实验 - 配置交换机安全功能

拓扑

地址分配表

设备	接口	IP 地址	子网掩码	默认网关
R1	G0/1	172.16.99.1	255.255.255.0	不适用
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

目标

第 1 部分：设置拓扑并初始化设备

第 2 部分：配置基本设备设置并验证连接

第 3 部分：配置并验证 S1 上的 SSH 访问

- 配置 SSH 访问。
- 修改 SSH 参数。
- 验证 SSH 配置。

第 4 部分：配置并验证 S1 上的安全功能

- 配置并验证常规安全功能。
- 配置并检验端口安全功能。

背景/场景

在 PC 和服务器上锁定访问并安装强安全功能十分常见。此外，为您的网络基础设施设备（例如，交换机和路由器）配置安全功能也十分重要。

在本实验中，您将遵循一些在 LAN 交换机上配置安全功能的最佳实践。您将仅允许 SSH 和安全 HTTPS 会话。您还将配置并验证端口安全，以锁定具有交换机无法识别的 MAC 地址的任何设备。

注：CCNA 上机实验所使用的路由器为采用思科 IOS 15.2(4)M3 版本软件（universalk9 映像）的思科 1941 集成服务路由器 (ISR)。使用的交换机为采用思科 IOS 15.0(2) 版本软件（lanbasek9 映像）的思科 Catalyst 2960。也可使用其他路由器、交换机以及其他思科 IOS 版本。根据型号和思科 IOS 版本，可用命令及其所产生的输出可能不同于本实验中的显示。请参考本实验末尾的“路由器接口汇总表”以了解正确的接口标识符。

注：请确保路由器和交换机的启动配置已经清除。如果您不确定，请联系您的教师或参考上一个实验，了解初始化交换机并重新加载设备的过程。

所需资源

- 1 台路由器（采用思科 IOS 15.2(4)M3 版通用映像的思科 1941 或同类路由器）
- 1 台交换机（采用思科 IOS 15.0(2) lanbasek9 版映像的思科 2960 或同类交换机）
- 1 台 PC（采用 Windows 7、Vista 或 XP 且支持终端模拟程序，比如 Tera Term）
- 1 条控制台电缆，用于通过控制台端口配置思科 IOS 设备
- 2 条以太网电缆，如拓扑所示

第 1 部分：设置拓扑并初始化设备

在第 1 部分中，您将设置网络拓扑并在必要时清除任何配置。

步骤 1： 建立如拓扑图所示的网络。

步骤 2： 初始化并重新加载路由器和交换机。

如果配置文件先前已保存在路由器或交换机上，请将这些设备初始化回其默认配置，然后重新加载。

第 2 部分：配置基本设备设置并验证连接

在第 2 部分中，您将在路由器、交换机和 PC 上配置基本设置。有关设备名称和地址信息，请参阅本实验开头的拓扑和地址分配表。

步骤 1： 配置 PC-A 的 IP 地址。

有关 IP 地址信息，请参阅地址分配表。

步骤 2： 在 R1 上配置基本设置。

a. 登录 R1 控制台，然后进入全局配置模式。

b. 复制以下基本配置并将其粘贴到 R1 上的运行配置中。

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited.#
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
interface g0/1
 ip address 172.16.99.1 255.255.255.0
 no shutdown
end
```

c. 将运行配置保存到启动配置中。

步骤 3： 在 S1 上配置基本设置。

a 登录 S1 控制台，然后进入全局配置模式。

b 复制以下基本配置并将其粘贴到 S1 上的运行配置中。

```
no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited.#
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

c 在交换机上创建 VLAN 99 并将其命名为 **Management**。

```
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

d 如地址分配表所示配置 VLAN 99 管理接口 IP 地址，然后启用该接口。

