# Introducción a las redes conmutadas

# Secuencia de inicio del switch

1. POST (*Power On Self-Test*)
2. El switch carga las instrucciones (cargador de arranque) de inicio de la NVRAM
3. Realiza la inicialización de la CPU a bajo nivel
4. Inicializa el sistema de archivos flash
5. Ubica y carga una imagen del software del sistema operativo en la memoria RAM y arranca el switch.

# Secuencia de inicio del switch

Con el fin de encontrar una imagen IOS adecuado, el switch sigue los siguientes pasos:

- Intenta iniciarse automáticamente utilizando la información de la variable de entorno de arranque
- Si esta variable no está definida, el switch realiza una búsqueda de arriba hacia abajo a través del sistema de archivos flash. Carga y ejecuta el primer archivo ejecutable, si puede.
- El sistema operativo IOS inicializa las interfaces usando los comandos de IOS de Cisco que se encuentran en el archivo de configuración de inicio que se almacena en la NVRAM.

**Nota**: los comandos **`boot system`** se puede utilizar para establecer la variable de entorno de arranque.

.

# Recovering From a System Crash

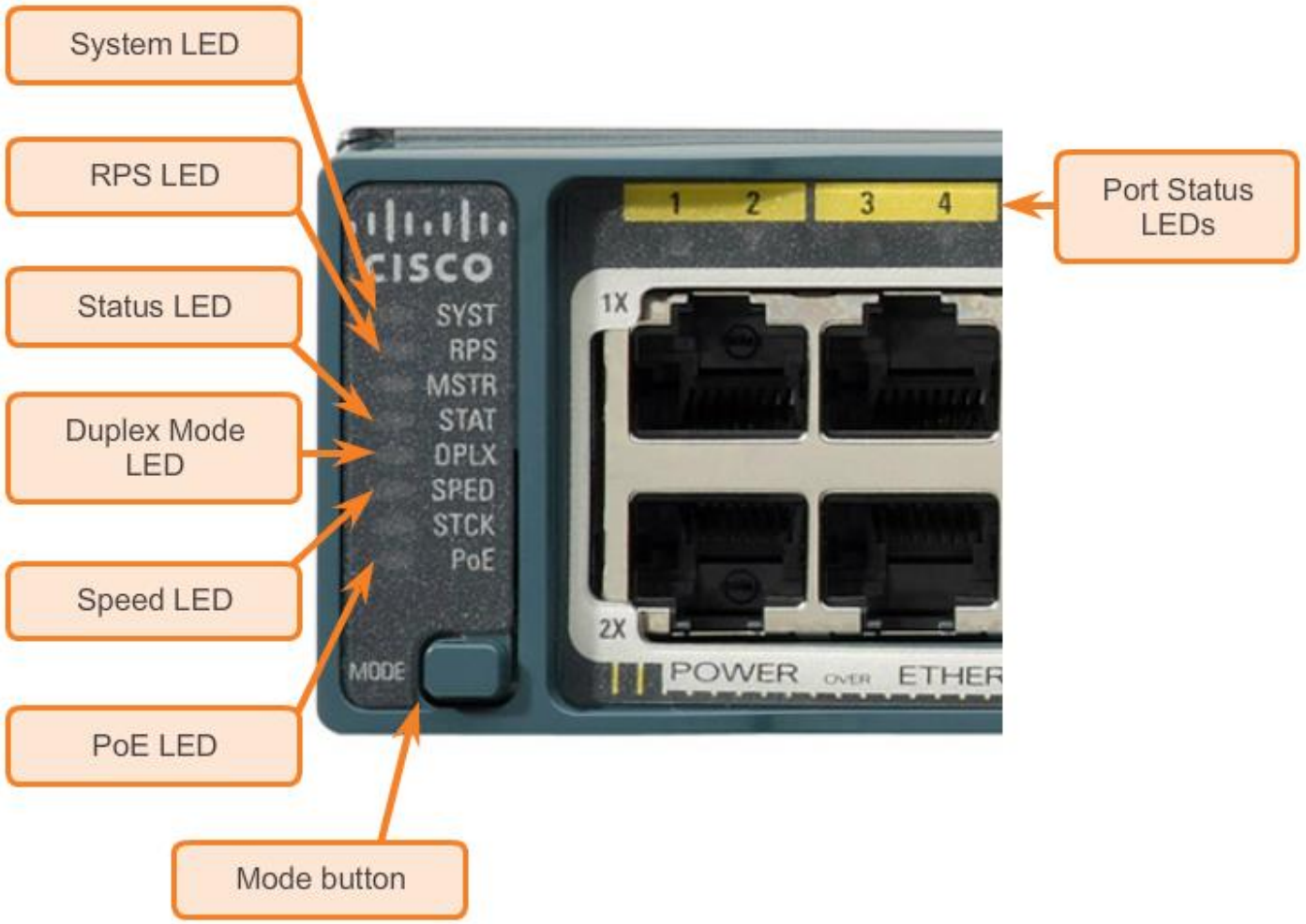
- El cargador de arranque también se puede utilizar para administrar el switch si el IOS no puede ser cargado.
- El cargador de arranque puede ser accesado a través de una conexión de consola:
  1. Conectar un PC mediante un cable de consola al puerto de consola del switch. Desconecte el cable de alimentación del switch,
  2. Vuelva a conectar el cable de alimentación al switch y presione y mantenga presionado el botón Mode.
  3. El LED Sistema de encendido cambia brevemente de ámbar a verde. Suelte el botón Mode.
- El cargador de arranque muestra "`switch:prompt`" en el software de emulación de terminal en el PC.

