

排除PPP (CHAP或PAP) 身份驗證故障

目錄

[簡介](#)

[必要條件](#)

[技術](#)

[需求](#)

[採用元件](#)

[慣例](#)

[故障排除流程圖](#)

[路由器是否執行CHAP或PAP身份驗證？](#)

[路由器是否執行單向或雙向CHAP身份驗證？](#)

[這是傳入故障嗎？](#)

[傳出質詢或響應中的使用者名稱是否與主機名相同？](#)

[遠端電腦是否是您有權訪問的思科路由器？](#)

[排除傳出CHAP故障](#)

[路由器不使用AAA或僅使用本地AAA](#)

[常見基於伺服器的AAA問題故障排除](#)

[相關資訊](#)

簡介

點對點通訊協定(PPP)驗證問題是撥號連結失敗的最常見原因之一。本文提供一些有關PPP身份驗證問題的故障排除過程。

必要條件

- 啟用[debug ppp negotiation](#)和[debug ppp authentication](#)。
- PPP身份驗證階段在鏈路控制協定(LCP)階段完成並處於開啟狀態之前不會開始。如果[debug ppp negotiation](#)未指示LCP處於開啟狀態，請在繼續之前解決此問題。
- 必須在兩端配置PPP身份驗證。根據需要發出以下命令：[兩台路由器](#)上的PPP身份驗證chap，用於雙向質詢握手身份驗證協定(CHAP)身份驗證。[用於單向身份驗證的ppp authentication chap callin](#)（在呼叫路由器上）。[兩台路由器上的ppp authentication pap](#)，用於PAP身份驗證。

技術

- **本地計算機**（或本地路由器）— 這是當前運行調試會話的系統。將調試會話從一個路由器移動到另一個路由器時，請將術語「本地電腦」應用到另一個路由器。
- **Peer** — 點對點連結的另一端。因此，裝置不是本地電腦。例如，如果您在RouterA上發出[debug ppp negotiation](#)命令，則它是本地機器，而RouterB是對等體。但是，如果將調試工作轉

移到RouterB，則它成為本地電腦，而RouterA成為對等體。

注意：術語「本地電腦和對等」並不意味著客戶端 — 伺服器關係。根據運行調試會話的位置，撥入客戶端可以是本地電腦或對等裝置。

需求

思科建議您瞭解以下主題：

- 您必須能夠讀取和理解debug ppp negotiation輸出。如需詳細資訊，請參閱[瞭解debug ppp negotiation輸出](#)檔案。

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](#)。

故障排除流程圖

本文檔包含一些流程圖以協助進行故障排除。按一下編號的圓可繼續進入下一個流程圖。

在身份驗證階段查詢CHAP:

```
*Mar 7 21:16:29.468: BR0:1 PPP: Phase is AUTHENTICATING, by this end
*Mar 7 21:16:29.468: BR0:1 CHAP: O CHALLENGE id 5 len 33 from "maui-soho-03"
```

PAP

在身份驗證階段查詢PAP:

```
*Mar 7 21:24:11.980: BR0:1 PPP: Phase is AUTHENTICATING, by both
*Mar 7 21:24:12.084: BR0:1 PAP: I AUTH-REQ id 1 len 23 from "maui-soho-01"
```

路由器是否執行單向或雙向CHAP身份驗證？

在debug ppp negotiation輸出中查詢以下消息之一：

```
BR0:1 PPP: Phase is AUTHENTICATING, by both
```

