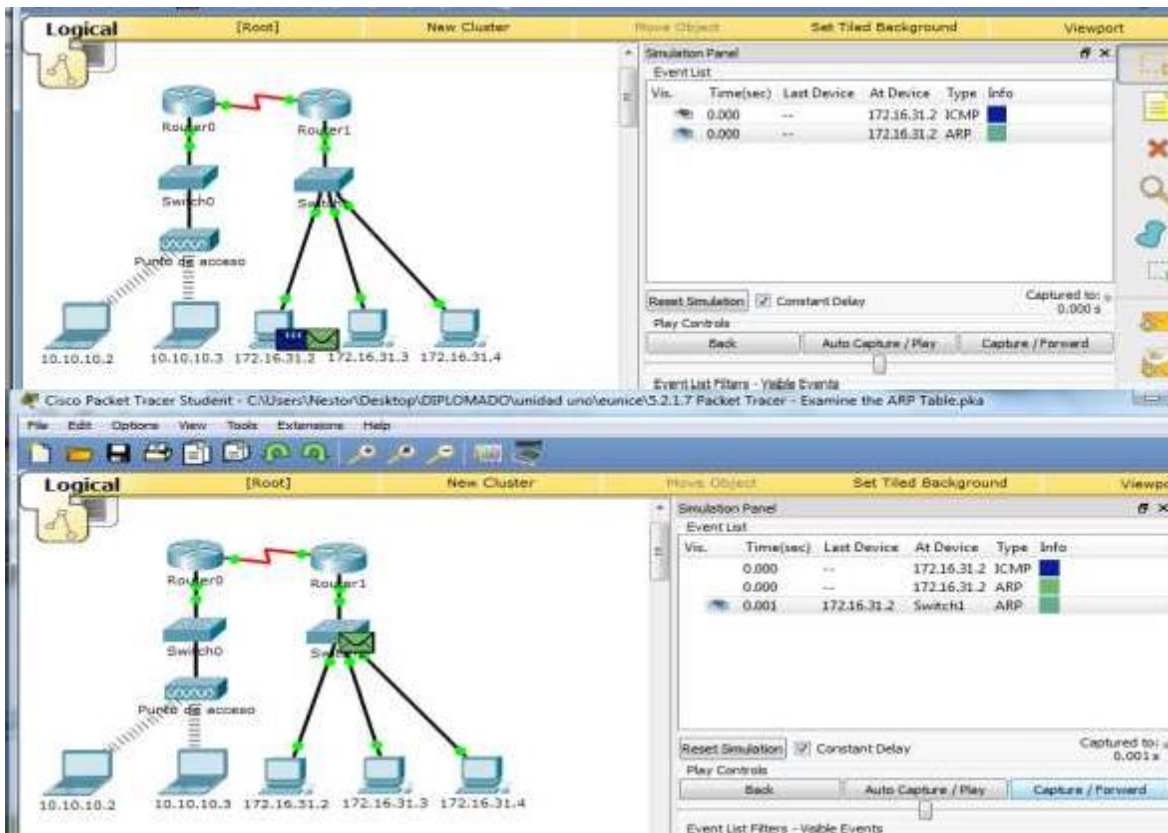
Repita el ping a 10.10.10.1. ¿Cuántas PDU aparecen? 2

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? 172.16.31.1

La dirección IP de destino no es 10.10.10.1. ¿Por qué? La dirección de Gateway de la interfaz del router se almacena en la configuración IPv4 de los hosts, si el host receptor no se encuentra en la misma red el origen utiliza el proceso ARP para determinar una dirección MAC.

```
Minimum = 4ms, Maximum = 59ms, Average = 21ms
PC>arp -d
PC>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
```



Paso 2: Examinar la tabla ARP en el Router1

Ingrese al modo EXEC privilegiado y, a continuación, introduzca el comando **show mac-address-table**. ¿Cuántas direcciones MAC figuran en la tabla? ¿Por qué? Ninguna este comando significa algo diferente al comando show mac address-table de un switch

