

設定PPP密碼驗證通訊協定(PAP)並疑難排解

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[單向與雙向身份驗證](#)

[組態命令](#)

[ppp authentication pap \[callin\]](#)

[username <username> password <password>](#)

[PPP pap sent-username <username> password <password>](#)

[組態範例](#)

[呼叫端 \(客戶端 \) 配置](#)

[接收端 \(伺服器 \) 配置](#)

[調試輸出](#)

[成功的單向PAP身份驗證的呼叫端 \(客戶端 \) 調試](#)

[成功的單向PAP身份驗證的被叫端 \(伺服器 \) 調試](#)

[疑難排解PAP](#)

[雙方沒有同意PAP作為身份驗證協定](#)

[PAP身份驗證未成功](#)

[相關資訊](#)

簡介

點對點通訊協定(PPP)目前支援兩種驗證通訊協定：密碼驗證通訊協定(PAP)和質詢握手驗證通訊協定(CHAP)。兩者都在RFC 1334中指定，並且在同步和非同步介面上受支援。

- PAP為遠端節點提供了一種使用雙向握手來建立其身份的簡單方法。在PPP鏈路建立階段完成後，遠端節點會反複通過鏈路傳送使用者名稱和密碼對（以明文形式），直到身份驗證得到確認或連線終止為止。
- PAP不是安全身份驗證協定。密碼以明文形式通過連結傳送，無法抵禦回放或試錯攻擊。遠端節點控制登入嘗試的頻率和時間。

有關PPP身份驗證故障排除（使用PAP或CHAP）的詳細資訊，請參閱[PPP \(CHAP或PAP \) 身份驗證故障排除](#)，以獲得對PPP身份驗證階段進行故障排除的完整分步流程圖。有關所有PPP階段（LCP、身份驗證、NCP）故障排除的詳細資訊，請參閱文檔[PPP故障排除流程](#)，瞭解所有相關PPP階段和協商引數的逐步故障排除的完整流程圖。

必要條件

[需求](#)

本文件沒有特定需求。

[採用元件](#)

本文件所述內容不限於特定軟體和硬體版本。

[慣例](#)

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

[背景資訊](#)

CHAP被認為更安全，因為使用者密碼絕不會通過連線傳送。有關CHAP的詳細資訊，請參閱[瞭解和配置PPP CHAP身份驗證](#)。

儘管PAP有缺點，但它可以在以下環境中使用：

- 大量不支援CHAP的客戶端應用程式
- CHAP的不同供應商實施之間的不相容性
- 必須提供明文密碼才能模擬遠端主機登入的情況

[單向與雙向身份驗證](#)

與大多數型別的身份驗證一樣，PAP支援雙向（雙向）和單向（單向）身份驗證。使用單向身份驗證時，只有接收呼叫的一端(NAS)對遠端端（客戶端）進行身份驗證。遠端客戶端不對伺服器進行身份驗證。

透過雙向驗證，每一端獨立傳送驗證請求(AUTH-REQ)並接收Authenticate-Acknowledge(AUTH-ACK)或Authenticate-Not Acknowledged(AUTH-NAK)。可從[debug ppp authentication](#) 指令中看到這些情況。以下是在使用者端進行偵錯的範例：

```
*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.
```

在上述調試輸出中，身份驗證是雙向的。但是，如果已配置單向身份驗證，我們只會看到前兩條調試線路。

[組態命令](#)

正常PAP身份驗證需要以下三個命令：

[ppp authentication pap \[callin\]](#)

在其上配置[ppp authentication pap](#)命令的路由器將使用PAP驗證另一端（對等體）的身份。這表示另一端（對等點）必須將其使用者名稱/密碼提供給本地裝置以進行驗證。

[callin](#)選項表示配置了[ppp authentication pap callin](#)命令的路由器在撥入呼叫期間將僅對另一端進行身份驗證。對於傳出呼叫，它不會驗證另一端。這表示發起呼叫的路由器不需要從另一端請求身份驗證(AUTH-REQ)

下表顯示何時配置[callin](#)選項：

驗證型別	客戶端（呼叫）	NAS（呼叫）
單向	ppp authentication pap callin	ppp authentication pap
雙向	ppp authentication pap	ppp authentication pap

[username <username> password <password>](#)

這是本地路由器用於驗證PPP對等體的使用者名稱和密碼。當對等體傳送其PAP使用者名稱和密碼時，本地路由器將檢查該使用者名稱和密碼是否在本地配置。如果匹配成功，對等體將進行身份驗證。

註：PAP的[username](#)命令的功能與其對CHAP的功能不同。使用CHAP時，此使用者名稱和密碼用於生成對質詢的響應，但PAP僅使用它來驗證傳入的使用者名稱和密碼是否有效。

對於單向身份驗證，僅在被叫路由器上需要此命令。對於雙向身份驗證，此命令在兩端都是必需的。

[PPP pap sent-username <username> password <password>](#)

啟用出站PAP身份驗證。本地路由器使用[ppp pap sent-username](#)命令指定的使用者名稱和密碼向遠端裝置驗證其自身。另一台路由器必須使用上述[username](#)命令配置此相同的使用者名稱/密碼。

如果使用單向身份驗證，則只有在發起呼叫的路由器上才需要使用此命令。對於雙向身份驗證，必須在兩端配置此命令。

[組態範例](#)

以下配置部分顯示了單向身份驗證方案的必要PAP命令。

註：僅顯示配置的相關部分。

[呼叫端（客戶端）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
```

```
! --- 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.
```

接收端 (伺服器) 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.
```

調試輸出

要調試PPP PAP問題，請使用[debug ppp negotiation](#) 和[debug ppp authentication](#) 命令。您必須注意兩個主要問題：

1. 雙方是否都同意PAP是身份驗證方法？
2. 如果是，PAP身份驗證是否成功？

有關如何正確回答這些問題的資訊，請參閱以下調試。此外，請參閱[瞭解debug ppp negotiation輸出](#)，瞭解在不同PPP階段（包括PPP身份驗證）期間所有不同調試線路及其相對含義的說明。本文有助於快速確定PPP協商失敗的原因。有關PPP身份驗證故障排除（使用PAP或CHAP）的詳細資訊，請參閱[PPP \(CHAP或PAP \) 身份驗證故障排除](#)，以獲得對PPP身份驗證階段進行故障排除的完整分步流程圖。

成功的單向PAP身份驗證的呼叫端 (客戶端) 調試

```
maui-soho-01#show debug
```

```
PPP:
```

```
PPP authentication debugging is on
```

```
PPP protocol negotiation debugging is on
```

```
maui-soho-01#ping 172.22.53.144
```

```
Type 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.

```

成功的單向PAP身份驗證的被叫端 (伺服器) 調試

```
maui-nas-06#show debug
```

```

PPP:
  PPP authentication debugging is on
  PPP protocol negotiation debugging is on
maui-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.

```

疑難排解PAP

對PAP進行故障排除時，請回答調試輸出部分中顯示的相同問題：

1. 雙方是否都同意PAP是身份驗證方法？
2. 如果是，PAP身份驗證是否成功？

有關PPP身份驗證故障排除（使用PAP或CHAP）的詳細資訊，請參閱[PPP \(CHAP或PAP \) 身份驗證故障排除](#)，以獲得對PPP身份驗證階段進行故障排除的完整分步流程圖。

雙方沒有同意PAP作為身份驗證協定

在某些配置中，您可以觀察到兩端並未同意PAP作為身份驗證協定，而是同意CHAP（當您需要PAP時）。使用以下步驟排除此類故障：

1. 驗證接收呼叫的路由器是否具有下列身份驗證命令之一

```
ppp authentication pap
    or
ppp authentication pap chap
    or
ppp authentication chap pap
```

2. 驗證發起呼叫的路由器是否配置了[ppp authentication pap callin](#)。
3. 確認呼叫端正確設定了[ppp pap sent-username username password](#) 指令，其中使用者名稱和密碼與接收路由器上設定的使用者名稱和密碼一致。
4. 在呼叫路由器的介面配置模式下配置[ppp chap refuse](#)命令。預設情況下，Cisco路由器將接受CHAP作為身份驗證協定。如果客戶端希望執行PAP，但接入伺服器可以執行PAP或CHAP(已配置[ppp authentication chap pap](#))，則可以使用[ppp chap refuse](#)命令強制客戶端接受PAP作為身份驗證協定。

```
maui-soho-01(config)#interface BRI 0
maui-soho-01(config-if)#ppp chap refuse
```

PAP身份驗證未成功

如果兩端都同意PAP作為身份驗證協定，但PAP連線失敗，則最有可能是使用者名稱/密碼問題。

1. 確認呼叫端正確設定了[ppp pap sent-username username password](#) 指令，其中使用者名稱和密碼與接收路由器上設定的使用者名稱和密碼一致。
2. 對於雙向身份驗證，請確認接收方正確配置了[ppp pap sent-username username password](#) 命令，其中使用者名稱和密碼與呼叫路由器上配置的使用者名稱和密碼匹配。執行雙向身份驗證時，如果接收路由器上不存在命令[ppp pap sent-username username password password](#)，並且PPP客戶端嘗試強制伺服器進行遠端身份驗證，則[debug ppp negotiation](#)(或[debug ppp authentication](#))的輸出將指示

```
*Jan  3 16:47:20.259: Se0:1 PAP: Failed request for PAP credentials.  Username maui-nas-06
此錯誤消息表示存在配置問題，而不一定是安全漏洞。
```

3. 驗證使用者名稱和密碼是否與對等項上命令[ppp pap sent-username username password](#) 中配置的使用者名稱和密碼匹配。如果它們不匹配，您將看到以下消息：

```
*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.

相關資訊

- [配置身份驗證](#)
- [PPP故障排除流程圖](#)
- [排除PPP \(CHAP或PAP \) 身份驗證故障](#)
- [瞭解debug ppp negotiation輸出](#)
- [使用ppp chap hostname和ppp authentication chap callin命令進行PPP身份驗證](#)
- [撥號技術：概觀和說明](#)
- [技術支援與文件 - Cisco Systems](#)