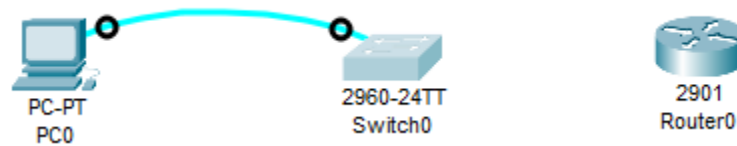


Contraseñas para modo usuario y privilegiado

Para la topología solo vamos a estar utilizando un switch y un pc, aunque podría usarse también un router.



De momento se ha dejado conectado un cable consola del PC al Switch0 para realizar pruebas a futuro.

Ingresando al modo privilegiado(#) del switch , se va a establecer un mensaje del día, un mensaje que puede establecer un administrador para comunicar cosas al personal que ingrese al equipo o un aviso legal.

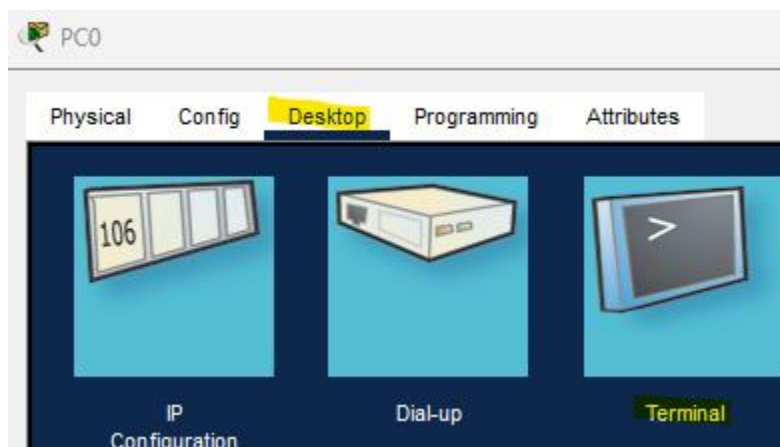
La sintaxis del comando es la siguiente: **banner motd Mensaje a dejar**

```
Switch(config)#banner motd "Bienvenido al equipo"
```

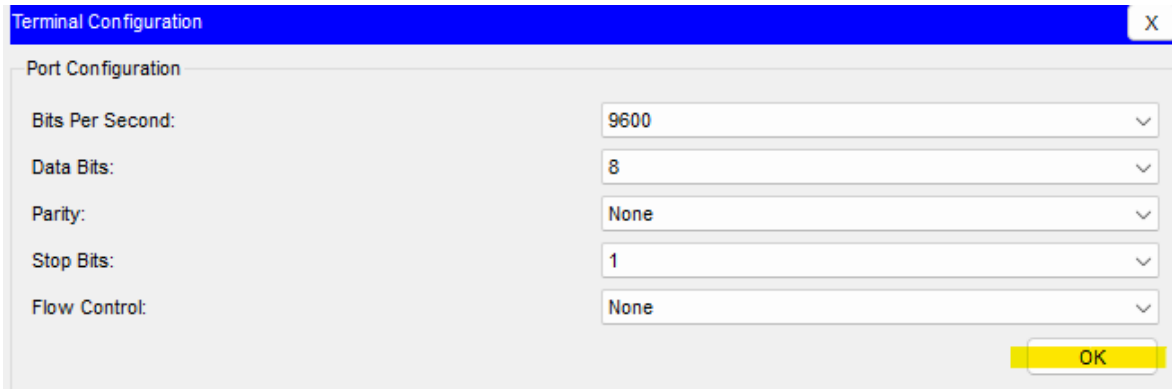
En varios casos lo normal es delimitar el mensaje, en este caso ha sido por comillas al inicio y al final, para guiarnos y no perder el hilo del mensaje, pero no es algo obligatorio, como se observa en el mensaje que establecemos en el Router0.

```
| Router(config)#banner motd ACCESO SOLO PARA PERSONAL DE TI
```

Para verificar la existencia del mensaje iremos al PC0, dentro de la pestaña Desktop buscaremos el Terminal, que va a simular el programa que usaremos en la vida real para ingresar al equipo mediante nuestro propio computador.



Dentro de la ventana emergente dejaremos todas las opciones por defecto y presionaremos el botón **OK**, que se encuentra debajo de todas las opciones.

