实验 – 保护网络设备

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	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	网卡	192.168.1.3	255.255.255.0	192.168.1.1

目标

第 1 部分：配置设备的基本设置

第 2 部分：在路由器上配置基本安全措施

第 3 部分：在交换机上配置基本安全措施

背景/场景

推荐所有网络设备配置至少最少量的最佳实践安全命令。这包括终端用户设备、服务器和网络设备（例如路由器和交换机）。

在本实验中，您将在拓扑中配置网络设备，以便接受用于远程管理的 SSH 会话。还将使用 IOS CLI 配置常用、基本最佳实践安全措施。然后测试安全措施，检验它们是否合理实施、正常工作。

注意：CCNA 动手实验所用的路由器是采用 Cisco IOS 15.2(4)M3 版（universalk9 映像）的 Cisco 1941 集成多业务路由器 (ISR)。所用的交换机是采用 Cisco IOS Release 15.0(2)（lanbasek9 映像）的 Cisco Catalyst 2960 系列。也可使用其他路由器、交换机以及其他 Cisco IOS 版本。根据型号以及 Cisco IOS 版本的不同，可用命令和产生的输出可能与实验显示的不一样。请参考本实验末尾的“路由器接口摘要表”以了解正确的接口标识符。

注意：确保路由器和交换机的启动配置已经清除。如果不确定，请联系教师。

所需资源

- 1 台路由器（支持 Cisco IOS 软件 15.2(4)M3 版通用映像的 Cisco 1941 或同类路由器）
- 1 台交换机（支持 Cisco IOS 15.0(2) lanbasek9 版映像的 Cisco 2960 或同类交换机）
- 1 台 PC（采用 Windows 7 或 8 且支持终端仿真程序，比如 Tera Term）
- 用于通过控制台端口配置 Cisco IOS 设备的控制台电缆
- 如拓扑图所示的以太网电缆

第 1 部分：配置设备的基本设置

在第 1 部分中，您将建立网络拓扑并配置基本设置，例如接口 IP 地址、设备访问和设备密码。

第 1 步：建立如拓扑图所示的网络。

按照拓扑图所示连接设备和电缆（如有必要）。

第 2 步：初始化并重新加载路由器和交换机。

第 3 步：配置路由器和交换机

a. 通过控制台连接到设备，并启用特权 EXEC 模式。

b. 根据地址分配表指定设备名称。

c. 要防止路由器尝试将错误输入的命令视为主机名，则禁用 DNS 查找。

d. 指定 **class** 作为特权 EXEC 加密密码。

e. 指定 **cisco** 作为控制台密码并启用登录。

f. 指定 **cisco** 作为 VTY 密码并启用登录。

g. 创建一个向访问设备者发出警告的标语：未经授权，禁止访问。

h. 使用地址分配表中包含的信息配置并激活路由器上的 G0/1 接口。

i. 使用地址分配表中包含的 IP 地址信息配置交换机上的默认 SVI。

j. 将运行配置保存到启动配置文件中。

第 2 部分：在路由器上配置基本安全措施

第 1 步：加密明文密码。

```
R1(config)# service password-encryption
```

第 2 步：加强密码。

管理员应确保密码符合强密码标准指南。这些指南规定在密码中组合使用字母、数字和特殊字符，并设置最小长度。

注意：最佳实践指南要求在生产环境中使用强密码（例如这里所示)。但是，为便于进行实验，该课程的另一个实验使用 cisco 和 class 密码。

a. 更改特权 EXEC 加密密码以符合指南要求。

```
R1(config)# enable secret Enablep@55
```

b. 所有密码要求至少使用 10 个字符。

```
R1(config)# security passwords min-length 10
```

第 3 步：启用 SSH 连接。

a. 指定域名为 **CCNA-lab.com**。

```
R1(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。密码应符合强密码标准，并且用户应具有用户 EXEC 访问权限。如果命令中未指定特权级别，用户将可默认进行用户 EXEC（15 级）访问。

```
R1(config)# username SSHadmin privilege 15 secret Admin1p@55
```

c. 配置 VTY 线路的 transport input，以便接受 SSH 连接，但不允许 Telnet 连接。

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

d. VTY 线路应使用本地用户数据库进行身份验证。

```
R1(config-line)# login local
R1(config-line)# exit
```

e. 使用系数 1024 位，生成 RSA 加密密钥。

```
R1(config)# crypto key generate rsa modulus 1024
```

第 4 步：保护控制台线路和 VTY 线路。

a. 您可设置路由器，使其注销空闲时间达到指定时间的线路。如果网络工程师登录到一台网络设备上，然后突然有事离开，此命令便会在指定时间后自动将该用户注销。如果您在 5 分钟内无任何操作，以下命令会使线路注销。

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

b. 以下命令用于防止暴力型登录尝试。当有人在 120 秒内两次登录失败，路由器将禁止其在接下来的 30 秒内登录。为方便实验，此处我们将该值特意设得较低。

