

Configuración del Switch

Clase “05”

Los switches se deben configurar para que sean resistentes a los ataques de todo tipo y, al mismo tiempo, protejan los datos de los usuarios y permitan que haya conexiones de alta velocidad. La seguridad de puertos es una de las características de seguridad que proporcionan los switches administrados por Cisco.

En este capítulo, se analizan algunas de las opciones de configuración básica de switch que se requieren para mantener un entorno LAN conmutado seguro y disponible.

Secuencia de arranque del switch



la variable de entorno BOOT se establece con el comando **boot system** del modo de configuración global. Observe que el IOS se ubica en una carpeta distinta y que se especifica la ruta de la carpeta. Use el comando **show boot** para ver la configuración actual del archivo de arranque de IOS.

Recuperación tras un bloqueo del sistema

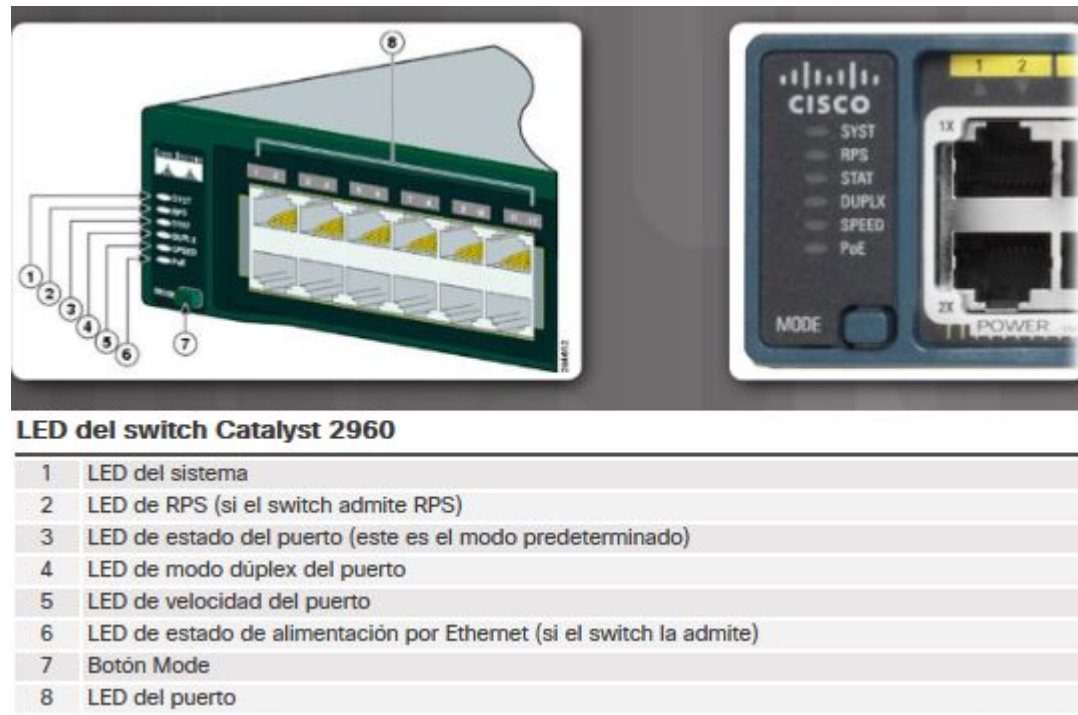
```
Switch# dir flash:
Directory of flash:/

 2 -rw- 11607161 Mar 1 2013 03:10:47 +00:00 c2960-lanbasek9-ms.150-2.3E.bin
 3 -rw-      1809 Mar 1 2013 00:02:48 +00:00 config.text
 5 -rw-      1919 Mar 1 2013 00:02:48 +00:00 private-config.text
 6 -rw-      59416 Mar 1 2013 00:02:49 +00:00 multiple-fs

32514048 bytes total (20841472 bytes free)
Switch#
```

