# Configuración básica de un Switch Cisco

## Objetivos:

- Breve repaso del laboratorio 1.
- Comprender qué es un switch y qué es una interfaz de gestión (SVI).
- Configurar el hostname del switch.
- Configurar contraseñas: enable secret, consola, VTY.
- Configurar un banner MOTD.
- Asignar una IP de gestión a una interfaz VLAN y entender la diferencia entre VLAN 1 y una VLAN de gestión dedicada.
- Configurar basicamente SSH para acceso seguro y entender por qué evitar Telnet.
- Guardar la configuración y verificar el estado del switch con comandos show.

## 1) Conceptos fundamentales

### ¿Qué es un switch?

Un switch es un dispositivo de red que opera en la **capa 2 (enlace de datos)** del modelo OSI. Su función principal es recibir tramas Ethernet en una interfaz, leer la dirección MAC de destino y reenviarlas por el puerto correcto según su tabla de direcciones MAC (**MAC Address Table**). A diferencia de un hub, el switch envía tramas sólo por el puerto de destino (no las difunde a todos), eso mejora el rendimiento y la seguridad.

### ¿Qué es una interfaz de gestión (SVI)?

Una **SVI (Switch Virtual Interface)** es una interfaz lógica asociada a una VLAN (por ejemplo la VLAN 1). Asignarle una IP permite administrar el switch de manera remota (Telnet/SSH, SNMP, etc.). Un switch L2 no enruta tráfico entre VLANs, la IP de la SVI es **solo para la gestión del switch.**

### ¿VLAN 1 o VLAN de gestión?

- **VLAN 1**: VLAN por defecto en los switches Cisco. Por simplicidad se usa en laboratorios, pero en redes reales **no es una buena práctica** usar la VLAN 1 para administración.
- **VLAN de gestión**: crear, por ejemplo, la **VLAN 99** y usar esta interface como SVI para gestión. Así se separa el tráfico de usuarios del tráfico de administración.

**Tipos de accesos al switch**

- **Consola (console)**: acceso físico directo, mediante un cable de consola, usado para la configuración inicial.
- **Telnet**: acceso remoto no cifrado (los datos se transmiten en texto plano). **No recomendado** en producción.
- **SSH**: acceso remoto cifrado. **Recomendado**.

**Modos de la CLI**

- User EXEC (`Switch>`): comandos básicos.
- Privileged EXEC (`Switch#`): permite ver configuraciones y entrar al modo de configuración global. Se accede con `enable`.
- Global Configuration (`Switch(config)#`): modo para cambiar la configuración global. Se accede con `configure terminal`.

## 2) Comandos fundamentales

A continuación se muestra cada bloque de configuración. Primero se explica la finalidad, luego se muestran los comandos y a continuación se da una explicación línea por línea.

### 2.1 Cambiar el hostname

**Por qué:** para poder identificar el dispositivo en la red.

**Comandos:**

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1
```

**Explicación línea por línea:**

- `enable`: pasa de User EXEC (`Switch>`) a Privileged EXEC (`Switch#`) para ejecutar comandos de configuración.
- `configure terminal`: se ingresa al modo de configuración global (`Switch(config)#`).
- `hostname SW1`: establece el nombre del dispositivo a SW1. El prompt cambia para mostrar SW1.

### 2.2 Proteger el modo privilegiado

**Por qué:** el modo privilegiado permite cambios críticos, la contraseña debe ser segura y estar cifrada.

**Comandos:**

```
SW1(config)# enable secret ClaveSegura123
```

**Explicación:**

- `enable secret ClaveSegura123`: define la contraseña para acceder al modo privilegiado (`SW1#`). `enable secret` almacena la contraseña cifrada (hasheada), a diferencia de `enable password` (en texto plano). Siempre usar `enable secret`.

### 2.3 Proteger el acceso por consola

**Por qué:** alguien con acceso físico se puede conectar a la consola, protegerla con contraseña y tiempos de inactividad mejoran la seguridad.

**Comandos:**

