網路安全概論

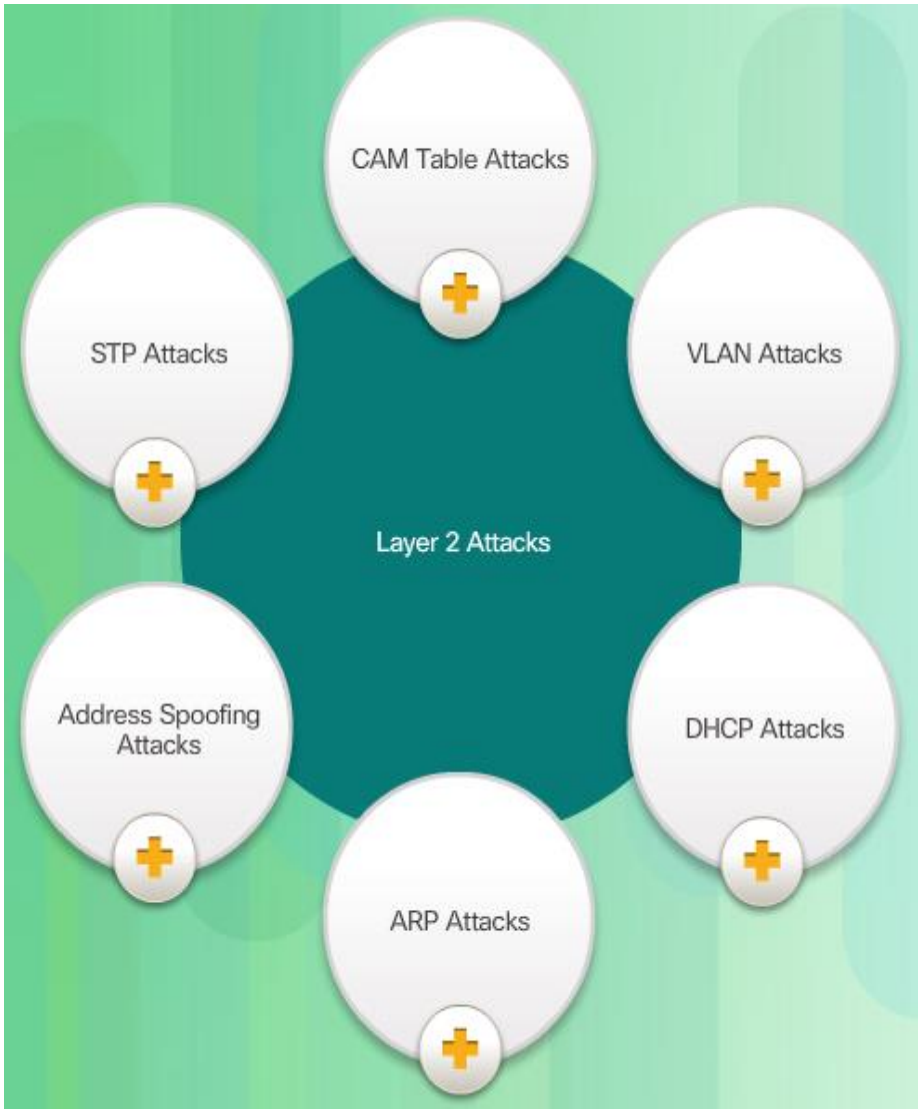
大綱

一.降低CAM攻擊
二.降低VLAN攻擊
三.降低DHCP攻擊
四.降低ARP攻擊
五.降低Address欺騙攻擊
六.降低STP攻擊

區域網路攻擊分類

Switch Attack Categories

1.CAM Table Attacks
2.VLAN Attacks
3.DHCP Attacks
4. ARP Attacks
5. Address Spoofing Attacks
6.STP Attacks



