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 les problèmes d'authentification PPP.

Conditions préalables

- Activez **debug ppp negotiation** et **debug ppp authentication**.
- La phase d'authentification PPP ne commence que lorsque la phase LCP (Link Control Protocol) est terminée et qu'elle est à l'état ouvert. Si **debug ppp negotiation** n'indique pas que LCP est ouvert, corrigez ce problème avant de continuer.
- L'authentification PPP doit être configurée des deux côtés. Émettez ces commandes selon les besoins :**ppp authentication chap** sur les deux routeurs, pour l'authentification CHAP (Challenge Handshake Authentication Protocol) bidirectionnelle.**ppp authentication chap callin** sur le routeur appelant, pour l'authentification unidirectionnelle.**ppp authentication pap** sur les deux routeurs, pour l'authentification PAP.

Terminologie

- **Machine locale** (ou routeur local) : système sur lequel la session de débogage est en cours d'exécution. Lorsque vous déplacez la session de débogage d'un routeur à l'autre, appliquez le terme machine locale à l'autre routeur.
- **Peer** - L'autre extrémité de la liaison point à point. Par conséquent, le périphérique n'est pas la machine locale.Par exemple, si vous émettez la commande **debug ppp negotiation** sur RouterA, c'est l'ordinateur local et RouterB est l'homologue. Cependant, si vous passez au débogage RouterB, il devient la machine locale et RouterA devient l'homologue.

Remarque : Les termes machine locale et homologue n'impliquent pas de relation client-serveur. Selon l'emplacement d'exécution de la session de débogage, le client de numérotation peut être l'ordinateur ou l'homologue local.

Conditions requises

Cisco recommande que vous ayez une connaissance de ce sujet :

- Vous devez être capable de lire et de comprendre le résultat de la négociation debug ppp. Référez-vous au document Présentation de la sortie de la négociation debug ppp pour plus d'informations.

Components Used

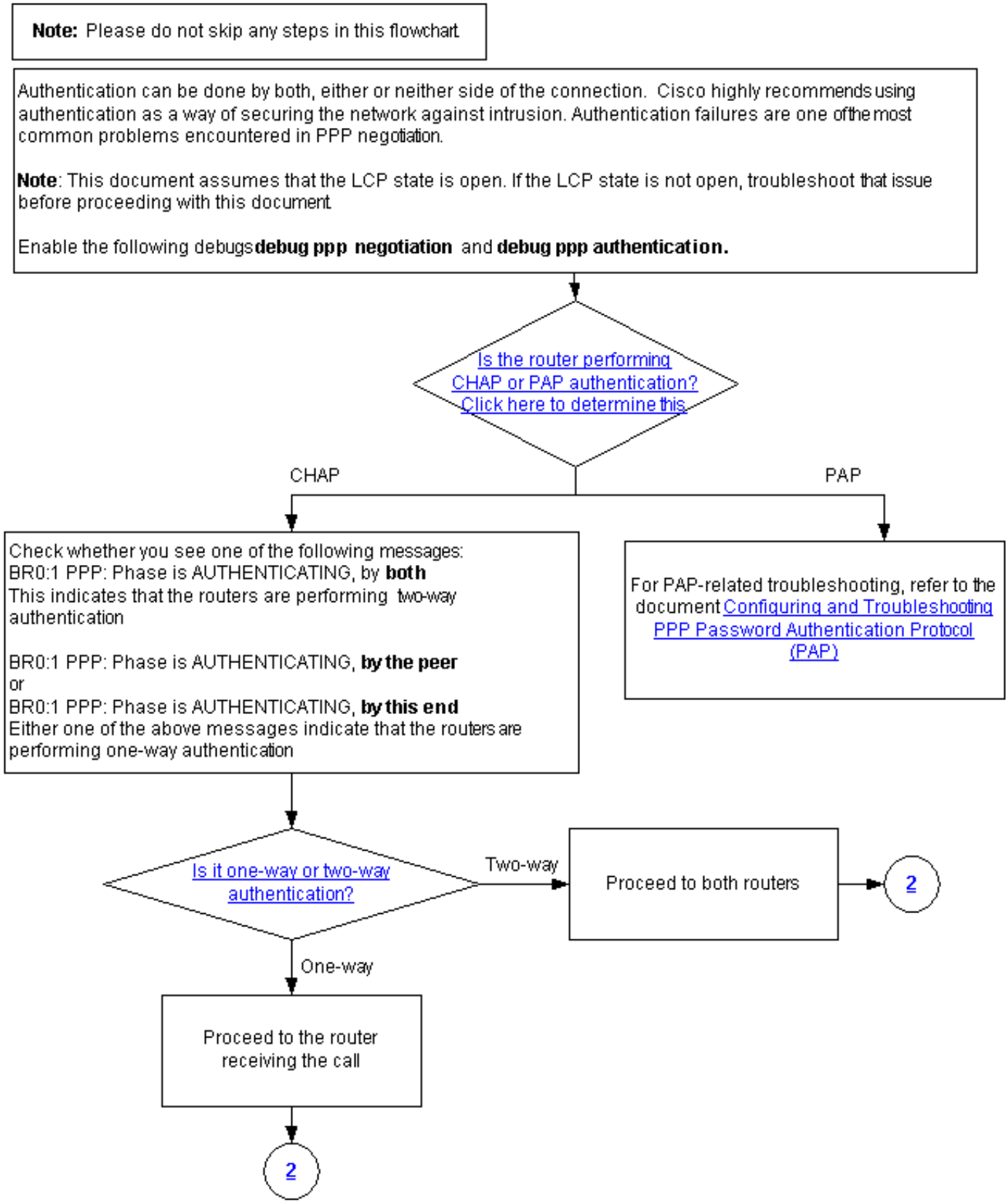
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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 comprend quelques organigrammes pour faciliter le dépannage. Vous pouvez passer à l'organigramme suivant en cliquant sur les cercles numérotés.



