

# 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[单向验证与双向验证](#)

[配置命令](#)

[ppp 身份验证 pap \[ 呼入\]](#)

[用户名<username> 密码<password>](#)

[Ppp pap 发送的用户名<username> 密码 <password>](#)

[配置示例](#)

[呼叫方\(客户端\) 配置](#)

[接收方\(服务器\) 配置](#)

[调试输出](#)

[成功的单向 PAP 验证的呼叫方\(客户端\) 调试](#)

[成功的单向 PAP 验证的被呼叫方\(服务器\) 调试](#)

[排除 PAP 故障](#)

[双方不同意将 PAP 作为身份验证协议](#)

[PAP 验证失败](#)

[相关信息](#)

## 简介

点对点协议 (PPP) 目前支持两种身份验证协议：密码验证协议 (PAP) 和质询握手身份验证协议 (CHAP)。这两个协议都是在 RFC 1334 中指定的，且在同步和异步接口上都受支持。

- PAP 使用双向握手为远程节点提供了建立其身份标识的简单方法。PPP链路建立阶段完成后，用户名和密码通过链路(在明文)进行不断重复发送，直到鉴权完成或连接终止为止。
- PAP 是一种不安全的身份验证协议。密码以明文形式通过链路发送，对于回放和试错法攻击没有防范能力。远程节点将控制登录尝试的频率和时间。

[如需了解PPP鉴权故障排除的更多信息 \(使用PAP或CHAP\)，请参见PPP \(CHAP或PAP\)鉴权故障排除章节，了解PPP鉴权阶段故障排除有关的完整的分步流程图。如需了解所有PPP阶段故障排除的更多信息 \(使用LCP鉴权或NCP\)，请参见PPP故障排除流程表，了解所有相关PP阶段和协商参数有关的故障排除的完整的分步流程图。](#)

## 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](#)。

## 背景信息

因为用户密码从未在整个连接上发送，所以CHAP被认为更加安全。有关 CHAP 的详细信息，请参阅[了解和配置 PPP CHAP 身份验证](#)。

尽管 PAP 存在缺点，其仍可用于以下环境：

- 当系统中安装了大量不支持 CHAP 的客户端应用程序时
- 当不同供应商实施的 CHAP 互不兼容时
- 此情况是，纯文本密码必须可用于模拟在远端主机登录。

## 单向验证与双向验证

与大多数鉴权类型一样，PAP支持双向（双程）和单向（单程）鉴权。使用单向身份验证时，仅接收呼叫的一端（NAS）对远程端（客户端）进行身份验证。远程客户端不对服务器进行身份验证。

通过双向认证，每边独立地发送验证请求(AUTH-REQ) 并且接收认证确认(AUTH-ACK)或没有认可的验证(AUTH-NAK)。这些可以用 [debug ppp authentication 命令](#) 查看。客户端上进行此调试的一个示例如下所示：

```
*Mar 6 19:18:53.322: BR0:1 PAP: O AUTH-REQ id 7 len 18 from "PAPUSER"! --- Outgoing PAP AUTH-REQ. We are sending out our username (PAPUSER) and password ! --- to the NAS. The NAS will verify that the username/password is correct. *Mar 6 19:18:53.441: BR0:1 PAP: I AUTH-ACK id 7 Len 5! --- Incoming AUTH-ACK. ! --- The NAS verified the username and password and responded with an AUTH-ACK. ! --- One-way authentication is complete at this point. *Mar 6 19:18:53.445: BR0:1 PAP: I AUTH-REQ id 1 Len 14 from "NAS"! --- Incoming AUTH-REQ from the NAS. This means we now verify the identity of the NAS. *Mar 6 19:18:53.453: BR0:1 PAP: Authenticating peer NAS! --- Performing a lookup for the username (NAS) and password. *Mar 6 19:18:53.457: BR0:1 PAP: O AUTH-ACK id 1 Len 5! --- Outgoing AUTH-ACK. ! --- We have verified the username/password of the NAS and responded with an AUTH-ACK. ! --- Two-way authentication is complete.
```

在上述调试输出中，身份验证是双向的。然而如果配置了单向验证，我们将只能看到前二条调试线路。

## 配置命令

如下所述，常规 PAP 身份验证需要三个命令：

### [ppp 身份验证 pap \[ 呼入\]](#)

[配置 ppp authentication pap callin 命令的路由器将使用 PAP 验证另一边\(对等体\)的身份。](#) 这意味着另一边(对等体)必须将用户名/密码提交给本地设备进行验证。

[呼入选项认为配置ppp authentication pap callin命令的路由器在流入呼叫期间将只验证另一边。](#)对于传出呼叫，它不会对另一端进行身份验证。这意味着发起呼叫的路由器不需要来自另一端的认证请求(AUTH-REQ)。