一、降低CAM攻擊
Mitigating CAM Table Attacks

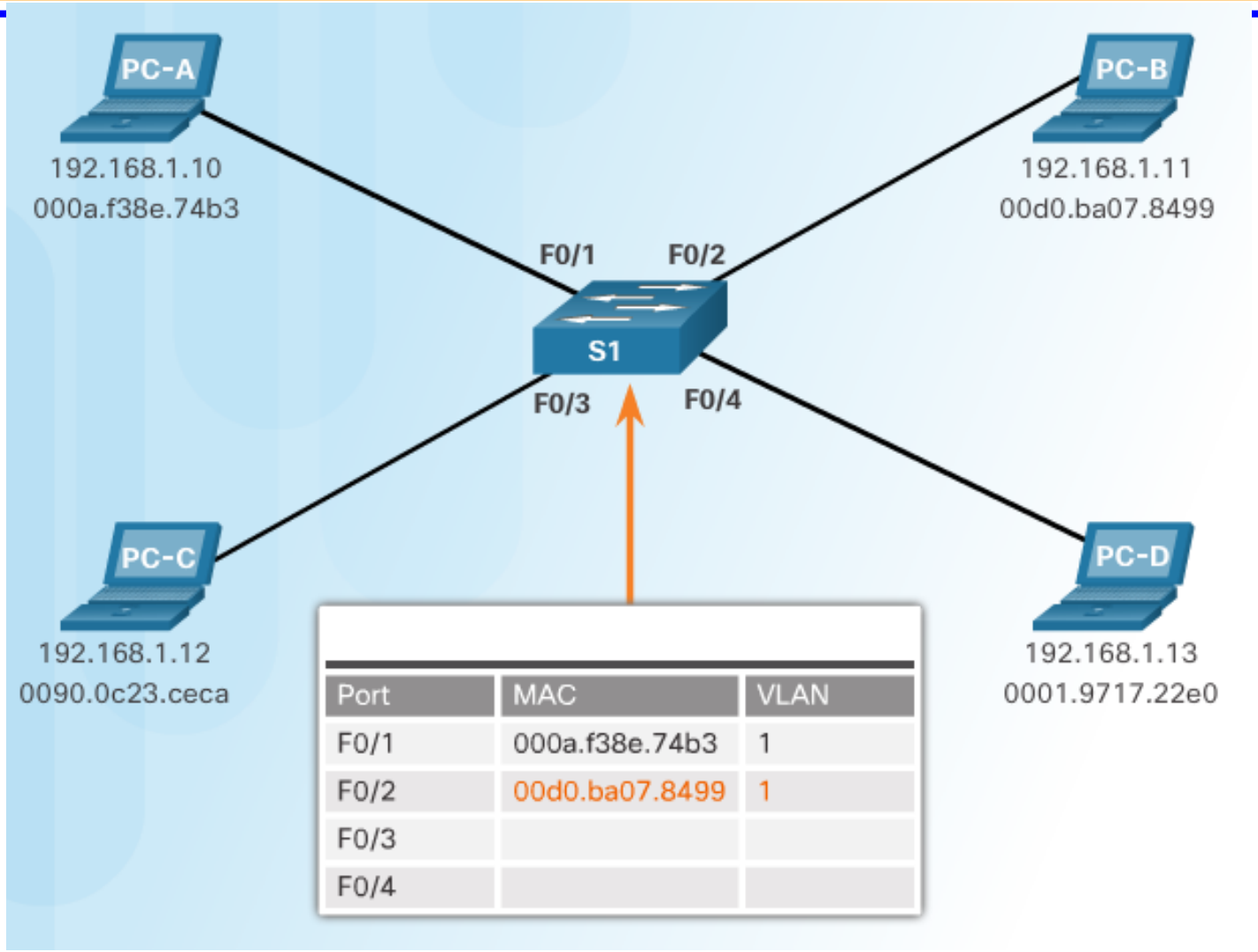
Switch 運作原理

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#
```

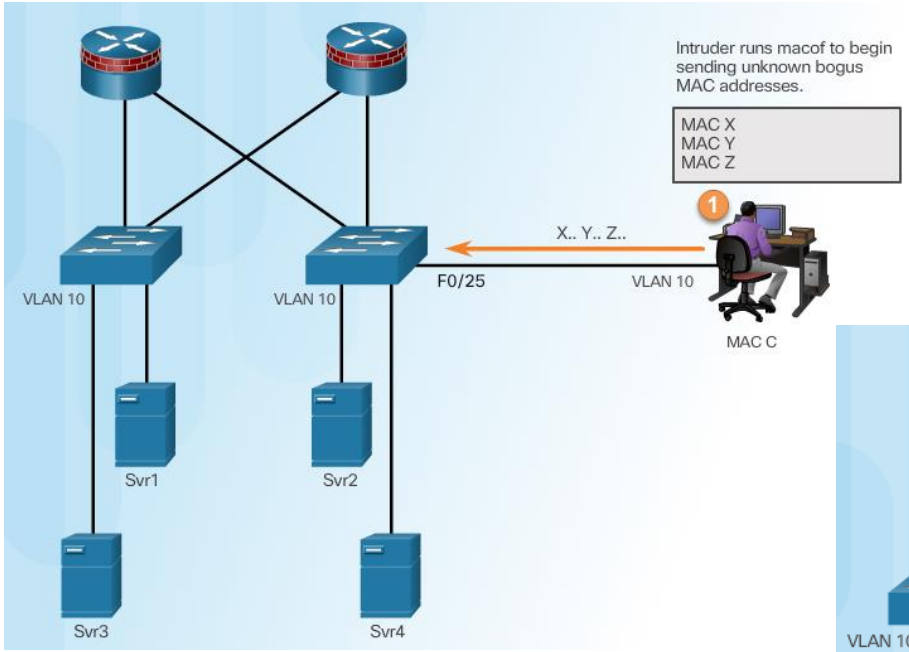
CAM 表運作範例

CAM Table Operation Example



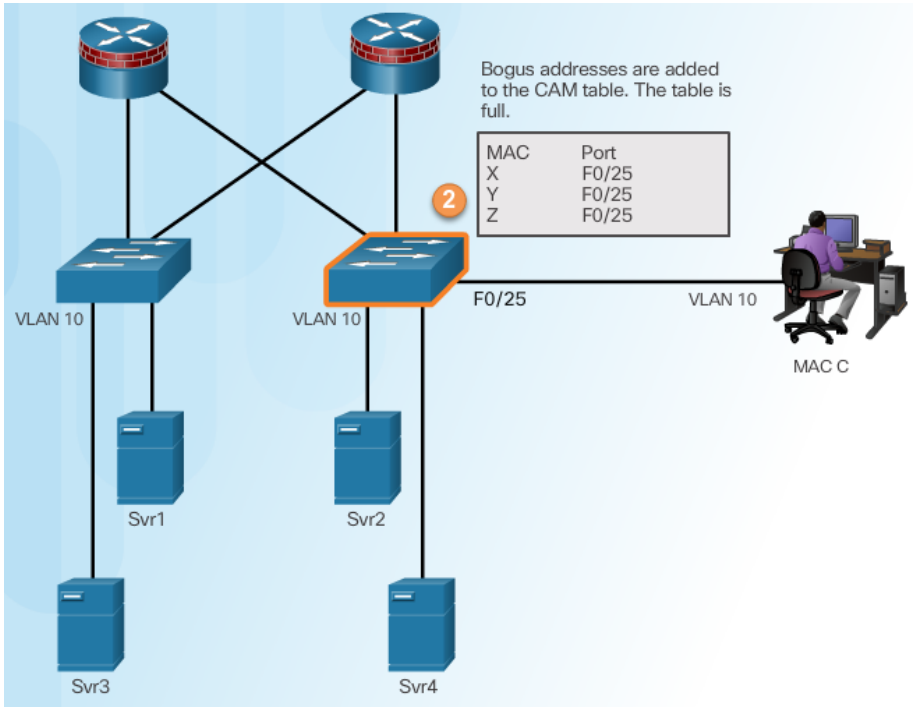
CAM 攻擊手段

CAM Table Attack



入侵者執行攻擊工具

Intruder Runs Attack Tool

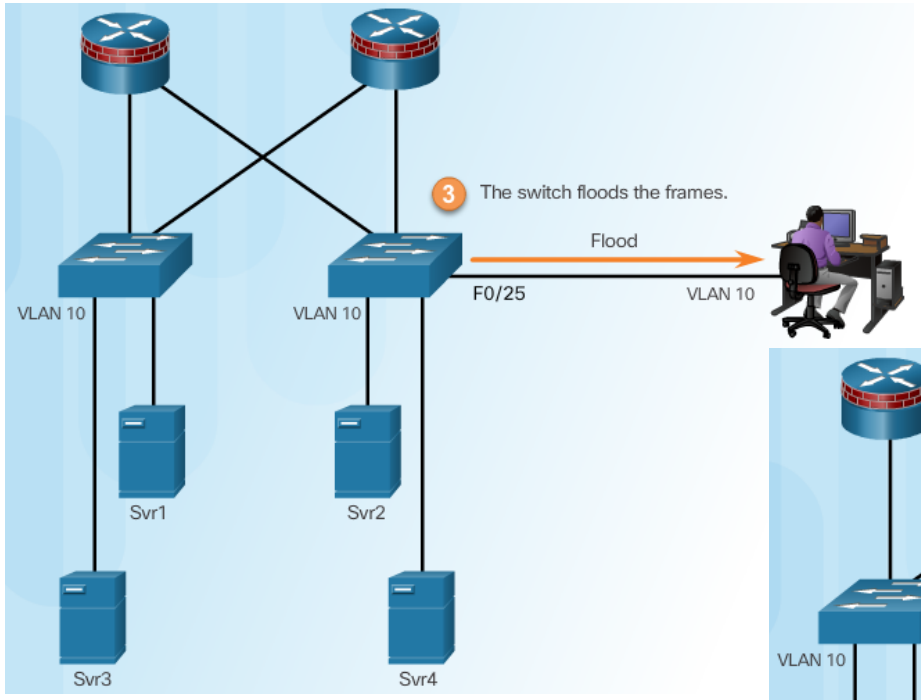


填滿CAM表

Fill CAM Table

CAM攻擊手段

CAM Table Attack

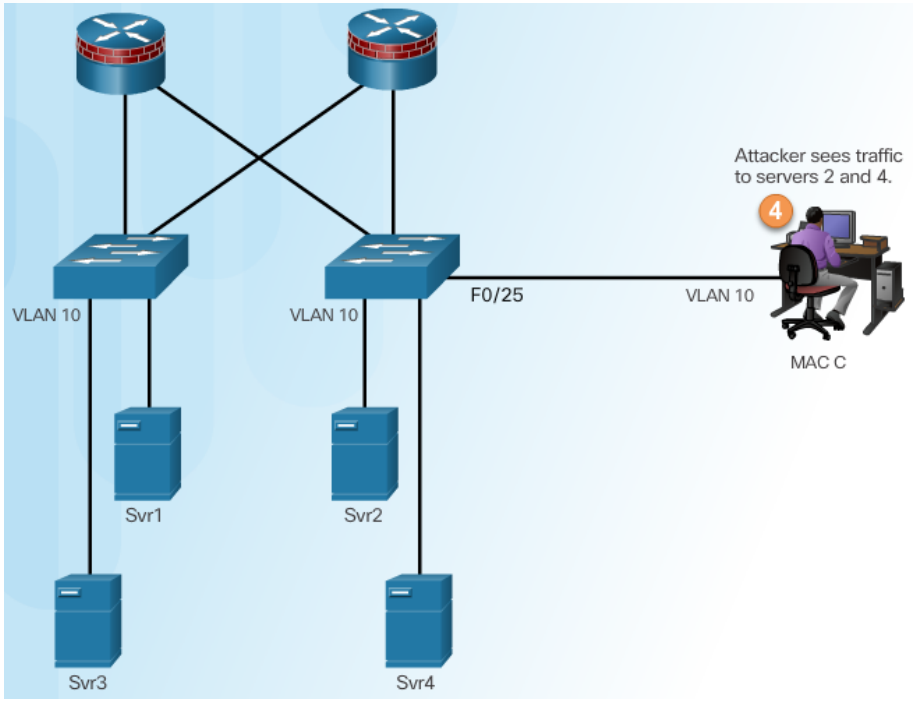


Switch 泛洪所有流量

Switch Floods All Traffic

攻擊者捕獲流量

Attacker Captures Traffic



CAM 攻擊工具

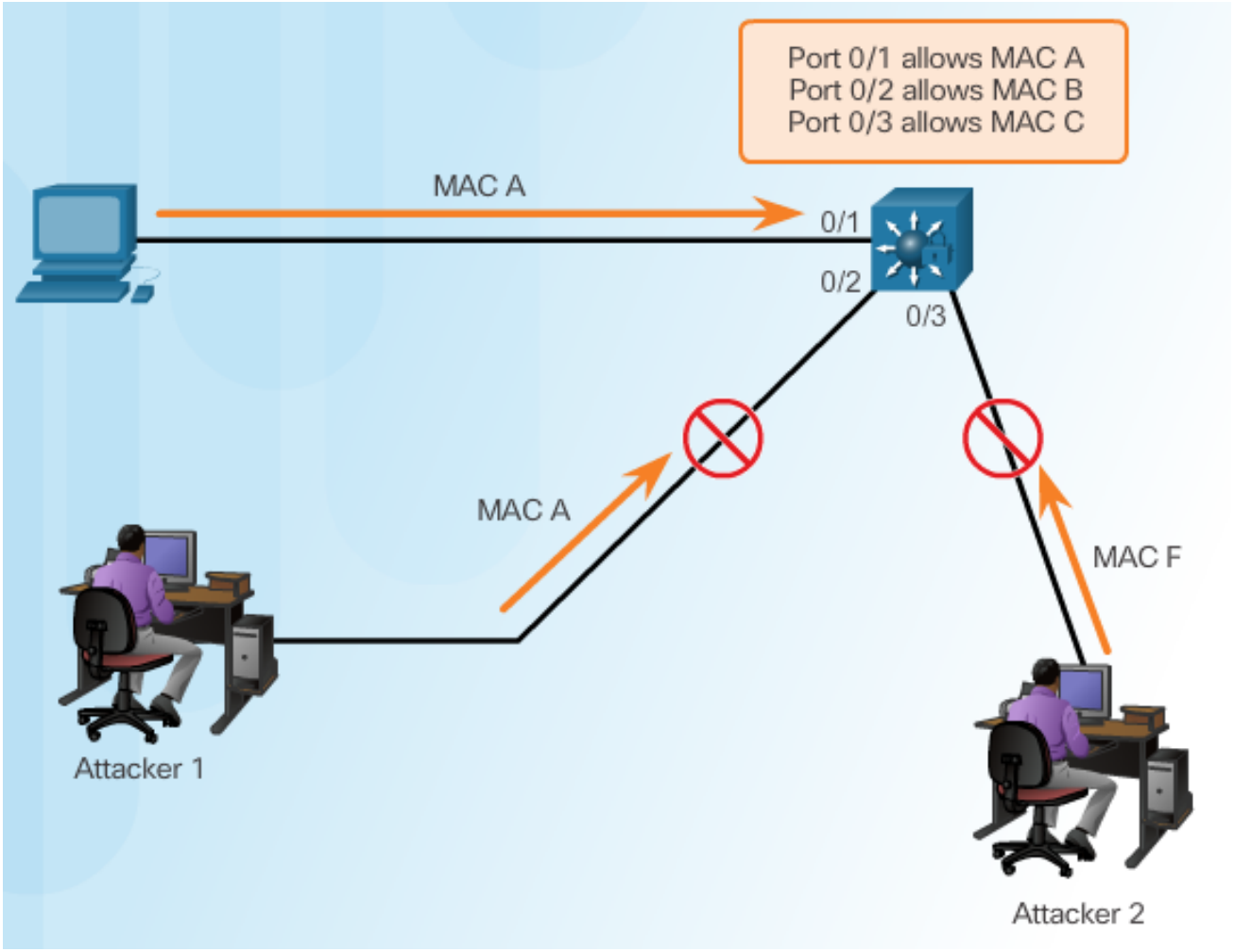
CAM Table Attack Tools

攻擊工具:MACOF(可以假冒MAC卡號的程式)

```
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
```

CAM攻擊對策

Countermeasure for CAM Table Attacks



Port Security 步驟

```
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#
```

啟動Port Security

Enabling Port Security

檢視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選項

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
```

啟動Port Security

Enabling Port Security Options

設定允許MAC數量(Setting the Maximum Number of Mac Addresses)

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

手動設定綁定的MAC address(Manually Configuring Mac Addresses)

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

學習目前所連結設備的MAC address (Learning Connected Mac Addresses Dynamically)

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

Port Security 違規因應方式

Port Security Violations

違規因應方式模式Security Violation Modes:

- 防禦(Protect)
- 限制(Restrict)
- 關閉(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效期

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.

