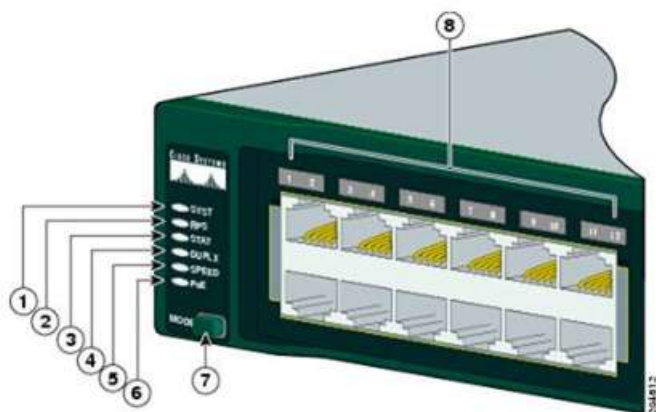


Redes 1

Modos y submodos de configuración
global

Comandos básicos

Sistema de arranque de un switch



Comando boot system

- Después de encender un switch Cisco, pasa por la siguiente secuencia de inicio de cinco pasos:
- **Paso 1:** Primero, el switch carga un programa de autodiagnóstico al encender (POST) almacenado en la memoria ROM. El POST verifica el subsistema de la CPU. Este comprueba la CPU, la memoria DRAM y la parte del dispositivo flash que integra el sistema de archivos flash.
- **Paso 2:** A continuación, el switch carga el software del cargador de arranque. El cargador de arranque es un pequeño programa almacenado en la memoria ROM que se ejecuta inmediatamente después de que el POST se completa correctamente.
- **Paso 3:** El cargador de arranque lleva a cabo la inicialización de la CPU de bajo nivel. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad.
- **Paso 4:** El cargador de arranque inicia el sistema de archivos flash en la placa del sistema.
- **Paso 5:** Por último, el cargador de arranque localiza y carga una imagen de software del sistema operativo de IOS en la memoria y delega el control del switch a IOS.

S1(config)# **boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin**

Indicadore led de un switch

- **LED del sistema**
- Muestra si el sistema está recibiendo energía y funciona correctamente. Si el LED está apagado, significa que el sistema no está encendido. Si el LED es de color verde, el sistema funciona normalmente. Si el LED es de color ámbar, el sistema recibe alimentación pero no funciona correctamente.
- **LED del sistema de alimentación redundante (RPS)**
- Muestra el estado de RPS. Si el LED está apagado, el RPS está apagado o no está conectado correctamente. Si el LED es de color verde, el RPS está conectado y listo para proporcionar alimentación de respaldo. Si el LED parpadea y es de color verde, el RPS está conectado pero no está disponible porque está proporcionando alimentación a otro dispositivo. Si el LED es de color ámbar, el RPS está en modo de reserva o presenta una falla. Si el LED parpadea y es de color ámbar, la fuente de alimentación interna del switch presenta una falla, y el RPS está proporcionando alimentación.

- **LED de estado del puerto**

- Indica que el modo de estado del puerto está seleccionado cuando el LED está verde. Este es el modo predeterminado. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados. Si el LED está apagado, no hay enlace, o el puerto estaba administrativamente inactivo. Si el LED es de color verde, hay un enlace presente. Si el LED parpadea y es de color verde, hay actividad, y el puerto está enviando o recibiendo datos. Si el LED alterna entre verde y ámbar, hay una falla en el enlace. Si el LED es de color ámbar, el puerto está bloqueado para asegurar que no haya un bucle en el dominio de reenvío y no reenvía datos (normalmente, los puertos permanecen en este estado durante los primeros 30 segundos posteriores a su activación). Si el LED parpadea y es de color ámbar, el puerto está bloqueado para evitar un posible bucle en el dominio de reenvío.

