

实验 - 配置和验证 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	不适用
	G0/1	192.168.1.1	255.255.255.0	不适用
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 上配置和应用访问控制列表

第 3 部分：使用 Telnet 验证访问控制列表

第 4 部分：练习 - 在 S1 上配置和应用访问控制列表

背景/场景

限制访问路由器管理接口（如控制台和 vty 线路）是一个好做法。访问控制列表 (ACL) 可用于允许访问特定 IP 地址，确保只有管理员 PC 有权使用 Telnet 或 SSH 登录到路由器。

注：在思科设备输出中，ACL 缩写为 access-list。

在本实验中，您将创建并应用一个命名的标准 ACL，以限制远程接入到路由器 vty 线路。

在创建和应用 ACL 之后，将使用 Telnet 从不同的 IP 地址访问路由器，对 ACL 进行测试和验证。

本实验将提供创建和应用 ACL 所必需的命令。

注：CCNA 动手实验所用的路由器是采用思科 IOS 15.2(4)M3 版（universalk9 映像）的思科 1941 集成多业务路由器 (ISR)。所用的交换机是采用思科 IOS 15.0(2) 版（lanbasek9 映像）的思科 Catalyst 2960 系列。也可使用其他路由器、交换机以及其他思科 IOS 版本。根据型号以及思科 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樣。请参阅本实验末尾的“路由器接口汇总表”了解正确的接口标识符。

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

注：思科 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。如果使用其他思科路由器型号，需要使用一个以太网交叉电缆。

第 1 部分：配置基本设备设置

在第 1 部分，您将设置网络拓扑，在路由器上配置接口 IP 地址、设备访问权限和密码。

步骤 1： 建立如拓扑图所示的网络。

步骤 2： 根据地址分配表配置 PC-A 和 PC-B 网络设置。

步骤 3： 初始化并重新加载路由器和交换机。

- 通过控制台连接到路由器，然后进入全局配置模式。
- 复制以下基本配置并将其粘贴到路由器上的运行配置中。

```
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
```

- 在接口上配置地址分配表中所列的 IP 地址。
- 将运行配置保存到启动配置文件中。
- 通过控制台连接到交换机，然后进入全局配置模式。
- 复制以下基本配置并将其粘贴到交换机上的运行配置中。

```
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
```

- g. 在 VLAN1 接口上配置地址分配表中所列的 IP 地址。
- h. 配置交换机的默认网关。
- i. 将运行配置保存到启动配置文件中。

第 2 部分：在 R1 上配置和应用访问控制列表

在第 2 部分，您将配置一个命名的标准 ACL，将它应用到路由器的虚拟终端线路，以限制对路由器的远程访问。

步骤 1：配置和应用命名的标准 ACL。

- a. 使用控制台登录到路由器 R1 并启用特权执行模式。
- b. 在全局配置模式下，通过使用空格和问号，查看 **ip access-list** 下的命令选项。

```
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. 通过使用空格和问号，查看 **ip access-list standard** 下的命令选项。

```
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. 将 **ADMIN-MGT** 添加到 **ip access-list standard** 命令的结尾，然后按 Enter。您现在处于命名的标准访问列表配置模式 (config-std-nacl)。

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

- e. 输入您的 ACL 允许或拒绝访问控制条目 (ACE)，也称为 ACE 语句，一次输入一行。记住，在 ACL 的末尾有一个隐式的 **deny any**，将有效拒绝所有流量。输入问号以查看您的命令选项。

```
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 192.168.1.3 的管理员 PC-A 创建一个 permit ACE，再创建另一个 permit ACE，以允许其他预留的管理 IP 地址（从 192.168.1.4 到 192.168.1.7）。注意，第一个 permit ACE 如何通过使用 **host** 关键字表示单个主机。可能已经改为使用 ACE **permit 192.168.1.3 0.0.0.0**。第二个 permit ACE 通过使用 0.0.0.3 通配符（也就是与 255.255.255.252 子网掩码相反）允许主机 192.168.1.4 至 192.168.1.7。

```
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
```

您不需要输入 deny ACE，因为在 ACL 末尾有一个隐式的 **deny any** ACE。

- g 现在已创建命名 ACL，将它应用到 vty 线路。

```
R1(config)# line vty 0 15
R1(config-line)# access-class ADMIN-MGT in
R1(config-line)# exit
```

第 3 部分：使用 Telnet 验证访问控制列表

在第 3 部分，您将使用 Telnet 访问路由器，验证命名的 ACL 是否正常允许。

注：SSH 比 Telnet 更安全，但是，SSH 需要配置网络设备以接受 SSH 连接。为了方便起见，在本实验中使用 Telnet。

- a 在 PC-A 上打开命令提示符，通过发出 **ping** 命令，验证您是否可以与路由器通信。

```
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 上的命令提示符，启用 Telnet 客户端程序，以远程登录到路由器。输入登录名，然后启用密码。您应该已经成功登录，看到横幅消息，并且收到 R1 路由器命令提示符。

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

Unauthorized access is prohibited!

