

## Laboratorio # 3

### Configuración básica de seguridad en un conmutador

**Fecha:** 14/6/2021

**Grupo:** -

**Integrantes:**

Natalia Ramírez Yépez

**Paralelo:** 107

**Profesor:** Ignacio Marín

**Tipo de trabajo:** ☐ Grupal ☒ Individual

#### Objetivo

Configurar los parámetros básicos de seguridad en un conmutador para la verificación de conectividad en una red LAN de manera correcta.

#### Duración

Ciento veinte (120) minutos.

#### Materiales y Herramientas

- Packet tracer 7.3
- Procesador de texto

#### Introducción

Las redes están formadas por tres equipos principales: *hosts*, conmutadores y enrutadores. En esta práctica de laboratorio, se configuran los parámetros básicos de seguridad en un conmutador, incluyendo el nombre del dispositivo, la descripción de interfaces, las contraseñas locales, el mensaje del día (MOTD), el direccionamiento IP, la configuración de una dirección MAC estática y la demostración del uso de una dirección IP de administración para la administración remota del conmutador.

También se mencionan los comandos *show* para mostrar la configuración en ejecución, la versión del *IOS* y el estado de la interfaz; y el comando *copy* para guardar las configuraciones de los dispositivos.

Además, se aplica direccionamiento IP a los *hosts* para habilitar la comunicación entre estos dispositivos. Finalmente, se usa el comando *ping* para verificar la conectividad.

#### Topología

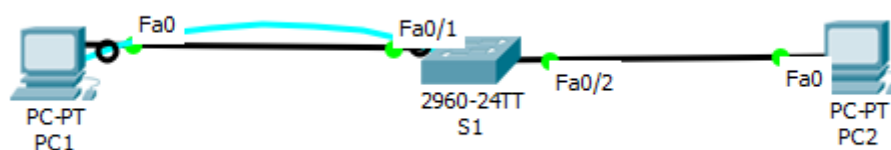


Figura 1. Topología de red.

## Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN99	192.168.30.2	255.255.255.0	192.168.30.1
PC1	NIC	192.168.30.10	255.255.255.0	192.168.30.1
PC2	NIC	192.168.30.11	255.255.255.0	192.168.30.1



Construya la topología de red de acuerdo con el gráfico mostrado anteriormente, conecte las PC al Conmutador según lo indicado en la topología.

## Procedimiento

### Actividad 1: Verificar la configuración predeterminada del conmutador.

En esta actividad, examinará la configuración predeterminada del conmutador, como la configuración actual, la información de IOS, las propiedades de las interfaces, información sobre VLAN, y la memoria flash. Todos los comandos IOS del conmutador se encuentran disponibles en el modo EXEC privilegiado.

Se restringirá el acceso al modo EXEC privilegiado a través de protección con contraseña para evitar el uso no autorizado, dado que proporciona acceso directo al modo de configuración global y a los comandos que se usan para configurar los parámetros de funcionamiento.

Las contraseñas serán establecidas más adelante en esta práctica de laboratorio.

- Partiendo del supuesto que el conmutador no cuenta con algún archivo de configuración almacenado en la memoria de acceso aleatorio no volátil (NVRAM), usted estará en la petición de entrada del modo EXEC del conmutador, con la petición de entrada **Switch>**. Use el comando **enable** para ingresar al modo EXEC privilegiado.



```
Switch> enable
Switch#
```

Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado. Verifique que el archivo de configuración esté limpio con el comando **show running-config** del modo EXEC privilegiado. Si se guardó un archivo de configuración anteriormente, se debe eliminar. Según cuál sea el modelo del conmutador y la versión del IOS, la configuración podría variar.


b) Examine el archivo de configuración activa actual.

	Switch# <code>show running-config</code>
-----------------------------------------------------------------------------------	------------------------------------------

**Preguntas:**

1. **¿Cuántas interfaces FastEthernet observa en su conmutador?**  
Hay 24 interfaces.
2. **¿Cuántas interfaces GigabitEthernet observa en su conmutador?**  
Hay 2 interfaces.
3. **¿Cuáles son los dígitos que acompañan a la línea vty?**  
(0,4) y (5,15)

c) Examine el archivo de configuración de inicio en la NVRAM.

