Dépannage de l'authentification PPP (CHAP ou PAP)

Contenu

Introduction

Les questions d'authentification de protocole point-à-point (PPP) sont l'une des causes classiques pour les pannes de liaison d'accès par réseau commuté. Ce document fournit quelques procédures de dépannage pour des questions d'authentification de PPP.

Conditions préalables

- Debug ppp negotiation et debug ppp authentication d'enable.
- La phase d'authentification de PPP ne commence pas jusqu'à ce que la phase du Link Control Protocol (LCP) soit complète et soit dans l'état ouvert. Si le **debug ppp negotiation** n'indique pas que LCP est ouvert, dépannez cette question avant de commencer.
- L'authentification de PPP doit être configurée des deux côtés. Émettez ces commandes comme appropriées :CHAP d'authentification de ppp sur les deux Routeurs, pour l'authentification bi-directionnelle de protocole d'authentification CHAP (Challenge Handshake Authentication Protocol).callin de CHAP d'authentification de ppp sur le routeur appelant, pour l'authentification à sens unique.authentification PAP de ppp sur les deux Routeurs, pour l'authentification PAP.

Terminologie

- **Ordinateur local** (ou routeur local) - C'est le système sur lequel la session d'élimination des imperfections actuellement est exécutée. Comme vous déplacez la session de débogage d'un routeur à l'autre, appliquez l'ordinateur local de terme à l'autre routeur.
- **Pair** - L'autre fin du lien point par point. Par conséquent, le périphérique n'est pas l'ordinateur local.Par exemple, si vous émettez la commande de **debug ppp negotiation** sur le RouterA, puis c'est l'ordinateur local et le RouterB est le pair. Cependant, si vous décalez le débogage plus d'au RouterB, puis ce devient l'ordinateur local et le RouterA va bien au pair.

Remarque: Les termes ordinateur local et pair n'impliquent pas des relations de client-serveur. Selon où la session de débogage est exécutée, le client entrant pourrait être l'ordinateur local ou le pair.

Conditions requises

Cisco recommande que vous ayez la connaissance de ce thème :

- Vous devez pouvoir lire et comprendre la sortie de debug ppp negotiation. Référez-vous derrière le pour en savoir plus de sortie de debug ppp negotiation de document compréhension.