```
S1(config)# interface vlan 99
S1(config-if)# ip address 172.16.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1#
```

e 在 S1 上发出 **show vlan** 命令。VLAN 99 的状态是什么？ _____

f 在 S1 上发出 **show ip interface brief** 命令。管理接口 VLAN 99 的状态和协议是什么？

_____

为什么即使您为接口 VLAN 99 发出了 **no shutdown** 命令，协议仍关闭？

_____

g 将端口 F0/5 和 F0/6 分配到交换机上的 VLAN 99。

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```

h 将运行配置保存到启动配置中。

i 在 S1 上发出 **show ip interface brief** 命令。为接口 VLAN 99 显示的状态和协议是什么？

_____

注：端口状态融合时可能会出现延迟。

步骤 4： 验证设备之间的连接。

a 从 PC-A，ping R1 上的默认网关地址。您的 ping 操作是否成功？_____

b 从 PC-A，ping S1 的管理地址。您的 ping 操作是否成功？_____

c 从 S1，ping R1 上的默认网关地址。您的 ping 操作是否成功？_____

d 从 PC-A，打开一个 Web 浏览器并转至 http://172.16.99.11。如果系统提示您输入用户名和密码，则将用户名留空并使用 **class** 作为密码。如果系统提示您是否进行安全连接，请回答 **No**。您是否能够访问 S1 上的 Web 接口？_____

e 关闭浏览器。

注：默认情况下，启用思科 2960 交换机上的非安全 Web 接口（HTTP 服务器）。常用安全措施是禁用此服务，如第 4 部分中所述。

第 3 部分：配置并验证 S1 上的 SSH 访问

步骤 1： 在 S1 上配置 SSH 访问。

a 在 S1 上启用 SSH。从全局配置模式，创建 **CCNA-Lab.com** 的域名。

```
S1(config)# ip domain-name CCNA-Lab.com
```

b 创建一个本地用户数据库条目，在通过 SSH 连接交换机时使用。用户应具有管理级别访问权限。

注：此处使用的密码非强密码。其仅用于实验目的。

```
S1(config)# username admin privilege 15 secret sshadmin
```

c 配置 vty 线路的传输输入以仅允许 SSH 连接，使用本地数据库进行身份验证。

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

d 使用系数 1024 位，生成 RSA 加密密钥。

```
S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

S1(config)#
S1(config)# end
```

e 验证 SSH 配置。

```
S1# show ip ssh
```

交换机使用的 SSH 的版本是多少？_____

SSH 允许进行几次身份验证尝试？_____

SSH 的默认超时设置是多少？_____

步骤 2： 修改 S1 上的 SSH 配置。

修改默认 SSH 配置。

```
S1# config t
S1(config)# ip ssh time-out 75
S1(config)# ip ssh authentication-retries 2
```

SSH 允许进行几次身份验证尝试？_____

SSH 的超时设置是多少？_____ 验证 S1 上的 SSH 配置。

a 在 PC-A 上使用 SSH 客户端软件（如，Tera Term），打开与 S1 的 SSH 连接。如果您在 SSH 客户端上收到有关主机密钥的消息，请接受。使用用户名 **admin** 和密码 **sshadmin** 登录。

连接是否成功？_____

S1 上显示什么提示？为什么？

_____

_____

_____

b 键入 **exit** 以在 S1 上结束 SSH 会话。

第 4 部分：配置并验证 S1 上的安全功能

在第 4 部分中，您将关闭未使用的端口，关闭交换机上运行的某些服务，并基于 MAC 地址配置端口安全。交换机可能遭受 MAC 地址表溢出攻击、MAC 欺骗攻击和与交换机端口的未授权连接。您将配置端口安全以限制可在交换机端口上获取的 MAC 地址数量，并在超出该数量后禁用端口。

步骤 1： 在 S1 上配置常规安全功能。

a 将 S1 上的每日提示信息 (MOTD) 横幅更改为“严禁未经授权访问。违者将受到法律最大限度的追究。”

b 在 S1 上发出 **show ip interface brief** 命令。哪些物理端口在运行？

_____

c 关闭交换机上所有未使用的物理端口。使用 **interface range** 命令。

```
S1(config)# interface range f0/1 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
```

```
S1(config-if-range)# end
S1#
```

d 在 S1 上发出 **show ip interface brief** 命令。端口 F0/1 至 F0/4 的状态是什么？

_____

e 发出 **show ip http server status** 命令。

HTTP 服务器状态是什么？_____

它使用哪个服务器端口？_____

HTTP 安全服务器状态是什么？_____

它使用哪个安全服务器端口？_____

f HTTP 会话以纯文本形式发送所有数据。您将禁用 S1 上运行的 HTTP 服务。

```
S1(config)# no ip http server
```

g 从 PC-A，打开一个 Web 浏览器并转至 http://172.16.99.11。您获得什么样的结果？

_____

h 从 PC-A，打开一个 Web 浏览器并转至 https://172.16.99.11。接受证书。不使用用户名，使用密码 **class** 登录。您获得什么样的结果？

_____

i 关闭 Web 浏览器。

步骤 2： 在 S1 上配置并验证端口安全。

a 记录 R1 G0/1 MAC 地址。从 R1 CLI，使用 **show interface g0/1** 命令并记录接口的 MAC 地址。

