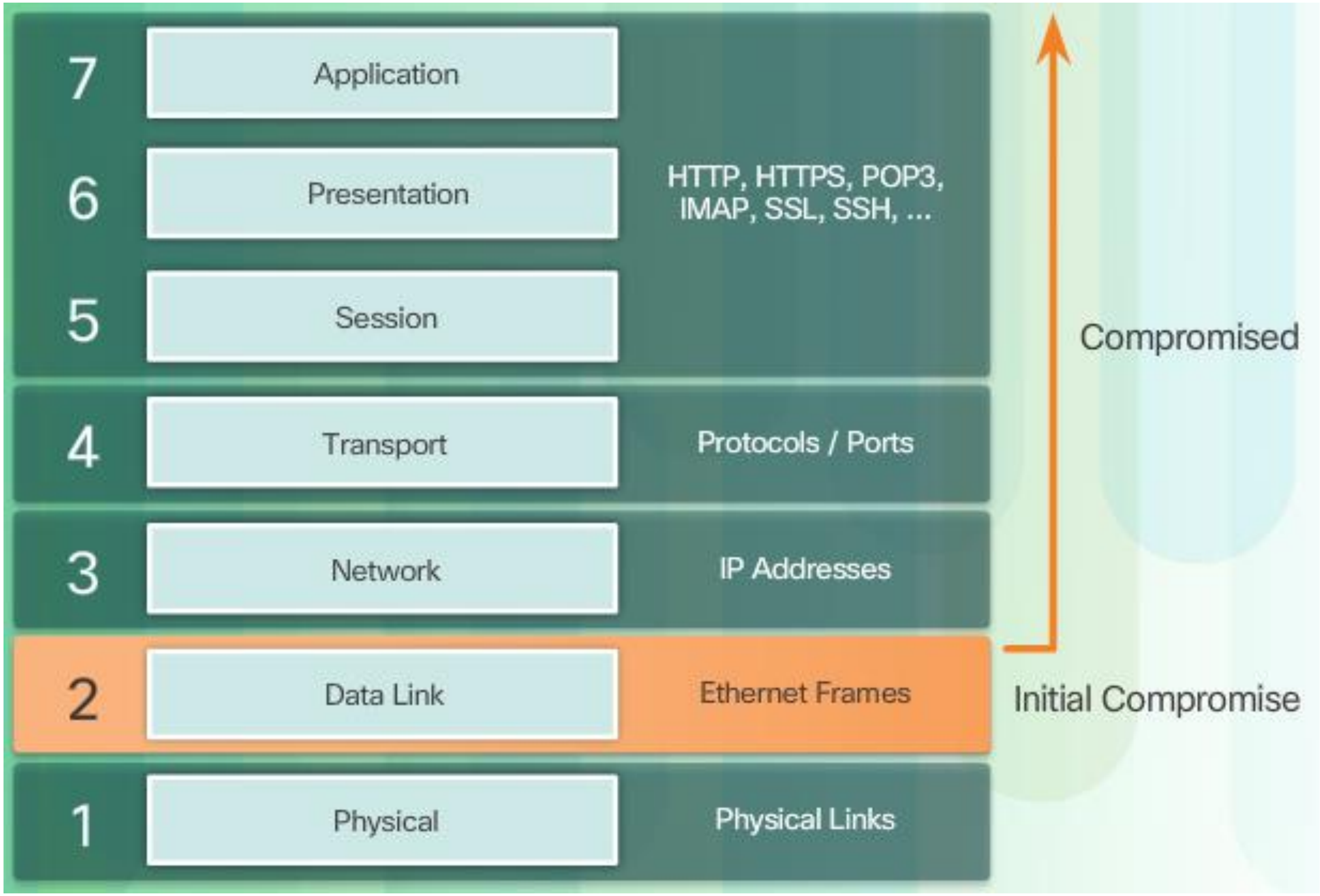
Securing the Local Area Network

Layer 2 Security Considerations

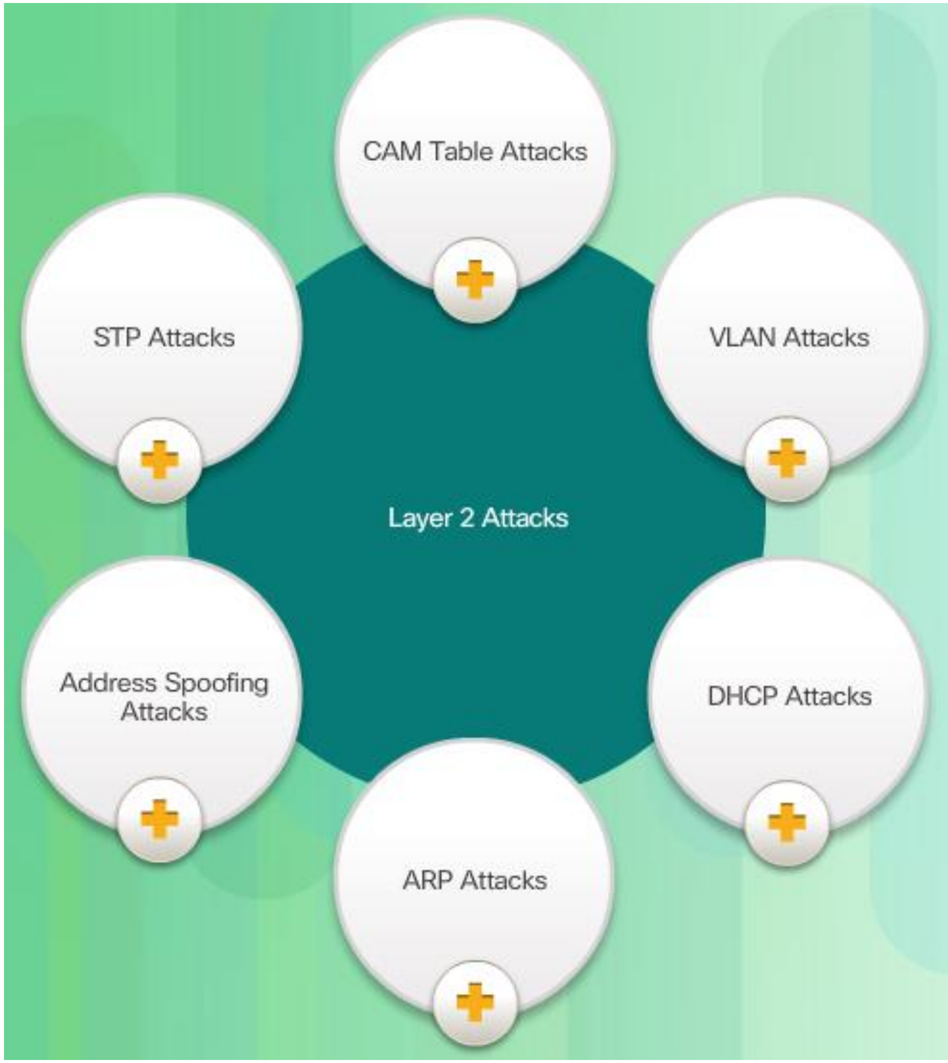
Upon completion of the section, you should be able to:

- Describe CAM table overflow attacks.
- Configure port security to mitigate CAM table overflow attacks.
- Configure VLAN Truck security to mitigate VLAN hopping attacks.
- Implement DHCP Snooping to mitigate DHCP attacks.
- Implement Dynamic Arp Inspection to mitigate ARP attacks.
- Implement IP Source Guard to mitigate address spoofing attacks.

