

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

## Contenido

[Introducción](#)

[Prerequisites](#)

[Terminology](#)

[Requirements](#)

[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.

## [Prerequisites](#)

- Active debug ppp negotiation y **debug ppp authentication**.
- La fase de autenticación PPP no comienza hasta que se complete la fase del protocolo de control de enlaces (LCP) y se encuentre en estado abierto. Si **debug ppp negotiation** no indica que el LCP está abierto, solucione este problema antes de continuar.
- Debe configurarse la Autenticación PPP en ambos lados. Ejecute estos comandos según corresponda: [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](#). [ppp authentication pap](#) en ambos routers, para la autenticación PAP.

## [Terminology](#)

- **Máquina local** (o router local): sistema en el que se está ejecutando actualmente la sesión de depuración. A medida que mueve la sesión de depuración de un router a otro, aplique el término máquina local al otro router.
- **Peer** - El otro extremo del link punto a punto. Por lo tanto, el dispositivo no es la máquina local. Por ejemplo, si ejecuta el comando [debug ppp negotiation en el RouterA, entonces es la máquina local y el RouterB es el par](#). Sin embargo, si cambia la depuración a RouterB, se convierte en la máquina local y el RouterA se convierte en el par.

**Nota:** Los términos máquina local y par no implican una relación cliente-servidor. Dependiendo de dónde se ejecute la sesión de depuración, el cliente de marcado podría ser la máquina local o el par.

## Requirements

Cisco le recomienda que tenga conocimiento acerca 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 Técnicos Cisco para obtener más información sobre las convenciones del documento](#).

## Diagrama de flujo de resolución de problemas

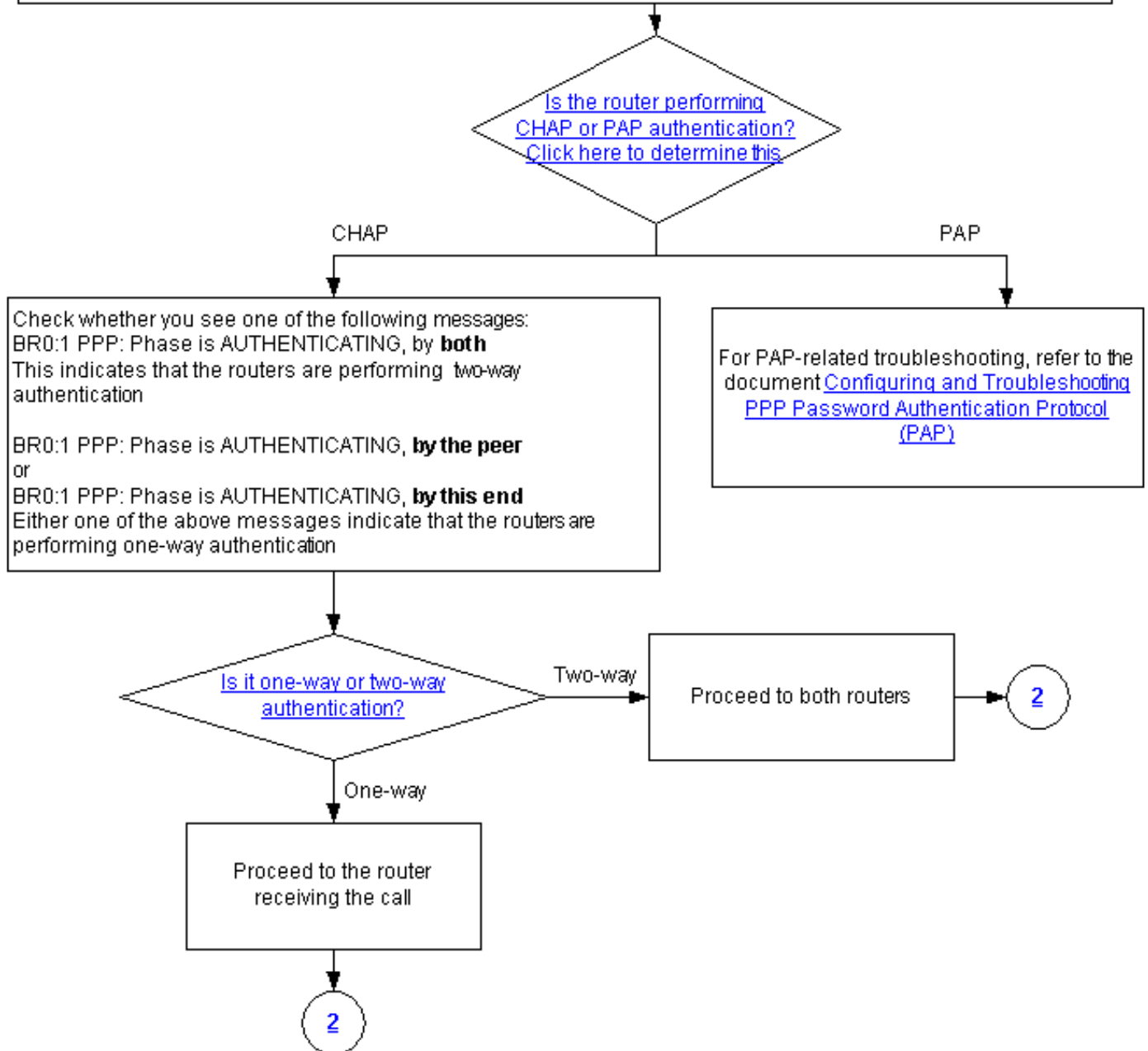
Este documento comprende algunos diagramas de flujo de utilidad en la resolución de problemas. Haga clic en los círculos numerados para continuar con el siguiente diagrama de flujo.

**Note:** Please do not skip any steps in this flowchart

Authentication can be done by both, either or neither side of the connection. Cisco highly recommends using authentication as a way of securing the network against intrusion. Authentication failures are one of the most common problems encountered in PPP negotiation.

**Note:** This document assumes that the LCP state is open. If the LCP state is not open, troubleshoot that issue before proceeding with this document

Enable the following debugs **debug ppp negotiation** and **debug ppp authentication**.



## [¿El router está realizando la autenticación de CHAP o PAP?](#)

Para determinar si el router está realizando la autenticación CHAP o PAP, busque estas líneas en la salida **debug ppp negotiation** y **debug ppp authentication**:

CHAP

Busque CHAP en la fase de AUTENTICACIÓN:

```
*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 PAP en la fase de AUTENTICACIÓN:

```
*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 el resultado `debug ppp negotiation`:

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

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

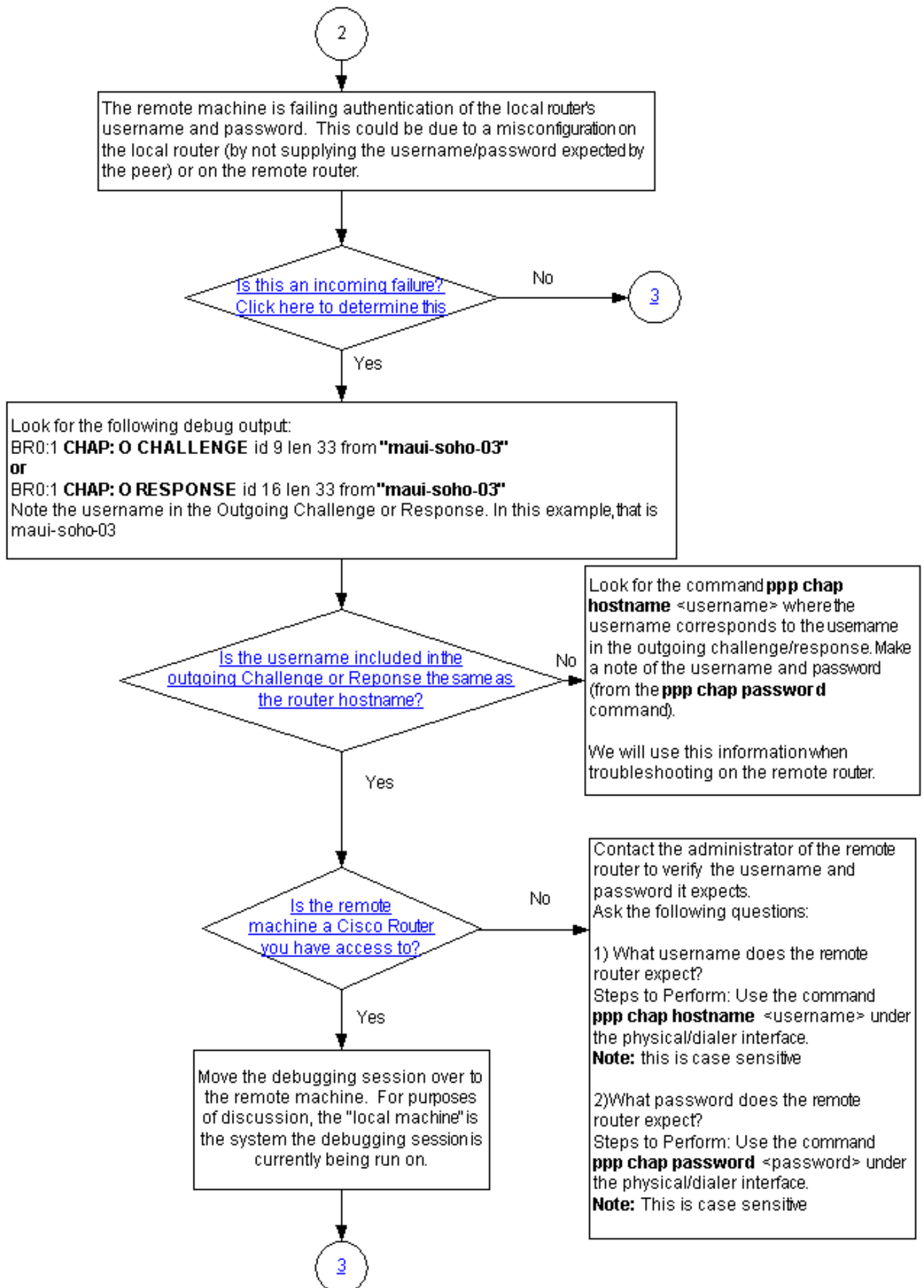
Cualquiera de los siguientes mensajes indica que los routers están realizando una autenticación unidireccional:

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

or

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

[¿Se trata de una falla entrante?](#)



Compruebe si está recibiendo mensajes de error o de termreq entrantes. Recuerde que "I" indica

que el mensaje es un mensaje entrante:

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

or

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

Una falla entrante indica que el par no puede autenticar el nombre de usuario y la 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 lo siguiente en el resultado **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 el nombre de usuario en el desafío o respuesta saliente. En este ejemplo, es **maui-soho-03**. Necesita esto para verificar que el nombre de usuario y la contraseña usados para la autenticación coincidan con el esperado por el lado remoto. Por ejemplo, si el router local se identifica al peer como A, pero el peer esperaba B, entonces la autenticación falla.

Si el nombre de usuario en el desafío saliente no es el mismo que el nombre de host, busque el comando [ppp chap hostname <username>](#), donde el nombre de usuario corresponde al nombre de usuario en el desafío saliente. Anote el nombre de usuario y la contraseña (en el comando **ppp chap password**) que lo acompaña. Utilizará esta información cuando resuelva problemas del 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 tiene acceso al router remoto de Cisco, resuelva los problemas en ese dispositivo.

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

Haga estas preguntas:

1. ¿Cuál es el nombre de usuario que espera el router remoto? Utilice el comando [ppp chap hostname <username>](#) bajo la interfaz física o dialer. Configure el nombre de usuario proporcionado por el administrador remoto aquí. **Nota:** Distingue entre mayúsculas y minúsculas.

2. ¿Qué contraseña espera el router remoto? Utilice el comando [ppp chap password <password>](#) bajo la interfaz física o dialer. **Nota:** Distingue entre mayúsculas y minúsculas. Para obtener más información, refiérase al documento [Autenticación PPP Usando los Comandos ppp chap hostname y ppp authentication chap callin](#).

## [Solución de problemas de fallas CHAP salientes](#)

If the peer detects an incoming failure message, this means the local router has failed to authenticate the peer and has sent out the message. Hence we must now move troubleshooting to the router on which the Outgoing Failure is seen.

The following messages on the local router indicates an outgoing failure:  
 BR0:1 CHAP: O FAILURE id 10 len 26 msg is "Authentication failure"  
 or  
 BR0:1 LCP: O TERMREQ [Open] id 22 len 4

Does the local router use Server-based AAA  
(Radius/TACACS+)?

yes

4

No, it uses either No AAA or  
local AAA

Choose from one the following error messages

BR0:1 CHAP: I RESPONSE id 18 len 33 from "<username>"  
 BR0:1 CHAP: Unable to validate Response. Username <username>  
 not found  
 BR0:1 CHAP: O FAILURE id 18 len 26 msg is "Authentication failure"  
 BR0:1 PPP: Phase is TERMINATING [0 sess, 0 load]

Configure the username and shared secret for  
the chap challenge  
Use the command  
**username <username> password <password>**  
**Note:** The username should be identical to the  
username in the incoming CHAP message, while  
the password should be the common secret

BR0:1 CHAP: Username <username> not found  
 BR0:1 CHAP: Unable to authenticate for peer  
 BR0:1 PPP: Phase is TERMINATING  
 BR0:1 LCP: O TERMREQ [Open] id 22 len 4

Configure the username and shared secret for  
the chap challenge  
Use the command  
**username <username> password <password>**  
**Note:** The username should be identical to the  
username in the incoming CHAP message, while  
the password should be the common secret

BR0:1 CHAP: I RESPONSE id 16 len 33 from "<username>"  
 BR0:1 CHAP: O FAILURE id 16 len 25 msg is "MD/DES compare  
failed"

Remove the existing username/password entry  
using the command:  
**no username <username>**  
 where <username> matches the one in the  
CHAP message

Configure the username and password using the  
command:  
**username <username> password <password>**  
 The username should be the same as in the  
CHAP message shown above. The password  
should match the password on the remote  
router.

Si el par detecta un mensaje de falla entrante, esto significa que el router local no ha podido autenticar el par y ha enviado el mensaje. Por lo tanto, ahora debe resolver los problemas del



router en el que se indica la falla saliente.

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

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

or

```
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 un sistema de autenticación, autorización y contabilidad (AAA) basado en servidor (Radius o Tacacs+), el router puede utilizar no AAA o AAA local. Compruebe si ve uno de los siguientes mensajes en el resultado de la depuración:

### Imposible validar la respuesta

#### Nombre de usuario *<username>* 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 discordancia de nombre de usuario puede deberse a dos razones:

1. El par no proporcionó el nombre de usuario esperado por el router local. Por ejemplo, esperábamos (y configuramos) el nombre de usuario RouterA, pero el par utilizó el 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 proporcionado por el par coincide con lo que esperaba el router local, configure el nombre de usuario y la 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 *<username>* se reemplaza por el nombre de usuario en el mensaje de error anterior.

#### Nombre de usuario *<username>* 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 discordancia de nombre de usuario puede deberse a dos razones:

1. El par no proporcionó el nombre de usuario esperado por el router local. Por ejemplo, esperábamos (y configuramos) el nombre de usuario RouterA. Sin embargo, el par utilizó el nombre RouterB. Puede configurar el nombre de usuario y la contraseña enviados por el par o actualizar el par con el nombre de usuario correcto.
2. El router local no tiene el nombre de usuario configurado. Si el nombre de usuario proporcionado por el par coincide con lo que esperaba el router local, configure el nombre de usuario y la 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 `<username>` se reemplaza por el nombre de usuario en el mensaje de error anterior.

## Error al comparar 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"
```

La causa de este error es que no coincide la contraseña. Esto podría deberse a dos razones:

1. El par no proporcionó la contraseña esperada por el router local. Por ejemplo, esperábamos (y configuramos) la contraseña *Letmein*, pero el par usó 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 ha verificado que la contraseña proporcionada por el par es correcta, vuelva a configurar el router local.

### Solución:

1. Quite el nombre de usuario y la entrada de contraseña existentes mediante este comando:

```
no username <username>
```

Donde `<username>` se reemplaza por el nombre de usuario en el mensaje de error. En este ejemplo, sería `maui-soho-03`.

2. Configure el nombre de usuario y la contraseña mediante este comando:

```
username password
```

El nombre de usuario debe ser el mismo que en el mensaje CHAP que se muestra arriba. La contraseña debe coincidir con la contraseña en el router remoto

## [Solución de problemas de AAA basados en el servidor general](#)

4

This section has some simple AAA troubleshooting points.  
It can be used to troubleshoot both CHAP and PAP authentication

Enable the following debugs:  
debug aaa authentication  
and  
debug radius  
or  
debug tacacs

**Note:** For Radius (prior to 12.2XB) , the debug output will need to be decoded. Use the [Output Interpreter tool](#).  
In the radius/tacacs debug output, check to see if you are receiving an Access-Accept from the server. For example:  
\*Mar 1 05:07:40.310: RADIUS: Received from id 4 172.22.53.201:1645, Access-Accept, len 50

Do you see an Access-Accept?

Yes

No

Check to see if you get a Sendauth failure, which happens only for Radius with two-way authentication. The following debug shows an example:

```
AAA/AUTHEN/START (776188141): port='BR0:1' list=""  
action=SENDAUTH service=PPP  
AAA/AUTHEN/START (776188141): using "default" list  
AAA/AUTHEN/START (776188141): Method=radius  
(radius)  
AAA/AUTHEN/SENDAUTH (776188141): missing  
password for maui-soho-03  
AAA/AUTHEN/SENDAUTH (776188141): Failed  
sendauthen for maui-soho-03  
AAA/AUTHEN (776188141): status = FAIL  
AAA/AUTHEN/START (776188141): no methods left to try  
AAA/AUTHEN (776188141): status = ERROR  
AAA/AUTHEN/START (776188141): failed to authenticate  
BR0:1 CHAP: Username maui-soho-03: lookup failure
```

Configure one-way authentication by configuring the command **ppp authentication chap callin** on the dialout side

Please perform the following general troubleshooting steps:

- 1) Check if you have connectivity with the AAA server (try to ping the AAA server from the local router)
- 2) Check if the AAA server is correctly specified using the radius-server host or tacacs-server host command
- 3) Check if the secret key used between the local router and the AAA server is correct (use the command radius-server key and tacacs-server key)
- 4) Check if the local router is correctly identified in the AAA server configuration
- 5) Check if the username and password that is used for authentication is correctly configured on the AAA server

For more information refer to the Radius/Security Technical Tips Page

If you see an Access-Accept and CHAP authentication still fails, then contact the Cisco TAC for further troubleshooting

**Nota:** Este documento no está diseñado como un recurso de solución de problemas AAA. Para obtener más información sobre la solución de problemas de AAA, consulte los siguientes recursos:

- [Operaciones AAA](#)
- [RADIUS](#)
- [TACACS](#)

### Problema: La autenticación PAP funciona para PPP, pero MsCHAPv2 falla

Es posible que no pueda autenticarse en un servidor ACS porque el servidor ACS no recibe la solicitud de autenticación, lo que hace que una sesión falle. Este comportamiento se observa y registra con el ID de bug de Cisco [CSCee04466](#) ([sólo](#) clientes registrados) . Como solución alternativa, utilice un servidor RADIUS para las sesiones PPP. Sin embargo, mantenga el servidor TACACS+ con 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](#)