PPP（CHAP 或 PAP）认证故障排除

Contents

Introduction

点对点协议 (PPP) 身份验证问题是拨号链路故障的最常见原因之一。本文为PPP认证问题提供一些故障检修程序。

Prerequisites

- Enable (event) **debug ppp协商**和**debug ppp authentication**。
- PPP认证阶段不开始，直到链路控制协议(LCP)阶段完成并且在打开状态。如果**debug ppp协商不**表明LCP是开放的，在进行前排除此问题故障。
- 在两边必须配置PPP认证。发出这些命令如适当：在两路由器的ppp authentication chap，双向质询握手验证协议(CHAP)认证的。在呼叫路由器的ppp authentication chap callin，单向验证的。在两路由器的ppp authentication pap， PAP认证的。

术语

- **本地设备**(或本地路由器) -这是调试会话当前运行的系统。您从一个路由器移动调试会话向其他，请适用于术语本地设备另一个路由器。
- **对等体**-点到点链路的另一个结尾。因此，设备不是本地设备。例如，如果发出debug ppp negotiation命令在RouterA，然后它是本地设备，并且RouterB是对等体。然而，如果转移调试到RouterB，然后它成为本地设备，并且RouterA成为对等体。

Note: 术语本地设备和对等体不暗示一个客户端服务器关系。根据调试会话运行的地方，拨入客户端可能是本地设备或对等体。

Requirements

Cisco建议您有此题目知识：

- 您一定能阅读和了解debug ppp协商输出。请参见了解debug ppp协商输出欲知更多信息的本文。

Components Used

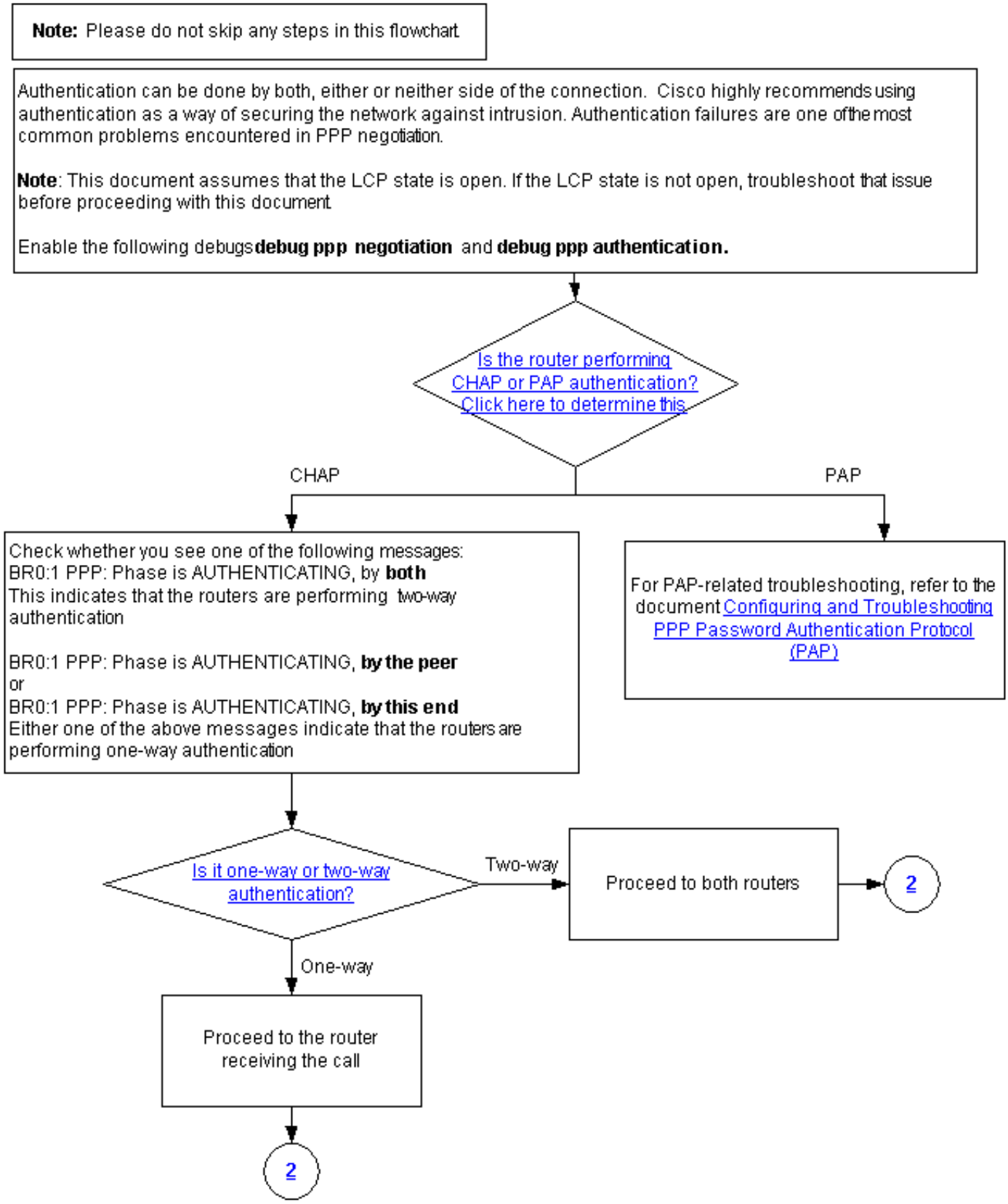
This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