Describe Layer 2 Vulnerabilities



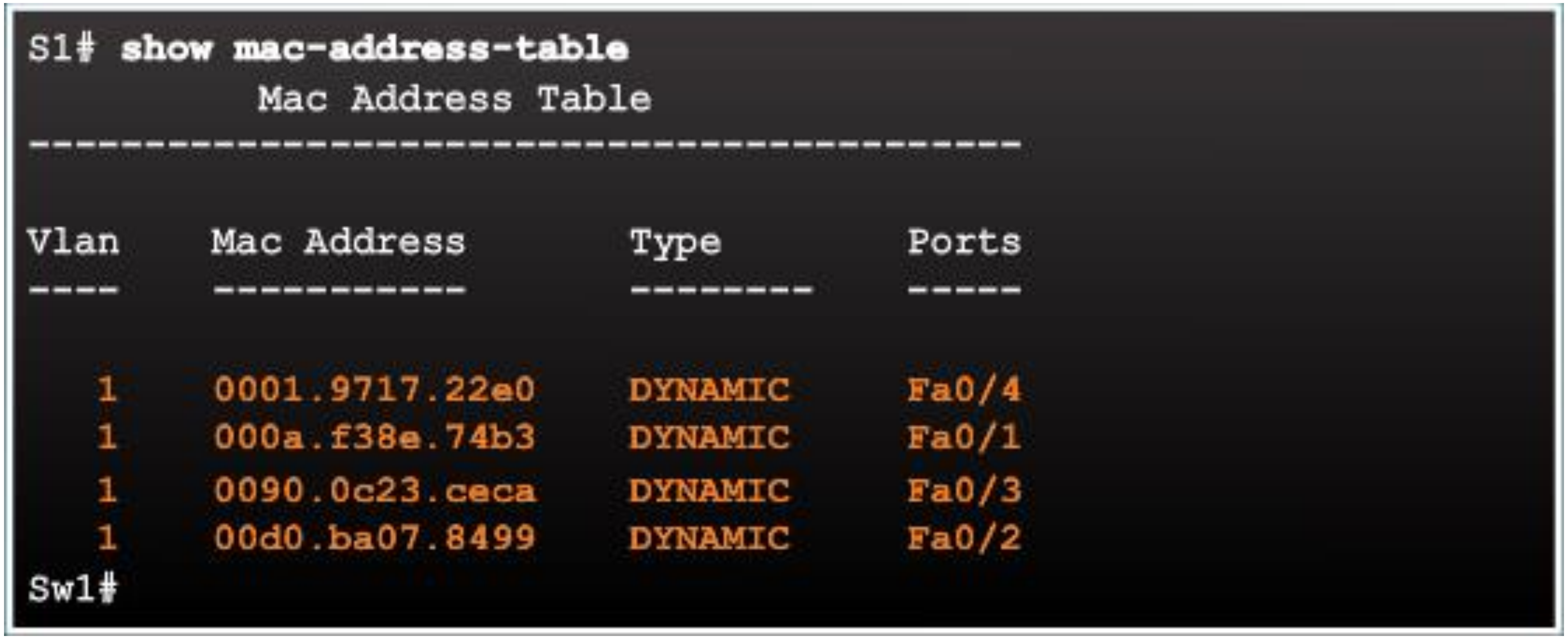
Switch Attack Categories



Topic 1:

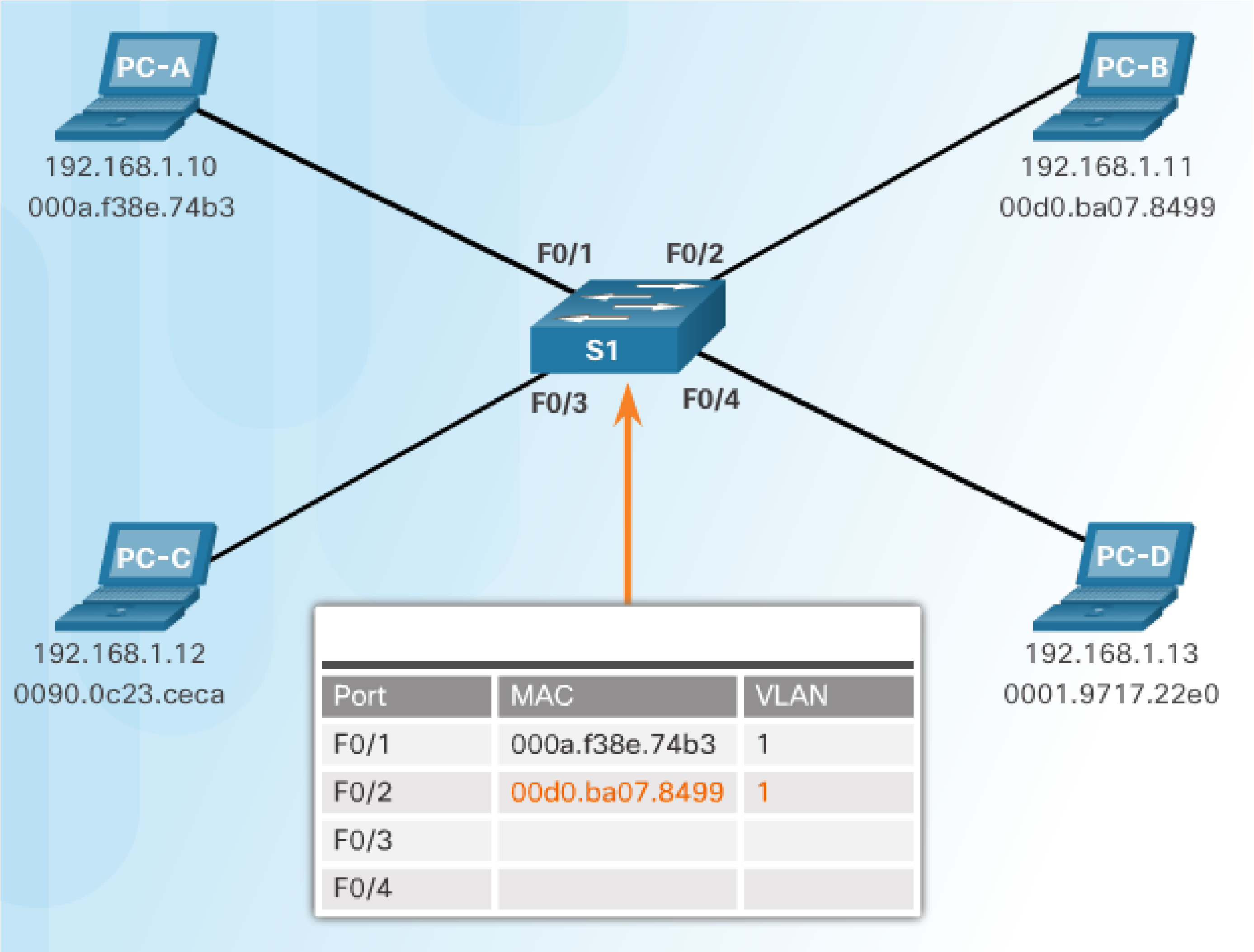
CAM Table Attacks

Basic Switch Operation



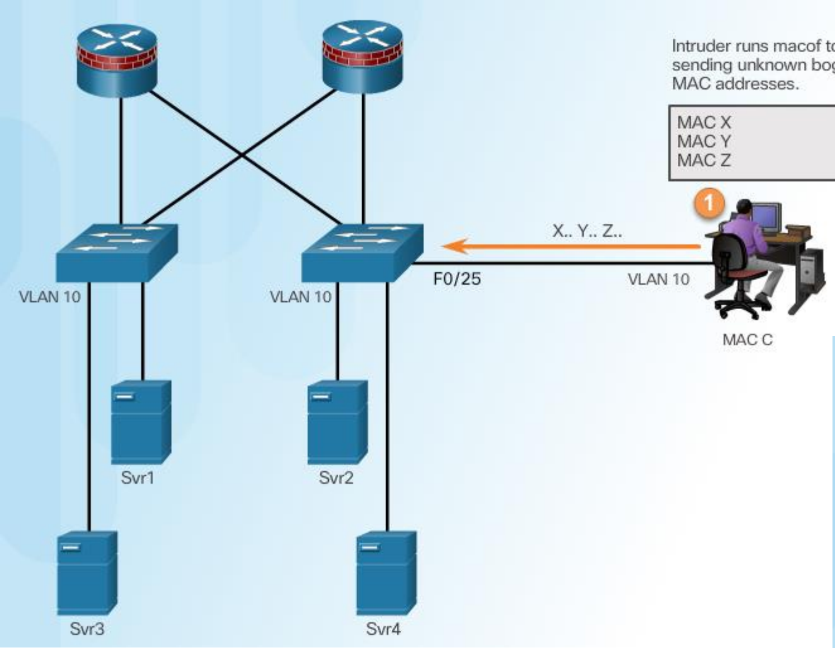
```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
Sw1#
```

CAM Table Operation Example



Port	MAC	VLAN
F0/1	000a.f38e.74b3	1
F0/2	00d0.ba07.8499	1
F0/3		
F0/4		

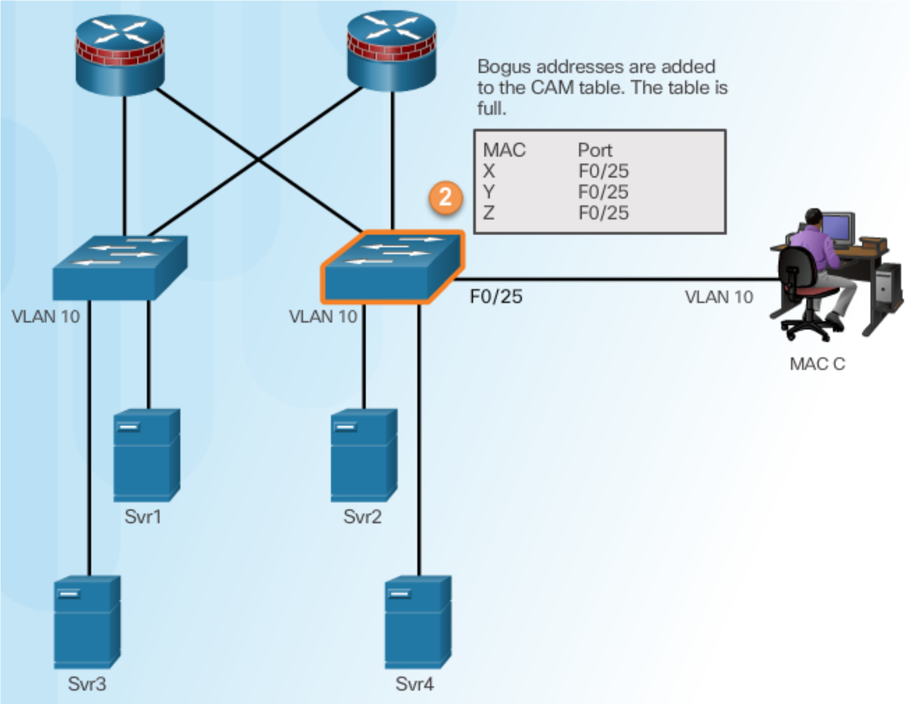
CAM Table Attack



Intruder runs macof to begin sending unknown bogus MAC addresses.

