Troubleshooting de Autenticação de PPP (CHAP ou PAP)

Contents

Introduction

Problemas com a autenticação do Point-to-Point Protocol (PPP) são uma das causas mais comuns das falhas de links dial-up. Este documento fornece alguns procedimentos para Troubleshooting de autenticação PPP.

Prerequisites

- Ative **debug ppp negotiation e debug ppp authentication.**
- A fase de autenticação do PPP não é iniciada até que a fase do LCP (Link Control Protocol) seja concluída e esteja em estado aberto. Se a negociação ppp de depuração não indicar que o LCP está aberto, solucione esse problema antes de continuar.
- A autenticação de PPP deve ser configurada em ambos os lados. Emita estes comandos conforme apropriado:**ppp authentication chap on both routers, para autenticação de Protocolo de Autenticação de Cumprimento de Desafio (CHAP) bidirecional.authentication ppp chap callin no roteador da chamada, para autenticação unidirecional.ppp authentication pap** em ambos os roteadores para a autenticação PAP.

Terminology

- **Máquina local** (ou roteador local) - Este é o sistema no qual a sessão de depuração está sendo executada no momento. À medida que você move a sessão de depuração de um roteador para outro, aplique o termo máquina local ao outro roteador.
- **Peer** - A outra extremidade do link ponto a ponto. Assim, o dispositivo não é a máquina local.Por exemplo, se você emitir o comando **debug ppp negotiation no RoteadorA, ele será a máquina local e o RoteadorB será o peer.** No entanto, se você transferir a depuração para RouterB, ela se tornará a máquina local e o RouterA se tornará o peer.

Observação: os termos máquina local e peer não implicam uma relação cliente-servidor. Dependendo de onde a sessão de depuração é executada, o cliente de discagem pode ser a máquina ou peer local.

Requirements

A Cisco recomenda ter conhecimento deste tópico:

- Você deve estar apto a ler e compreender a saída debug ppp negotiation. Consulte o documento Compreendendo a Saída de negociação de ppp de depuração para obter mais informações.

Componentes Utilizados

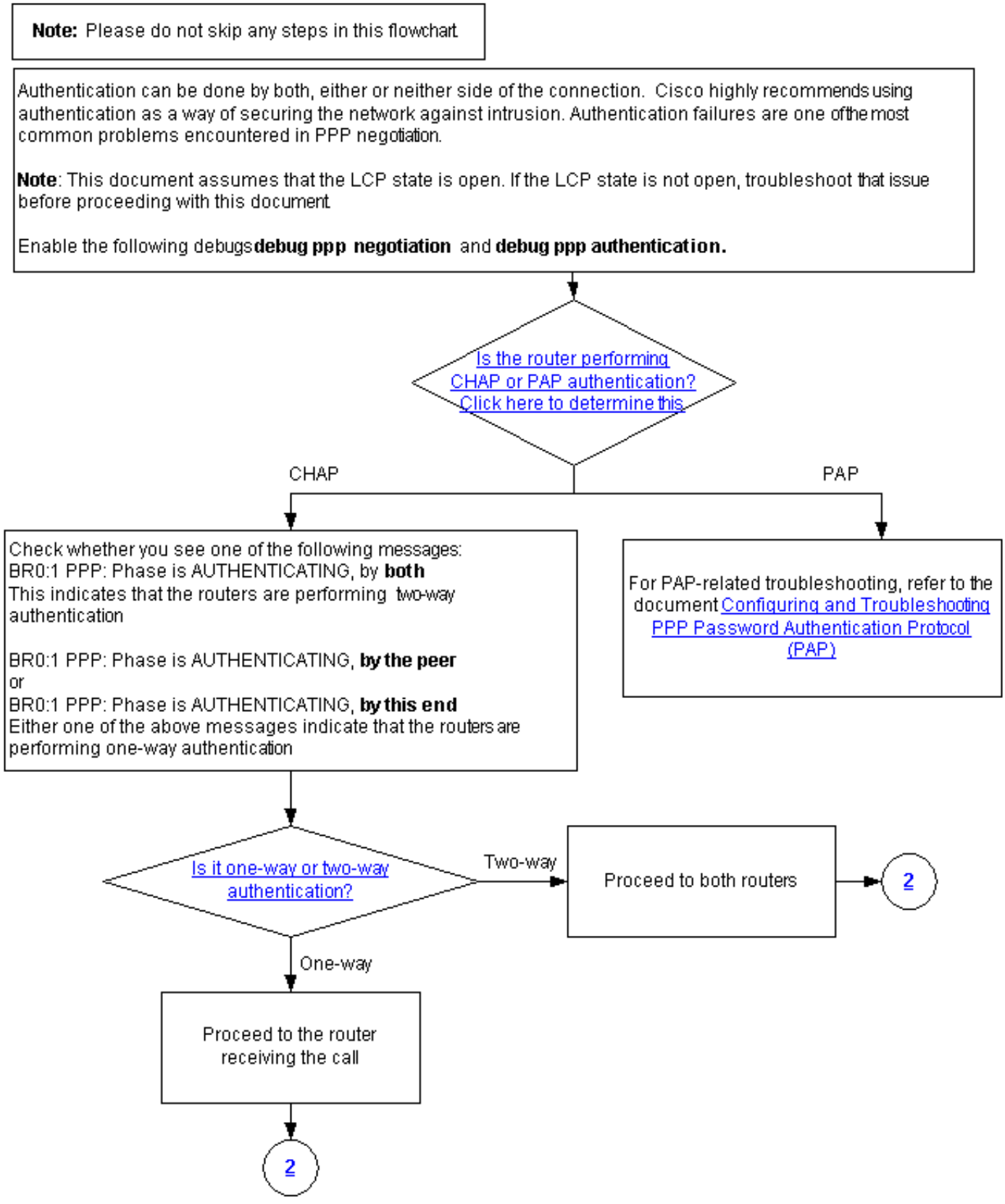
Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Fluxograma de Troubleshooting