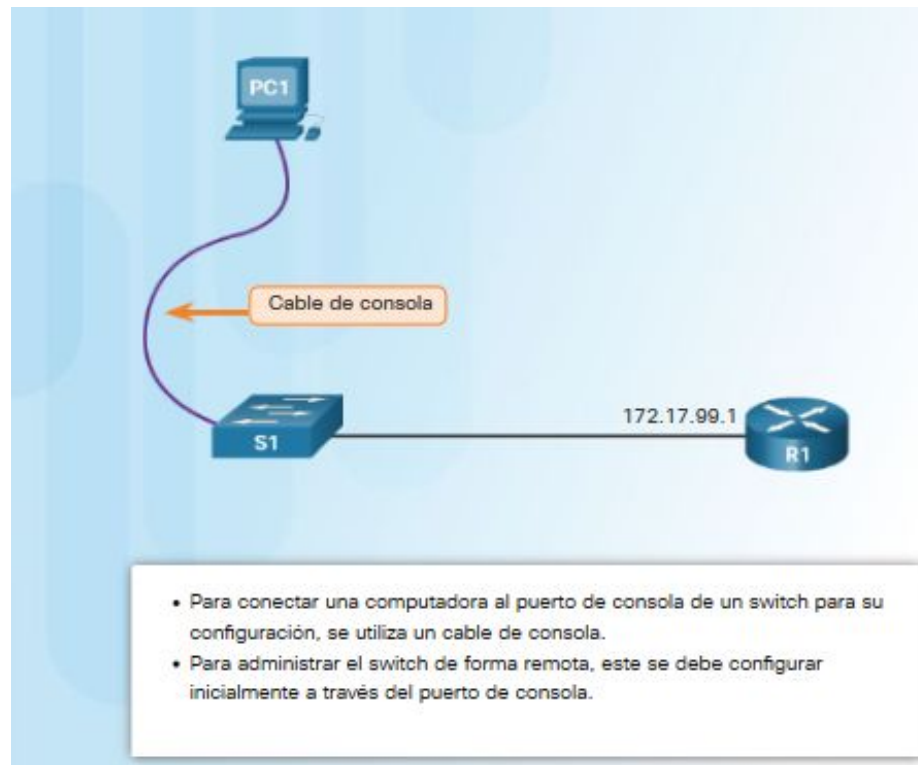
La línea de comandos de boot loader admite comandos para formatear el sistema de archivos flash, volver a instalar el software del sistema operativo y recuperar una contraseña perdida u olvidada. Por ejemplo, el comando **dir** se puede usar para ver una lista de archivos dentro de un directorio específico, como se muestra en la figura.

Indicadores LED de los switches



Configuración Básica del Switch

Preparación para la administración básica de un switch



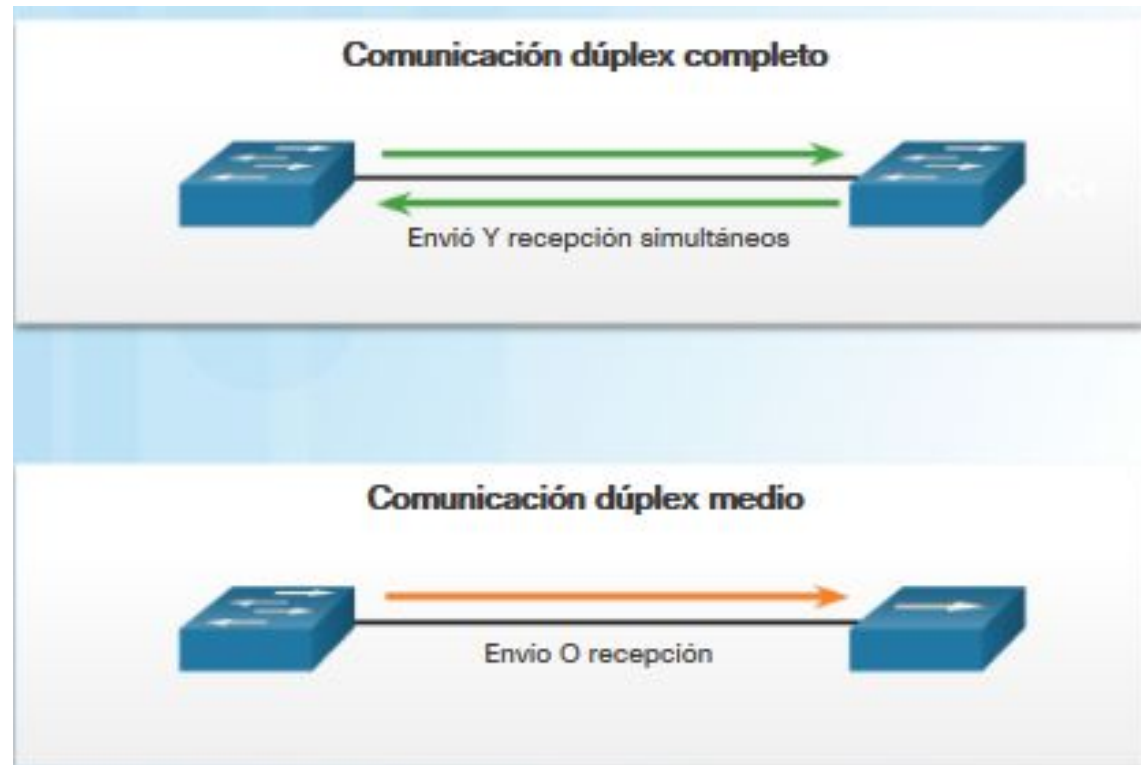
Configuración del acceso a la administración básica de un switch con IPv4

