

PPP(CHAP 또는 PAP) 인증 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[용어](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[문제 해결 순서도](#)

[라우터가 CHAP 또는 PAP 인증을 수행합니까?](#)

[라우터가 단방향 또는 양방향 CHAP 인증을 수행합니까?](#)

[수신 오류입니까?](#)

[발신 챌린지 또는 응답의 사용자 이름이 호스트 이름과 동일합니까?](#)

[원격 시스템이 액세스 권한이 있는 Cisco 라우터입니까?](#)

[발송 CHAP 실패 문제 해결](#)

[라우터가 AAA 없음 또는 로컬 AAA만 사용](#)

[일반 서버 기반 AAA 문제 해결](#)

[관련 정보](#)

소개

PPP(Point-to-Point Protocol) 인증 문제는 전화 접속 링크 장애의 가장 일반적인 원인 중 하나입니다. 이 문서에서는 PPP 인증 문제에 대한 몇 가지 문제 해결 절차를 제공합니다.

사전 요구 사항

- 디버그 **ppp 협상** 및 디버그 **ppp 인증**을 활성화합니다.
- PPP 인증 단계는 LCP(Link Control Protocol) 단계가 완료되고 열린 상태가 될 때까지 시작되지 않습니다. debug ppp **협상**이 열려 있음을 나타내지 않으면 계속하기 전에 이 문제를 해결하십시오.
- PPP 인증은 양쪽에서 구성해야 합니다. 다음 명령을 적절히 실행합니다. **양방향 CHAP(Challenge Handshake Authentication Protocol)** 인증을 위한 두 라우터의 **ppp 인증 chap** 단방향 인증을 위해 발신자 라우터에서 **ppp 인증 chap 호출**을 수행합니다. **PAP** 인증을 위한 두 라우터의 **ppp 인증 pap**.

용어

- **로컬 컴퓨터(또는 로컬 라우터)** - 디버깅 세션이 현재 실행 중인 시스템입니다. 디버그 세션을 한 라우터에서 다른 라우터로 이동할 때 로컬 시스템이라는 용어를 다른 라우터에 적용합니다.
- **Peer** - 포인트-투-포인트 링크의 다른 끝입니다. 따라서 디바이스가 로컬 시스템이 아닙니다.예

를 들어, RouterA에서 debug ppp negotiation 명령을 실행하면 로컬 시스템이고 RouterB가 피어입니다. 그러나 디버깅을 RouterB로 전환하면 로컬 시스템이 되고 RouterA가 피어가 됩니다.
참고: 로컬 시스템과 피어라는 용어는 클라이언트-서버 관계를 의미하지 않습니다. 디버그 세션이 실행되는 위치에 따라 전화 접속 클라이언트는 로컬 시스템 또는 피어일 수 있습니다.

[요구 사항](#)

Cisco에서는 이 주제에 대해 알고 있는 것이 좋습니다.

- 디버그 ppp 협상 출력을 읽고 이해할 수 있어야 합니다. 자세한 내용은 디버그 ppp [협상 출력 이해 문서](#)를 참조하십시오.

[사용되는 구성 요소](#)

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

[표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

[문제 해결 순서도](#)

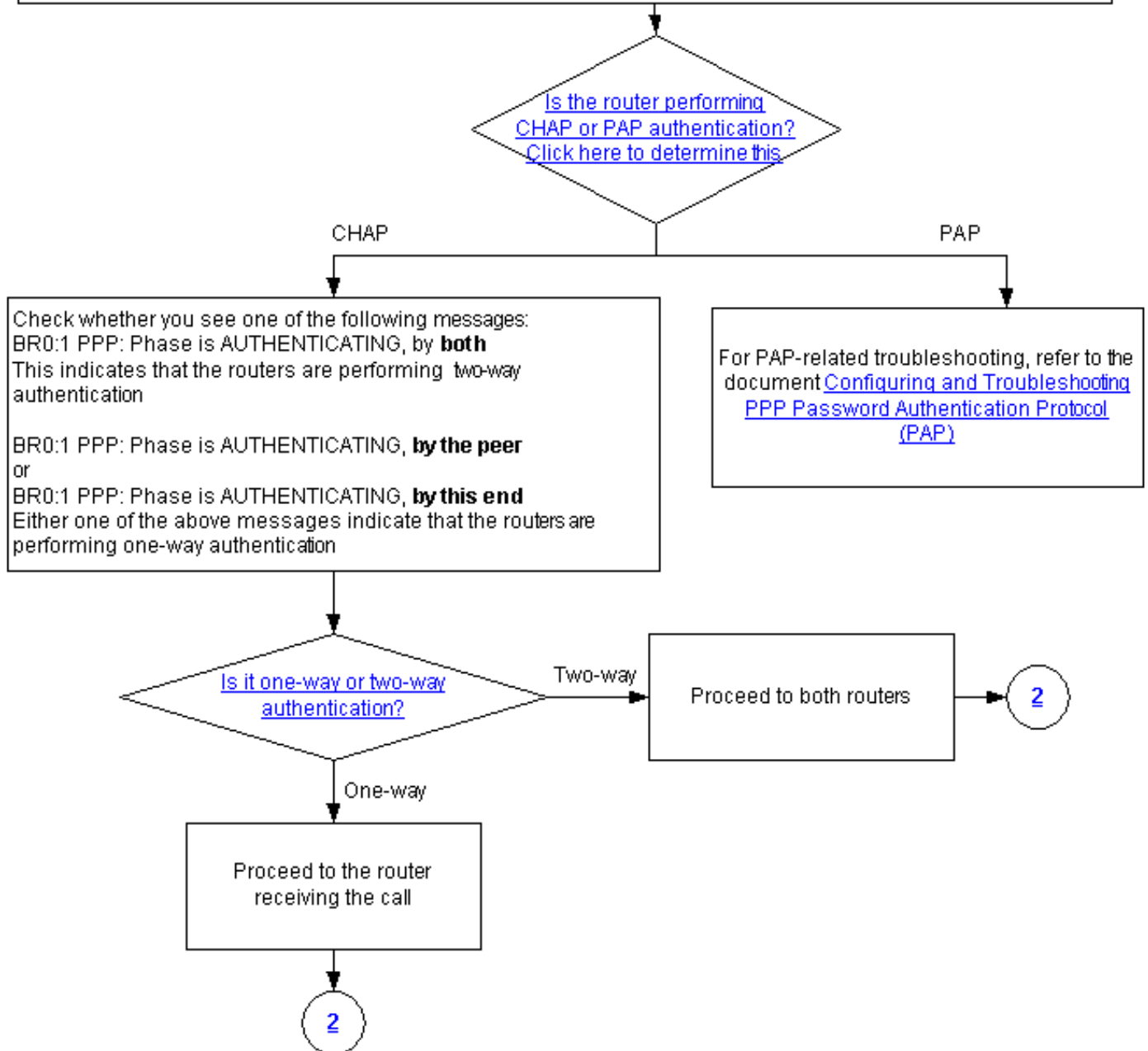
이 문서에는 문제 해결에 도움이 되는 몇 가지 순서도 포함되어 있습니다. 번호가 매겨진 원을 클릭하여 다음 순서도로 진행할 수 있습니다.

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**.



[라우터가 CHAP 또는 PAP 인증을 수행합니까?](#)

라우터가 CHAP 또는 PAP 인증을 수행 중인지 확인하려면 디버그 ppp 협상 및 debug ppp 인증 출력에서 다음 행을 찾습니다.

CHAP

인증 단계에서 CHAP를 찾습니다.

```
*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

인증 단계에서 PAP를 찾습니다.

```
*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"
```

라우터가 단방향 또는 양방향 CHAP 인증을 수행합니까?

디버그 ppp 협상 출력에서 다음 메시지 중 하나를 찾습니다.

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

위의 메시지는 라우터가 양방향 인증을 수행 중임을 나타냅니다.

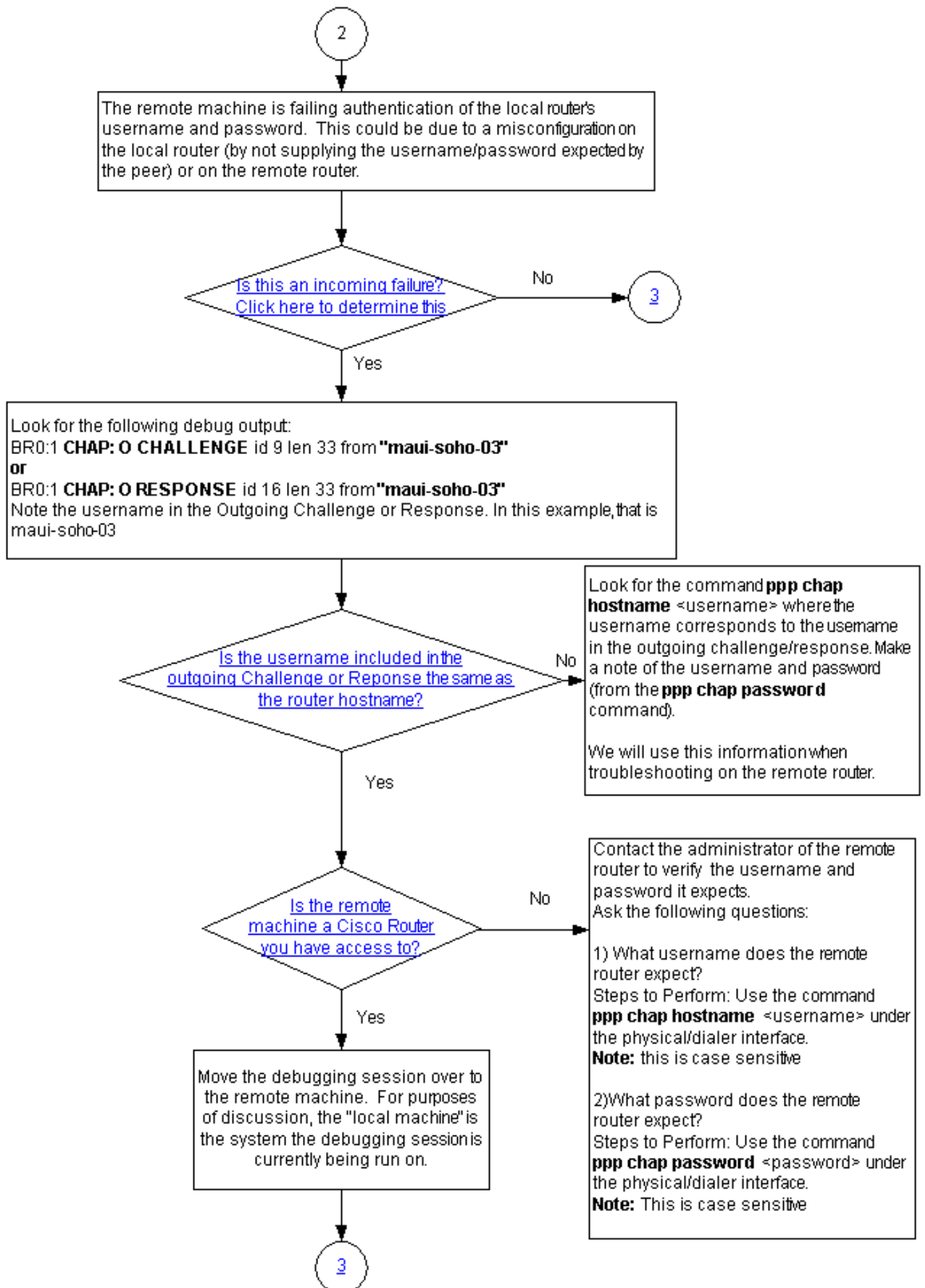
아래 메시지 중 하나는 라우터가 단방향 인증을 수행 중임을 나타냅니다.

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

또는

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

수신 오류입니까?



수신 터미널 또는 실패 메시지를 수신하는지 확인합니다. "I"는 메시지가 수신 메시지임을 나타냅니다

다.

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

또는

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

수신 오류는 피어가 로컬 라우터의 사용자 이름 및 비밀번호를 인증하지 못함을 나타냅니다. 이는 로컬 라우터의 컨피그레이션 오류(피어에서 요구하는 사용자 이름과 비밀번호를 제공하지 않음) 또는 원격 라우터에서 발생할 수 있습니다.

발신 챌린지 또는 응답의 사용자 이름이 호스트 이름과 동일합니까?

디버그 ppp 협상 출력에서 다음을 찾습니다.

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

또는

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

발신 과제 또는 응답의 사용자 이름을 확인합니다. 이 예에서는 **maui-soho-03**입니다. 인증에 사용된 사용자 이름과 암호가 원격 측에서 예상한 사용자 이름과 일치하는지 확인하려면 이 항목이 필요합니다. 예를 들어 로컬 라우터가 피어에 자신을 A로 식별하지만 피어가 B를 예상하는 경우 인증이 실패합니다.

발신 챌린지의 사용자 이름이 호스트 이름과 동일하지 않은 경우 [ppp chap 호스트 이름 <username>](#) 명령을 찾습니다. 여기서 사용자 이름은 발신 챌린지의 사용자 이름에 해당합니다. 사용자 이름 및 비밀번호를 기록해 둡니다(함께 제공되는 ppp chap password 명령). 원격 라우터의 문제를 해결할 때 이 정보를 사용합니다.

원격 시스템이 액세스 권한이 있는 Cisco 라우터입니까?

로컬 라우터가 수신 오류를 수신한 것으로 확인했으므로 피어에서 오류가 발생했음을 알 수 있습니다. 원격 Cisco 라우터에 액세스할 수 있는 경우 해당 디바이스에서 문제를 해결하십시오.

원격 라우터에 대한 액세스 권한이 없는 경우 해당 라우터의 관리자에게 문의하여 필요한 사용자 이름과 암호를 확인하십시오.

다음 질문을 하십시오.

1. 원격 라우터에서 기대하는 사용자 이름은 무엇입니까? 물리적 또는 다이얼러 인터페이스에서 [ppp chap hostname <username>](#) 명령을 사용합니다. 여기서 원격 관리자가 제공한 사용자 이름을 구성합니다. **참고:** 대소문자를 구분합니다.
2. 원격 라우터에서 기대하는 비밀번호 물리적 또는 다이얼러 인터페이스에서 [ppp chap password <password>](#) 명령을 사용합니다. **참고:** 대소문자를 구분합니다.

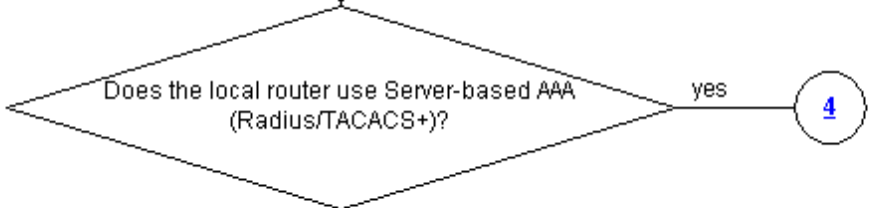
자세한 내용은 ppp chap 호스트 이름을 [사용하여 PPP 인증 및 ppp 인증 chap 호출 명령](#) 문서를 참조하십시오.

발송 CHAP 실패 문제 해결

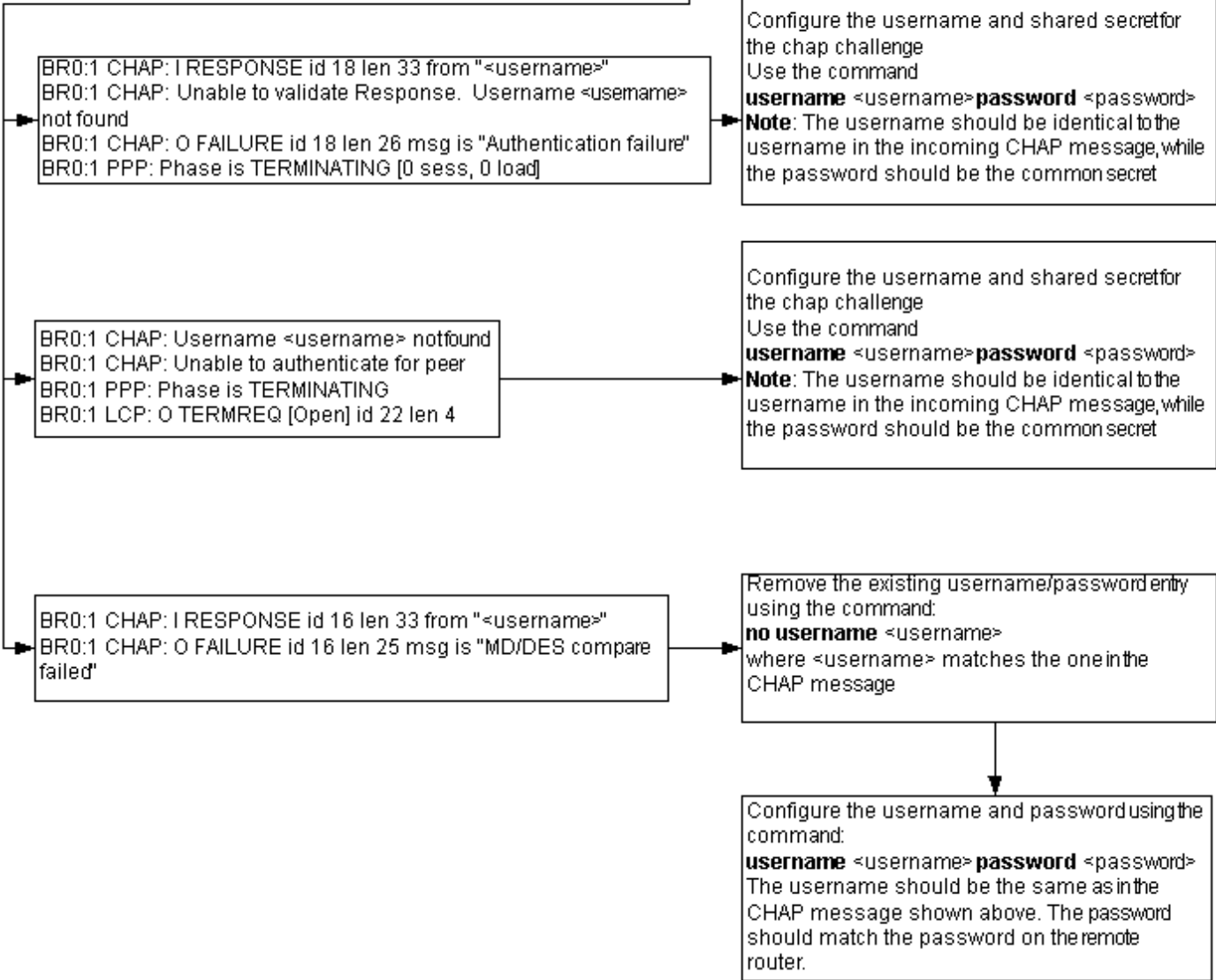
3

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



Choose from one the following error messages



피어가 수신 실패 메시지를 탐지하면 로컬 라우터가 피어를 인증하지 못하고 메시지를 전송했음을 의미합니다. 따라서 이제 발신 오류를 나타내는 라우터의 문제를 해결해야 합니다.

로컬 라우터의 이러한 메시지는 발신 실패를 나타냅니다.

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

또는

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

라우터가 AAA 없음 또는 로컬 AAA만 사용

라우터가 서버 기반 인증, 권한 부여 및 계정 관리(AAA) 시스템(Radius 또는 Tacacs+)을 사용하지 않는 경우 라우터는 AAA 또는 로컬 AAA를 사용할 수 없습니다. 디버그 출력에 다음 메시지 중 하나가 표시되는지 확인합니다.

응답을 검증할 수 없음

사용자 이름 <username>을 찾을 수 없음

```
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]
```

사용자 이름 불일치는 두 가지 이유로 인해 발생할 수 있습니다.

1. 피어가 로컬 라우터에 필요한 사용자 이름을 제공하지 않았습니다. 예를 들어, 사용자 이름 RouterA가 예상(및 구성)되었지만 피어가 RouterB라는 이름을 사용했습니다. 피어가 전송한 사용자 이름과 비밀번호를 구성하거나 올바른 사용자 이름으로 피어를 수정할 수 있습니다.
2. 로컬 라우터에 구성된 사용자 이름이 없습니다. 피어에서 제공한 사용자 이름이 로컬 라우터의 예상 사용자 이름과 일치하는 경우 사용자 이름과 비밀번호를 구성합니다.

이 문제는 피어가 [ppp chap hostname](#) 명령을 사용하여 라우터 호스트 이름 이외의 사용자 이름을 구성할 때 가장 자주 나타납니다.

username <username> password<password> 명령을 사용합니다. 여기서 <username>은 위의 오류 메시지에서 사용자 이름으로 바뀝니다.

사용자 이름 <username>을 찾을 수 없음

피어에 대해 인증할 수 없음

```
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.
```

사용자 이름 불일치는 두 가지 이유로 인해 발생할 수 있습니다.

1. 피어가 로컬 라우터에 필요한 사용자 이름을 제공하지 않았습니다. 예를 들어, 사용자 이름 RouterA를 예상(및 구성)했습니다. 그러나 피어가 RouterB라는 이름을 사용했습니다. 피어가 보낸 사용자 이름과 비밀번호를 구성하거나 올바른 사용자 이름으로 피어를 업데이트할 수 있습니다.
2. 로컬 라우터에 구성된 사용자 이름이 없습니다. 피어에서 제공한 사용자 이름이 로컬 라우터의 예상 사용자 이름과 일치하는 경우 사용자 이름과 비밀번호를 구성합니다.

이 문제는 피어가 `ppp chap hostname` 명령을 사용하여 라우터 호스트 이름 이외의 사용자 이름을 구성할 때 가장 자주 나타납니다.

`username <username> password <password>` 명령을 사용합니다. 여기서 `<username>`은 **위의 오류 메시지에서 사용자 이름으로 바뀝니다.**

MD/DES 비교 실패