Le routeur effectue-t-il l'authentification CHAP ou PAP ?

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

CHAP

Recherchez CHAP dans la phase 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

Recherchez PAP dans la phase 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"
```

Le routeur effectue-t-il une authentification CHAP unidirectionnelle ou bidirectionnelle ?

Recherchez l'un de ces messages dans la sortie **debug ppp negotiation** :

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

Le message ci-dessus indique que les routeurs effectuent une authentification bidirectionnelle.

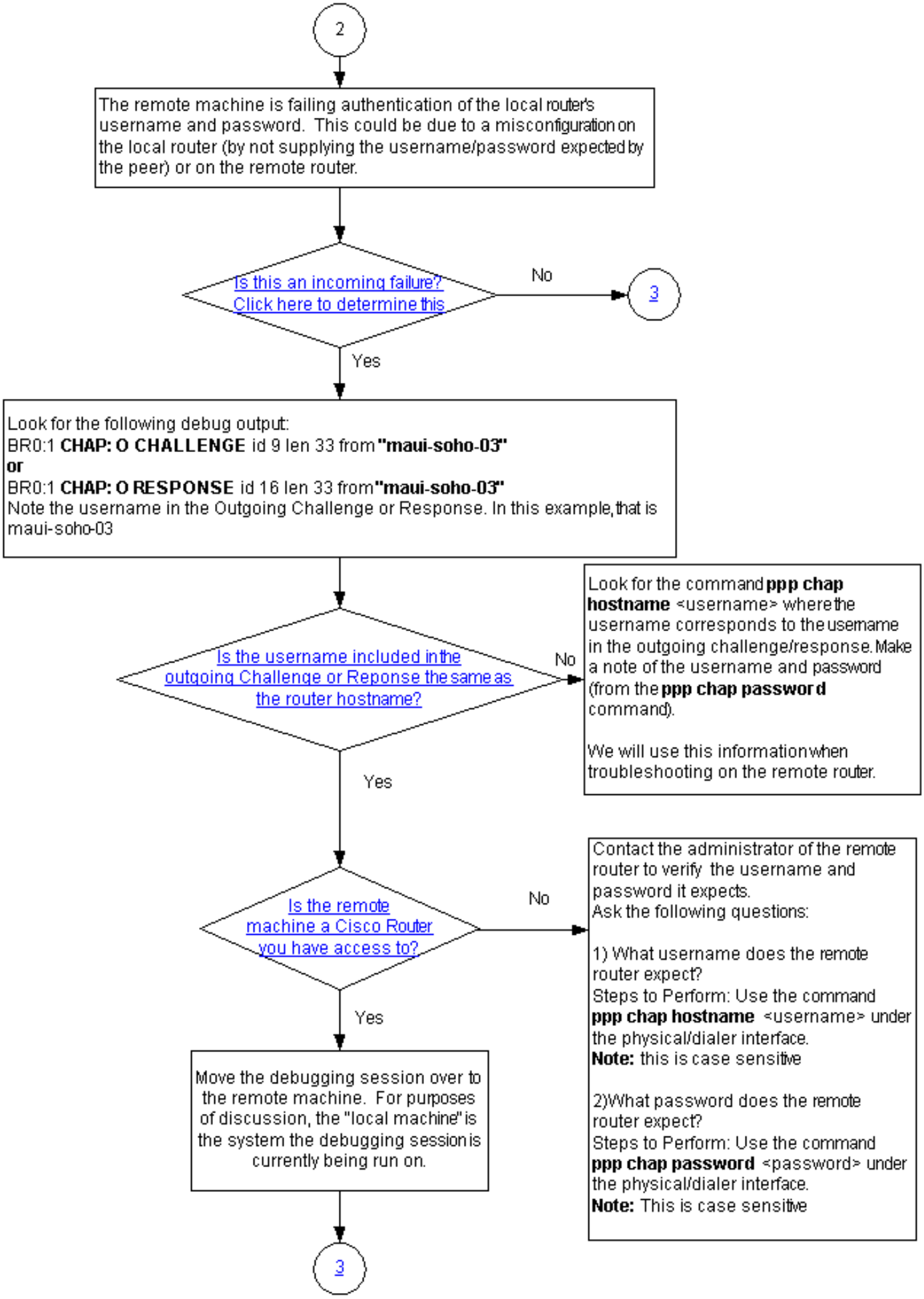
L'un des messages ci-dessous indique que les routeurs effectuent une authentification unidirectionnelle :

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

ou

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

S'agit-il d'un échec entrant ?



Vérifiez si vous recevez des messages de requête ou d'échec entrants. N'oubliez pas que « I »

indique que le message est un message entrant :

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

ou

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

Un échec entrant indique que l'homologue ne parvient pas à authentifier le nom d'utilisateur et le mot de passe du routeur local. Cela peut être dû à une mauvaise configuration sur le routeur local (en ne fournissant pas le nom d'utilisateur et le mot de passe attendus par l'homologue) ou sur le routeur distant.

Le nom d'utilisateur dans le défi ou la réponse sortants est-il identique au nom d'hôte ?

Recherchez ce qui suit dans la sortie **debug ppp negotiation** :

```
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 sortante. Dans cet exemple, c'est **maui-soho-03**. Vous devez vérifier que le nom d'utilisateur et le mot de passe utilisés pour l'authentification correspondent à celui attendu par le côté distant. Par exemple, si le routeur local s'identifie à l'homologue en tant que A, mais que l'homologue attendait B, l'authentification échoue.

Si le nom d'utilisateur dans le défi sortant n'est pas le même que le nom d'hôte, recherchez la commande ppp chap hostname *<nom d'utilisateur>* , où le nom d'utilisateur correspond au nom d'utilisateur dans le défi sortant. Notez le nom d'utilisateur et le mot de passe (dans la commande **ppp chap password** qui l'accompagne). Vous utiliserez ces informations lors du dépannage du routeur distant.

La machine distante est-elle un routeur Cisco auquel vous avez accès ?

Puisque nous avons déterminé que le routeur local a reçu une défaillance entrante, nous savons que la défaillance se produit sur l'homologue. Si vous avez accès au routeur Cisco distant, procédez au dépannage 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 le mot de passe qu'il attend.