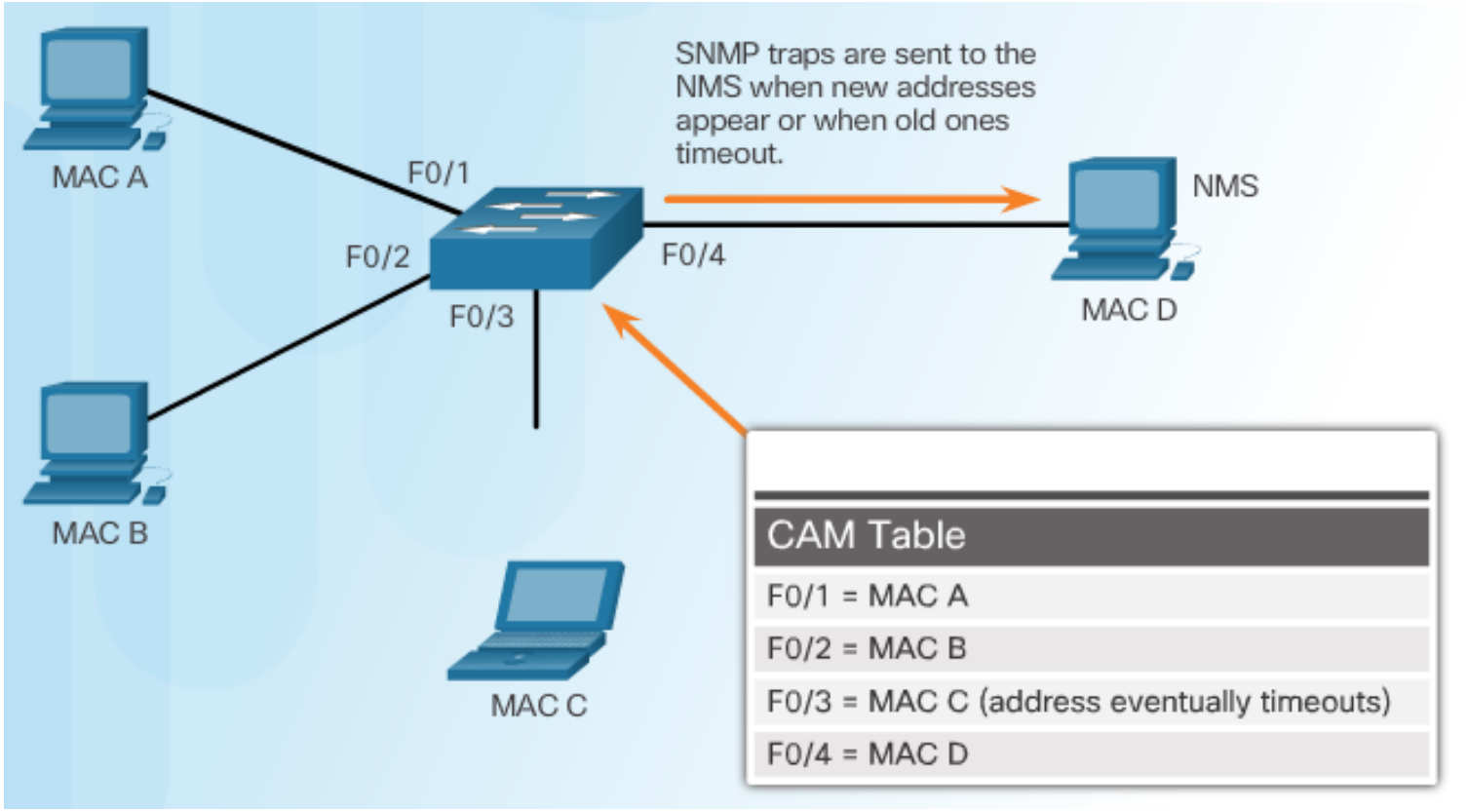
在IP Phones對應埠口設定Port Security

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)#
```

利用SNMP發送MAC Adress更變通知

SNMP MAC Address Notification

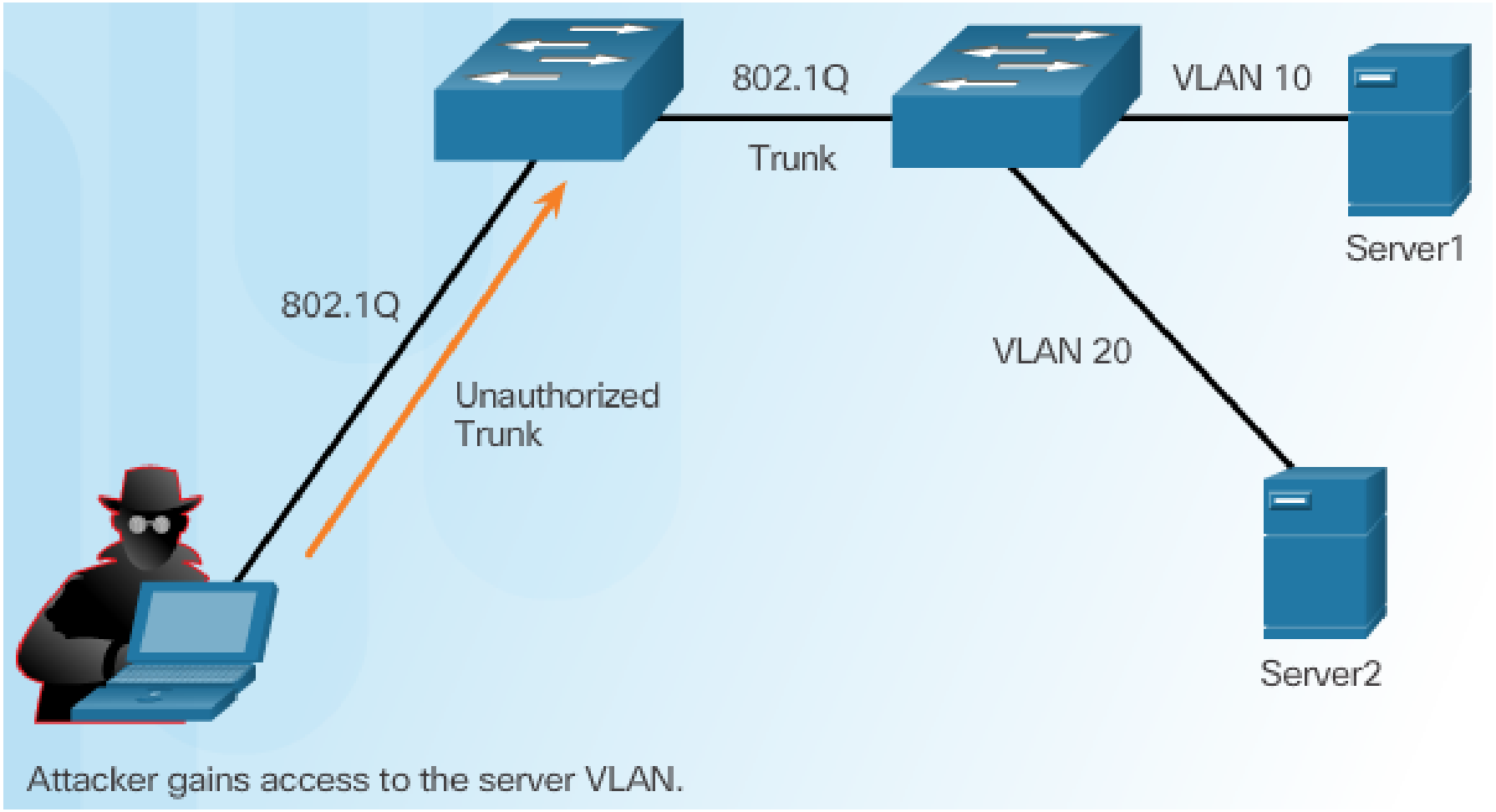


二、降低VLAN攻擊

Mitigating VLAN Attacks

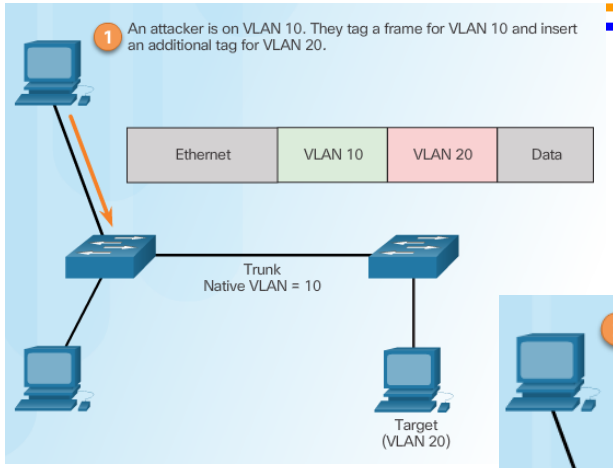
VLAN跳板攻擊

VLAN Hopping Attacks

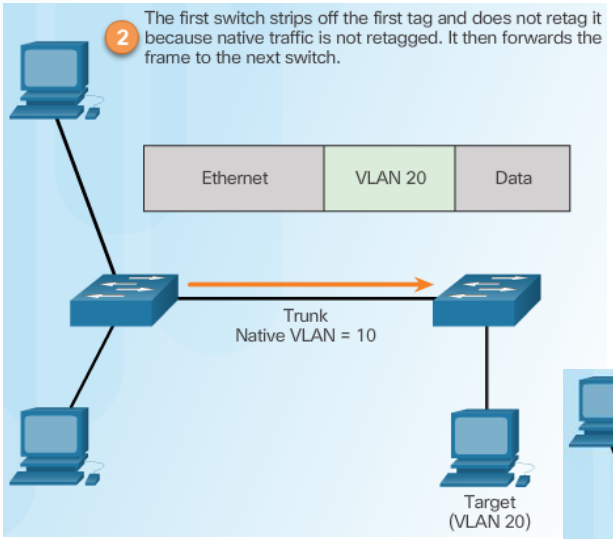


VLAN雙重標籤攻擊

VLAN Double-Tagging Attack

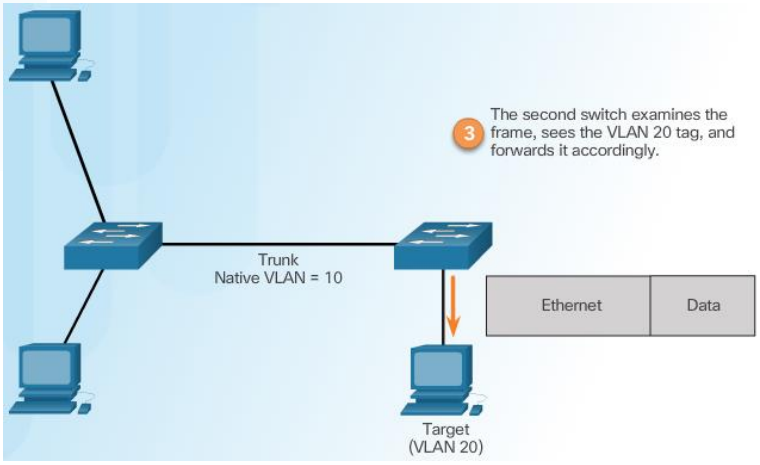


Step 1 – Double Tagging Attack



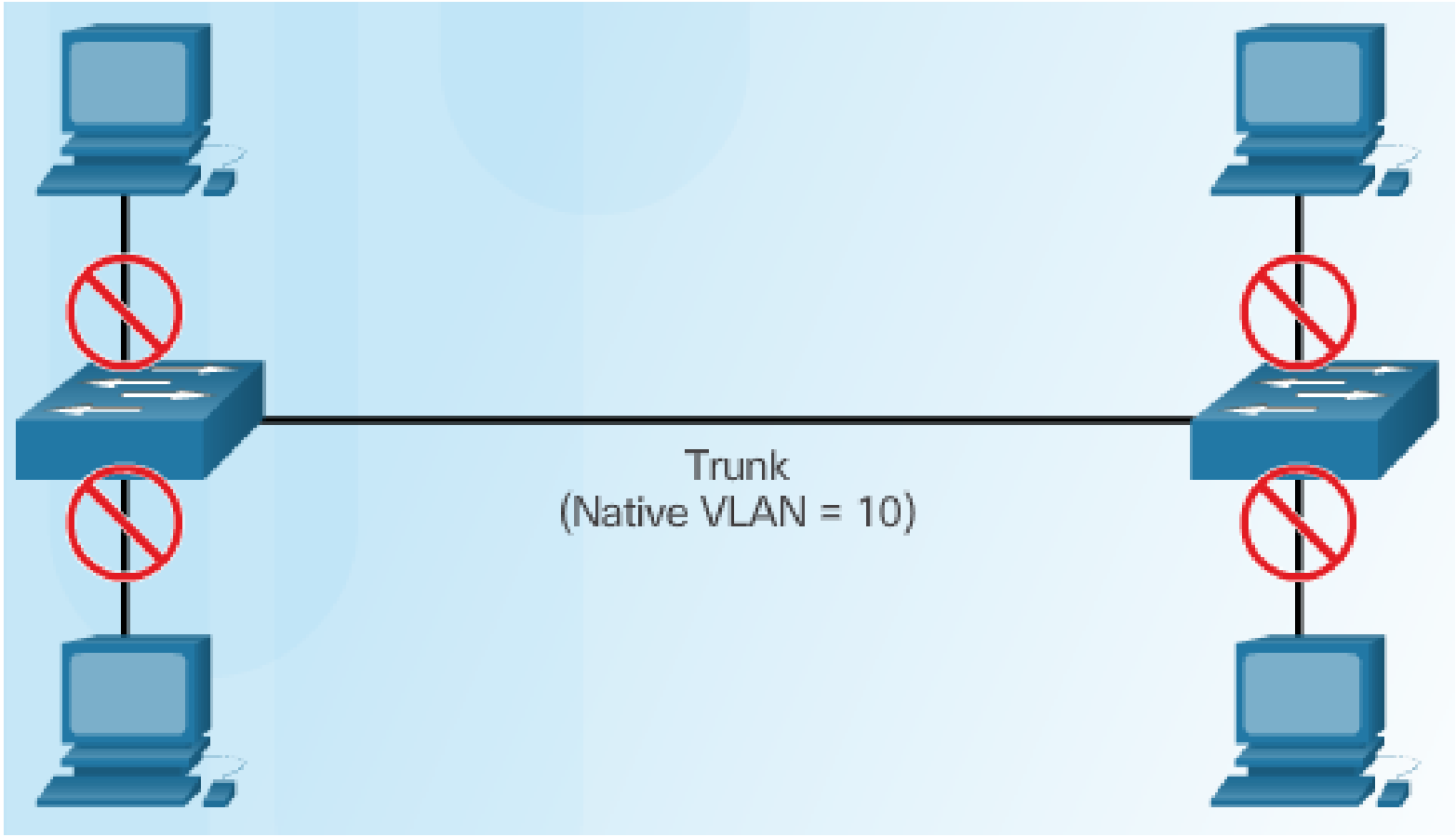
Step 2 – Double Tagging Attack

Step 3 – Double Tagging Attack



降低VLAN跳板攻擊

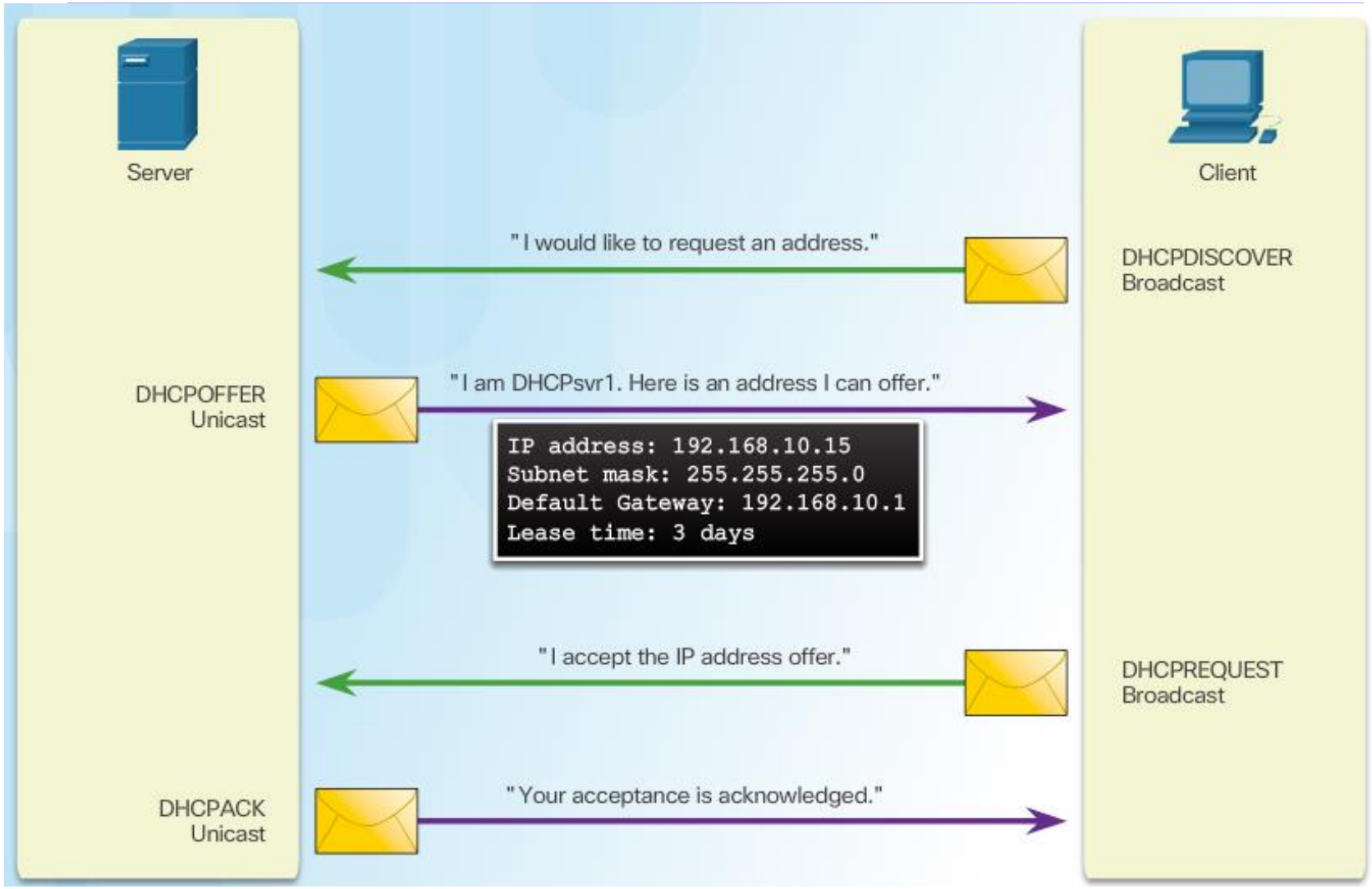
Mitigating VLAN Hopping Attacks



