

第三章用户访问和权限管理

3.1. 设置用户名和密码

提问 为每个单独的人员设置不同的用户名和密码

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#username neoshi password ioscookbook (username weak nopassword)
```

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa authentication login local_auth local
```

```
Router1(config)#line vty 0 4
```

```
Router1(config-line)#login authentication local_auth
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释 设置单独的用户名和密码的好处就不用多说了，这里只提一个就是在日志中会显示谁做了修改，比如 %SYS-5-RELOAD: Reload requested by kdooley on vty0 (172.25.1.1). 另外在 username 这个命令里面还有一个 autocommand 的选项，实现登录以后自动执行某个特定的命令的作用，下面 的例子就是一个用户名为 run 无密码，登录以后显示完端口状态就自动退出的例子，很好用吧

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa authentication login default local
```

```
Router1(config)#aaa authorization exec default local
```

```
Router1(config)#username run nopassword noescape
```

```
Router1(config)#username run autocommand show ip interface brief
```

```
Router1(config)#end
```

```
Router1#
```

3.2. 加密密码

提问 加密密码从而在配置文件中不明文显示

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#enable password oreilly
```

```
Router1(config)#line vty 0 4
```

```
Router1(config-line)#password cookbook
```

```
Router1(config-line)#line con 0
```

```
Router1(config-line)#password cookbook
```

```
Router1(config-line)#line aux 0
```

```
Router1(config-line)#password cookbook
```

```
Router1(config-line)#exit
```

```
Router1(config)#service password-encryption
```

```
Router1(config)#end
```

```
Router1#
```

注释 这种加密方式很弱，很容易被破解

3.3. Using Better Password-Encryption Techniques

提问 使用强度高的加密方式而不是思科缺省的加密技术

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#enable secret ORAbooks
```

```
Router1(config)#end
```

```
Router1#
```

在 IOS 12.2(8)T 后也可以对 username 的密码做高强度的加密

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#username ijbrown secret oreilly
```

```
Router(config)#end
```

```
Router#
```

注释 由于这种加密方式使用的是 MD5 所以破解难度相对增大了。对于 enable secret 的密码有个小技巧就是密码设定正常没有？，不过可以通过 ^V+？的方式来输入。

3.4. 移去配置文件中的密码信息

提问 不想在配置文件中显示密码

回答 使用脚本略去

注释 简单的用 show tech 命令也可以

3.5. 解密思科的弱密码

提问 破解思科缺省的密码算法

回答 使用脚本略去

注释 可以使用 BOSON 网站上的免费工具

3.6. 显示当前登录用户

提问 显示当前登录设备的用户

回答

```
Router1#show users (who)
```

注释 无

3.7. 发信息给其它用户

提问 试图发送信息给登录在同一设备的其它用户

回答

```
Router1#send *
```

```
Router1#send console 0
```

```
Router1#send vty 2
```

```
Router1#send 66
```

注释 很好用的特性，比如当你重启的时候需要告诉别人，文本信息^+Z 结束

3.8. 修改可用 VTY 数目

提问 增加或者减少可登录用户的数目

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#line vty 0 9
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释 缺省可登录 vty 数目为 5，不能删除，对于增加的可以使用 no line vty x 删除，不能不能删除单独的 vty，是删除所有大于 x 的 vty

3.9. 修改 VTY 的超时时长

提问 修改超时避免用户登录超时被系统断开

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#line vty 0 4
```

```
Router1(config-line)#exec-timeout 0 0    (exec-timeout 240 0)
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释 缺省用户 10 分钟空闲就会被踢掉系统，0 0 可以用不超时，第一个 0 是分钟，第二个 0 是秒。同时为了防止有些用户掉死但是还占用 vty 端口的情况，建议使用下面命令来防止：

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#service tcp-keepalives-in
```

```
Router1(config)#end
```

```
Router1#
```

3.10. 限制用户登录可以使用的协议

提问 只允许用户用特定的协议来进行系统登录

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#line vty 0 4
```

```
Router1(config-line)#transport input telnet
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释 缺省情况下除了可以 telnet 登录，还支持以下协议登录 lat pad v120 lapb-ta rlogin ssh

3.11. 配置用户登录可用总时长 Enabling Absolute Timeouts on VTY Lines

提问 对用户登录总时长进行限制，不论是否在空闲还是活动

回答 Router1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#line vty 0 4
```

```
Router1(config-line)#absolute-timeout 5
```

```
Router1(config-line)#logout-warning 30
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释 无

3.12. 部署 Banners

提问 设置登录时显示的警示性信息

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#banner exec # This is an exec banner #
```

```
Router1(config)#banner login # This is a login banner #
```

```
Router1(config)#banner motd $ This is a motd banner $
```

```
Router1(config)#end
```

```
Router1#
```

注释 不使用 welcome 之类的字样，下面是一个 FBI 的路由器登录 banner 做参考

```
Router1(config)#banner login #
```

```
Enter TEXT message. End with the character '#'.  
  