故障检修流程图

本文包括一些流程图协助解决排除故障。您能进行到下张流程图通过单击在被编号的圈子。



路由器是否进行 CHAP 或 PAP 验证？

要确定路由器是否进行CHAP或PAP认证，请寻找在输出的**debug ppp协商**和**debug ppp authentication**的这些线路：

CHAP

寻找在验证的阶段的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

寻找在验证的阶段的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"
```

路由器进行单向或双向CHAP验证？

寻找这些消息之一在debug ppp协商输出中：

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

上述消息表明路由器进行双向认证。

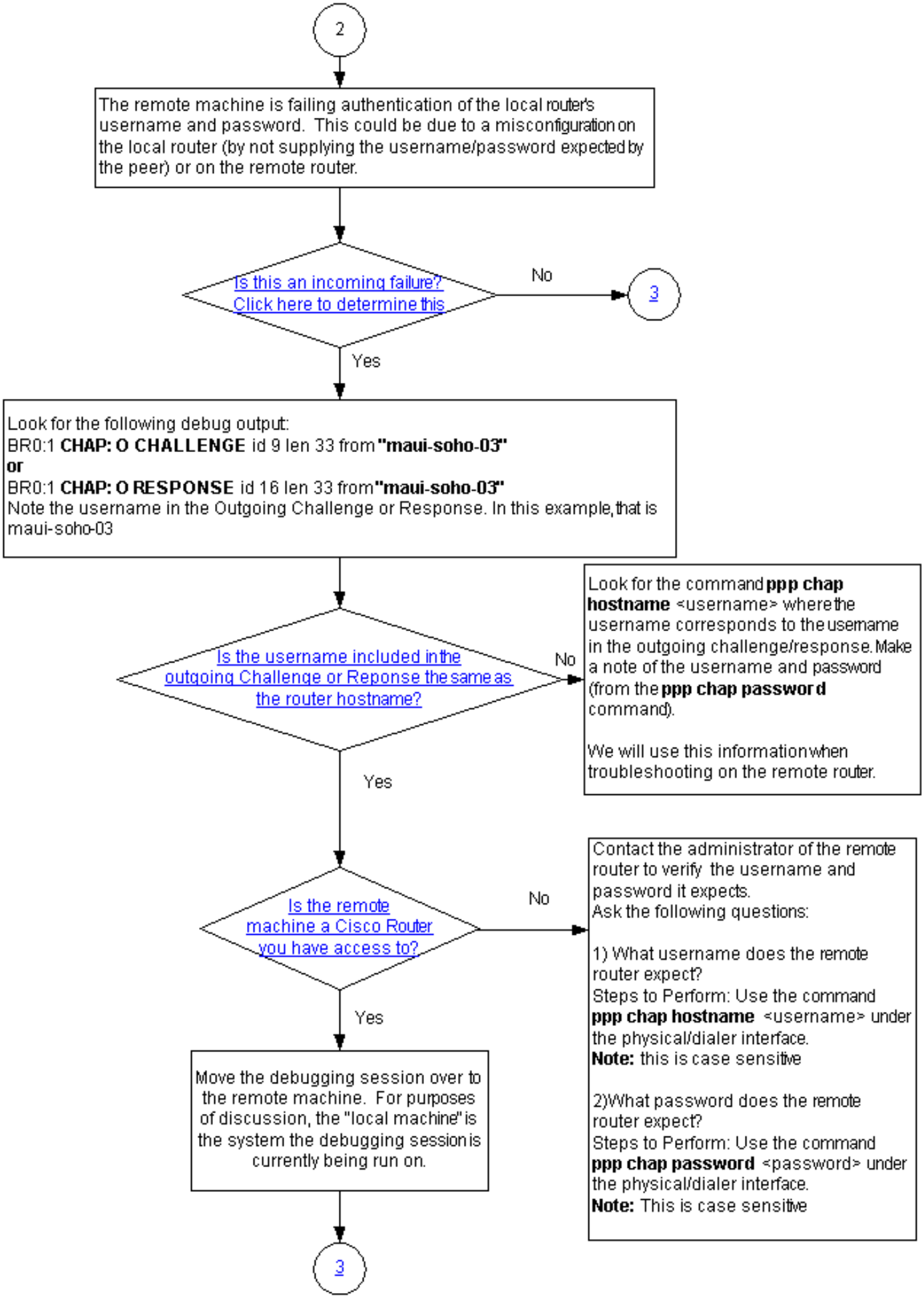
二者之一下面其中一个的消息表明路由器进行单向验证：

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

或

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

这是传入的故障吗?



确认是否收到流入termreq或故障消息。切记“我”表明消息是一个流入的消息：

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

或

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

一个进入故障表明对等体是失败验证本地路由器的用户名和密码。这可能归结于一误配置在本地路由器(通过不供应对等体预计的用户名和密码)或在远程路由器。

在流出的挑战或回应的用户名同主机名一样？

寻找以下在**debug ppp**协商输出中：