```
R1(config)# login block-for 30 attempts 2 within 120
```

以上命令中的 **2 within 120** 是什么意思？

以上命令中的 **block-for 30** 是什么意思？

第 5 步：检验所有未使用的端口是否禁用。

路由器端口默认禁用，但其总能谨慎检验所有未使用端口是否按规定处于关闭状态。可通过发出 **show ip interface brief** 命令快速检查。所有未按规定关闭的未使用端口应使用接口配置模式下的 **shutdown** 命令将其禁用。

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                unassigned      YES NVRAM  administratively down down
R1#
```

第 6 步: 检验您的安全措施是否已经正确实施。

a. 使用 Tera Term 通过 telnet 连接到 R1。

R1 接受 Telnet 连接吗? 说明原因。

b. 使用 Tera Term 通过 SSH 访问 R1。

R1 接受 SSH 连接吗?

c. 刻意错误键入用户和密码信息，在尝试两次后看是否阻止登录访问。

第二次登录失败后会发生什么?

d. 从您的路由器控制台会话，发出 **show login** 命令以检查登录状态。在下面的例子中，在 30 秒登录阻止时间内发出 **show login** 命令并显示路由器处于静默模式。14 秒内路由器不会接受任何登录尝试。

```
R1# show login
     A default login delay of 1 second is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 30 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 14 seconds.
     Denying logins from all sources.
R1#
```

e. 30 秒期限过后，SSH 再次连接到 R1 并使用用户名 **SSHadmin** 和密码 **Admin1p@55** 登录。

成功登录后显示什么?

f. 进入特权 EXEC 模式，并使用 **Enablep@55** 作为密码。

如果您错误键入该密码，在 120 秒内两次尝试登录失败后会与 SSH 会话断开连接吗？说明原因。

g. 在特权 EXEC 提示符处发出 **show running-config** 命令，查看您应用的安全设置。

第 3 部分: 在交换机上配置基本安全措施

第 1 步: 加密明文密码。

```
S1(config)# service password-encryption
```

第 2 步: 加强交换机密码。

更改特权 EXEC 加密密码以符合强密码指南要求。

```
S1(config)# enable secret Enablep@55
```

注意：安全 **password min-length** 命令不适用于 2960 交换机。

第 3 步: 启用 SSH 连接。

a. 指定域名为 **CCNA-lab.com**。

```
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。密码应符合强密码标准，并且用户应具有用户 EXEC 访问权限。如果命令中特权等级不确定，用户将可默认进行用户 EXEC（1 级）访问。

```
S1(config)# username SSHadmin privilege 1 secret Admin1p@55
```

c. 配置 VTY 线路的 transport input，以便允许 SSH 连接，但不允许 Telnet 连接。

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

d. VTY 线路应使用本地用户数据库进行身份验证。

```
S1(config-line)# login local
S1(config-line)# exit
```

e. 使用系数 1024 位，生成 RSA 加密密钥。

```
S1(config)# crypto key generate rsa modulus 1024
```

第 4 步: 保护控制台线路和 VTY 线路。

a. 配置交换机以注销已持续空闲 10 分钟的线路。

```
S1(config)# line console 0
S1(config-line)# exec-timeout 10 0
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

b. 为防止暴力型登录尝试，配置交换机以便在 120 内两次登录访问失败时阻止登录访问 30 秒。为方便实验，此处我们将该值特意设得较低。

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

第 5 步: 检验所有未使用的端口是否禁用。

默认情况下，交换机接口被启用。关闭交换机上所有未使用的端口。

a. 使用 **show ip interface brief** 命令检验交换机端口状态。

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
```

```
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

b. 使用 **interface-range** 命令逐一关闭多个接口。

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

c. 检验所有非活动接口是否已经按规定关闭。

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

第 6 步: 检验您的安全措施是否已经正确实施。

a. 检验交换机上的 Telnet 是否被禁用。

b. 通过 SSH 连接到交换机，并刻意错误键入用户和密码信息，看是否阻止登录访问。

c. 30 秒期限过后，SSH 再次连接到 R1 并使用用户名 **SSHadmin** 和密码 **Admin1p@55** 登录。

您成功登录后出现标语了吗？

d. 使用 **Enablep@55** 作为密码进入特权 EXEC 模式。

e. 在特权 EXEC 提示符处发出 **show running-config** 命令，查看您应用的安全设置。

思考

1. 在第 1 部分中，为您的基本配置中的控制台和 VTY 线路输入 **password cisco** 命令。在应用最佳实践安全措施后什么时候使用该密码？

2. 预配置的密码少于 10 个字符会受到 **security passwords min-length 10** 命令影响吗？

路由器接口摘要表

路由器接口摘要				
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 (S0/0/0)	Serial 0/1/1 (S0/0/1)
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)

注意：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 Cisco IOS 命令中用来代表接口。