下表显示了在什么情况下要配置 callin 选项：

认证类型	客户端 (主叫)	NAS (被叫)
单向	ppp authentication pap callin	ppp authentication pap
双向	ppp authentication pap	ppp authentication pap

### [用户名<username> 密码<password>](#)

这是本地路由器用于验证 PPP 对等体的用户名和密码。当对等体发送其PAP用户名和口令时，本地路由器将检查是否该用户名和密码在本地配置。如果匹配成功，则会验证对等体。

**注意：** username 命令对于 PAP 的作用不同于其对于 CHAP 的作用。通过CHAP，此用户名和口令只用于回应挑战，但PAP只用它验证流入的用户名和口令是否有效。

对于单向验证，只有被叫路由器上需要使用此命令。对于双向验证，两端都需要使用此命令。

### [Ppp pap 发送的用户名<username> 密码 <password>](#)

启用出站 PAP 身份验证。[本地路由器通过ppp pap sent-username命令指定的用户名和密码，将其验证到远端设备。](#)另一个路由器必须使用上述所描述的username命令配置此用户名/密码。

如果使用单向验证，此命令只在路由器初始呼叫的时候需要。对于双向验证，两端都必须配置此命令。

## [配置示例](#)

以下配置部分显示了单向身份验证情景所需的 PAP 命令。

**注意：** 仅显示了配置的相关部分。

### [呼叫方\(客户端\) 配置](#)

```
interface BRI0! --- BRI interface for the dialout. ip address negotiated encapsulation ppp! ---  
Use PPP encapsulation. This command is a required for PAP. dialer string 3785555 class 56k! ---  
Number to dial for the outgoing connection. dialer-group 1 isdn switch-type basic-ni isdn spid1  
51299611110101 9961111 isdn spid2 51299622220101 9962222 ppp authentication pap callin! --- Use  
PAP authentication for incoming calls. ! --- The callin keyword has made this a one-way  
authentication scenario. ! --- This router (client) will not request that the peer (server)  
authenticate ! --- itself back to the client. ppp pap sent-username PAPUSER password 7  
<deleted>! --- Permit outbound authentication of this router (client) to the peer. ! --- Send a  
PAP AUTH-REQ packet to the peer with the username PAPUSER and password. ! --- The peer must have  
the username PAPUSER and password configured on it.
```

### [接收方\(服务器\) 配置](#)

```
username PAPUSER password 0 cisco! --- Username PAPUSER is the same as the one sent by the
client. ! --- Upon receiving the AUTH-REQ packet from the client, we will verify that the ! ---
username and password match the one configured here.interface Serial0:23! --- This is the D-
channel for the PRI on the access server receiving the call. ip unnumbered Ethernet0 no ip
directed-broadcast encapsulation ppp! --- Use PPP encapsulation. This command is a required for
PAP. dialer-group 1 isdn switch-type primary-ni isdn incoming-voice modem peer default ip
address pool default fair-queue 64 256 0 ppp authentication pap! --- Use PAP authentication for
incoming calls. ! --- This router (server) will request that the peer authenticate itself to us.
! --- Note: the callin option is not used as this router is not initiating the call.
```

## 调试输出

要调试 PPP PAP 问题，请使用 [debug ppp negotiation](#) 和 [debug ppp authentication](#) 命令。您必须注意两个主要问题：

1. 两端是否都同意将 PAP 作为身份验证方法？
2. 如果都同意，PAP 身份验证是否成功？

参见下列调试获得如何正确回答这些问题的信息。[也请参见“了解debug ppp协商输出”，用它们的相关意思定义不同PPP阶段期间的所有调试行为（包括PPP鉴权）。](#)本文档对于快速确定 PPP 协商失败的原因很有用。[如需了解PPP鉴权故障排除的更多信息（使用PAP或CHAP），请参见PPP（CHAP或PAP）鉴权故障排除章节，了解PPP鉴权阶段故障排除有关的完整的分步流程图。](#)