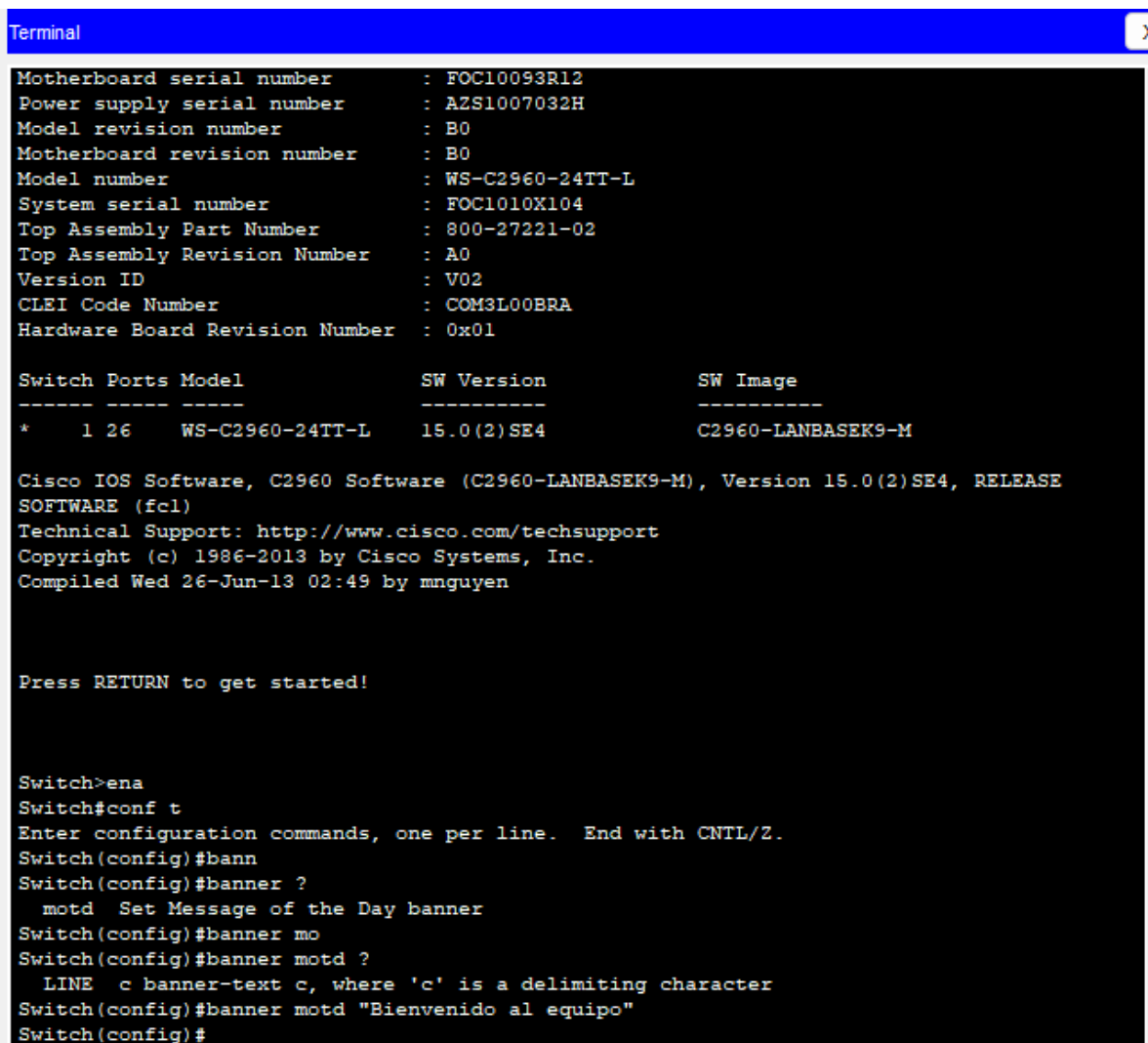


The image shows a 'Terminal Configuration' dialog box with a blue title bar and a close button (X). It contains a 'Port Configuration' section with five dropdown menus: 'Bits Per Second' (9600), 'Data Bits' (8), 'Parity' (None), 'Stop Bits' (1), and 'Flow Control' (None). An 'OK' button is located at the bottom right.

Port Configuration	
Bits Per Second:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None

OK

Como no ha pasado mucho tiempo desde que hicimos algo en el equipo la terminal mostrara el CLI del switch.



