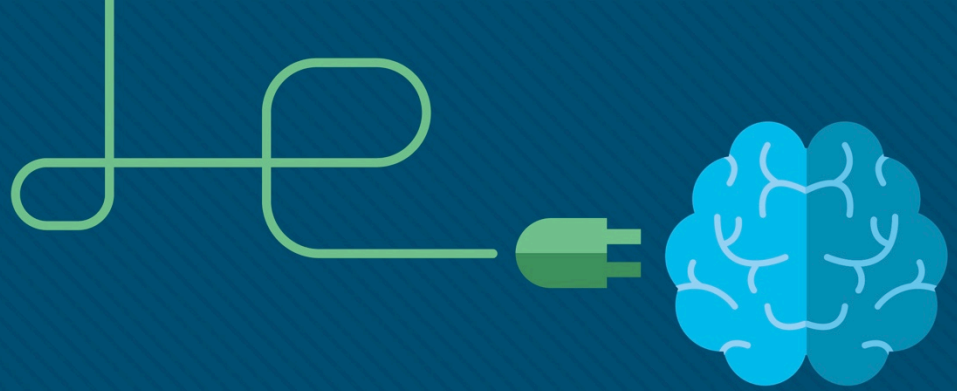


12 交换机安全配置

单元目标

模块主题： 交换机安全配置

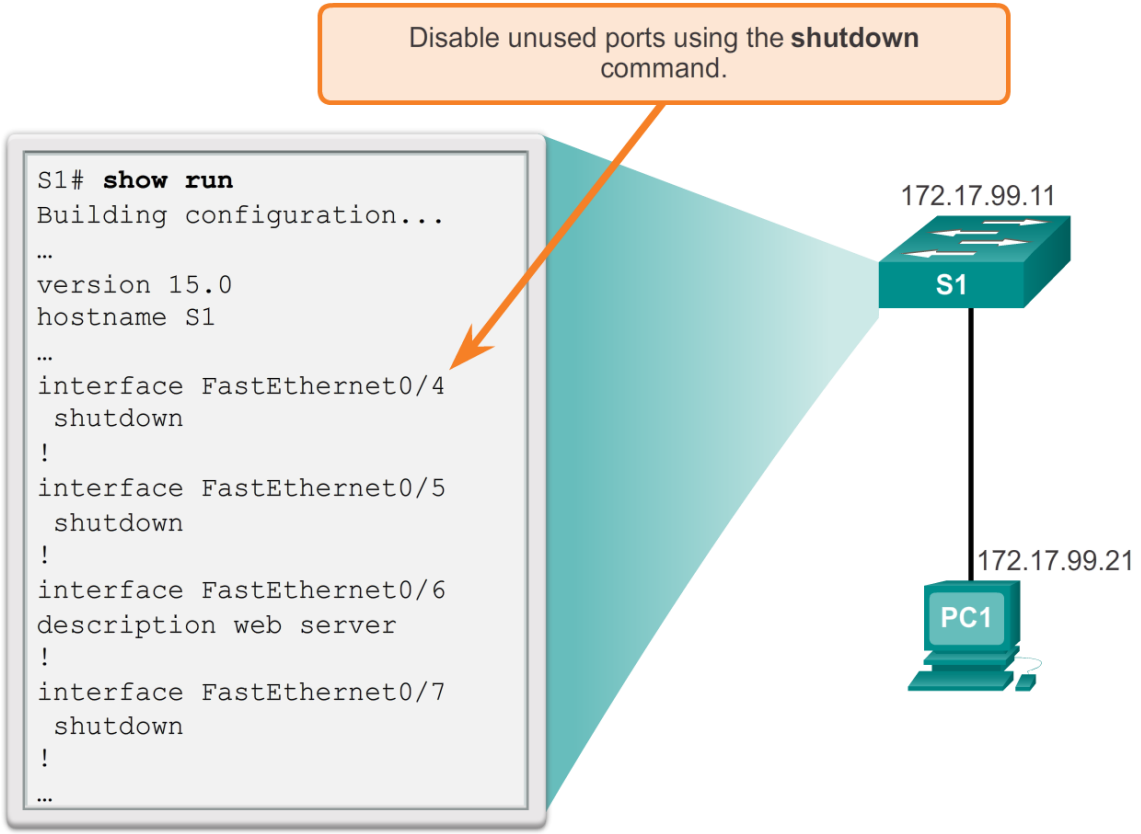
模块目标： **配置交换机安全以缓解局域网攻击。**

主题标题	主题目标
实施端口安全	实施端口安全功能，缓解 MAC 地址表攻击。
缓解 VLAN 攻击	解释如何配置 DTP 和本征 VLAN，缓解 VLAN 攻击。
缓解 DHCP 攻击	解释如何配置 DHCP 侦听，缓解 DHCP 攻击。
缓解 ARP 攻击	解释如何配置 ARP 检查，缓解 ARP 攻击。
缓解 STP 攻击	解释如何配置PortFast和BPDU防御，缓解STP攻击。