上面的消息表明路由器正在執行雙向身份驗證。

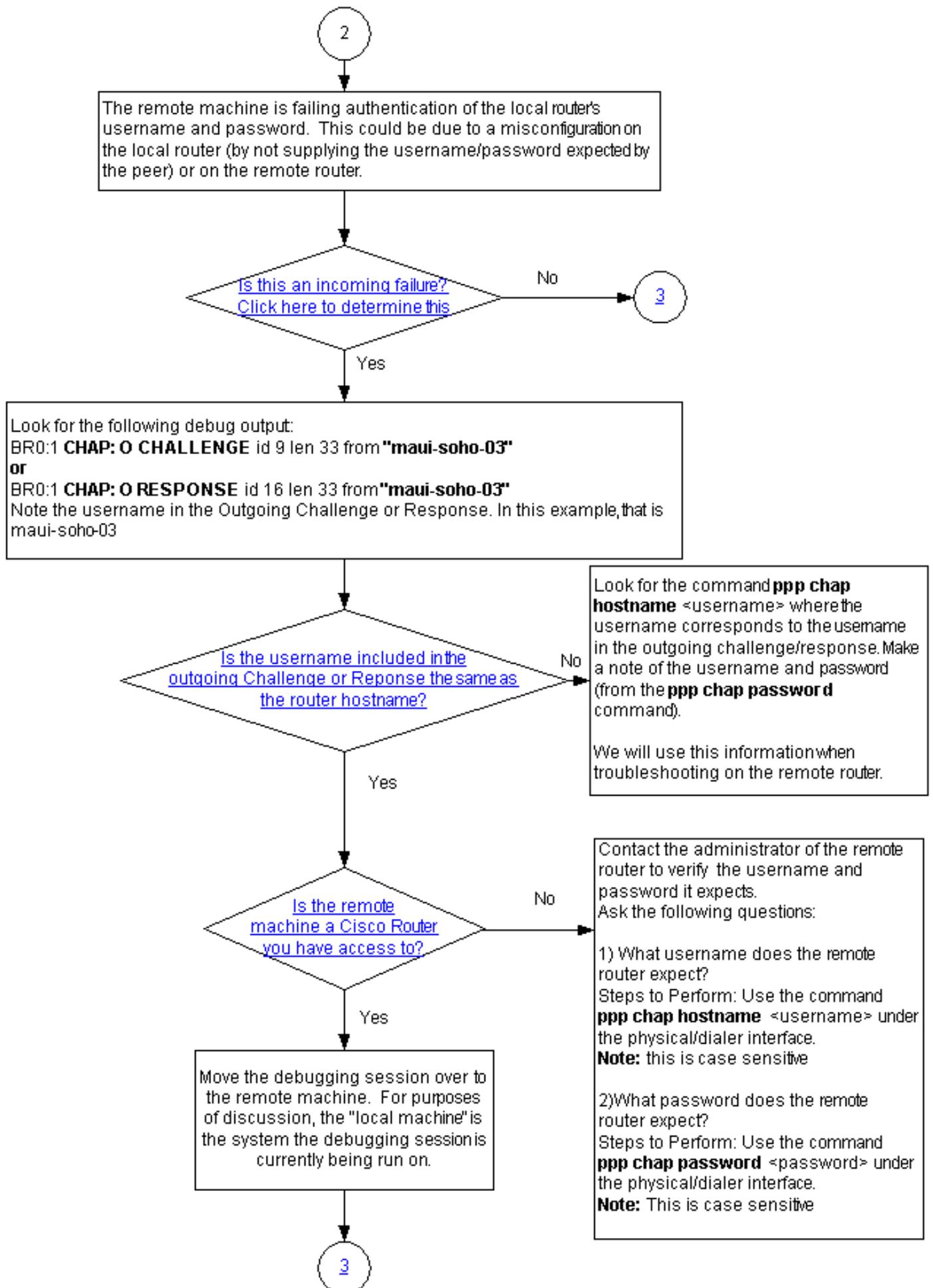
以下任一訊息表示路由器正在執行單向驗證：

```
BR0:1 PPP: Phase is AUTHENTICATING, by the peer
```