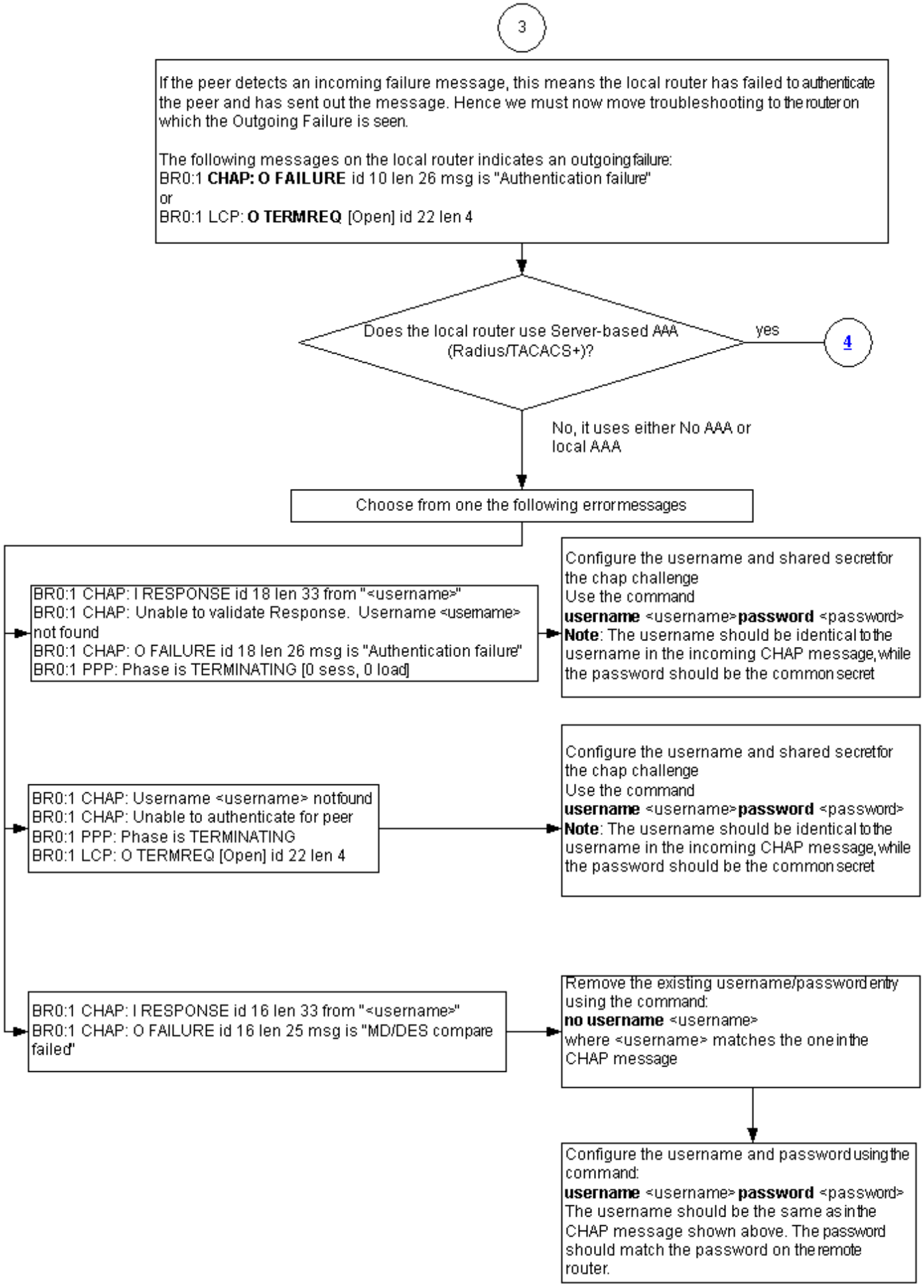
Posez les questions suivantes :

1. Quel nom d'utilisateur le routeur distant attend-il ?Utilisez la commande ppp chap hostname *<username>* sous l'interface physique ou de numérotation. Configurez ici le nom d'utilisateur fourni par l'administrateur distant.**Remarque :** Cette valeur est sensible à la casse.

2. Quel mot de passe le routeur distant attend-il ?Utilisez la commande ppp chap password *<password>* sous l'interface physique ou de numérotation.**Remarque :** Cette valeur est sensible à la casse.

Pour plus d'informations, référez-vous au document Authentification PPP à l'aide des commandes ppp chap hostname et ppp authentication chap callin.

