# onfiguring and Troubleshooting PPP Password Authentication

# Table of Contents

# Configuring and Troubleshooting PPP Password Authentication Protocol (PAP)



## Introduction

Point−to−Point Protocol (PPP) currently supports two authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Both are specified in RFC 1334 and are supported on synchronous and asynchronous interfaces.

- PAP provides a simple method for a remote node to establish its identity using a two−way handshake. After the PPP link establishment phase is complete, a username and password pair is repeatedly sent by the remote node across the link (in clear text) until authentication is acknowledged, or until the connection is terminated.

- PAP is not a secure authentication protocol. Passwords are sent across the link in clear text and there is no protection from playback or trail−and−error attacks. The remote node is in control of the frequency and timing of the login attempts.

## Before You Begin

### Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

## Prerequisites

There are no specific prerequisites for this document.

## Components Used

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

## Background Information

CHAP is considered to be more secure because the user password is never sent across the connection. For more information on CHAP refer to the document PPP Authentication Using the **ppp chap hostname** and **ppp authentication chap callin** Commands.

Despite its shortcomings, PAP may be used in the following environments:

- A large installed base of client applications that do not support CHAP
- Incompatibilities between different vendor implementations of CHAP
- Situations where a plaintext password must be available to simulate a login at the remote host

# Unidirectional Vs Bi−directional Authentication

As with most types of authentication, PAP supports bi−directional (two way) and unidirectional (one way) authentication. With unidirectional authentication, only the side receiving the call (NAS) authenticates the remote side (client). The remote client does not authenticate the server.

With bi−directional authentication, each side independently sends an Authenticate−Request (AUTH−REQ) and receives either an Authenticate−Acknowledge (AUTH−ACK) or Authenticate−Not Acknowledged (AUTH−NAK). These can be seen with the **debug ppp authentication** command. An example of this debug at the client is shown below:

```
*Mar  6 19:18:53.322: BR0:1 PAP: O AUTH-REQ id 7 len 18 from "PAPUSER"

! --- Outgoing PAP AUTH-REQ. We are sending out our username (PAPUSER)and password
! --- to the NAS. The NAS will verify that the username/password is correct.

*Mar  6 19:18:53.441: BR0:1 PAP: I AUTH-ACK id 7 Len 5

! --- Incoming AUTH-ACK.
! --- The NAS verified the username and password and responded with an AUTH-ACK.
! --- One-way authentication is complete at this point.

*Mar  6 19:18:53.445: BR0:1 PAP: I AUTH-REQ id 1 Len 14 from "NAS"

! --- Incoming AUTH-REQ from the NAS. This means we now verify the identity of the NAS.

*Mar  6 19:18:53.453: BR0:1 PAP: Authenticating peer NAS

! --- Performing a lookup for the username (NAS) and password.
```

```
*Mar  6 19:18:53.457: BR0:1 PAP: O AUTH-ACK id 1 Len 5

! --- Outgoing AUTH-ACK.
! --- We have verified the username/password of the NAS and responded with an AUTH-ACK.
! --- Two-way authentication is complete.
```

In the above debug output, the authentication was bi−directional. However if unidirectional authentication had been configured, we would only see the first two debug lines.

# Configuration Commands

There are three commands required for normal PAP authentication described below:

## ppp authentication pap [callin]

The router that the **ppp authentication pap** command is configured on will use PAP to verify the identity of the other side (peer). This means the other side (peer) must present it's username/password to the local device for verification.

The **callin** option says the router that the **ppp authentication pap callin** command is configured on will only authenticate the other side during an incoming call. For an outgoing call, it will not authenticate the other side. This means the router initiating the call does not require a request for authentication (AUTH−REQ) from the other side

The following table shows when to configure the **callin** option:

| Authentication Type | Client (calling) | NAS (called) |
|---|---|---|
| Unidirectional | **ppp authentication pap callin** | **ppp authentication pap** |
| Bi−directional | **ppp authentication pap** | **ppp authentication pap** |

## username <username> password <password>

This is the username and password used by the local router to authenticate the PPP peer. When the peer sends its PAP username and password, the local router will check whether that username and password are configured locally. If there is a successful match, the peer is authenticated.