Comandos de IOS de un switch Cisco

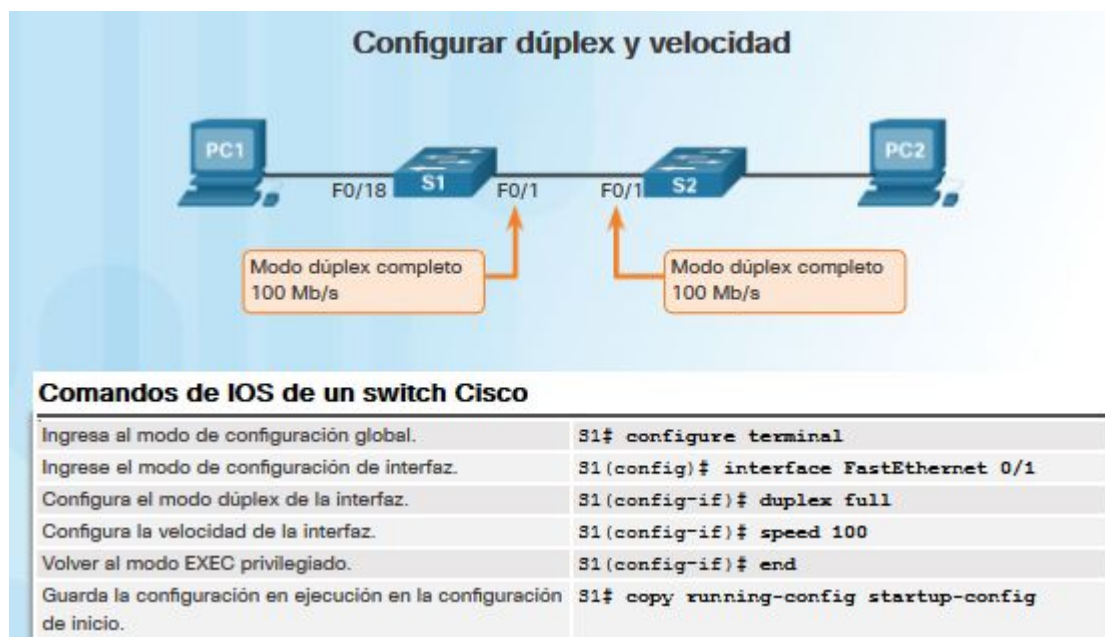
Ingresa al modo de configuración global.	<code>S1# configure terminal</code>
Configure el gateway predeterminado para el switch.	<code>S1(config)# ip default-gateway 172.17.99.1</code>
Vuelva al modo EXEC privilegiado.	<code>S1(config)# end</code>
Guarda la configuración en ejecución en la configuración de inicio.	<code>S1# copy running-config startup-config</code>



Comunicación dúplex

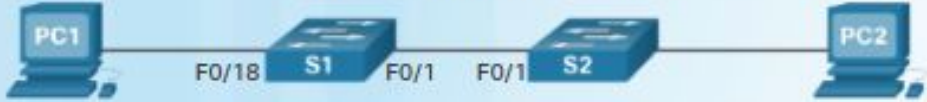


Configuración de puertos de switch en la capa física



Auto-MDIX

Configure auto-MDIX



The diagram illustrates a network topology for configuring Auto-MDIX. It consists of two switches, S1 and S2, connected in series. PC1 is connected to S1 at interface F0/18, and PC2 is connected to S2 at interface F0/1. The connection between S1 and S2 is at interface F0/1 on both switches.

