Ethernet LANs

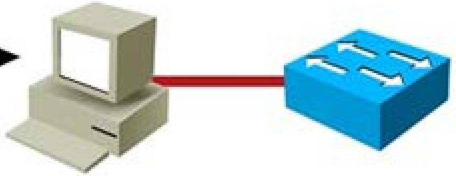
Understanding Switch Security

Common Threats to Physical Installations

- Hardware threats
- Environmental threats
- Electrical threats
- Maintenance threats

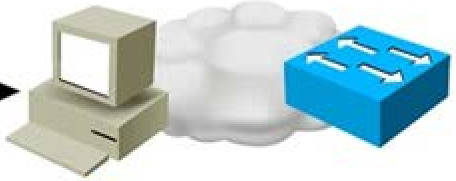
Configuring a Switch Password

```
SwitchX(config)#line console 0
SwitchX(config-line)#login
SwitchX(config-line)#password cisco
```



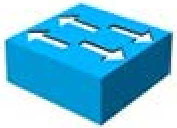
- Set the Console Password

```
SwitchX(config)#line vty 0 4
SwitchX(config-line)#login
SwitchX(config-line)#password sanjose
```



- Set the Virtual Terminal Password

```
SwitchX(config)#enable password cisco
```



- Set the Enable Password

```
SwitchX(config)#enable secret sanfran
```

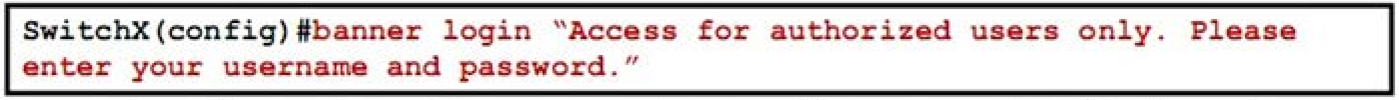
- Set the Enable Secret Password

```
SwitchX(config)#service password-encryption
SwitchX(config)#no service password-encryption
```

301P_256

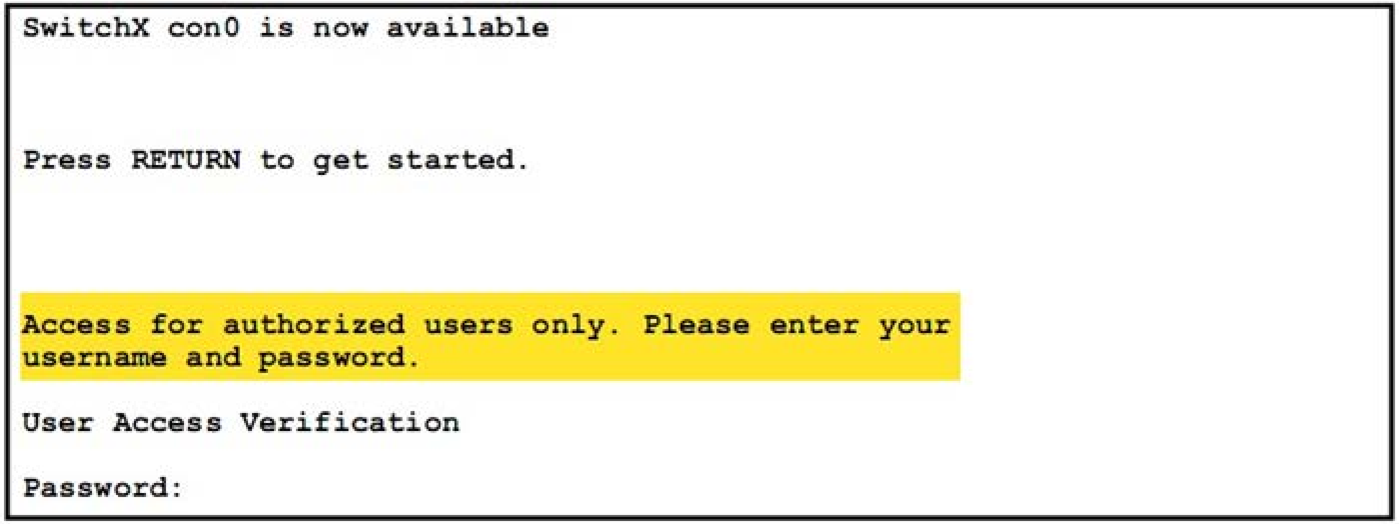
- Set the Service Password Encryption

Configuring the Login Banner



```
SwitchX(config)#banner login "Access for authorized users only. Please
enter your username and password."
```

- Enable and configure a customized banner to be displayed before the username and password login prompts.