Composants utilisés

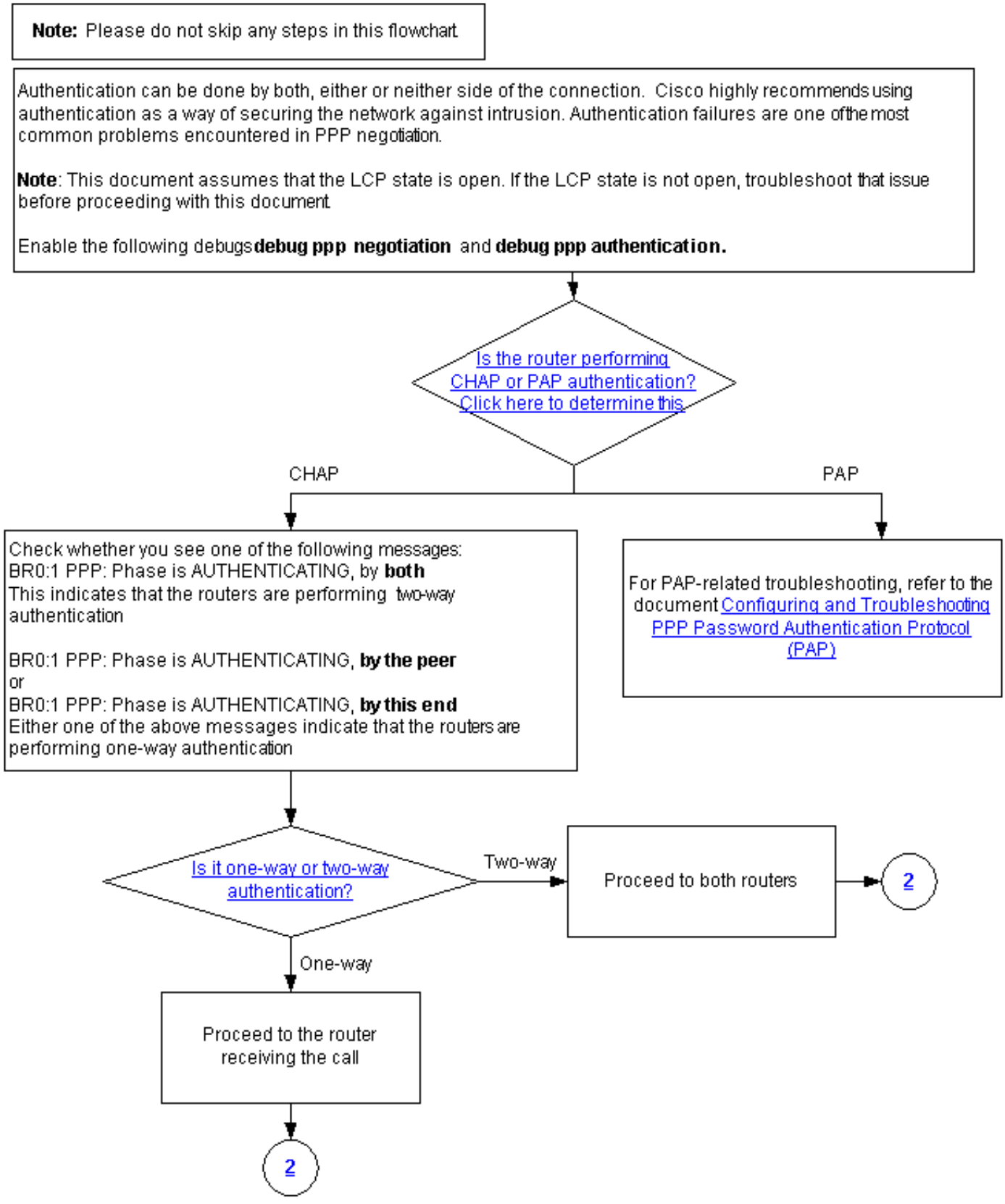
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Diagramme de dépannage

Ce document comporte quelques organigrammes pour aider au dépannage. Vous pouvez poursuivre au prochain organigramme en cliquant sur sur les cercles numérotés.



Le routeur exécute-il le CHAP ou l'authentification PAP ?

Pour déterminer si le routeur exécute le CHAP ou l'authentification PAP, recherchez ces lignes dans le **debug ppp negotiation** et le **debug ppp authentication** sortis :

CHAP

Recherchez le CHAP pendant la phase AUTHENTIFIANTE :

```
*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

Recherchez le PAP pendant la phase AUTHENTIFIANTE :

```
*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"
```

Exécuter de routeur est-il de l'authentification CHAP à sens unique ou bi-directionnelle ?

Recherchez un de ces messages dans le **debug ppp negotiation** sorti :

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

Le message ci-dessus indique que les Routeurs exécutent l'authentification bi-directionnelle.

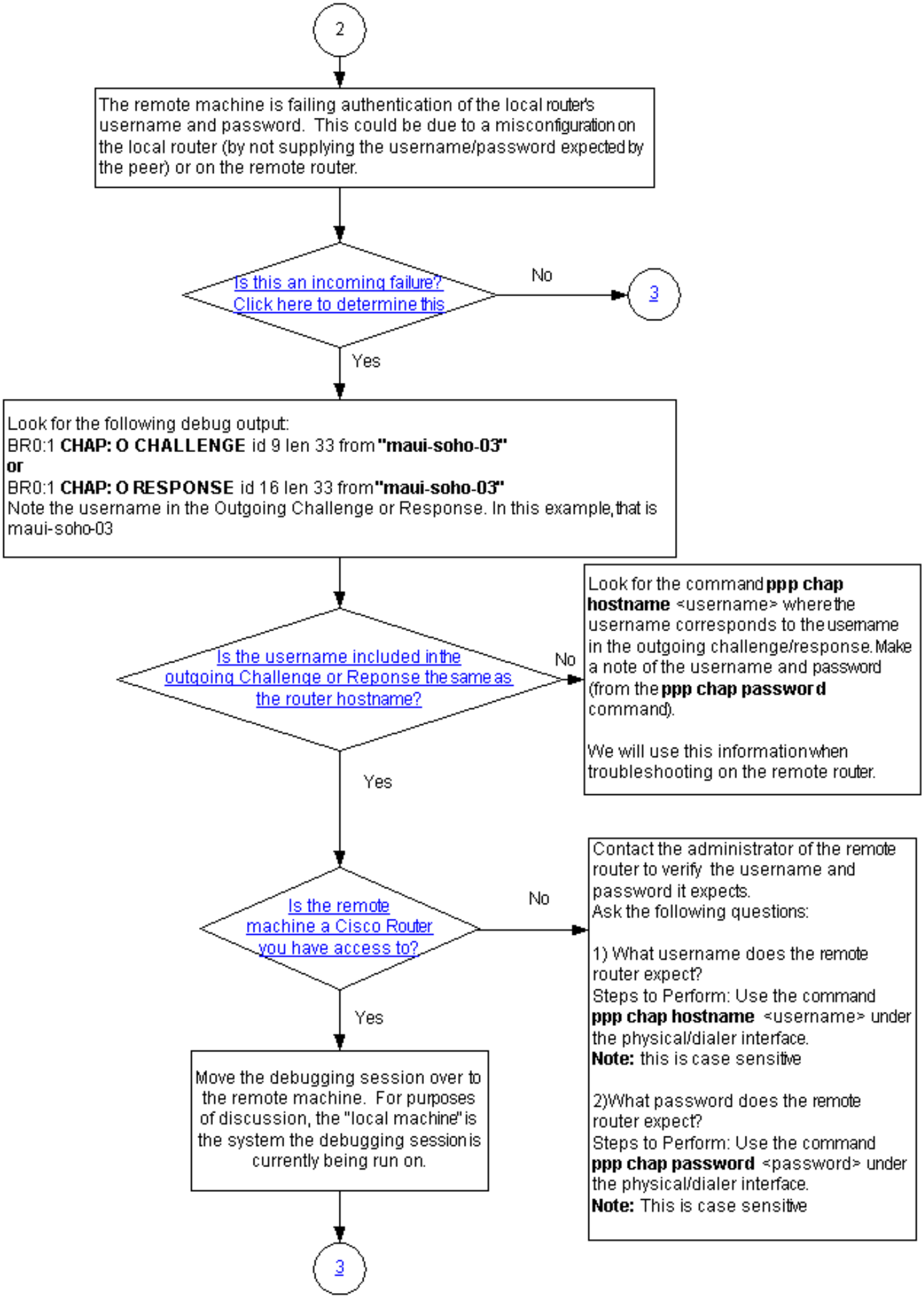
L'un ou l'autre un des messages ci-dessous indique que les Routeurs exécutent l'authentification à sens unique :

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

ou

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

Est-ce que c'est une panne entrante ?



Vérifiez pour voir si vous recevez le termreq ou les messages d'échec entrants. Souvenez-vous

que « je » indique que le message est un message entrant :

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

ou

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

Une panne entrante indique que le pair n'authentifie pas le nom d'utilisateur et mot de passe du routeur local. Ceci pourrait être dû à une mauvaise configuration sur le routeur local (en ne fournissant pas le nom d'utilisateur et mot de passe prévu par le pair) ou sur le routeur distant.

Le nom d'utilisateur dans le défi ou la réponse sortant est-il les mêmes que l'adresse Internet ?

Recherchez le suivant dans le **debug ppp negotiation** sorti :

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

ou

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

Notez le nom d'utilisateur dans le défi ou la réponse sortant. Dans cet exemple, c'est **maui-soho-03**. Vous avez besoin de ceci pour vérifier que le nom d'utilisateur et mot de passe utilisé pour l'authentification apparie celui prévu par le côté distant. Par exemple, si le routeur local s'identifie au pair comme A, mais le pair attendait B, puis l'authentification échoue.

Si le nom d'utilisateur dans le défi sortant n'est pas identique que l'adresse Internet, recherchez le *<username> de* **ppp chap hostname de** commande, où le nom d'utilisateur correspond au nom d'utilisateur dans le défi sortant. Notez le nom d'utilisateur et mot de passe (dans la commande de accompagnement de **ppp chap password**). Vous utiliserez ces informations quand vous dépannez le routeur distant.

L'ordinateur distant est-il un routeur de Cisco que vous avez accès à ?

Puisque nous avons déterminé que le routeur local a reçu une panne entrante, nous savons que la panne se produit sur le pair. Si vous avez accès au routeur distant de Cisco, alors dépannez sur ce périphérique.

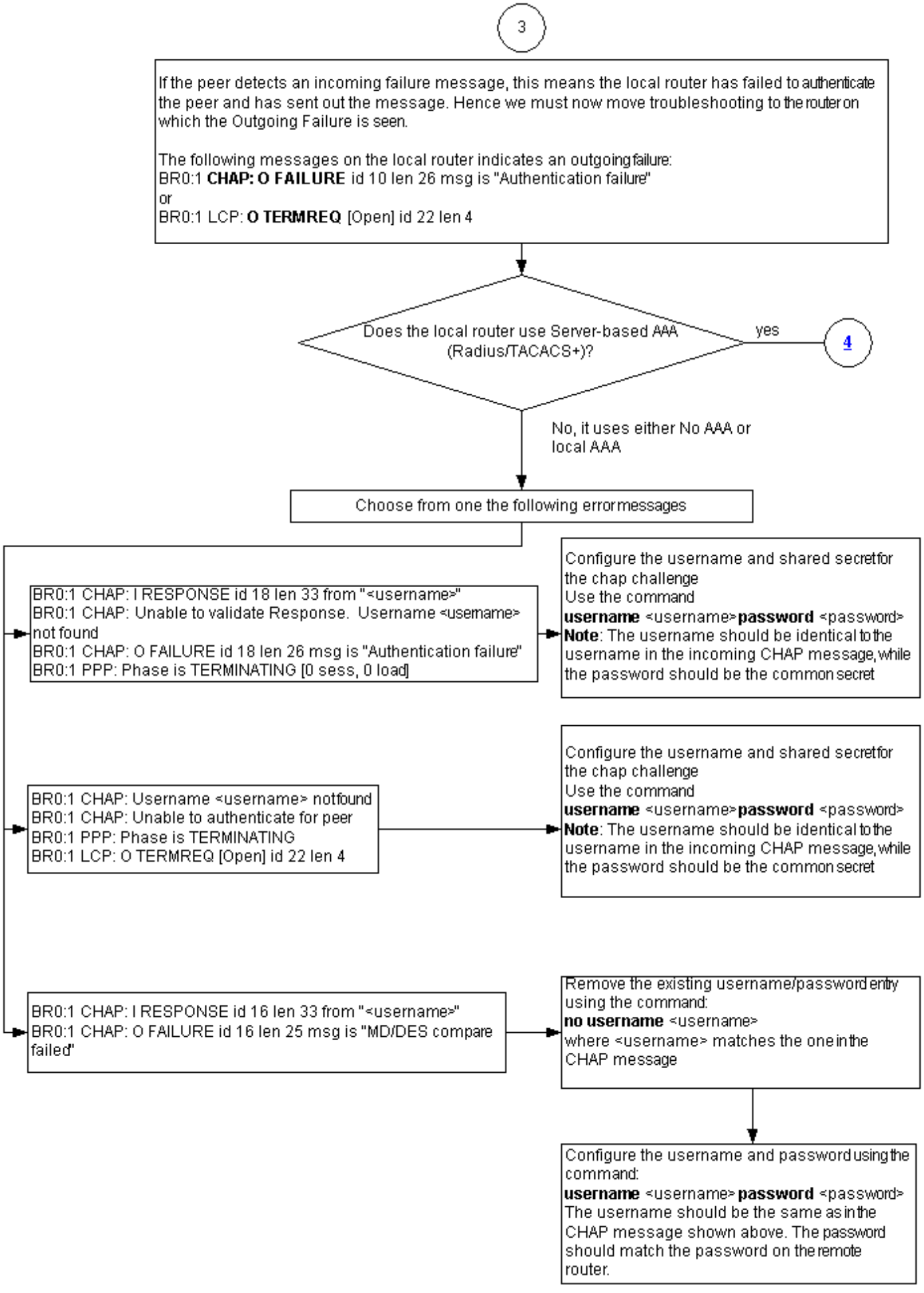
Si vous n'avez pas accès au routeur distant, contactez l'administrateur de ce routeur pour vérifier le nom d'utilisateur et mot de passe qu'il prévoit.

Posez ces questions :