12.1 实施端口安全

保护没有使用的端口

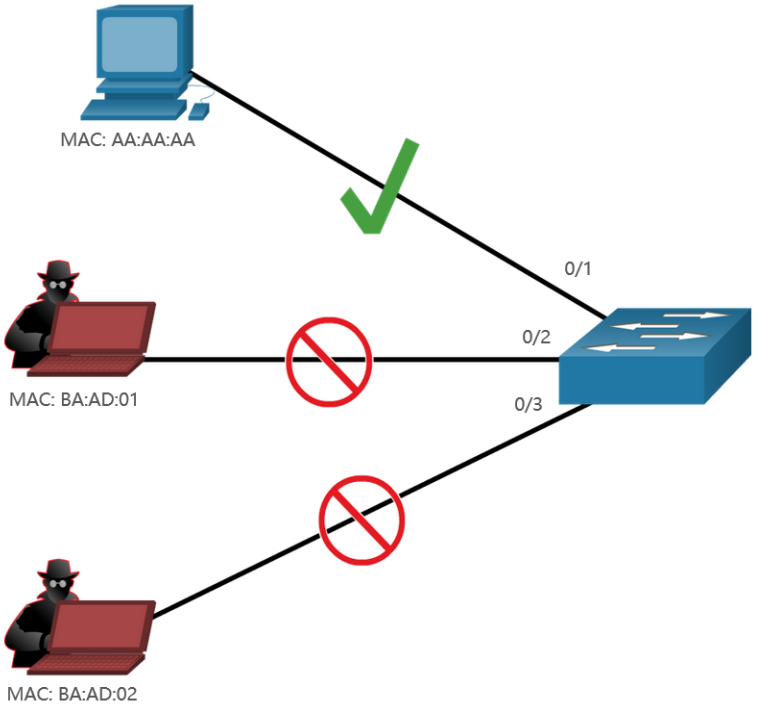
- **禁用未使用的端口是一种简单但有效的安全原则。**




```
S1(config)# interface range fa0/8 - 24
S1(config-if-range)# shutdown
```

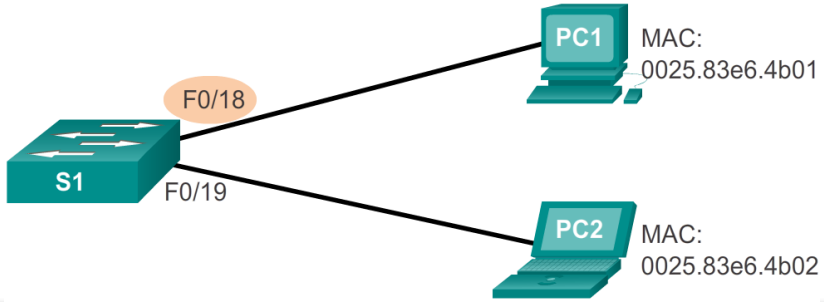
启用端口安全

- **启用端口安全**是防止MAC地址表溢出攻击最简单，最有效的方法
- 端口安全限制端口上所允许的有效 MAC 地址数量
- 允许访问合法设备的 MAC 地址，而拒绝访问其他 MAC 地址
- 任何通过未知 MAC 地址进行连接的尝试都会导致安全违规



启用端口安全

- **启用端口安全**
  - 端口必须手工设置为access模式



Cisco IOS CLI Commands	
Specify the interface to be configured for port security.	`S1(config)# interface fastethernet 0/18`
Set the interface mode to access.	`S1(config-if)# switchport mode access`
Enable port security on the interface.	`S1(config-if)# switchport port-security`

启用端口安全

- **show port-security interface命令显示当前端口安全配置**

```
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
```

启用端口安全

- 端口安全默认配置

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Sticky address learning	Disabled

限制和学习MAC地址

- 设置端口允许的**最大MAC地址数量**，使用如下命令:

Switch(config-if)# **switchport port-security maximum** *value*

- 默认值为**1**。
- 不同交换机和操作系统MAC地址的最大数不同

限制和学习MAC地址

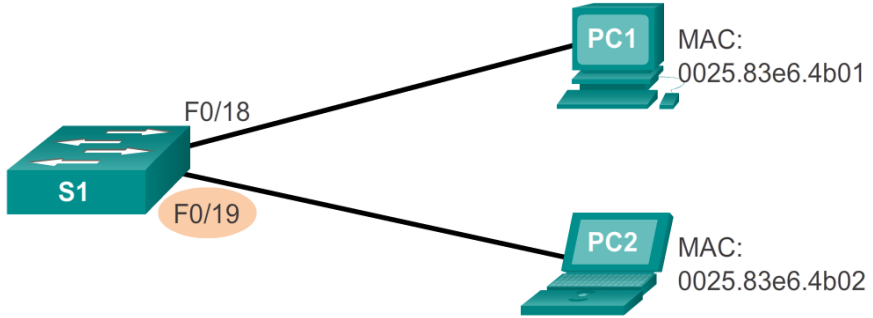
- 可以通过三种方式**配置安全 MAC 地址：**
  1. **静态安全MAC地址**

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

  2. **动态安全MAC 地址**
     - **默认配置**
  3. **动态粘滞安全MAC地址（粘连的MAC会自动加到running-config）**

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

限制和学习MAC地址



- 配置端口安全**粘滞**

Cisco IOS CLI Commands	
Specify the interface to be configured for port security.	`S1(config)# interface fastethernet 0/19`
Set the interface mode to access.	`S1(config-if)# switchport mode access`
Enable port security on the interface.	`S1(config-if)# switchport port-security`
Set the maximum number of secure addresses allowed on the port.	`S1(config-if)# switchport port-security maximum 10`
Enable sticky learning.	`S1(config-if)# switchport port-security mac-address sticky`

限制和学习MAC地址

```
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
```

- 检验端口安全粘滞

```
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
```

限制和学习MAC地址

```
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
```

- 检验端口安全粘滞

```
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      -
------------------------------------------------------------
```

端口安全老化（aging）

- 老化（aging）是指安全地址到达一定时间后会从端口删除。
- 默认情况下，学习到的MAC地址不会老化。

```
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
```

```
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      -
------------------------------------------------------------
```

端口安全老化（aging）

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

- **端口安全老化**可设置**静态和动态**安全地址老化时间，每个端口支持两种类型：
  - **Absolute**-在指定的老化时间后，将删除端口上的安全地址。
  - **Inactivity**-如果端口上的安全地址在指定时间内不活动，则将其删除。
  - 使用老化来删除安全端口上的安全MAC地址，而无需手动删除。
- 使用**switchport port-security aging**命令启用或禁用安全端口的静态老化，或设置老化时间或类型。

端口安全老化（aging）

Switch(config-if)# **switchport port-security aging time 10**
Switch(config-if)# **switchport port-security aging type inactivity**

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b(
Security Violation Count   : 0
```

```
S1# show port-security address
Secure Mac Address Table
-----------------------------------------------------------
Vlan    Mac Address       Type             Ports   Remaining Age
                                                     (mins)
----    -----------       ----             -----   -------------
1       0025.83e6.4b01    SecureDynamic    Fa0/18      9(I)
1       0025.83e6.4b02    SecureSticky     Fa0/19
-----------------------------------------------------------
```

端口安全违规模式

- 当出现以下任一情况时，交换机会将其视为**安全违规**：
  - 端口下的MAC地址数量超过了设置的**最大值**。
  - 一个安全接口上学习或配置MAC出现在相同VLAN 的**另一个安全接口**上。

Security violation modes include: Protect, Restrict, and 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

端口处于错误禁用状态

- 端口安全违规会使交换机处于**错误禁用状态**
- **默认关闭**处于错误禁用状态的端口
- 交换机将通过**控制台消息**传达这些事件

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

端口处于错误禁用状态

- **show interface** 命令也显示了处于错误禁用状态的交换机端口

```
S1# show interface fa0/18 status
Port Name   Status        Vlan   Duplex   Speed    Type
Fa0/18      err-disabled  1      auto     auto     10/100BaseTX

S1# show port-security interface fastethernet 0/18
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   : 000c.292b.4c75:1
Security Violation Count   : 1
```

端口处于错误禁用状态

- 必须发出 shutdown/no shutdown 接口命令重新启用端口

