Antonio Cianfrani

Inter-VLAN Routing

Inter-VLAN Routing

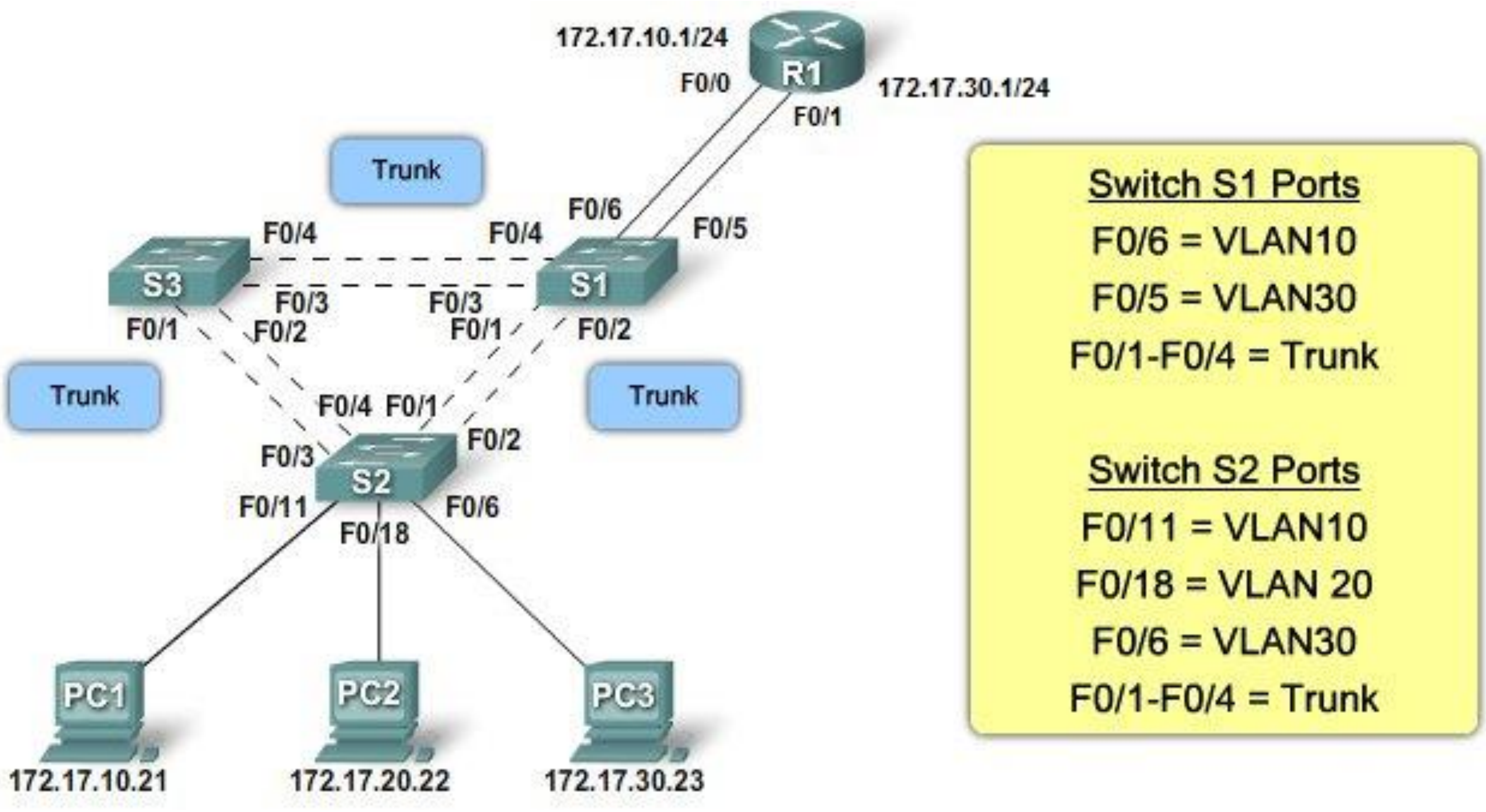
- In a LAN with many VLANs, the communication among host belonging to different VLANs (inter-VLAN routing) is not possible.
- To allow inter-VLAN routing, a router must be present.
- To different ways to implement inter-VLAN routing:
  - ✓ Traditional Inter-VLAN;
  - ✓ "Router-on-a-stick" Inter-VLAN.

Traditional Inter-VLAN

- A router must be connected to a switch.
- The router must be connected to the switch with a certain amount of physical interfaces.
- The number of router-to-switch physical links is equal to the number of VLANs able to communicate each other.
- Each router interface is associated to a VLAN → an IP address of the VLAN block must be assigned to it.
- The switch ports connected to the router must be configured in **access** mode.