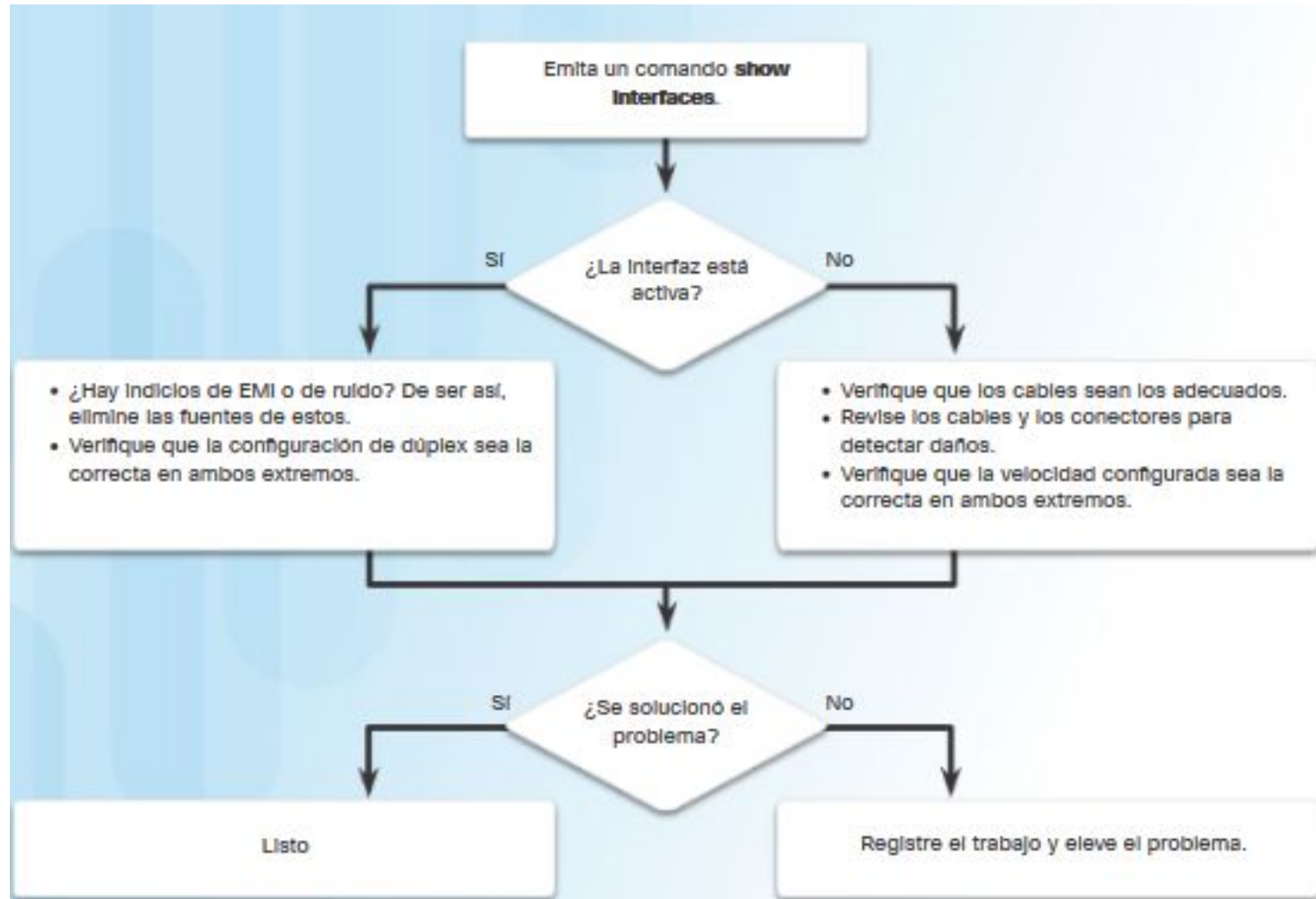
Comandos de IOS de un switch Cisco

Ingresa al modo de configuración global.	S1# <code>configure terminal</code>
Ingresa el modo de configuración de interfaz.	S1(config)# <code>interface fastethernet 0/1</code>
Configura la interfaz para autonegociar la comunicación dúplex con el dispositivo conectado.	S1(config-if)# <code>duplex auto</code>
Configura la interfaz para negociar automáticamente la velocidad con el dispositivo conectado.	S1(config-if)# <code>speed auto</code>
Habilita auto-MDIX en la interfaz.	S1(config-if)# <code>mdix auto</code>
Vuelve al modo EXEC privilegiado.	S1(config-if)# <code>end</code>
Guarda la configuración en ejecución en la configuración de inicio.	S1# <code>copy running-config startup-config</code>

Verificación de la configuración de puertos de un switch

Comandos de IOS de un switch Cisco	
Muestra el estado y la configuración de la interfaz.	S1# <code>show interfaces [interface-id]</code>
Muestra la configuración de inicio actual.	S1# <code>show startup-config</code>
Muestra la configuración de funcionamiento actual.	S1# <code>show running-config</code>
Muestra información sobre el sistema de archivos flash.	S1# <code>show flash</code>
Muestra el estado del hardware y el software del sistema.	S1# <code>show version</code>
Muestra el historial de comandos introducidos.	S1# <code>show history</code>
Muestra información de IP de una interfaz.	S1# <code>show ip [interface-id]</code>
Muestra la tabla de direcciones MAC.	S1# <code>show mac-address-table</code>
	OR S1# <code>show mac address-table</code>