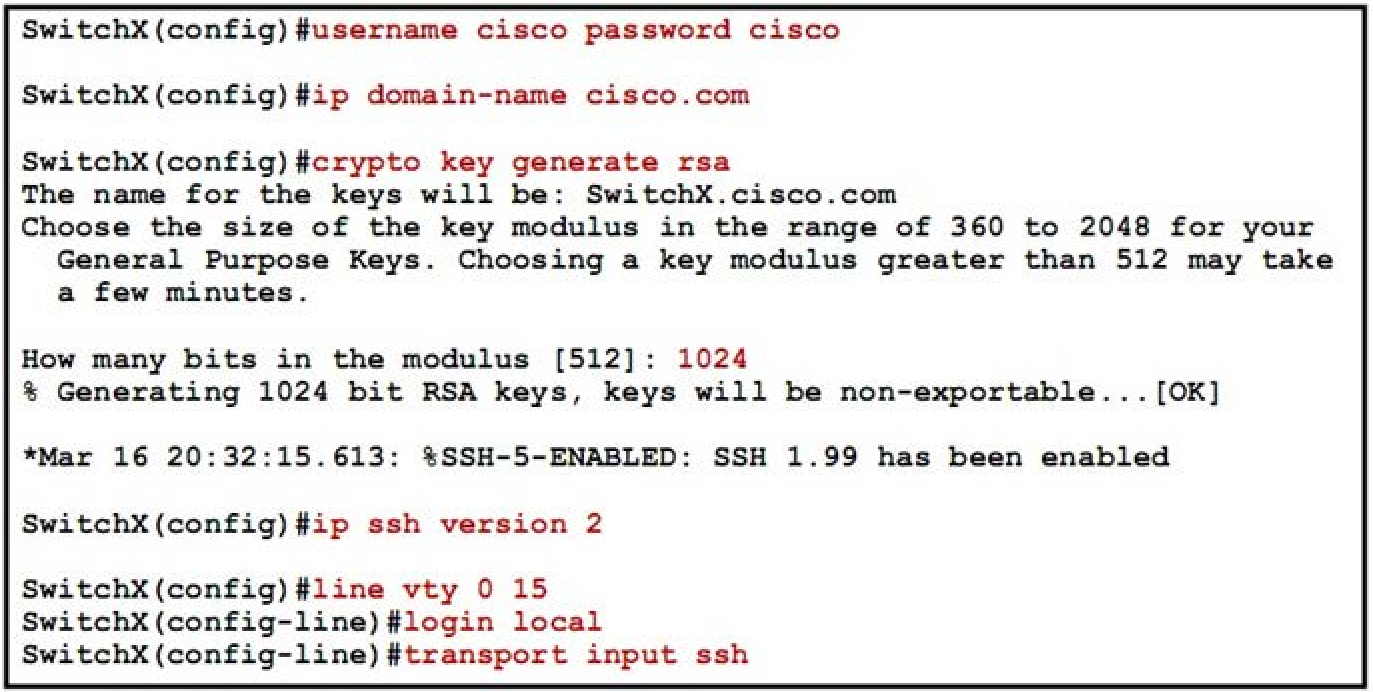


```
SwitchX con0 is now available



Press RETURN to get started.




Access for authorized users only. Please enter your
username and password.

User Access Verification

Password:
```

Telnet vs. SSH Access

- Telnet
  - Most common access method
  - Unsecure
- SSH
  - Encrypted
  - Secure