三、降低DHCP攻擊
Mitigating DHCP Attacks

DHCP流程

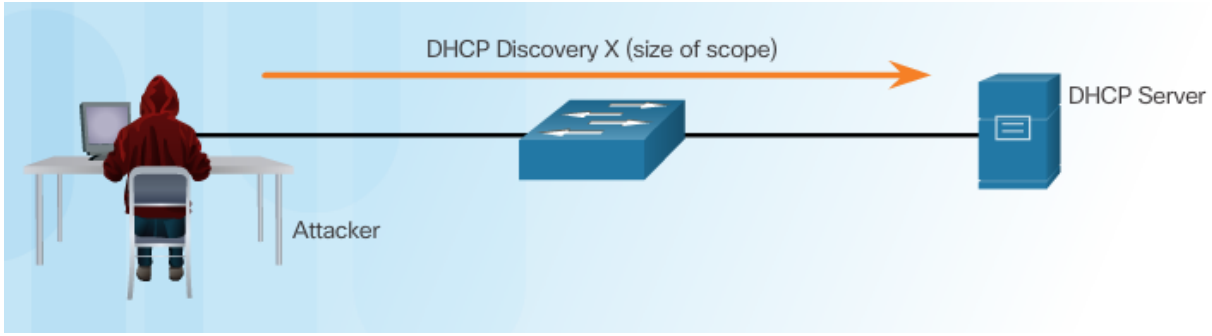
DHCP Procedures



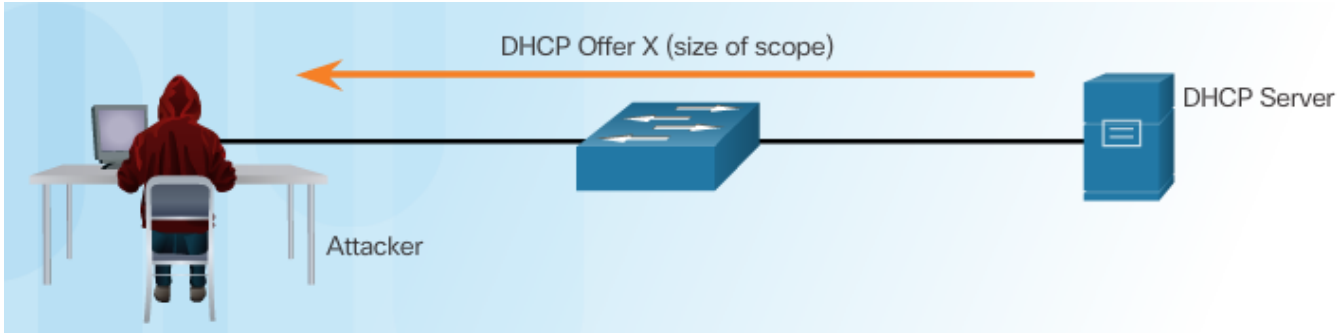
DHCP飢餓攻擊

DHCP Starvation Attack

Attacker Initiates a Starvation Attack



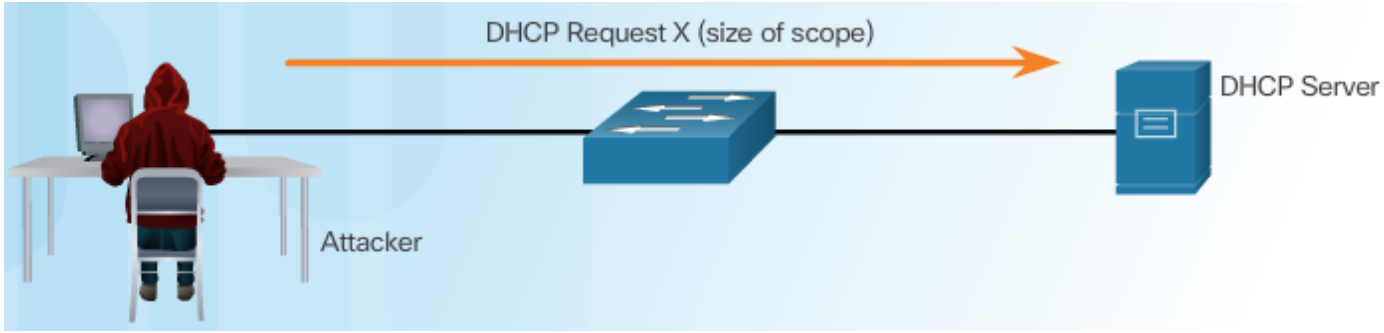
DHCP Server Offers Parameters



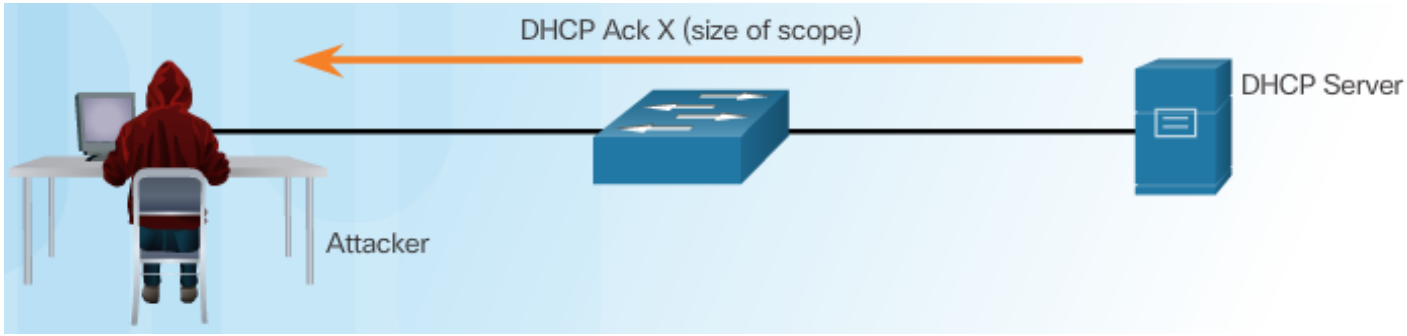
DHCP飢餓攻擊

DHCP Starvation Attack

Client Requests all Offers

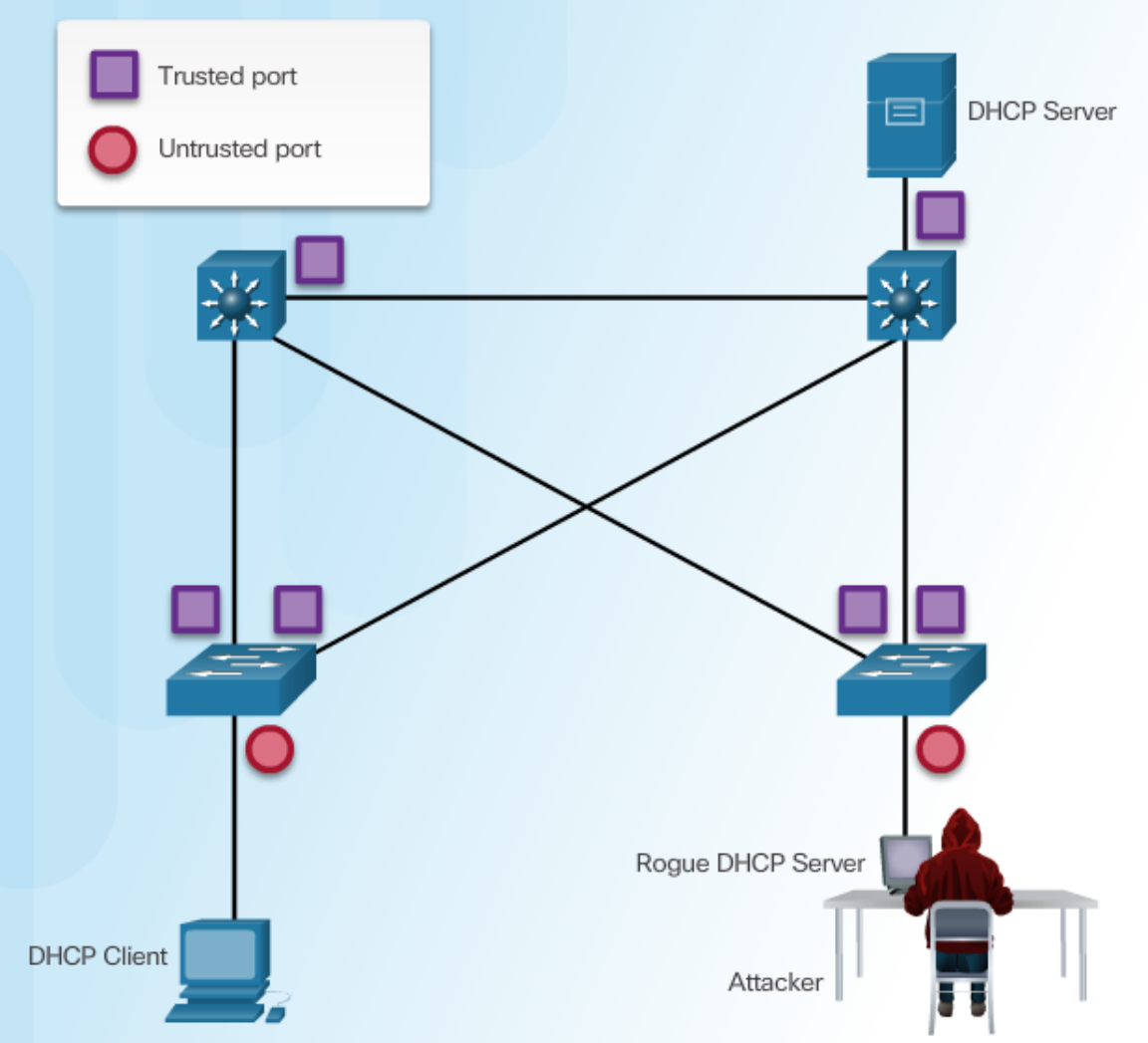


DHCP Server Acknowledges All Requests



設定DHCP窺查

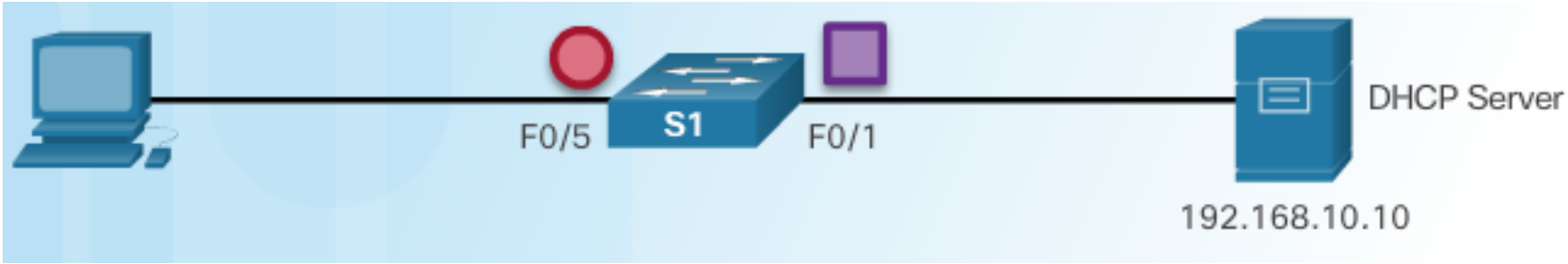
Configuring DHCP Snooping



設定DHCP窺探範例

Configuring DHCP Snooping Example

DHCP Snooping Reference Topology



Configuring a Maximum Number of MAC Addresses