Dépannage des échecs CHAP sortants



Si l'homologue détecte un message d'échec entrant, cela signifie que le routeur local n'a pas pu authentifier l'homologue et a envoyé le message. Par conséquent, vous devez maintenant

dépanner le routeur sur lequel indique la défaillance sortante.

Ces messages sur le routeur local indiquent une défaillance 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 utilise No AAA ou Local AAA uniquement

Si le routeur n'utilise pas de système AAA (Authentication, Authorization, and Accounting) basé sur le serveur (Radius ou Tacacs+), le routeur peut alors utiliser un AAA local ou AAA. Vérifiez si vous voyez l'un des messages suivants dans la sortie de débogage :

Impossible de valider la réponse

Nom d'utilisateur *<nom d'utilisateur>* introuvable

```
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-correspondance de nom d'utilisateur peut être causée par deux raisons :

1. L'homologue n'a pas fourni le nom d'utilisateur attendu par le routeur local. Par exemple, nous attendions (et configurons) le nom d'utilisateur RouterA, mais l'homologue utilisait le nom RouterB. Vous pouvez configurer le nom d'utilisateur et le mot de passe envoyés par l'homologue ou corriger l'homologue avec le nom d'utilisateur approprié.
2. Le nom d'utilisateur du routeur local n'est pas configuré. Si le nom d'utilisateur fourni par l'homologue correspond à ce que le routeur local attendait, configurez le nom d'utilisateur et le mot de passe.

Ce problème apparaît le plus souvent lorsque l'homologue utilise la commande **ppp chap hostname** pour configurer un nom d'utilisateur autre que le nom d'hôte du routeur.

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

Nom d'utilisateur *<nom d'utilisateur>* introuvable

Impossible de s'authentifier pour l'homologue

```
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-correspondance de nom d'utilisateur peut être causée par deux raisons :

1. L'homologue n'a pas fourni le nom d'utilisateur attendu par le routeur local. Par exemple, nous attendions (et configurons) le nom d'utilisateur RouterA. Cependant, l'homologue a utilisé le nom RouterB. Vous pouvez configurer le nom d'utilisateur et le mot de passe envoyés par l'homologue ou mettre à jour l'homologue avec le nom d'utilisateur correct.
2. Le nom d'utilisateur du routeur local n'est pas configuré. Si le nom d'utilisateur fourni par l'homologue correspond à ce que le routeur local attendait, configurez le nom d'utilisateur et le mot de passe.

Ce problème apparaît le plus souvent lorsque l'homologue utilise la commande **ppp chap hostname** pour configurer un nom d'utilisateur autre que le nom d'hôte du routeur.