# LED Indicadores del switch

- Cada puerto de los switches Cisco Catalyst tiene LED que indica el estado del puerto.
- Por defecto estos LED reflejan la actividad del puerto, pero también pueden proporcionar otra información sobre el switch a través del botón MODE.
- Los siguientes modos están disponibles en Cisco Catalyst 2960 switches:
  - LED de sistema
  - LED de Sistema de alimentación redundante (RPS)
  - LED de estado del puerto
  - LED de puerto Duplex
  - LED de velocidad de puerto
  - LED de modo de Alimentación a través de Ethernet (PoE)

# LED Indicadores del switch

- Cisco Catalyst 2960 switch modes



# Preparación para la administración básica del switch

- Con el fin de administrar de forma remota un switch Cisco, este tiene que ser configurado para acceder a la red.
- Una dirección IP y una máscara de subred deben ser configuradas.
- Si la administración se hará desde una red remota, se debe configurar una puerta de enlace predeterminada.
- La información de IP (dirección IP, máscara de subred, puerta de enlace) se va a asignar a una SVI del switch (interfaz virtual del switch).
- Aunque esta configuración IP permiten la gestión remota y acceso remoto al switch, que no permiten que el switch enrute paquetes (capa 3).

# Preparación para la administración básica del switch

| Cisco Switch IOS Commands | |
|---|---|
| Enter global configuration mode. | S1# **configure terminal** |
| Enter interface configuration mode for the SVI. | S1(config)# **interface vlan99** |
| Configure the management interface IP address. | S1(config-if)# **ip address 172.17.99.11** |
| Enable the management interface. | S1(config-if)# **no shutdown** |
| Return to the privileged EXEC mode. | S1(config-if)# **end** |
| Save the running config to the startup config. | S1# **copy running-config startup-config** |

| Cisco Switch IOS Commands | |
|---|---|
| Enter global configuration mode. | S1# **configure terminal** |
| Configure the default gateway for the switch. | S1(config)# **ip default-gateway 172.17.99.** |
| Return to the privileged EXEC mode. | S1(config-if)# **end** |
| Save the running config to the startup config. | S1# **copy running-config startup-config** |