Resolución de problemas de la capa de acceso a la red

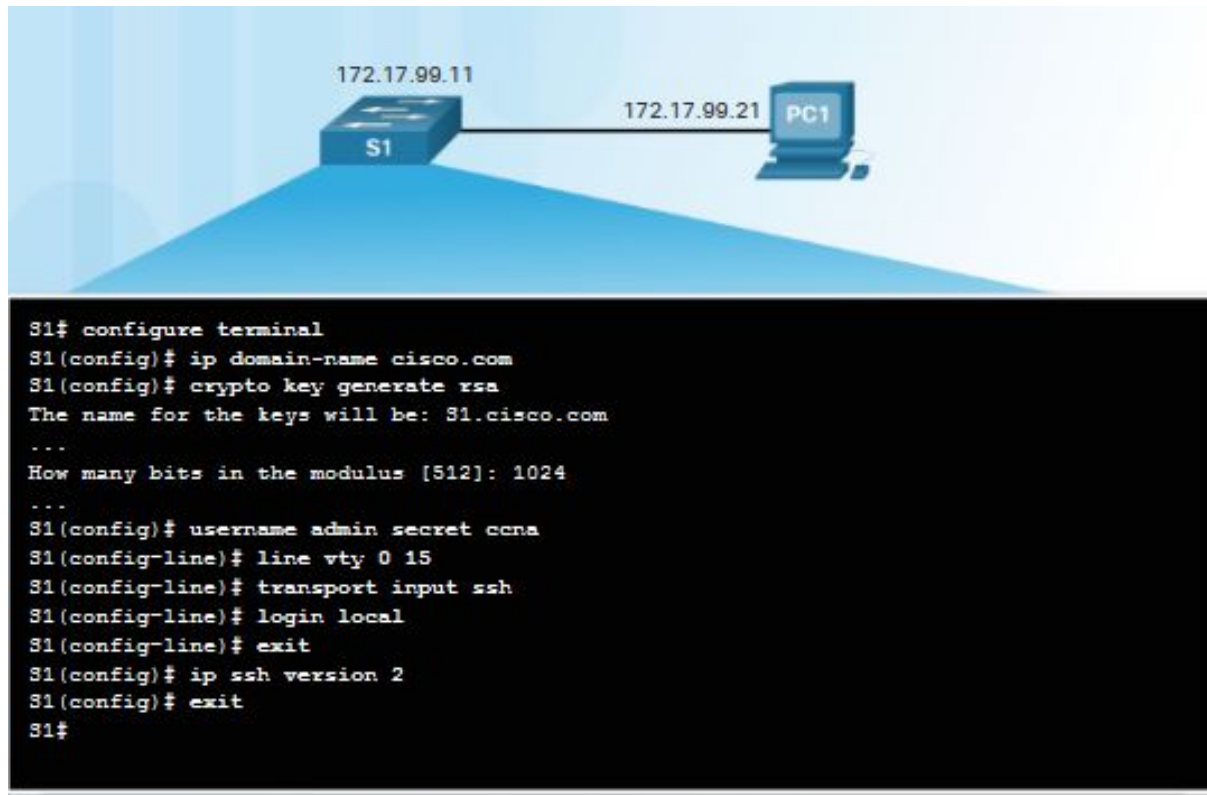


Funcionamiento de SSH

Shell seguro (SSH) es un protocolo que proporciona una conexión de administración segura (cifrada) a un dispositivo remoto. El SSH debe reemplazar a Telnet para las conexiones de administración. Telnet es un protocolo más antiguo que usa la transmisión no segura de texto no cifrado de la autenticación de inicio de sesión (nombre de usuario y contraseña) y de los datos transmitidos entre los dispositivos que se comunican.

```
S1> show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M),
Version 15.0(2)SE, RELEASE SOFTWARE (fc1)
<se omitió el resultado>
```

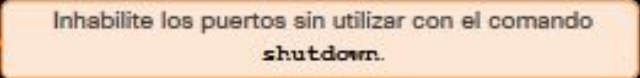

Configuración de SSH



Seguridad de puertos

Asegurar los puertos sin utilizar

```
31# show run
Building configuration...
...
version 15.0
hostname 31
...
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 description web server
!
interface FastEthernet0/7
 shutdown
!
...
```



Seguridad de puertos: funcionamiento



Implemente seguridad en todos los puertos del switch

- Especificar una única dirección MAC o un grupo de direcciones MAC válidas permitidas en un puerto.
- Especificar que un puerto se desactive automáticamente si se detectan direcciones MAC no autorizadas.

Seguridad de puertos: modos de violación de seguridad

Los modos de violación de seguridad incluyen los siguientes: Protect, Restrict y Shutdown.

Modos de violación de seguridad

Modo de violación	Envía tráfico	Envía mensaje de syslog	Muestra mensaje de error	Incrementa el contador de violaciones	Desactiva el puerto
Protect	No	No	No	No	No
