Cisco − Troubleshooting PPP (CHAP or PAP) Authenticatio

Table of Contents

Troubleshooting PPP (CHAP or PAP) Authentication

Introduction

Point−to−Point Protocol (PPP) authentication issues are one of the most common causes for dialup link failures. This document provides some troubleshooting procedures for PPP authentication issues.

Terminology

Local machine (or local router): This is the system the debugging session is currently being run on. As we move the debug session from one router to the other, we should apply the term local machine to the other router.

Peer: The other end of the point−to−point link. Hence the device is not the local machine.

For example, if we run **debug ppp negotiation** on RouterA, then it is the local machine, and RouterB is the peer. However, if we shift debugging over to RouterB, then it becomes the local machine and RouterA becomes the peer.

Note: The terms local machine and peer do not imply a client−server relationship. Depending on where the debug session is run, the dialin client could be the local machine or peer.

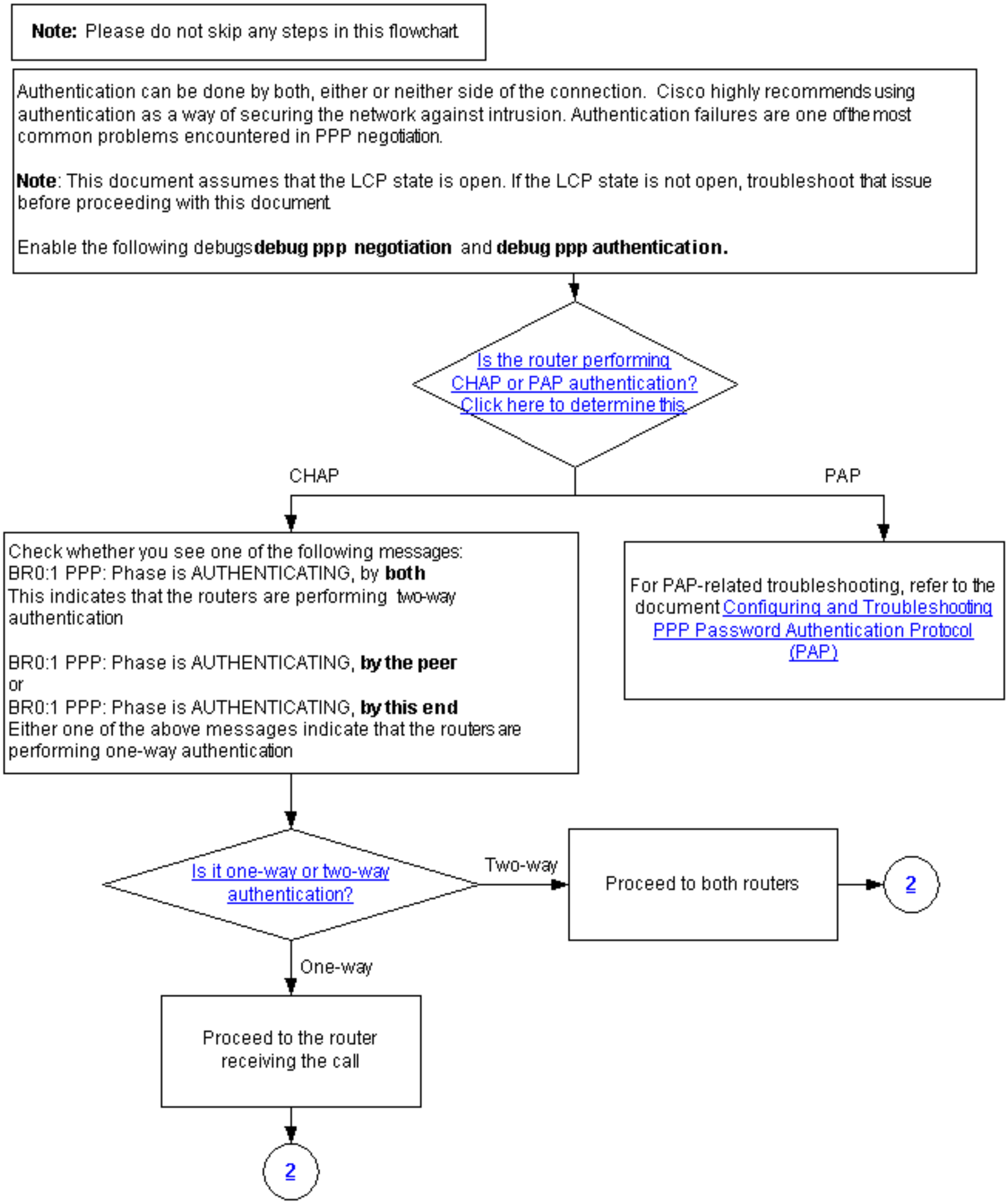
Prerequisites

- Enable **debug ppp negotiation** and **debug ppp authentication**.
- You must be able to read and understand the **debug ppp negotiation** output. Refer to the document Understanding `debug ppp negotiation` Output for more information

- The PPP authentication phase does not begin until the Link Control Protocol (LCP) phase is complete and is in state open. If **debug ppp negotiation** does not indicate that LCP is open, troubleshoot this issue before proceeding.
- PPP Authentication must be configured on both sides. Use the following commands as appropriate:
    - **ppp authentication chap** on both routers, for two−way Challenge Handshake Authentication Protocol (CHAP) authentication.
    - **ppp authentication chap callin** on the calling router, for one−way authentication.
    - **ppp authentication pap** on both routers, for PAP authentication.

Troubleshooting Flowchart

This document includes some flowcharts to assist in troubleshooting. You can proceed to the next flowchart by clicking on the numbered circles.



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.**

Is the router performing CHAP or PAP authentication? Click here to determine this

Check whether you see one of the following messages:
BR0:1 PPP: Phase is AUTHENTICATING, by **both**
This indicates that the routers are performing two-way authentication

BR0:1 PPP: Phase is AUTHENTICATING, **by the peer**
or
BR0:1 PPP: Phase is AUTHENTICATING, **by this end**
Either one of the above messages indicate that the routers are performing one-way authentication

For PAP-related troubleshooting, refer to the document Configuring and Troubleshooting PPP Password Authentication Protocol (PAP)

Is it one-way or two-way authentication?

Proceed to both routers

Proceed to the router receiving the call

Is the Router Performing CHAP or PAP Authentication?

To determine if the router is performing CHAP or PAP authentication, look for the following lines in the **debug ppp negotiation** and **debug ppp authentication** output:

CHAP

Look for CHAP in the AUTHENTICATING phase.

```
*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

Look for PAP in the AUTHENTICATING phase.

```
*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"
```

Is the Router Performing One−Way or Two−Way CHAP Authentication?

Look for one of the following messages in the **debug ppp negotiation** output:

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

The above message indicates that the routers are performing two−way authentication.

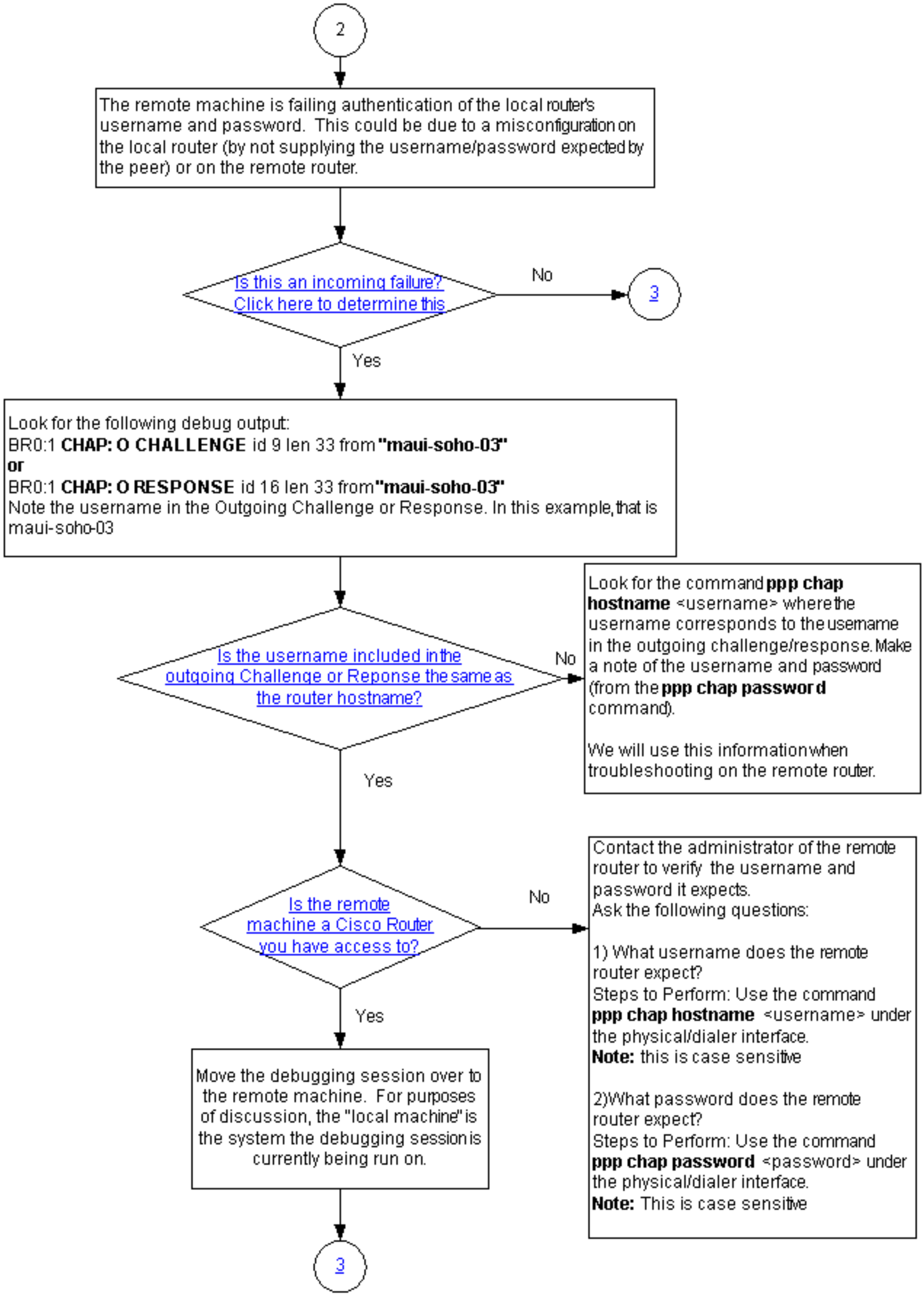
Either one of the messages below indicates that the routers are performing one−way authentication:

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

or

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

Is this an Incoming Failure?


2
The remote machine is failing authentication of the local router's username and password. This could be due to a misconfiguration on the local router (by not supplying the username/password expected by the peer) or on the remote router.
Is this an incoming failure? Click here to determine this
No
3
Yes
Look for the following debug output:
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"**
Note the username in the Outgoing Challenge or Response. In this example, that is maui-soho-03
Is the username included in the outgoing Challenge or Reponse the same as the router hostname?
No
Look for the command **ppp chap hostname** <username> where the username corresponds to the username in the outgoing challenge/response. Make a note of the username and password (from the **ppp chap password** command).
We will use this information when troubleshooting on the remote router.
Yes
Is the remote machine a Cisco Router you have access to?
No
Contact the administrator of the remote router to verify the username and password it expects.
Ask the following questions:
1) What username does the remote router expect?
Steps to Perform: Use the command **ppp chap hostname** <username> under the physical/dialer interface.
Note: this is case sensitive
2)What password does the remote router expect?
Steps to Perform: Use the command **ppp chap password** <password> under the physical/dialer interface.
Note: This is case sensitive
Yes
Move the debugging session over to the remote machine. For purposes of discussion, the "local machine" is the system the debugging session is currently being run on.
3

Check to see if you are receiving incoming `termreq` or `failure` messages. Remember that "I" indicates that the message is an incoming message:

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

or

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

An incoming failure indicates that the peer is failing to authenticate the local router's username and password. This could be due to a misconfiguration on the local router (by not supplying the username and password expected by the peer) or on the remote router.

Is the Username in the Outgoing Challenge or Response the Same as the Hostname?

Look for the following in the **debug ppp negotiation** output:

```
       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"
```

Note the username in the outgoing challenge or response. In this example, it is maui−soho−03. You need this to verify that the username and password used for authentication matches the one expected by the remote side. For example, if the local router identifies itself to the peer as A, but the peer was expecting B, then authentication fails.

If the username in the outgoing challenge is not the same as the hostname, look for the command **ppp chap hostname** <*username*>, where the username corresponds to the username in the outgoing challenge. Make a note of the username and password (in the accompanying **ppp chap password** command). We will use this information when troubleshooting on the remote router.

Is the Remote Machine a Cisco Router you have Access to?

Since we have determined that the local router received an incoming failure, we know that the failure is occurring on the peer. If you have access to the remote Cisco router, then troubleshoot on that device.

If you do not have access to the remote router, contact the administrator of that router to verify the username and password it expects.

Ask the following questions:

1. What username does the remote router expect?

   Use the command **ppp chap hostname** <*username*> under the physical or dialer interface. Configure the username provided by the remote administrator here.

   Note: This is case sensitive.

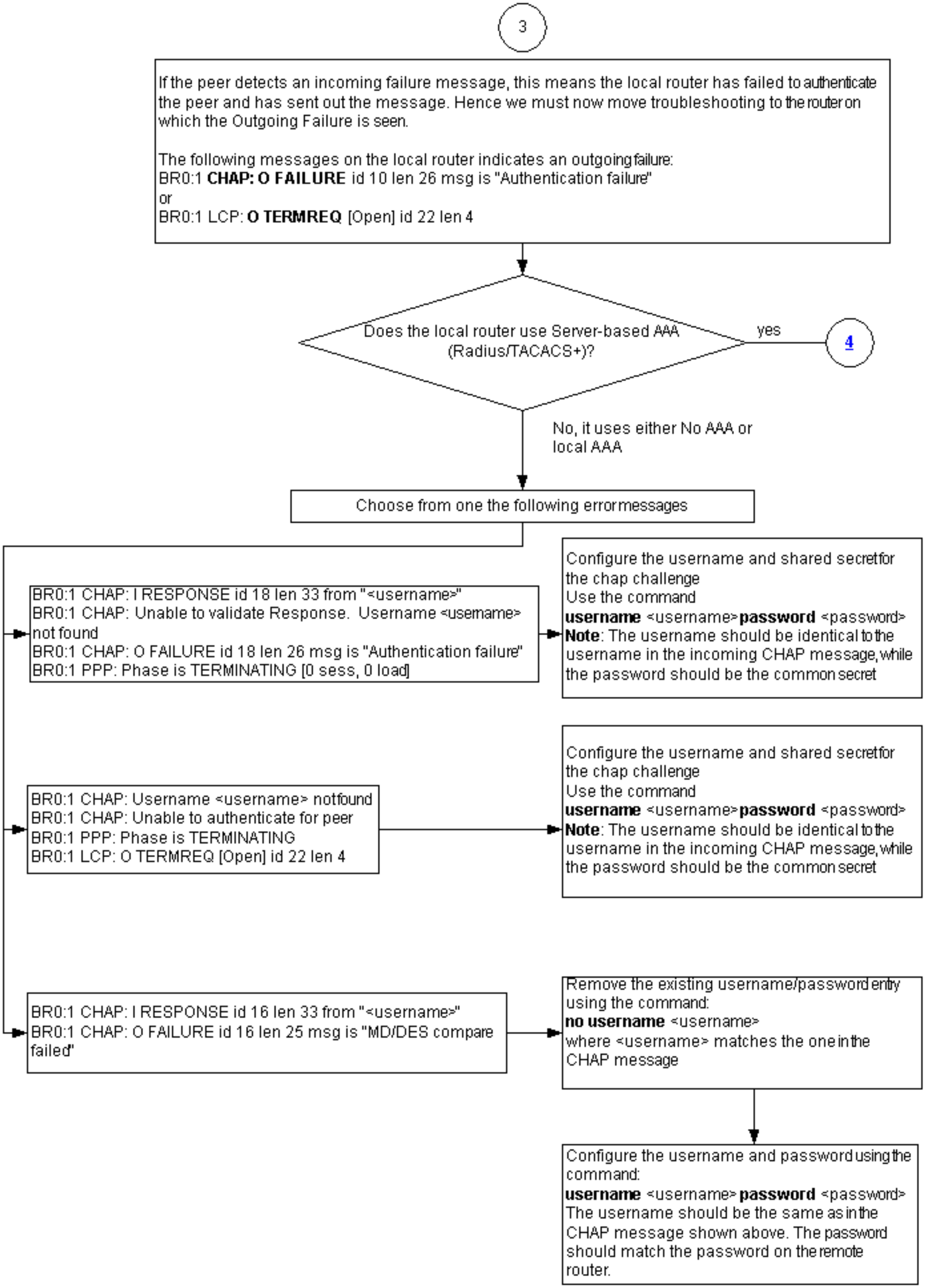
2. What password does the remote router expect?

   Use the command **ppp chap password** <*password*> under the physical or dialer interface.

Note: This is case sensitive.

For more information, refer to the document PPP Authentication Using the `ppp chap hostname` and `ppp authentication chap callin` Commands.

Troubleshooting Outgoing CHAP Failures



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+)?

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.

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 troubleshoot on the router on which we can see the outgoing failure.

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
```

The Router Uses No AAA or Only Local AAA

If the router does not use a server−based authentication, authorization, and accounting (AAA) system (Radius or Tacacs+), then the router can use either no AAA or local AAA. Check whether you see one of the following messages in the debug output:

Unable to Validate Response
Username <*username*> Not Found

```
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]
```

A username mismatch can be caused by two reasons:

1. The peer did not supply the username expected by the local router. For example, we expected (and configured) the username RouterA, but the peer used the name RouterB. You can either configure the username and password sent by the peer or correct the peer with the right username.

2. The local router does not have the username configured. If the username supplied by the peer matches what the local router expected, then configure the username and password.

This issue is most often seen when the peer uses the **ppp chap hostname** command to configure a username other than the router hostname.

Use the command **username** <*username*> **password** <*password*>, where <*username*> is replaced by the username in the error message above.

Username <*username*> Not Found
Unable to Authenticate for 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.
```

A username mismatch can be caused by two reasons:

1. The peer did not supply the username expected by the local router. For example, we expected (and configured) the username RouterA, however the peer used the name RouterB. You can either configure the username and password sent by the peer or correct the peer with the right username.

2. The local router does not have the username configured. If the username supplied by the peer matches what the local router expected, then configure the username and password

This issue is most often seen when the peer uses the **ppp chap hostname** command to configure a username other than the router hostname.

Use the command **username** <*username*> **password** <*password*>, where <*username*> is replaced by the username in the error message above.

MD/DES Compare Failed

