PPP（CHAP または PAP）認証に関するトラブルシューティング

目次

概要

Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）の認証の問題は、ダイヤルアップ リンクの障害の最も一般的な原因の 1 つです。 このドキュメントでは、PPP 認証に関する問題のトラブルシューティング手順を紹介しています。

前提条件

- debug ppp negotiation および debug ppp authentication をイネーブルにします。
- PPP 認証フェーズは、Link Control Protocol（LCP; リンク制御プロトコル）フェーズが完了してオープン状態になるまで開始されません。 debug ppp negotiation が LCP がオープンであることを示さない場合、先に進む前にこの問題を解決する必要があります。
- PPP 認証は、両側で設定されている必要があります。 必要に応じて、次のコマンドを発行します。双方向のチャレンジ ハンドシェイク認証プロトコル（CHAP）認証を設定する場合は、両方のルータで ppp authentication chap を発行します。単方向認証の場合は、発呼側ルータで ppp authentication chap callin コマンドを発行します。PAP 認証の場合は、両方のルータで ppp authentication pap を発行します。

用語

- **ローカル マシン**（またはローカル ルータ）：これは、現在デバッグ セッションが実行されているシステムです。 あるルータから他のルータにデバッグ セッションを移動した場合、「ローカル マシン」という用語は、新たに対象となったルータに対して適用されます。
- **ピア**：ポイント ツー ポイント リンクの他方の端を意味します。 したがって、このデバイスはローカル マシンではありません。たとえば、RouterA で debug ppp negotiation コマンドを発行する場合、これがローカル マシンとなり、RouterB がピアになります。 ただし、デバッグの対象を RouterB に変更した場合は、RouterB がローカル マシンになり、RouterA がピアになります。

注: ローカル マシンとピアという用語は、クライアント サーバの関係を意味するものではありません。 デバッグ セッションがどこで実行されているかによって、ダイヤルイン クライアントはローカル マシンまたはピアになります。

要件

次の項目に関する知識があることが推奨されます。

- debug ppp negotiation の出力を読み取って理解できる必要があります。 詳細は、『debug ppp negotiation 出力について』を参照してください。

使用するコンポーネント

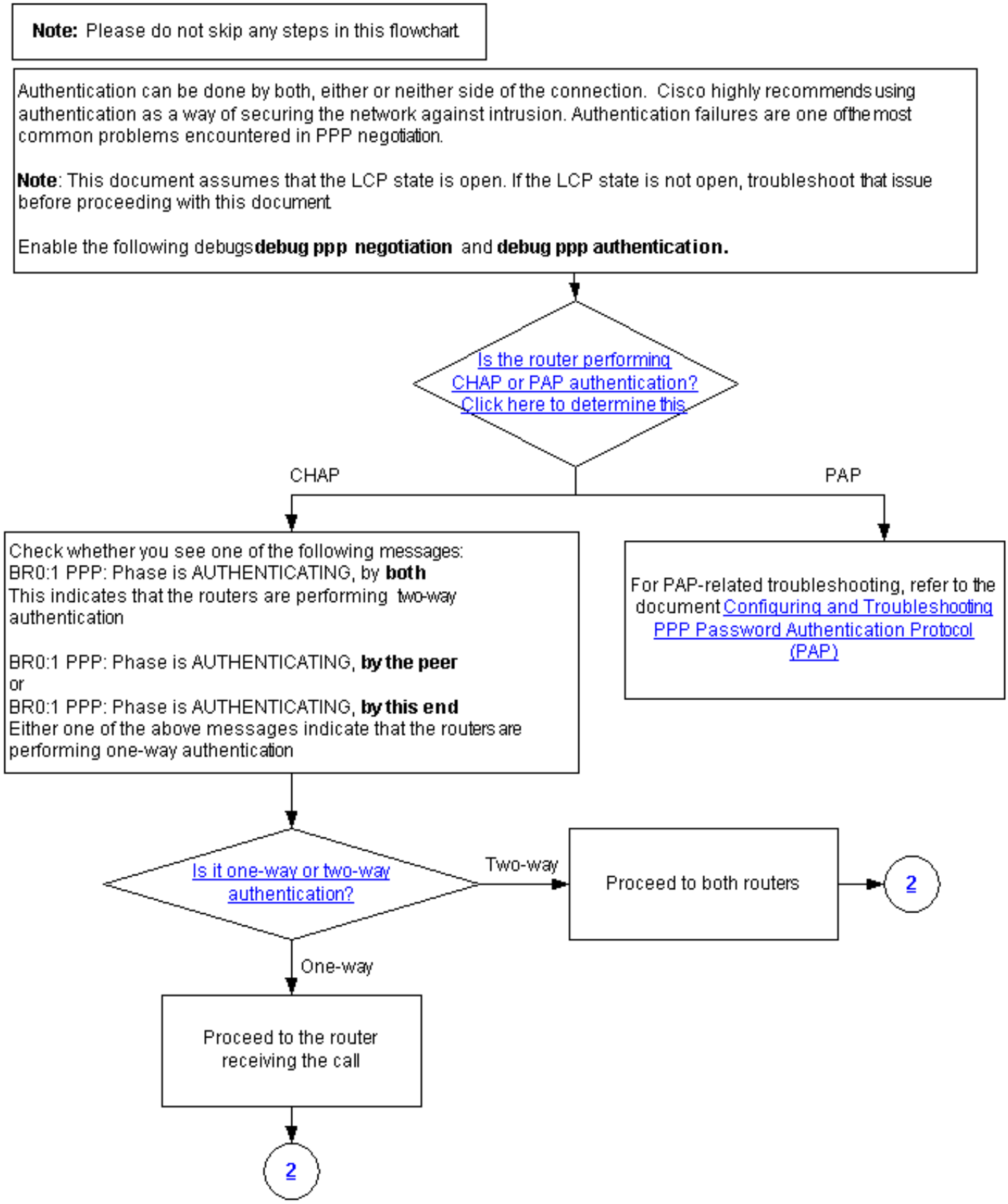
このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