**Note:** The function of the username command for PAP is different than its function for CHAP. With CHAP, this username and password are used to generate the response to the challenge, but PAP only uses it to verify that an incoming username and password are valid.

For one−way authentication, this command is only required on the called router. For two−way authentication this command is necessary on both sides.

### PPP pap sent−username <username> password <password>

Enables outbound PAP authentication. The local router uses the username and password specified by the **ppp pap sent−username** command to authenticate itself to a remote device. The other router must have this same username/password configured using the **username** command described above.

If you are using one−way authentication, this command is only necessary on the router initiating the call. For two−way authentication this command must be configured on both sides.

## Configuration Example

The following configuration sections show the necessary PAP commands for a one way authentication scenario.

**Note:** Only the relevant sections of the configuration are shown.

### Calling Side (Client) Configuration

```
interface BRI0

! −−− BRI interface for the dialout.

 ip address negotiated
 encapsulation ppp

! −−− Use PPP encapsulation. This command is a required for PAP.

 dialer string 3785555 class 56k

! −−− Number to dial for the outgoing connection.

 dialer−group 1
 isdn switch−type basic−ni
 isdn spid1 51299611110101 9961111
 isdn spid2 51299622220101 9962222
 ppp authentication pap callin

! −−− Use PAP authentication for incoming calls.
! −−− The callin keyword has made this a one−way authentication scenario.
! −−− This router (client) will not request that the peer (server) authenticate
! −−− itself back to the client.

 ppp pap sent−username PAPUSER password 7 <deleted>

! −−− Permit outbound authentication of this router (client) to the peer.
! −−− Send a PAP AUTH−REQ packet to the peer with the username PAPUSER and password.
! −−− The peer must have the username PAPUSER and password configured on it.
```

### Receiving Side (Server) Configuration

```
username PAPUSER password 0 cisco

! −−− Username PAPUSER is the same as the one sent by the client.
! −−− Upon receiving the AUTH−REQ packet from the client, we will verify that the
! −−− username and password match the one configured here.
```

```
interface Serial0:23

! --- This is the D-channel for the PRI on the access server receiving the call.

 ip unnumbered Ethernet0
 no ip directed-broadcast
 encapsulation ppp

! --- Use PPP encapsulation. This command is a required for PAP.

 dialer-group 1
 isdn switch-type primary-ni
 isdn incoming-voice modem
 peer default ip address pool default
 fair-queue 64 256 0
 ppp authentication pap

! --- Use PAP authentication for incoming calls.
! --- This router (server) will request that the peer authenticate itself to us.
! --- Note: the callin option is not used as this router is not initiating the call.
```

# Debug Outputs

To debug a PPP PAP issue use the **debug ppp negotiation** and **debug ppp authentication** commands. There are two main issues that you must watch out for:

1. Do both sides agree that PAP is the method of authentication?
2. If so, does the PAP authentication succeed?

Refer to the debugs below for information on how to properly answer the these questions.