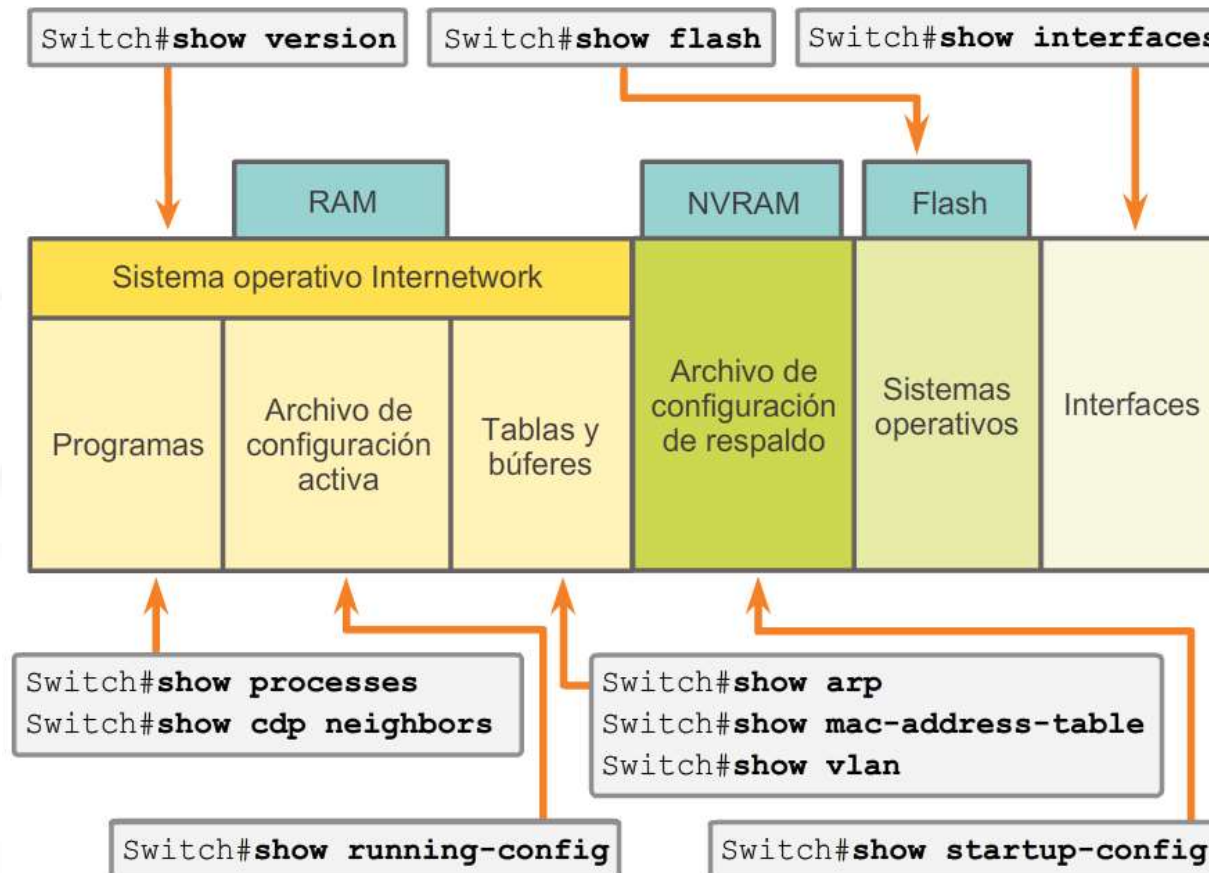
LED de modo dúplex del puerto

- Indica que el modo dúplex del puerto está seleccionado cuando el LED está verde. Al seleccionarlo, los LED del puerto que están apagados están en modo semidúplex. Si el LED del puerto es de color verde, el puerto está en modo dúplex completo.
- **LED de velocidad del puerto**
- Indica que el modo de velocidad del puerto está seleccionado. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados. Si el LED está apagado, el puerto está funcionando a 10 Mbps. Si el LED es verde, el puerto está funcionando a 100 Mbps. Si el LED parpadea en verde, el puerto está funcionando a 1000 Mbps.