トラブルシューティング フローチャート

この文書には、トラブルシューティングに役立つように、いくつかのフローチャートを掲載しています。 次のフローチャートに進むには、丸印の中の番号をクリックしてください。



ルータで、CHAP 認証または PAP 認証を実行していますか。

ルータで CHAP 認証または PAP 認証が実行されているかどうかを判別するには、**debug ppp negotiation** および **debug ppp authentication** の出力の次の行を調べます。

CHAP

AUTHENTICATING フェーズで CHAP を探します。

```
*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

AUTHENTICATING フェーズで PAP を探します。

```
*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"
```

ルータで、単方向または双方向の CHAP 認証を実行していますか

debug ppp negotiation の出力で次のメッセージのいずれかを探します。

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

上記のメッセージは、ルータが双方向の認証を実行していることを示しています。

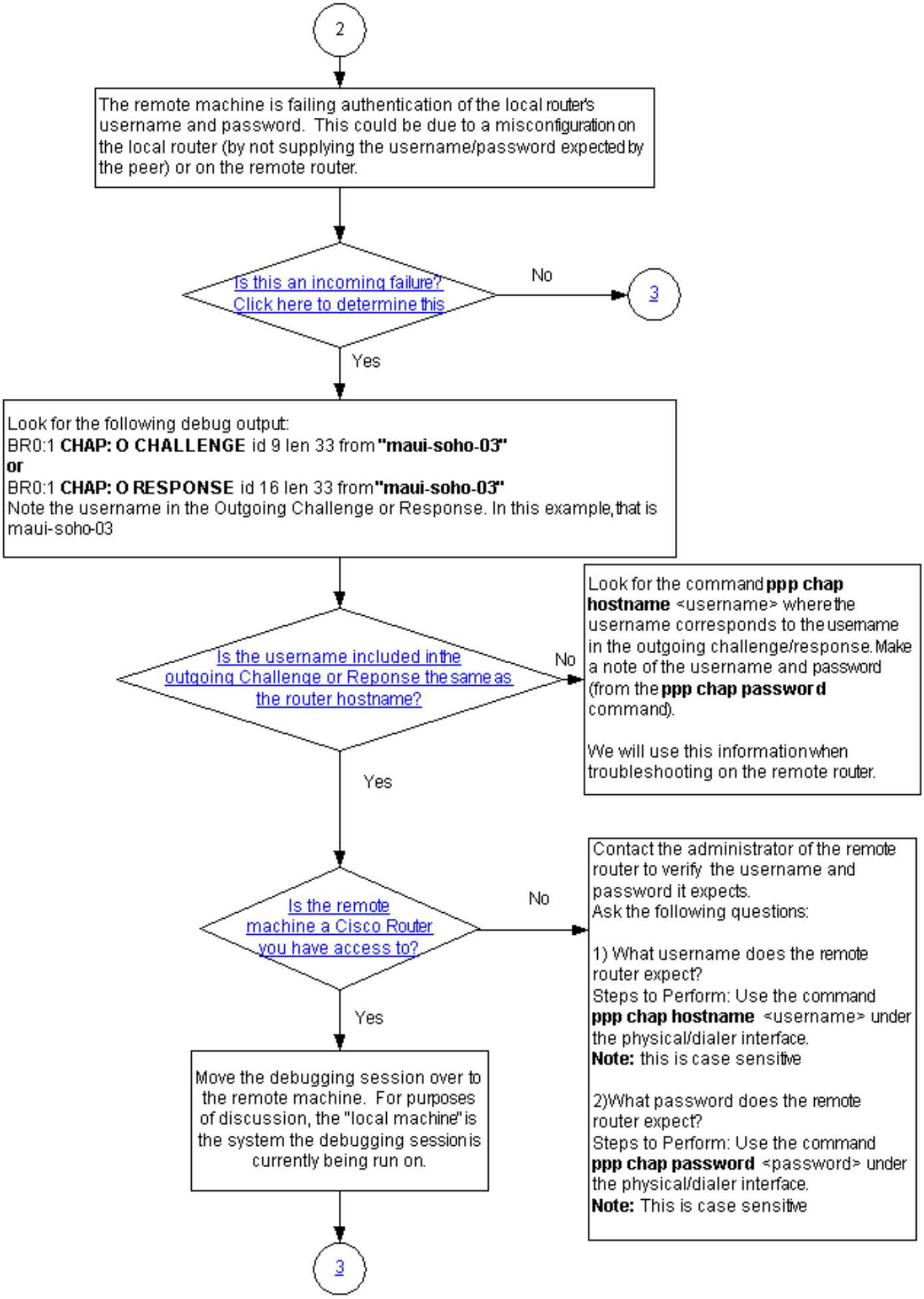
次のメッセージは、いずれもルータが単方向の認証を実行していることを示しています。

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

または

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

着信に関する障害ですか



着信メッセージ termreq または failure が受信されていないかどうかを調べます。「I」はこのメ

ッセージが着信（incoming）メッセージであることを示しています。

```
BR0:1 LCP: I TERMREQ
```
または

```
BR0:1 CHAP: I FAILURE
```
着信に関する障害は、ピア側でローカル ルータのユーザ名とパスワードの認証ができなかったことを意味しています。 これには、ローカル ルータまたはリモート ルータ側での設定ミス（ピア側が期待していたユーザ名とパスワードが指定されなかった）が考えられます。

発信チャレンジまたは応答のユーザ名はホスト名と同じですか。

debug ppp negotiation の出力で次のメッセージのいずれかを探します。

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