The image shows a terminal window with a blue title bar and a close button (X). It displays the output of the 'show version' command on a Cisco switch, followed by the 'enable' command and the start of the configuration mode. The output includes hardware details, a table of switch ports, and software information.

```
Motherboard serial number      : FOC10093R12
Power supply serial number     : AZS1007032H
Model revision number          : B0
Motherboard revision number    : B0
Model number                   : WS-C2960-24TT-L
System serial number           : FOC1010X104
Top Assembly Part Number       : 800-27221-02
Top Assembly Revision Number   : A0
Version ID                     : V02
CLEI Code Number               : COM3L00BRA
Hardware Board Revision Number : 0x01

Switch Ports Model          SW Version        SW Image
-----
*  1 26  WS-C2960-24TT-L  15.0(2)SE4       C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnnguyen

Press RETURN to get started!

Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#bann
Switch(config)#banner ?
    motd  Set Message of the Day banner
Switch(config)#banner mo
Switch(config)#banner motd ?
    LINE  c banner-text c, where 'c' is a delimiting character
Switch(config)#banner motd "Bienvenido al equipo"
Switch(config)#
```

En caso de haber pasado mucho más tiempo, apenas ingresemos al equipo aparecerá el mensaje que establecimos anteriormente.

```
Bienvenido al equipo
Switch>
```

Antes de poder crear las contraseñas, hay que asegurarse de que sean seguras dentro del equipo de la siguiente manera: encriptándolas con el comando **service password-encryption** en el modo privilegiado.

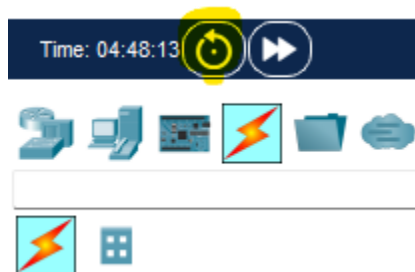
```
Switch(config)#service password-encryption
Switch(config)#
```

Para crear contraseñas, para poder ingresar al equipo mediante otros equipos o directamente en el mismo equipo, se escribirán los siguientes comandos dentro del modo privilegiado:

- **line console 0**: El comando nos permite entrar en la línea de consola, la línea que permite ingresar a la consola del equipo a otros equipos. Normalmente solo se tiene una línea los equipos que es la línea 0.
- **password contraseña**: Ayuda a establecer la contraseña para la línea consola, solo hay que reemplazar contraseña por la contraseña que deseamos.
- **login**: El comando le indica al equipo que debe pedir la contraseña establecida anteriormente.

```
Switch(config)#line console 0
Switch(config-line)#password 123456
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#
```

Para probar el funcionamiento de la contraseña, guardaremos la configuración del equipo con el comando **do write**, en modo privilegiado, o con el comando **write**, en modo usuario, para después reiniciar los equipos en el botón indicado.



Ahora si regresamos al PC0 e ingresamos por la terminal se nos pedirá inmediatamente la contraseña que hemos ingresado anteriormente.

```
Bienvenido al equipo
User Access Verification
Password:
```

Para la contraseña del modo privilegiado se seguirán los siguientes comandos:

- **enable secret contraseña**: Establece la contraseña del modo usuario. La contraseña será lo que escribamos en lugar de contraseña.
- **ip domain-name nombre.dominio**: Crearemos un nombre de dominio que estará funcionando posteriormente con SSH para la autenticación, el dominio será lo que escribamos reemplazando nombre.dominio.
- **crypto key generate rsa**: Genera las claves, pública y privada, para el cifrado y la autenticación del algoritmo RSA. Escribiremos 2048 para establecer el tamaño de bits. Este comando debe ser ingresado en un equipo cuyo hostname no sea el hostname por defecto.
- **ip ssh version 2**: Establecemos la versión de SSH que se usara.

```
Switch(config)#enable secret kevin
Switch(config)#ip domain-name prueba.com
Switch(config)#crypto key generate rsa
% Please define a hostname other than Switch.
Switch(config)#hostname SW
SW(config)#crypto key generate rsa
The name for the keys will be: SW.prueba.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

SW(config)#ip ssh version 2
*Mar 1 0:15:17.314: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

- **line vty 0 15**: Estas son las líneas que se utilizan para conectarse de manera remota mediante SSH o Telnet. Con el comando tenemos acceso a las 16 líneas VTY.
- **login local**: Le indicamos al equipo que debe buscar en su base de datos a los usuarios y contraseñas creados en el equipo.
- **transport input ssh**: Aquí permitimos que solo se conecten por SSH a las líneas VTY.

```
SW(config)#line vty 0 15
SW(config-line)#login local
SW(config-line)#transport input ssh
SW(config-line)#exit
```

- **username usuario privilege 15 secret contraseña:** Finalmente, creamos el usuario y contraseña que podrá ingresar en el equipo, usuario en este caso que tendrá todos los privilegios y podrá ejecutar cualquier comando.