```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to up
```

检验端口安全

- show port-security
- show port-security interface
- show port-security address
- show run

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/1              1            0                  0         Shutdown
      Fa0/2              1            0                  0         Shutdown
      Fa0/3              1            0                  0         Shutdown
(output omitted)
     Fa0/24              1            0                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

12.2 缓解VLAN攻击

VLAN攻击回顾

VLAN跳跃攻击的三种方式：

1. 攻击主机的**DTP**消息欺骗。
2. 引入**恶意交换机**并启用中继。
3. **双重标签**（或双重封装）攻击。

缓解VLAN跳跃攻击的步骤

缓解VLAN跳跃攻击的步骤：

1. 使用 ***switchport mode access*** 接口配置命令在非中继端口上禁用DTP协商。
2. **禁用未使用的端口，并将其放入未使用的VLAN。**
3. 使用 ***switchport mode trunk*** 命令在中继端口手动启用中继链路。
4. 使用 ***switchport nonegotiate*** 命令禁用中继端口上的DTP协商。
5. 使用 ***switchport trunk native vlan*** *vlan_number* 命令将本征VLAN设置为没有用户的VLAN。

缓解VLAN跳跃攻击的步骤

```
S1(config)# interface Fastethernet 0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10

S1(config)# interface Fastethernet 0/4
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate
S1(config-if)# switchport trunk native vlan 99