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

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

Router1

Physical Config CLI

IOS Command Line Interface

```

adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.0.1 (Serial10/0/0) is down: holding
time expired
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.0.1 (Serial10/0/0) is up: new
adjacency
%DUAL-5-NBRCHANGE: IPv6-EIGRP 1: Neighbor FE80::206:2AFF:FE3E:1E01 (Serial10/0/0)
is down: Interface Goodbye received
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.0.1 (Serial10/0/0) is down:
Interface Goodbye received
%DUAL-5-NBRCHANGE: IPv6-EIGRP 1: Neighbor FE80::206:2AFF:FE3E:1E01 (Serial10/0/0)
is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.0.1 (Serial10/0/0) is up: new
adjacency

Router>enable
Router#show mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
-----

```

IOS Command Line Interface

```

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.0.1 (Serial10/0/0) is up: new
adjacency
%DUAL-5-NBRCHANGE: IPv6-EIGRP 1: Neighbor FE80::206:2AFF:FE3E:1E01 (Serial10/0/0)
is down: Interface Goodbye received
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.0.1 (Serial10/0/0) is down:
Interface Goodbye received
%DUAL-5-NBRCHANGE: IPv6-EIGRP 1: Neighbor FE80::206:2AFF:FE3E:1E01 (Serial10/0/0)
is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.0.1 (Serial10/0/0) is up: new
adjacency

Router>enable
Router#show mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
-----

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      3          000C.85CC.1DA7 ARPA   GigabitEthernet0/0
Router#

```

Topología

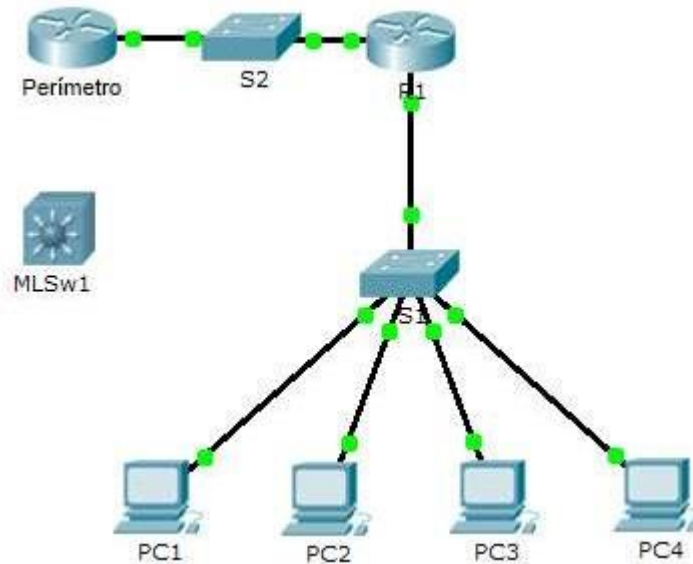


Tabla de direccionamiento

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

Objetivos

Parte 1: Documentar la configuración actual de la red

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

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. Trabaja después del horario laboral para minimizar los inconvenientes para la empresa.

Packet Tracer: Configuración de switches de capa 3

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**.

- Haga clic en **R1** y, a continuación, haga clic en la ficha **CLI**.
- Utilice los comandos disponibles para recopilar información sobre el direccionamiento de interfaces.



```
interface GigabitEthernet0/0
ip address 172.16.31.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.0.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
encapsulation ppp
clock rate 2000000
shutdown
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
--More--
```


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

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

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

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

- Haga clic en **MLSw1** y, a continuación, en la ficha **CLI**.
- Ingrese al modo de configuración de interfaz para **GigabitEthernet 0/1**.
- Cambie el puerto al modo de enrutamiento introduciendo el comando **no switchport**.
- Configure la dirección IP para que sea la misma que la dirección de **R1 GigabitEthernet 0/1** y active el puerto.
- Ingrese al modo de configuración de interfaz para **interface VLAN1**.
- Configure la dirección IP para que sea la misma que la dirección de **R1 GigabitEthernet 0/0** y active el puerto.
- Guarde la configuración.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int
Switch(config)#interface giga
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#no swit
Switch(config-if)#no switchport
Switch(config-if)#ip add
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)#
Switch(config-if)#int vlan1
Switch(config-if)#ip add
Switch(config-if)#ip address 172.16.31.1 255.255.255.0
Switch(config-if)#noshut
Switch(config-if)#noshut

% Invalid input detected at '^' marker.