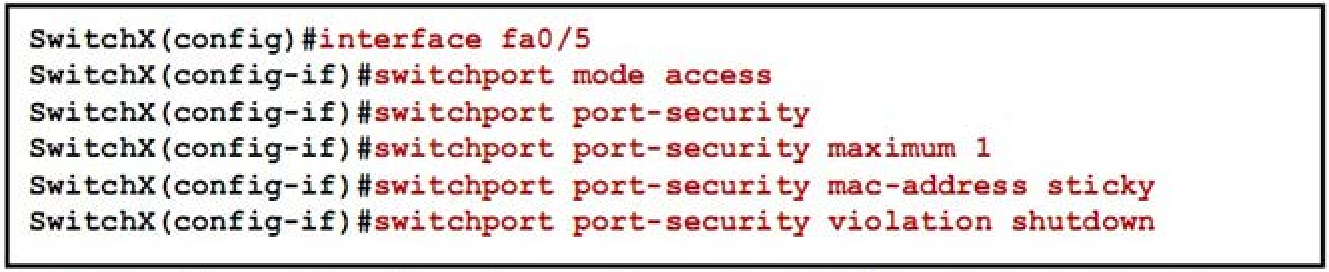
Telnet vs. SSH Access (Cont.)



```
SwitchX(config)#username cisco password cisco

SwitchX(config)#ip domain-name cisco.com

SwitchX(config)#crypto key generate rsa
The name for the keys will be: SwitchX.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 16 20:32:15.613: %SSH-5-ENABLED: SSH 1.99 has been enabled

SwitchX(config)#ip ssh version 2

SwitchX(config)#line vty 0 15
SwitchX(config-line)#login local
SwitchX(config-line)#transport input ssh
```

- Configure SSH access on vty lines

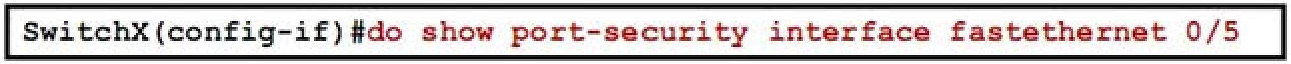
Configuring Port Security



```
SwitchX(config)#interface fa0/5
SwitchX(config-if)#switchport mode access
SwitchX(config-if)#switchport port-security
SwitchX(config-if)#switchport port-security maximum 1
SwitchX(config-if)#switchport port-security mac-address sticky
SwitchX(config-if)#switchport port-security violation shutdown
```

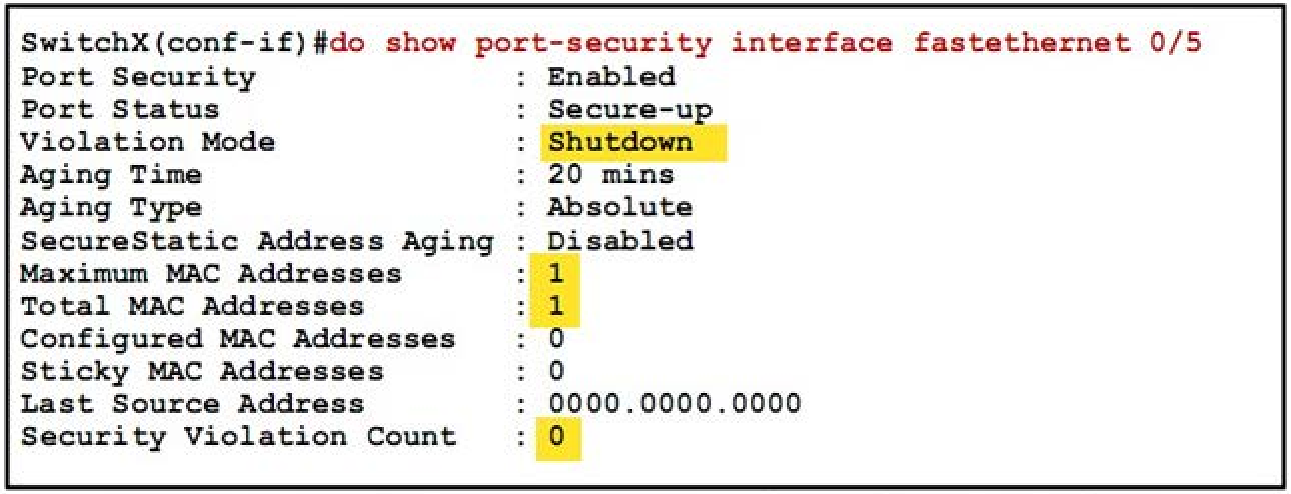
- Configuration of port security on the fa0/5 port to limit and identify MAC addresses of the stations that are allowed to access the port