	Switch# <code>show startup-config</code> startup-config is not present
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------

**Pregunta:**

4. **¿Por qué aparece este mensaje?**  
Porque la configuración de inicio no ha sido guardada todavía.

d) Examine la información de la versión del IOS de Cisco del conmutador.

	Switch# <code>show version</code>
-------------------------------------------------------------------------------------	-----------------------------------

**Pregunta:**

5. **¿Cuál es el nombre del archivo de imagen del sistema?**  
"flash:c2960-lanbasek9-mz.150-2.SE4.bin"

e) Examine las propiedades predeterminadas de la interfaz FastEthernet que usa la PC1.

	Switch# <code>show interface f0/1</code>
-------------------------------------------------------------------------------------	------------------------------------------


**Preguntas:**

6. **¿La interfaz está activa o inactiva?**  
Está activa.
7. **¿Cuál es la dirección MAC de la interfaz?**  
000b.be8c.1e01
8. **¿Cuál es la configuración de velocidad y de dúplex de la interfaz?**  
Full dúplex 100Mb/s

f) Examine la memoria flash.

Ejecute uno de los siguientes comandos para examinar el contenido del

directorio flash.

	Switch# <b>show flash</b>
	Switch# <b>dir flash:</b>

**Pregunta:**


**9. ¿Cuál es el nombre de archivo de la imagen de IOS de Cisco?**

2960-lanbasek9-mz.150-2.SE4.bin

## **Actividad 2: Configurar los parámetros básicos de los dispositivos de red.**

En este paso, configurará la computadora y los parámetros básicos del conmutador, como el nombre de host y la dirección IP para la SVI (Switch Virtual Interface) de administración del conmutador. La asignación de una dirección IP en el conmutador es solo el primer paso. Como administrador de red, debe especificar cómo se administra el conmutador. Telnet y SSH son los dos métodos de administración que más se usan. No obstante, Telnet no es un protocolo seguro. Toda la información que fluye entre los dos dispositivos se envía como texto no cifrado. Las contraseñas y otra información confidencial pueden ser fáciles de ver si se las captura mediante un programa detector de paquetes.

**a)** Ingrese al modo de configuración global.

	Switch# <b>configure terminal</b>
	Switch(config)#


La petición de entrada volvió a cambiar para reflejar el **modo de configuración global**.

**b)** Asigne un nombre al conmutador.


	Switch(config)# <b>hostname S1</b>
	S1(config)#

**c)** Asigne **class** como contraseña secreta para el acceso al modo EXEC privilegiado.


	S1(config)# <b>enable secret class</b>
	S1(config)#

	Para evitar las búsquedas DNS no deseadas, puede usar el comando: <b>no ip domain-lookup</b>
	En el modo de configuración global.

**d)** Configure un mensaje de bienvenida "MOTD".

	S1(config)# <b>banner motd #</b>
	Enter Text message. End with the character '#'. <b>Prohibido el acceso no autorizado. #</b>

**e)** Para verificar la configuración de acceso, alterne entre los modos EXEC, EXEC privilegiado y configuración global.

	<pre> S1(config)# exit S1# *Mar 1 00:19:19.490: %SYS-5-CONFIG_I: Configured from console by console S1# exit S1 con0 is now available  Press RETURN to get started.  Prohibido el acceso no autorizado. S1&gt;           </pre>
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


- f) Vuelva al modo EXEC privilegiado desde el modo EXEC del usuario. Introduzca la contraseña establecida en el literal **c**.


	<pre> S1&gt; enable Password: S1#           </pre>
-----------------------------------------------------------------------------------	----------------------------------------------------

- g) Para administrar el S1 en forma remota desde la PC1, debe asignar una dirección IP al conmutador. El conmutador está configurado de manera predeterminada para que la administración de este se realice a través de VLAN 1. Sin embargo, la práctica recomendada para la configuración básica del conmutador es cambiar la VLAN de administración a otra VLAN distinta de la VLAN 1.