```
BR0:1 CHAP: O RESPONSE id 16 len 33 from "maui-soho-03"
```
発信チャレンジまたは応答の中のユーザ名に注意してください。 この例では、**maui-soho-03** になります。 これは、認証に使用されるユーザ名およびパスワードがリモート側で想定されているものと一致することを確認するのに必要です。 たとえば、ローカル ルータが自身をピアに対して A であると示しているものの、ピア側では B を期待していた場合、認証は正しく行われません。

発信チャレンジのユーザ名がホストネームと同じでない場合は、ppp chap hostname <username> コマンドを調べます。ここで使用するユーザ名は発信チャレンジのユーザ名です。このユーザ名とパスワード（**ppp chap password** コマンドで指定されているもの）をメモしてください。 この情報は、リモート ルータのトラブルシューティングの際に使用します。

リモート マシンはアクセス可能な Cisco ルータですか。

ローカル ルータで着信障害が受信されていると判断できたことから、障害はピア側で起きていることが分かります。 リモートの Cisco ルータにアクセスできる場合は、そのデバイスでトラブルシューティングを行います。

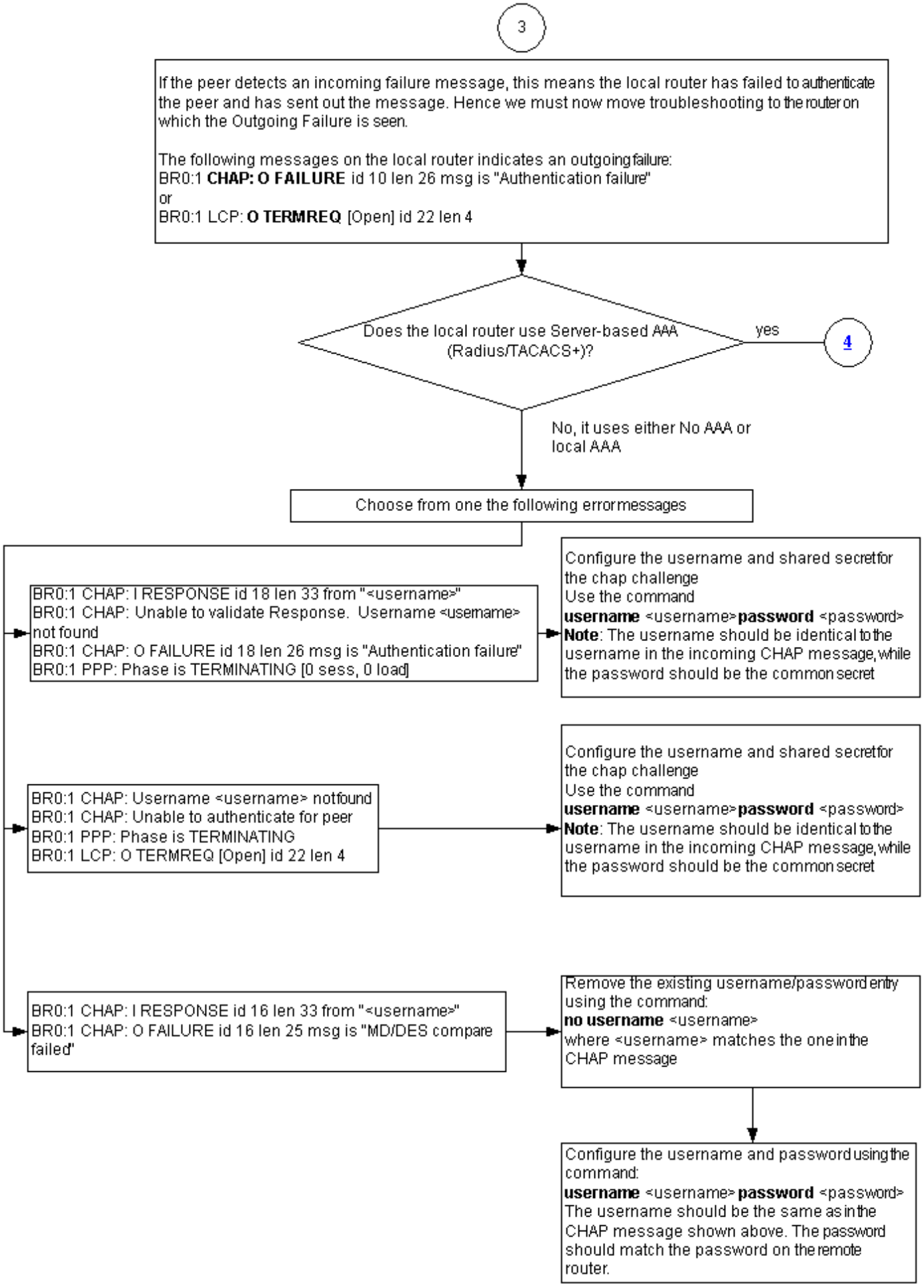
リモート ルータにアクセスできない場合は、そのルータの管理者に連絡して、ルータが期待しているユーザ名とパスワードを確認してください。

次の質問に答えてください。

1. リモート ルータが期待しているユーザ名は何か。物理インターフェイスまたはダイヤラ インターフェイスで ppp chap hostname <username> コマンドを実行します。 ここでは、リモート ルータの管理者から指定されたユーザ名を設定します。**注:** 大文字と小文字を区別して入力します。
2. リモート ルータが期待しているパスワードは何か。物理インターフェイスまたはダイヤラ インターフェイスで ppp chap password <password> コマンドを実行します。**注:** 大文字と小文字を区別して入力します。

詳細は、ドキュメント『ppp chap hostname および ppp authentication chap callin コマンドを使用した PPP 認証』を参照してください。

発信 CHAP の障害のトラブルシューティング



ピア側で着信障害のメッセージが検出された場合は、ローカル ルータがピアの認証に失敗し、このメッセージを送信したことを意味しています。 したがって、発信障害を起こしているルータを

トラブルシューティングする必要があります。

ローカル ルータ上の次のメッセージは、発信障害を示しています。

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

