Resolución de problemas de autenticación de PPP (CHAP o PAP)

Contenido

Introducción
prerrequisitos
Terminología
Requisitos
Componentes Utilizados
Convenciones
Diagrama de flujo de resolución de problemas
¿El router está realizando la autenticación de CHAP o PAP?
¿Qué tipo de autenticación CHAP está ejecutando el router, unidireccional o bidireccional?
¿Se trata de una falla entrante?
¿El nombre de usuario en Impugnación o respuesta saliente es igual al nombre de host?
¿Es la máquina remota un router Cisco al que tenga acceso?
Solución de problemas de fallas CHAP salientes
El router no utiliza AAA o utiliza AAA local solamente
Solución de problemas de AAA basados en el servidor general
Información Relacionada

Introducción

Los problemas de autenticación PPP (Point-to-Point Protocol) son una de las causas más comunes de los errores de link de marcación manual. Este documento proporciona algunos procedimientos de solución de problemas de autenticación de PPP.

prerrequisitos

- Active debug ppp negotiation y debug ppp authentication.
- La fase de la autenticación PPP no comienza hasta que la fase del (LCP) del Link Control Protocol sea completa y esté en el estado abierto. Si debug ppp negotiation no indica que el LCP está abierto, solucione este problema antes de continuar.
- Debe configurarse la Autentificación PPP en ambos lados. Publique estos comandos como apropiados:ppp authentication chap en ambos routers para la autenticación bidireccional de protocolo de autenticación de intercambio de señales (CHAP).ppp authentication chap callin on the calling router, para autenticaciones unidireccionales.autenticación PPP pap en ambo Routers, para la autenticación PAP.

Terminología

- **Máquina local** (o router local) - Éste es el sistema en el cual están funcionando con a la sesión de debugging actualmente. Como usted mueve la sesión del debug a partir de un router al otro, aplique la máquina local del término al otro router.
- **Par** - El otro extremo del enlace punto a punto. Por lo tanto, el dispositivo no es la máquina local.Por ejemplo, si usted publica el **comando debug ppp negotiation** en el routerA, después es la máquina local y el routerB es el par. Sin embargo, si usted desplaza hacer el debug de encima al routerB, después se convierte en la máquina local y el routerA siente bien al par.

Nota: Los términos máquina local y par no implican una relación cliente-servidor. Dependiendo de donde se funciona con la sesión del debug, el cliente dial in podría ser la máquina local o el par.

Requisitos

Cisco recomienda que usted tiene conocimiento de este tema:

- Es necesario que pueda leer y entender los resultados de las negociaciones de depuración ppp. Consulte el documento Introducción a la Salida del Comando debug ppp negotiation para más información.