```
S1(config)# ip dhcp snooping
S1(config)#
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)#
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if-range)# exit
S1(config)#
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)#
```

設定DHCP窺探範例

Configuring DHCP Snooping Example

Verifying DHCP Snooping

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/1            yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/5            no         no              6
  Custom circuit-ids:
FastEthernet0/6            no         no              6
  Custom circuit-ids:

<output omitted>
```

Configuring a Maximum Number of MAC Addresses

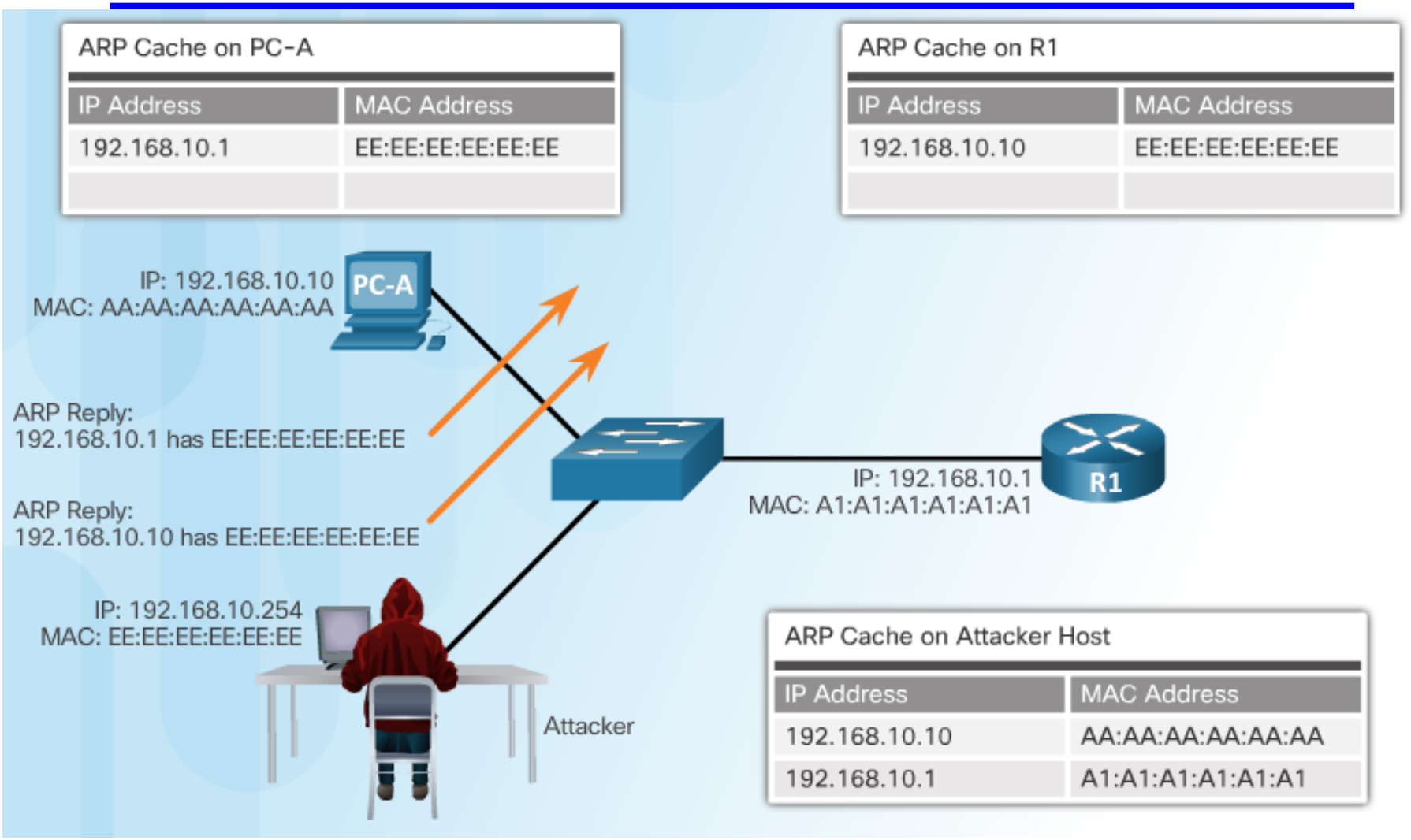
```
S1# show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN Interface
------------------  --------------- ----------  -------------  ---- --------------------
00:03:47:B5:9F:AD   192.168.10.10   193185      dhcp-snooping  5    FastEthernet0/5
```