```
BR0:1 LCP: O TERMREQ [Open] id 22 len 4
```
ルータが AAA を使用しない、またはローカル AAA しか使用しない場合

ルータ側でサーバベースの認証、許可、およびアカウンティング（AAA）システム（Radius または Tacacs+）が使用されていない場合には、ルータで AAA がまったく使用されていない場合と、ローカル AAA が使用されている場合とがあります。 デバッグ出力に次のメッセージのいずれかが表示されているかどうか、確認してください。

Unable to Validate Response

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]
```
ユーザ名の不一致は、次の 2 つの理由で発生します。

1. ローカル ルータ側で期待しているユーザ名がピア側から渡されない。 たとえば、RouterA というユーザ名を期待（および設定）しているのに、ピア側では RouterB をいう名前を使用している場合です。 ピア側から送られるユーザ名とパスワードを設定するか、ピア側の名前を正しいものに訂正します。
2. ローカル ルータにユーザ名が設定されていない。 ピアから渡されるユーザ名がローカル ルータ側で期待していたものと一致する場合は、そのユーザ名とパスワードを設定します。

この問題は、ピア側で ppp chap hostname コマンドを使用して、ルータのホスト名以外のユーザ名を設定しているときに最も頻繁に発生します。

コマンド username <username> password <password> を使用します。<username> は、上記のエラー メッセージ内にあるユーザ名で置き換えます。

Username <username> Not Found

Unable to Authenticate for Peer

```
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.
```
ユーザ名の不一致は、次の 2 つの理由で発生します。

1. ローカル ルータ側で期待しているユーザ名がピア側から渡されない。 たとえば、

RouterA（および設定）という名前を使用している場合です。 ただし、ピア側では RouterB という名前を使用します。 ピア側から送られるユーザ名とパスワードを設定するか、ピア側のユーザ名を正しいものにアップデートします。
2. ローカル ルータにユーザ名が設定されていない。 ピアから渡されるユーザ名がローカル ルータ側で期待していたものと一致する場合は、そのユーザ名とパスワードを設定します。

この問題は、ピア側で ppp chap hostname コマンドを使用して、ルータのホスト名以外のユーザ名を設定しているときに最も頻繁に発生します。

コマンド **username <username> password <password>** を使用します。**<username>** は、上記のエラー メッセージ内にあるユーザ名で置き換えます。

MD/DES Compare Failed

```
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"
```