Componentes Utilizados

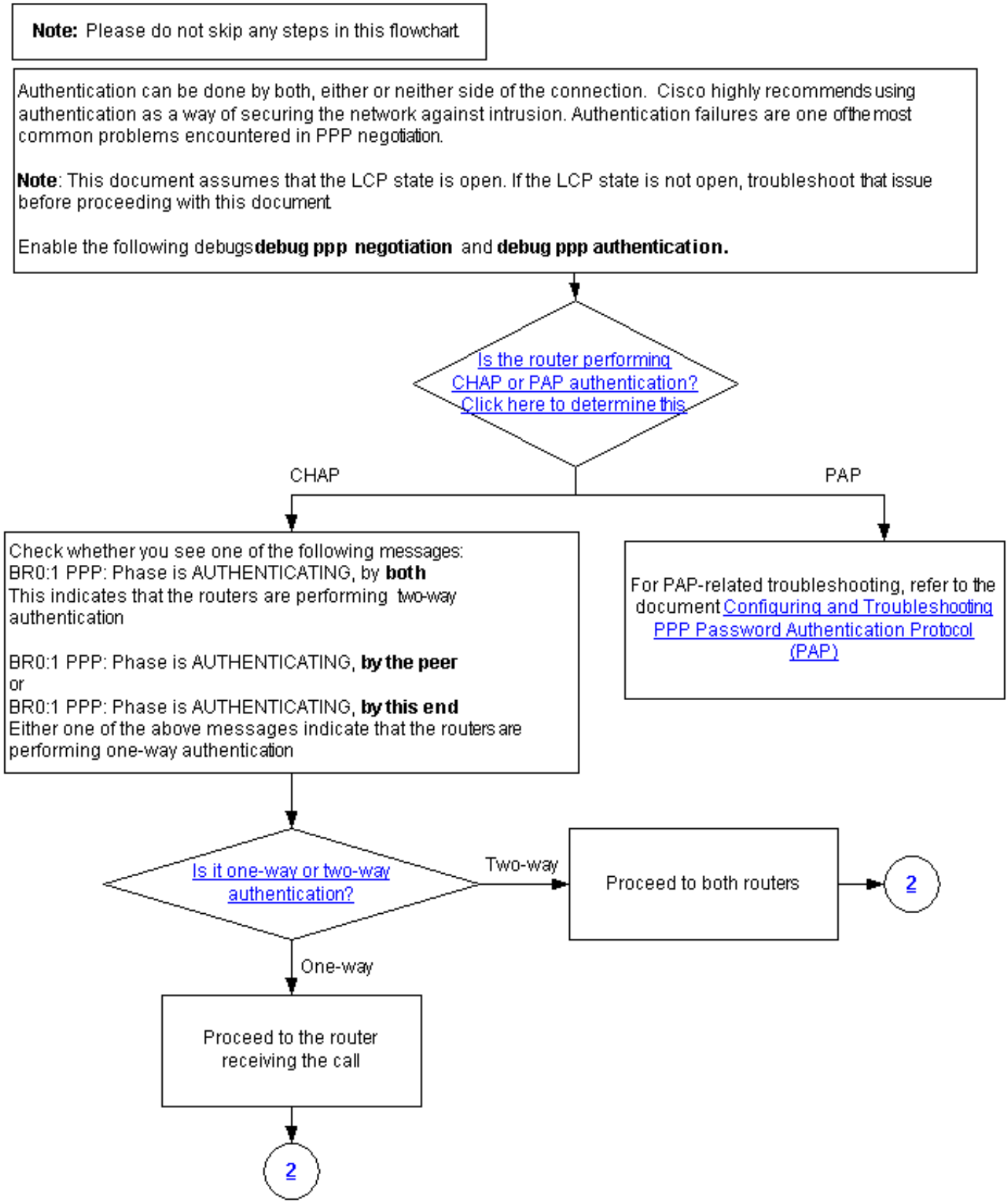
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Diagrama de flujo de resolución de problemas

Este documento comprende algunos diagramas de flujo de utilidad en la resolución de problemas. Haga clic en los círculos numerados para continuar con el siguiente diagrama de flujo.



¿El router está realizando la autenticación de CHAP o PAP?

Para determinar si el router está realizando la GRIETA o la autenticación PAP, busque estas líneas en la **negociación ppp del debug** y **haga el debug de la autenticación PPP** hecha salir:

GRIETA

Busque la GRIETA en la fase de AUTENTICIDAD:

```
*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

Busque el PAP en la fase de AUTENTICIDAD:

```
*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"
```

¿Qué tipo de autenticación CHAP está ejecutando el router, unidireccional o bidireccional?

Busque uno de estos mensajes en los **resultados de la negociación ppp del debug**:

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

El mensaje anterior indica que los routers están realizando una autenticación de doble sentido.

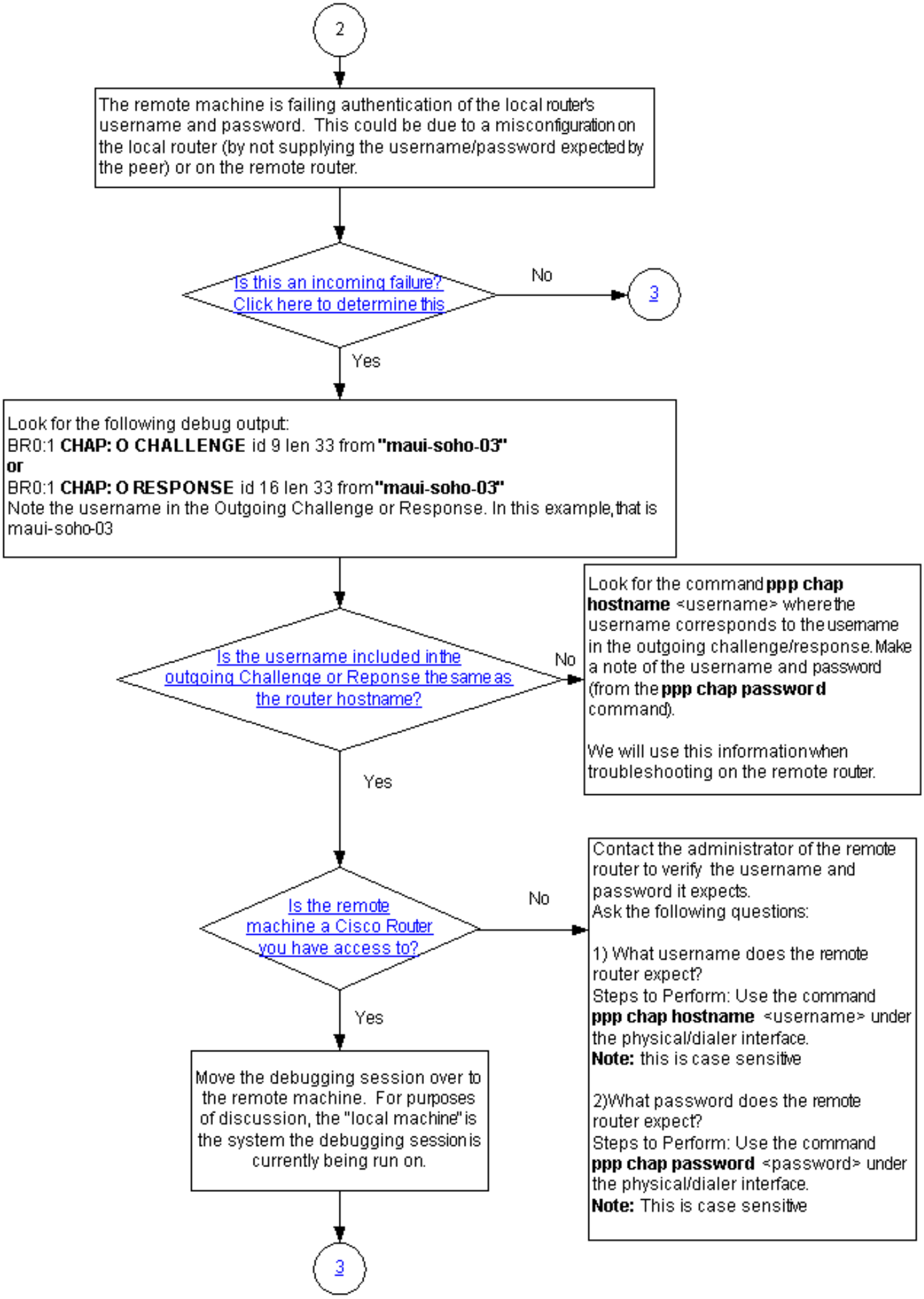
Cualquiera uno de los mensajes abajo indica que el Routers está realizando la autenticación unidireccional:

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

o

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

¿Se trata de una falla entrante?



Marque para ver si usted está recibiendo el termreq o los mensajes de error entrantes. Recuerde

que “” indico que el mensaje es un mensaje entrante:

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

o

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

Una falla entrante indica que el par no está pudiendo autenticar el nombre de usuario y contraseña del router local. Esto debe ser el resultado de un error de configuración en el router local (al no proveer el nombre de usuario y la contraseña que el par esperaba) o en el router remoto.

¿El nombre de usuario en Impugnación o respuesta saliente es igual al nombre de host?

Busque el siguiente en los **resultados de la negociación ppp del debug**:

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

o

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

Observe el nombre de usuario en el desafío o la respuesta saliente. En este ejemplo, es **maui-soho-03**. Usted necesita esto verificar que el nombre de usuario y contraseña usado para la autenticación haga juego el que está esperado por el lado remoto. Por ejemplo, si el router local se identifica al par como A, solamente el par contaba con B, después la autenticación falla.

Si el nombre de usuario en el desafío saliente no es lo mismo que el nombre de host, busque el *<username> del* **comando ppp chap hostname**, donde el nombre de usuario corresponde al nombre de usuario en el desafío saliente. Anote el nombre de usuario y contraseña (en el comando accompanying ppp chap password). Usted utilizará esta información cuando usted resuelve problemas al router remoto.