Este documento inclui alguns fluxogramas para ajudar no Troubleshooting. Você pode ir para o próximo fluxograma, clicando nos círculos numerados.



O roteador está realizando a autenticação CHAP ou PAP?

Para determinar se o roteador está executando a autenticação CHAP ou PAP, procure estas linhas na saída de **debug ppp negotiation** e **debug ppp authentication**:

CHAP

Procure CHAP na fase AUTHENTICATING:

```
*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

Procure PAP na fase AUTHENTICATING:

```
*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"
```

O roteador está executando uma autenticação de CHAP uni ou bidirecional?

Procure uma destas mensagens na saída **debug ppp negotiation**:

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

A mensagem acima indica que os roteadores estão fazendo uma autenticação em dois sentidos.

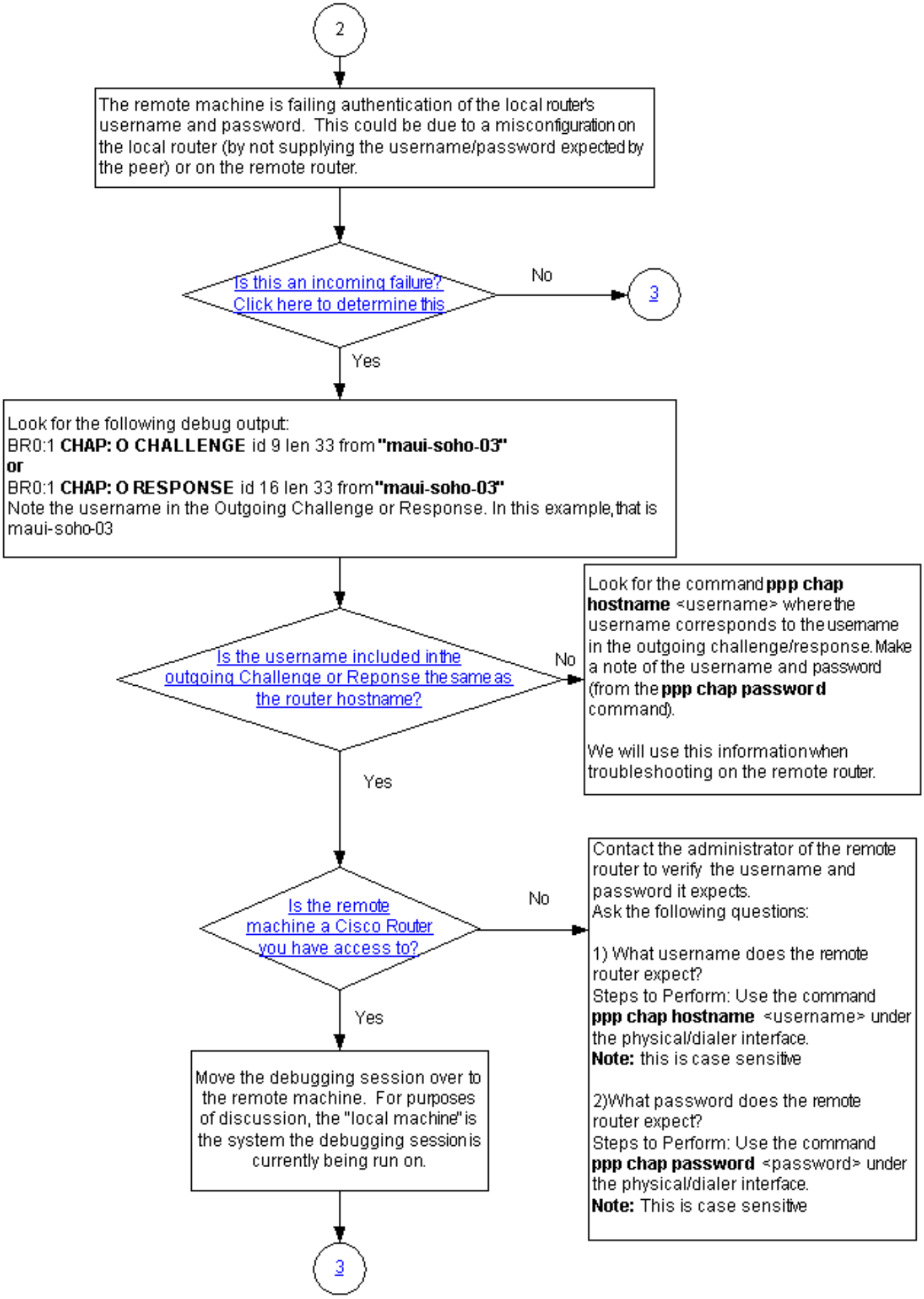
Qualquer uma das mensagens abaixo indica que os roteadores estão executando a autenticação unidirecional:

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

or

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

Esta é uma falha de recebimento?



Verifique se você está recebendo as mensagens de entrada termreq ou failure. Lembre-se de que

"I" indica que a mensagem é de entrada:

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

or

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

Uma mensagem de entrada failure indica que o peer não está autenticando o nome de usuário e a senha do roteador local. Isso pode ocorrer devido a um erro de configuração no roteador local (não fornecendo o nome de usuário e senha esperados pelo peer) ou no roteador remoto.

O nome de usuário no desafio ou resposta de saída é o mesmo nome do host?

Procure o seguinte na saída do comando **debug ppp negotiation:**

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

or

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

Observe o nome de usuário na resposta ou no desafio de saída. Neste exemplo, é maui-soho-03. Você precisa disso para verificar se o nome de usuário e a senha usados para autenticação correspondem ao esperado pelo lado remoto. Por exemplo, se o roteador local se identificar para o peer como A, mas o peer esperar B, a autenticação falhará.

Se o nome de usuário no desafio de saída não for igual ao nome do host, procure o comando ppp chap hostname<username>, onde username corresponde ao nome de usuário no desafio de saída. Anote o nome de usuário e a senha (no comando **ppp chap password que acompanha).** Você usará essas informações ao solucionar problemas do roteador remoto.

A Máquina Remota é um Cisco Router ao Qual Você Tem Acesso?

Uma vez determinado que o roteador local aceitou uma falha recebida, sabe-se que tal falha ocorre no correspondente. Se você tiver acesso ao Cisco Router remoto, resolva os problemas nesse dispositivo.

Se você não tiver acesso ao roteador remoto, contate o administrador desse roteador para verificar o nome de usuário e a senha esperados.

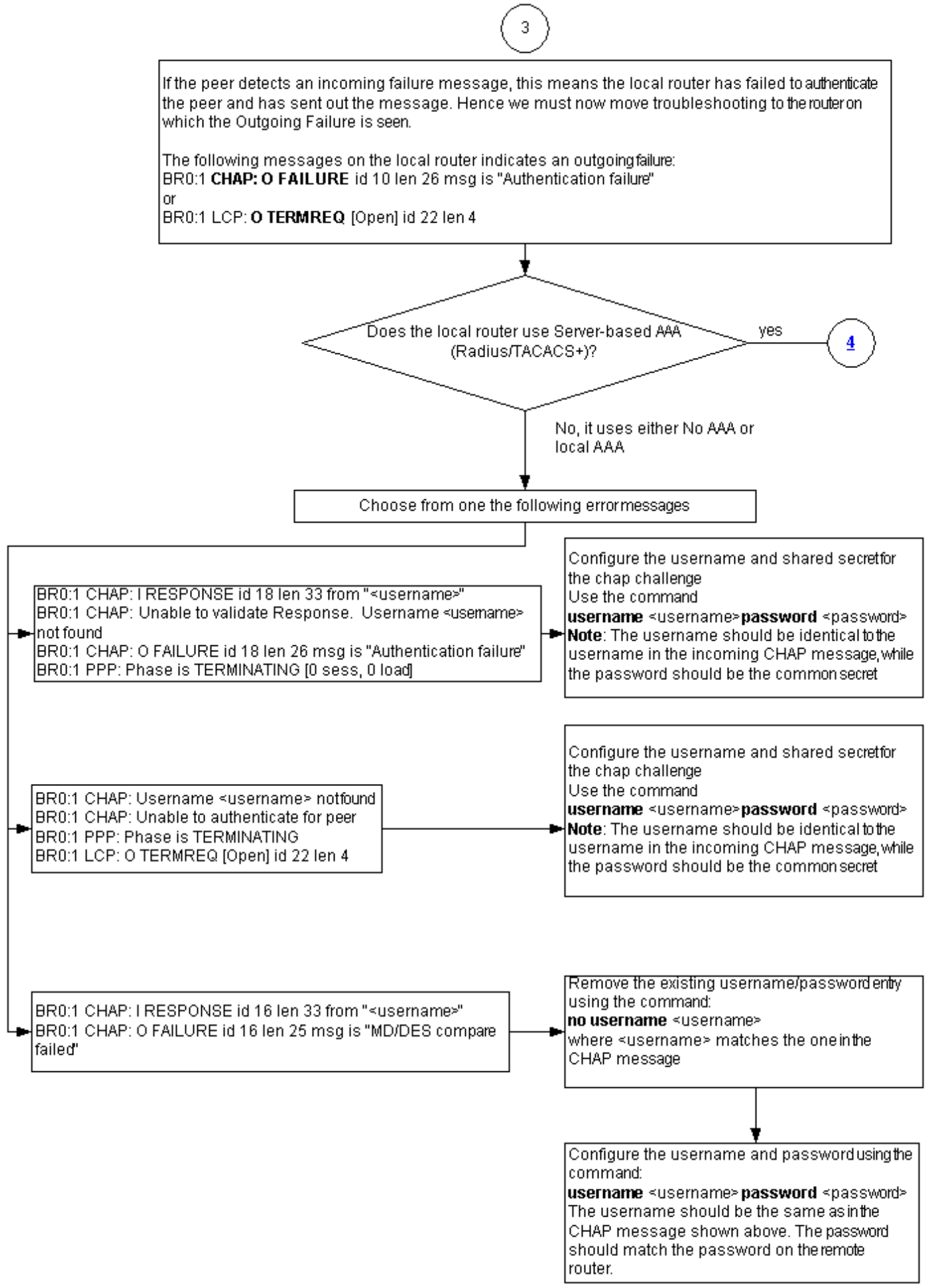
Faça estas perguntas:

1. Qual nome de usuário o roteador remoto espera?Use o comando **ppp chap hostname *<username> na interface física ou do discador.*** Configure o nome de usuário fornecido pelo administrador remoto aqui.**Observação:** isso diferencia maiúsculas de minúsculas.
2. Que senha o roteador remoto espera?Use o comando **ppp chap password *<password> na interface física ou do discador.***Observação: isso diferencia maiúsculas de minúsculas.

Para obter mais informações, consulte o documento Autenticação PPP Usando os Comandos ppp

chap hostname e ppp authentication chap callin.

Troubleshooting de Falhas de CHAP de Saída



Se o peer detectar uma mensagem de entrada failure, significa que o roteador local não autenticou o peer e enviou a mensagem. Portanto, agora você deve identificar e solucionar o

problema do roteador no qual a falha de saída é indicada.

Essas mensagens no roteador local indicam uma falha de saída:

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

or

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

O roteador não usa AAA ou AAA somente local

Se o roteador não usar um sistema de Autenticação, Autorização e Auditoria (AAA, authentication, authorization, and accounting) baseado no servidor (Radius ou Tacacs+), ele poderá usar AAA ou AAA local. Verifique se você vê uma das seguintes mensagens na saída da debugação:

Incapaz de validar a resposta

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]
```

Uma incompatibilidade de nome de usuário pode ser causada por duas razões:

1. O correspondente não forneceu o nome de usuário esperado pelo roteador local. Por exemplo, nós esperamos (e configuramos) o nome de usuário RoteadorA, mas o peer usou o nome RoteadorB. É possível configurar o nome de usuário e a senha enviados pelo correspondente ou corrigir o correspondente com o nome de usuário correto.
2. O nome do usuário do roteador local não está configurado. Se o nome de usuário fornecido pelo peer corresponder ao que o roteador local esperava, configure o nome de usuário e a senha.

Esta questão é vista com mais freqüência quando o peer utiliza o comando ppp chap hostname para configurar um nome de usuário diferente do nome do host do roteador.

Use o comando **username *<username>* password *<password>*** , em que *<username>* é substituído pelo nome de usuário na mensagem de erro acima.

Username <username> Not Found

Autenticação impossível para ponto de correspondência

```
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.
```

Uma incompatibilidade de nome de usuário pode ser causada por duas razões:

1. O correspondente não forneceu o nome de usuário esperado pelo roteador local. Por exemplo, esperamos (e configuramos) o nome de usuário RouterA. No entanto, o peer usou o nome RouterB. Você pode configurar o nome de usuário e a senha enviados pelo peer ou atualizar o peer com o nome de usuário correto.
2. O nome do usuário do roteador local não está configurado. Se o nome de usuário fornecido pelo peer corresponder ao que o roteador local esperava, configure o nome de usuário e a senha.

Esta questão é vista com mais freqüência quando o peer utiliza o comando ppp chap hostname para configurar um nome de usuário diferente do nome do host do roteador.

Use o comando **username *<username>* password *<password>*** , em que *<username>* é substituído pelo nome de usuário na mensagem de erro acima.

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"
```

Este erro é causado por incompatibilidade de senha. Isso pode ter ocorrido por duas razões:

1. O peer não forneceu a senha esperada pelo roteador local. Por exemplo, nós esperamos (e configuramos) a senha LetmeIn, mas o peer usou a senha letmein. Você pode reconfigurar o nome de usuário e a senha enviados pelo peer ou corrigir o peer com o nome de usuário correto.
2. A senha do roteador local não está corretamente configurada. Se você verificou que a senha fornecida pelo peer está correta, reconfigure o roteador local.

Solução:

1. Remova o nome de usuário e a entrada de senha existentes usando este comando:

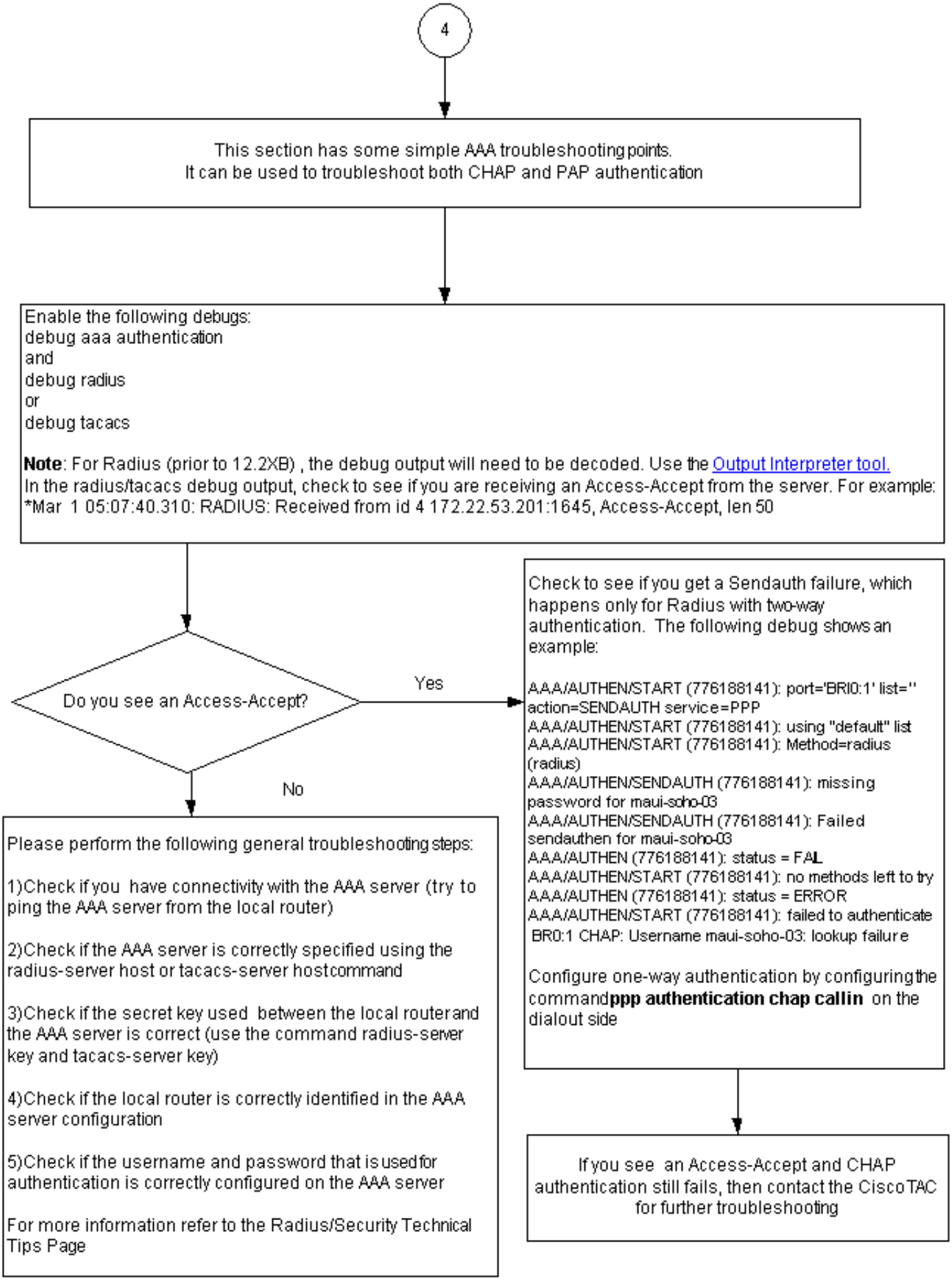
   ```
   no username <username>
   ```

   Onde **<username> é substituído pelo nome de usuário na mensagem de erro.** Nesse exemplo, seria maui-soho-03.
2. Configure o nome de usuário e a senha usando este comando:

   ```
   username password
   ```

   O nome de usuário deve ser igual ao da mensagem CHAP mostrada acima. A senha deve corresponder à senha no roteador remoto.

Troubleshooting de Problemas de AAA baseados no Servidor Geral



Observação: este documento não se destina a um recurso de solução de problemas AAA. Para obter mais informações sobre troubleshooting de Autenticação, Autorização e Auditoria, consulte os seguintes recursos:

- Operações de AAA
- RADIUS
- TACACS

Problema: A autenticação PAP funciona para PPP, mas o MsCHAPv2 falha

Talvez você não consiga autenticar em um servidor ACS porque o servidor ACS não recebe a solicitação de autenticação, o que faz com que uma sessão falhe. Esse comportamento é observado e registrado na ID de bug da Cisco CSCee04466 (somente clientes registrados) . Como solução alternativa, use um servidor RADIUS para sessões PPP. No entanto, mantenha o servidor TACACS+ para fins administrativos no roteador.

Informações Relacionadas

- Entendendo a saída de negociação de debug ppp
- Entendendo e configurando a autenticação de PPP CHAP
- Autenticação PPP Usando os Comandos ppp chap hostname e ppp authentication chap callin
- Configurando e Troubleshooting de PPP Password Authentication Protocol (PAP)
- Suporte à tecnologia de discagem e acesso
- Suporte Técnico e Documentação - Cisco Systems