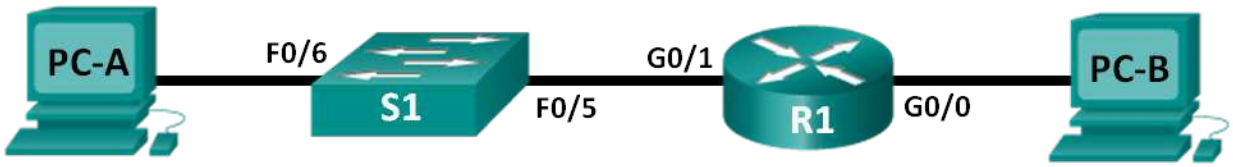
实验 - 配置并检验 VTY 限制

拓扑



地址分配表

设备	接口	IP 地址	子网掩码	默认网关
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

目标

第 1 部分：配置基本设备设置

第 2 部分：在 R1 上配置并应用访问控制列表

第 3 部分：使用 Telnet 检验访问控制列表

第 4 部分：提示问题 - 在 S1 上配置并应用访问控制列表

背景/场景

一种比较好的做法是限制对路由器管理接口的访问，例如控制台和 vty 线路。访问控制列表 (ACL) 可用于允许对特定 IP 地址的访问，从而确保只有管理员 PC 有权限通过 Telnet 或 SSH 连接到路由器。

注意：在思科设备输出中，ACL 简写为 access-list。

在本实验中，您将创建并应用一个命名标准 ACL，以限制对路由器 vty 线路的远程访问。

在创建并应用 ACL 后，您将使用 Telnet 访问来自不同 IP 地址的路由器，从而测试并检验该 ACL。

本实验将提供创建并应用 ACL 所需的命令。

注意：CCNA 动手实验所用的路由器是采用 Cisco IOS Release 15.2(4)M3（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 Cisco IOS 版本。根据型号以及 Cisco IOS 版本不同，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：确保所使用的路由器和交换机的启动配置都已擦除。如果不确定，请联系教师。

所需资源

- 1 台路由器（支持 Cisco IOS 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）
- 2 台 PC（采用 Windows 7、Vista 或 XP 且支持终端模拟程序，比如 Tera Term）
- 用于通过控制台电缆配置 Cisco IOS 设备的控制台端口
- 如拓扑图所示的以太网电缆

注意：Cisco 1941 路由器上的 Gigabit Ethernet 接口是自动感应的，而且路由器与 PC-B 之间可能使用以太网直通电缆。如果使用其他型号的思科路由器，需要使用一个以太网交叉电缆。

第 1 部分：配置设备的基本设置

在第 1 部分，您将建立网络拓扑并配置接口 IP 地址、设备访问和路由器密码。

第 1 步：建立如拓扑图所示的网络。

第 2 步：根据地址分配表配置 PC-A 和 PC-B 的网络设置。

第 3 步：初始化并重新加载路由器和交换机。

a. 禁用 DNS 查找。

b. 根据拓扑图配置设备名称。

c. 指定 **class** 作为特权 EXEC 加密密码。

d. 指定 **cisco** 作为控制台密码，激活 logging synchronous，并启用登录。

e. 指定 **cisco** 作为 vty 密码，激活 logging synchronous，并启用登录。

f. 加密明文密码。

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. 根据地址分配表配置接口的 IP 地址。

i. 配置交换机的默认网关。

j. 将运行配置保存到启动配置文件中。

第 2 部分：在 R1 上配置并应用访问控制列表

在第 2 部分，您将配置一个命名标准 ACL 并将其应用到路由器虚拟终端线路，以限制对路由器的远程访问。

第 1 步：配置并应用标准命名 ACL。

a. 通过控制台连接到路由器 R1 并启用特权 EXEC 模式。

b. 在全局配置模式下，使用一个空格和一个问号查看 **ip access-list** 的命令选项。

```
R1(config)# ip access-list ?
  extended    Extended Access List
  helper      Access List acts on helper-address
  log-update  Control access list log updates
```

```
  logging     Control access list logging
  resequence  Resequence Access List
  standard    Standard Access List
```

c. 使用一个空格和一个问号查看 **ip access-list standard** 的命令选项。

```
R1(config)# ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
```

d. 在 **ip access-list standard** 命令末尾添加 **ADMIN-MGT**，然后按 Enter。您现在处于标准命名访问列表的配置模式 (config-std-nacl)。

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)#
```

e. 输入您的 ACL permit 或 deny 访问控制条目 (ACE)，也称为 ACL 语句，一条语句占一行。切记，ACL 的末尾有一条隐式 **deny any**，能够有效拒绝所有流量。输入问号查看您的命令选项。

```
R1(config-std-nacl)# ?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
```

f. 为 IP 地址为 192.168.1.3 的管理员 PC-A 创建一个 permit ACE，然后额外创建一个 permit ACE 来允许 192.168.1.4 到 192.168.1.7 之间的其他保留管理性 IP 地址。注意，通过使用 **host** 关键字，第一个 permit ACE 表示单个主机，而本应该使用 ACE **permit 192.168.1.3 0.0.0.0**。通过使用 0.0.0.3 通配符，第二个 permit ACE 允许 192.168.1.4 到 192.168.1.7 之间的主机，该通配符是 255.255.255.252 子网掩码的反码。

