

使用TACACS+，配置拨号认证的Cisco路由器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[Microsoft Windows设置](#)

[用于用户 1 和 2 的 Microsoft Windows 设置](#)

[逐步指导](#)

[用于用户 3 的 Microsoft Windows 设置](#)

[验证](#)

[故障排除](#)

[路由器](#)

[服务器](#)

[相关信息](#)

简介

本文描述如何配置在UNIX运作拨号验证的一个Cisco路由器与TACACS+。TACACS+不提供许多个功能作为商业可用的[Cisco Secure ACS for Windows](#)或[用于UNIX的Cisco Secure ACS](#)。

Cisco Systems 以前提供的 TACACS+ 软件已停产并且不再受 Cisco Systems 支持。

今天，当您在您最喜爱的 Internet 搜索引擎上搜索“TACACS+ 免费软件”时，您可以找到许多可用的 TACACS+ 免费软件版本。Cisco 并不具体推荐任何特定的 TACACS+ 免费软件版本实施。

Cisco 安全访问控制服务器 (ACS) 可通过世界范围内的常规 Cisco 销售和分销渠道购买。Cisco Secure ACS for Windows 包括在 Microsoft Windows 工作站实施独立安装所需的全部必要组件。Cisco Secure ACS 解决方案引擎随附有预先安装的 Cisco Secure ACS 软件许可证。参考产品编号的[Cisco Secure ACS 4.0产品公告](#)。访问 [Cisco 订购主页](#) ([仅限注册用户](#)) 下订单。

注意：您需要一个CCO帐户以一个相关的服务合同获得[Cisco Secure ACS for Windows的\(仅限注册用户\)](#) 90天试用版本。

本文档中的路由器配置是根据运行 Cisco IOS® 软件版本 11.3.3 的路由器制定的。Cisco IOS软件版本12.0.5.T而不是TACACS+的及以后使用组tacacs+。语句例如aaa authentication login default radius enable出现作为aaa authentication login default group tacacs+ enable。

您能由匿名文件传送协议下载TACACS+免费软件和用户指南到在/pub/tacacs目录的ftp-eng.cisco.com。

[先决条件](#)

[要求](#)

本文档没有任何特定的要求。

[使用的组件](#)

本文档不限于特定的软件和硬件版本。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[配置](#)

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用 [命令查找工具](#) ([仅限注册用户](#))，查找关于本文所使用命令的更多信息。

本文档使用以下配置：

- [路由器配置](#)
- [免费软件服务器上的 TACACS+ 配置文件](#)

路由器配置

```
!  
aaa new-model  
aaa authentication login default tacacs+ enable  
aaa authentication ppp default if-needed tacacs+  
aaa authorization exec default tacacs+ if-authenticated  
aaa authorization commands 1 default tacacs+ if-  
authenticated  
aaa authorization commands 15 default tacacs+ if-  
authenticated  
aaa authorization network default tacacs+  
enable password ww  
!  
chat-script default "" at&fls0=1&h1&r2&c1&d2&ble0q2 OK  
!  
interface Ethernet0  
 ip address 10.6.1.200 255.255.255.0  
!  
 !--- Challenge Handshake Authentication Protocol !---  
(CHAP/PPP) authentication user. interface Async1 ip  
unnumbered Ethernet0 encapsulation ppp async mode  
dedicated peer default ip address pool async no cdp  
enable ppp authentication chap ! !--- Password  
Authentication Protocol (PAP/PPP) authentication user.  
interface Async2 ip unnumbered Ethernet0 encapsulation  
ppp async mode dedicated peer default ip address pool  
async no cdp enable ppp authentication pap ! !---  
Authentication user with autocommand PPP. interface
```

```
Async3 ip unnumbered Ethernet0 encapsulation ppp async
mode interactive peer default ip address pool async no
cdp enable ! ip local pool async 10.6.100.101
10.6.100.103 tacacs-server host 171.68.118.101 tacacs-
server timeout 10 tacacs-server key cisco ! line 1
session-timeout 20 exec-timeout 120 0 autoselect during-
login script startup default script reset default modem
Dialin transport input all stopbits 1 rxspeed 115200
txspeed 115200 flowcontrol hardware ! line 2 session-
timeout 20 exec-timeout 120 0 autoselect during-login
script startup default script reset default modem Dialin
transport input all stopbits 1 rxspeed 115200 txspeed
115200 flowcontrol hardware ! line 3 session-timeout 20
exec-timeout 120 0 autoselect during-login autoselect
ppp script startup default script reset default modem
Dialin autocommand ppp transport input all stopbits 1
rxspeed 115200 txspeed 115200 flowcontrol hardware ! end
```