1. Quel nom d'utilisateur le routeur distant attend-il ?Utilisez la commande de *<username> de* **ppp chap hostname** sous l'examen médical ou l'interface de numérotation. Configurez le nom d'utilisateur fourni par l'administrateur distant ici.**Remarque:** Ce distingue les majuscules et minuscules.
2. Quel mot de passe le routeur distant attend-il ?Utilisez la commande de *<password> de* **ppp chap password** sous l'examen médical ou l'interface de numérotation.**Remarque:** Ce distingue les majuscules et minuscules.

Le pour en savoir plus, se rapportent à l'authentification de PPP de document utilisant les commandes de callin de CHAP d'authentification de ppp chap hostname et de ppp.

Dépannage des pannes sortantes de CHAP



Si le pair détecte un message d'échec entrant, ceci signifie que le routeur local n'a pas authentifié le pair et a envoyé le message. Par conséquent, vous devez maintenant dépanner le routeur sur lequel indique la panne sortante.

Ces messages sur le routeur local indiquent une panne sortante :

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

ou

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

Le routeur n'utilise aucun AAA ou seulement AAA local

Si le routeur n'utilise pas une authentification sur serveur, une autorisation, et un système de comptabilité (AAA) (rayon ou Tacacs+), alors le routeur peut n'utiliser aucun AAA ou AAA local. Vérifiez si vous voyez un des messages suivants dans la sortie de débogage :

Incapable de valider la réponse

<username> de nom d'utilisateur non trouvé