En esta práctica, utilice la VLAN 99. Primero, cree la nueva VLAN 99 en el conmutador, luego, asigne la dirección IP 192.168.30.2 con máscara de subred 255.255.255.0 en la interfaz virtual VLAN 99.


Ingresa al modo de configuración global para establecer la dirección IP de la SVI del conmutador. Esto permite la administración remota del conmutador.

	<pre> S1# configure terminal S1(config)# vlan 99 S1(config-vlan)# exit S1(config)# interface vlan99 %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down S1(config-if)#ip address 192.168.30.2 255.255.255.0 S1(config-if)# no shutdown S1(config-if)# exit S1(config)#           </pre>
-------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


	<p>Observe que la interfaz VLAN 99 está en estado down, aunque haya introducido el comando <b>no shutdown</b>. Actualmente, la interfaz se encuentra en estado down debido a que no se asignaron puertos del conmutador a la VLAN 99.</p>
-------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- h) Asigne todos los puertos de usuario a VLAN 99.


	<pre> S1(config)# interface range f0/1 - 24 S1(config-if-range)# switchport access vlan 99 S1(config-if-range)# exit S1(config)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up </pre>
-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Para establecer la conectividad entre el host y el conmutador, los puertos que usa el host deben estar en la misma VLAN.</p>
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------


- i) Configure una puerta de enlace predeterminada (*gateway*) para S1. Sin un gateway predeterminado, no se puede administrar el conmutador desde una red remota. Al finalizar la práctica se incluirá un *gateway* externo, el cual conectará la LAN a un enrutador para tener acceso externo. Suponiendo que la interfaz LAN en el enrutador es 192.168.30.1, asigne esta dirección como *gateway* predeterminado para el conmutador S1:

	<pre> S1(config)# ip default-gateway 192.168.30.1 S1(config)# </pre>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------

- j) También se debe restringir el acceso a través del puerto de consola. Predeterminadamente se permiten todas las conexiones de consola sin necesidad de introducir una contraseña. Para evitar que los mensajes de consola interrumpen los comandos, use la opción **logging synchronous**.

	<pre> S1(config)# line con 0 S1(config-line)# password cisco S1(config-line)# login S1(config-line)# logging synchronous S1(config-line)# exit S1(config)# </pre>
-------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------

- k) Configure las líneas de terminal virtual (vty) para que el conmutador permita el acceso por Telnet. Si no configura una contraseña de vty, no puede acceder al conmutador mediante telnet.

	<pre> S1(config)# line vty 0 15 S1(config-line)# password cisco S1(config-line)# login S1(config-line)# end S1# *Mar 1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console </pre>
-------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- l) Cifrar las contraseñas sin cifrar del dispositivo.

	<pre> S1(config)# service password-encryption S1(config)# </pre>
-------------------------------------------------------------------------------------	------------------------------------------------------------------

## Preguntas:

### 10. ¿Por qué se requiere el comando login?

Porque sin él el usuario no podría acceder al conmutador ya que no se presentaría un pedido de login.

### Actividad 3: Configurar las direcciones IP en la PC1 y PC2.

Asigne a la computadora la dirección IP y la máscara de subred que se muestran en la tabla de direccionamiento. En esta topología, introducir como Gateway la ip 192.168.30.1 para simular que es el enrutador conectado al S1.

### Actividad 4: Verificar y probar la conectividad de red.

En la parte 4, verificará y registrará la configuración del conmutador, probará la conectividad de extremo a extremo entre la PC1, PC2 y el S1, y probará la capacidad de administración remota del conmutador.

### Paso 1. Mostrar la configuración del conmutador.

Desde la conexión de consola en la PC1, muestre y verifique la configuración del conmutador. El comando **show running-config** o **show run** (abreviación) muestra la configuración en ejecución completa, de a una página por vez. Utilice la barra espaciadora para avanzar por las páginas.

- a) Aquí se muestra un ejemplo de configuración. Los parámetros que configuró están en color verde. Las demás son opciones de configuración predeterminadas del IOS.