Verifying Port Security on the Catalyst 2960 Series



```
SwitchX(config-if)#do show port-security interface fastethernet 0/5
```

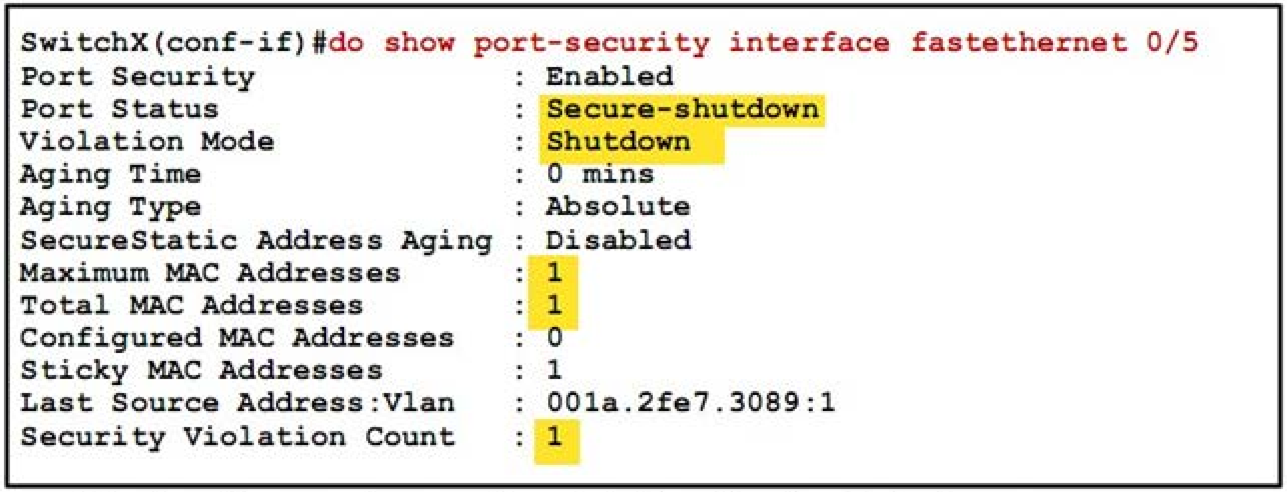
- Use **do** command to execute user EXEC or privileged EXEC commands from any configuration modes or submodes.



```
SwitchX(conf-if)#do show port-security interface fastethernet 0/5
Port Security                 : Enabled
Port Status                   : Secure-up
Violation Mode                : Shutdown
Aging Time                    : 20 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           : 0000.0000.0000
Security Violation Count      : 0
```