四、降低ARP攻擊

Mitigating ARP Attacks

ARP欺騙與ARP毒化攻擊

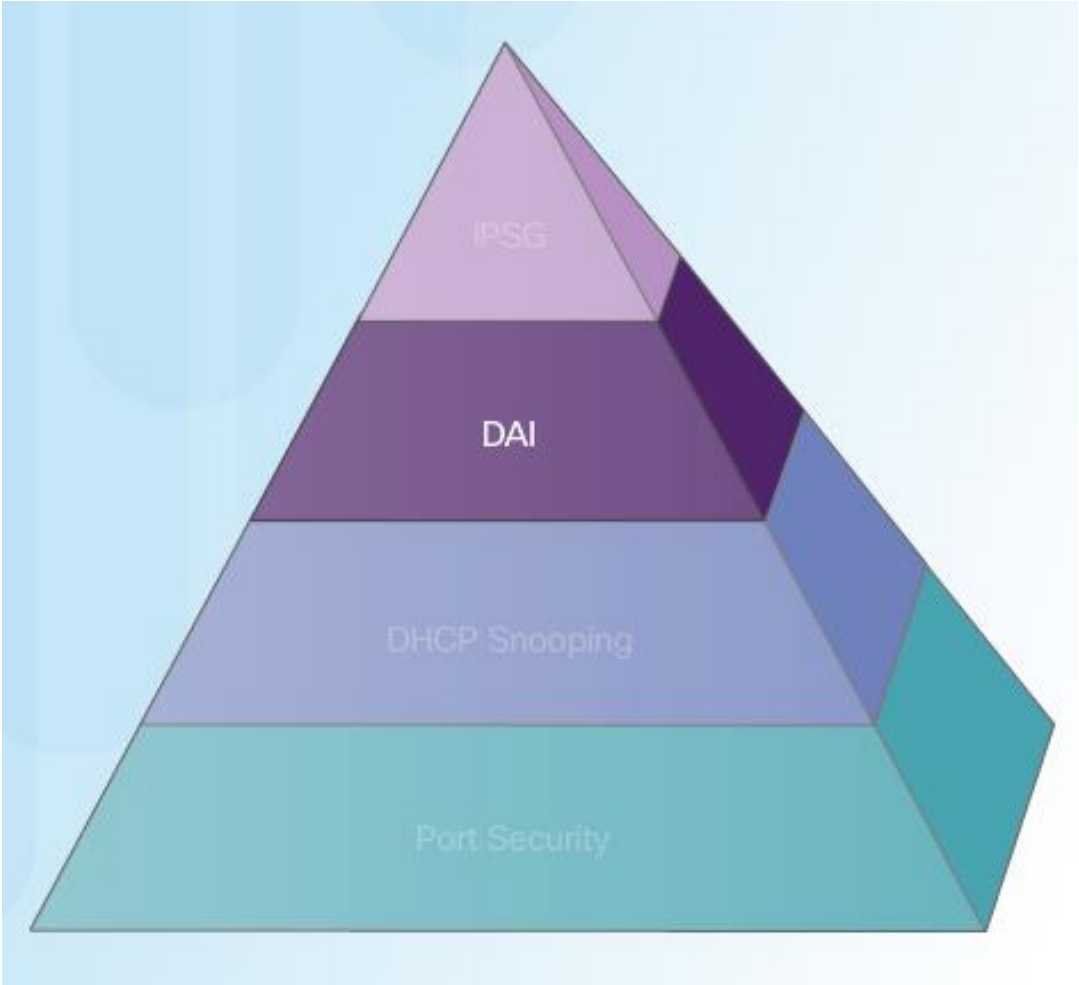
ARP Spoofing and ARP Poisoning Attack



降低ARP攻擊
Mitigating ARP Attacks

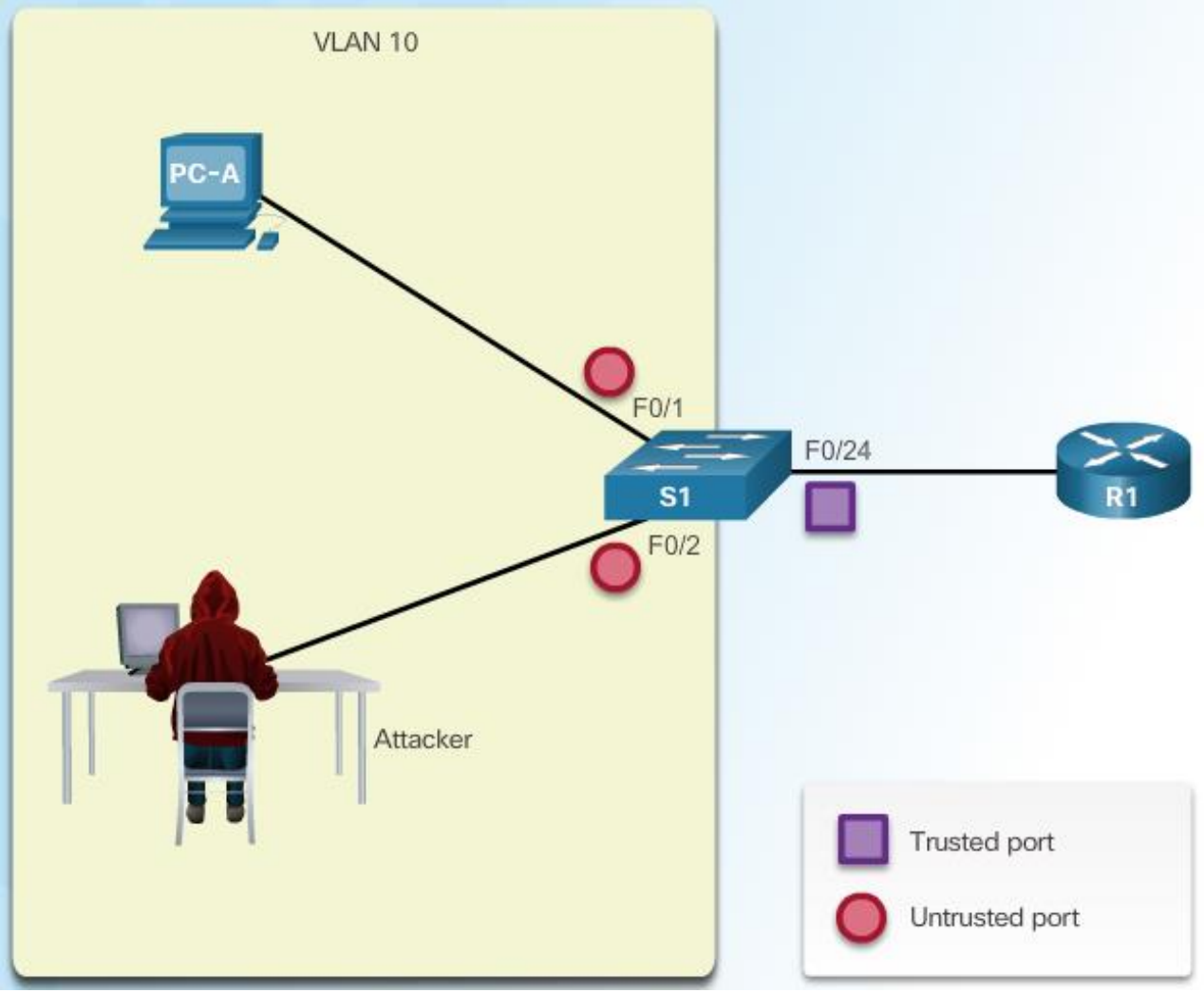
DAI(Dynamic ARP Inspection):

動態ARP的檢查:



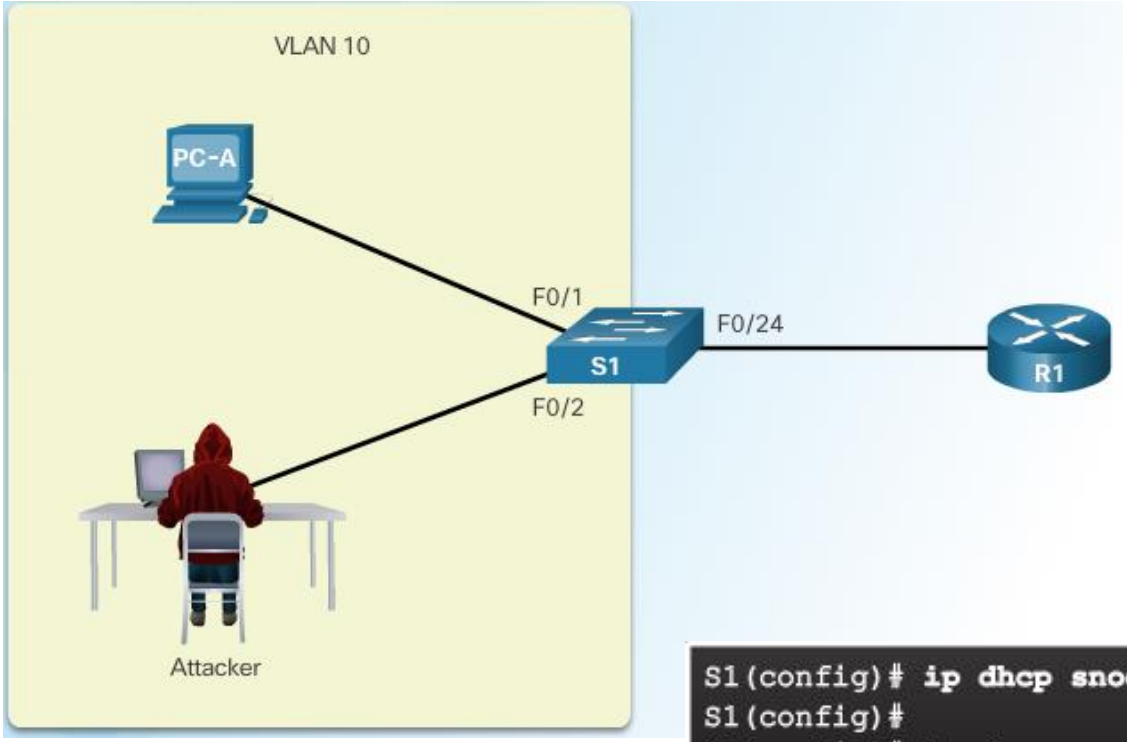
設定動態ARP檢查

Configuring Dynamic ARP Inspection



設定DHCP窺探範例

Configuring DHCP Snooping Example



ARP Reference Topology

Configuring Dynamic ARP Inspection

```
S1(config)# ip dhcp snooping
S1(config)#
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)#
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection  trust
S1(config-if)#
```

設定DHCP窺探範例

Configuring DHCP Snooping Example

Checking Source, Destination, and IP

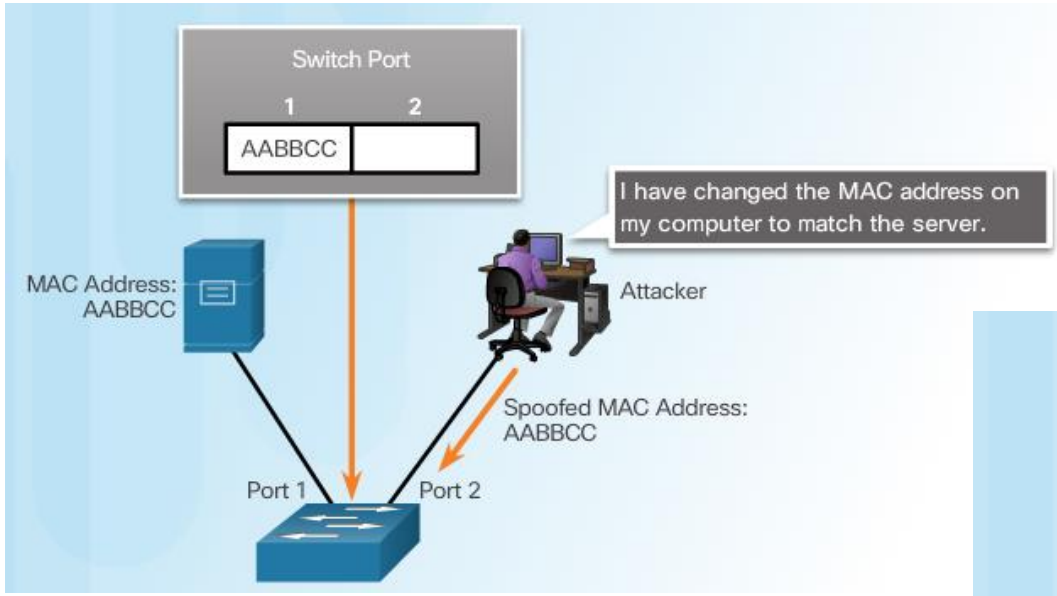
```
S1(config)# ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address

S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)#
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)#
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)#
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

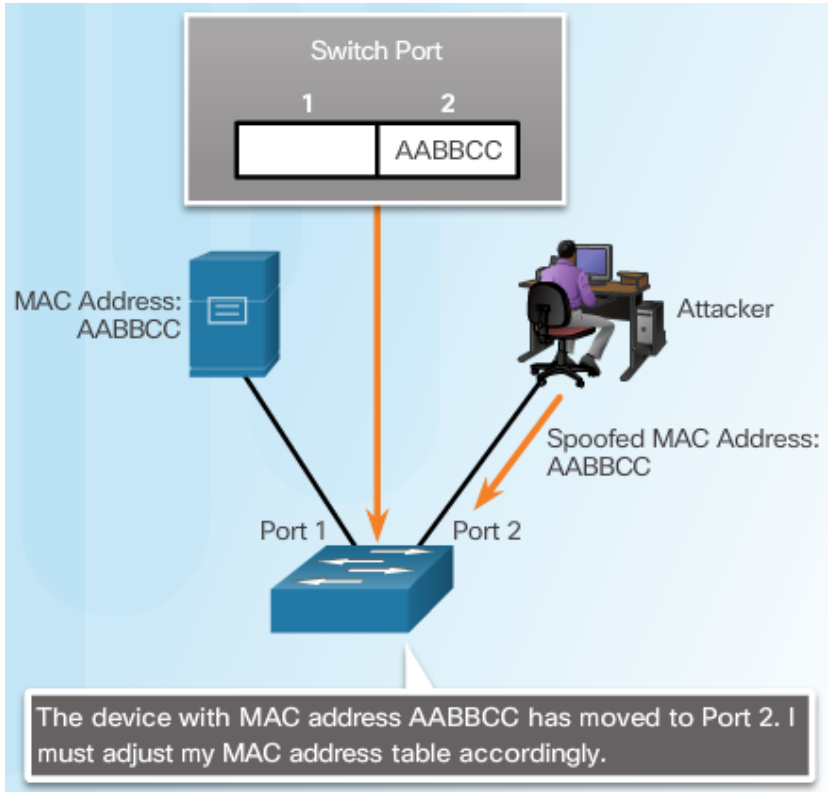
五、降低Address欺騙攻擊

Mitigating Address Spoofing Attacks

Address欺騙攻擊

Address Spoofing Attack





降低Address欺騙攻擊

Mitigating Address Spoofing Attacks

在各未授權的埠，他們IP流量安全過濾有兩種可能等級

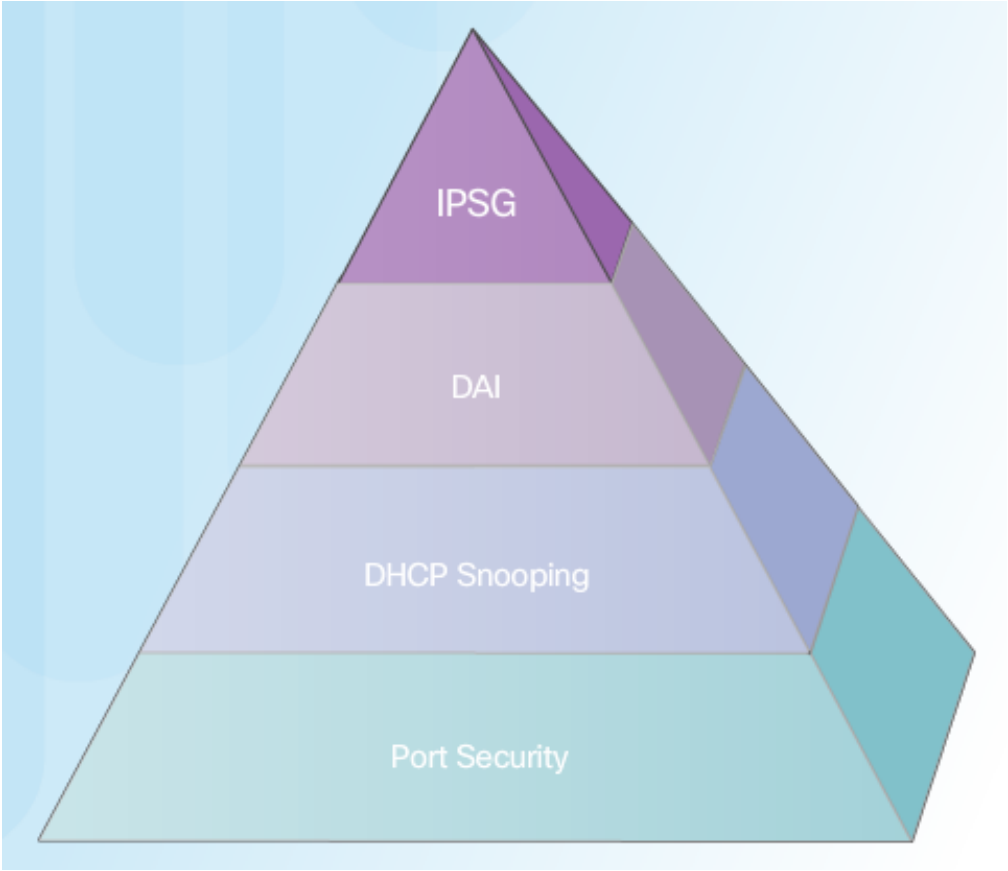
For each untrusted port, there are two possible levels of IP traffic security filtering:

- 來源IP address 過濾

  Source IP address filter

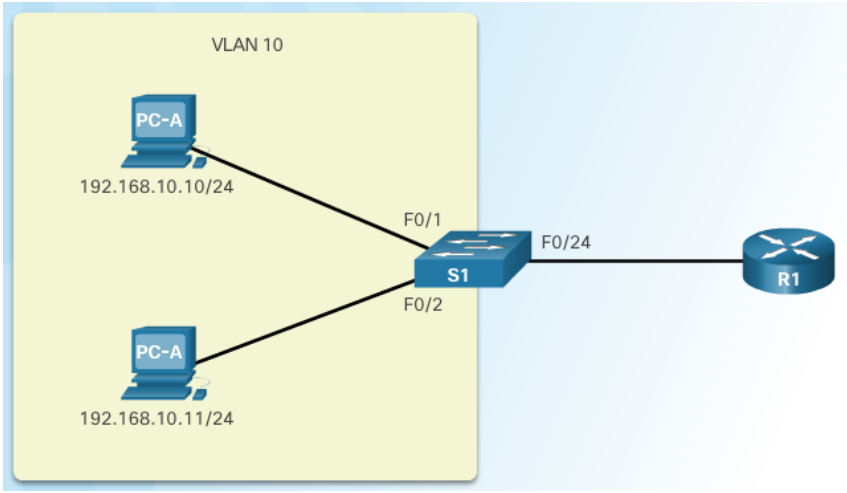
- 來源IP address 和MAC過濾

  Source IP and MAC address filter



設定IP來源防範

Configuring IP Source Guard



IP來源防範反饋拓譜

IP Source Guard Reference Topology

設定IP來源防範

Configuring IP Source Guard