```
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"
```

This error is caused by a password mismatch. This could be cause by two reasons:

1. The peer did not supply the password expected by the local router. For example, we expected (and configured) the password LetmeIn, but the peer used the password letmein. You can either re−configure the username and password sent by the peer or correct the peer with the right username.

2. The local router does not have the password correctly configured. If you have verified that the password supplied by the peer is correct, then reconfigure the local router.

Solution:

1. Remove the existing username and password entry using the command:

   no username <*username*>

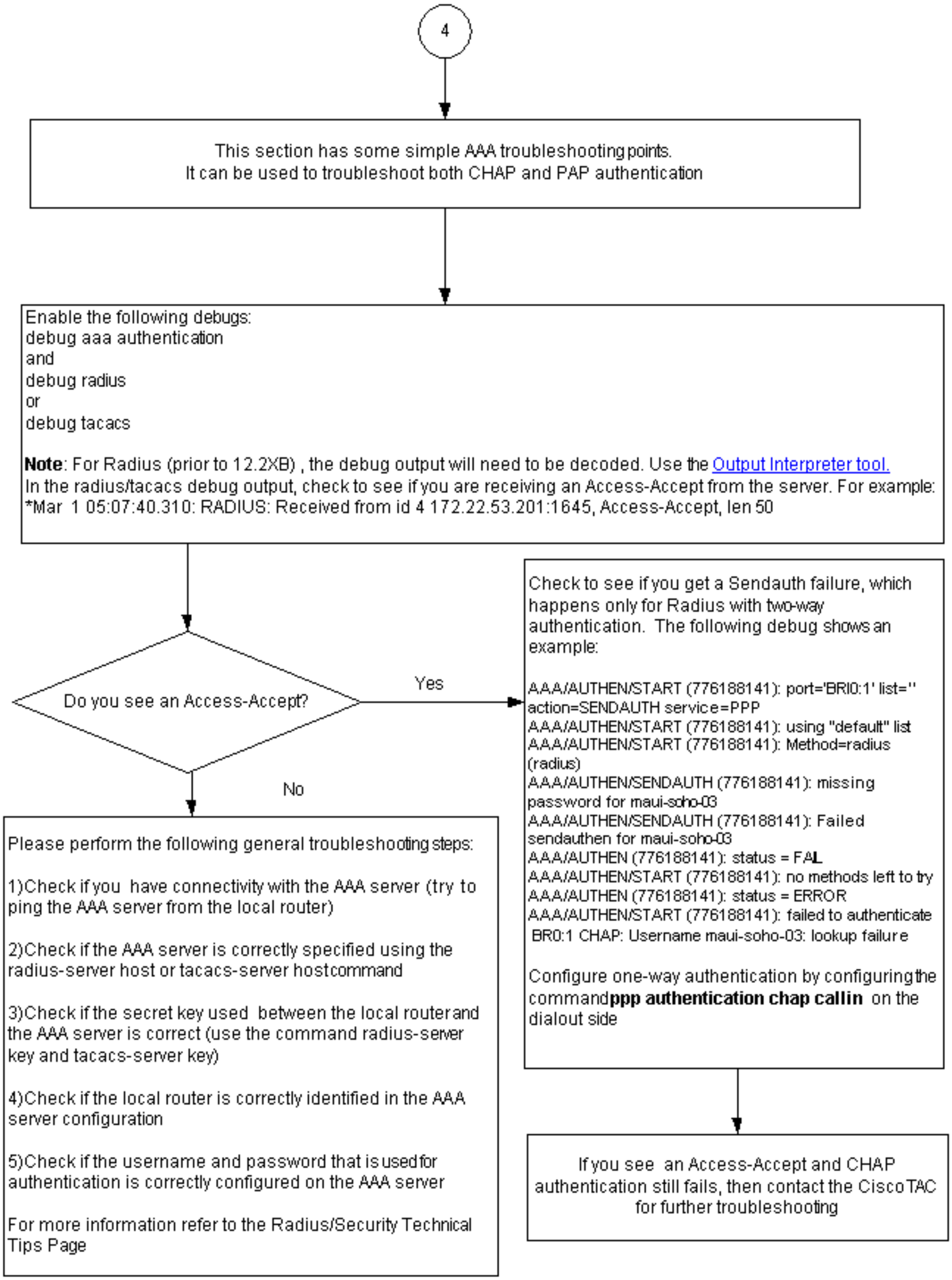
   where <*username*> is replaced by the username in the error message. In this example, that would be maui−soho−03.

2. 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.

Troubleshooting General Server−based AAA Issues



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
```

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='BRI0:1' 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

Note: This document is not intended as a AAA troubleshooting resource. For more information on troubleshooting AAA, refer to the following resources:

- Diagnosing and Troubleshooting AAA Operations
- RADIUS
- TACACS

Related Information

- **Understanding debug ppp negotiation Output**
- **Understanding and Configuring PPP CHAP Authentication**
- **PPP Authentication Using the ppp chap hostname and ppp authentication chap callin Commands**
- **Configuring and Troubleshooting PPP Password Authentication Protocol (PAP)**
- **Understanding PPP and PPP Authentication**
- **Dial Technology Support Pages**