

Risoluzione dei problemi di autenticazione PPP (CHAP o PAP)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Terminologia](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Diagramma di flusso per la risoluzione dei problemi](#)

[Il router esegue l'autenticazione CHAP o PAP?](#)

[Il router esegue l'autenticazione CHAP unidirezionale o bidirezionale?](#)

[Si tratta di un errore in entrata?](#)

[Il nome utente nella richiesta di verifica o risposta in uscita è uguale al nome host?](#)

[Il computer remoto è un router Cisco a cui si ha accesso?](#)

[Risoluzione dei problemi relativi agli errori CHAP in uscita](#)

[Il router non utilizza AAA o solo AAA locale](#)

[Risoluzione dei problemi generali dei server AAA](#)

[Informazioni correlate](#)

Introduzione

I problemi di autenticazione PPP (Point-to-Point Protocol) sono una delle cause più comuni degli errori dei collegamenti di connessione remota. In questo documento vengono descritte alcune procedure di risoluzione dei problemi relativi all'autenticazione PPP.

Prerequisiti

- Abilitare la **negoziazione ppp di debug** e l'**autenticazione ppp di debug**.
- La fase di autenticazione PPP non inizia finché la fase LCP (Link Control Protocol) non è completata e non si trova nello stato aperto. Se la **negoziazione PPP di debug** non indica che LCP è aperto, risolvere il problema prima di procedere.
- L'autenticazione PPP deve essere configurata su entrambi i lati. Utilizzare i seguenti comandi come appropriato: [chap di autenticazione ppp](#) su entrambi i router, per autenticazione CHAP (Challenge Handshake Authentication Protocol) bidirezionale. [chiamata chap di autenticazione ppp](#) sul router chiamante, per autenticazione unidirezionale. [app di autenticazione ppp](#) su entrambi i router, per l'autenticazione PAP.

Terminologia

- **Computer locale** (o router locale): sistema su cui è in esecuzione la sessione di debug. Quando si sposta la sessione di debug da un router all'altro, applicare il termine computer locale all'altro router.
- **Peer** - L'altra estremità del collegamento point-to-point. Pertanto, il dispositivo non è il computer locale. Ad esempio, se si esegue il comando [debug ppp negotiation](#) sul router A, questo sarà il computer locale e il router B sarà il peer. Tuttavia, se si passa il debug al router B, questo diventa il computer locale e il router A diventa il peer.

Nota: i termini computer locale e peer non implicano una relazione client-server. A seconda della posizione in cui viene eseguita la sessione di debug, il client di chiamata in ingresso potrebbe essere il computer locale o il peer.

Requisiti

Cisco raccomanda la conoscenza di questo argomento:

- È necessario essere in grado di leggere e comprendere l'output della negoziazione PPP di debug. Per ulteriori informazioni, consultare il documento [Descrizione dell'output della negoziazione PPP di debug](#).

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Diagramma di flusso per la risoluzione dei problemi