S1# show run

```
Building configuration...
Current configuration : 2206 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4
06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
<output omitted>
!
interface FastEthernet0/24
```

```
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan99
ip address 192.168.30.2 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.30.1
ip http server
ip http secure-server
!
banner motd ^C
Prohibido el acceso no autorizado. ^C
!
line con 0
password 7 104D000A0618
logging synchronous
login
line vty 0 4
password 7 14141B180F0B
logging synchronous
login
line vty 5 15
password 7 14141B180F0B
logging synchronous
```

<pre>switchport access vlan 99 ! interface GigabitEthernet0/1 ! interface GigabitEthernet0/2 !</pre>	<pre>login ! end</pre>
------------------------------------------------------------------------------------------------------	------------------------

## Paso 2. Probar la conectividad.

- a) En el símbolo del sistema de la PC1, haga ping a la dirección de la PC2.



```
C:\Users\User1> ping 192.168.30.11
```

- b) En el símbolo del sistema de la PC1, haga ping a la dirección de administración de SVI del S1.



```
C:\Users\User1> ping 192.168.30.2
```

## Paso 3. Probar y verificar la administración remota del S1.

Ahora utilizará Telnet para acceder al conmutador en forma remota. En esta práctica de laboratorio, la PC1 y el S1 se encuentran uno junto al otro. En una red de producción, el conmutador podría estar en un armario de cableado en el piso superior, mientras que la computadora de administración podría estar ubicada en la planta baja. En este paso, utilizará Telnet para acceder al conmutador S1 en forma remota mediante la dirección de administración de SVI. Telnet no es un protocolo seguro; sin embargo, lo usará para probar el acceso remoto. Con Telnet, toda la información, incluidos los comandos y las contraseñas, se envía durante la sesión como texto no cifrado.

- a) Con la ventana *cmd* abierta en la PC1, emita un comando de Telnet para conectarse a S1 a través de la dirección de administración de SVI. La contraseña es **cisco**. También puede hacerlo a través del software Putty.



```
C:\Users\User1> telnet 192.168.30.2
```

- b) Después de introducir la contraseña **cisco**, quedará en la petición de entrada del modo EXEC del usuario. Acceda al modo EXEC privilegiado.
- c) Escriba **exit** para finalizar la sesión de Telnet.

## Paso 4. Guardar el archivo de configuración en ejecución del conmutador.

Guarde la configuración.



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





También puede usar el comando **write** para guardar la configuración en ejecución.

### Actividad 5: Administración de la tabla de direcciones MAC.

A continuación, determinará las direcciones MAC que detectó el conmutador, configurará una dirección MAC estática en una interfaz del conmutador y, a continuación, eliminará la dirección MAC estática de esa interfaz.

#### Paso 1. Registrar las direcciones MAC del host.

En el símbolo del sistema de la PC1 y PC2, emita el comando **ipconfig /all** para consultar las direcciones (físicas) de capa 2 de la NIC de las computadoras.

<b>MAC PC1</b>	0090.2B0B.E5B3
<b>MAC PC2</b>	0030.A3A3.C077

#### Paso 2. Determine las direcciones MAC que el conmutador ha aprendido.

Muestre las direcciones MAC con el comando **show mac address-table**.



```
S1# show mac address-table
```

#### Preguntas:

11. ¿Cuántas direcciones dinámicas hay?  
2
12. ¿Cuántas direcciones MAC hay en total?  
2
13. ¿Las direcciones MAC dinámicas coinciden con las direcciones MAC de PC1 y PC2?  
Sí

#### Paso 3. Enumerar las opciones del comando show mac address-table.

- a) Muestre las opciones de la tabla de direcciones MAC.



```
S1# show mac address-table ?
```

#### Pregunta:

14. ¿Cuáles opciones se encuentran disponibles para el comando show mac address-table? Explique cada una.  
Dynamic: recibe una entrada de tipo dinámico  
Interface: recibe una entrada de tipo interface  
Static: recibe una entrada de tipo estático

