



## Capítulo 5: Configuración de un switch



## Routing and Switching Essentials v6.0

Cisco | Networking Academy®  
Mind Wide Open™



## 5.1 Configuración básica de un switch



Cisco | Networking Academy®  
Mind Wide Open™



Configurar un switch con parámetros iniciales

# Configurar el acceso a la administración de un switch

## Configurar interfaz de administracion de switch

### Comandos de IOS de un switch Cisco

Ingrese al modo de configuración global.	<b>S1# configure terminal</b>
Ingrese al modo de configuración de interfaz para la SVI.	<b>S1(config)# interface vlan 99</b>
Configura la dirección IP de la interfaz de administración.	<b>S1(config-if)# ip address 172.17.99.11 255.255.255.0</b>
Habilita la interfaz de administración.	<b>S1(config-if)# no shutdown</b>
Vuelva al modo EXEC privilegiado.	<b>S1(config-if)# end</b>
Guarda la configuración en ejecución en la configuración de inicio.	<b>S1# copy running-config startup-config</b>

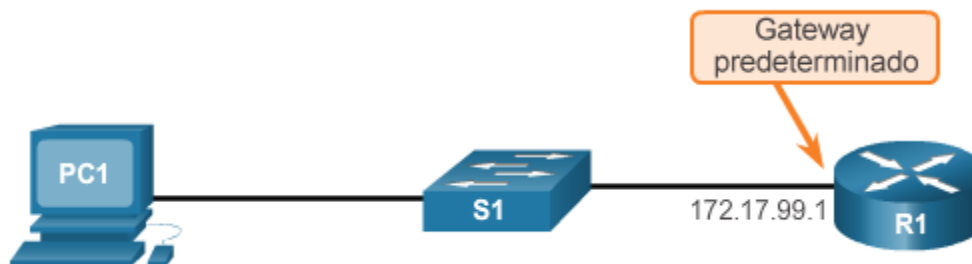


Configurar un switch con parámetros iniciales

# Configurar el acceso a la administración de un switch (continuación)

## Configuración del gateway predeterminado de un switch

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>





Configurar un switch con parámetros iniciales

# Configurar el acceso a la administración de un switch (continuación)

Verificación de la configuración de la interfaz de administración de un switch

```
S1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan99	172.17.99.11	YES	manual	up	down

<output omitted>





## 5.2 Seguridad de switches: Administración e implementación



Cisco | Networking Academy®  
Mind Wide Open™



## Acceso remoto seguro

# Funcionamiento de SSH

- Shell seguro (SSH) es un protocolo que proporciona una conexión segura (cifrada) a un dispositivo remoto basada en la línea de comandos.
- SSH debería reemplazar a Telnet para las conexiones de administración, debido a sus sólidas características de cifrado.
- SSH utiliza el puerto TCP 22 de manera predeterminada.
- Telnet utiliza el puerto TCP 23.
- Para habilitar SSH en switches Catalyst 2960, se requiere una versión del software de IOS que incluya características y capacidades criptográficas (cifradas).

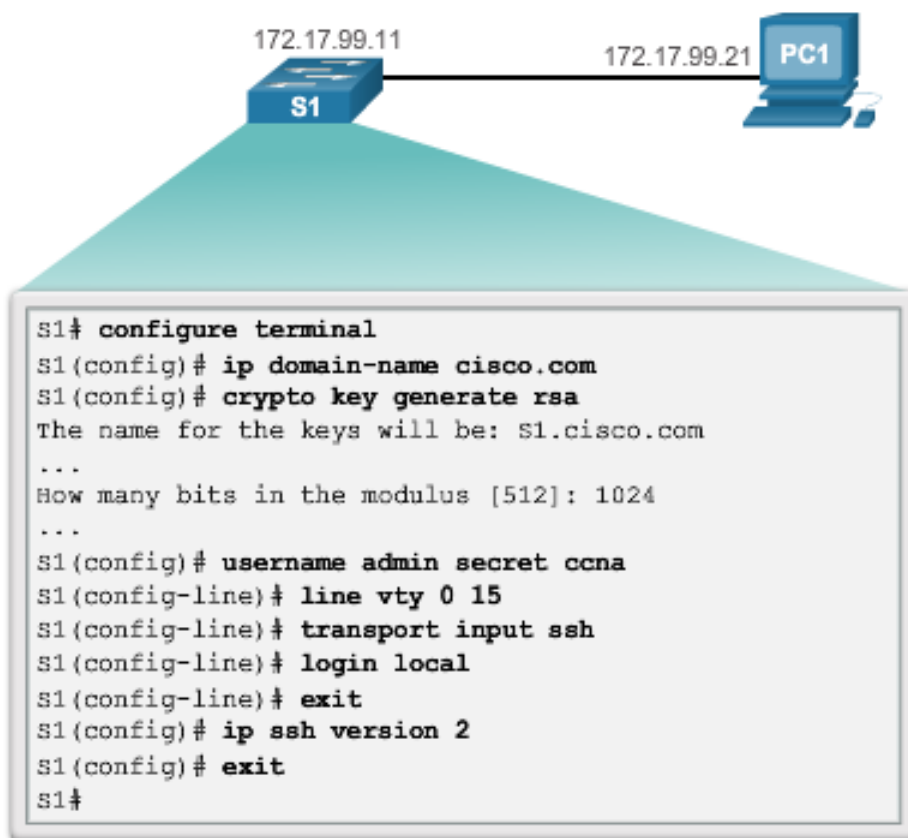


## Acceso remoto seguro

# Configuración de SSH

### Configuración de SSH para la administración remota

1. Verificar la compatibilidad con SSH: `show ip ssh`.
2. Configurar el dominio IP
3. Generar pares de claves RSA
4. Configurar la autenticación de usuario
5. Configurar las líneas vty
6. Habilitar la versión 2 de SSH.





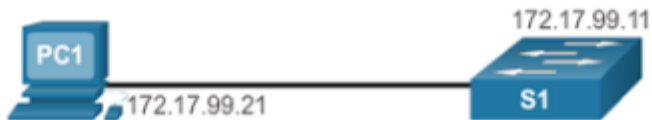


## Acceso remoto seguro

# Verificación de SSH

**ssh -l admin 172.16.99.11**

Conexión de SSH para la administración remota