```
SW1(config)# line console 0
SW1(config-line)# password consola123
SW1(config-line)# login
SW1(config-line)# exec-timeout 5 0
SW1(config-line)# exit
```

**Explicación:**

- `line console 0`: selecciona la línea de consola física (solo hay una, de ahí el número 0).
- `password consola123`: establece la contraseña requerida al acceder por consola.
- `login`: obliga al dispositivo a solicitar la contraseña en la consola.
- `exec-timeout 5 0`: establece el tiempo de inactividad a 5 minutos (5 min 0 seg), tras el cual la sesión se cierra automáticamente. Mejora la seguridad.
- `exit`: sale del contexto line.

**Buenas prácticas:** además de contraseñas, restringir acceso físico a los dispositivos de red.

### 2.4 Proteger acceso remoto VTY y preferir SSH a Telnet

**Por qué:** Telnet transmite credenciales sin cifrar (en texto plano). SSH cifra la comunicación (datos y credenciales).

**Ejemplo con Telnet (sólo para laboratorios):**

```
SW1(config)# line vty 0 4
SW1(config-line)# password telnet123
SW1(config-line)# login
SW1(config-line)# exit
```

**Explicación:**

- `line vty 0 4`: selecciona las líneas VTYs 0 a 4, que permiten hasta 5 sesiones remotas simultáneas (la cantidad de líneas varía de acuerdo al modelo de dispositivo).
- `password telnet123`: se establece la contraseña para Telnet.
- `login`: habilita la contraseña.
- `exit`: sale del submodo.

**Ahora, cómo configurar SSH (recomendado):**

**Pasos:**

```
SW1(config)# ip domain-name ejemplo.local
SW1(config)# crypto key generate rsa modulus 2048
SW1(config)# username admin secret AdminPass2025
SW1(config)# ip ssh version 2
SW1(config)# line vty 0 4
SW1(config-line)# login local
SW1(config-line)# transport input ssh
SW1(config-line)# exit
```

**Explicación:**

- `ip domain-name ejemplo.local`: configura el nombre de dominio, requerido para generar las claves RSA que usa SSH.
- `crypto key generate rsa modulus 2048`: genera el par de claves RSA con longitud 2048 bits; necesarias para SSH.
- `username admin secret AdminPass2025`: crea una cuenta local admin con contraseña cifrada *AdminPass2025*.
- `ip ssh version 2`: fuerza uso de SSH versión 2 (mejor y más seguro que la versión 1).
- `line vty 0 4`: entra al modo de configuración de líneas VTY (la cantidad de

líneas varía de acuerdo al dispositivo).

- `login local`: indica que las conexiones remotas usarán las cuentas locales (los `username`) para autenticarse.
- `transport input ssh`: permite solo SSH en las VTY (bloquea Telnet).
- `exit`: sale del submodo line.

**Nota**: si se quiere permitir tanto SSH como Telnet (no recomendado), usar `transport input ssh telnet`. Lo recomendable es bloquear Telnet.

### 2.5 Banner MOTD (advertencia legal)

**Por qué:** informa al usuario que el acceso está restringido, útil en ambientes corporativos por motivos legales y de seguridad.

**Comando:**

```
SW1(config)# banner motd #ADVERTENCIA: Acceso restringido.
Uso autorizado únicamente.#
```

**Explicación:**

- `banner motd`: inicia la definición del banner (Message Of The Day).
- `#`: es el carácter delimitador, se puede usar cualquier otro carácter que no aparezca en el texto. El texto entre los delimitadores se mostrará a quien intente conectarse.

### 2.6 Configurar IP de gestión en una VLAN (SVI)

**Por qué:** para administrar el switch remotamente mediante la IP. En laboratorios se usa la VLAN 1, en producción, crear una VLAN de gestión dedicada.

**Ejemplo con VLAN 1:**

```
SW1(config)# interface vlan 1
SW1(config-if)# ip address 192.168.1.10 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit
```

**Explicación:**

- `interface vlan 1`: abre la interfaz virtual asociada a VLAN 1.
- `ip address 192.168.1.10 255.255.255.0`: asigna la dirección IP.
- `no shutdown`: activa la interfaz SVI (puede o no estar en shutdown).
- `exit`: salir del submodo.

**Nota:** Una SVI estará en estado `up` solo si existe al menos un puerto físico en esa VLAN que esté up (`administratively up` y conectado). Si aparece el mensaje `Interface VLAN1 is down`, se debe verificar que exista un puerto en la VLAN1 con cable y link up.

Si el switch debe comunicarse fuera de su subnet (por ejemplo para acceder desde otra red), se debe configurar un default gateway:

```
SW1(config)# ip default-gateway 192.168.1.1
```

### 2.7 Guardar configuración

**Por qué:** los cambios se aplican en running-config (RAM) y se pierden si el dispositivo es reiniciado.

**Comando:**

```
SW1# copy running-config startup-config
```

**Explicación:**

- `copy running-config startup-config`: copia la configuración activa (running-config) al archivo que se carga al arrancar (startup-config) en NVRAM. Cuando el switch se reinicie, cargará esa configuración guardada.

### 2.8 Comandos de verificación útiles

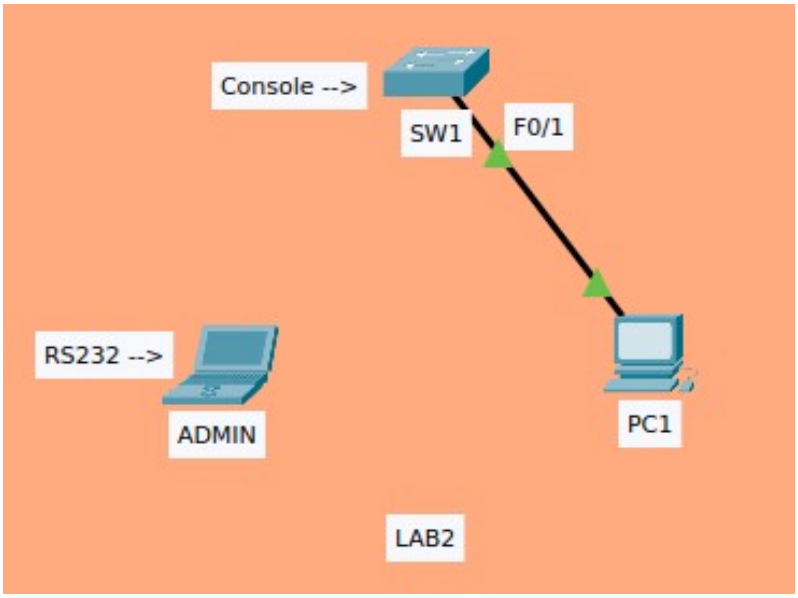
- `show running-config`: muestra la configuración activa.
- `show startup-config`: muestra la configuración guardada.
- `show ip interface brief`: muestra un resumen de las interfaces y direcciones IP.
- `show ip interface vlan 1`: detalles de la SVI (VLAN 1 en este caso).
- `show users`: sesiones activas.
- `show line`: muestra info de líneas físicas y virtuales.

# Laboratorio en Packet Tracer

## Objetivo

Configurar un switch Cisco con parámetros básicos de identificación, seguridad y administración, aplicando las mejores prácticas aprendidas.

## Topología




## Actividades

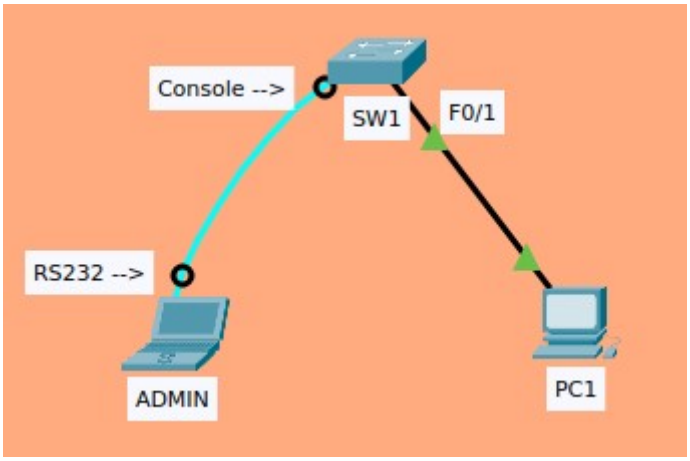
1. Conectar la PC ADMIN a la consola del switch, acceder a la CLI y cambiar el hostname a **SW1**.
2. Configurar contraseña en modo privilegiado con `enable secret`.
3. Configurar contraseña de acceso a la consola.
4. Configurar contraseña para líneas VTY (sólo SSH).
5. Crear un banner MOTD con un mensaje de advertencia.
6. Configurar la dirección IP 192.168.1.100/24 en la VLAN 1 y habilitarla.
7. Guardar la configuración en la NVRAM y reiniciar el switch.
8. Probar conectividad desde la PC1 hacia el switch (la PC1 ya fue configurada).

## Resultado esperado

- El switch debe mostrar el hostname **SW1.**
- El acceso privilegiado debe requerir contraseña.
- La consola y las líneas VTY deben quedar protegidas.
- Se debe mostrar un mensaje de advertencia al conectarse.
- La PC1 debe poder hacer ping y conectarse mediante SSH al switch.
- La configuración debe permanecer después de reiniciar el dispositivo.

## Resolución del laboratorio

### 1. Conectar la PC ADMIN al switch




Acceder a la CLI y cambiar el hostname:

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1
SW1(config)#
```