#
```

```
+-----+  
|                                     |  
|                               WARNING                               |  
|                               -----                               |  
|                                     |  
| This system is solely for the use of authorized users for official |  
| purposes. You have no expectation of privacy in its use and to    |  
| ensure that the system is functioning properly, individuals using  |  
| this computer system are subject to having all of their activities |  
| monitored and recorded by system personnel. Use of this system    |  
| evidences an express consent to such monitoring and agreement that |  
| if such monitoring reveals evidence of possible abuse or criminal   |  
| activity, system personnel may provide the results of such        |  
| monitoring to appropriate officials.                                |  
+-----+  
  
#
```

```
Router1(config)#end
```

```
Router1#
```

3. 13. 在特定端口禁用 Banners 显示

提问 aux 口用于 modem 连接，为了避免出现问题希望关闭 banner 显示

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#line aux 0
```

```
Router1(config-line)#no motd-banner
```

```
Router1(config-line)#no exec-banner
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释

3. 14. 禁用 Line 登录

提问 禁止在 AUX 或者 Line 端口进行设备登录

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#line aux 0
```

```
Router1(config-line)#transport input none
```

```
Router1(config-line)#no exec
```

```
Router1(config-line)#exec-timeout 0 1
```

```
Router1(config-line)#no password
```

```
Router1(config-line)#exit
```



```
Router1(config)#end
```

```
Router1#
```

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#access-list 98 deny any log
```

```
Router1(config)#line vty 0 4
```

```
Router1(config-line)#transport input none
```

```
Router1(config-line)#exec-timeout 0 1
```

```
Router1(config-line)#no exec
```

```
Router1(config-line)#access-class 98 in
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释 无

3. 15. 为管理员保留特定的登录端口

提问 防止所有的登录端口都被占用，为管理员留一个后门

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#access-list 9 permit 172.25.1.1
```

```
Router1(config)#line vty 4
```

```
Router1(config-line)#access-class 9 in
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

或者

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#access-list 9 permit 172.25.1.1
```

```
Router1(config)#line vty 5 7
```

```
Router1(config-line)#rotary 25
```

```
Router1(config-line)#access-class 9 in
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释 在使用第二种 rotary 命令时就相应的改变登录时的端口号码，不是缺省的 23，而是 3000+rotary 的号码 25=3025

3. 16. 限制特定地址的 Telnet 登录

提问 只允许特定的机器进行 Telnet 登录

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#access-list 99 permit 172.25.1.0 0.0.0.255
```

```
Router1(config)#access-list 99 deny any log
```

```
Router1(config)#line vty 0 4
```

```
Router1(config-line)#access-class 99 in
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释 无

3.17. 对 Telnet 访问进行日志记录

提问 记录每次 telnet 的日志

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#access-list 90 permit any log
```

```
Router1(config)#line vty 0 4
```

```
Router1(config-line)#access-class 90 in
```

```
Router1(config-line)#exit
```

```
Router1(config)#end
```

```
Router1#
```

注释 需要注意的是不管登录成功还是失败，在日志中都是显示的 permitted:

```
%SEC-6-IPACCESSLOGS: list 90 permitted 172.25.1.1 1 packet
```

3.18. 设置发起 Telnet 的源地址

提问 有时对端设备有安全设置只允许特定的地址发起 telnet 请求

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#ip telnet source-interface loopback0
```

```
Router1(config)#end
```

Router1#

或者

Router1#telnet 172.25.1.5 /source-interface loopback0

注释 缺省情况路由器会使用到目的地所使用的端口来做 Telnet 的源地址

3.19. 自动登录

注释 使用脚本略去，其实用 SecueCRT 很容易设定

3.20. 使用 SSH 登录

提问 启用 SSH 这种加密的登录方式

回答

Router1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#hostname Router1

Router1(config)#ip domain-name neoshi.net

Router1(config)#crypto key generate rsa

The name for the keys will be: Router1.oreilly.com

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

Generating RSA keys ...

[OK]

Router1(config)#

Jun 27 15:04:15: %SSH-5-ENABLED: SSH 1.5 has been enabled

```
Router1(config)#ip ssh time-out 120
```

```
Router1(config)#ip ssh authentication-retries 4
```

```
Router1(config)#end
```

```
Router1#
```

注释 从 IOS 12.3(4)T 开始支持 SSH v2，之前只支持 v1，首先要确认你的 IOS 版本，然后确认支持安全特性 3DES，才能开启 SSH 的特性

<!--[if !supportLists]-->3.21. <!--[endif]-->改变 IOS 命令的特权等级

提问 修改特定 IOS 命令的特权等级

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#privilege exec level 1 show startup-config
```

```
Router1(config)#end
```

```
Router1#
```

注释 缺省情况路由器支持 16 种特权等级，命令一般归属于 0, 1 和 15 三种特权等级，在特权等级 0 下面只支持 disable, enable, exit, help, 和 logout 命令，1 下面不能对配置进行修改，15 就是 enable 的特权等级

3.22. 基于用户的特权等级 Defining Per User Privileges

提问 给不同的用户赋予不同的特权等级

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa authentication login default local
```

```
Router1(config)#aaa authorization exec default local
```

```
Router1(config)#username neoshi privilege 10 password ioscookbook
```

```
Router1(config)#privilege exec level 10 show ip route
```

```
Router1(config)#privilege exec level 1 show ip
```

```
Router1(config)#privilege exec level 1 show
```

```
Router1(config)#end
```

```
Router1#
```

注释 通常的 0, 1 和 15 三种等级弹性不足, 可以定义更多的等级给不同的用户

<!--[if !supportLists]-->3.22. <!--[endif]-->基于端口的特权等级

提问 根据登录的不同端口自动赋予特定的特权等级

回答

```
Router1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router1(config)#line aux 0
```

```
Router1(config-line)#privilege level 5
```

```
Router1(config-line)#exit
```

```
Router1(config)#privilege exec level 5 show ip route
```

```
Router1(config)#privilege exec level 1 show ip
```

```
Router1(config)#privilege exec level 1 show
```

```
Router1(config)#end
```

```
Router1#
```