```

172.17.99.11 - PuTTY
Login as: admin
Using keyboard-interactive
authentication.
Password:

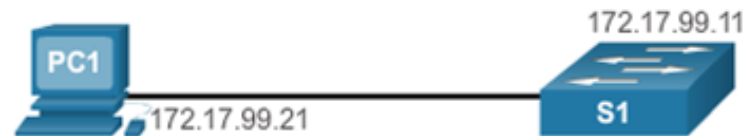
S1>enable
Password:
S1#
  
```



## Acceso remoto seguro

# Verificación de SSH (continuación)

### Verificación del estado y la configuración de 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
AAAAB3NzaC1yc2EAAAADAQABAAQGCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVluKNqVMOMtLg8Ud4qAiLbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGM088OUJQL3Q==

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



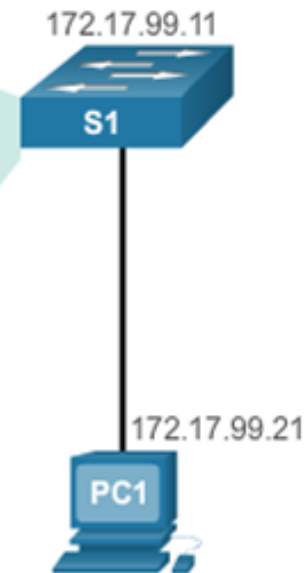
## Seguridad de los puertos de un switch

# Seguridad de los puertos sin utilizar

### Deshabilitar puertos en desuso

Inhabilite los puertos sin utilizar con el comando **shutdown**.