# Verificando la configuración de los puertos de switch

## Verification Commands

| Cisco Switch IOS Commands | |
|---|---|
| Display interface status and configuration. | S1# **show interfaces [interface-id]** |
| Display current startup configuration. | S1# **show startup-config** |
| Display current operating config. | S1# **show running-config** |
| Displays info about flash filesystem. | S1# **show flash** |
| Displays system hardware & software status. | S1# **show version** |
| Display history of commands entered. | S1# **show history** |
| Display IP information about an interface. | S1# **show ip [interface-id]** |
| Display the MAC address table. | S1# **show mac-address-table** |

# Características de la capa de acceso

**Display interface status and statistics.**

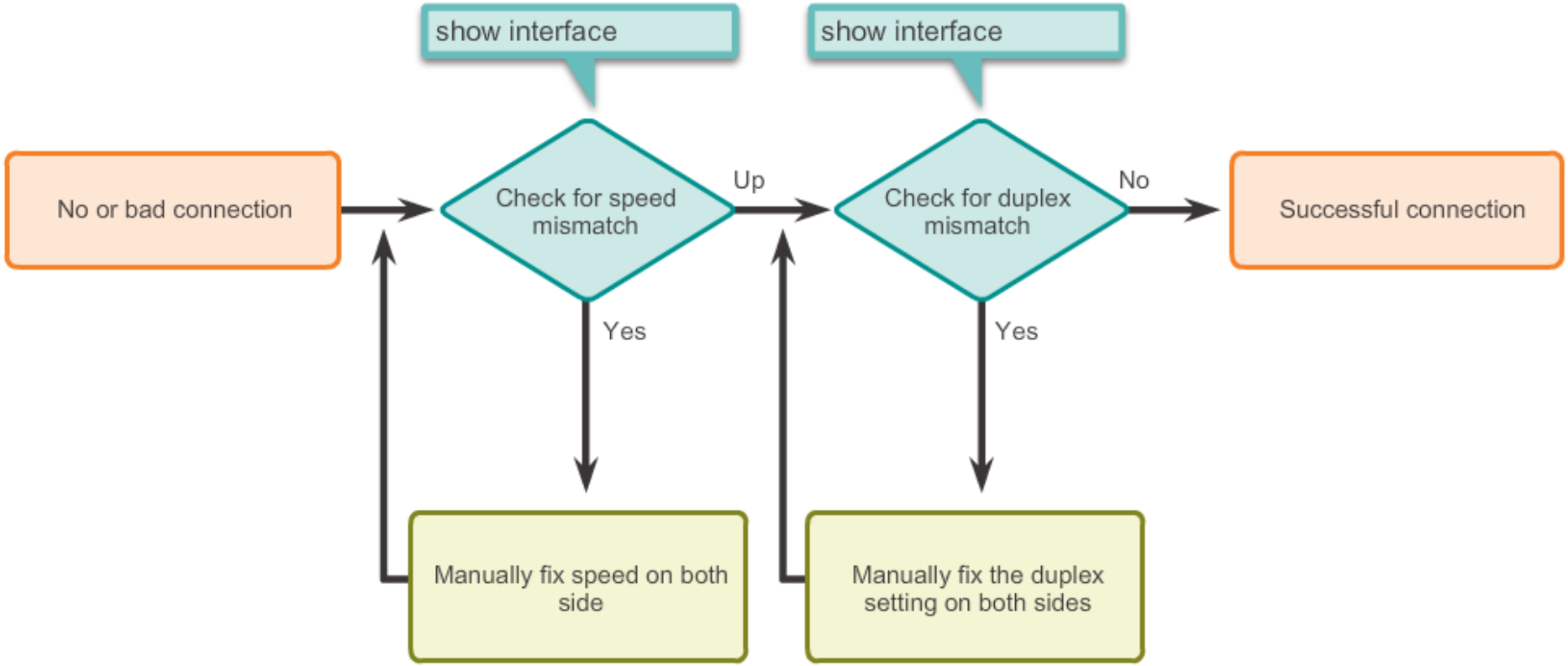
```
S1# show interface FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast
Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)MTU
1500 bytes, BW 100000 Kbit, DLY 100 usec,
<...output omitted...>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0
  throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 multicast, 0 pause input
  0 input packets with dribble condition detected
  3594664 packets output, 436549843 bytes, 0 underruns
  8 output errors,1790 collisions,10 interface resets
  0 unknown protocol drops
  0 babbles, 235 late collision, 0 deferred
<output omitted>
```