```
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]
```

Une non-concordance de nom d'utilisateur peut sont provoqué par par deux raisons :

1. Le pair n'a pas fourni le nom d'utilisateur prévu par le routeur local. Par exemple, nous avons attendu (et a configuré) le RouterA de nom d'utilisateur, mais le pair a utilisé le RouterB de nom. Vous pouvez configurer le nom d'utilisateur et mot de passe envoyé par le pair ou corriger le pair avec le bon nom d'utilisateur.
2. Le routeur local ne fait pas configurer le nom d'utilisateur. Si le nom d'utilisateur fourni par le pair apparie ce que le routeur local prévu, alors configure le nom d'utilisateur et mot de passe.

Cette question le plus souvent est vue quand le pair utilise la commande de ppp chap hostname de configurer un nom d'utilisateur autre que le nom de hôte du routeur.

Utilisez la commande de *<password> de* mot de passe de *<username> de* nom d'utilisateur, où le *<username>* est remplacé par le nom d'utilisateur dans le message d'erreur ci-dessus.

<username> de nom d'utilisateur non trouvé

Incapable d'authentifier pour le pair

```
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.
```

Une non-concordance de nom d'utilisateur peut sont provoqué par par deux raisons :

1. Le pair n'a pas fourni le nom d'utilisateur prévu par le routeur local. Par exemple, nous avons attendu (et a configuré) le RouterA de nom d'utilisateur. Cependant, le pair a utilisé le RouterB de nom. Vous pouvez configurer le nom d'utilisateur et mot de passe envoyé par le pair ou mettre à jour le pair avec le nom d'utilisateur correct.
2. Le routeur local ne fait pas configurer le nom d'utilisateur. Si le nom d'utilisateur fourni par le pair apparie ce que le routeur local prévu, alors configure le nom d'utilisateur et mot de passe.

Cette question le plus souvent est vue quand le pair utilise la commande de ppp chap hostname de configurer un nom d'utilisateur autre que le nom de hôte du routeur.

Utilisez la commande de *<password> de* **mot de passe de** *<username> de* **nom d'utilisateur**, où le *<username>* est remplacé par le nom d'utilisateur dans le message d'erreur ci-dessus.

MD/DES comparent manqué