Switch(config-if)#no shut
Switch(config-if)#no shutdown

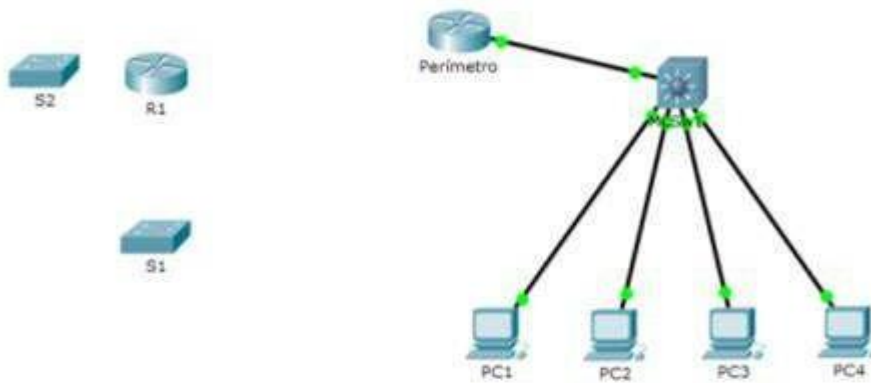
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

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**.
- 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.



```

PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=1ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
  
```

File Edit Options View Tools Windows Help

Activity Results

Time Elapsed: 00:41:33

Congratulations! You completed the activity.

Overall Feedback Assessment Details Connectivity Tests

Expand/Collapse All

Assessment Item	Status	Points	Component(s)	Feedback
network				
MCSA)				
Ports				
GigabitEthernet0/1				
IP Address	Correct	15	Layer 3 Switch	
Port Status	Correct	15	Device Interface	
Subnet M.	Correct	15	Layer 3 Switch	
Trunking	Correct	15	Layer 3 Switch	
Vlan1				
IP Address	Correct	15	Layer 3 Switch	
Port Status	Correct	15	Device Interface	
Subnet M.	Correct	15	Layer 3 Switch	
PC1				
Ports				
FastEthernet0/24				
Link to Hub/1	Correct	1	Physical Device Conn.	
Type	Correct	1	Other	
PC2				
Ports				
FastEthernet0/24				
Link to Hub/1	Correct	1	Physical Device Conn.	
Type	Correct	1	Other	
PC3				
Ports				
FastEthernet0/24				
Link to Hub/1	Correct	1	Physical Device Conn.	
Type	Correct	1	Other	
PC4				
Ports				
FastEthernet0/24				
Link to Hub/1	Correct	1	Physical Device Conn.	
Type	Correct	1	Other	

Score : 98/98

Item Count : 11/11

Component	Items/Total	Score
Device Connections	4/4	8/8
Device Interface Configuration	3/3	30/30
Layer 3 Switch Configuration	4/4	76/76

Close

CONCLUSIONES

El desarrollo de las temáticas para esta primera etapa como son Exploración de la red, Configuración de un sistema operativo de red, Protocolos y comunicaciones de red, Acceso a la red, Ethernet, Capa de red, fueron de gran importancia para el aprendizaje individual y consecutivamente grupal, por medio de la simulación y conceptualización de cada uno de los temas que cuenta esta primera unidad.

La iteración y socialización de los laboratorios en el foro propuesto para el desarrollo de las tareas fue de gran ayuda, pues nos fortalecimos unos a otros con el compromiso de adquirir nuevos conocimientos a partir de los informes expuestos por todos y cada uno de los miembros del grupo.

REFERENCIAS BIBLIOGRÁFICAS

Principios básicos de routing y switching: Traducción de direcciones de red para IPv4. (2017), Tomado de: <https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#11.0>

DHCP. Principios de Enrutamiento y Conmutación. (2014) Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

Es.wikipedia.org. (2018). Open Shortest Path First. [online] disponible en: https://es.wikipedia.org/wiki/Open_Shortest_Path_First [12 Dic 2018].