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

Échec de la comparaison MD/DES

```
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 causée par une non-correspondance de mot de passe. Cela peut être dû à deux raisons :

1. L'homologue n'a pas fourni le mot de passe attendu par le routeur local. Par exemple, nous attendions (et configurons) le mot de passe *LetmeIn*, mais l'homologue a utilisé le mot de passe *letmein*. Vous pouvez soit reconfigurer le nom d'utilisateur et le mot de passe envoyés par l'homologue, soit corriger l'homologue avec le bon nom d'utilisateur.
2. Le mot de passe du routeur local n'est pas correctement configuré. Si vous avez vérifié que le mot de passe fourni par l'homologue est correct, reconfigurez le routeur local.

Solution :

1. Supprimez l'entrée de nom d'utilisateur et de mot de passe existante à l'aide de cette commande :

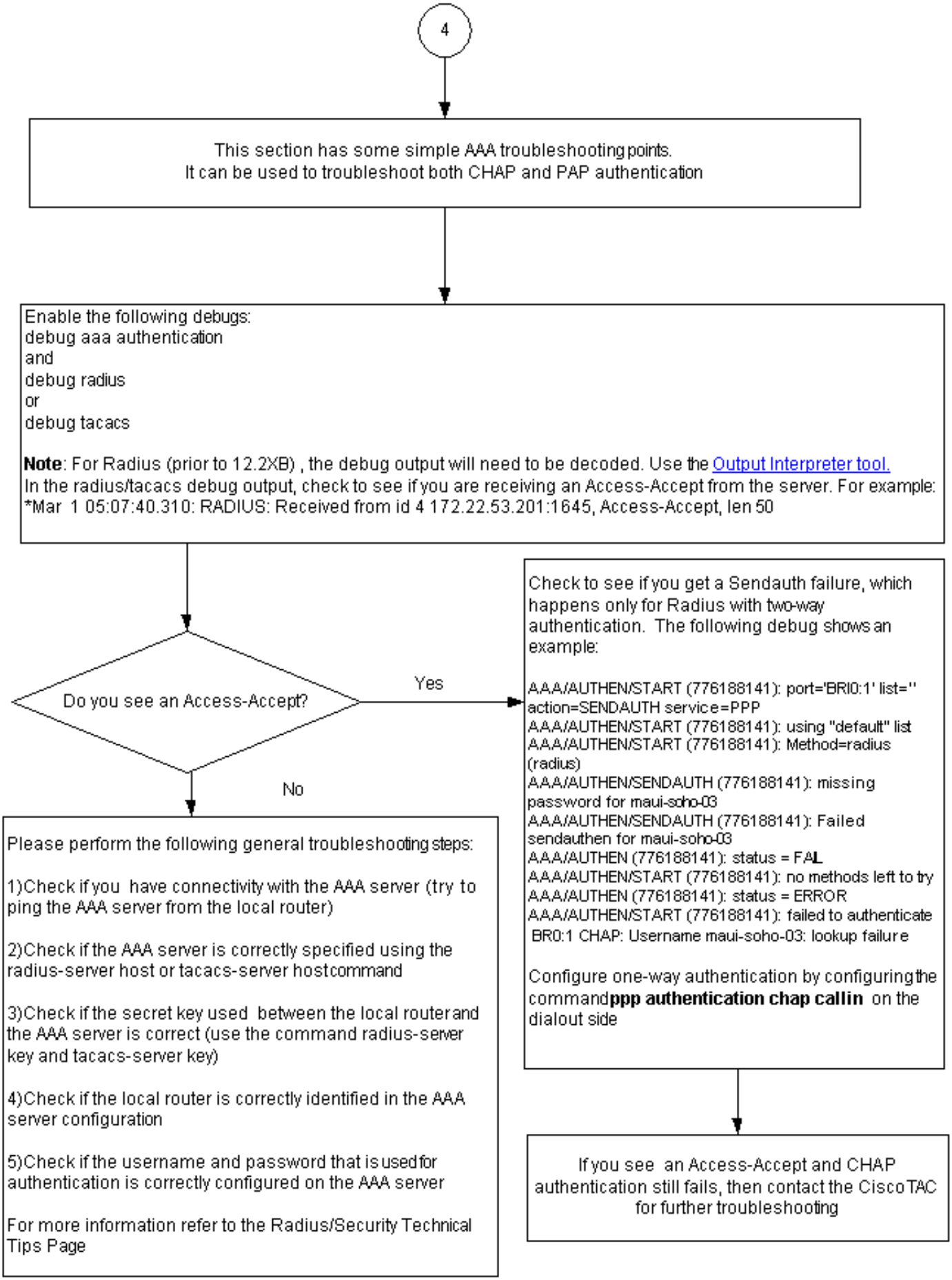
   no username <*username*>

   Où *<nom d'utilisateur>* 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 le mot de passe à l'aide de cette commande :

   username password

   Le nom d'utilisateur doit être identique au message CHAP ci-dessus. Le mot de passe doit correspondre à celui du routeur distant.

Dépannage des problèmes AAA généraux basés sur serveur



Remarque : Ce document n'est pas destiné à être une ressource de dépannage AAA. Pour plus d'informations sur le dépannage d'AAA, reportez-vous aux ressources suivantes :

- Opérations AAA

- RADIUS
- TACACS

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

Il se peut que vous ne puissiez pas vous authentifier auprès d'un serveur ACS, car le serveur ACS ne reçoit pas la demande d'authentification, ce qui entraîne l'échec d'une session. Ce comportement est observé et consigné sous l'ID de bogue Cisco CSCee04466 (clients enregistrés uniquement). Comme solution de contournement, utilisez un serveur RADIUS pour les sessions PPP. Cependant, conservez 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