# Características de la capa de acceso

| Parameter | Description |
|---|---|
| Runts | Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt. |
| Giants | Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant. |
| Input errors | Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. |
| CRC | CRC errors are generated when the calculated checksum is not the same as the checksum received. |
| Output errors | Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined. |
| Collisions | Number of messages retransmitted because of an Ethernet collision. |
| Late collisions | Jammed signal could not reach to ends. |

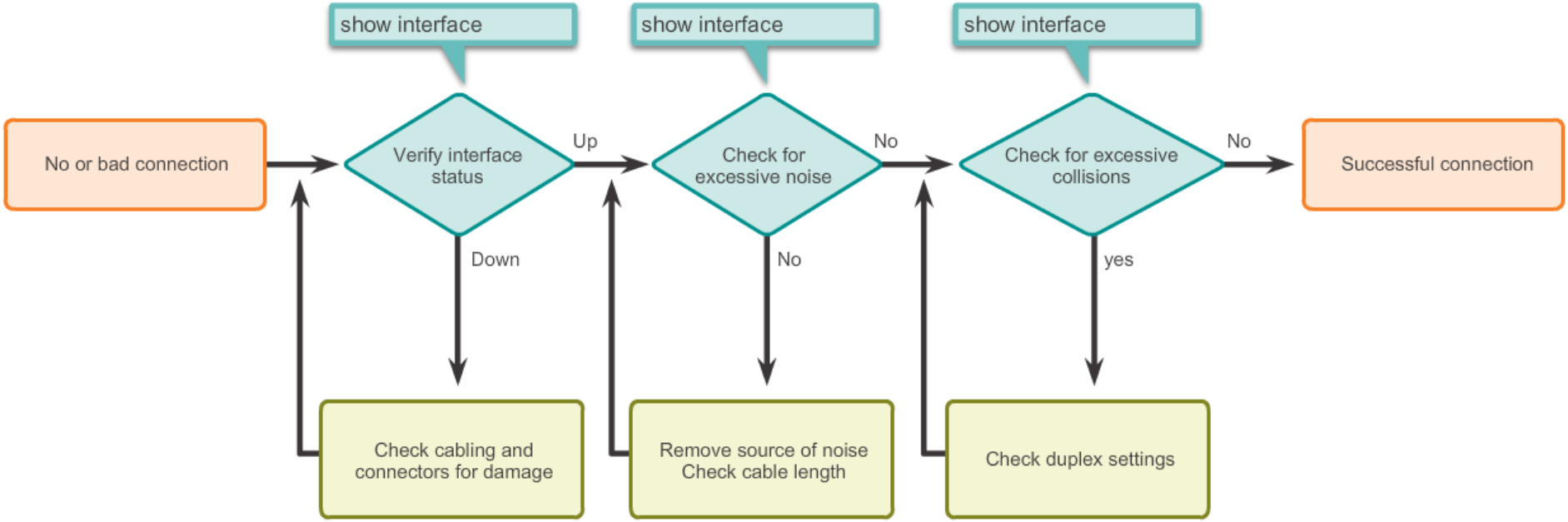
# Características de la capa de acceso

- Troubleshooting Switch Media (connection) issues



# Características de la capa de acceso

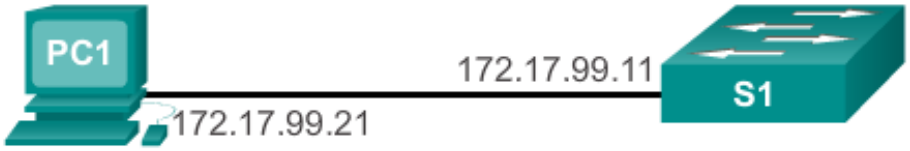
- Troubleshooting Interface-related issues