```
SW(config)#username marvin privilege 15 secret 654321
SW(config)#
```

Como datos extra, los privilegios se establecen de la siguiente manera:

- **privilege 0:** El usuario solo puede usar comandos básicos como logout, enable, disable, etc.
- **Privilege 1:** Nivel por defecto, solo puede ver configuraciones básicas pero no aplicar cambios.
- **Privilege 2-14:** Del nivel 2 al 14 son personalizables, nosotros indicamos que comandos puede utilizar cada usuario.
- **Privilege 15:** Acceso total, puede ver y realizar cambios y usar todos los comandos libremente.

Un ejemplo de nivel 2-14 es el siguiente:

```
SW(config)#username yanira privilege 4 secret clavel23456
SW(config)#privilege exec level 5 show
```

Se utiliza el comando **privilege exec level 5 show** para indicar que todo usuario de nivel 5 puede usar el comando show.

Si probamos nuevamente la conexión, veremos que para ingresar al modo usuario, después del comando enable, se nos pedirá la contraseña que establecimos para el modo usuario.

```
Bienvenido al equipo
User Access Verification
Password:
SW>ena
Password:
Password:
SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW(config)#
```

Para poder comprobar la conexión SSH es necesario configurar una IP en el switch, esto se realiza solo si se necesita que sea administrado de manera remota.

Para agregarla se ingresará dentro de la vlan 1 como se muestra en la siguiente imagen.

```
SW(config)#interface vlan 1
SW(config-if)#ip add
SW(config-if)#ip address 192.168.1.3 255.255.255.0
SW(config-if)#exit
SW(config)#
```

También nos aseguramos que la vlan 1 se encuentre activa y establecemos que su Gateway sea la primera dirección de la red, esta dirección es establecida en el router.

```
SW(config-if)#no shutdown

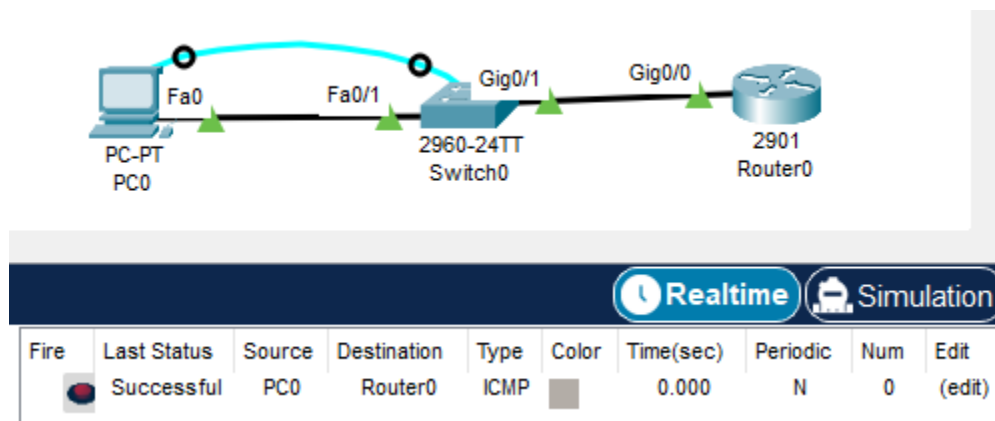
SW(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

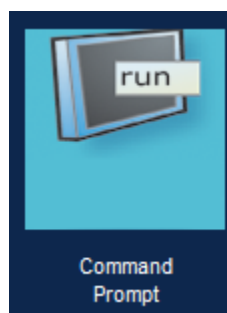
SW(config-if)#ip def
SW(config-if)#ip default-gateway 192.168.1.1

Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

Ahora observamos que la topología ha quedado de la siguiente manera y hay comunicación.



Dentro del PC0 usaremos el Command Prompt para el ingreso por SSH. Esta opción sería la equivalente al CMD en un equipo físico.



Para ingresar por SSH al equipo, usando un usuario creado, usamos el siguiente comando:

ssh -l nombre_usuario ip_equipo.

Ingresamos el usuario y la ip correspondiente y si todo funciona correctamente nos pedirán la contraseña del usuario.

```
C:\>ssh -l marvin 192.168.1.3

Password:

Bienvenido al equipo

SW>ena
Password:
Password:
SW#ena
SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW(config)#
```

Y así es como se habrán establecido las contraseñas para los equipos.