Troubleshooting PPP (CHAP or PAP) Authentication

Contents

Introduction
Prerequisites
Terminology
Requirements
Components Used
Conventions
Troubleshooting Flowchart
Is the Router Performing CHAP or PAP Authentication?
Is the Router Performing One-Way or Two-Way CHAP Authentication?
Is this an Incoming Failure?
Is the Username in the Outgoing Challenge or Response the Same as the Hostname?
Is the Remote Machine a Cisco Router you have Access to?
Troubleshooting Outgoing CHAP Failures
The Router Uses No AAA or Only Local AAA
Troubleshooting General Server-based AAA Issues
Related Information

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.

Prerequisites

- Enable **debug ppp negotiation** and **debug ppp authentication**.
- The PPP authentication phase does not begin until the Link Control Protocol (LCP) phase is complete and is in the open state. If **debug ppp negotiation** does not indicate that LCP is open, troubleshoot this issue before proceeding.
- PPP Authentication must be configured on both sides. Issue these 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.

Terminology

- **Local machine** (or local router) - This is the system on which the debugging session is currently being run. As you move the debug session from one router to the other, 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 you issue the **debug ppp negotiation** command on RouterA, then it is the local machine and RouterB is the peer. However, if you 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 dial-in client could be the local machine or peer.

Requirements

Cisco recommends that you have knowledge of this topic:

- 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.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Troubleshooting Flowchart

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

Is the Router Performing CHAP or PAP Authentication?

To determine if the router is performing CHAP or PAP authentication, look for these 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 these 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?

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

or

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

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). You will use this information when you troubleshoot 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 these questions:

1. What username does the remote router expect?Use the **ppp chap hostname *<username>*** command 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 **ppp chap password *<password>*** command 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, you must now troubleshoot the router on which indicates the outgoing failure.

These messages on the local router indicate 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 **username <*username*> password <*password*>** command, 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 update the peer with the correct 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 **username <*username*> password <*password*>** command, 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 this 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 this 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

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

- AAA Operations
- RADIUS
- TACACS

Problem: PAP authentication works for PPP, but MsCHAPv2 fails

You might not be able to authenticate to an ACS server because the ACS server does not receive the authentication request, which causes a session to fail. This behavior is observed and logged under Cisco bug ID CSCee04466 (registered customers only) . As a workaround, use a RADIUS server for PPP sessions. However, keep the TACACS+ server for administrative purposes on the router.

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)**
- **Dial and Access Technology Support**
- **Technical Support & Documentation - Cisco Systems**