S1(config)# interface Fastethernet 0/20（不使用）
S1(config-if)# shutdown
```

12.3 缓解DHCP攻击

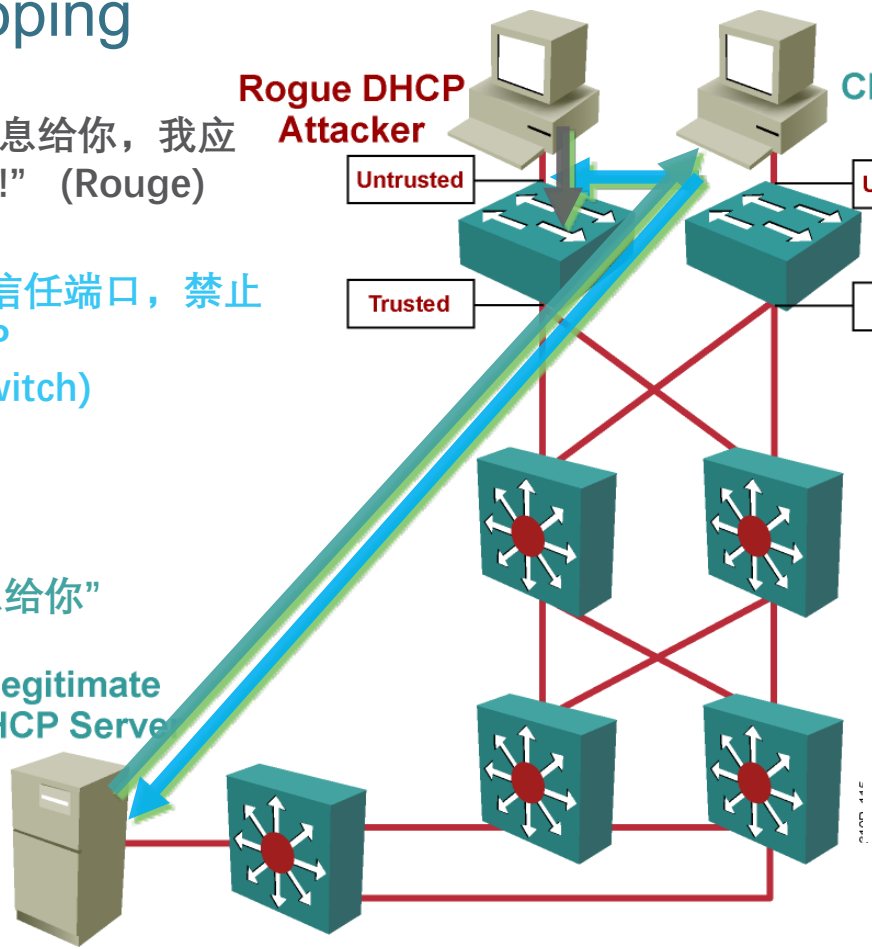
缓解DHCP攻击

DHCP snooping

- DHCP侦听是用来缓解DHCP欺骗攻击的有效手段。
- DHCP侦听将交换机端口分为信任和不信任两种类型。
  - 信任端口可以发送和接收所有DHCP消息
  - 不信任端口只能发送DHCP请求
  - 如果不信任端口接收到DCHP响应，则该端口将会关闭。
  - 不信任端口不应响应任何DHCP服务，例如DHCPOFFER，DHCPACK或DHCPNAK。
- 不信任端口会构建DHCP绑定表
  - 记录的用户MAC地址，IP地址，租约时间，绑定类型，VLAN号和端口号。

缓解DHCP攻击

DHCP snooping



“收到，信息给你，我应该是第一个!” (Rouge)

“我需要IP地址/掩码，默认网关和DNS服务器”

“收到，多谢!”

“这是非信任端口，禁止接收 DHCP Offer” (Switch)