```
R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia
3047.0da3.1821)
```

R1 G0/1 接口的 MAC 地址是什么？

_____

b 从 S1 CLI，通过特权执行模式发出 **show mac address-table** 命令。找到端口 F0/5 和 F0/6 的动态条目。将它们记录在下面。

F0/5 MAC 地址：_____

F0/6 MAC 地址：_____

c 配置基本端口安全。

注：通常，将在交换机上的所有访问端口上执行此过程。此处显示 F0/5 作为示例。

1) 从 S1 CLI，进入连接到 R1 的端口的接口配置模式。

```
S1(config)# interface f0/5
```

2) 关闭端口。

```
S1(config-if)# shutdown
```

3) 在 F0/5 上启用端口安全。

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

注：输入 **switchport port-security** 命令可将最大 MAC 地址数设置为 1，将违规操作对策设置为关闭。**switchport port-security maximum** 和 **switchport port-security violation** 命令可用于更改默认行为。

4) 为步骤 2a 中记录的 R1 G0/1 接口的 MAC 地址，配置静态条目。

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

（xxxx.xxxx.xxxx 是路由器 G0/1 接口的实际 MAC 地址）

注：或者，您可以使用 **switchport port-security mac-address sticky** 命令将在端口上动态获取的所有安全 MAC 地址（最高为设置的最大值）添加到交换机运行配置中。

5) 启用交换机端口。

```
S1(config-if)# no shutdown
S1(config-if)# end
```

d 通过发出 **show port-security interface** 命令验证 S1 F0/5 上的端口安全。

```
S1# show port-security interface f0/5
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   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

F0/5 的端口状态是什么？

_____

e 从 R1 命令提示符，ping PC-A 以验证连接。

```
R1# ping 172.16.99.3
```

f 此时，您将通过更改路由器接口上的 MAC 地址违反安全性。进入 G0/1 的接口配置模式，然后将其关闭。

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```

g 为接口配置新的 MAC 地址，使用 **aaaa.bbbb.cccc** 作为地址。

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

h 若可能，在 S1 上的控制台连接保持打开的同时执行接下来两个步骤。最终，您将看到 S1 的控制台连接上显示指示违反安全性的消息。在 R1 上启用 G0/1 接口。

```
R1(config-if)# no shutdown
```

i 从 R1 特权执行模式下，ping PC-A。ping 是否成功？原因是什么？

_____

j 在交换机上，使用以下命令验证端口安全。

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
      Fa0/5            1           1                1         Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/5
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   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : aaaa.bbbb.cccc:99
Security Violation Count   : 1

S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<省略部分输出>

S1# show port-security address
                Secure Mac Address Table
------------------------------------------------------------------------
Vlan     Mac Address       Type                  Ports      Remaining Age
                                                             (mins)
----     -----------       ----                  -----   -------------
  99     30f7.0da3.1821    SecureConfigured      Fa0/5         -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

k 在路由器上，关闭 G0/1 接口，从路由器上删除硬编码的 MAC 地址，然后重新启用 G0/1 接口。

```
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end
```

l 从 R1，在 172.16.99.3 上再次 ping PC-A。ping 是否成功？ _____

m 在交换机上发出 **show interface f0/5** 命令以确定 ping 失败的原因。记录您的发现。

_____

n 清除 S1 F0/5 错误禁用状态。

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

注：端口状态融合时可能会出现延迟。

o 在 S1 上发出 **show interface f0/5** 命令以验证 F0/5 不再处于错误禁用模式。

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

p 从 R1 命令提示符处，再次 ping PC-A。该 ping 操作应该能够成功。

思考

1. 为什么要在交换机上启用端口安全？

_____

2. 为什么要禁用交换机上未使用的端口？

_____

路由器接口汇总表

路由器接口汇总				
路由器型号	**以太网接口 1**	**以太网接口 2**	**串行接口 1**	**串行接口 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

注：若要了解如何配置路由器，请查看接口来确定路由器类型以及路由器拥有的接口数量。我们无法为每类路由器列出所有的配置组合。下表列出了设备中以太网和串行接口组合的标识符。此表中未包含任何其他类型的接口，但实际的路由器可能会含有其他接口。例如 ISDN BRI 接口。括号中的字符串是约定缩写，可在思科 IOS 命令中用来代表接口。