

Fehlerbehebung Authentifizierung nach PPP (CHAP oder PAP)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Terminologie](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Fehlerbehebung Flussdiagramm](#)

[Führt der Router eine CHAP- oder PAP-Authentifizierung durch?](#)

[Führt der Router eine unidirektionale oder bidirektionale CHAP-Authentifizierung durch?](#)

[Handelt es sich um einen eingehenden Fehler?](#)

[Entspricht der Benutzername bei der ausgehenden Challenge oder die Antwort dem Hostnamen?](#)

[Ist das Remote-System ein Cisco Router, auf den Sie Zugriff haben?](#)

[Fehlerbehebung bei ausgehenden CHAP-Fehlern](#)

[Der Router verwendet kein AAA oder nur lokales AAA.](#)

[Fehlerbehebung bei allgemeinen serverbasierten AAA-Problemen](#)

[Zugehörige Informationen](#)

Einführung

Probleme mit der Point-to-Point Protocol (PPP)-Authentifizierung sind eine der häufigsten Ursachen für Fehler bei der DFÜ-Verbindung. Dieses Dokument enthält einige Verfahren zur Fehlerbehebung bei Problemen mit der PPP-Authentifizierung.

Voraussetzungen

- Aktivieren Sie **Debug-PPP-Aushandlung** und **Debug-PPP-Authentifizierung**.
- Die PPP-Authentifizierungsphase beginnt erst, wenn die Phase des Link Control Protocol (LCP) abgeschlossen ist und sich im offenen Zustand befindet. Wenn **Debug-PPP-Aushandlung** nicht anzeigt, dass LCP offen ist, beheben Sie dieses Problem, bevor Sie fortfahren.
- Die PPP-Authentifizierung muss auf beiden Seiten konfiguriert werden. Führen Sie diese Befehle ggf. aus: [ppp-Authentifizierungskap](#) auf beiden Routern für die Zwei-Wege-Challenge Handshake Authentication Protocol (CHAP)-Authentifizierung. [ppp-Authentifizierungs-chap-Anruf](#) für die unidirektionale Authentifizierung auf dem anrufenden Router. [ppp-Authentifizierungspopp](#) auf beiden Routern für die PAP-Authentifizierung.

Terminologie

- **Lokaler Computer** (oder lokaler Router) - Dies ist das System, auf dem die Debugsitzung derzeit ausgeführt wird. Wenn Sie die Debugsitzung von einem Router zum anderen verschieben, wenden Sie den Begriff "lokales System" auf den anderen Router an.
- **Peer** - Das andere Ende der Punkt-zu-Punkt-Verbindung. Daher ist das Gerät nicht der lokale Computer. Wenn Sie beispielsweise den **Befehl [debug ppp negotiation](#) auf RouterA** ausgeben, dann ist dies der lokale Computer, und RouterB ist der Peer. Wenn Sie das Debuggen jedoch auf RouterB verschieben, wird dieser zum lokalen Computer und RouterA zum Peer.

Hinweis: Die Begriffe "lokales System" und "Peer" implizieren keine Beziehung zwischen Client und Server. Je nachdem, wo die Debugsitzung ausgeführt wird, kann der Einwahlclient der lokale Computer oder Peer sein.

Anforderungen

Cisco empfiehlt, über Kenntnisse in diesem Bereich zu verfügen:

- Sie müssen in der Lage sein, die Debug-ppp-Aushandlung zu lesen und zu verstehen. Weitere Informationen finden Sie im Dokument [Understanding debug ppp negotiation Output](#) for more information.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Fehlerbehebung Flussdiagramm

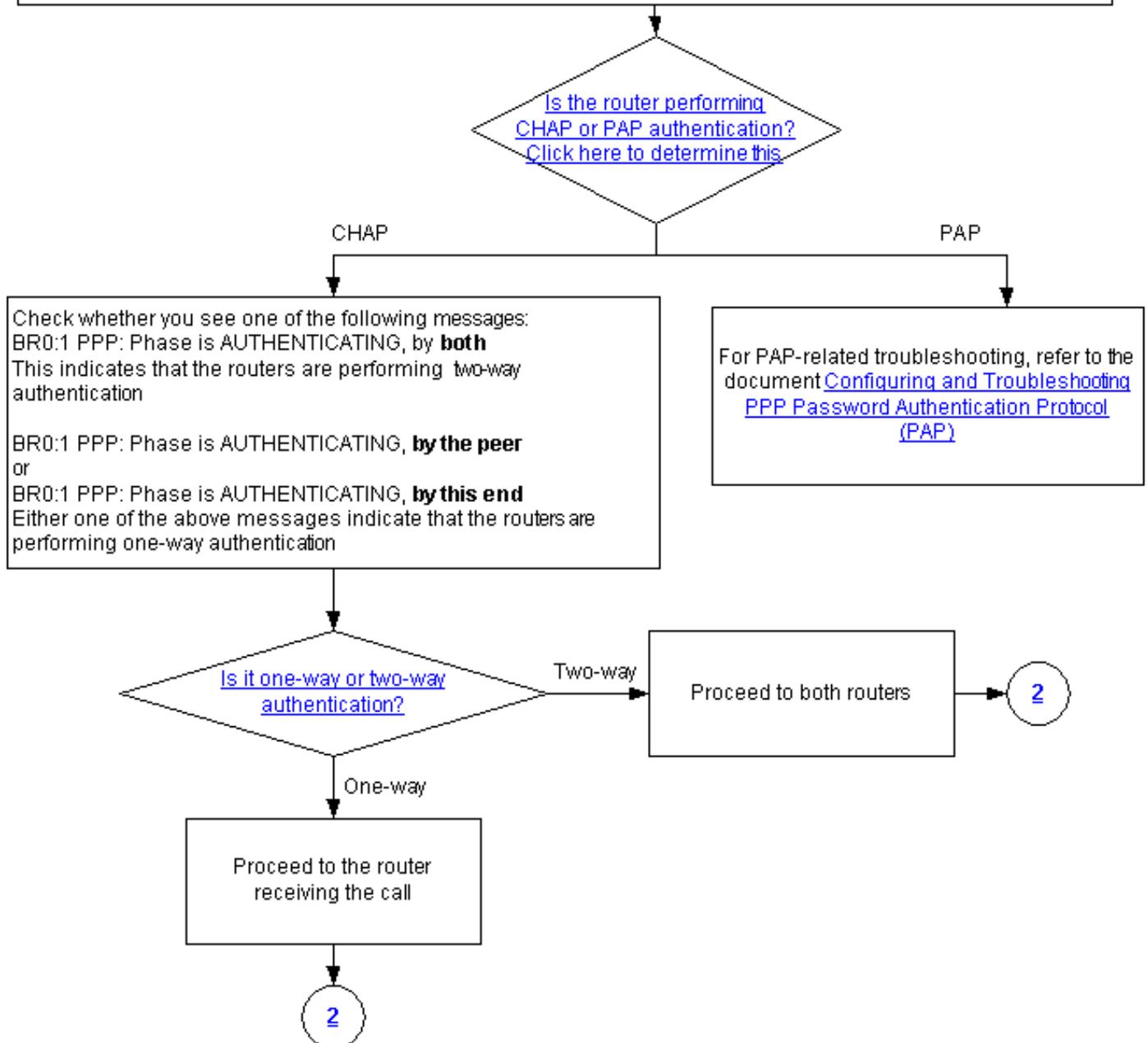
Dieses Dokument enthält Ablaufdiagramme, die bei der Fehlerbehebung helfen. Sie können mit dem nächsten Flussdiagramm fortfahren, indem Sie auf die nummerierten Kreise klicken.

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**.



Führt der Router eine CHAP- oder PAP-Authentifizierung durch?

Um festzustellen, ob der Router die CHAP- oder PAP-Authentifizierung durchführt, suchen Sie in der **Debug-ppp-Aushandlung** und in der **Debug-ppp-Authentifizierungsausgabe** nach diesen Zeilen:

CHAP

Suchen Sie in der AUTHENTIFIZIERUNGsphase nach CHAP:

```
*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

Suchen Sie in der AUTHENTIFIZIERUNGsphase nach PAP:

```
*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"
```

[Führt der Router eine unidirektionale oder bidirektionale CHAP-Authentifizierung durch?](#)

Suchen Sie in der **Debug-ppp-Aushandlung** nach einer dieser Meldungen:

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

Die obige Meldung weist darauf hin, dass die Router eine Zwei-Wege-Authentifizierung durchführen.

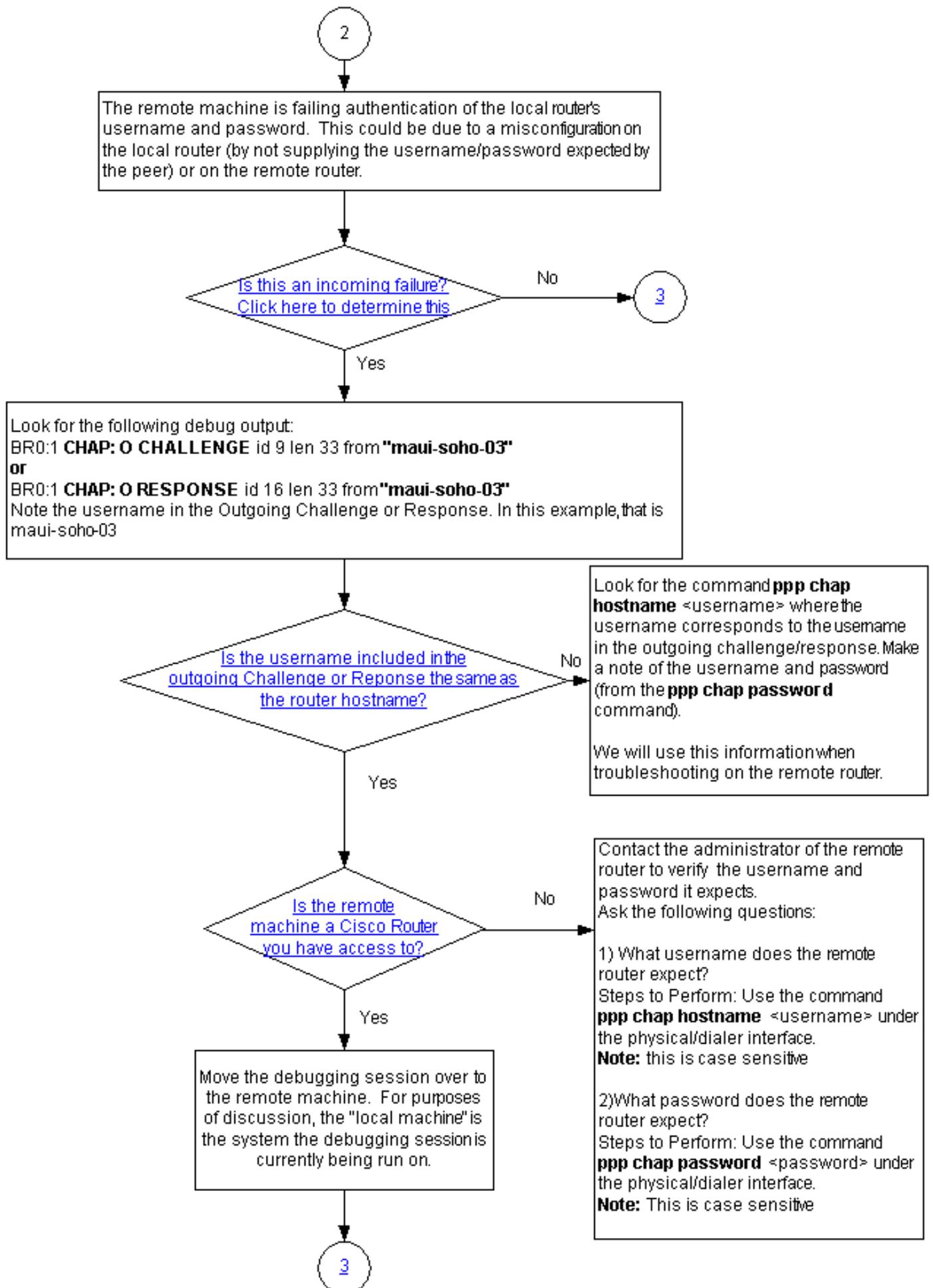
Eine der folgenden Meldungen weist darauf hin, dass die Router eine unidirektionale Authentifizierung durchführen:

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

oder

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

[Handelt es sich um einen eingehenden Fehler?](#)



Überprüfen Sie, ob Sie eingehende Termreq- oder Fehlermeldungen erhalten. Denken Sie daran,

dass "I" bedeutet, dass es sich bei der Nachricht um eine eingehende Nachricht handelt:

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

oder

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

Ein eingehender Fehler weist darauf hin, dass der Peer den Benutzernamen und das Kennwort des lokalen Routers nicht authentifiziert. Dies kann auf eine Fehlkonfiguration des lokalen Routers (durch Nichtbereitstellung des vom Peer erwarteten Benutzernamen und Kennworts) oder des Remote-Routers zurückzuführen sein.

Entspricht der Benutzername bei der ausgehenden Challenge oder die Antwort dem Hostnamen?

Suchen Sie in der **Debug-ppp-Aushandlung** folgende Punkte:

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

oder

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

Notieren Sie den Benutzernamen in der ausgehenden Herausforderung oder Antwort. In diesem Beispiel ist es **maui-soho-03**. Sie müssen dies tun, um sicherzustellen, dass der für die Authentifizierung verwendete Benutzername und das Kennwort mit dem von der Außenstelle erwarteten übereinstimmen. Wenn sich der lokale Router beispielsweise für den Peer als A identifiziert, aber der Peer B erwartet hat, schlägt die Authentifizierung fehl.

Wenn der Benutzername in der ausgehenden Challenge nicht mit dem Hostnamen übereinstimmt, suchen Sie den Befehl [ppp chap hostname <username>, wobei der Benutzername dem Benutzernamen in der ausgehenden Challenge entspricht](#). Notieren Sie sich den Benutzernamen und das Kennwort (im zugehörigen Befehl **ppp chap password**). Diese Informationen werden bei der Fehlerbehebung für den Remote-Router verwendet.

Ist das Remote-System ein Cisco Router, auf den Sie Zugriff haben?

Da festgestellt wurde, dass der lokale Router einen eingehenden Ausfall erhalten hat, wissen wir, dass der Fehler auf dem Peer auftritt. Wenn Sie Zugriff auf den Remote-Router von Cisco haben, führen Sie eine Fehlerbehebung für dieses Gerät durch.

Wenn Sie keinen Zugriff auf den Remote-Router haben, wenden Sie sich an den Administrator dieses Routers, um den Benutzernamen und das Kennwort zu überprüfen, die er erwartet.

Stellen Sie folgende Fragen:

1. Welchen Benutzernamen erwartet der Remote-Router? Verwenden Sie den Befehl [ppp chap hostname <username> unter der physischen oder Dialer-Schnittstelle](#). Konfigurieren Sie hier den vom Remote-Administrator bereitgestellten Benutzernamen. **Hinweis:** Groß- und

Kleinschreibung beachten.

2. Welches Kennwort erwartet der Remote-Router? Verwenden Sie den Befehl `ppp chap password <password>` unter der physischen oder Dialer-Schnittstelle. Hinweis: Groß- und Kleinschreibung beachten.

Weitere Informationen finden Sie im Dokument [PPP Authentication Using the ppp chap hostname and ppp authentication chap callin Commands](#).

Fehlerbehebung bei ausgehenden CHAP-Fehlern

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.

Wenn der Peer eine eingehende Fehlermeldung erkennt, bedeutet dies, dass der lokale Router den Peer nicht authentifiziert hat und die Nachricht gesendet hat. Daher müssen Sie jetzt eine

Fehlerbehebung für den Router durchführen, der den ausgehenden Ausfall anzeigt.

Diese Meldungen auf dem lokalen Router weisen auf einen ausgehenden Fehler hin:

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

oder

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

Der Router verwendet kein AAA oder nur lokales AAA.

Wenn der Router kein serverbasiertes AAA-System (Authentication, Authorization, Accounting) (Radius oder TACACS+) verwendet, kann der Router entweder kein AAA oder lokales AAA verwenden. Überprüfen Sie, ob eine der folgenden Meldungen in der Debugausgabe angezeigt wird:

Antwort konnte nicht validiert werden

Benutzername <Benutzername> Nicht gefunden

```
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]
```

Eine Nichtübereinstimmung mit einem Benutzernamen kann aus zwei Gründen verursacht werden:

1. Der Peer hat den vom lokalen Router erwarteten Benutzernamen nicht bereitgestellt. Wir hatten beispielsweise den Benutzernamen RouterA erwartet (und konfiguriert), der Peer jedoch den Namen RouterB verwendet. Sie können entweder den vom Peer gesendeten Benutzernamen und das Kennwort konfigurieren oder den Peer mit dem richtigen Benutzernamen korrigieren.
2. Auf dem lokalen Router ist der Benutzername nicht konfiguriert. Wenn der vom Peer bereitgestellte Benutzername mit dem vom lokalen Router erwarteten Benutzernamen übereinstimmt, konfigurieren Sie den Benutzernamen und das Kennwort.

Dieses Problem tritt am häufigsten auf, wenn der Peer den **Befehl [ppp chap hostname](#)** zum Konfigurieren eines anderen Benutzernamens als des Router-Hostnamens verwendet.

Verwenden Sie den Befehl **username <username> password <password>**, wobei **<Benutzername>** in der obigen Fehlermeldung durch den Benutzernamen ersetzt wird.

Benutzername <Benutzername> Nicht gefunden

Authentifizierung für Peer nicht möglich

```
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.
```

Eine Nichtübereinstimmung mit einem Benutzernamen kann aus zwei Gründen verursacht werden:

1. Der Peer hat den vom lokalen Router erwarteten Benutzernamen nicht bereitgestellt. Wir haben beispielsweise den Benutzernamen RouterA erwartet (und konfiguriert). Der Peer verwendete jedoch den Namen RouterB. Sie können entweder den vom Peer gesendeten Benutzernamen und das Kennwort konfigurieren oder den Peer mit dem richtigen Benutzernamen aktualisieren.
2. Auf dem lokalen Router ist der Benutzername nicht konfiguriert. Wenn der vom Peer bereitgestellte Benutzername mit dem vom lokalen Router erwarteten Benutzernamen übereinstimmt, konfigurieren Sie den Benutzernamen und das Kennwort.

Dieses Problem tritt am häufigsten auf, wenn der Peer den **Befehl `ppp chap hostname`** zum Konfigurieren eines anderen Benutzernamens als des Router-Hostnamens verwendet.

Verwenden Sie den Befehl `username <username> password <password>`, wobei **<Benutzername>** in der obigen Fehlermeldung durch den Benutzernamen ersetzt wird.

Vergleich von MD/DES fehlgeschlagen

```
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"
```

Dieser Fehler wird durch eine Kennwortungleichheit verursacht. Dies kann aus zwei Gründen geschehen:

1. Der Peer hat das vom lokalen Router erwartete Kennwort nicht angegeben. Zum Beispiel erwarteten (und konfigurierten) wir das Kennwort *Letmein*, aber der Peer verwendete das Kennwort *letmein*. Sie können entweder den vom Peer gesendeten Benutzernamen und das Kennwort neu konfigurieren oder den Peer mit dem richtigen Benutzernamen korrigieren.
2. Das Kennwort des lokalen Routers ist nicht korrekt konfiguriert. Wenn Sie überprüft haben, dass das vom Peer angegebene Kennwort korrekt ist, konfigurieren Sie den lokalen Router neu.

Lösung:

1. Entfernen Sie den vorhandenen Benutzernamen und das vorhandene Kennwort mit dem folgenden Befehl:

```
no username <username>
```

Dabei wird **<Benutzername>** in der Fehlermeldung durch den Benutzernamen ersetzt. In diesem Beispiel wäre das `maui-soho-03`.

2. Konfigurieren Sie den Benutzernamen und das Kennwort mit dem folgenden Befehl:

```
username password
```

Der Benutzername muss mit der CHAP-Nachricht oben übereinstimmen. Das Kennwort sollte mit dem Kennwort des Remote-Routers übereinstimmen.

[Fehlerbehebung bei allgemeinen serverbasierten AAA-Problemen](#)

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=SENAUTH service=PPP  
AAA/AUTHEN/START (776188141): using "default" list  
AAA/AUTHEN/START (776188141): Method=radius  
(radius)  
AAA/AUTHEN/SENAUTH (776188141): missing  
password for maui-soho-03  
AAA/AUTHEN/SENAUTH (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

Hinweis: Dieses Dokument ist nicht als Ressource zur AAA-Fehlerbehebung vorgesehen. Weitere Informationen zur AAA-Fehlerbehebung finden Sie in den folgenden Ressourcen:

- [AAA-Operationen](#)

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

[Problem: PAP-Authentifizierung funktioniert für PPP, aber MSCHAPv2 schlägt fehl](#)

Sie können sich möglicherweise nicht bei einem ACS-Server authentifizieren, da der ACS-Server die Authentifizierungsanforderung nicht empfängt, was dazu führt, dass eine Sitzung fehlschlägt. Dieses Verhalten wird unter der Cisco Bug ID [CSCee04466](#) beobachtet und protokolliert (nur [registrierte](#) Kunden). Verwenden Sie als Problemumgehung einen RADIUS-Server für PPP-Sitzungen. Behalten Sie jedoch den TACACS+-Server für administrative Zwecke auf dem Router bei.

[Zugehörige Informationen](#)

- [Debugging-PPP-Aushandlung](#)
- [PPP CHAP-Authentifizierung verstehen und konfigurieren](#)
- [PPP-Authentifizierung mit dem PPP-chap-Hostnamen und den ppp-Authentifizierungschap-Callin-Befehlen](#)
- [Konfiguration und Fehlerbehebung für PPP Password Authentication Protocol \(PAP\)](#)
- [Unterstützung von DFÜ- und Zugriffstechnologie](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)