## 成功的单向 PAP 验证的呼叫方(客户端) 调试

```
maui-soho-01#show debugPPP: PPP authentication debugging is on PPP protocol negotiation
debugging is onmaui-soho-01#ping 172.22.53.144Type escape sequence to abort.Sending 5, 100-byte
ICMP Echos to 172.22.53.144, timeout is 2 seconds:*Mar 6 21:33:26.412: %LINK-3-UPDOWN:
Interface BRI0:1, changed state to up*Mar 6 21:33:26.432: BR0:1 PPP: Treating connection as a
callout*Mar 6 21:33:26.436: BR0:1 PPP: Phase is ESTABLISHING, Active Open [0 sess, 0 load]*Mar
6 21:33:26.440: BR0:1 PPP: No remote authentication for call-out! --- The client will not
authenticate the server for an outgoing call. ! --- Remember this is a one-way authentication
example. *Mar 6 21:33:26.444: BR0:1 LCP: O CONFREQ [Closed] id 82 Len 10*Mar 6 21:33:26.448:
BR0:1 LCP: MagicNumber 0x2F1A7C63 (0x05062F1A7C63)! --- Outgoing CONFREQ (CONFigure-REQuest).
! --- Notice that we do not specify an authentication method, ! --- since only the peer will
authenticate us. *Mar 6 21:33:26.475: BR0:1 LCP: I CONFREQ [REQsent] id 13 Len 14*Mar 6
21:33:26.479: BR0:1 LCP: AuthProto PAP (0x0304C023)! --- Incoming LCP CONFREQ (Configure-
Request) indicating that ! --- the peer(server) wishes to use PAP. *Mar 6 21:33:26.483: BR0:1
LCP: MagicNumber 0x3DBEE95B (0x05063DBEE95B)*Mar 6 21:33:26.491: BR0:1 LCP: O CONFACK [REQsent]
id 13 Len 14*Mar 6 21:33:26.495: BR0:1 LCP: AuthProto PAP (0x0304C023)! --- This shows the
outgoing LCP CONFACK (CONFigure-ACKnowledge) indicating that ! --- the client can do PAP.*Mar 6
21:33:26.499: BR0:1 LCP: MagicNumber 0x3DBEE95B (0x05063DBEE95B)*Mar 6 21:33:26.511: BR0:1 LCP:
I CONFACK [ACKsent] id 82 Len 10*Mar 6 21:33:26.515: BR0:1 LCP: MagicNumber 0x2F1A7C63
(0x05062F1A7C63)*Mar 6 21:33:26.519: BR0:1 LCP: State is Open! --- This shows LCP negotiation
is complete.*Mar 6 21:33:26.523: BR0:1 PPP: Phase is AUTHENTICATING, by the peer [0 sess, 0
load]! --- The PAP authentication (by the peer) begins.*Mar 6 21:33:26.531: BR0:1 PAP: O AUTH-
REQ id 20 Len 18 from "PAPUSER"! --- The client sends out a PAP AUTH-REQ with username PAPUSER.
! --- This username is configured with the ppp pap sent-username command. *Mar 6 21:33:26.555:
BR0:1 PAP: I AUTH-ACK id 20 Len 5! --- The Peer responds with a PPP AUTH-ACK, indicating that !
--- it has successfully authenticated the client.
```

## 成功的单向 PAP 验证的被呼叫方(服务器) 调试

```
maui-nas-06#show debugPPP: PPP authentication debugging is on PPP protocol negotiation
debugging is onmaui-nas-06#Jan 3 14:07:57.872: %LINK-3-UPDOWN: Interface Serial0:4, changed
state to up*Jan 3 14:07:57.876: Se0:4 PPP: Treating connection as a callin! --- Since the
connection is incoming, we will authenticate the client.*Jan 3 14:07:57.876: Se0:4 PPP: Phase is
ESTABLISHING, Passive Open*Jan 3 14:07:57.876: Se0:4 LCP: State is Listen*Jan 3 14:07:58.120:
Se0:4 LCP: I CONFREQ [Listen] id 83 Len 10*Jan 3 14:07:58.120: Se0:4 LCP: MagicNumber 0x2F319828
(0x05062F319828)*Jan 3 14:07:58.124: Se0:4 LCP: O CONFREQ [Listen] id 13 Len 14*Jan 3
14:07:58.124: Se0:4 LCP: AuthProto PAP (0x0304C023)! --- Outgoing CONFREQ (Configure-Request)
```

```
! --- use PAP for the peer authentication.*Jan 3 14:07:58.124: Se0:4 LCP: MagicNumber 0x3DD5D5B9 (0x05063DD5D5B9)*Jan 3 14:07:58.124: Se0:4 LCP: O CONFACK [Listen] id 83 Len 10*Jan 3 14:07:58.124: Se0:4 LCP: MagicNumber 0x2F319828 (0x05062F319828)*Jan 3 14:07:58.172: Se0:4 LCP: I CONFACK [ACKsent] id 13 Len 14*Jan 3 14:07:58.172: Se0:4 LCP: AuthProto PAP (0x0304C023)! --- This shows the incoming LCP CONFACK (Configure-Acknowledge) indicating that ! --- the client can do PAP.*Jan 3 14:07:58.172: Se0:4 LCP: MagicNumber 0x3DD5D5B9 (0x05063DD5D5B9)*Jan 3 14:07:58.172: Se0:4 LCP: State is Open*Jan 3 14:07:58.172: Se0:4 PPP: Phase is AUTHENTICATING, by this end! --- The PAP authentication (by this side) begins.*Jan 3 14:07:58.204: Se0:4 PAP: I AUTH-REQ id 21 Len 18 from "PAPUSER"! --- Incoming AUTH-REQ from the peer. This means we must now verify ! --- the identity of the peer.*Jan 3 14:07:58.204: Se0:4 PPP: Phase is FORWARDING*Jan 3 14:07:58.204: Se0:4 PPP: Phase is AUTHENTICATING*Jan 3 14:07:58.204: Se0:4 PAP: Authenticating peer PAPUSER! --- Performing a lookup for the username (PAPUSER) and password.*Jan 3 14:07:58.208: Se0:4 PAP: O AUTH-ACK id 21 Len 5! --- This shows the outgoing AUTH-ACK. ! --- We have verified the username and password and responded with an AUTH-ACK. ! --- One-way authentication is complete.
```