Traditional Inter-VLAN: example (1/3)

- Assumption: only VLAN 10 and VLAN 30 are allowed to communicate.



Switch S1 Ports

F0/6 = VLAN10

F0/5 = VLAN30

F0/1-F0/4 = Trunk

Switch S2 Ports

F0/11 = VLAN10

F0/18 = VLAN 20

F0/6 = VLAN30

F0/1-F0/4 = Trunk

Traditional Inter-VLAN: example (2/3)

- **Router**: interfaces configuration

```
R1(config)# interface Fa 0/0
R1(config-if)#ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# interface Fa 0/1
R1(config-if)#ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
```

Traditional Inter-VLAN: example (3/3)

- **Switch**: configuration of the ports connected to the router

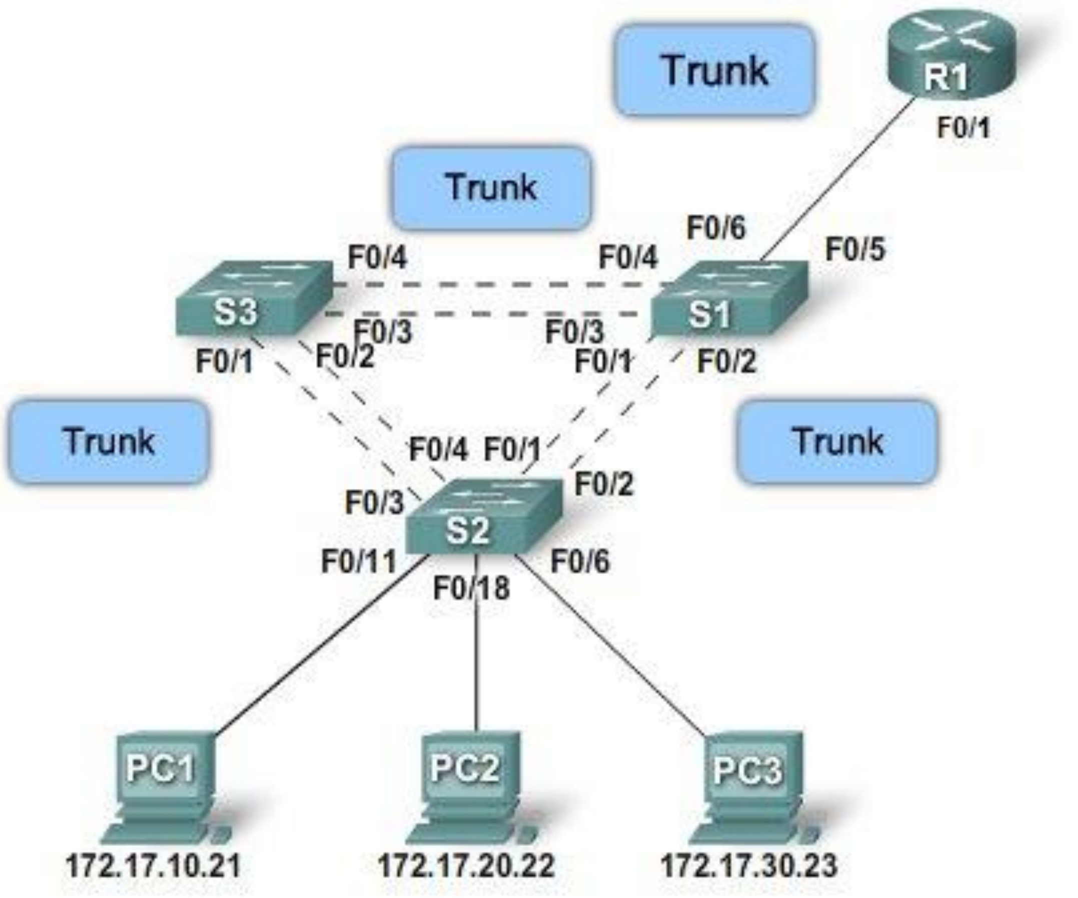
```
S1(config)# interface Fa 0/6
S1(config-if)# switchport access vlan 10

S1(config)# interface Fa 0/5
S1(config-if)# switchport access vlan 30
```

“Router-on-a-stick” Inter-VLAN

- Even in this case, a router is present.
- The router is connected to a switch by means of a single physical interface.
- The physical interface of the router is split into virtual interfaces (the number of virtual interfaces is equal to the number of VLANs able to communicate each other).
- Each virtual interface (subinterface) of the router is associated to a single VLAN (it must have an IP address of the VLAN block).
- The switch port connected to the router must be configured in **trunk** mode.

“Router-on-a-stick” Inter-VLAN: example (1/3)

- Only VLAN 10 and VLAN 30 are allowed to communicate.



R1 Subinterfaces

F0/0.10: 172.17.10.1

F0/0.20: 172.17.20.1

F0/0.30: 172.17.30.1

Switch S1 Ports

F0/1-F0/4 = Trunk

F0/5 = Trunk

Switch S2 Ports

F0/11 = VLAN10

F0/18 = VLAN20

F0/6 = VLAN30

F0/1-F0/4 = Trunk

“Router-on-a-stick” Inter-VLAN: example (2/3)

- **Router**: the interface connected to the switch must be split in two subinterfaces, one belonging to VLAN 10 and one to VLAN 30

```
R1(config)# interface Fa 0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0

R1(config)# interface Fa 0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0

R1(config)# interface Fa 0/0
R1(config-if)# no shutdown
```

“Router-on-a-stick” Inter-VLAN: example (3/3)

- **Switch**: the port connected to the router is configured in trunk mode

```
S1(config)# vlan 10
S1(config)# vlan 20
S1(config)# vlan 30
S1(config)# interface Fa 0/5
S1(config-if)# switchport mode trunk
```

Antonio Cianfrani

Ethernet Security

Security attacks in LAN (1/2)

- The classical attack in a LAN is the **MAC Address Flooding**.
- It exploits the security weakness of MAC forwarding table learning mechanism:
  - If an incoming frame with a new MAC source address is received, the switch add a row in the forwarding table
  - If an incoming frame has a destination MAC address not present in the forwarding table, the switch acts as an hub
  - The forwarding tables have a limited size
- MAC Address Flooding:
  - Frames with artificial source MAC address → the forwarding table is saturated → frames with new MAC destination address are forwarded in broadcast

Security attacks in LAN (2/2)

- **DHCP Spoofing:** a malicious DHCP server is inserted in the LAN, so that fake info (default gateway) are notified to LAN hosts. This is a man-in-the-middle attack

- **DHCP starvation:** attack to the DHCP servers, sending a huge amount of DHCP requests so that to use oll the available IP addresses.

Port Security (1/4)

- **Port Security**: option to be configured on switch interface/s to increase the security level of the network
- The idea of Port Security is to limit the end devices that can be connected to a specific switch interface
- The security policy is based on the source MAC address of incoming packets and on the number of different source MAC addresses allowed on the interface.

Port Security (2/4)

- If a frame having a MAC source address not allowed is received, the interface switch to ***Violation Mode:***
  - ✓ Shutdown by default (restrict).
- It is possible to allow the access to a single MAC address or to a range of MAC addresses.
- The association among the interface and the allowed MAC address/es can be dynamic or static

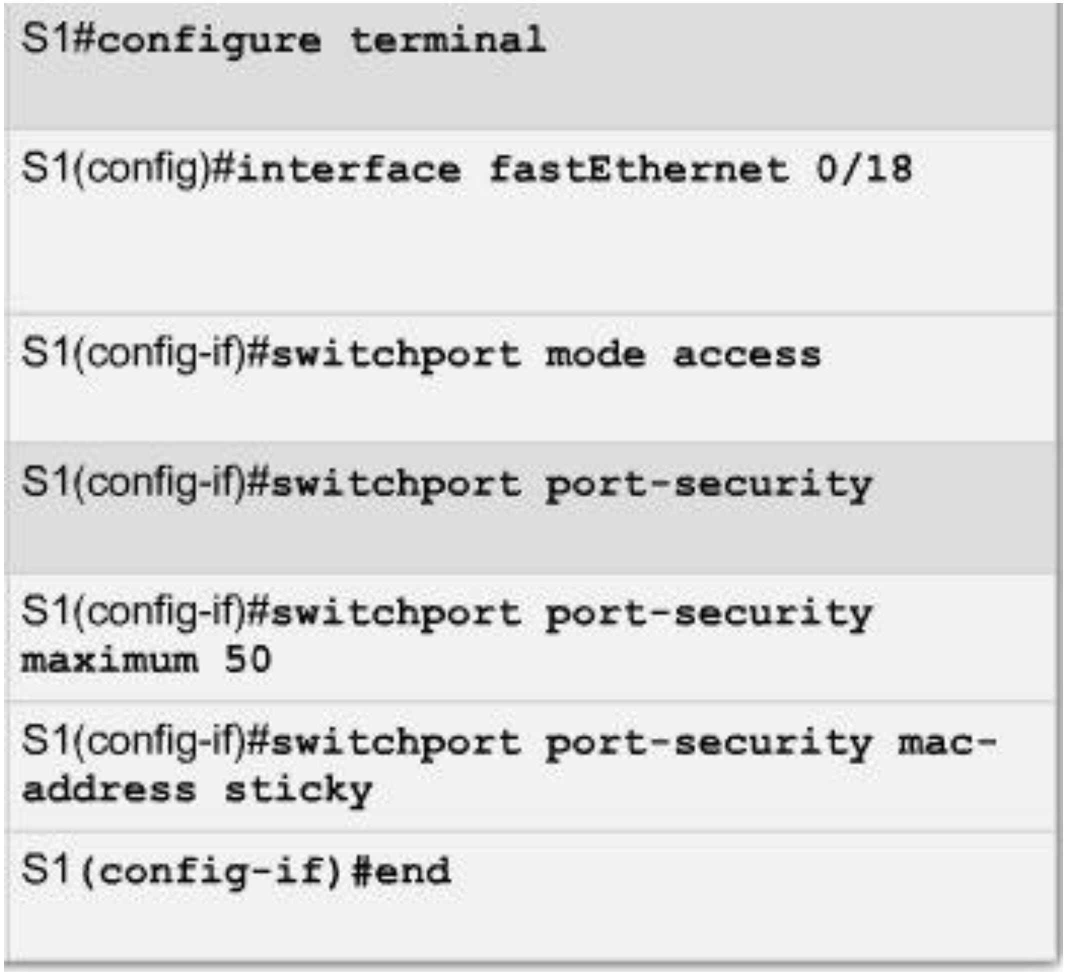
Port Security (3/4)

- Three different Port Security configuration modes:
  - Static: the allowed MAC address/es are statically configured by the LAN administrator with the command

    switchport port-security mac-address *mac-address*

  - Dynamic: the allowed MAC addresses are learned dynamically up to a fixed number (1 by default) and saved only in the secure MAC address table
  - Sticky Dynamic: the allowed MAC addresses are learned dynamically up to a fixed number and saved in the secure MAC address table and in the running configuration file.

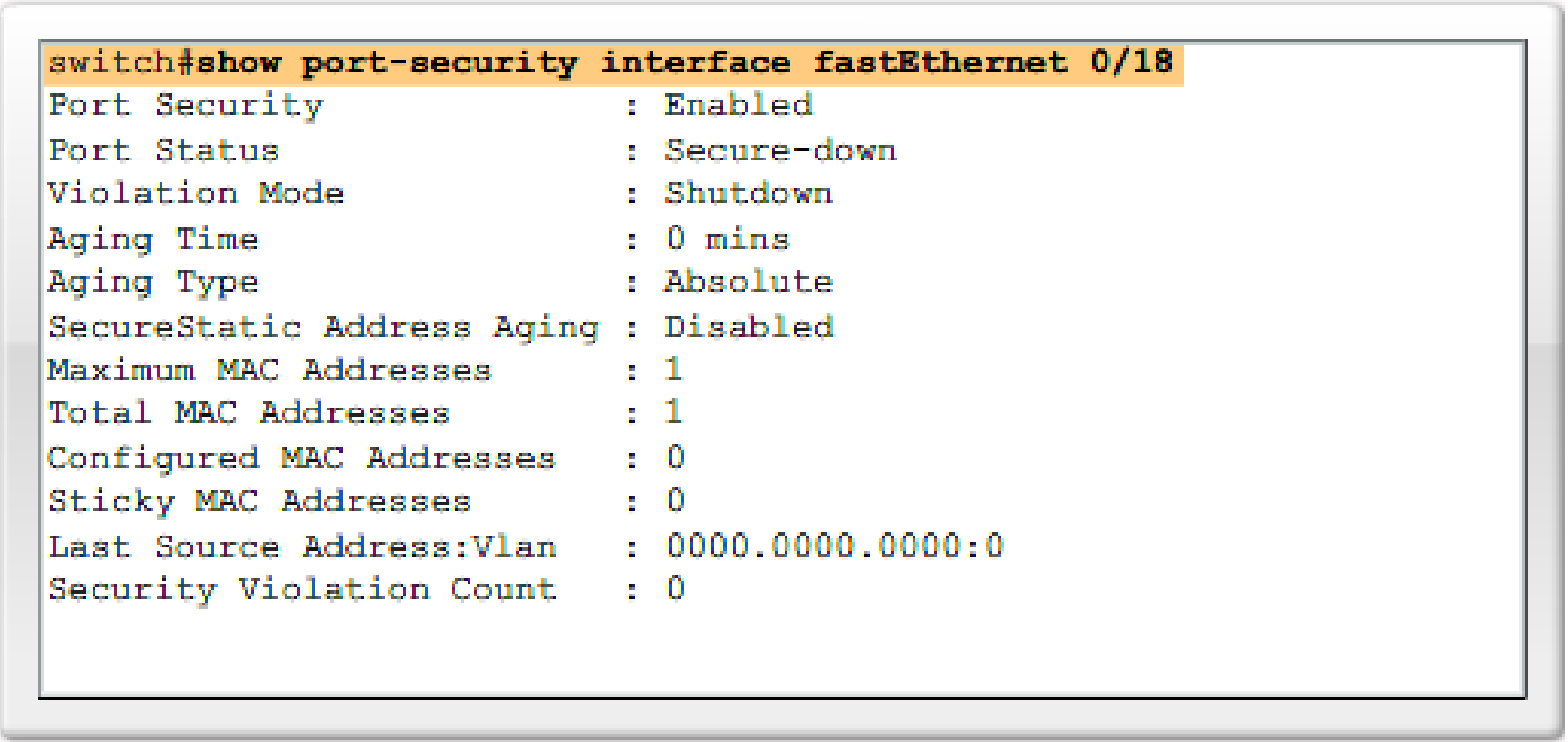
Port Security (4/4)



```
S1#configure terminal
S1(config)#interface fastEthernet 0/18
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security
maximum 50
S1(config-if)#switchport port-security mac-
address sticky
S1(config-if)#end
```

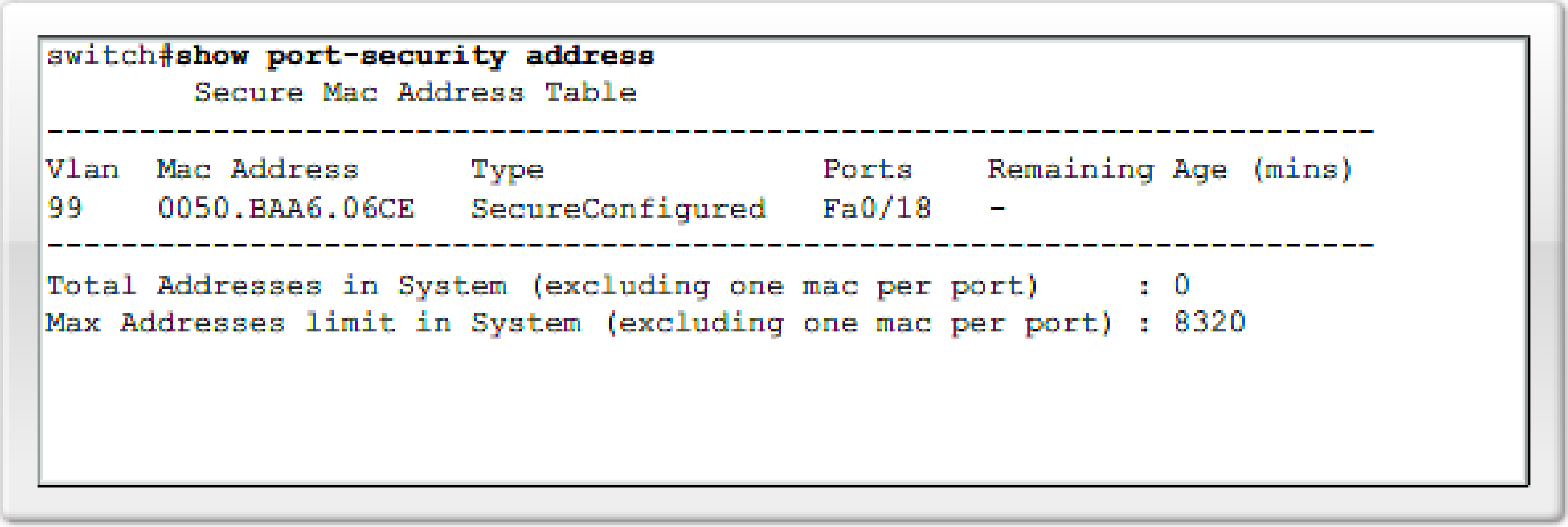
switchport port-security violation X

Port Security checking (1/2)



```
switch#show port-security interface fastEthernet 0/18
Port Security              : Enabled
Port Status                : Secure-down
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   : 0000.0000.0000:0
Security Violation Count   : 0
```

Port Security checking (1/2)



```
switch#show port-security address
        Secure Mac Address Table
------------------------------------------------------------------------
Vlan  Mac Address           Type                Ports     Remaining Age (mins)
99    0050.BAA6.06CE        SecureConfigured    Fa0/18    -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8320
```