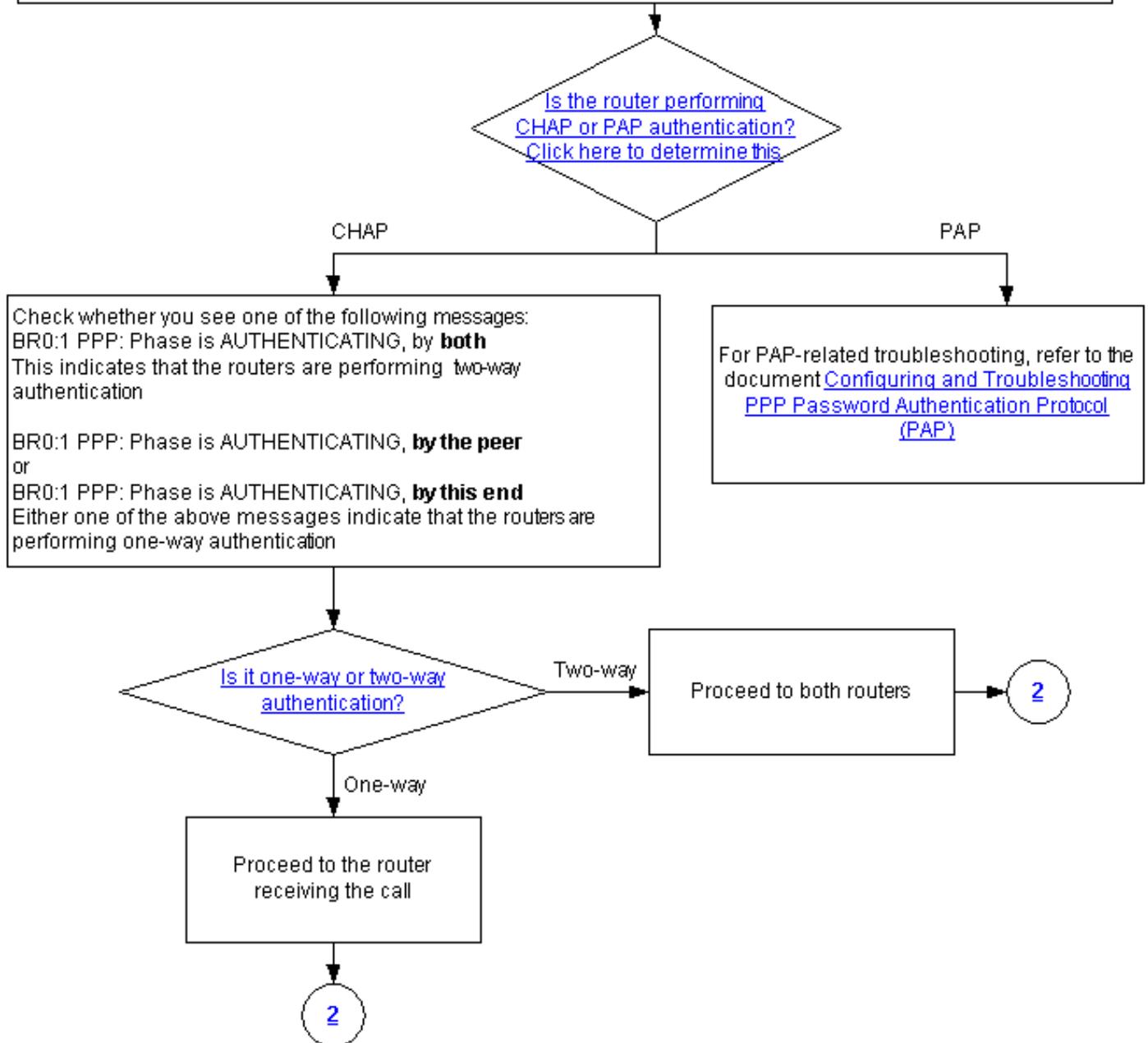
Questo documento include alcuni diagrammi di flusso per agevolare la risoluzione dei problemi. È possibile passare al diagramma di flusso successivo facendo clic sui cerchi numerati.

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**.



[Il router esegue l'autenticazione CHAP o PAP?](#)

Per determinare se il router sta eseguendo l'autenticazione CHAP o PAP, cercare queste righe nell'output della **negoziazione PPP di debug** e dell'**autenticazione PPP di debug**:

CHAP

Cercare CHAP nella fase 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

Cercare PAP nella fase 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"
```

[Il router esegue l'autenticazione CHAP unidirezionale o bidirezionale?](#)

Cercare uno dei messaggi seguenti nell'output della **negoziazione PPP di debug**:

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

Il messaggio precedente indica che i router stanno eseguendo l'autenticazione bidirezionale.

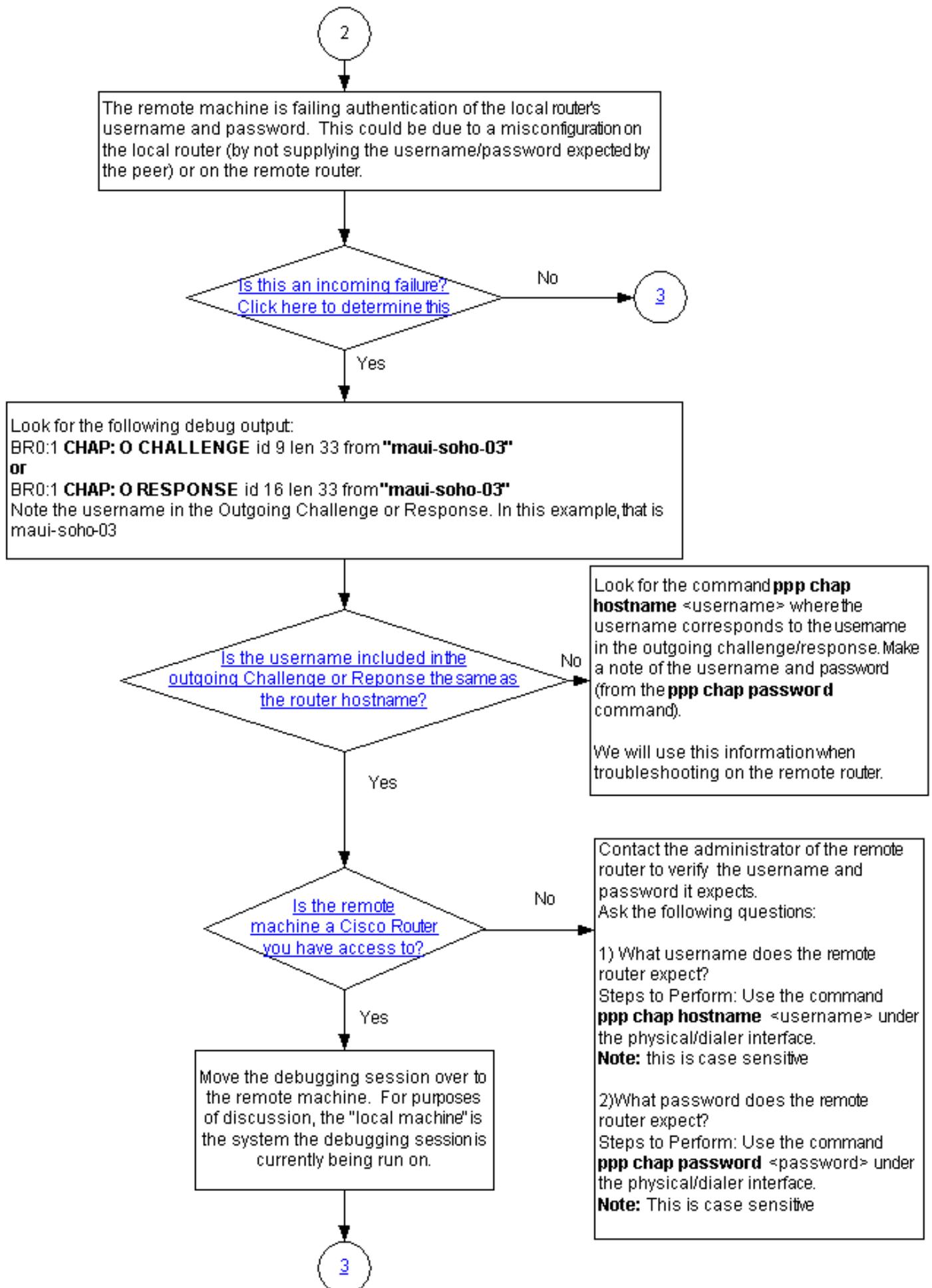
Uno dei messaggi seguenti indica che i router stanno eseguendo l'autenticazione unidirezionale:

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

O

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

[Si tratta di un errore in entrata?](#)



Verificare se si ricevono messaggi termreq o di errore in arrivo. Tenere presente che la lettera "l"

indica che il messaggio è in arrivo:

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

O

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

Un errore in ingresso indica che il peer non riesce ad autenticare il nome utente e la password del router locale. Ciò potrebbe essere dovuto a una configurazione errata sul router locale (non fornendo il nome utente e la password previsti dal peer) o sul router remoto.

Il nome utente nella richiesta di verifica o risposta in uscita è uguale al nome host?

Cercare quanto segue nell'output della **negoziazione PPP di 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"
```

Annotare il nome utente nella richiesta di verifica o nella risposta in uscita. In questo esempio il valore è **maui-soho-03**. È necessario verificare che il nome utente e la password utilizzati per l'autenticazione corrispondano a quelli previsti dal lato remoto. Ad esempio, se il router locale si identifica al peer come A, ma il peer si aspettava B, l'autenticazione non riesce.

Se il nome utente nella richiesta di verifica in uscita non è uguale al nome host, cercare il comando [ppp chap hostname <nome utente>](#), dove il nome utente corrisponde al nome utente nella richiesta di verifica in uscita. Prendere nota del nome utente e della password (nel comando **ppp chap password** associato). Queste informazioni verranno utilizzate per la risoluzione dei problemi relativi al router remoto.

Il computer remoto è un router Cisco a cui si ha accesso?

Poiché è stato determinato che il router locale ha ricevuto un errore in ingresso, è noto che l'errore si sta verificando sul peer. Se si dispone dell'accesso al router Cisco remoto, eseguire la risoluzione dei problemi su tale dispositivo.

Se non si dispone dell'accesso al router remoto, contattare l'amministratore del router per verificare il nome utente e la password previsti.

Fai queste domande:

1. Nome utente previsto dal router remoto Usare il comando [ppp chap hostname <nomeutente>](#) nell'interfaccia fisica o di connessione. Configurare qui il nome utente fornito dall'amministratore remoto. **Nota:** fa distinzione tra maiuscole e minuscole.
2. Quale password è prevista per il router remoto? Usare il comando [ppp chap password <password>](#) nell'interfaccia fisica o di composizione. **Nota:** fa distinzione tra maiuscole e

minuscole.

Per ulteriori informazioni, consultare il documento relativo all'[autenticazione PPP mediante i comandi nome host e chiamata chap di autenticazione ppp](#).

Risoluzione dei problemi relativi agli errori CHAP in uscita

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.