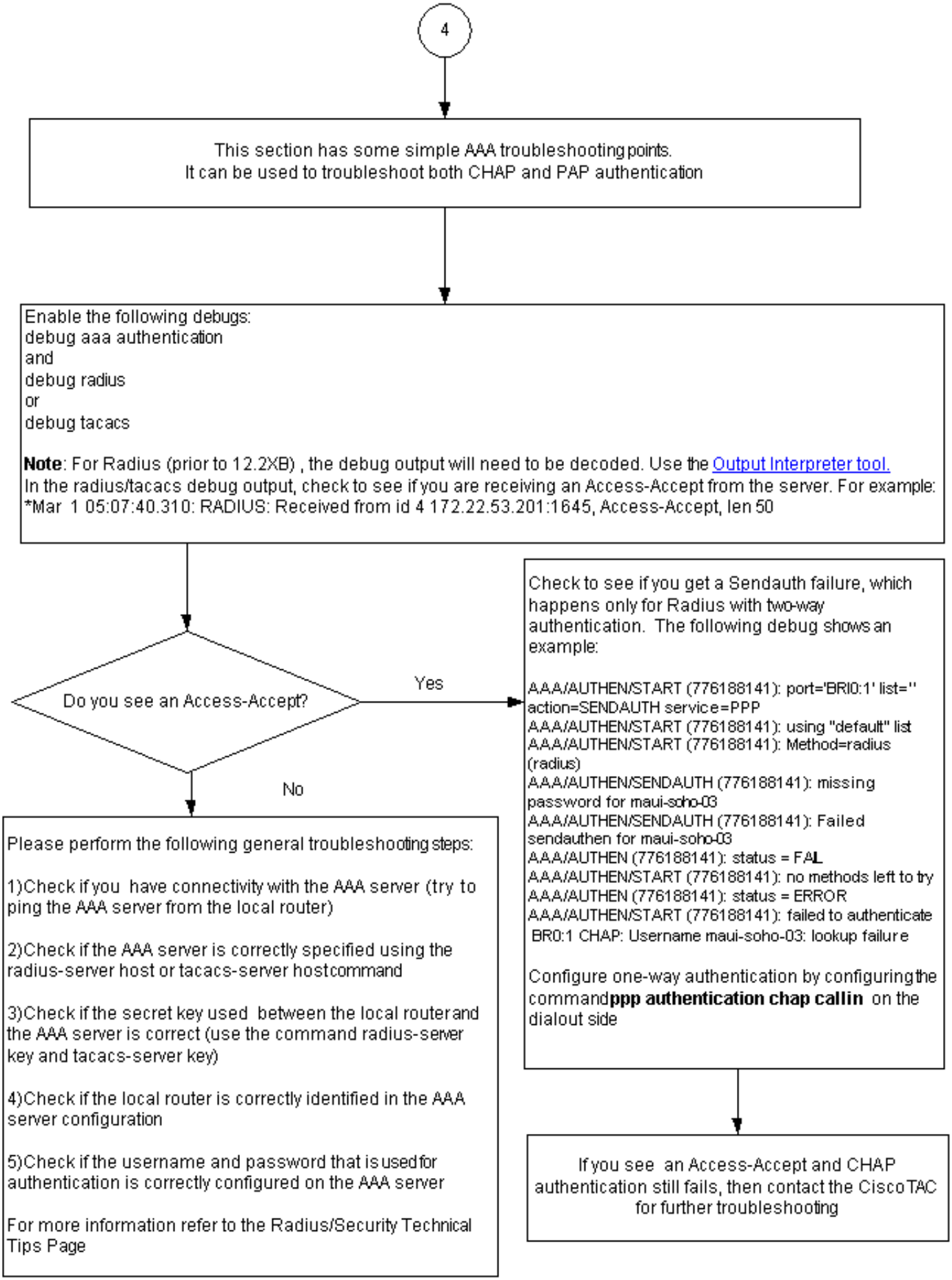
このエラーは、パスワードの不一致によって発生します。 これには、次の 2 つの理由が考えられます。

1. ローカル ルータ側で期待しているパスワードがピア側から渡されていない。 たとえば、*LetmeIn* というパスワードを期待（および設定）しているのに、ピア側では *letmein* をいうパスワードを使用している場合です。 ピア側から送られるユーザ名とパスワードで再設定するか、ピア側のユーザ名を正しいものに訂正します。
2. ローカル ルータにパスワードが正しく設定されていない。 ピア側から送られるパスワードの方が正しいと確認できた場合は、ローカル ルータ側を再設定します。

解決策：

1. 次のコマンドを使用して、既存のユーザ名とパスワードのエントリを削除します。
   no username *<username>* ここで、**<username>** をエラー メッセージで示されているユーザ名に置き換えます。 この例では、maui-soho-03 になります。
2. 次のコマンドを使用して、ユーザ名とパスワードを設定します。
   username *<username>* **password** *<password>* このユーザ名は、上記の CHAP メッセージの中にあるものと同じである必要があります。 また、パスワードはリモート ルータ側のパスワードと同じものである必要があります。

一般的なサーバベースの AAA に関する問題のトラブルシューティング



注: この文書は、AAA のトラブルシューティングを目的とするものではありません。 AAA のトラブルシューティングに関する詳細は、次のドキュメントを参照してください。

- AAA の処理

- RADIUS
- TACACS

問題： PAP 認証は PPP では動作するが、MsCHAPv2 では失敗する

ACS サーバが認証要求を受信しなかったため、セッションが失敗して ACS サーバを認証できない場合があります。 この動作は、Cisco Bug ID CSCee04466（登録ユーザのみ）に記述されています。 回避策として、PPP セッション用に RADIUS サーバを使用します。 ただし、ルータの TACACS+ サーバを管理上の目的でのみ使用してください。

関連情報

- debug ppp negotiation の出力について
- PPP CHAP 認証の理解および設定
- ppp chap hostname コマンドおよび ppp authentication chap callin コマンドを使用する PPP 認証
- PPP パスワード認証プロトコル（PAP）の設定とトラブルシューティング
- ダイヤルおよびアクセスに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems