PPP（CHAP 或 PAP）认证故障排除

目录

简介
先决条件
术语
要求
使用的组件
规则
故障排除流程图
路由器是否进行 CHAP 或 PAP 验证？
路由器进行的是单向还是双向 CHAP 验证？
这是传入的故障吗？
传出的质询或回应中的用户名是否与主机名相同？
您访问的远程计算机是否是 Cisco 路由器？
排除传出的 CHAP 故障
路由器不使用 AAA 或仅使用本地 AAA
排除一般的基于服务器的 AAA 故障
相关信息

简介

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。本文提供一些针对 PPP 身份验证问题的故障排除过程。

先决条件

- 启用 **debug ppp negotiation 和 debug ppp authentication**。
- 直到链路控制协议(LCP)阶段完成并处于打开状态，PPP鉴权阶段才开始。如果 **debug ppp negotiation 未指示 LCP 处于打开状态，则应在解决此问题后再继续。**
- 必须在两端都配置 PPP 身份验证。根据需要发出以下命令：**对于双向质询握手身份验证协议 (CHAP) 身份验证，在两个路由器上使用 ppp authentication chap**。**对于单向身份验证，在主叫路由器上使用 ppp authentication chap callin**。**对于 PAP 身份验证，在两个路由器上使用 ppp authentication pap**。

术语

- **本地计**算机（或本地路由器）— 这是当前正在运行调试会话的系统。将调试会话从一台路由器移动到另一台路由器时，请将术语“本地计算机”应用到另一台路由器。
- **对等** — 点对点链路的另一端。因此，设备不是本地机器。例如，如果在RouterA上发出debug ppp negotiation命令，则它是本地计算机，而RouterB是对等体。但是，如果将调试转移到

RouterB，则它将成为本地计算机，而RouterA将成为对等设备。

注意：术语“本地计算机”和“对等体”不表示客户端 — 服务器关系。根据调试会话的运行位置，拨入客户端可能是本地计算机或对等体。

要求

Cisco 建议您了解以下主题：

- 您必须能够查看和理解 debug ppp negotiation 输出。有关详细信息，请参阅文档了解debug ppp negotiation输出。

使用的组件

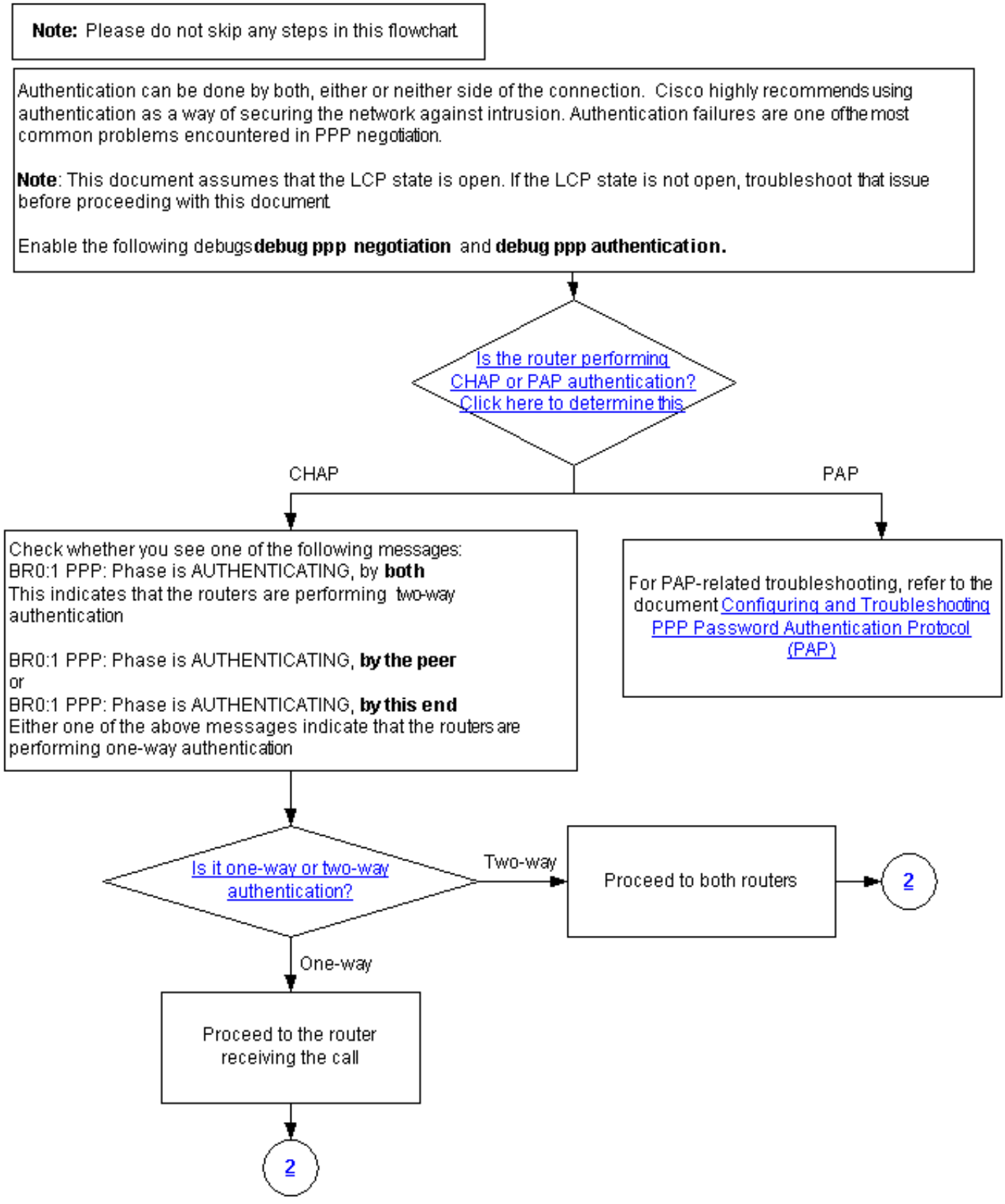
本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

故障排除流程图

本文包括一些流程图来协助解决排错。单击带编号的圆圈，即可转到下一个流程图。



路由器是否进行 CHAP 或 PAP 验证？

要确定路由器是执行CHAP还是PAP身份验证，请在debug ppp negotiation和debug ppp authentication输出中查找以下行：

CHAP

在身份验证阶段查找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

在身份验证阶段查找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"
```

路由器进行的是单向还是双向 CHAP 验证？

在debug ppp negotiation输出中查找以下消息之一：

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

上述消息指示路由器执行的是双向身份验证。

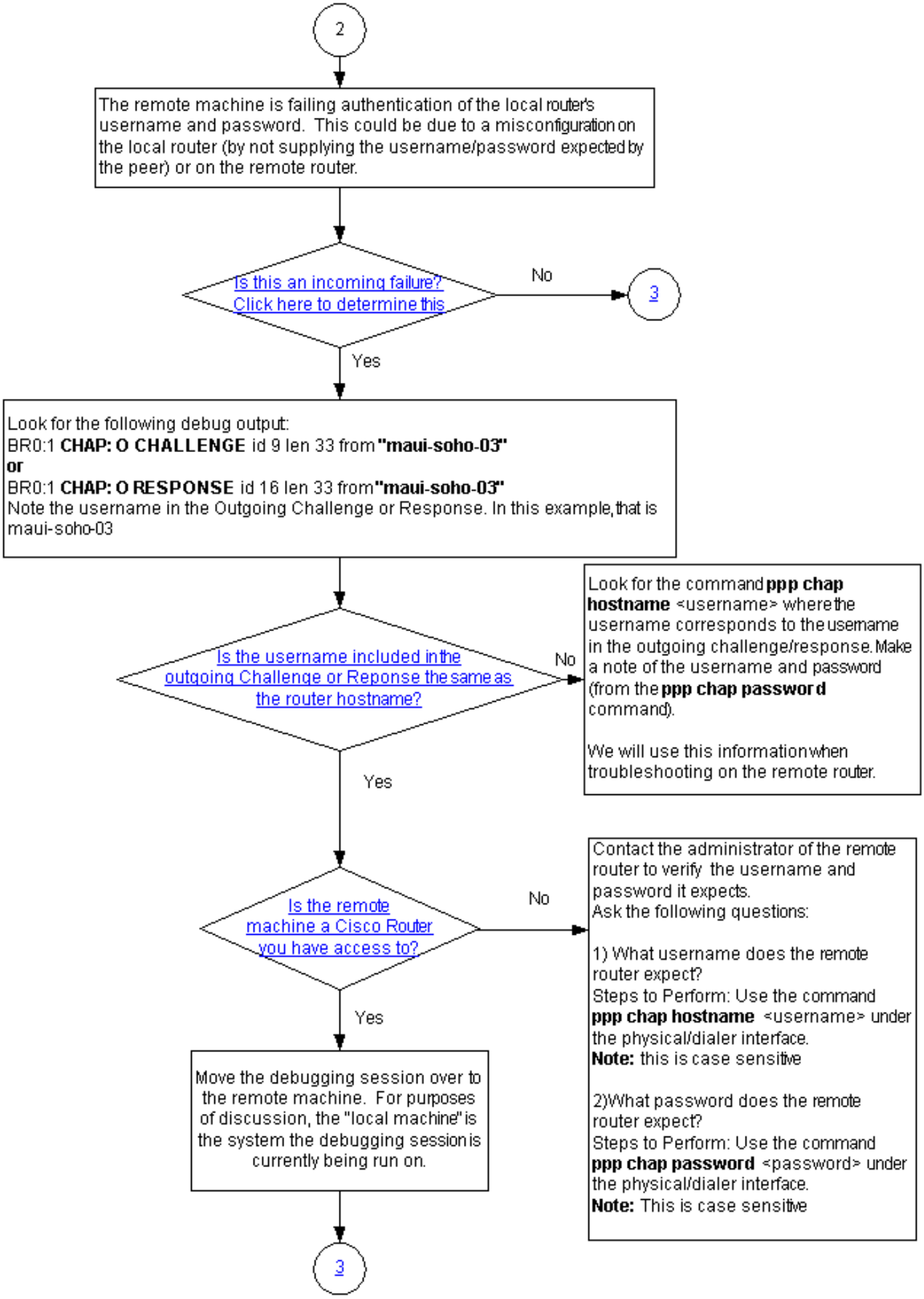
以下消息只要有一条存在即指示路由器执行的是单向身份验证：

```
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？



检查是否收到传入的 termreq 或 failure 消息。请记住，“I”指示消息是传入消息：

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

或

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

传入故障表明对等体无法对本地路由器的用户名和口令进行身份验证。这可能是由本地路由器（未提供对等体所需的用户名和口令）或远程路由器上的错误配置导致的。

传出的质询或回应中的用户名是否与主机名相同？

在 debug ppp negotiation 输出中查找以下行：

```
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"
```

您会看到输出质询或响应中的用户名。在本例中，它是maui-soho-03。您需要此命令来验证用于身份验证的用户名和密码是否与远程端预期的用户名和密码匹配。例如，如果本地路由器向对等体将自身标识为 A，而对等体需要的是 B，则身份验证失败。

如果传出质询中的用户名与主机名不同，请查找 ppp chap hostname <username> 命令，其中 username 与传出质询中的用户名相对应。记下用户名和口令（在附带的 ppp chap password 命令中）。 在对远程路由器进行故障排除时，您将使用此信息。