MAC X
MAC Y
MAC Z

Intruder Runs Attack Tool



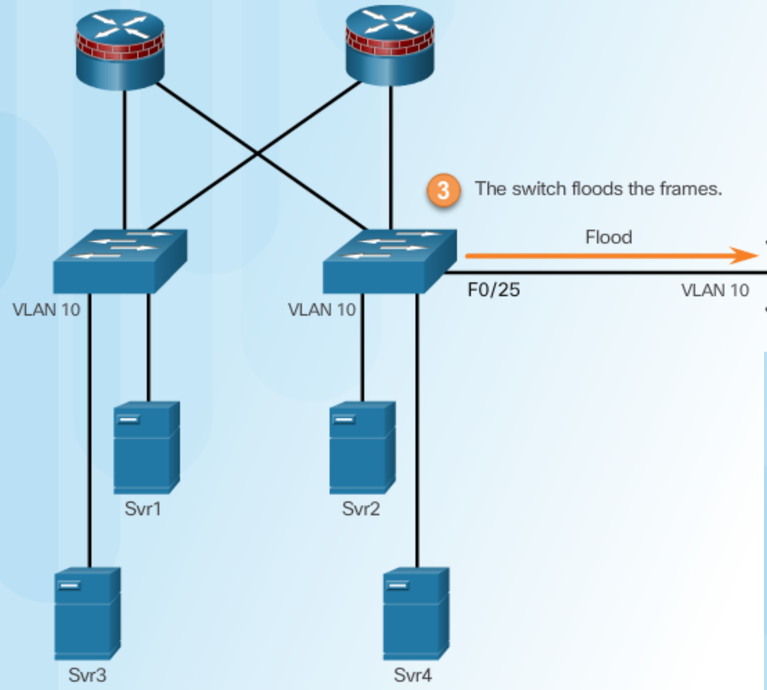
Bogus addresses are added to the CAM table. The table is full.