或

```
BR0:1 PPP: Phase is AUTHENTICATING, by this end
```

這是傳入故障嗎？



檢查您是否正在接收傳入的termreq或failure消息。請記住，「I」表示消息是傳入消息：

```
BR0:1 LCP: I TERMREQ
```

或

```
BR0:1 CHAP: I FAILURE
```

傳入故障表示對等體無法驗證本地路由器的使用者名稱和密碼。這可能是由於本地路由器（未提供對等體預期的使用者名稱和密碼）或遠端路由器上的配置錯誤所致。

傳出質詢或響應中的使用者名稱是否與主機名相同？

在debug ppp negotiation輸出中查詢以下內容：

```
BR0:1 CHAP: O CHALLENGE id 9 len 33 from "maui-soho-03"
```

或

```
BR0:1 CHAP: O RESPONSE id 16 len 33 from "maui-soho-03"
```

請注意傳出質詢或響應中的使用者名稱。在本例中，它是maui-soho-03。您需要此示例來驗證用於身份驗證的使用者名稱和密碼是否與遠端預期的使用者名稱和密碼匹配。例如，如果本地路由器將自身標識為對等體A，但對等體期望為B，則身份驗證失敗。

如果傳出質詢中的使用者名稱與主機名不同，請查詢命令 [ppp chap hostname <username>](#)，其中使用者名稱與傳出質詢中的使用者名稱相對應。記下使用者名稱和密碼(在隨附的ppp chap password命令中)。您將在對遠端路由器進行故障排除時使用此資訊。

遠端電腦是否是您有權訪問的思科路由器？

由於我們已經確定本地路由器收到傳入故障，因此我們知道該故障發生在對等路由器上。如果您有權訪問遠端Cisco路由器，請對該裝置進行故障排除。

如果您無法訪問遠端路由器，請聯絡該路由器的管理員以驗證所需的使用者名稱和密碼。

提出以下問題：

1. 遠端路由器需要什麼使用者名稱？在物理或撥號器介面下使用 [ppp chap hostname <username>](#) 命令。在此處配置遠端管理員提供的使用者名稱。**注意：**區分大小寫。
2. 遠端路由器需要什麼口令？在物理或撥號器介面下使用 [ppp chap password <password>](#) 命令。**注意：**區分大小寫。

有關詳細資訊，請參閱 [使用ppp chap hostname和ppp authentication chap callin命令的PPP身份驗證](#)。

排除傳出CHAP故障

If the peer detects an incoming failure message, this means the local router has failed to authenticate the peer and has sent out the message. Hence we must now move troubleshooting to the router on which the Outgoing Failure is seen.

The following messages on the local router indicates an outgoing failure:
 BR0:1 CHAP: O FAILURE id 10 len 26 msg is "Authentication failure"
 or
 BR0:1 LCP: O TERMREQ [Open] id 22 len 4

Does the local router use Server-based AAA (Radius/TACACS+)?

yes

4

No, it uses either No AAA or local AAA

Choose from one the following error messages

BR0:1 CHAP: I RESPONSE id 18 len 33 from "<username>"
 BR0:1 CHAP: Unable to validate Response. Username <username>
 not found
 BR0:1 CHAP: O FAILURE id 18 len 26 msg is "Authentication failure"
 BR0:1 PPP: Phase is TERMINATING [0 sess, 0 load]

Configure the username and shared secret for the chap challenge
 Use the command
username <username> password <password>
Note: The username should be identical to the username in the incoming CHAP message, while the password should be the common secret

BR0:1 CHAP: Username <username> not found
 BR0:1 CHAP: Unable to authenticate for peer
 BR0:1 PPP: Phase is TERMINATING
 BR0:1 LCP: O TERMREQ [Open] id 22 len 4

Configure the username and shared secret for the chap challenge
 Use the command
username <username> password <password>
Note: The username should be identical to the username in the incoming CHAP message, while the password should be the common secret

BR0:1 CHAP: I RESPONSE id 16 len 33 from "<username>"
 BR0:1 CHAP: O FAILURE id 16 len 25 msg is "MD/DES compare failed"

Remove the existing username/password entry using the command:
no username <username>
 where <username> matches the one in the CHAP message

Configure the username and password using the command:
username <username> password <password>
 The username should be the same as in the CHAP message shown above. The password should match the password on the remote router.

如果對等體檢測到傳入的故障消息，則意味著本地路由器無法驗證對等體並已發出該消息。因此，現在必須排除路由器故障，該路由器指示出站故障。

本地路由器上的以下消息表示傳出故障：

```
BR0:1 CHAP: O FAILURE id 10 len 26 msg is "Authentication failure"
```

或

```
BR0:1 LCP: O TERMREQ [Open] id 22 len 4
```

路由器不使用AAA或僅使用本地AAA

如果路由器不使用基於伺服器的驗證、授權和記帳(AAA)系統 (Radius或Tacacs+) ，則路由器可以使用no AAA或本地AAA。檢查調試輸出中是否看到以下消息之一：

無法驗證響應

Username <username> Not Found

```
BR0:1 CHAP: I RESPONSE id 18 len 33 from "maui-soho-03"
! -- Incoming CHAP response to our challenge. ! -- The username used in the response is maui-soho-03. BR0:1 CHAP: Unable to validate Response. Username maui-soho-03 not found
! -- The username supplied by the peer is not configured on the router. ! -- We assume the peer does not have permission to connect. BR0:1 CHAP: O FAILURE id 18 len 26 msg is "Authentication failure"
! -- Outgoing CHAP failure message. ! -- The peer will see this as an incoming failure. BR0:1
PPP: Phase is TERMINATING [0 sess, 0 load]
```

使用者名稱不相符的原因可能有兩個：

1. 對等體未提供本地路由器預期的使用者名稱。例如，我們需要 (並配置了) 使用者名稱 RouterA，但對等體使用了名稱RouterB。您可以配置對等體傳送的使用者名稱和密碼，或使用正確的使用者名稱更正對等體。
2. 本地路由器未配置使用者名稱。如果對等體提供的使用者名稱與本地路由器預期的使用者名稱匹配，則配置使用者名稱和密碼。

當對等體使用[ppp chap hostname](#) 命令配置除路由器主機名以外的使用者名稱時，最常出現此問題。

使用username <username> password <password>命令，其中<username>替換為上述錯誤消息中的使用者名稱。

Username <username> Not Found

無法驗證對等體

```
BR0:1 CHAP: I CHALLENGE id 17 len 33 from "maui-soho-01"
! -- Incoming challenge from maui-soho-01. ! -- This router must look up the username specified ! -- in order to create the CHAP response. BR0:1 CHAP: Username maui-soho-01 not found
! -- The username (maui-soho-01) supplied by the peer is not configured locally. BR0:1 CHAP: Unable to authenticate for peer
! -- Since this router does not recognize the username ! -- it cannot create the outgoing CHAP RESPONSE. BR0:1 PPP: Phase is TERMINATING ! -- Authentication fails.
```

使用者名稱不相符的原因可能有兩個：

1. 對等體未提供本地路由器預期的使用者名稱。例如，我們需要（並配置了）使用者名稱 RouterA。但是，對等體使用名稱 RouterB。您可以配置對等體傳送的使用者名稱和密碼，或使用正確的使用者名稱更新對等體。
2. 本地路由器未配置使用者名稱。如果對等體提供的使用者名稱與本地路由器預期的使用者名稱匹配，則配置使用者名稱和密碼。

當對等體使用 [ppp chap hostname](#) 命令配置除路由器主機名以外的使用者名稱時，最常出現此問題。

使用 `username <username> password <password>` 命令，其中 <username> 替換為上述錯誤消息中的使用者名稱。

MD/DES比較失敗

```
BR0:1 CHAP: I RESPONSE id 16 len 33 from "maui-soho-03"  
BR0:1 CHAP: O FAILURE id 16 len 25 msg is "MD/DES compare failed"
```

此錯誤是由密碼不匹配引起的。這可能有兩個原因：

1. 對等體未提供本地路由器預期的密碼。例如，我們需要（並配置了）密碼 *Letmein*，但對等體使用了密碼 *letmein*。您可以重新配置對等體傳送的使用者名稱和密碼，或使用正確的使用者名稱更正對等體。
2. 本地路由器的口令配置不正確。如果您已驗證對等體提供的密碼是否正確，請重新配置本地路由器。