# Operación de SSH

- Secure Shell (SSH) es un protocolo que proporciona una conexión segura (cifrada) basada en línea de comandos hacia un dispositivo remoto.
- SSH se utiliza comúnmente en los sistemas basados en UNIX.
- Cisco IOS también es compatible con SSH.
- Es necesaria una versión del software IOS que incluya características y capacidades de cifrado (cifrado) con el fin de habilitar SSH en los switch Catalyst 2960.
- Debido a sus fuertes características de encriptación, SSH debería sustituir Telnet para conexiones de administración.
- SSH utiliza el puerto TCP 22 por defecto. Telnet utiliza el puerto TCP 23

# Operación de SSH

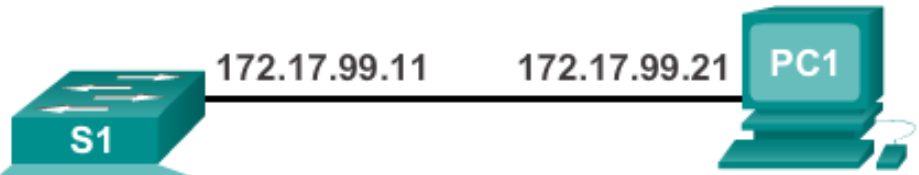



172.17.99.11 - PuTTY

```
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

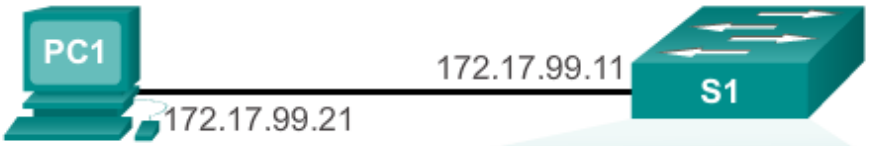
# Configurando SSH




```
S1 # configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin password ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config)# end
```

## Secure Remote Access

# Verificando SSH