```
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"
```

注释在流出的挑战或回应的用户名。在本例中，它是**maui-soho-03**。您需要此验证用于认证的用户名和密码匹配远端预计的那个。例如，如果本地路由器识别自己对对等体作为A，但是对等体期待B，然后认证发生故障。

如果在流出的挑战的用户名不是相同的作为主机名-，请寻找ppp chap hostname命令 *<username>*，用户名对应于在流出的挑战的用户名。记录下来用户名和密码(在accompanying ppp chap password命令)。当您排除远程路由器故障，您将使用此信息。

远端计算机是否是您访问的Cisco路由器？

因为我们确定本地路由器接受了一个进入故障，我们知道故障在对等体发生。如果访问远程Cisco路由器，则请排除故障在该设备。

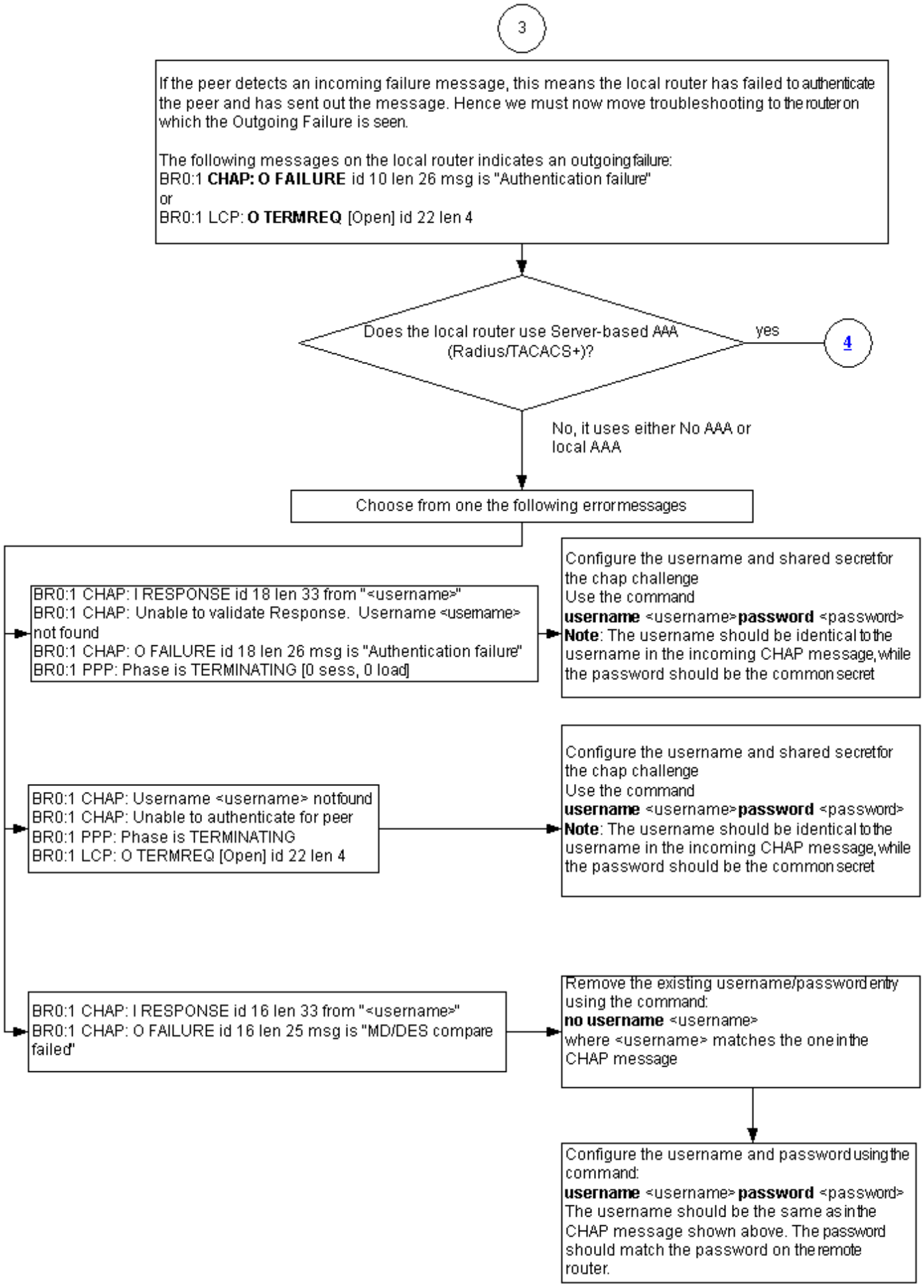
如果不访问远程路由器，与该路由器的管理员联系验证预计的用户名和密码。

询问这些问题：

1. 远程路由器期待什么用户名？请使用ppp chap hostname *<username>*命令在物理或拨号程序接口下。配置远程管理员提供的用户名这里。**Note:** 这区分大小写。
2. 远程路由器期望什么密码？请使用ppp chap password *<password>*命令在物理或拨号程序接口下。**Note:** 这区分大小写。

使用ppp chap hostname和ppp authentication chap callin命令，欲知更多信息，请参见本文PPP认证。

排除流出的CHAP故障故障



如果对等体发现一个进入故障消息，这意味着本地路由器未能验证对等体和派出了消息。因此，您必须当前排除指示流出故障的路由器故障。

在本地路由器的这些消息指示一个流出故障：