## Calling Side (client) debug for a successful one-way PAP authentication

```
maui-soho-01#show debug
PPP:
  PPP authentication debugging is on
  PPP protocol negotiation debugging is on
maui-soho-01#ping 172.22.53.144

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.53.144, timeout is 2 seconds:

*Mar  6 21:33:26.412: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
*Mar  6 21:33:26.432: BR0:1 PPP: Treating connection as a callout
*Mar  6 21:33:26.436: BR0:1 PPP: Phase is ESTABLISHING, Active Open [0 sess, 0 load]
*Mar  6 21:33:26.440: BR0:1 PPP: No remote authentication for call-out

! --- The client will not authenticate the server for an outgoing call.
! --- Remember this is a one-way authentication example.

*Mar  6 21:33:26.444: BR0:1 LCP: O CONFREQ [Closed] id 82 Len 10
*Mar  6 21:33:26.448: BR0:1 LCP:    MagicNumber 0x2F1A7C63 (0x05062F1A7C63)

! --- Outgoing CONFREQ (CONFigure-REQuest).
```

```
! --- Notice that we do not specify an authentication method,
! --- since only the peer will authenticate us.

*Mar  6 21:33:26.475: BR0:1 LCP: I CONFREQ [REQsent] id 13 Len 14
*Mar  6 21:33:26.479: BR0:1 LCP:    AuthProto PAP (0x0304C023)

! --- Incoming LCP CONFREQ (Configure-Request) indicating that
! --- the peer(server) wishes to use PAP.

*Mar  6 21:33:26.483: BR0:1 LCP:    MagicNumber 0x3DBEE95B (0x05063DBEE95B)
*Mar  6 21:33:26.491: BR0:1 LCP: O CONFACK [REQsent] id 13 Len 14
*Mar  6 21:33:26.495: BR0:1 LCP:    AuthProto PAP (0x0304C023)

! --- This shows the outgoing LCP CONFACK (CONFigure-ACKnowledge) indicating that
! --- the client can do PAP.

*Mar  6 21:33:26.499: BR0:1 LCP:    MagicNumber 0x3DBEE95B (0x05063DBEE95B)
*Mar  6 21:33:26.511: BR0:1 LCP: I CONFACK [ACKsent] id 82 Len 10
*Mar  6 21:33:26.515: BR0:1 LCP:    MagicNumber 0x2F1A7C63 (0x05062F1.A7C63)
*Mar  6 21:33:26.519: BR0:1 LCP: State is Open

! --- This shows LCP negotiation is complete.

*Mar  6 21:33:26.523: BR0:1 PPP: Phase is AUTHENTICATING, by the peer [0 sess, 0 load]

! --- The PAP authentication (by the peer) begins.

*Mar  6 21:33:26.531: BR0:1 PAP: O AUTH-REQ id 20 Len 18 from "PAPUSER"

! --- The client sends out a PAP AUTH-REQ with username PAPUSER.
! --- This username is configured with the ppp pap sent-username command.

*Mar  6 21:33:26.555: BR0:1 PAP: I AUTH-ACK id 20 Len 5

! --- The Peer responds with a PPP AUTH-ACK, indicating that
! --- it has successfully authenticated the client.
```

## Called Side (server) debug for a successful one−way PAP authentication

```
maui-nas-06#show debug
PPP:
  PPP authentication debugging is on
  PPP protocol negotiation debugging is on
maui-nas-06#
*Jan  3 14:07:57.872: %LINK-3-UPDOWN: Interface Serial0:4, changed state to up
*Jan  3 14:07:57.876: Se0:4 PPP: Treating connection as a callin

! --- Since the connection is incoming, we will authenticate the client.

*Jan  3 14:07:57.876: Se0:4 PPP: Phase is ESTABLISHING, Passive Open
*Jan  3 14:07:57.876: Se0:4 LCP: State is Listen
*Jan  3 14:07:58.120: Se0:4 LCP: I CONFREQ [Listen] id 83 Len 10
*Jan  3 14:07:58.120: Se0:4 LCP:    MagicNumber 0x2F319828 (0x05062F319828)
*Jan  3 14:07:58.124: Se0:4 LCP: O CONFREQ [Listen] id 13 Len 14
*Jan  3 14:07:58.124: Se0:4 LCP:    AuthProto PAP (0x0304C023)

! --- Outgoing CONFREQ (Configure-Request)
! --- use PAP for the peer authentication.

*Jan  3 14:07:58.124: Se0:4 LCP:    MagicNumber 0x3DD5D5B9 (0x05063DD5D5B9)
*Jan  3 14:07:58.124: Se0:4 LCP: O CONFACK [Listen] id 83 Len 10
```

```
*Jan  3 14:07:58.124: Se0:4 LCP:    MagicNumber 0x2F319828 (0x05062F319828)
*Jan  3 14:07:58.172: Se0:4 LCP: I CONFACK [ACKsent] id 13 Len 14
*Jan  3 14:07:58.172: Se0:4 LCP:    AuthProto PAP (0x0304C023)

! --- This shows the incoming LCP CONFACK (Configure-Acknowledge) indicating that
! --- the client can do PAP.

*Jan  3 14:07:58.172: Se0:4 LCP:    MagicNumber 0x3DD5D5B9 (0x05063DD5D5B9)
*Jan  3 14:07:58.172: Se0:4 LCP: State is Open
*Jan  3 14:07:58.172: Se0:4 PPP: Phase is AUTHENTICATING, by this end

! --- The PAP authentication (by this side) begins.

*Jan  3 14:07:58.204: Se0:4 PAP: I AUTH-REQ id 21 Len 18 from "PAPUSER"

! --- Incoming AUTH-REQ from the peer. This means we must now verify the identity


! --- of the peer.

*Jan  3 14:07:58.204: Se0:4 PPP: Phase is FORWARDING
*Jan  3 14:07:58.204: Se0:4 PPP: Phase is AUTHENTICATING
*Jan  3 14:07:58.204: Se0:4 PAP: Authenticating peer PAPUSER

! --- Performing a lookup for the username (PAPUSER) and password.

*Jan  3 14:07:58.208: Se0:4 PAP: O AUTH-ACK id 21 Len 5

! --- This shows the outgoing AUTH-ACK.
! --- We have verified the username and password and responded with an AUTH-ACK.
! --- One-way authentication is complete.
```