#### Paso 4. Configuración de una dirección MAC estática.

- a) Limpie la tabla de direcciones MAC. Para eliminar las direcciones MAC

existentes, use el comando `clear mac address-table` del modo EXEC privilegiado. En caso que no se limpie, emita el comando varias veces; caso contrario, desconecte el cable Ethernet de la computadora.



```
S1# clear mac address-table dynamic
```

- b) Verifique que la tabla de direcciones MAC se haya eliminado.



```
S1# show mac address-table
```

- c) Examine nuevamente la tabla de direcciones MAC

Es muy probable que una aplicación en ejecución en la computadora ya haya enviado una trama por la NIC hacia el S1. Observe nuevamente la tabla de direcciones MAC en el modo EXEC privilegiado para ver si S1 volvió a detectar la dirección MAC para la PC1.



```
S1# show mac address-table
```

### Preguntas:

#### 15. ¿Cambió algo? ¿por qué?

El conmutador obtuvo nuevamente la dirección MAC de la PC1 porque se realizó una comunicación dinámica.



El conmutador volvió a adquirir dinámicamente la dirección MAC de la computadora. Si el S1 aún no volvió a detectar la dirección MAC de la PC1, haga ping a la dirección IP de la VLAN 99 del conmutador desde la PC1 y, a continuación, repita el comando **show mac address-table**.

- d) Configure una dirección MAC estática.



```
S1(config)# mac address-table static 0050.56BE.6C89  
vlan 99 interface fastethernet 0/1
```



La dirección MAC 0050.56BE.6C89 se usa solo en el ejemplo. Use la dirección MAC de su PC1.

Para especificar a qué puertos se puede conectar un host, una opción es crear una asignación estática de la dirección MAC del host a un puerto. Configure una dirección MAC estática en Fa0/1 con la dirección que se registró para la PC1 en la actividad 5, paso 1. La dirección MAC 0050.56BE.6C89 se usa solo como ejemplo. Debe usar la dirección MAC de la PC1, que es distinta de la del ejemplo.

- e) Verifique las entradas de la tabla de direcciones MAC.

	S1# show mac address-table
-----------------------------------------------------------------------------------	----------------------------

**Preguntas:**

16. ¿Cuántas direcciones MAC hay en total?

1


17. ¿Cuántas direcciones estáticas hay?


1

18. Intercambie las conexiones de los hosts y haga ping entre ambos. ¿Qué sucede y por qué?

Se muestra la dirección de la PC1 como estática pero la de la PC2 como dinámica en la tabla.

- f) Elimine la entrada de MAC estática. Ingrese al modo de configuración global y elimine el comando escribiendo **no** delante de la cadena de comandos.

	S1(config)# no mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/1
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------

	La dirección MAC 0050.56BE.6C89 se usa solo en el ejemplo. Use la dirección MAC de su PC1.
-------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------

- g) Verifique que la dirección MAC estática se haya borrado.

	S1# show mac address-table
-------------------------------------------------------------------------------------	----------------------------

**Preguntas de reflexión**

1. ¿Para qué se configura la línea vty en el conmutador?

Para que se pueda tener acceso a Telnet.

2. ¿Cómo puede evitar que las contraseñas se envíen como texto no cifrado en un acceso remoto al dispositivo?

Haciendo que el conmutador cifre las contraseñas él mismo antes de enviarlas.


**Actividad 6: Inicialización y recarga de un conmutador.**

**Paso 1. Inicializar y volver a cargar el conmutador.**


- a) Acceda al conmutador mediante el puerto de consola e ingrese al modo EXEC privilegiado.

	S1> enable S1#
-------------------------------------------------------------------------------------	-------------------


- b) Utilice el comando **show flash** para determinar si se crearon VLAN en el conmutador.

	<pre> S1# show flash Directory of flash:/     2  -rwx 1919 Mar 1 1993 00:06:33 +00:00       private-config.text    3  -rwx 1632 Mar 1 1993 00:06:33 +00:00       config.text    4  -rwx 13336 Mar 1 1993 00:06:33 +00:00       multiple-fs    5  -rwx 11607161 Mar 1 1993 02:37:06 +00:00       c2960-lanbasek9-mz.150-2.SE.bin    6  -rwx 616 Mar 1 1993 00:07:13 +00:00       vlan.dat  32514048 bytes total (20886528 bytes free) S1# </pre>
-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


- c) Si se encontró el archivo vlan.dat en la memoria flash, elimínelo.