Restrict	No	Sí	No	Sí	No
Apagado	No	No	No	Sí	Sí

La violación a la seguridad ocurre en estas situaciones

- Una estación cuya dirección MAC no figura en la tabla de direcciones intenta acceder a la interfaz cuando la tabla está completa.
- Una dirección se utiliza en dos interfaces seguras en la misma VLAN.

Seguridad de puertos: configuración

Comandos de CLI de Cisco IOS

Especifica la interfaz que se debe configurar para la seguridad de puertos.	<code>S1(config)# interface fastethernet 0/18</code>
Establezca la interfaz en modo de acceso.	<code>S1(config-if)# switchport mode access</code>
Establezca la seguridad de puerto en la interfaz.	<code>S1(config-if)# switchport port-security</code>

Comandos de CLI de Cisco IOS

Especifica la interfaz que se debe configurar para la seguridad de puertos.	<code>S1(config)# interface fastethernet 0/19</code>
Establezca la interfaz en modo de acceso.	<code>S1(config-if)# switchport mode access</code>
Establezca la seguridad de puerto en la interfaz.	<code>S1(config-if)# switchport port-security</code>
Establece la cantidad máxima de direcciones seguras permitidas en el puerto.	<code>S1(config-if)# switchport port-security maximum 10</code>
Habilita el aprendizaje por persistencia.	<code>S1(config-if)# switchport port-security mac-address sticky</code>

Seguridad de puertos: verificación

```
S1# show port-security interface fastethernet 0/18
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0025.83e6.4b01:1
Security Violation Count : 0
```

Puertos en estado de inhabilitación por errores

```
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
```


¿Preguntas?

Laboratorio

Gracias por su atención