

Telnet , 在Cisco路由器配置示例的控制台和AUX端口密码

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[背景信息](#)

[在线路上配置口令](#)

[配置过程](#)

[验证配置](#)

[排除登录故障](#)

[配置特定于本地用户的口令](#)

[配置过程](#)

[验证配置](#)

[排除特定于用户的口令故障](#)

[配置AUX线路密码](#)

[配置过程](#)

[验证配置](#)

[配置登录 AAA 身份验证](#)

[配置过程](#)

[验证配置](#)

[排除 AAA 登录故障](#)

[Related Information](#)

[Introduction](#)

本文档将提供配置入站 EXEC 到路由器连接的口令保护配置示例。

[Prerequisites](#)

[Requirements](#)

为了执行本文档中描述的任务，您必须具有对路由器命令行界面 (CLI) 的特权 EXEC 访问权限。要了解命令行使用信息以及命令模式，请参阅[使用 Cisco IOS 软件](#)。

有关将控制台连接到路由器的说明，请参阅路由器的随附文档，或者参阅设备的[在线文档](#)。

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco 2509 路由器
- Cisco IOS® 软件版本 12.2(19)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

背景信息

使用口令保护控制或限制对路由器命令行界面 (CLI) 的访问是整个安全计划的基本要素之一。

保护路由器免于非授权远程访问（通常为 Telnet）是需要配置的最常见的安全性，但是保护路由器免于非授权本地访问也不能忽视。

Note: 在一个有效深入的网络安全方案中，口令保护只是您应使用的众多步骤之一。防火墙、物理访问列表和控制对设备的是必须考虑，当实现您的安全计划时的其他元素。

命令行或对路由器的 EXEC 访问可以多种方式实现，但在所有情况中，到路由器的入站连接都是通过 TTY 线路实现的。TTY 线路有四个主要类型，正如本示例 **show line** 输出中所示：

```
2509#show line
  Tty Typ      Tx/Rx    A Modem  Roty  AccO  AccI   Uses   Noise  Overruns  Int
*   0 CTY          - -      - -      - -    0      0      0/0    -
  1 TTY    9600/9600 - -      - -      - -    0      0      0/0    -
  2 TTY    9600/9600 - -      - -      - -    0      0      0/0    -
  3 TTY    9600/9600 - -      - -      - -    0      0      0/0    -
  4 TTY    9600/9600 - -      - -      - -    0      0      0/0    -
  5 TTY    9600/9600 - -      - -      - -    0      0      0/0    -
  6 TTY    9600/9600 - -      - -      - -    0      0      0/0    -
  7 TTY    9600/9600 - -      - -      - -    0      0      0/0    -
  8 TTY    9600/9600 - -      - -      - -    0      0      0/0    -
  9 AUX    9600/9600 - -      - -      - -    0      0      0/0    -
 10 VTY          - -      - -      - -    0      0      0/0    -
 11 VTY          - -      - -      - -    0      0      0/0    -
 12 VTY          - -      - -      - -    0      0      0/0    -
 13 VTY          - -      - -      - -    0      0      0/0    -
 14 VTY          - -      - -      - -    0      0      0/0    -
```

2509#

CTY 线路类型为控制台端口。在所有路由器上，该类型在路由器配置中显示为 **line con 0**，在 **show line** 命令输出中显示为 **cty**。控制台端口主要用于使用控制台终端进行的本地系统访问。

TTY 线路是用于入站或出站调制解调器和终端连接的异步线路，可以看到在路由器或访问服务器配置中该线路显示为 **line x**。特定线路编号是内置于或安装在路由器或访问服务器上的硬件功能。

AUX 线路为辅助端口，在配置中显示为 **line aux 0**。

VTY 线路为路由器的虚拟终端线路，仅用于控制入站 Telnet 连接。他们虚拟，也就是说他们是软件的功能-没有与他们产生关联的硬件。它们在配置中显示为 **line vty 0 4**。

以上每种线路类型都可以配置口令保护。线路可以配置为所有用户使用一个口令，或特定于用户的口令。可以在路由器本地配置特定于用户的口令，或者使用身份验证服务器提供身份验证。