```
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"
```

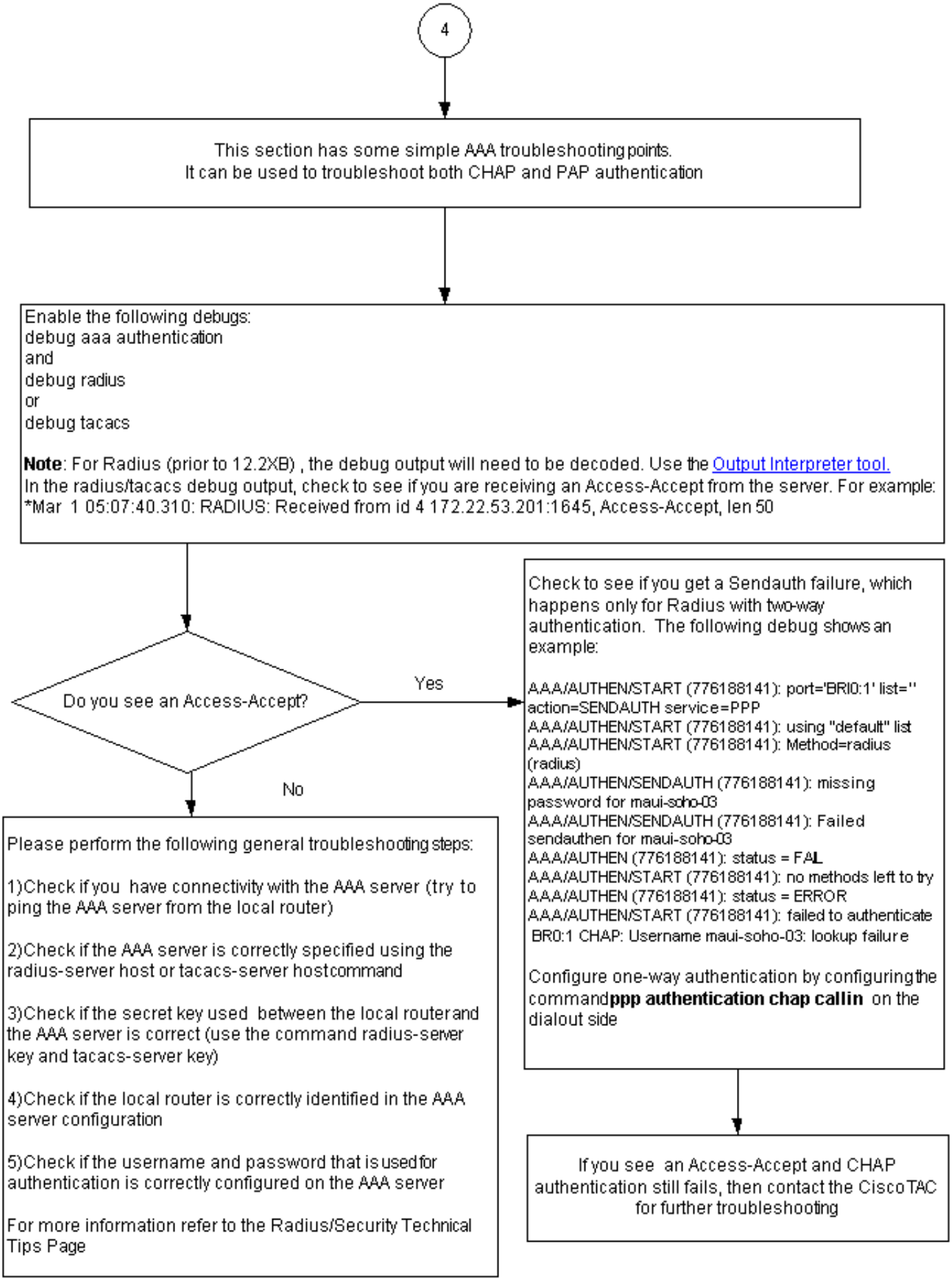
Cette erreur est provoqué par par une non-concordance de mot de passe. Ceci a pu être cause par deux raisons :

1. Le pair n'a pas fourni le mot de passe prévu par le routeur local. Par exemple, nous avons attendu (et a configuré) le mot de passe *Letmeln*, mais le pair a utilisé le *letmein de* mot de passe. Vous pouvez modifier le nom d'utilisateur et mot de passe envoyé par le pair ou corriger le pair avec le bon nom d'utilisateur.
2. Le routeur local ne fait pas configurer correctement le mot de passe. Si vous avez vérifié que le mot de passe fourni par le pair est correct, alors modifiez le routeur local.

Solution :

1. Retirez l'entrée existante de nom d'utilisateur et mot de passe utilisant cette commande : **no username** *<username>* Là où le *<username>* est remplacé par le nom d'utilisateur dans le message d'erreur. Dans cet exemple, ce serait `maui-soho-03`.
2. Configurez le nom d'utilisateur et mot de passe utilisant cette commande : **username** *<username>* **password** *<password>* Le nom d'utilisateur devrait être identique que dans le message de CHAP affiché ci-dessus. Le mot de passe devrait apparier le mot de passe sur le routeur distant.

Dépannage des questions générales d'AAA sur serveur



Remarque: Ce document n'est pas destiné comme AAA dépannant la ressource. Pour plus d'informations sur l'AAA de dépannage, référez-vous aux ressources suivantes :

- Exécutions d'AAA

- RAYON
- TACACS

Problème : L'authentification PAP fonctionne pour le PPP, mais MsCHAPv2 échoue

Vous ne pourriez pas pouvoir authentifier à un serveur ACS parce que le serveur ACS ne reçoit pas la demande d'authentification, qui fait échouer une session. Ce comportement est observé et connecté sous l'ID de bogue Cisco CSCee04466 (clients enregistrés seulement). Comme contournement, utilisez un serveur de RAYON pour des sessions PPP. Cependant, gardez le serveur TACACS+ à des fins administratives sur le routeur.

Informations connexes

- Présentation de la sortie de négociation de débogage ppp
- Présentation et configuration de l'authentification PPP CHAP
- Authentification PPP par le biais des commandes ppp chap hostname et ppp authentication chap callin
- Configuration et dépannage du protocole PAP (Password Authentication Protocol) pour PPP
- Numérotation et accès de l'assistance technique
- Support et documentation techniques - Cisco Systems