```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption  Hmac       State         Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started ricky
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started ricky
%No SSHv1 server connections running.
S1#
```

# Network Security Tools: Options

- Las herramientas de seguridad de la red son muy importantes para los administradores de red.
- Estas herramientas permiten a los administradores para comprobar la fortaleza de las medidas de seguridad implementadas.
- Un administrador puede lanzar un ataque contra la red y analizar los resultados.
- Esto es también para determinar cómo ajustar las políticas de seguridad para mitigar esos tipos de ataques.
- La auditoría de seguridad y pruebas de penetración son dos funciones básicas que las herramientas de seguridad de red realizan.

# Network Security Tools: Audits

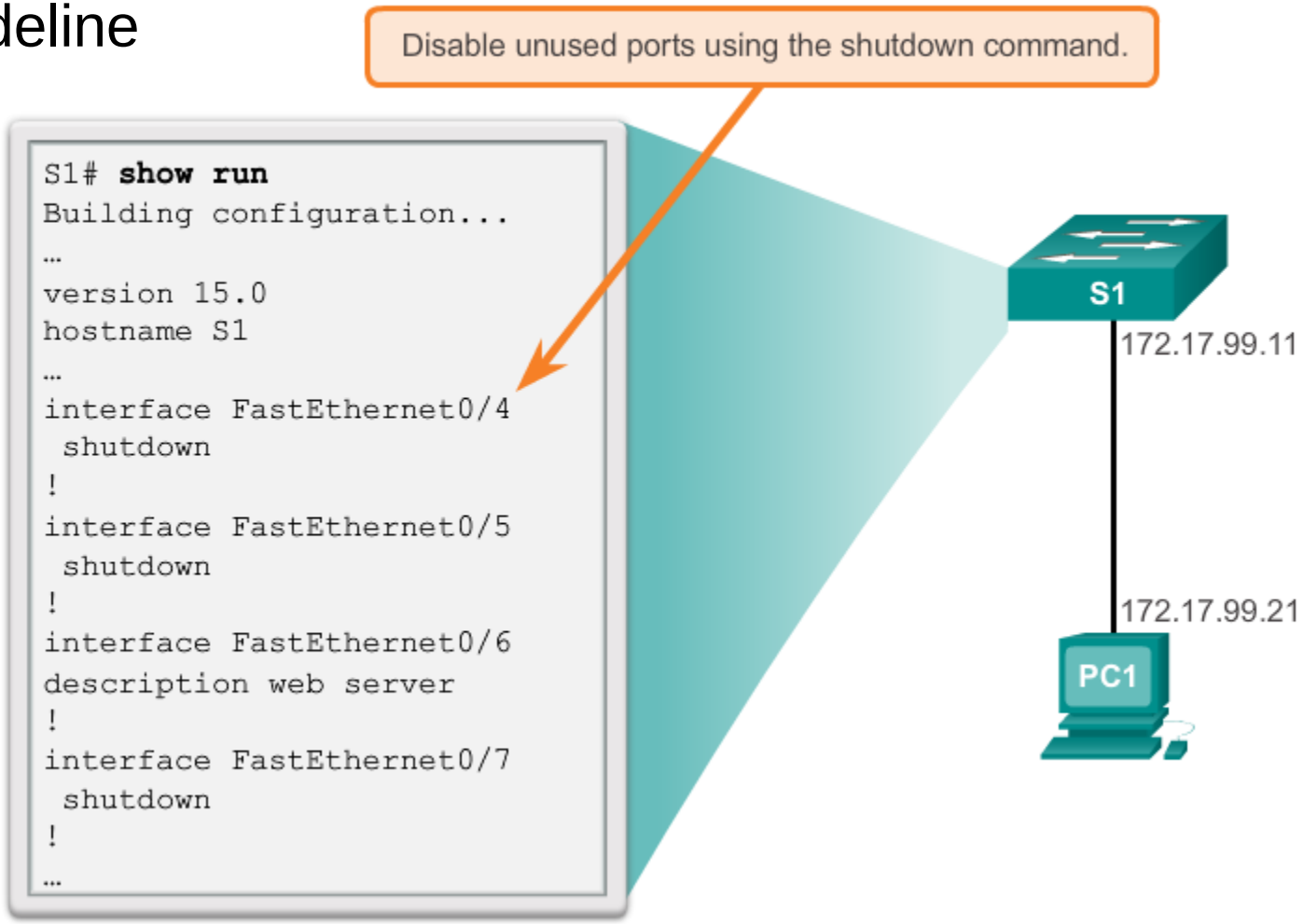
- Las herramientas de seguridad de red se puede utilizar para auditar la red
- Mediante el control de la red, el administrador puede evaluar qué tipo de información un atacante sería capaz de obtener.
- Por ejemplo, al atacar e inundando la tabla CAM de un switch, un administrador podría aprender qué puertos del switch son vulnerables a las inundaciones MAC y corregir el problema.
- Herramientas de seguridad de la red también pueden ser utilizados como herramientas de pruebas de penetración

# Network Security Tools: Audits

- Las pruebas de penetración es un ataque simulado.
- Ayuda a determinar la vulnerabilidad de la red cuando está bajo un ataque real.
- Debilidades en la configuración de dispositivos de red se pueden identificar sobre la base de los resultados de estas pruebas.
- Se pueden hacer cambios para hacer a los dispositivos más resistentes a los ataques
- Tales pruebas pueden dañar la red y deben ser llevados a cabo bajo condiciones muy controladas.

# Asegurar los puertos no utilizados

- Disable Unused Ports is a simple yet efficient security guideline



# Port Security: Operation

- Port security limita el número de direcciones MAC válidas permitidas para un puerto.
- Una dirección MAC legítima será permitida, mientras que otra será denegada.