Se il peer rileva un messaggio di errore in ingresso, significa che il router locale non è riuscito ad autenticare il peer e ha inviato il messaggio. È quindi necessario risolvere i problemi del router su

cui è indicato il problema in uscita.

Questi messaggi sul router locale indicano un errore in uscita:

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

O

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

Il router non utilizza AAA o solo AAA locale

Se il router non usa un sistema di autenticazione, autorizzazione e accounting (AAA) basato su server (Radius o Tacacacs+), il router può usare no AAA o AAA locale. Controllare se nell'output del comando debug è visualizzato uno dei seguenti messaggi:

Impossibile convalidare la risposta

Nome utente *<nomeutente>* non trovato

```
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 mancata corrispondenza del nome utente può essere causata da due motivi:

1. Il peer non ha fornito il nome utente previsto dal router locale. Ad esempio, era previsto (e configurato) il nome utente RouterA, ma il peer ha utilizzato il nome RouterB. È possibile configurare il nome utente e la password inviati dal peer oppure correggere il peer con il nome utente corretto.
2. Il nome utente del router locale non è configurato. Se il nome utente fornito dal peer corrisponde a quello previsto dal router locale, configurare il nome utente e la password.

Questo problema si verifica in genere quando il peer utilizza il comando [ppp chap hostname](#) per configurare un nome utente diverso dal nome host del router.

Utilizzare il comando **username *<username>* password *<password>*** , dove *<username>* viene sostituito dal nome utente indicato nel messaggio di errore precedente.

Nome utente *<nomeutente>* non trovato

Impossibile eseguire l'autenticazione per il peer

```
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 mancata corrispondenza del nome utente può essere causata da due motivi:

1. Il peer non ha fornito il nome utente previsto dal router locale. Ad esempio, era previsto (e configurato) il nome utente RouterA. Tuttavia, il peer ha utilizzato il nome RouterB. È possibile configurare il nome utente e la password inviati dal peer oppure aggiornare il peer con il nome utente corretto.
2. Il nome utente del router locale non è configurato. Se il nome utente fornito dal peer corrisponde a quello previsto dal router locale, configurare il nome utente e la password.

Questo problema si verifica in genere quando il peer utilizza il comando [ppp chap hostname](#) per configurare un nome utente diverso dal nome host del router.

Utilizzare il comando **username <username> password <password>**, dove <username> viene sostituito dal nome utente indicato nel messaggio di errore precedente.

Confronto MD/DES non riuscito

```
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"
```

Questo errore è causato da una mancata corrispondenza della password. Ciò può essere dovuto a due motivi:

1. Il peer non ha fornito la password prevista dal router locale. Ad esempio, era prevista (e configurata) la password *Letmein*, ma il peer ha utilizzato la *lettera* della password. È possibile riconfigurare il nome utente e la password inviati dal peer oppure correggere il peer con il nome utente corretto.
2. La password del router locale non è configurata correttamente. Se la password fornita dal peer è corretta, riconfigurare il router locale.

Soluzione:

1. Rimuovere il nome utente e la password esistenti utilizzando questo comando:

```
no username <username>
```

Dove <username> viene sostituito dal nome utente nel messaggio di errore. Nell'esempio, questo valore è `maui-soho-03`.

2. Configurare il nome utente e la password utilizzando questo comando:

```
username password
```

Il nome utente deve essere lo stesso del messaggio CHAP mostrato sopra. La password deve corrispondere a quella del router remoto.

[Risoluzione dei problemi generali dei server AAA](#)

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

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

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

Nota: questo documento non deve essere considerato una risorsa per la risoluzione dei problemi AAA. Per ulteriori informazioni sulla risoluzione dei problemi relativi al processo AAA, consultare le seguenti risorse:

- [Operazioni AAA](#)
- [RAGGIO](#)
- [TACACS](#)

Problema: L'autenticazione PAP funziona per PPP, ma MsCHAPv2 non riesce

Potrebbe non essere possibile eseguire l'autenticazione a un server ACS perché il server ACS non riceve la richiesta di autenticazione e di conseguenza una sessione non riesce. Questo comportamento è stato osservato e registrato con l'ID bug Cisco [CSCee04466](#) (solo utenti [registrati](#)). Per risolvere il problema, utilizzare un server RADIUS per le sessioni PPP. Tuttavia, mantenere il server TACACS+ per scopi amministrativi sul router.

Informazioni correlate

- [Informazioni sull'output del comando debug ppp negotiation](#)
- [Descrizione e configurazione dell'autenticazione CHAP nei server PPP](#)
- [Autenticazione PPP utilizzando i comandi ppp chap hostname e ppp authentication chap callin](#)
- [Configurazione e risoluzione dei problemi del protocollo PAP \(PPP Password Authentication Protocol\)](#)
- [Supporto della tecnologia Dial and Access](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)