```
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或仅本地AAA

如果路由器不使用一个基于服务器的验证、授权和记帐(AAA)系统(Radius或TACACS+)，则路由器不能使用AAA或本地AAA。证实您是否在调试输出中看到下列信息之一：

无法验证回应

没找到的用户名*<username>*

```
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]
```

用户名不匹配可以由两个原因导致：

1. 对等体没有供应本地路由器预计的用户名。例如，我们期待(和配置了)用户名RouterA，但是对等体使用了名字RouterB。您能配置对等体发送的用户名和密码或更正对等体与正确的用户名。
2. 本地路由器没有被配置的用户名。如果对等体供应的用户名匹配什么预计的本地路由器，则配置用户名和密码。

除路由器主机名之外时，当对等体使用ppp chap hostname命令配置用户名此问题比较常见。

请使用**password <password>命令用户名的*<username>***，其中*<username>*被在上面错误信息的用户名替换。

没找到的用户名*<username>*

无法为对等体验证

```
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.
```

用户名不匹配可以由两个原因导致：

1. 对等体没有供应本地路由器预计的用户名。例如，我们期待(和配置了)用户名RouterA。然而

，对等体使用了名字RouterB。您能配置对等体发送的用户名和密码或更新对等体与正确的用户名。

2. 本地路由器没有被配置的用户名。如果对等体供应的用户名匹配什么预计的本地路由器，则配置用户名和密码。

除路由器主机名之外时，当对等体使用ppp chap hostname命令配置用户名此问题比较常见。

请使用**password <password>命令用户名的*<username>***，其中*<username>*被在上面错误信息的用户名替换。

MD/DES比较失败

```
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"
```

此错误是由密码不匹配造成的。这能是原因由两个原因：

1. 对等体没有供应本地路由器期望的密码。例如，我们期待(和配置了)密码*Letmein*，但是对等体使用了密码*letmein*。您能重新配置对等体发送的用户名和密码或更正与正确的用户名的对等体。
2. 本地路由器没有正确地被配置的密码。如果验证对等体供应的密码是正确的，则请重新配置本地路由器。