“这是信任端口，允许接收 DHCP Offer” (Switch)

“收到，信息给你” (Legitimate)

部署DHCP snooping的步骤

- 配置DHCP snooping步骤如下:

1. 在全局配置下使用 **ip dhcp snooping** 命令启用DHCP侦听。
2. 在信任端口使用 **ip dhcp snooping trust** 命令。
3. 在非信任端口使用 **ip dhcp snooping limit rate** *packets-per-second* 命令限制DHCP discovery 信息频率。
4. 在全局配置下使用 **ip dhcp snooping vlan** 命令确定在哪些VLAN启用 DHCP 侦听。

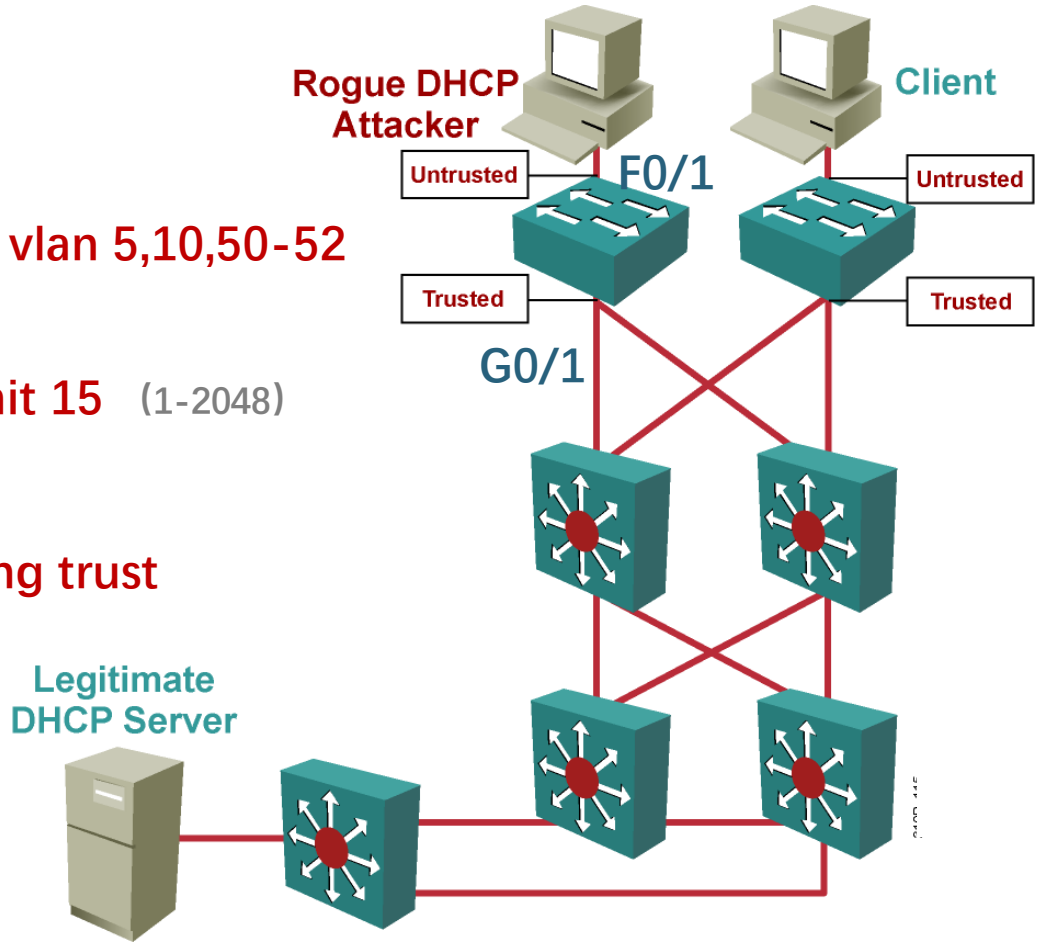
注：所有端口默认为非信任接口

DHCP snooping 配置举例

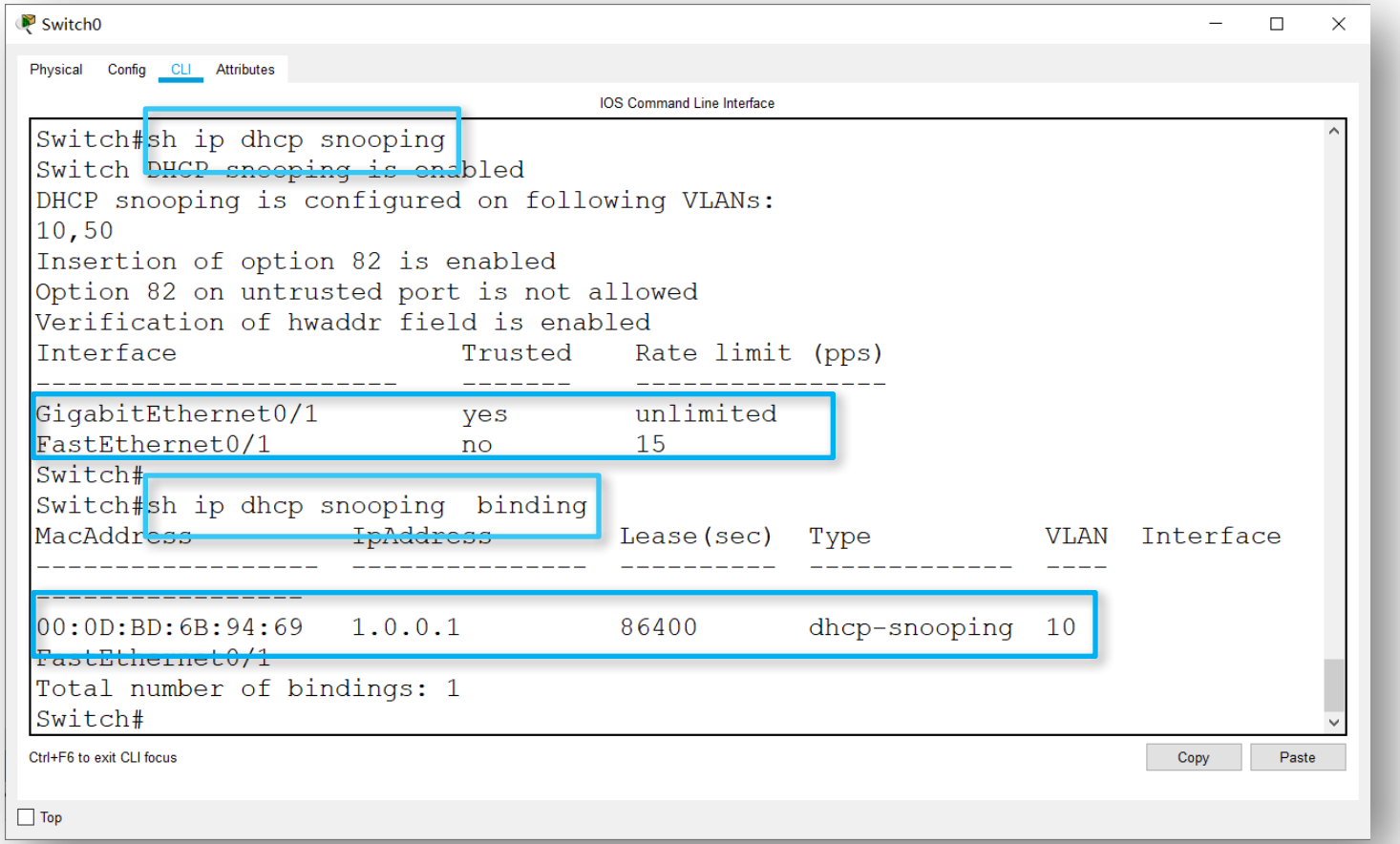
```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 5,10,50-52