```
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"
```

이 오류는 암호 불일치로 인해 발생합니다. 다음과 같은 두 가지 이유로 인해 발생할 수 있습니다.

1. 피어가 로컬 라우터에서 요구하는 비밀번호를 제공하지 않았습니다. 예를 들어, Letmein의 비밀번호가 예상(및 구성)으로 구성되었지만 피어가 비밀번호 문자를 사용했습니다. 피어에서 전송한 사용자 이름과 비밀번호를 다시 구성하거나 올바른 사용자 이름으로 피어를 수정할 수 있습니다.
2. 로컬 라우터에 암호가 올바르게 구성되지 않았습니다. 피어에서 제공한 비밀번호가 올바른지 확인한 경우 로컬 라우터를 다시 구성합니다.

해결책:

1. 다음 명령을 사용하여 기존 사용자 이름 및 비밀번호 항목을 제거합니다.

```
no username <username>
```

여기서 `<username>`은 오류 메시지에서 사용자 이름으로 바뀝니다. 이 예에서는 --03.

2. 다음 명령을 사용하여 사용자 이름 및 비밀번호를 구성합니다.

```
username password
```

사용자 이름은 위에 표시된 CHAP 메시지와 동일해야 합니다. 비밀번호는 원격 라우터의 비밀번호와 일치해야 합니다.

일반 서버 기반 AAA 문제 해결

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

참고: 이 문서는 AAA 문제 해결 리소스로 사용할 수 없습니다. AAA 문제 해결에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- [AAA 운영](#)

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

[문제/장애: PAP 인증은 PPP에 대해 작동하지만 msCHAPv2에 실패](#)

ACS 서버가 인증 요청을 받지 않아 세션이 실패하게 되므로 ACS 서버에 인증할 수 없습니다. 이 동작은 Cisco 버그 ID CSCee04466 [에서 관찰되고 기록됩니다](#)([등록된](#) 고객만 해당). 이를 해결하려면 PPP 세션에 RADIUS 서버를 사용합니다. 그러나 라우터에서 관리 목적으로 TACACS+ 서버를 유지합니다.

[관련 정보](#)

- [디버그 ppp 협상 출력 이해](#)
- [PPP CHAP 인증 이해 및 구성](#)
- [PPP 인증 ppp chap 호스트 이름 및 ppp 인증 chap 호출 명령 사용](#)
- [PPP PAP\(Password Authentication Protocol\) 구성 및 문제 해결](#)
- [전화 접속 및 액세스 기술 지원](#)
- [기술 지원 및 문서 - Cisco Systems](#)