¿Es la máquina remota un router Cisco al que tenga acceso?

Dado que hemos determinado que el router local recibe una falla entrante, tenemos conocimiento de que la falla se produce en el par. Si usted tiene acceso al router Cisco remoto, después resuelva problemas en ese dispositivo.

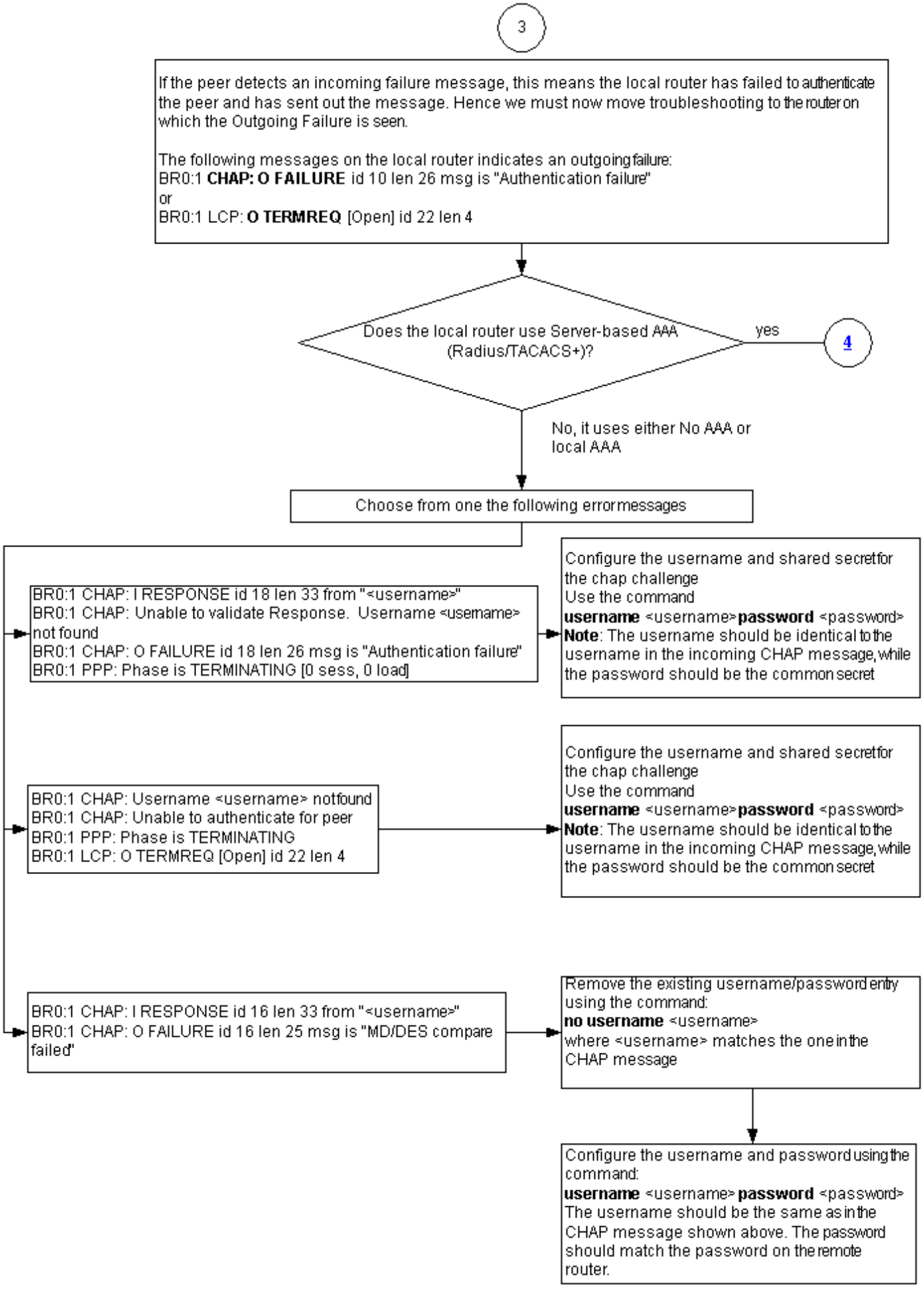
Si usted no tiene acceso al router remoto, entre en contacto al administrador de ese router para verificar el nombre de usuario y contraseña que espera.

Haga estas preguntas:

1. ¿Cuál es el nombre de usuario que espera el router remoto?Utilice el comando del *<username> del* **nombre de host del PPP chap** bajo la comprobación o interfaz del dialer. Configure el nombre de usuario proporcionado por el administrador remoto aquí.**Nota:** Debe respetar las mayúsculas y minúsculas.
2. ¿Qué contraseña el router remoto cuenta con?Utilice **ppp chap password el** *comando <password>* bajo la comprobación o interfaz del dialer.**Nota:** Debe respetar las mayúsculas y minúsculas.

Para más información, refiera a la autenticación PPP del documento usando el nombre de host y los comandos ppp authentication chap callin del PPP chap.

Solución de problemas de fallas CHAP salientes



Si el par detecta un mensaje de la falla entrante, éste significa que el router local no ha podido autenticar al par y que ha enviado el mensaje. Por lo tanto, usted debe ahora resolver problemas al router en quien indica la falla de salida.

Estos mensajes en el router local indican una falla de salida:

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

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

El router no utiliza AAA o utiliza AAA local solamente

Si el router no utiliza una autenticación basada en el servidor, una autorización, y un sistema de las estadísticas (AAA) (radio o Tacacs+), después el router no puede utilizar ningún AAA o el AAA local. Marque si usted ve uno de los siguientes mensajes en la salida de los debugs:

Imposible validar la respuesta

<username> del nombre de usuario no encontrado