User Access Verification
```

Password:

R1>enable

密码:

R1#

Telnet 是否连接成功? _____

- c 在命令提示符处键入 **exit**，按 Enter 退出 Telnet 会话。
- d 更改您的 IP 地址，测试命名的 ACL 是否阻止了不允许使用的 IP 地址。在 PC-A 上将 IPv4 地址更改为 192.168.1.100。
- e 再次尝试远程登录到 192.168.1.1 的 R1。Telnet 会话是否成功?

收到了什么消息? _____

- f 更改 PC-A 上的 IP 地址，测试命名的 ACL 是否允许 IP 地址介于 192.168.1.4 到 192.168.1.7 范围之间的主机远程登录到路由器。在 PC-A 上更改 IP 地址，打开 Windows 命令提示符，然后尝试远程登录到路由器 R1。

Telnet 会话是否成功?

- g 从 R1 上的特权执行模式，键入 **show ip access-lists** 命令，然后按 Enter。在命令提示符处，注意思科 IOS 如何按增量 10 自动为 ACL ACE 分配行号，并且显示每个 permit ACE 已成功匹配的次数（在括号内）。

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)

由于与路由器之间已建立了两个成功的 Telnet 连接，每个 Telnet 会话从与 permit ACE 之一匹配的 IP 地址发起，因此每个 permit ACE 都存在匹配。

当每个 IP 地址只发起一个连接时，为什么您会认为每个 permit ACE 有两个匹配?

在 Telnet 连接期间，您如何确定 Telnet 协议在何时导致了两个匹配?

- h 在 R1 上，进入全局配置模式。
- i 进入 ADMIN-MGT 命名访问列表的访问列表配置模式，在访问列表末尾添加一个 **deny any** ACE。

R1(config)# **ip access-list standard ADMIN-MGT**

R1(config-std-nacl)# **deny any**

R1(config-std-nacl)# **exit**

注：由于在所有 ACE 的末尾都有一个隐式的 **deny any** ACE，因此不必要添加一个显式的 **deny any** ACE。但是，ACL 末尾的显式 **deny any** 对于网络管理员记录或简单地了解 **deny any** 访问列表 ACE 匹配了多少次仍然非常有帮助。

- j 尝试从 PC-B 远程登录到 R1。这会创建 ADMIN-MGT 命名访问列表中的 **deny any** ACE 的匹配。
- k 从特权执行模式，键入 **show ip access-lists** 命令，然后按 Enter。您现在应该会看到 **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)
```

相比成功的 Telnet 连接，失败的 Telnet 连接会生成显式 **deny any** ACE 的更多匹配。您认为为什么会发生此情况？

第 4 部分：练习 - 在 S1 上配置和应用访问控制列表

步骤 1：在 S1 上为 vty 线路创建命名的标准 ACL。

- a 在不查阅 R1 配置命令的情况下，尝试在 S1 上配置 ACL，只允许 PC-A 的 IP 地址。
- b 为 S1 vty 线路应用 ACL。记住，交换机上的 vty 线路要比路由器多。

步骤 2：在 S1 上测试 vty ACL。

从每个 PC 使用 Telnet 远程登录，验证 vty ACL 是否正常工作。您应该能够从 PC-A 远程登录到 S1，但是从 PC-B 则不能。

思考

1. 正如远程 vty 接入所证明的，ACL 是强大的内容过滤器，可应用于多个入站和出站网络接口。还能使用哪些方法应用 ACL？

2. 应用到 vty 远程管理接口的 ACL 是否能提高 Telnet 连接的安全性？这是否使得 Telnet 成为更切实可行的远程访问管理工具？

3. 为什么将 ACL 应用到 vty 线路而不是特定接口是明智的选择？

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)
<p>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。</p>				