允许在不同线路上配置不同类型的口令保护。实际上常见的是，在路由器上，控制台对应单一口令，其他入站连接对应特定于用户的口令。

以下是 **show running-config** 命令的路由器输出示例：

```
2509#show running-config
Building configuration...

Current configuration : 655 bytes
!
version 12.2
.
.
.
!--- Configuration edited for brevity line con 0 line 1 8 line aux 0 line vty 0 4 ! end
```

在线路上配置口令

要指定线路上的口令，请在线路配置模式下使用 **password** 命令。要启用登录时检查口令，请在线路配置模式下使用 **login** 命令。

Note: 要查找本文档所用命令的其他信息，请使用[命令查找工具](#) ([仅限注册用户](#))。

配置过程

在本示例中，将为所有尝试使用控制台的用户配置口令。

1. 从特权 EXEC (或“启用”) 提示符处，进入配置模式，然后使用以下命令切换到线路配置模式。请注意，提示符将发生更改以反映当前模式。

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#line con 0
router(config-line)#
```

2. 配置口令，并启用登录时检查口令。

```
router(config-line)#password letmein
router(config-line)#login
```

3. 退出配置模式。

```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

Note: 请勿保存对 **line con 0** 的配置更改，除非您的登录权限已得到验证。

Note: 在线路控制台配置下，必须使用 **login** 配置命令才能启用登录时检查口令。控制台身份验证需要使用 **password** 和 **login** 命令才能正常工作。

验证配置

检查路由器配置，验证是否已正确输入命令：

[命令输出解释程序工具](#) ([仅限注册用户](#)) 支持某些 **show** 命令，使用此工具可以查看对 **show** 命令输出的分析。

- **show running-config** - 显示路由器的当前配置。

```
router#show running-config
Building configuration...
...
!--- Lines omitted for brevity ! line con 0 password letmein
login
line 1 8
line aux 0
line vty 0 4
!
end
```

要测试配置，请从控制台注销，然后再次登录，使用配置的口令访问路由器：

```
router#exit

router con0 is now available

Press RETURN to get started.

User Access Verification
Password:
!--- Password entered here is not displayed by the router router>
```

Note: 在执行该测试前，请确保您拥有到路由器的备用连接，如 Telnet 或拨入，以防止再次登录到路由器时出现问题。

排除登录故障

如果无法再次登录到路由器并且未保存配置，则重新加载路由器将删除您所作的全部配置更改。

如果已保存配置更改，但无法登录路由器，您将必须执行口令恢复。请参阅[口令恢复过程](#)，找到对您特定平台的说明。

配置特定于本地用户的口令

要建立一个基于用户名的身份验证系统，请在全局配置模式下使用 **username** 命令。要启用登录时检查口令，请在线路配置模式下使用 **login local** 命令。

配置过程

在本示例中，将为尝试使用 Telnet 连接到 VTY 线路上路由器的用户配置口令。

1. 从特权 EXEC (或“启用”) 提示符处，进入配置模式，然后为允许访问路由器的每个用户输入一个用户名/口令组合：

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#username russ password montecito
router(config)#username cindy password belgium
router(config)#username mike password rottweiler
```

2. 使用以下命令切换到线路配置模式。请注意，提示符将发生更改以反映当前模式。

```
router(config)#line vty 0 4
router(config-line)#
```

3. 配置登录时的口令检查。

```
router(config-line)#login local
```

4. 退出配置模式。

```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

Note: 为了在 CLI 中键入名称时禁用自动 Telnet，请在使用的线路上配置 **no logging preferred**。虽然 **transport preferred none** 提供同样的输出，但同时也会对配置了 **ip host** 命令的已定义主机禁用自动 Telnet。这不同于 **no logging preferred** 命令，该命令会对未定义的主机禁用自动 Telnet，对定义的主机则允许自动 Telnet 正常工作。

验证配置

检查路由器配置，验证是否已正确输入命令：

- **show running-config** - 显示路由器的当前配置。

```
router#show running-config
Building configuration...
!
!--- Lines omitted for brevity ! username russ password 0 montecito
username cindy password 0 belgium
username mike password 0 rottweiler
!
!--- Lines omitted for brevity ! line con 0 line 1 8 line aux 0 line vty 0 4 login local
!
end
```