- Cualquier intento adicional de conexión de una dirección MAC desconodida generará una violación a la seguridad.
- Las direcciones MAC seguras pueden ser indicadas de la siguiente forma:
  - Static secure MAC addresses
  - Dynamic secure MAC addresses
  - Sticky secure MAC addresses

# Port Security: Violation Modes

- IOS considera una violación de seguridad ante cualquiera de estas situaciones:
  - Un número máximo de direcciones MAC seguras, por interface, han sido agregadas a la CAM, y una dirección MAC que no está en la tabla intenta el acceso a la interface.
  - Una dirección aprendida o configurada en una interfaz segura se ve en otra interfaz segura en la misma VLAN.
- Hay tres posibles acciones a tomar cuando se detecta una violación:
  - **Protect (proteger)**
  - **Restrict (restringir)**
  - **Shutdown (apagar**)

# Port Security: Configurando

- Dynamic Port Security Defaults

| Feature | Default Setting |
|---|---|
| Port security | Disabled on a port. |
| Maximum number of secure MAC addresses | 1 |
| Violation mode | Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent. |
| Sticky address learning | Disabled. |

# Port Security: Configurando

- Configurando la Seguridad del Puerto Dinámico


| Cisco IOS CLI Commands | |
|---|---|
| S1(config)#**interface fastethernet 0/18** | Specify the interface to be configured for port security. |
| S1(config-if)#**switchport mode access** | Set the interface mode to access. |
| S1(config-if)#**switchport port-security** | Enable port security on the interface. |

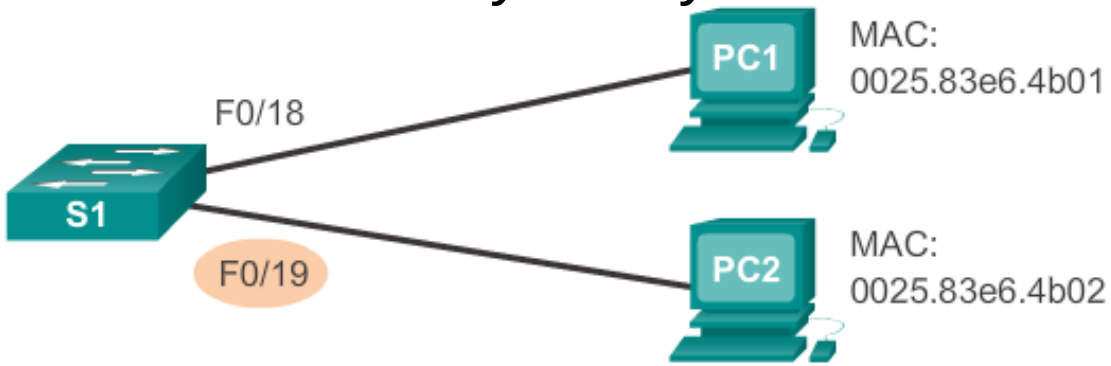
# Port Security: Configurando

- Configurando la Seguridad del Puerto Sticky


| Cisco IOS CLI Commands | |
|---|---|
| S1(config)#**interface fastethernet 0/18** | Specify the interface to be configured for port security. |
| S1(config-if)#**switchport mode access** | Set the interface mode to access. |
| S1(config-if)#**switchport port-security** | Enable port security on the interface. |
| S1(config-if)#**switchport port-security maximum 50** | Set the maximum number of secure addresses allowed on the port. |
| S1(config-if)#**switchport port-security mac-address sticky** | Enable sticky learning. |

# Port Security: Verificando

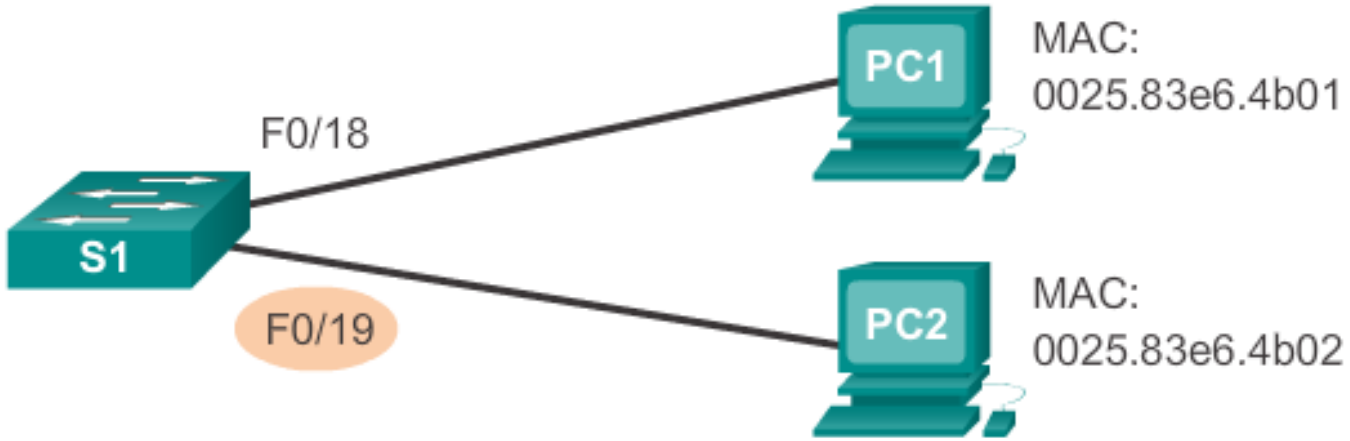
- Verificando Port Security Sticky