您访问的远程计算机是否是 Cisco 路由器？

由于已确定本地路由器收到传入故障，因此我们知道在对等体上发生了故障。如果您有权访问远程 Cisco 路由器，请在该设备上进行故障排除。

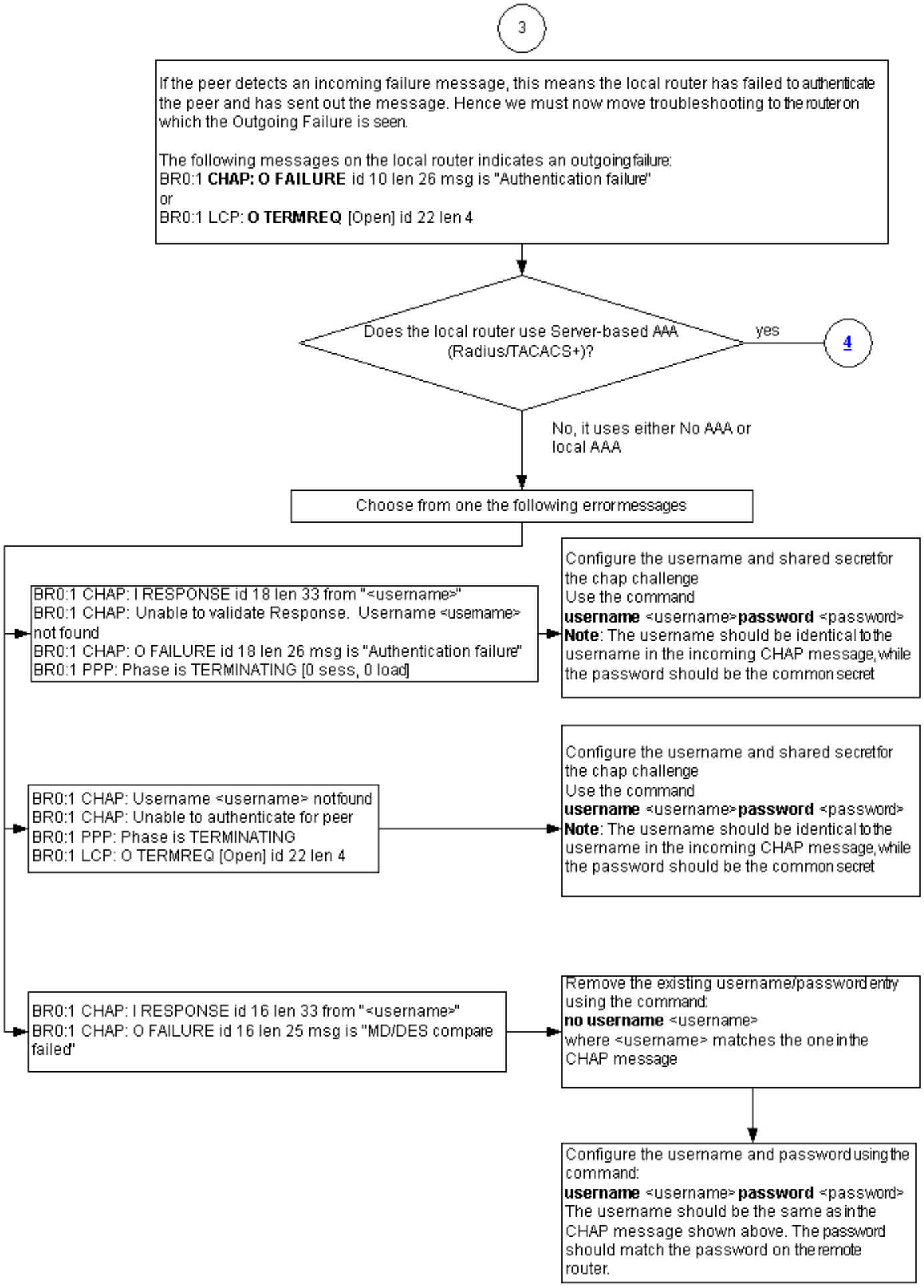
如果您无权访问远程路由器，请与该路由器的管理员联系以确认所需的用户名和口令。

提出以下问题：

1. 远程路由器所需的用户名是什么？在物理或拨号器接口下使用ppp chap hostname <username>命令。在此处配置远程管理员提供的用户名。**注意**：区分大小写。
2. 远程路由器所需的口令是什么？在物理或拨号器接口下使用ppp chap password<password>命令。**注意**：区分大小写。