- Display the port security settings defined for the interface FastEthernet 0/5

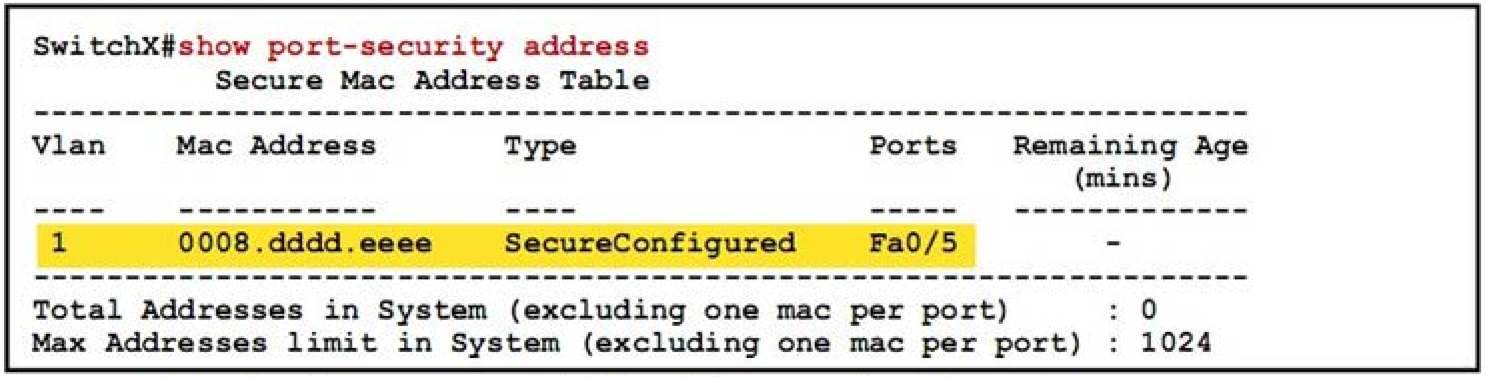
Port Security Violation Example



```
SwitchX(conf-if)#do show port-security interface fastethernet 0/5
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         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : 001a.2fe7.3089:1
Security Violation Count    : 1
```

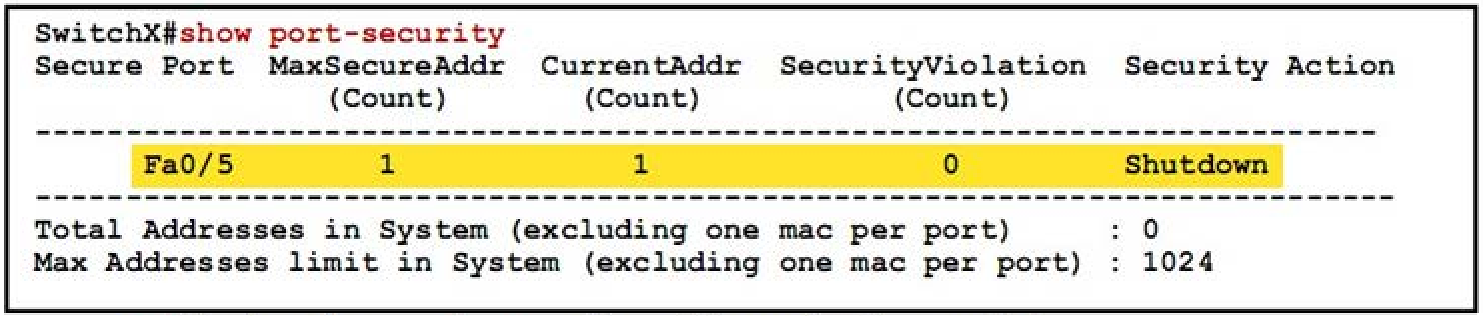
- Display the port security violation for the interface FastEthernet 0/5

Verifying Port Security on the Catalyst 2960 Series (Cont.)