```
S1# show port-security interface fastethernet 0/19
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 50
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```

# Port Security: Verificando

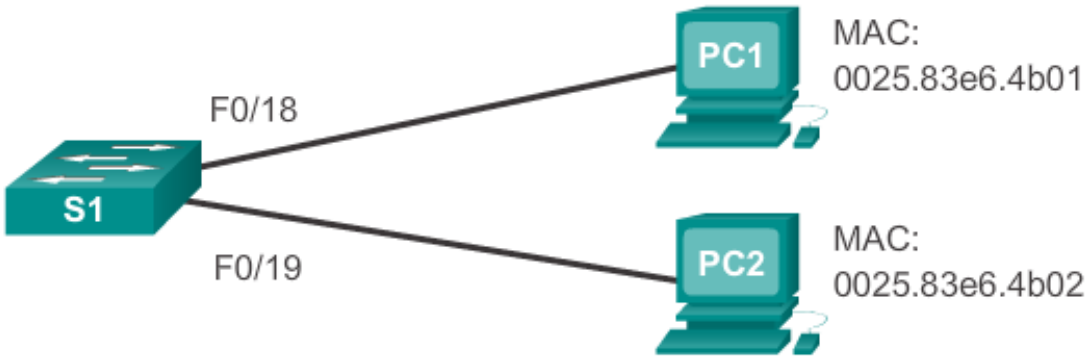
- Verificando Port Security Sticky – Running Config




```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

# Port Security: Verificando

- Verificando Port Security Direcciones MAC Seguras




```
S1# show port-security address
Secure Mac Address Table
-----------------------------------------------------------
Vlan    Mac Address       Type              Ports   Remaining Age
                                                      (mins)
----    -----------       ----              -----   -------------
1       0025.83e6.4b01    SecureDynamic     Fa0/18      -
1       0025.83e6.4b02    SecureSticky      Fa0/19      -
-----------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port
```

# Puertos en estado: Error Disabled

- Una violación a la seguridad de puerto puede dejar al puerto en un estado de “error disabled” (deshabilitado por error)
- Un puerto en error disabled está shutdown
- El switch comunicará estos hechos a través de mensajes de la consola
- El interruptor se comunicará estos hechos a través de mensajes de la consola

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

# Estado del Puerto en el estado Error Disabled

- El comando show interface también revela un puerto del switch en el estado error disabled

```
S1# show interface fa0/18 status
Port Name  Status        Vlan  Duplex  Speed   Type
Fa0/18     err-disabled  1     auto    auto    10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.292b.4c75:1
Security Violation Count   : 1
```