MAC	Port
X	F0/25
Y	F0/25
Z	F0/25

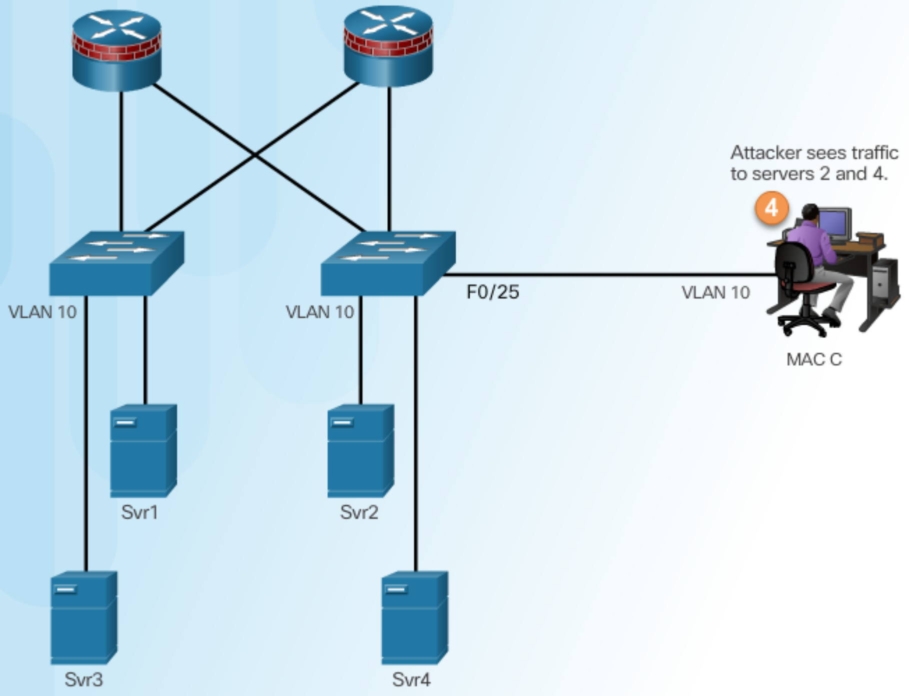
Fill CAM Table

CAM Table Attack

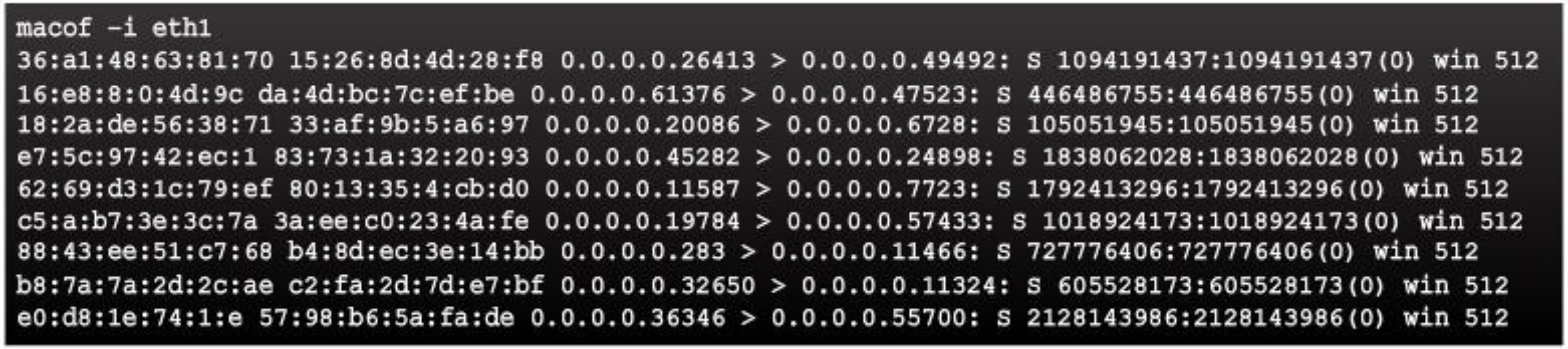
Switch Floods All Traffic



Attacker Captures Traffic



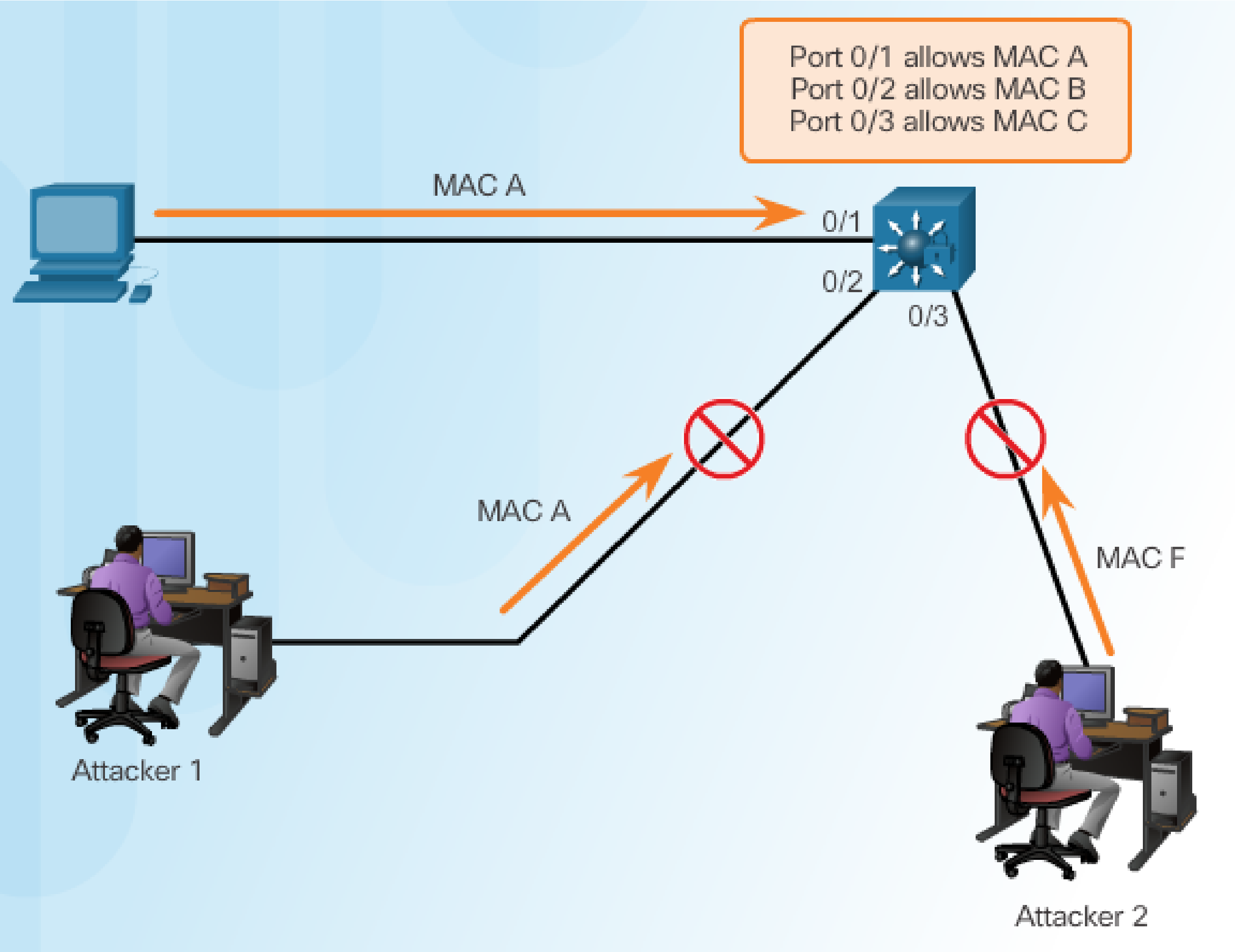
CAM Table Attack Tools



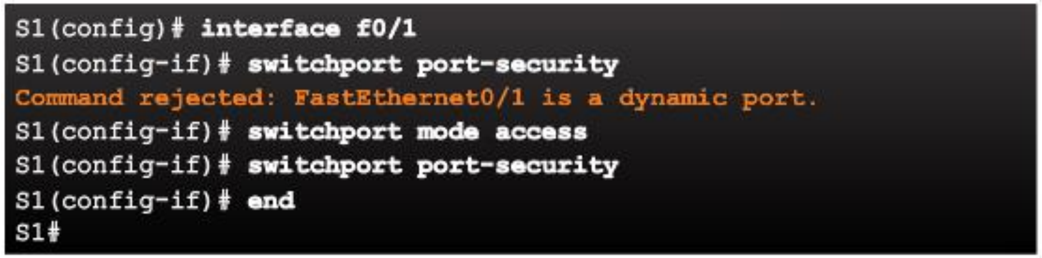
```
macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

Mitigating CAM Table Attacks

Countermeasure for CAM Table Attacks



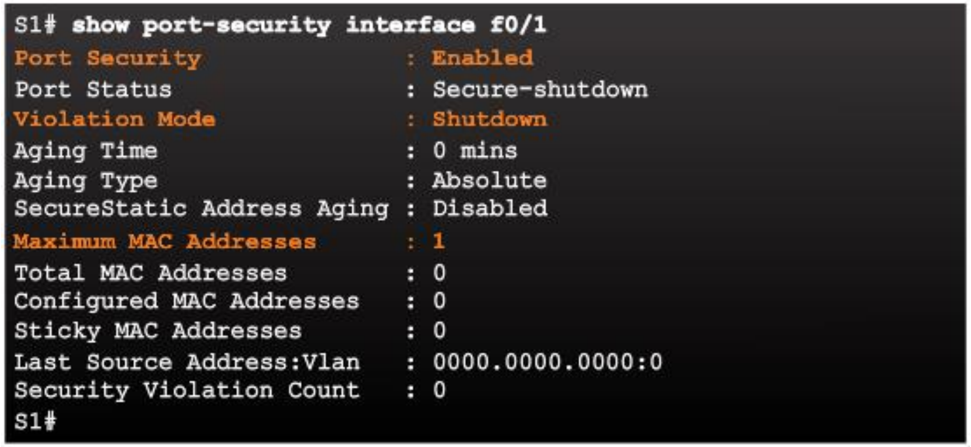
Port Security



```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

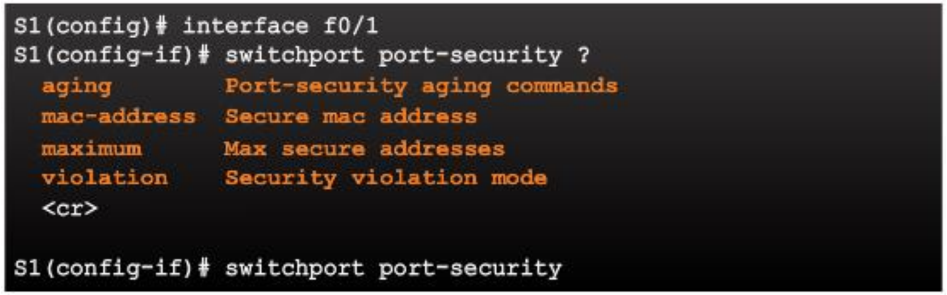
Enabling Port Security

Verifying Port Security



```
S1# show port-security interface f0/1
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   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

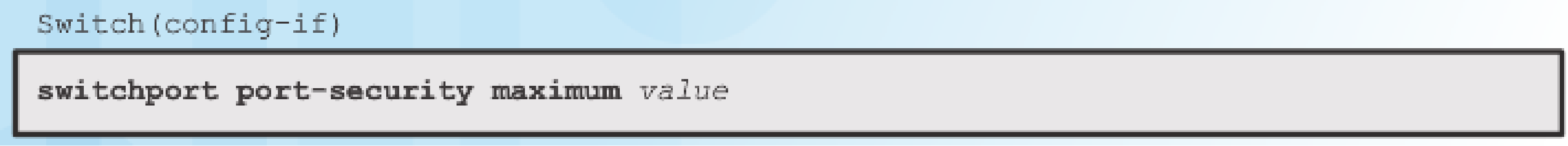
Port Security Options



```
S1(config)# interface f0/1
S1(config-if)# switchport port-security ?
  aging        Port-security aging commands
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>

S1(config-if)# switchport port-security
```

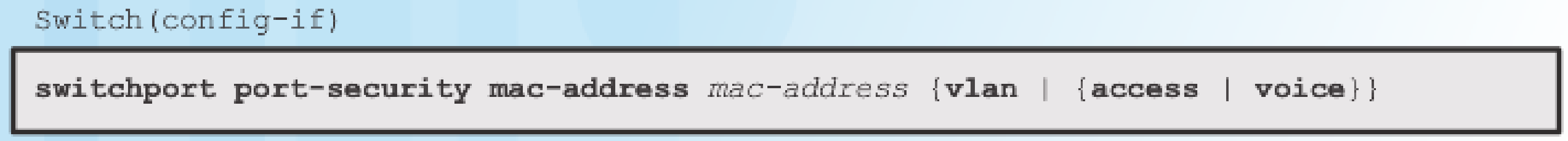
Enabling Port Security Options

Setting the Maximum Number of Mac Addresses



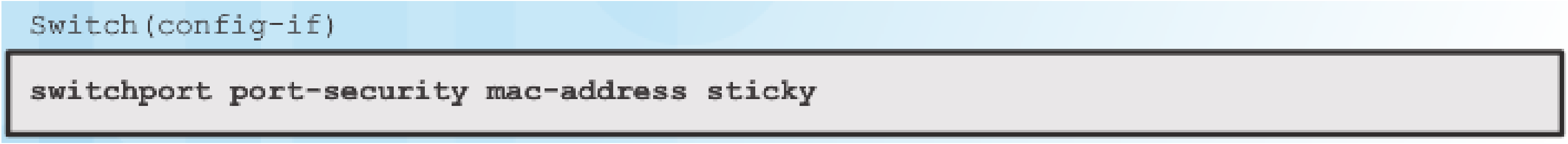
```
Switch(config-if)
switchport port-security maximum value
```

Manually Configuring Mac Addresses