Switch(config)# interface f 0/1
Switch(config-if)# ip dhcp rate limit 15    (1-2048)

Switch(config)# interface g 0/1
Switch(config-if)# ip dhcp snooping trust
```



DHCP snooping 配置举例



12.4 缓解ARP攻击

动态ARP检查（DAI）

- 为了防止ARP欺骗或“中毒”，交换机必须确保仅中继有效的ARP请求和响应。
- DAI通过拦截和验证所有ARP请求和响应来防止这些攻击。
  - 在将非信任端口截获的ARP应答转发到PC之前，都要对MAC地址和Ip地址进行绑定验证。
  - 无效设备的ARP应答将被丢弃和记录（log）。
  - DAI根据DHCP侦听或静态ARP条目建立的有效MAC地址到IP地址的绑定数据库来确定ARP数据包的有效性。
  - 如果超过了DAI配置的ARP数据包数量，则错误禁用接口。

动态ARP检查（DAI）实施指南

- DAI 实施指南:
- **全局启用** DHCP snooping
- 选择**VLAN**启用 DHCP snooping
- 在选择的VLAN**启用 DAI**
- 在**信任端口**配置 DHCP snooping 和 ARP inspection

注：所有端口默认为DAI非信任接口

DAI配置举例

S1(config)# **ip dhcp**

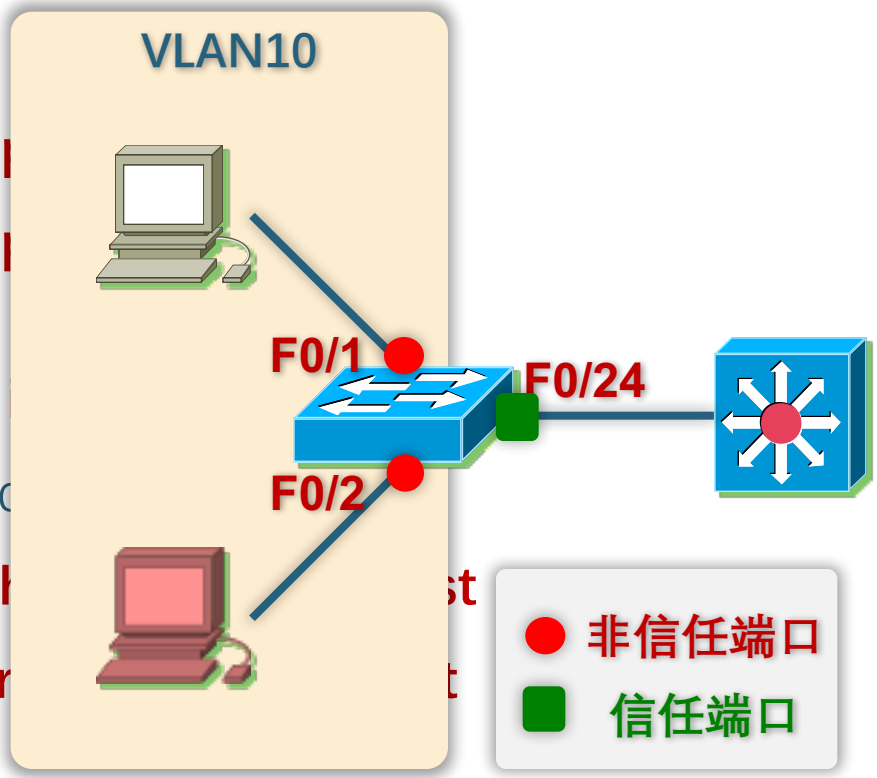
S1(config)# **ip dhcp**
10

S1(config)# **ip arp**

S1(config)# interfac

S1(config-if)# **ip dh** **st**

S1(config-if)# **ip ar** **t**



DAI配置举例

- DAI还可以检查目的MAC、源MAC和IP地址：
  - **目的MAC：**对照ARP中的目标MAC检查帧头中的目的MAC地址。
  - **源MAC：**对照ARP中的发送者MAC检查帧头中的源MAC地址。
  - **IP地址：**检查ARP中是否包含无效和非期望的IP地址，包括地址0.0.0.0、255.255.255.255和所有IP组播地址。

命令：