有关详细信息，请参阅使用 ppp chap hostname 和 ppp authentication chap callin 命令进行 PPP 身份验证一文。

排除传出的 CHAP 故障



如果对等体检测到传入故障消息，这表明本地路由器未能对对等体进行身份验证，因此发出了该消息。因此，您现在必须对指示传出故障的路由器进行故障排除。

本地路由器上的以下消息表示传出故障：

```
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 或仅使用本地 AAA

如果路由器不使用基于服务器的身份验证、授权和记帐 (AAA) 系统（Radius 或 Tacacs+），则路由器不能使用 AAA 和本地 AAA。检查 debug 输出中是否有以下消息之一：

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]
```

导致用户名不匹配的原因有两个：

1. 对等体未提供本地路由器所需的用户名。例如，我们需要（并已配置）用户名 RouterA，但对等体使用的名称是 RouterB。可以配置对等体发送的用户名和口令，或者使用正确的用户名更正对等体。
2. 本地路由器未配置用户名。如果对等体提供的用户名与本地路由器所需的用户名匹配，则配置用户名和口令。

当对等体使用 **ppp chap hostname 命令配置路由器主机名之外的用户名时，通常会发生此问题。**

使用**username *<username>* password *<password>***命令，其中*<username>*将替换为上*述错*误消息中的用户名。

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.
```

导致用户名不匹配的原因有两个：

1. 对等体未提供本地路由器所需的用户名。例如，我们期望（并配置）用户名RouterA。但是

，对等体使用了名称RouterB。您可以配置对等体发送的用户名和密码，或者使用正确的用户名更新对等体。
2. 本地路由器未配置用户名。如果对等体提供的用户名与本地路由器所需的用户名匹配，则配置用户名和口令。

当对等体使用 ppp chap hostname **命令配置路由器主机名之外的用户名时，通常会发生此问题。**

使用username *<username>* password *<password>*命令，其中*<username>*将替换为上*述错*误消息中的用户名。

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"
```

此错误是由口令不匹配造成的。这可能由两个原因导致：

1. 对等体未提供本地路由器所需的口令。例如，我们需要（并已配置）口令 LetmeIn，但对等体使用的口令是 letmein。可以重新配置对等体发送的用户名和口令，或者使用正确的用户名更正对等体。
2. 本地路由器未正确配置口令。如果已验证对等体所提供的口令正确无误，请重新配置本地路由器。

解决方案：

1. 使用以下命令删除现有用户名和密码条目：

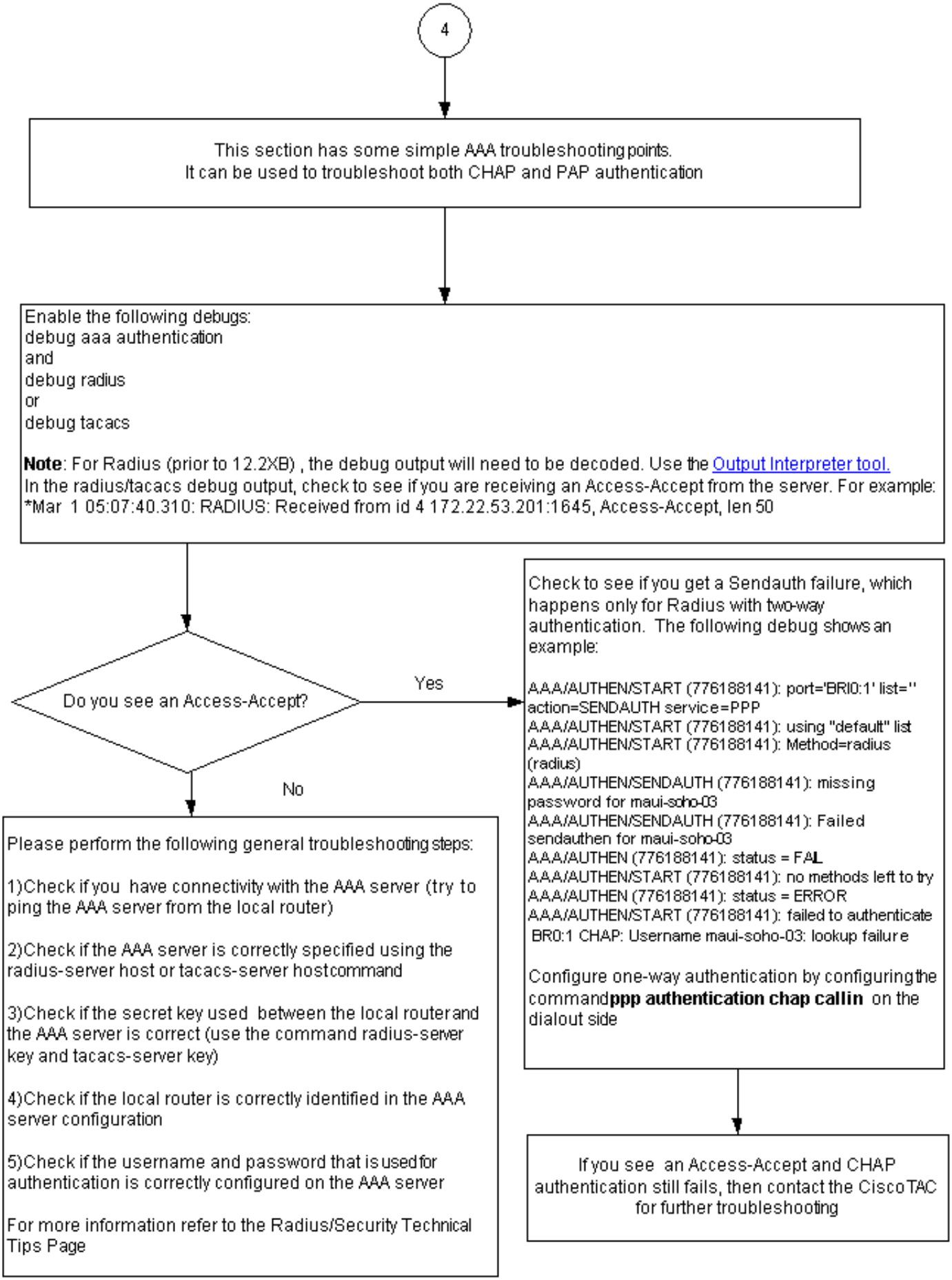
   ```
   no username <username>
   ```

   其中 **<username> 替换为错误消息中的用户名。**在此示例中，该用户名是 maui-soho-03。
2. 使用以下命令配置用户名和密码：

   ```
   username password
   ```

   用户名应与上面显示的 CHAP 消息中的相同。口令应与远程路由器上的口令相匹配。

排除一般的基于服务器的 AAA 故障



注意：本文档不用作AAA故障排除资源。有关 AAA 故障排除的详细信息，请参阅下列资源：

- AAA操作

- RADIUS
- TACACS

问题：PAP身份验证适用于PPP，但MsCHAPv2失败

您可能无法向ACS服务器进行身份验证，因为ACS服务器未收到身份验证请求，导致会话失败。此行为在Cisco Bug ID CSCee04466(仅限注册客户)下观察和记录。 解决方法是使用RADIUS服务器进行PPP会话。但是，请保留TACACS+服务器，以便在路由器上进行管理。

相关信息

- 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
- 技术支持和文档 - Cisco Systems