```
S1(config)# interface range fastethernet 0/1 - 2
S1(config-if-range)# ip verify source
S1(config-if-range)# end
S1#
```

檢查IP來源防範

Checking IP Source Guard

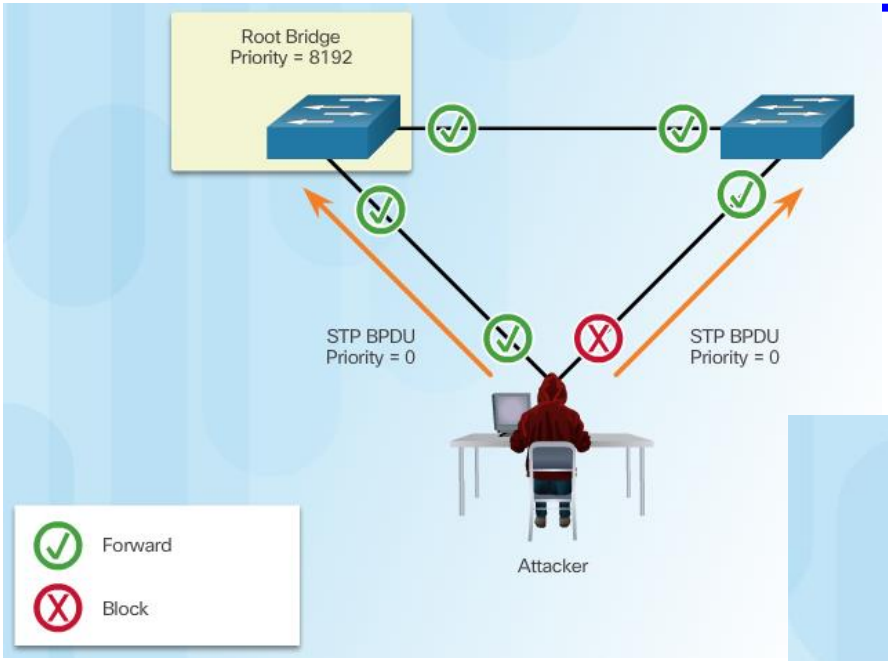
```
S1# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
F0/1       ip           active       192.168.10.10                       10
F0/2       ip           active       192.168.10.11                       10
S1#
```

六、降低STP攻擊

Mitigating STP Attacks