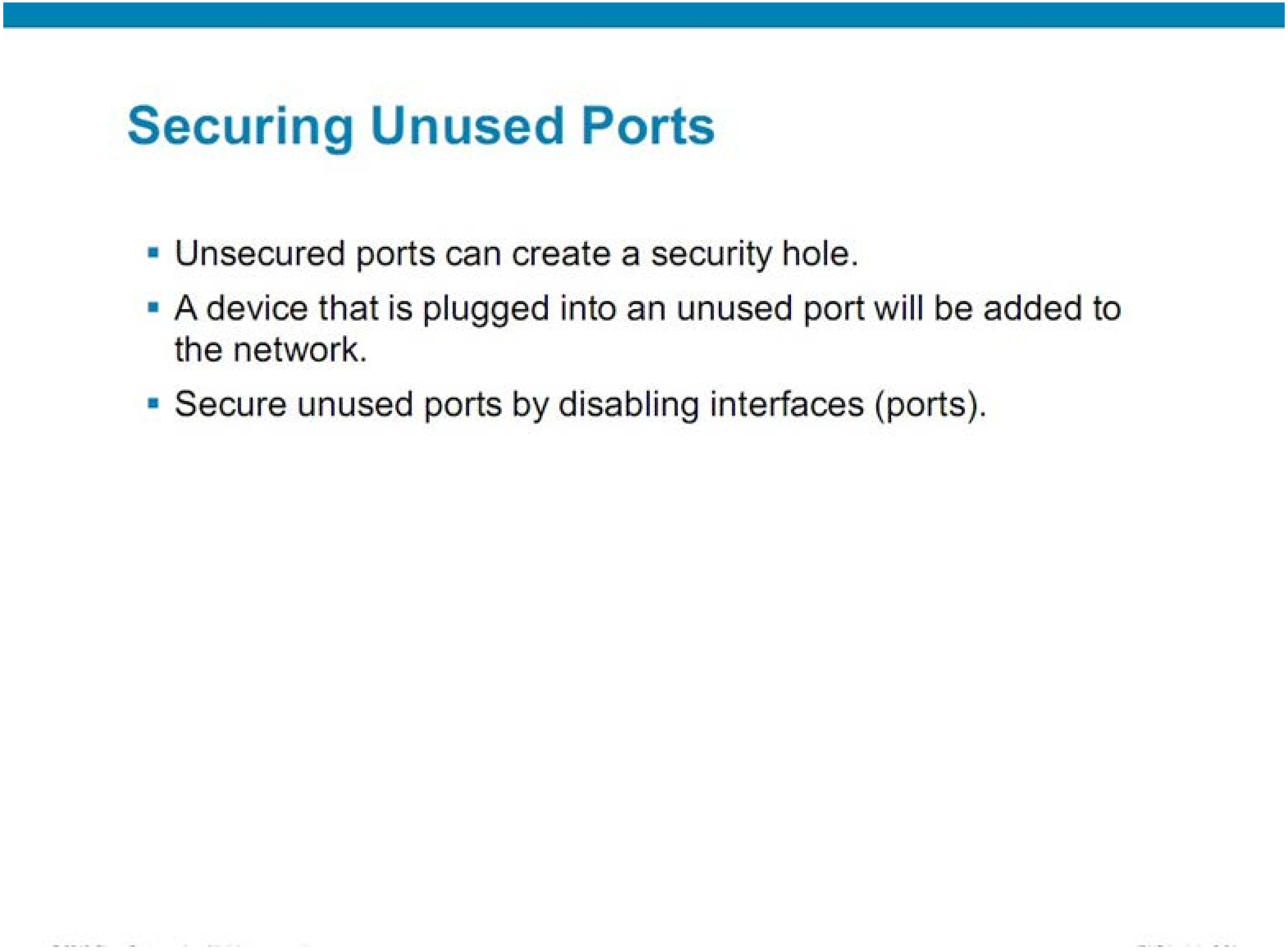
```
SwitchX#show port-security address
          Secure Mac Address Table
-------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
 1      0008.dddd.eeee    SecureConfigured    Fa0/5         -
-------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

- Display the secure MAC addresses for all ports



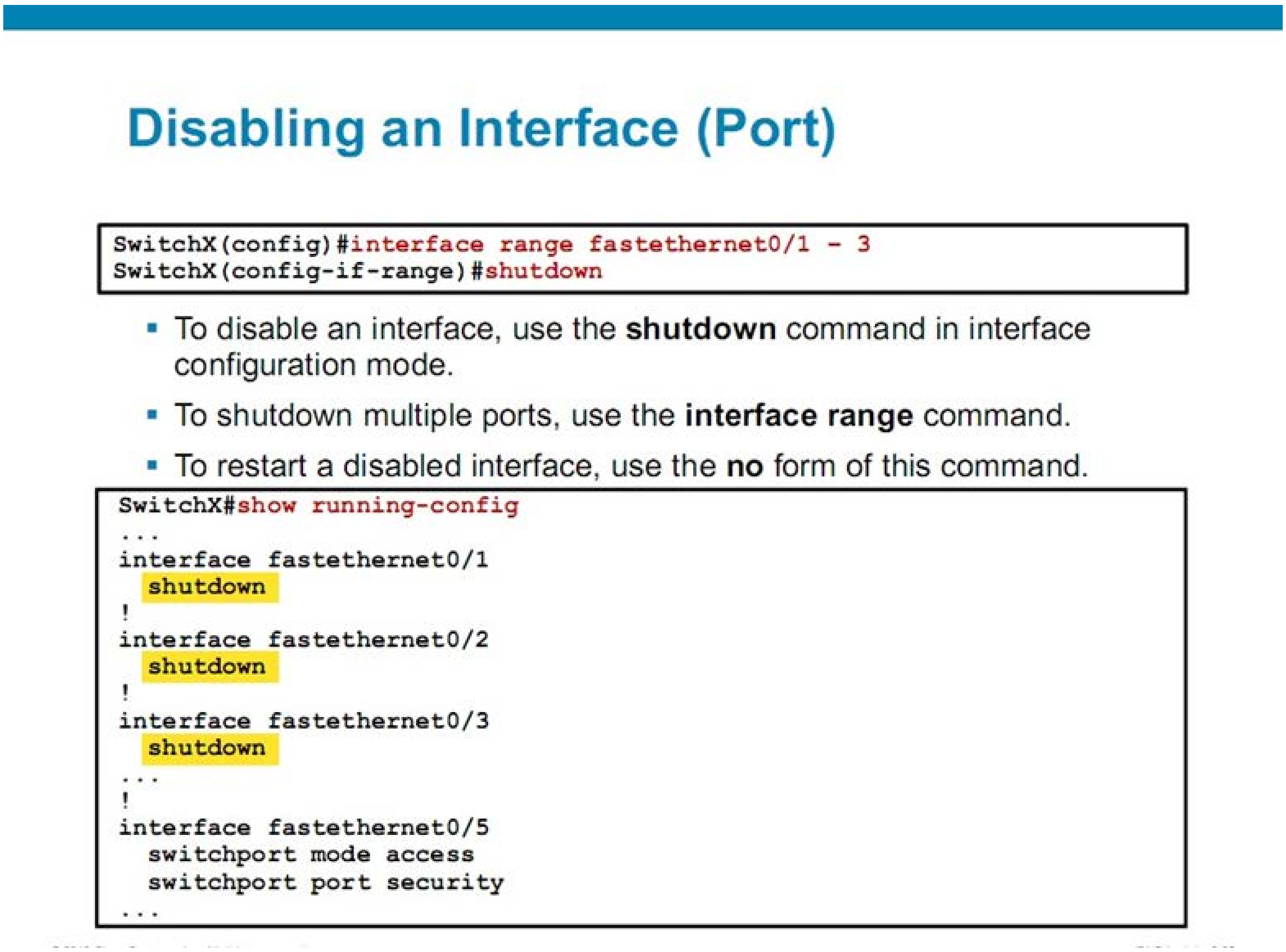
```
SwitchX#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/5           1              1                0          Shutdown
----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

- Display the port security settings for the switch



Securing Unused Ports

- Unsecured ports can create a security hole.
- A device that is plugged into an unused port will be added to the network.
- Secure unused ports by disabling interfaces (ports).



Disabling an Interface (Port)

```
SwitchX(config)#interface range fastethernet0/1 - 3
SwitchX(config-if-range)#shutdown
```

- To disable an interface, use the **shutdown** command in interface configuration mode.
- To shutdown multiple ports, use the **interface range** command.
- To restart a disabled interface, use the **no** form of this command.

```
SwitchX#show running-config
...
interface fastethernet0/1
  shutdown
!
interface fastethernet0/2
  shutdown
!
interface fastethernet0/3
  shutdown
...
!
interface fastethernet0/5
  switchport mode access
  switchport port security
...
```

Summary

- The first level of security is physical.
- Passwords can be used to limit access to users that have been given the password.
- The login banner can be used to display a message before the user is prompted for a username.
- Telnet sends session traffic in cleartext; SSH encrypts the session traffic.
- Port security can be used to limit MAC addresses to a port.
- Unused ports should be shut down.