```
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]
```

Una falta de coincidencia en el nombre de usuario se puede causar por dos razones:

1. El par no proporcionó el nombre de usuario esperado por el router local. Por ejemplo, contábamos con (y configuró) el nombre de usuario RouterA, pero el par utilizó nombre RouterB. Puede configurar el nombre de usuario y la contraseña enviados por el par o corregir el par con el nombre de usuario correcto.
2. El router local no tiene el nombre de usuario configurado. Si el nombre de usuario suministrado por el par hace juego lo que esperó el router local, después configure el nombre de usuario y contraseña.

Este problema se ve con mayor frecuencia cuando el par utiliza el comando ppp chap hostname para configurar un nombre de usuario distinto de el nombre del host del router.

Utilice el **comando username <username> password <password>**, donde el *<username>* es substituido por el nombre de usuario en el mensaje de error arriba.

<username> del nombre de usuario no encontrado

No se puede autenticar el par.

```
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.
```

Una falta de coincidencia en el nombre de usuario se puede causar por dos razones:

1. El par no proporcionó el nombre de usuario esperado por el router local. Por ejemplo, contábamos con (y configuró) el nombre de usuario RouterA. Sin embargo, el par utilizó nombre RouterB. Usted puede configurar el nombre de usuario y contraseña enviado por el par o poner al día al par con el nombre de usuario correcto.
2. El router local no tiene el nombre de usuario configurado. Si el nombre de usuario suministrado por el par hace juego lo que esperó el router local, después configure el nombre de usuario y contraseña.

Este problema se ve con mayor frecuencia cuando el par utiliza el comando ppp chap hostname para configurar un nombre de usuario distinto de el nombre del host del router.

Utilice el **comando username <username> password <password>**, donde el *<username>* es substituido por el nombre de usuario en el mensaje de error arriba.

El MD/DES compara fallado

```
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"
```

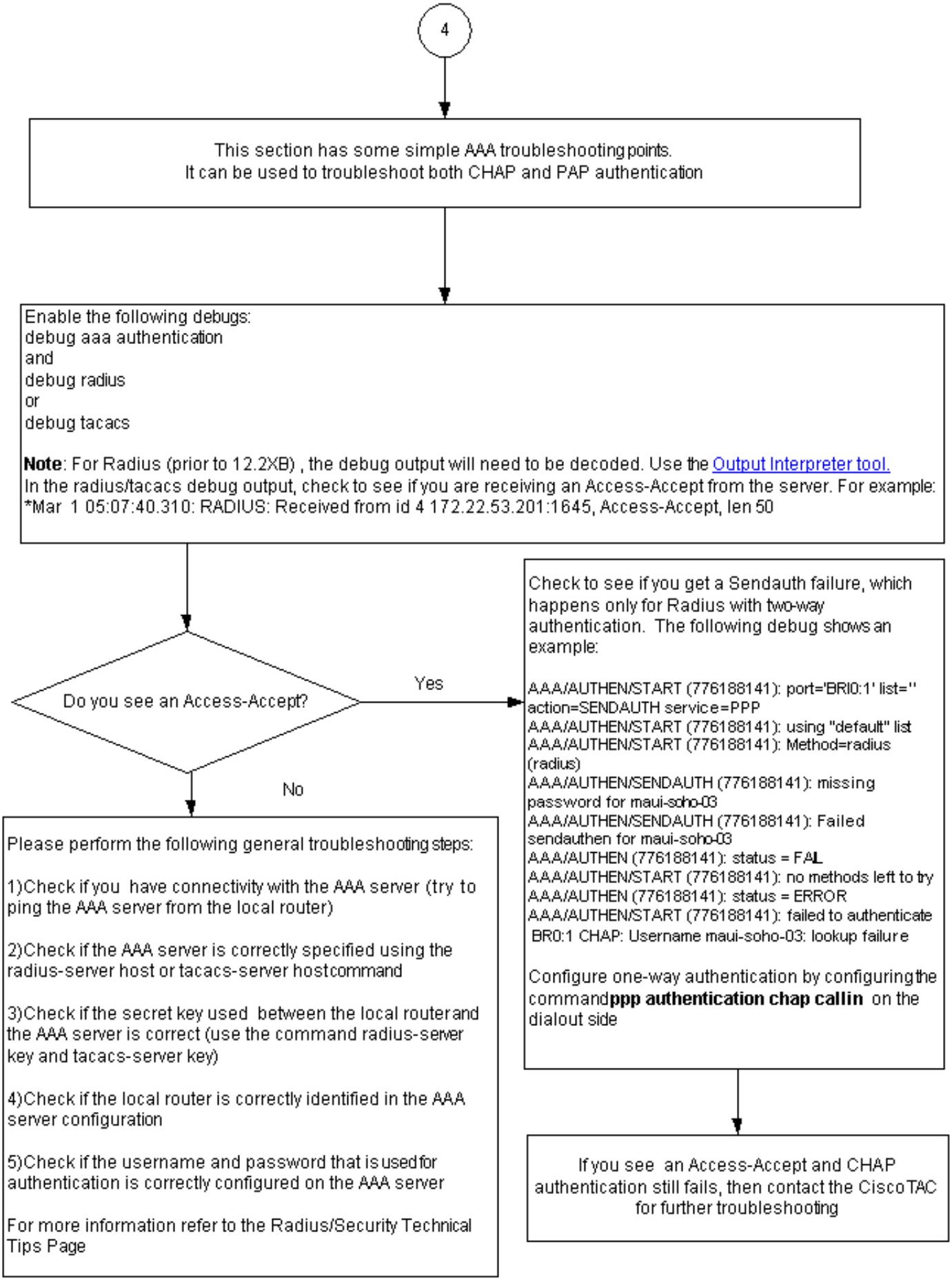
La causa de este error es que no coincide la contraseña. Ésta podía ser causa por dos razones:

1. El par no proporcionó la contraseña esperada por el router local. Por ejemplo, contábamos con (y configuró) la contraseña letmein, pero el par utilizó la contraseña letmein. Puede volver a configurar el nombre de usuario y la contraseña que el par le envió o corregir el par con el nombre de usuario correcto.
2. La contraseña del router local no está configurada de manera correcta. Si usted ha verificado que la contraseña suministrada por el par está correcta, después configure de nuevo al router local.

Solución:

1. Quite la entrada existente del nombre de usuario y contraseña usando este comando: **no username** *<username>* Donde el *<username>* es substituido por el nombre de usuario en el mensaje de error. En este ejemplo, ése sería `maui-soho-03`.
2. Configure el nombre de usuario y contraseña usando este comando: **username** *<username>* **password** *<password>* El nombre de usuario debe ser lo mismo según lo en el mensaje de la GRIETA mostrado arriba. La contraseña debe coincidir con la contraseña en el router remoto

Solución de problemas de AAA basados en el servidor general



Nota: Este documento no constituye un recurso de solución de problemas AAA. Para más información sobre resolver problemas el AAA, refiera a los recursos siguientes:

- Funcionamientos de AAA

- RADIUS
- TACACS

Problema: La autenticación PAP trabaja para el PPP, pero MsCHAPv2 falla

Usted puede ser que no pueda autenticar a un servidor ACS porque el servidor ACS no recibe el pedido de autenticación, que hace una sesión fallar. Este comportamiento se observa y se registra bajo el Id. de bug Cisco CSCee04466 (clientes registrados solamente). Como solución alternativa, utilice a un servidor de RADIUS para las sesiones PPP. Sin embargo, guarde el servidor TACACS+ para fines administrativos en el router.

Información Relacionada

- Introducción al resultado de debug ppp negotiation
- Cómo funciona y se configura la autenticación PPP CHAP
- Autenticación de PPP utilizando los comandos ppp chap hostname y ppp authentication chap callin
- Configuración y resolución de problemas del Protocolo de autenticación de contraseñas (PAP, por sus siglas en inglés) de PPP
- Soporte de Tecnología de Discado y Acceso
- Soporte Técnico y Documentación - Cisco Systems