```
S1# show run
Building configuration...
...
version 15.0
hostname S1
...
interface FastEthernet0/4
  shutdown
!
interface FastEthernet0/5
  shutdown
!
interface FastEthernet0/6
  description web server
!
interface FastEthernet0/7
  shutdown
!
...
```





## Seguridad de los puertos de un switch

# Seguridad de puertos: Funcionamiento

- Se permite el acceso a las direcciones MAC de los dispositivos legítimos, mientras que otras direcciones MAC se rechazan.
- Cualquier intento adicional de conexión por parte de direcciones MAC desconocidas generará una violación de seguridad.
- Las direcciones MAC seguras se pueden configurar de varias maneras:
  - **Direcciones MAC seguras estáticas:** se configuran manualmente y se agregan a la configuración en ejecución (`switchport port-security mac-address dirección-mac`)
  - **Direcciones MAC seguras dinámicas:** se eliminan al reiniciarse el switch
  - **Direcciones MAC seguras persistentes:** se agregan a la configuración en ejecución y se obtienen en forma dinámica (comando del modo de configuración de interfaces `switchport port-security mac-address sticky`)



## Seguridad de los puertos de un switch

# Seguridad de puertos: Funcionamiento

### ■ Direcciones MAC seguras estáticas:

`switchport port-security mac-address dirección-mac`

- Se configura manualmente.
- Se agrega a la tabla de direcciones CAM (Content Addressable Memory).
- Se guarda en la *running-config*.
- Se puede hacer permanente guardando la configuración.

### ■ Direcciones MAC seguras dinámicas:

- Se aprende del tráfico que atraviesa la interfaz.
- Se la guarda en la tabla de direcciones CAM (Content Addressable Memory).
- Se pierde cuando se reinicia el equipo.

### ■ Direcciones MAC seguras persistentes:

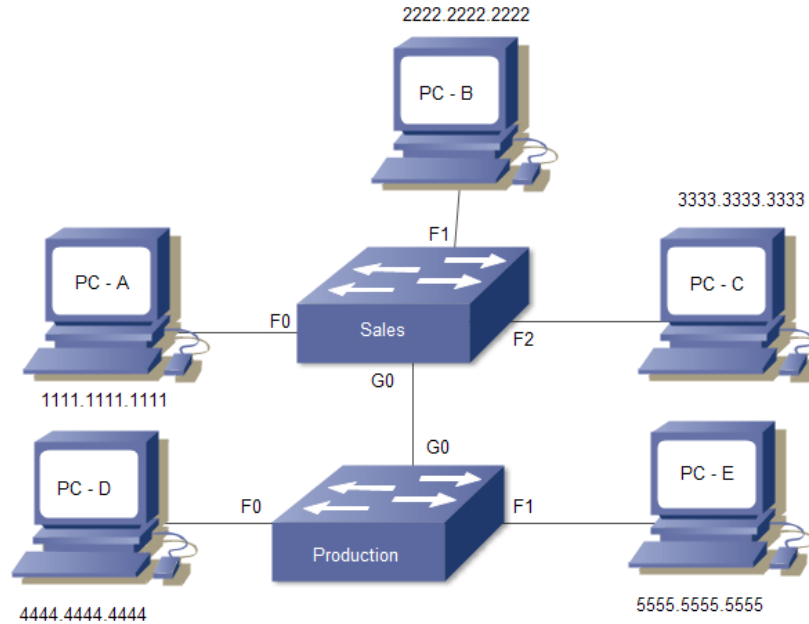
`switchport port-security mac-address sticky`

- Le dice al switch que de forma dinámica aprenda la dirección MAC de origen y agregue los comandos port-security al running-config.



## Tabla CAM

# CAM (Content Addressable Memory)



Sales

Production

MAC Address	Port
1111.1111.1111	F0
2222.2222.2222	F1
3333.3333.3333	F2
4444.4444.4444	G0
5555.5555.5555	G0

MAC Address	Port
1111.1111.1111	G0
2222.2222.2222	G0
3333.3333.3333	G0
4444.4444.4444	F0
5555.5555.5555	F1



## Seguridad de los puertos de un switch

# Seguridad de puertos: Modos de violación de seguridad

- IOS considera que hay una violación de seguridad cuando:
  - Se agregó la cantidad máxima de direcciones MAC seguras a la tabla CAM para esa interfaz, y una estación cuya dirección MAC no figura en la tabla de direcciones intenta acceder a la interfaz.
- Cuando se detecta una violación, hay tres acciones posibles que se pueden realizar:
  - Proteger: no se recibe ninguna notificación
  - Restringir: se recibe una notificación sobre una violación de seguridad
  - Apagar
  - Comando del modo de configuración de interfaces **switchport port-security violation {*protect* | *restrict* | *shutdown*}**



## Seguridad de los puertos de un switch

# Seguridad de puertos: Modos de violación de seguridad (continuación)

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
Proteger	No	No	No	No	No
Restringir	No	Sí	No	Sí	No
Apagar	No	No	No	Sí	Sí





## Seguridad de los puertos de un switch

# Seguridad de puertos: Configuración

### Opciones predeterminadas de seguridad de puerto

Característica	Configuración predeterminada
Seguridad del puerto	Inhabilitada en un puerto.
Número máximo de direcciones MAC seguras	1
Modo de violación	Shutdown. El puerto se desactiva cuando se supera la cantidad máxima de direcciones MAC seguras.
Aprendizaje de direcciones sin modificación	Deshabilitado

### Configurar la seguridad de los puertos dinámicos



#### 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 el modo de interfaz en 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>

### Configurar la seguridad de puerto sin modificación



#### 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 el modo de interfaz en 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 los puertos de un switch

# Seguridad de puertos: Verificación

### Verificación de dirección MAC: configuración dinámica

```
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
```

### Verificación de dirección MAC: configuración persistente

```
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    : 10
Total MAC Addresses      : 1
Configured MAC Addresses : 0
Sticky MAC Addresses     : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```



## Seguridad de los puertos de un switch

# Seguridad de puertos: Verificación (continuación)

Verificación de MAC persistente: configuración en ejecución

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
switchport mode access
switchport port-security maximum 10
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0025.83e6.4b02
```

Verificar las 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	-



# Seguridad de los puertos de un switch

## VLAN rangos

Switch# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	