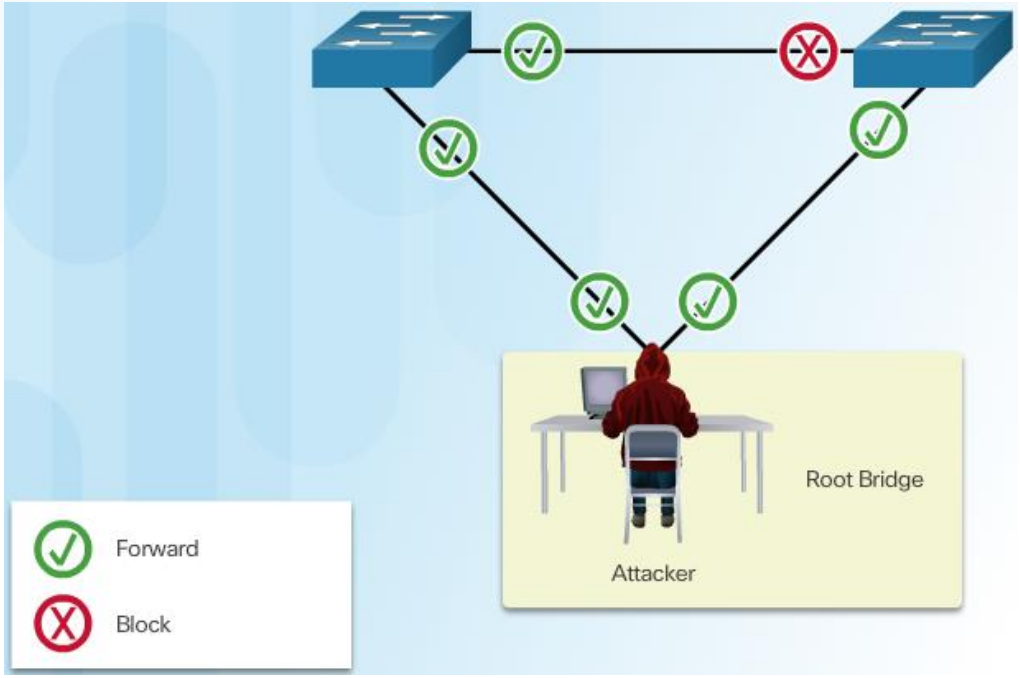
STP操作攻擊

STP Manipulation Attacks



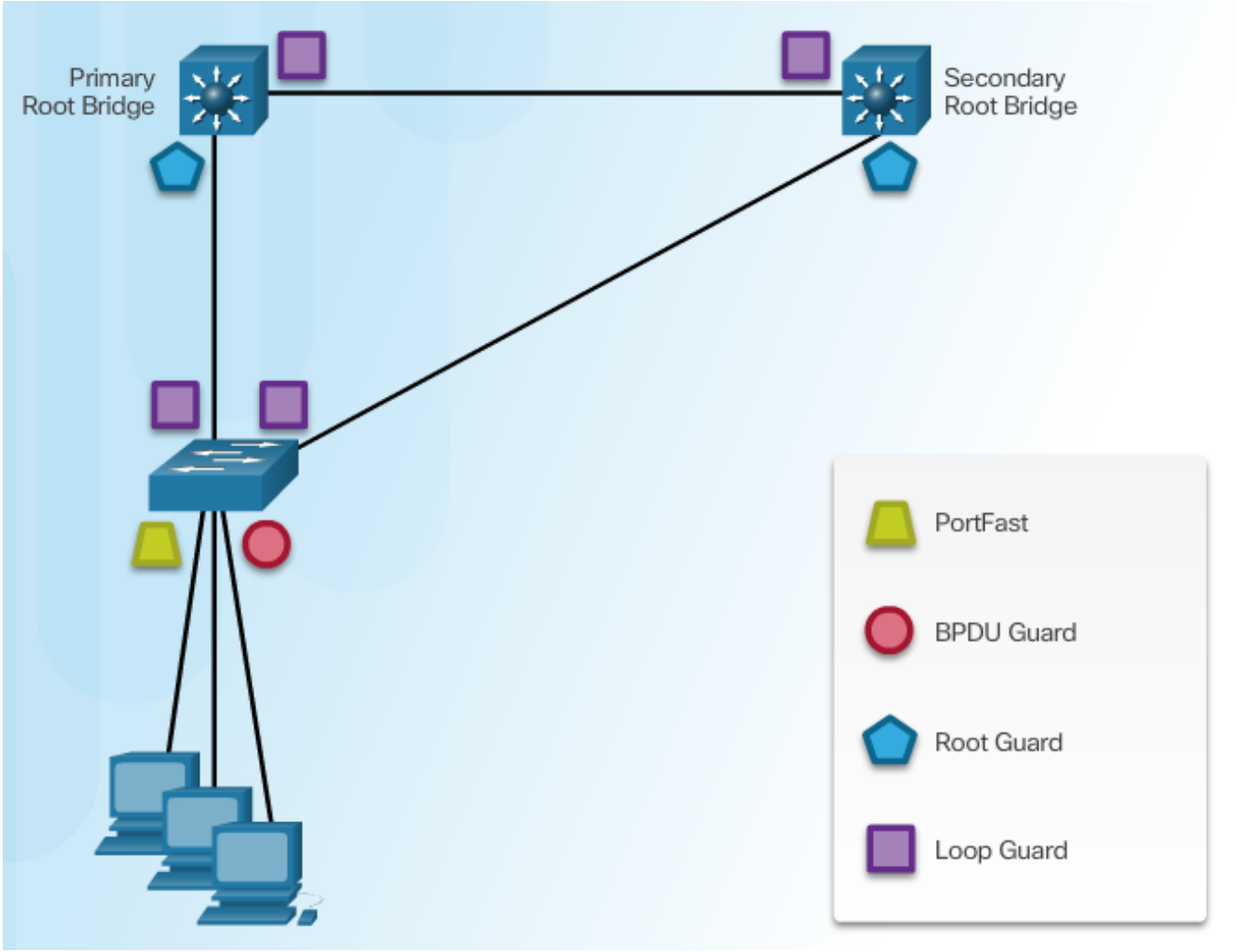
Spoofing the Root Bridge

Successful STP Manipulation Attack



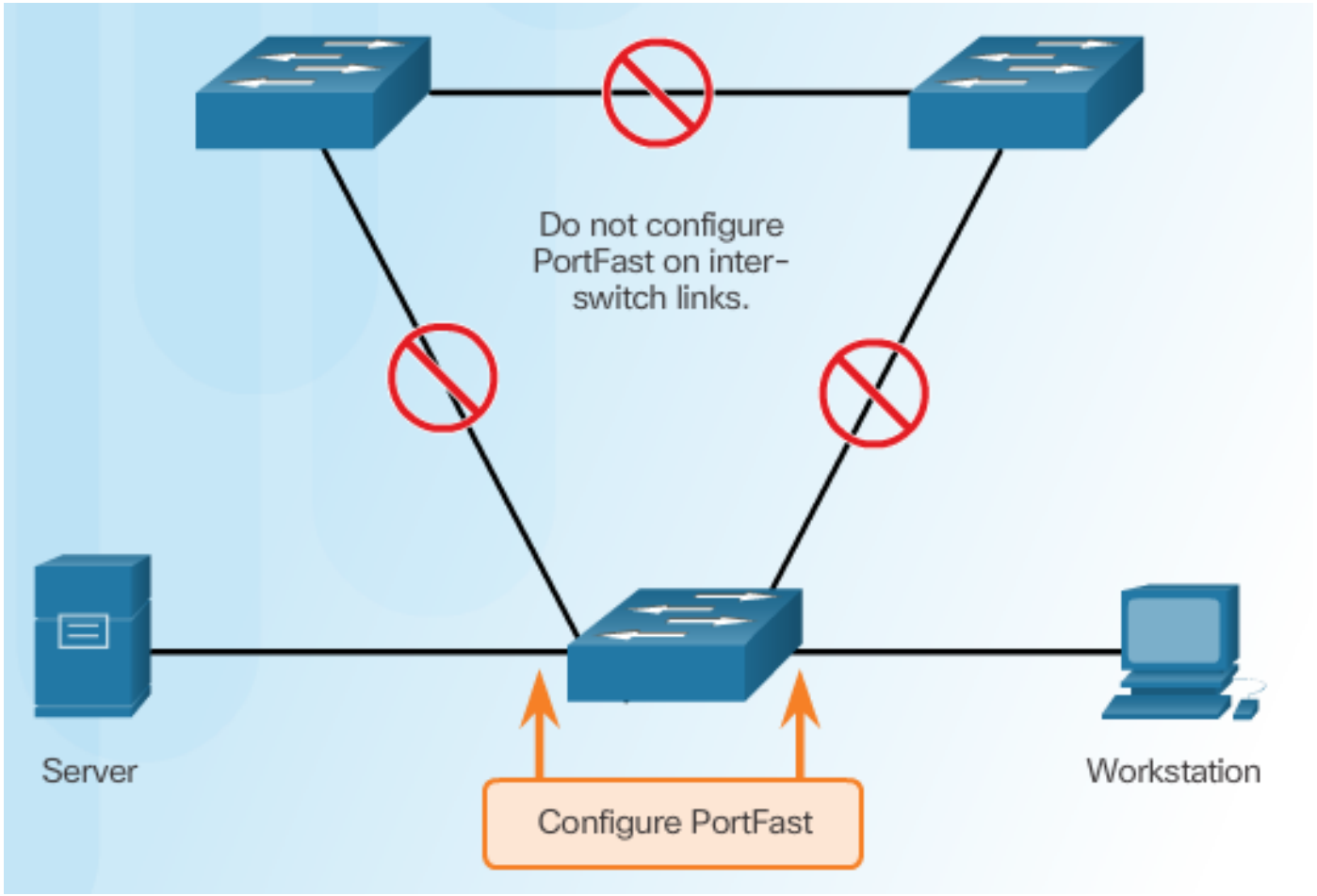
降低STP攻擊

Mitigating STP Attacks



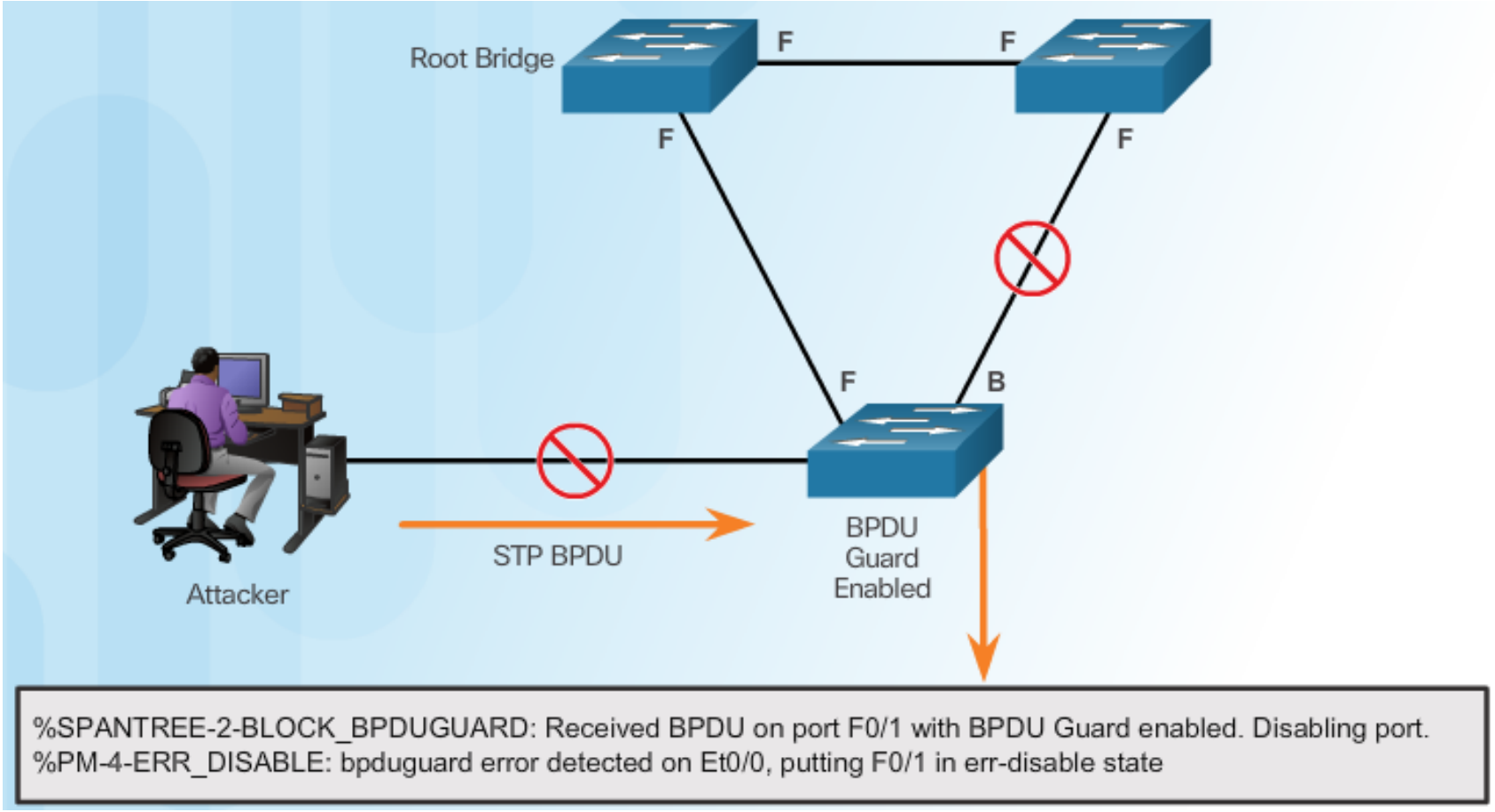
設定PortFast

Configuring PortFast



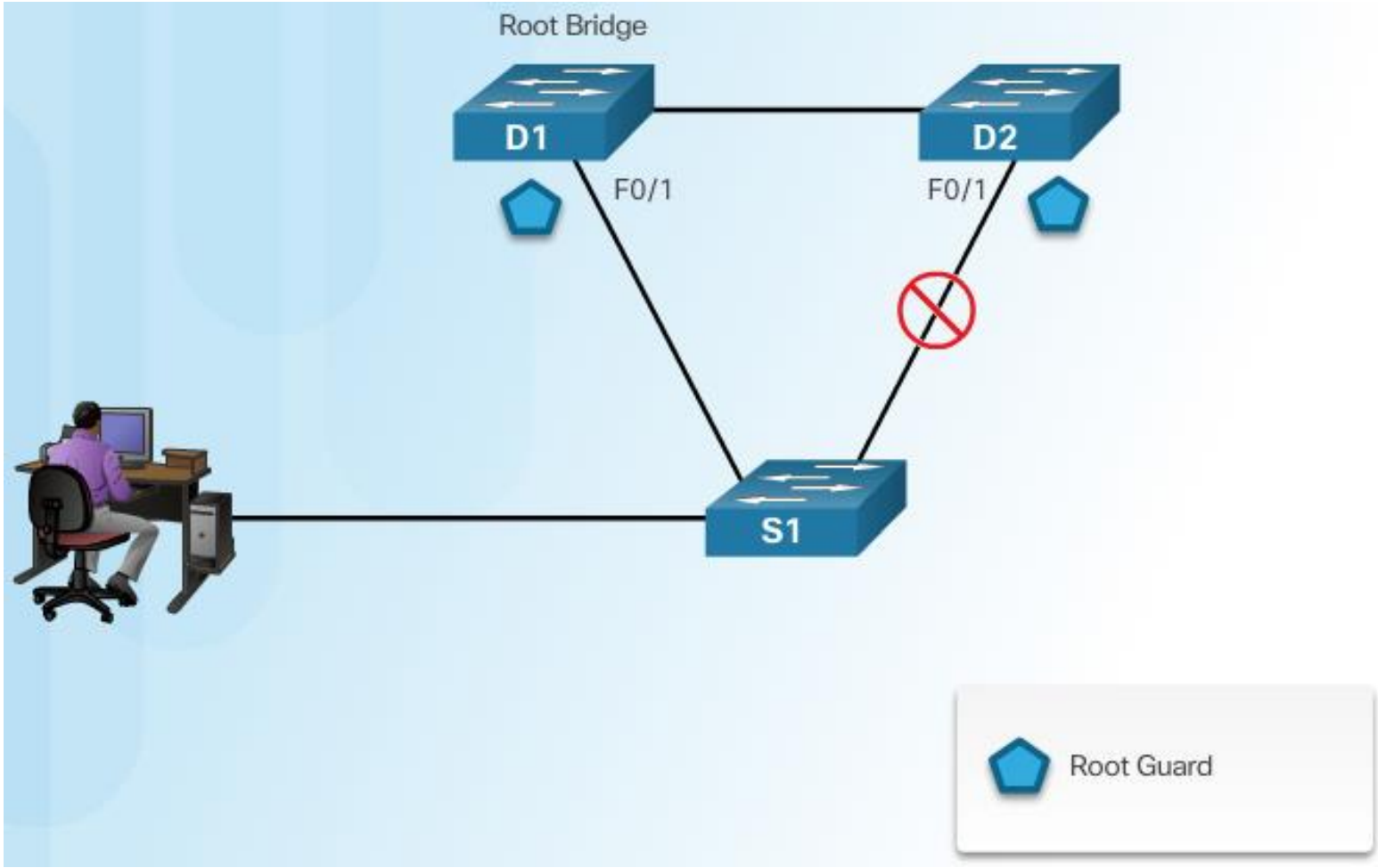
設定BDPU防護

Configuring BDPU Guard



設定根防護

Configuring Root Guard



設定迴路防護

Configuring Loop Guard