	<pre> S1# delete vlan.dat Delete filename [vlan.dat]? </pre>
-----------------------------------------------------------------------------------	--------------------------------------------------------------

- d) Se le solicitará que verifique el nombre de archivo. Si introdujo el nombre correctamente, presione **Enter**; de lo contrario, puede cambiar el nombre de archivo.
- e) Se le solicita que confirme la eliminación de este archivo. Presione **Enter** para confirmar.

	<pre> Delete flash:/vlan.dat? [confirm] Commutador# </pre>
-------------------------------------------------------------------------------------	------------------------------------------------------------

- f) Utilice el comando **erase startup-config** para eliminar el archivo de configuración de inicio de la NVRAM. Se le solicita que elimine el archivo de configuración. Presione **Enter** para confirmar.

	<pre> S1r# erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete S1# </pre>
-------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------

- g) Vuelva a cargar el conmutador para eliminar toda información de configuración antigua de la memoria. Luego, recibirá una petición de entrada para confirmar la recarga del conmutador. Presione **Enter** para continuar.

	<pre> S1# reload Proceed with reload? [confirm] </pre>
-------------------------------------------------------------------------------------	--------------------------------------------------------



Es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el conmutador. Responda escribiendo **no** y presione **Enter**.



System configuration has been modified. Save?  
[yes/no]: **no**

- h) Una vez que se vuelve a cargar el conmutador, debe ver una petición de entrada del diálogo de configuración inicial. Responda escribiendo **no** en la petición de entrada y presione **Enter**.



Would you like to enter the initial configuration dialog? [yes/no]: **no**  
Switch>

## Conclusiones

El saber configurar los parámetros básicos de seguridad de un conmutador correctamente es de suma importancia incluso para las redes más pequeñas. El no entender de qué forma se relacionan estas configuraciones en el proceso de comunicación es fatal ya que dar por alto un paso tan simple (como lo es ingresar el comando "login" al colocar una clave de acceso, por ejemplo) puede resultar en el fallo de todo el proceso. La unión de todos estos pequeños conceptos y su correcta comprensión hacen que el desempeño al trabajar en esto sea eficaz y eficiente.

## Recomendaciones

Verificar en todo momento que las configuraciones finales hayan sido guardadas correctamente.

## Bibliografía

[1] Cisco, "Curricula CCNA1: Introducción a Redes versión 5.0". Accessed Septiembre 2017. [Online]. Available: <http://static-course-assets.s3.amazonaws.com/ITN50ES/index.html>

## Rúbrica de evaluación

Criterio	Excelencia	Desarrollado	En desarrollo	Inicial
Configura los parámetros básicos en un conmutador	Configura los parámetros básicos en un conmutador y comprende su uso	Configura los parámetros básicos en un conmutador de forma sistemática sin comprender su uso	Configura los parámetros básicos en un conmutador de forma incompleta	No configura los parámetros básicos en un conmutador
Configura la seguridad en la interfaz de un conmutador	Configura la seguridad en la interfaz de un conmutador y comprende su uso	Configura la seguridad en la interfaz de un conmutador de forma sistemática sin comprender su uso	Configura la seguridad en la interfaz de un conmutador de forma incompleta	No configura la seguridad en la interfaz de un conmutador
Conclusiones	Da su opinión tomando en cuenta las actividades realizadas y sus	Da su opinión tomando en cuenta las actividades realizadas, sus	Da su opinión tomando en cuenta las actividades	Da su opinión sin tomar en cuenta las actividades realizadas,

	argumentos son válidos dando a conocer información relevante tratada durante la práctica	argumentos son válidos, pero no menciona información relevante	realizadas, pero carece de argumentos detallados	o, no presenta las conclusiones solicitadas
--	------------------------------------------------------------------------------------------	----------------------------------------------------------------	--------------------------------------------------	---------------------------------------------