解決方案：

1. 使用以下命令刪除現有使用者名稱和密碼條目：

```
no username <username>
```

其中 <username> 被錯誤訊息中的使用者名稱取代。在本例中，將是 `maui-soho-03`。

2. 使用以下命令配置使用者名稱和密碼：

```
username password
```

使用者名稱應與上面顯示的 CHAP 消息中的使用者名稱相同。密碼應與遠端路由器上的密碼匹配。

[常見基於伺服器的 AAA 問題故障排除](#)

4

This section has some simple AAA troubleshooting points.
It can be used to troubleshoot both CHAP and PAP authentication

Enable the following debugs:
debug aaa authentication
and
debug radius
or
debug tacacs

Note: For Radius (prior to 12.2XB) , the debug output will need to be decoded. Use the [Output Interpreter tool](#).
In the radius/tacacs debug output, check to see if you are receiving an Access-Accept from the server. For example:
*Mar 1 05:07:40.310: RADIUS: Received from id 4 172.22.53.201:1645, Access-Accept, len 50

Do you see an Access-Accept?

Yes

No

Check to see if you get a Sendauth failure, which happens only for Radius with two-way authentication. The following debug shows an example:

```
AAA/AUTHEN/START (776188141): port='BR0:1' list=""  
action=SENDAUTH service=PPP  
AAA/AUTHEN/START (776188141): using "default" list  
AAA/AUTHEN/START (776188141): Method=radius  
(radius)  
AAA/AUTHEN/SENDAUTH (776188141): missing  
password for maui-soho-03  
AAA/AUTHEN/SENDAUTH (776188141): Failed  
sendauthen for maui-soho-03  
AAA/AUTHEN (776188141): status = FAIL  
AAA/AUTHEN/START (776188141): no methods left to try  
AAA/AUTHEN (776188141): status = ERROR  
AAA/AUTHEN/START (776188141): failed to authenticate  
BR0:1 CHAP: Username maui-soho-03: lookup failure
```

Configure one-way authentication by configuring the command **ppp authentication chap callin** on the dialout side

If you see an Access-Accept and CHAP authentication still fails, then contact the Cisco TAC for further troubleshooting

Please perform the following general troubleshooting steps:

- 1) Check if you have connectivity with the AAA server (try to ping the AAA server from the local router)
- 2) Check if the AAA server is correctly specified using the radius-server host or tacacs-server host command
- 3) Check if the secret key used between the local router and the AAA server is correct (use the command radius-server key and tacacs-server key)
- 4) Check if the local router is correctly identified in the AAA server configuration
- 5) Check if the username and password that is used for authentication is correctly configured on the AAA server

For more information refer to the Radius/Security Technical Tips Page

注意：本文檔不作為AAA故障排除資源。有關AAA故障排除的詳細資訊，請參閱以下資源：

- [AAA操作](#)

- [RADIUS](#)
- [TACACS](#)

[問題：PAP身份驗證適用於PPP，但MsCHAPv2失敗](#)

您可能無法向ACS伺服器進行身份驗證，因為ACS伺服器未收到身份驗證請求，從而導致會話失敗。此行為在Cisco錯誤ID [CSCee04466](#)(僅限[註冊](#)客戶)下觀察和記錄。解決方法是，將RADIUS伺服器用於PPP會話。但是，請將TACACS+伺服器保留在路由器上以供管理之用。

[相關資訊](#)

- [瞭解debug ppp negotiation輸出](#)
- [瞭解和設定 PPP CHAP 驗證](#)
- [使用ppp chap hostname和ppp authentication chap callin命令進行PPP身份驗證](#)
- [設定PPP密碼驗證通訊協定\(PAP\)並疑難排解](#)
- [撥號和存取技術支援](#)
- [技術支援與文件 - Cisco Systems](#)