Tejas de acceso rápido y métodos abreviados

- **Tabulación:** completa el resto de un comando o de una palabra clave que se escribió parcialmente.
- **Ctrl-R:** vuelve a mostrar una línea.
- **Ctrl-A:** el cursor se traslada al comienzo de la línea.
- **Ctrl-Z:** sale del modo de configuración y vuelve al modo EXEC del usuario.
- **Flecha abajo:** permite al usuario desplazarse hacia delante a través de los comandos anteriores.
- **Flecha arriba:** permite al usuario desplazarse hacia atrás a través de los comandos anteriores.
- **Ctrl-Mayús-6:** permite al usuario interrumpir un proceso de IOS, como **ping** o **traceroute**.
- **Ctrl-C:** cancela el comando actual y sale del modo de configuración.

Comandos de examen de IOS



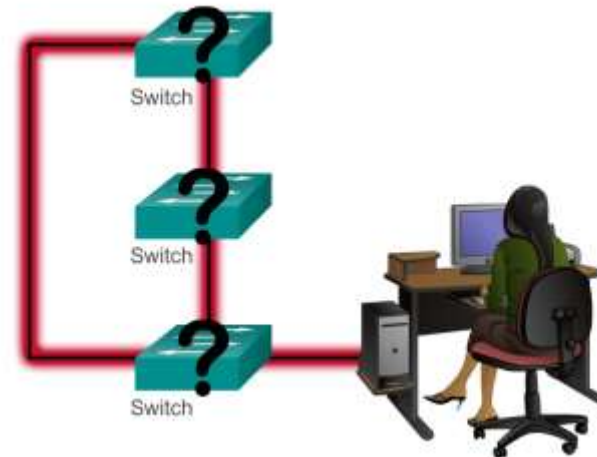
Los comandos **show** del IOS pueden proporcionar información sobre la configuración, el funcionamiento y el estado de las partes de un switch o router Cisco.

Nombres de dispositivos

Según ciertas pautas de convenciones de denominación, los nombres deberían:

- Comenzar con una letra
- No contener espacios.
- Finalizar con una letra o dígito
- **Utilizar solamente letras, dígitos y guiones.**
- Tener menos de 64 caracteres de longitud.

Sin nombres, es difícil identificar los dispositivos de red para propósitos de configuración.



Protección del acceso a los dispositivos

Las contraseñas ingresadas aquí son:

- **Contraseña de enable:** limita el acceso al modo EXEC privilegiado.
 - **Contraseña secreta de enable:** contraseña encriptada que limita el acceso al modo EXEC privilegiado.
 - **Contraseña de consola:** limita el acceso a los dispositivos mediante la conexión de consola.
 - **Contraseña de VTY:** limita el acceso a los dispositivos a través de Telnet.
- Nota:** en la mayoría de las prácticas de laboratorio de este curso, se utilizan contraseñas simples como **cisco** o **class**.

Protección del acceso a EXEC privilegiado

- Utilizar el comando **enable secret**, no el comando anterior **enable password**.
- El comando **enable secret** proporciona mayor seguridad porque la contraseña está encriptada.

```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

Protección del acceso a EXEC del usuario

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

- Se debe aportar seguridad al puerto de consola.
 - Así se reducen las posibilidades de que personal no autorizado conecte físicamente un cable al dispositivo y obtenga acceso a él.
- Las líneas vty permiten el acceso a un dispositivo Cisco a través de Telnet.
 - La cantidad de líneas vty admitidas varía según el tipo de dispositivo y la versión de IOS.

Configuración de la encriptación de contraseñas

Introduzca el comando para encriptar las contraseñas de texto no cifrado.

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

Salga del modo de configuración global y vea la configuración en ejecución.

```
Switch(config)#exit
```

```
Switch#show running-config
```

```
!
```

```
<resultado omitido>
```

```
!
```

```
line con 0
```

```
password 7 094F471A1A0A
```

```
login
```

```
!
```

```
line vty 0 4
```

```
password 7 03095A0F034F38435B49150A1819
```

```
login
```

```
!
```

```
!
```

```
end
```

service password-encryption

- Impide que las contraseñas aparezcan como texto no cifrado cuando se visualiza la configuración.
- El propósito de este comando es evitar que personas no autorizadas vean las contraseñas en el archivo de configuración.
- Una vez que se aplica, cancelar el servicio de encriptación no revierte la encriptación.

Limitación del acceso a las configuraciones de los dispositivos

Mensajes de aviso

- Son una parte importante en los procesos legales en el caso de una demanda por ingreso no autorizado a un dispositivo.
- No es adecuado utilizar palabras que sugieran que “se invita” al usuario a iniciar sesión o que es “bienvenido”.
- Con frecuencia, se usa para notificaciones legales ya que se visualiza en todas las terminales conectadas.

Limitación del acceso a los dispositivos: MOTD