解决方案：

1. 使用此命令，去除现有的用户名和密码条目：

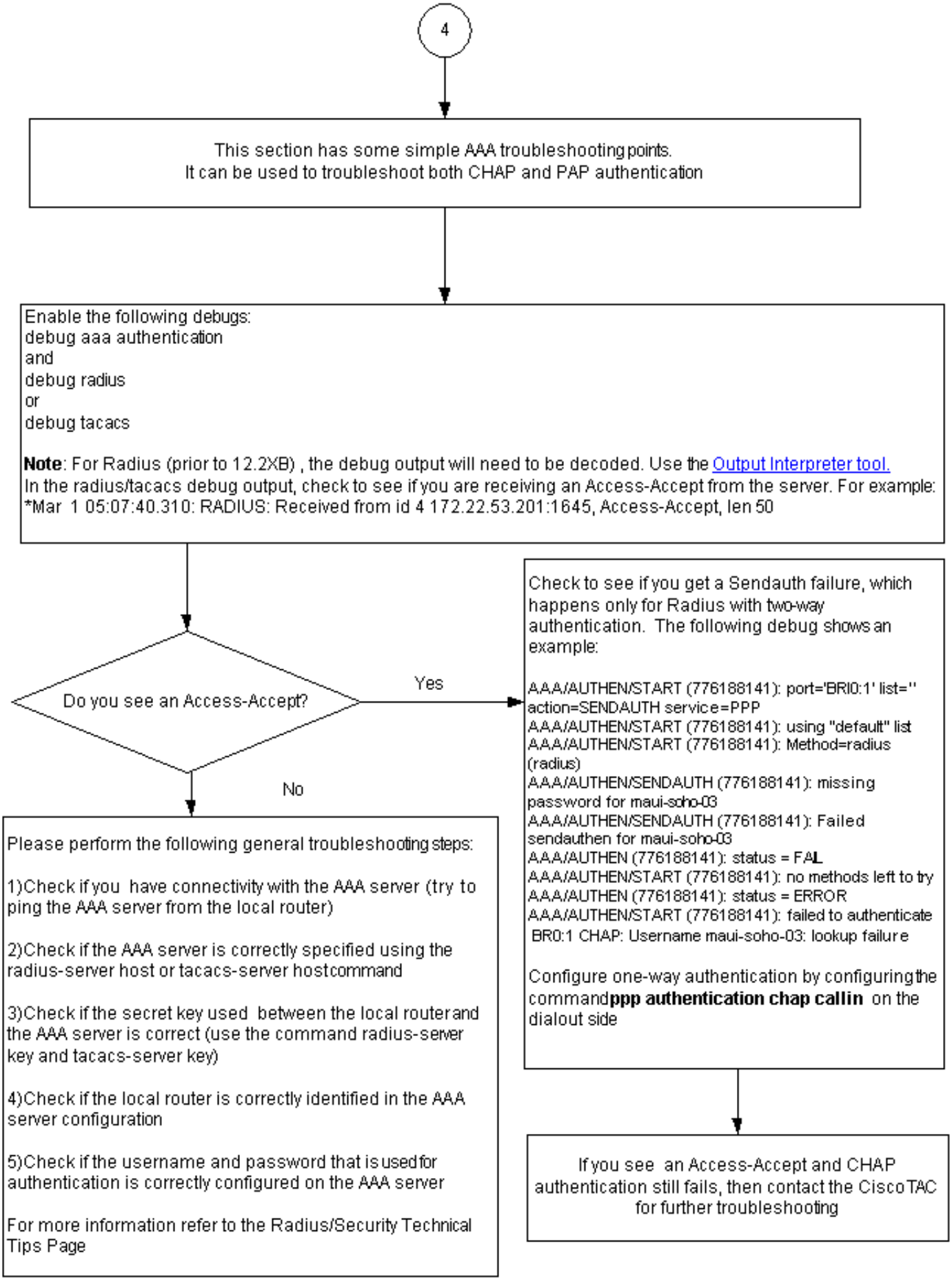
   no username *<username>*

   那里*<username>*被在错误信息的用户名替换。在本例中，那是maui-soho-03。
2. 使用此命令，配置用户名和密码：

   username *<username>* **password** *<password>*

   用户名应该是相同的正如在表示的CHAP消息如上。密码应该匹配在远程路由器的密码。

排除一般基于服务器的AAA问题故障



Note: 本文没有打算作为AAA故障检修资源。关于排除AAA故障的更多信息，请参见以下资源：

- AAA操作

- RADIUS
- TACACS

问题：PAP认证为PPP工作，但是MsCHAPv2发生故障

您也许不能验证到ACS服务器，因为ACS服务器不收到认证请求，引起一次会话发生故障。此工作情况被观察并且被记录在Cisco Bug ID CSCee04466 (仅限注册用户)下。作为解决方法，请使用一个RADIUS服务器PPP会话。然而，为管理请保持TACACS+服务器在路由器。

Related Information

- 了解 debug ppp negotiation 输出
- 了解和配置PPP CHAP认证
- 使用 ppp chap hostname 和 ppp authentication chap callin 命令的 PPP 认证
- PPP 口令认证协议 (PAP) 的配置与故障排除
- 拨号和接入技术支持
- Technical Support & Documentation - Cisco Systems