## 排除 PAP 故障

当对 PAP 进行故障排除时，请回答“调试输出”部分显示的不同问题：

1. 两端是否都同意将 PAP 作为身份验证方法？
2. 如果都同意，PAP 身份验证是否成功？

[如需了解PPP鉴权故障排除的更多信息（使用PAP或CHAP），请参见PPP（CHAP或PAP）鉴权故障排除章节，了解PPP鉴权阶段故障排除有关的完整的分步流程图。](#)

## 双方不同意将 PAP 作为身份验证协议

在特定配置中，您会发现两端没有同时达成协议将PAP当成认证协议，或者相反地，它们将CHAP当成认证协议（而此时您需要PAP）。请使用以下步骤对这些问题进行故障排除：

1. 确认接听呼叫的路由器具有下列其中一个身份验证命令：`ppp authentication pap` or `ppp authentication pap chap` or `ppp authentication chap pap`
2. 确认进行呼叫的路由器已配置 [ppp authentication pap callin](#)。
3. [验证主叫方正确地配置 ppp pap sent-username username password password 命令，其中用户名和密码与接受路由器上的用户名和密码匹配。](#)
4. 在接口配置模式下，在呼叫路由器上配置 [ppp chap refuse 命令](#)。默认情况下，思科路由器会接受 CHAP 作为身份验证协议。[在客户端希望执行PAP但接入服务器能执行PAP或CHAP \(pap配置的ppp authentication chap\)的情况下，可以使用ppp chap refuse命令迫使客户端将PAP用作鉴权协议。](#) `maui-soho-01(config)#interface BRI 0maui-soho-01(config-if)#ppp chap refuse`

## PAP 验证失败

如果双方同意将PAP作为认证协议，但PAP连接失败，它就很可能是用户名/密码的问题。

1. 验证主叫方正确地配置 `ppp pap sent-username username password password` 命令，其中用户名和密码与接受路由器上的用户名和密码匹配。
2. 对于双向认证来说，验证接收端有正确配置的命令 `PPP PAP Sent-Username Username Password password`，用户名和密码与配置在主叫路由器上的命令匹配。执行双向认证时，如果接收路由器没有出现 `PPP PAP Sent-Username Username Password password` 命令，并且PPP客户端尝试强制服务器远程鉴权，这时将显示 `debug ppp negotiation(或debug ppp authentication)` 输出。`maui-soho-01(config)#interface BRI 0maui-soho-01(config-if)#ppp chap refuse` 出现此错误消息表示存在配置问题，而不一定是安全漏洞。

### 3. 3. 验证用户名和密码，并与对等体的PPP PAP Sent-Username Username Password

Password命令中配置的用户名和密码匹配。如果它们不匹配，您会看到以下消息：  
\*Jan 3 17:18:57.559: Se0:3 PAP: I AUTH-REQ id 25 Len 18 from "PAPUSER"\*Jan 3 17:18:57.559: Se0:3  
PPP: Phase is FORWARDING\*Jan 3 17:18:57.559: Se0:3 PPP: Phase is AUTHENTICATING\*Jan 3  
17:18:57.559: Se0:3 PAP: Authenticating peer PAPUSER\*Jan 3 17:18:57.559: Se0:3 PAP: **O  
AUTH-NAK** id 25 Len 32 msg is **"Password validation failure"!** --- *This is an outgoing AUTH-  
NAK. This means that the mismatch occurred ! --- on this router. Verify that the username  
and password configured locally is ! --- identical to that on the peer.*

## 相关信息

- [配置身份验证](#)
- [Ppp故障排除流程图](#)
- [PPP \( CHAP 或 PAP \) 认证故障排除](#)
- [了解 debug ppp negotiation 输出](#)
- [使用 ppp chap hostname 和 ppp authentication chap callin 命令的 PPP 认证](#)
- [拨号技术：概述和解释](#)
- [技术支持和文档 - Cisco Systems](#)