```
Sw1-Floor-1 (config) #banner motd # This is a secure system. Authorized Access ONLY!!! #
```

Esta configuración tiene como resultado este anuncio de mensaje del día.

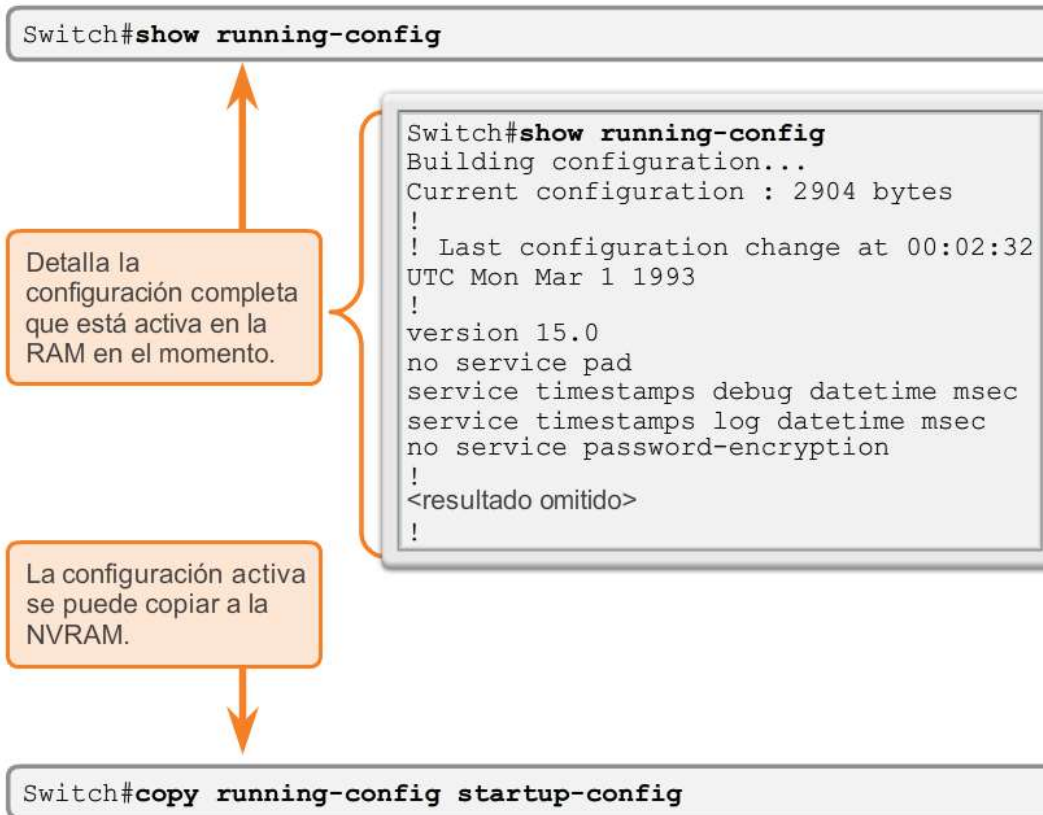
Los caracteres delimitadores no se incluyen en el mensaje.

```
Sw1-Floor-1 con0 is now available
Press RETURN to get started.
This is a secure system. Authorized
Access ONLY!!!
User Access Verification
password:
Sw1-Floor-1>enable
Password:
Sw1-Floor-1#
```


Cómo guardar configuraciones

Archivos de configuración

Cómo guardar y borrar la configuración



■ Switch# reload

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

Proceed with reload?
[confirm]

■ La configuración de inicio se elimina utilizando el comando **erase startup-config**.

Switch# **erase startup-config**

■ En un switch, también se debe emitir el comando **delete vlan.dat**.

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

Delete flash:vlan.dat?
[confirm]

Bibliografía

- CCNA 1 Cisco