```
R1(config-std-nacl)# permit host 192.168.1.3
R1(config-std-nacl)# permit 192.168.1.4 0.0.0.3
R1(config-std-nacl)# exit
```

由于 ACL 的末尾有一条隐式 **deny any** ACE，因此无需输入 deny ACE。

g. 创建好命名 ACL 后，请将其应用到 vty 线路。

```
R1(config)# line vty 0 4
R1(config-line)# access-class ADMIN-MGT in
R1(config-line)# exit
```

第 3 部分：使用 Telnet 检验访问控制列表

在第 3 部分，您将使用 Telnet 访问路由器，以检验该命令 ACL 是否正常运行。

注意：SSH 比 Telnet 更加安全；但是，SSH 要求将网络设备配置为接受 SSH 连接。为了方便起见，本实验使用 Telnet。

a. 在 PC-A 上打开命令提示符，发出 **ping** 命令以检验能否与路由器通信。

```
C:\Users\user1> ping 192.168.1.1
```

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\Users\user1>
```

b. 使用 PC-A 的命令提示符，启动 Telnet 客户端程序，以通过 Telnet 连接到路由器。输入登录密码，然后输入使能密码。您应该能够成功登录、看到标语消息并收到 R1 路由器的命令提示符。

```
C:\Users\user1> telnet 192.168.1.1

Unauthorized access is prohibited!

User Access Verification

Password:
R1>enable
Password:
R1#
```

Telnet 连接是否成功？

c. 在命令提示符后键入 **exit** 并按 Enter 退出 Telnet 会话。

d. 更改 IP 地址，测试该命名 ACL 是否会阻止非允许的 IP 地址。将 PC-A 的 IPv4 地址更改为 192.168.1.100。

e. 再次尝试通过 Telnet 连接至 R1 (192.168.1.1)。Telnet 会话是否成功？

收到什么消息？

f. 更改 PC-A 的 IP 地址，测试该命名 ACL 是否允许 IP 地址在 192.168.1.4 到 192.168.1.7 范围内的主机通过 Telnet 连接到路由器。更改 PC-A 的 IP 地址后，打开 Windows 命令提示符窗口并尝试通过 Telnet 连接到路由器 R1。

Telnet 会话是否成功？

g. 在 R1 的特权 EXEC 模式下，输入 **show ip access-lists** 命令并按 Enter。从命令输出中，注意 Cisco IOS 如何以增量为 10 自动分配 ACL ACE 的行号，以及如何显示每条 permit ACE 成功匹配的次数（在括号中）。

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
    10 permit 192.168.1.3 (2 matches)
    20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
```

由于已经和路由器成功建立了两个 Telnet 连接，并且每个 Telnet 会话都是从匹配其中一个 permit ACE 的 IP 地址发起的，因此每个 permit ACE 都有多次匹配。

每个 IP 地址只发起了一个连接，为什么您认为每个 permit ACE 有两次匹配？

如何确定 Telnet 协议在 Telnet 连接过程中导致两次匹配的时间？

h. 在 R1 上进入全局配置模式。

i. 进入 ADMIN-MGT 命名访问列表的 access-list 配置模式，然后在访问列表的末尾添加 **deny any** ACE。

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
```

注意：由于所有 ACL 的末尾都有隐式 **deny any** ACE，因此不需要添加显式 **deny any** ACE，但是如果网络管理员要记录或想知道 **deny any** access-list ACE 的匹配次数，此操作还是有用的。

j. 尝试通过 Telnet 从 PC-B 连接至 R1。这会在 ADMIN-MGT 命名访问列表中创建 **deny any** ACE 的一个匹配。

k. 在特权 EXEC 模式下，键入 **show ip access-lists** 命令并按 Enter。现在应会看到 **deny any** ACE 的多个匹配。

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
    10 permit 192.168.1.3 (2 matches)
    20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
    30 deny any (3 matches)
```

失败的 Telnet 连接会比成功的 Telnet 连接生成更多显式 deny ACE 的匹配。这是为什么？

第 4 部分：提示问题 - 在 S1 上配置并应用访问控制列表

第 1 步：为 S1 上的 vty 线路配置并应用标准命名 ACL。

a. 请勿参考 R1 的配置命令，尝试在 S1 上配置 ACL，仅允许 PC-A 的 IP 地址。

b. 将 ACL 应用到 S1 的 vty 线路。切记，交换机比路由器拥有更多 vty 线路。

第 2 步: 测试 S1 上的 vty ACL。

从每个 PC 尝试 Telnet 连接，以检验 vty ACL 是否正常运行。您应该能够从 PC-A 到 S1 建立 Telnet 连接，但是不能从 PC-B 建立连接。

思考

1. 从远程 vty 访问可以看出，ACL 可以作为强大的内容过滤器，不仅仅是应用于入站和出站网络接口。ACL 还能应用在哪些方面？

2. 应用到 vty 远程管理接口的 ACL 是否能够提高 Telnet 连接的安全性？这是否让 Telnet 成为更加可行的远程访问管理工具？

3. 为什么需要对 vty 线路应用 ACL，而不对特定接口应用？

路由器接口摘要表

路由器接口摘要				
路由器型号	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #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。