```
S1(config)# ip arp inspection validate {[src-mac] [dst-mac] [ip]}
```

注：只能配置一个命令

12.5 缓解STP攻击

PortFast 和 BPDU Guard

- 缓解STP攻击，使用PortFast和BPDU Guard结合来防护：
  - **PortFast**
    - PortFast会立即使端口从阻塞状态进入**转发状态**，从而绕过侦听和学习状态，可能导致STP环路出现。
    - 应用于所有**最终用户**访问端口。
  - **BPDU Guard**
    - BPDU Guard会立即错误禁用接收BPDU的端口。
    - 与PortFast一样，BPDU Guard应用于最终用户访问端口。

PortFast 和 BPDU Guard

- 启用Port Fast

PortFast 和 BPDU Guard

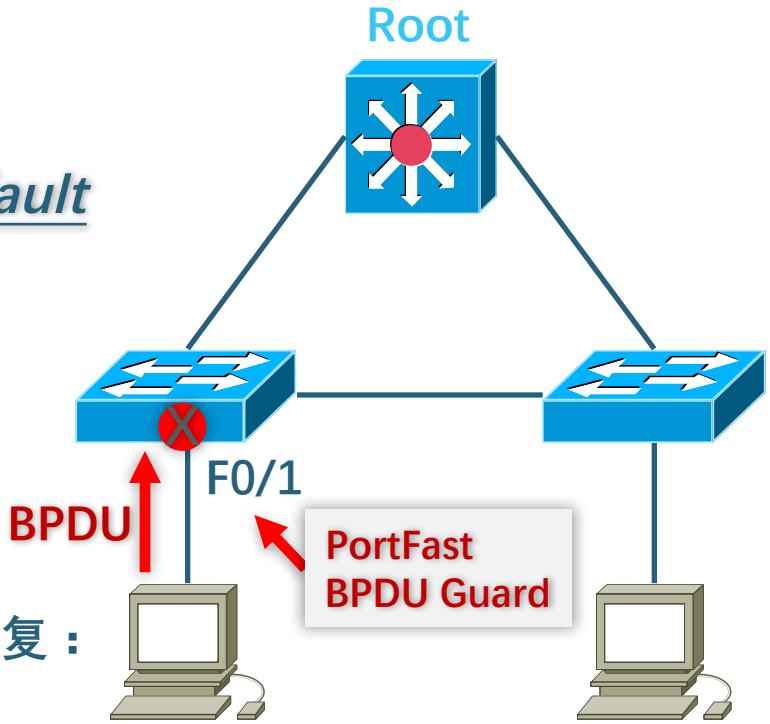
启用 BPDU Guard

- **全局启用：**

spanning-tree portfast bpduguard default

- **端口启用：**

spanning-tree bpduguard enable



- 端口收到BPDU，则进入error-disabled状态，默认要手工恢复。也可以使用全局命令自动恢复：

errdisable recovery cause psecure_violation

12.6 - 单元练习与测验

Packet Tracer – 交换机安全配置

在这个Packet Tracer测试中，您会：

- 保护未使用端口的安全
- 实施端口安全
- 缓解 VLAN 跳跃攻击
- 缓解 DHCP 攻击
- 缓解 ARP 攻击
- 缓解 STP 攻击
- 验证交换机安全配置

实验 – 交换机安全配置

在本实验中，您将：

- 保护未使用端口的安全
- 实施端口安全
- 缓解 VLAN 跳跃攻击
- 缓解 DHCP 攻击
- 缓解 ARP 攻击
- 缓解 STP 攻击
- 验证交换机安全配置

我在这个模块中学到了什么？

- 在部署交换机以用于生产之前，所有交换机端口（接口）都应该进行保护。
- 在默认情况下，二层交换机都会设置为dynamic auto默认（支持中继模式）。
- 防止 CAM 表溢出攻击最简单有效的方法是启用端口安全。
- 交换机可以通过配置，来通过三种方式之一在安全端口上学习MAC地址，这三种方式是：手动配置、动态学习和动态学习-sticky（粘滞）。
- 如果连接到端口的设备 MAC 地址与安全地址列表不一致，则会触发端口违规。在默认情况下，这个端口就会进入error-disabled状态。当一个端口进入了error-disabled状态，那么这个端口就既不会发送、也不会接收流量。
- 通过禁用DTP协商、禁用未使用的端口、按需手动设置中继、使用VLAN 1之外的VLAN来充当本征VLAN这些措施，可以缓解VLAN跳跃攻击。

在这个模块中我学到了什么？（续）

- DHCP耗竭攻击的目的是对连接的客户端发起拒绝服务攻击（DoS）。通过在可信端口上使用 DHCP 监听可缓解 DHCP 欺骗攻击。
- 它的作用是判断DHCP消息是否来自于管理员配置的可信或不可信源。接下来，它就会对DHCP消息执行过滤，并且对来自不可信源的DHCP流量执行限速。
- 动态ARP检查（DAI）需要启用DHCP监听，这个特性会验证ARP流量，从而防止ARP攻击。
- 实施动态 ARP 检查 (Dynamic Arp Inspection) 来缓解ARP欺骗和ARP毒化。
- 为了缓解生成树（STP）操纵攻击，应该使用PortFast和BPDU（桥协议数据单元）防护特性。

New Terms and Commands

- interface range
- switchport port-security
- switchport port-security interface
- switchport port-security maximum
- switchport port-security mac-address
- switchport port-security mac-address sticky
- switchport port-security aging time #
- switchport port-security aging type
- switchport port-security violation
- show switchport port-security
- switchport mode access|trunk
- switchport nonegotiate
- switchport trunk native vlan #
- ip dhcp snooping
- ip dhcp snooping vlan #
- ip dhcp snooping limit rate
- show ip dhcp snooping
- ip arp inspection vlan #
- ip dhcp snooping trust
- ip arp inspection trust
- ip arp inspection validate
- spanning-tree portfast {default}
- spanning-tree bpduguard enable
- spanning-tree porfast bpduguard default


CISCO