### 2. Configurar contraseña en modo privilegiado

```
SW1(config)# enable secret MiEnableSecret!
```

### 3. Configurar contraseña para consola

```
SW1(config)# line console 0
SW1(config-line)# password Cons0Pass!
SW1(config-line)# login
SW1(config-line)# exec-timeout 10 0
SW1(config-line)# logging synchronous
SW1(config-line)# exit
```

**4. Configuración líneas VTY (SSH)**

```
SW1(config)# ip domain-name miempresa.local
SW1(config)# crypto key generate rsa modulus 2048
SW1(config)# username admin secret SSHPass2025!
SW1(config)# ip ssh version 2
SW1(config)# line vty 0 4
SW1(config-line)# login local
SW1(config-line)# transport input ssh
SW1(config-line)# exit
```

**5. Crear un banner MOTD**

```
SW1(config)# banner motd #Acceso restringido a personal
autorizado.#
```

**6. Configurar interface VLAN 1**

```
SW1(config)# interface vlan 1
SW1(config-if)# ip address 192.168.1.100 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# end
```

**7. Guardad la configuración en la NVRAM**

```
SW1# copy running-config startup-config
Destination filename [startup-config]?   (ENTER)
Building configuration…
[OK]
SW1# reload
```

**8. Probar conectividad desde la PC1 a SW1**

```
C:\> ping 192.168.1.100
Pinging 192.168.1.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.100: bytes=32 time<1ms TTL=255
Reply from 192.168.1.100: bytes=32 time<1ms TTL=255
Reply from 192.168.1.100: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.100:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>telnet 192.168.1.100
Trying 192.168.1.100 ...Open
[Connection to 192.168.1.100 closed by foreign host]
C:\>ssh -l admin 192.168.1.100
Password:               (SSHPass2025!)

Acceso restringido a personal autorizado.

SW1>enable
Password:               (MiEnableSecret!)
SW1#
```

## Conclusión

La configuración básica de un switch es fundamental antes de integrarlo en una red productiva. En este laboratorio se aplicaron las configuraciones mínimas para identidad, acceso seguro y administración.

Es importante resaltar que:

- Un switch L2 necesita una configuración mínima para ser gestionable y seguro: **hostname**, **enable secret**, protección de **consola** y **VTY**, **banner**, **SVI** con IP de gestión y **guardar** la configuración.
- **Telnet** transmite contraseñas en texto claro y **no** se debe usar en producción, **SSH** es el método seguro y requiere generar claves RSA y tener usuarios locales.
- **VLAN 1** se usa en laboratorios por simplicidad, pero en producción conviene usar una **VLAN de gestión dedicada**.
- Guardar con `copy running-config startup-config` para persistencia.

Este laboratorio es un paso clave que prepara el camino para configuraciones más avanzadas, como segmentación con VLANs, enrutamiento y seguridad de red.