要测试此配置，必须与路由器建立 Telnet 连接。这可以通过从网络上的不同主机进行连接来实现，但也可以从路由器本身进行测试，方法是通过远程登录连接到路由器上的任何接口 IP 地址，该接口应在 **show interfaces** 命令输出中显示为 up/up 状态。以下是 **interface ethernet 0** 地址为 10.1.1.1 时的示例输出：

```
router#telnet 10.1.1.1
Trying 10.1.1.1 ... Open

User Access Verification

Username: mike
Password:
!--- Password entered here is not displayed by the router router
```

排除特定于用户的口令故障

用户名和口令区分大小写。使用大小写错误的用户名或口令尝试登录的用户将被拒绝。

如果用户无法使用他们的特定口令登录路由器，请在路由器上重新配置用户名和口令。

配置AUX线路密码

为了指定密码在AUX线路，请发出**password**命令在线路配置模式。为了检查在登录的特权密码，发

出login命令在线路配置模式。

配置过程

在本例中，密码为尝试所有的用户被配置使用Aux端口。

1. 发出show line命令为了验证Aux端口使用的线路。

```
R1#show line
```

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int	
*	0	CTY		-	-	-	-	-	0	0	0/0	-
	65	AUX	9600/9600	-	-	-	-	0	1	0/0		-
	66	VTY		-	-	-	-	-	0	0	0/0	-
	67	VTY		-	-	-	-	-	0	0	0/0	-

2. 在本例中，Aux端口在第65行。发出这些命令为了配置路由器AUX线路：

```
R1# conf t
R1(config)# line 65
R1(config-line)#modem inout
R1(config-line)#speed 115200
R1(config-line)#transport input all
R1(config-line)#flowcontrol hardware
R1(config-line)#login
R1(config-line)#password cisco
R1(config-line)#end
R1#
```

验证配置

检查路由器的配置为了验证命令适当地被输入：

- show running-config命令显示路由器的当前配置：

```
R1#show running-config
Building configuration...
!
!--- Lines omitted for brevity. line aux 0
password cisco
login
modem InOut
transport input all
speed 115200
flowcontrol hardware

!--- Lines omitted for brevity. ! end
```

配置登录 AAA 身份验证

要对登录启用身份验证、授权以及记账 (AAA) 身份验证，请在线路配置模式下使用 login authentication 命令。同时必须配置 AAA 服务。

配置过程

在本示例中，路由器将配置为在用户尝试连接路由器时从 TACACS+ 服务器检索用户口令。

Note: 将路由器配置为使用其他类型的 AAA 服务器 (如 RADIUS) 与之类似。有关详细信息，请参阅[配置身份验证](#)。

Note: 本文档不对 AAA 服务器配置本身进行讨论。有关配置 AAA 服务器的信息，请参阅[安全服务器协议](#)。

1. 从特权 EXEC (或“启用”) 提示符处，进入配置模式，然后输入命令，将路由器配置为使用 AAA 服务进行身份验证：

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login my-auth-list tacacs+
router(config)#tacacs-server host 192.168.1.101
router(config)#tacacs-server key letmein
```

2. 使用以下命令切换到线路配置模式。请注意，提示符将发生更改以反映当前模式。

```
router(config)#line 1 8
router(config-line)#
```

3. 配置登录时的口令检查。

```
router(config)#line 1 8
router(config-line)#
```

4. 退出配置模式。

```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

验证配置

检查路由器配置，验证是否已正确输入命令：

- **show running-config** - 显示路由器的当前配置。

```
router#write terminal
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
aaa new-model
aaa authentication login my-auth-list tacacs+
!
!--- Lines omitted for brevity ... ! tacacs-server host 192.168.1.101
tacacs-server key letmein
!
line con 0
line 1 8
  login authentication my-auth-list
line aux 0
line vty 0 4
!
end
```

要测试这一特定配置，必须与线路建立入站或出站连接。请参阅[调制解调器 - 路由器连接指南](#)，获取有关为调制解调器连接配置异步线路的具体信息。

或者，您可以配置一个或多个 VTY 下路以执行 AAA 身份验证，然后执行测试。

[排除 AAA 登录故障](#)

发出 **debug** 命令之前，请参阅[关于 Debug 命令的重要信息](#)。

要对登录尝试失败进行故障排除，请对应您的配置使用 **debug** 命令：

- [debug aaa authentication](#)
- [debug radius](#)
- [debug kerberos](#)

[Related Information](#)

- [配置身份验证](#)
- [Cisco IOS Debug 命令参考](#)
- [Technical Support - Cisco Systems](#)