免费软件服务器上的 TACACS+ 配置文件

```
!--- Handshake with router !--- AS needs 'tacacs-server
key cisco'. key = "cisco" !--- User who can Telnet in to
configure. user = admin { default service = permit login
= cleartext "admin" } !--- CHAP/PPP authentication line
1 - !--- password must be cleartext per CHAP
specifications. user = chapuser { chap = cleartext
"chapuser" service = ppp protocol = ip { default
attribute = permit } } !--- PPP/PAP authentication line
2. user = papuser { login = file /etc/passwd service =
ppp protocol = ip { default attribute = permit } } !---
Authentication user line 3. user = authauto { login =
file /etc/passwd service = ppp protocol = ip { default
attribute = permit } }
```

Microsoft Windows 设置

用于用户 1 和 2 的 Microsoft Windows 设置

本部分提供有关如何配置本文档所述功能的信息。

逐步指导

完成下面这些步骤。

注意： PC配置能变化轻微基于您使用的操作系统版本。

1. 选择**Start > Programs > Accessories > Dial-Up Networking**打开拨号网络窗口。
2. 从Connections菜单选择**Make New Connection**，并且输入一名称对于您的连接。
3. 输入您的特定调制解调器信息并且单击**配置**。
4. 在General Properties Page请选择高速度您的调制解调器，但是请勿检查**唯一连接在此速度...方框**。
5. 在配置/连接属性页，请使用8数据位、无奇偶校验和1个结束位。使用的呼叫首选是**等待拨号音，在拨号前并且取消呼叫，如果没连接在200秒之后**。
6. 在连接页，请点击**先进**。在先进的连接设置，请选择仅**硬件流控制**和**调制类型英文虎报**。在Properties页的配置/的选项，不应该检查什么都除了在状态控制下的方框。

7. 点击OK键**其次**然后单击。
8. 输入目的地的电话号码，**其次**再单击和然后单击**芬通社**。
9. 一旦新连接图标出现，请用鼠标右键单击它并且选择**Properties > Server Type**。
10. 选择**PPP : WINDOWS 95 , WINDOWS NT 3.5 , 互联网**，并且不检查任何高级选项。
11. 检查**TCP/IP**在允许网络协议下。
12. 在**TCP/IP**设置下...，请选择**服务器指定的IP地址，服务器分配的域名服务器地址和使用默认网关在远程网络**然后单击OK键。
13. 当用户双击图标使Connect To窗口显示为了拨号时，用户必须填写用户名和密码字段，然后单击**连接**。

用于用户 3 的 Microsoft Windows 设置

用户3的(有自动命令PPP的认证用户配置)是相同的象为用户1和2有这些例外：

- 在Properties页的配置/的选项(步骤6)，检查**Bring up terminal window after dialing**。
- 当用户双击图标打开Connect To窗口拨号(步骤13)，用户不填写用户名和密码字段。用户单击**连接**。在对路由器的联系被建立后，用户类型在出现的黑色窗口的用户名和密码。在验证以后，用户按**Continue(F7)**。

验证

当前没有可用于此配置的验证过程。

故障排除

路由器

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

- **terminal monitor** - 显示当前终端和会话的 **debug** 命令输出和系统错误消息。
- **debug ppp协商**—在PPP启动期间，显示PPP发送的数据包，PPP选项协商。
- **debug ppp packet** —显示被发送并且接收的PPP数据包。（此命令显示低级数据包转储信息。）
- **debug ppp chap** —显示信息关于客户端是否通过验证(Cisco IOS软件版本早于11.2)。
- **debug aaa authentication** — 显示有关身份验证、授权和记帐 (AAA)/TACACS+ 身份验证的信息。
- **debug aaa authorization** - 显示有关 AAA/TACACS+ 授权的信息。

服务器

注意： 这假设思科的TACACS+免费软件服务器代码。

```
tac_plus_executable -C config.file -d 16  
tail -f /var/tmp/tac_plus.log
```

相关信息

- [TACACS+ 支持页](#)
- [IOS 文档中的 TACACS+](#)
- [思科安全访问控制服务器](#)
- [安装和调试 CiscoSecure 2.x TACACS+](#)
- [技术支持和文档 - Cisco Systems](#)