```
Switch(config-if)
switchport port-security mac-address mac-address {vlan | {access | voice}}
```

Learning Connected Mac Addresses Dynamically

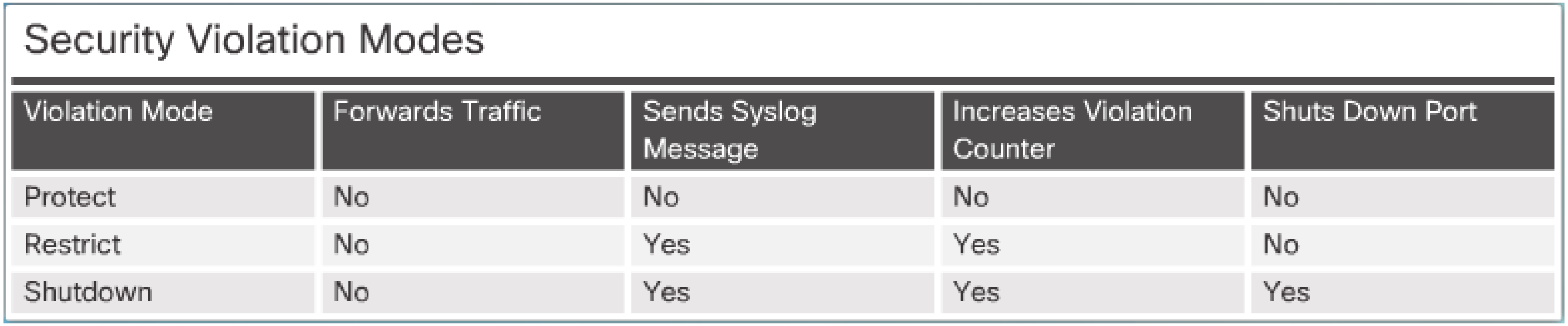


```
Switch(config-if)
switchport port-security mac-address sticky
```

Port Security Violations

Security Violation Modes:

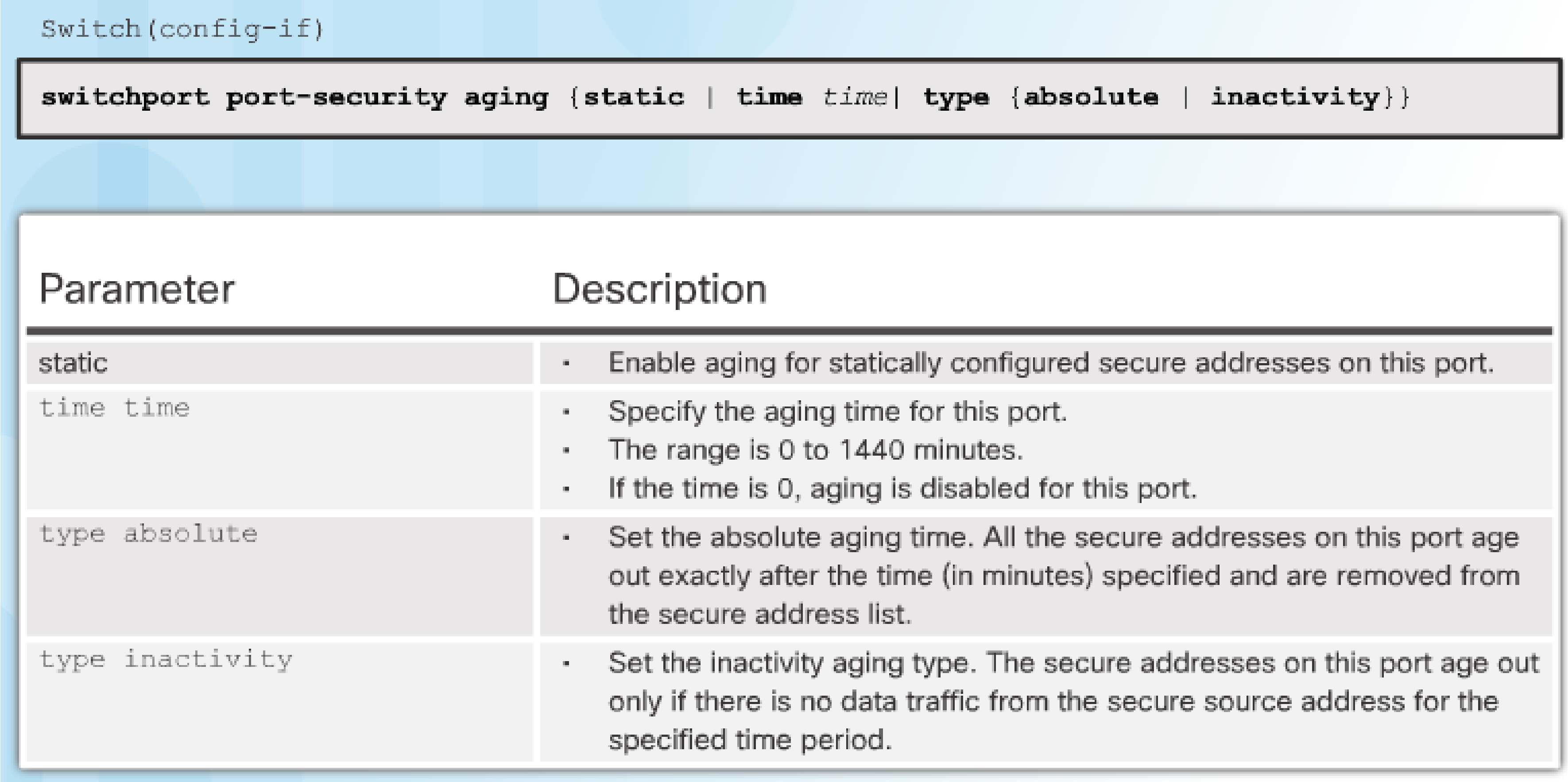
- Protect
- Restrict
- Shutdown



Security Violation Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No
Restrict	No	Yes	Yes	No
Shutdown	No	Yes	Yes	Yes

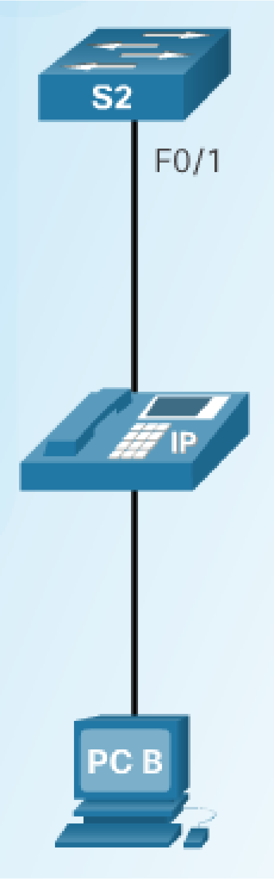
Port Security Aging

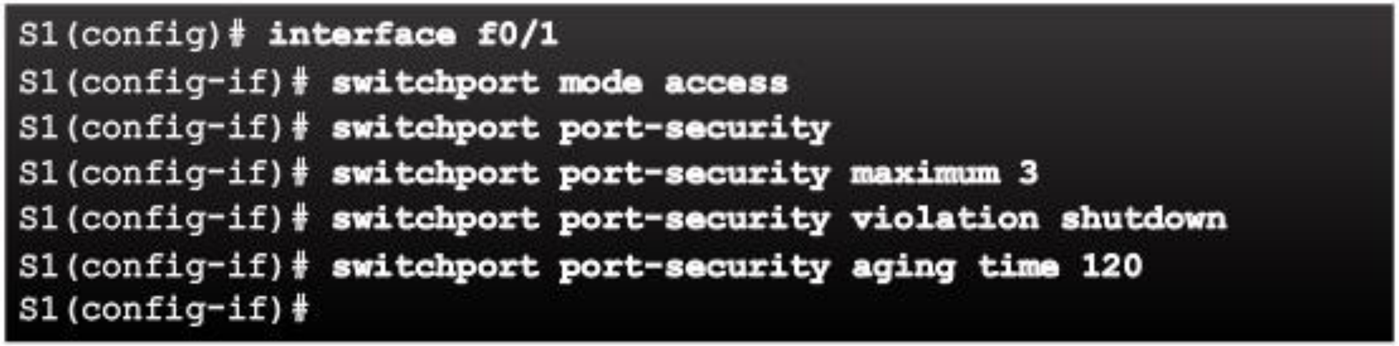


```
Switch(config-if)
switchport port-security aging {static | time time| type {absolute | inactivity}}
```

Parameter	Description
static	- Enable aging for statically configured secure addresses on this port.
`time time`	- Specify the aging time for this port. - The range is 0 to 1440 minutes. - If the time is 0, aging is disabled for this port.
`type absolute`	- Set the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list.
`type inactivity`	- Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Port Security with IP Phones



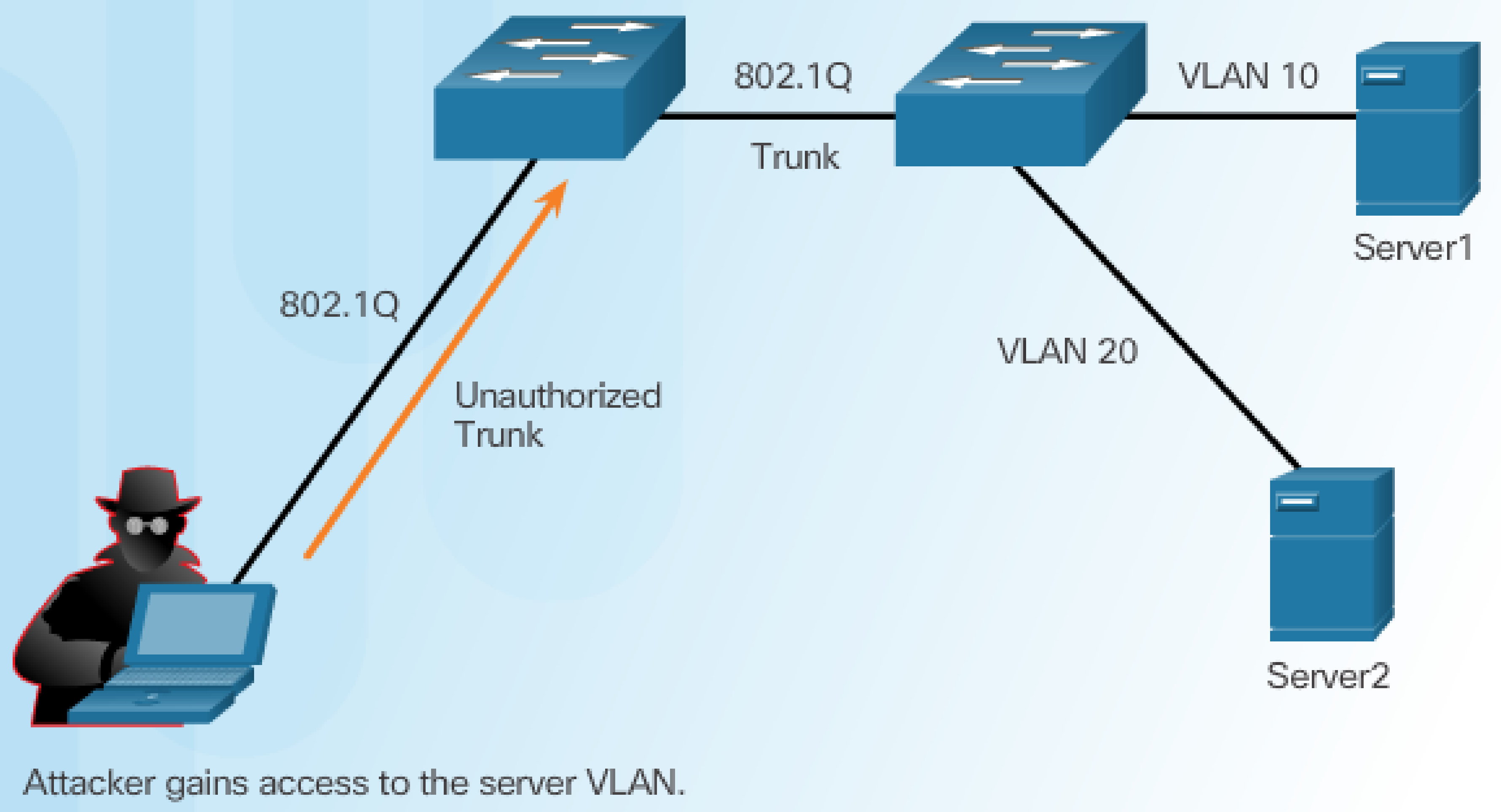


```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# switchport port-security aging time 120
S1(config-if)#
```

Topic 2:

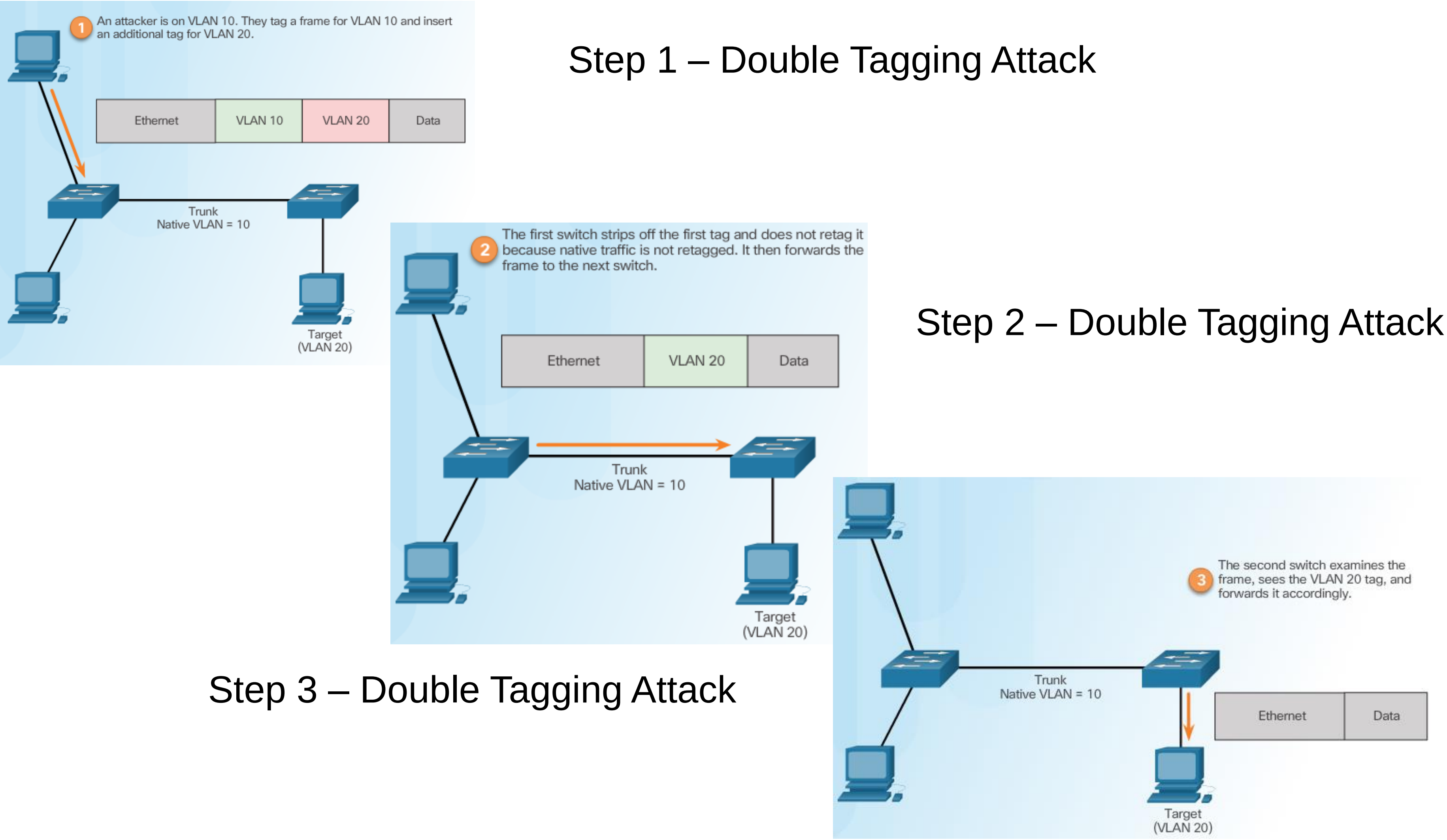
Mitigating VLAN Attacks

VLAN Hopping Attacks



Attacker gains access to the server VLAN.

VLAN Double-Tagging Attack



Step 1 – Double Tagging Attack

1 An attacker is on VLAN 10. They tag a frame for VLAN 10 and insert an additional tag for VLAN 20.

Ethernet	VLAN 10	VLAN 20	Data

Step 2 – Double Tagging Attack

2 The first switch strips off the first tag and does not retag it because native traffic is not retagged. It then forwards the frame to the next switch.

Ethernet	VLAN 20	Data

Step 3 – Double Tagging Attack

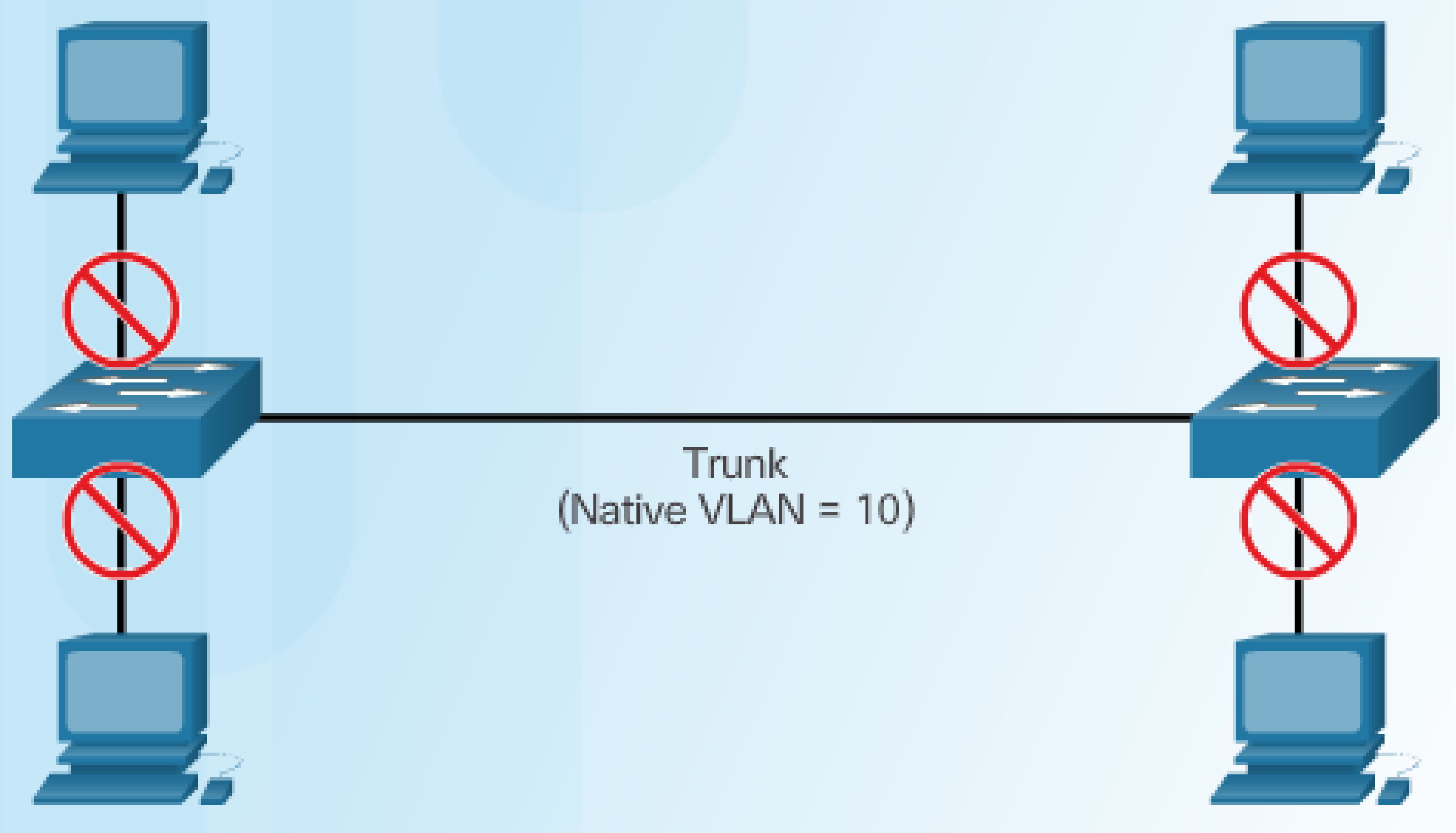
3 The second switch examines the frame, sees the VLAN 20 tag, and forwards it accordingly.

Ethernet	Data

Mitigating VLAN Hopping Attacks

```
switch(config-if)# switchport mode access
```

- Configure port as an access port



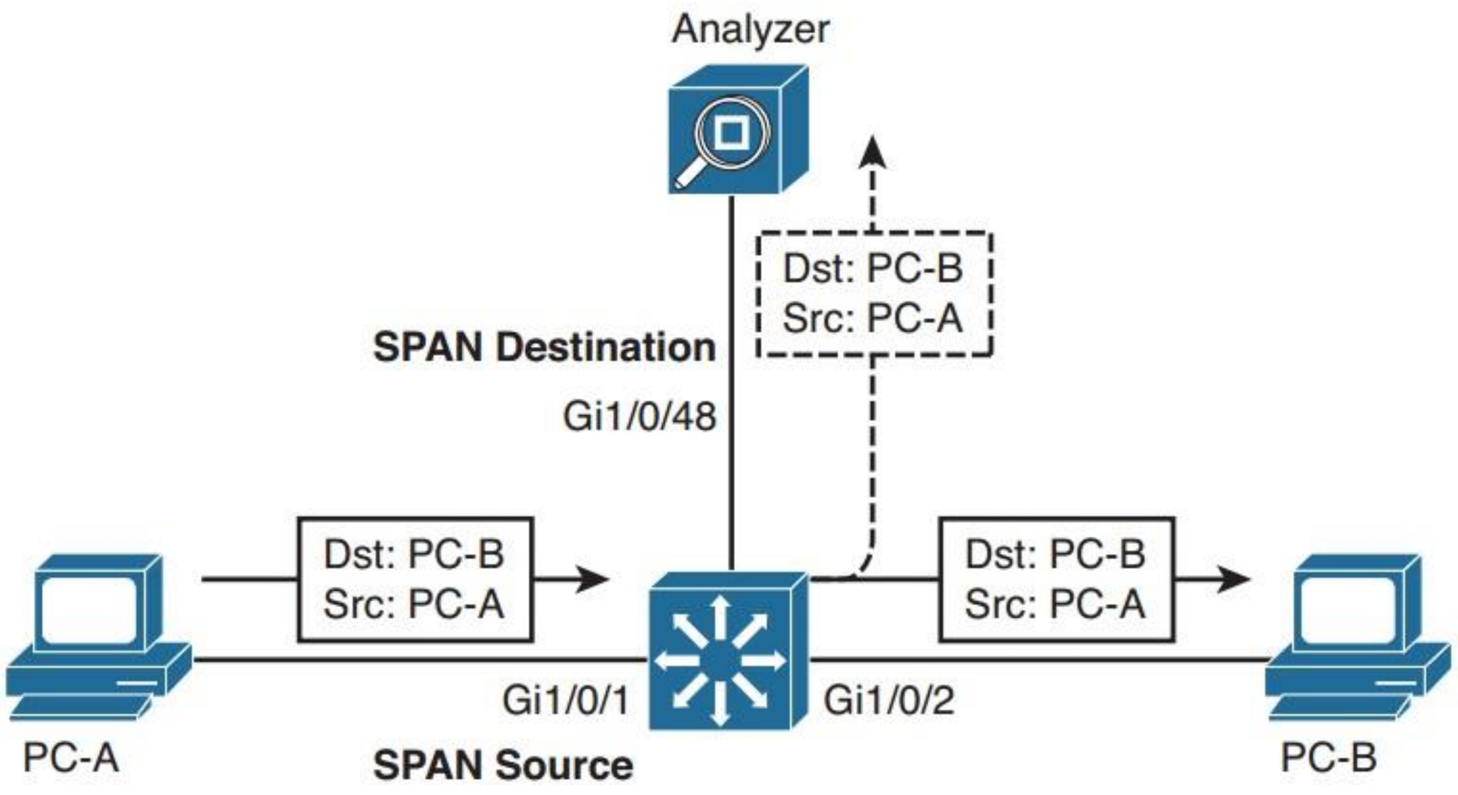
Implementing Switch Port Analyzer

SPAN

Switch Port Analyzer

- The Switch Port Analyzer (SPAN) feature is used to mirror traffic from one source switch port or VLAN to a destination port.
- It allows a monitoring device, such as a network analyzer or “sniffer”, to be attached to the destination port for capturing traffic.
- SPAN is available in two different forms:
  - **SPAN:** Both the SPAN source and destination are located on the same switch.
  - **Remote SPAN (RSPAN):** The SPAN source and destination are located on different switches. Mirrored traffic is copied over a special – purpose VLAN across trunks between switches from the source to the destination.

SPAN



Both the SPAN source and destination are located on the same switch.

SPAN Configuration

Define the source of the SPAN session data:

```
Switch(config)# monitor session-id source {vlan vlan-list | interface interface-number} [tx | rx | both]
```

- ***session-id:*** Uniquely identify the SPAN session.
- **source interface *interface-number:*** Specify the interface which traffic incoming or outgoing traffic will be monitored.
- **source vlan *vlan-list:*** Specify the VLANs which traffic transit through will be monitored.
- **tx | rx | both:** Traffic can be selected for mirroring based on the direction it is traveling the SPAN source (tx: transmitted from the source, rx: received from the source, both: traffic in both directions).

SPAN Configuration (Cont.)

Identify the SPAN destination:

```
Switch(config)# monitor session-id destination interface
interface-number [encapsulation replicate][ingress {vlan
vlan-id | dot1q vlan vlan-id | isl}]
```

- ***session-id:*** Uniquely identify the SPAN session.
- **destination interface *interface-number:*** Identify the destination interface used by the session.
- **encapsulation replicate*:*** Capture any VLAN tagging information of the Layer 2 Protocol packets.
- **ingress vlan *vlan-id:*** Allows sending traffic into the destination port. Sending traffic will be sent untagged to VLAN vlan-id.
- **ingress {dot1q vlan *vlan-id* | isl}*:*** Allows sending traffic into the destination port. Sending traffic will be sent with tag dot1q or ISL. With dot1q tag, native VLAN is specified.

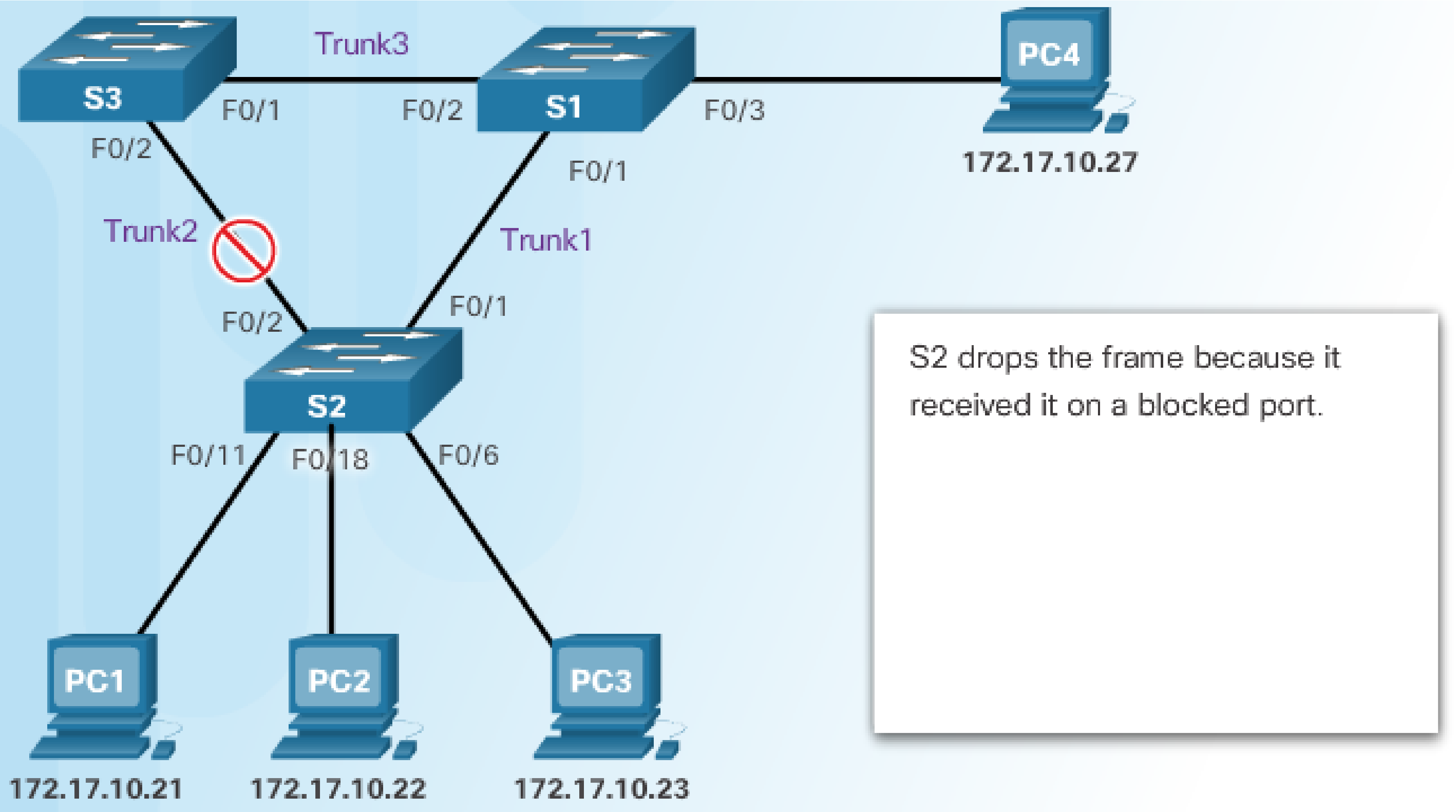
SPAN Configuration (Cont.)

- Example:

```
SW(config)# monitor session 1 source interface g1/0/1 both
SW(config)# monitor session 1 destination interface g1/0/48
```

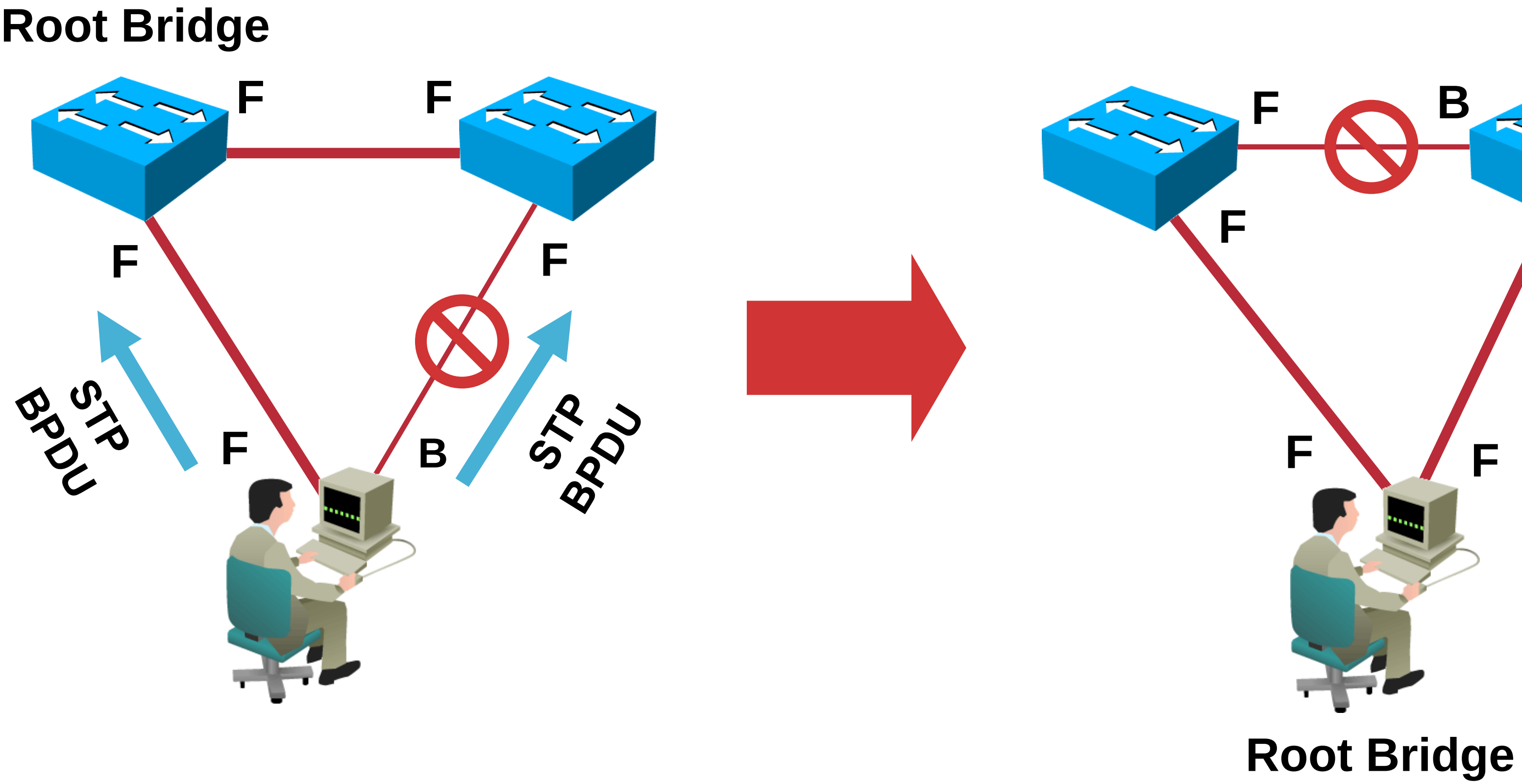
- Monitoring traffic going to and coming from a device connected to the interface g1/0/1 and the network analyzer is connected to the interface g1/0/48.

Introduction to the Spanning Tree Protocol



S2 drops the frame because it received it on a blocked port.

Spanning Tree Manipulation



Implementing BPDUGuard to Mitigate Spanning Tree Manipulation

```
Switch(config)#spanning-tree portfast bpduguard

or

Switch(config-if)#spanning-tree bpduguard enable
```

- The BPDU – guard feature shuts down ports when ports receive BPDU.

Auto recovery from err-disable state

- If the BPDU – guard feature has shutdown a port, the port can be restored to an operational state using the error-disable recovery procedure.
- Enable recovery cause is BPDU – guard :

```
Switch(config)#errdisable recovery cause bpduguard
```

- Set a global recovery timeout by using the command:

```
Switch(config)#errdisable recovery interval seconds
```

© 2013 Cisco and/or its affiliates. All rights reserved.