# Troubleshooting PAP

When troubleshooting PAP, answer the same questions shown in the Debug Output Section:

1. Do both sides agree that PAP is the method of authentication?
2. If so, does the PAP authentication succeed?

## The two side do not agree on PAP as the authentication protocol

In certain configuration you may observe that the two sides do not agree on PAP as the authentication protocol or instead agree on CHAP (when you wanted PAP). Use the following steps to troubleshoot such issues:

1. Verify that the router receiving the call has one of the following authentication commands

```
ppp authentication pap
      or
ppp authentication pap chap
      or
ppp authentication chap pap
```

2.

Verify that the router making the call has **ppp authentication pap callin** configured.

3. Verify that the calling side has the command **ppp pap sent−username *username* password *password*** correctly configured, where the username and password match the one configured on the receiving router.

4. Configure the command **ppp chap refuse** in interface configuration mode on the calling router.

   Cisco routers will, by default, accept CHAP as the authentication protocol. In a situation where the client wishes to do PAP but the access server can do PAP or CHAP ( **ppp authentication chap pap** configured), the **ppp chap refuse** command can be used to force the client to accept PAP as the authentication protocol.

```
maui−soho−01(config)#interface BRI 0
maui−soho−01(config−if)#ppp chap refuse
```

## PAP Authentication Does not Succeed

If the two sides agree on PAP as the authentication protocol, but the PAP connection fails, it is most likely a username/password issue.

1. Verify that the calling side has the command **ppp pap sent−username *username* password *password*** correctly configured, where the username and password match the one configured on the receiving router.

2. For two−way authentication, verify that the receiving side has the command **ppp pap sent−username *username* password *password*** correctly configured, where the username and password match the one configured on the calling router.

   When doing two−way authentication, if the command **ppp pap sent−username *username* password *password*** were not present on the receiving router and the PPP client attempts to force the server to authenticate remotely, the output of **debug ppp negotiation** (or **debug ppp authentication**) would indicate

```
*Jan  3 16:47:20.259: Se0:1 PAP: Failed request for PAP credentials.  Username maui-
```

   This error message is an indication of a configuration issue and not necessarily a security breach.

3. 3. Verify that the username and password, matches the one configured in the command **ppp pap sent−username *username* password *password*** on the peer.

   If they do not match you will see the following message:

```
*Jan  3 17:18:57.559: Se0:3 PAP: I AUTH−REQ id 25 Len 18 from "PAPUSER"
*Jan  3 17:18:57.559: Se0:3 PPP: Phase is FORWARDING
*Jan  3 17:18:57.559: Se0:3 PPP: Phase is AUTHENTICATING
*Jan  3 17:18:57.559: Se0:3 PAP: Authenticating peer PAPUSER
*Jan  3 17:18:57.559: Se0:3 PAP: O AUTH−NAK id 25 Len 32 msg is
 "Password validation failure"
```

```
! --- This is an outgoing AUTH-NAK. This means that the mismatch occurred
! --- on this router. Verify that the username and password configured locally is
! --- identical to that on the peer.
```

## Related Information

- **Configuring Authentication**
- **Dialup Technology: Overviews and Explanations**
- **Understanding PPP and PPP Authentication**
- **Technical Support − Cisco Systems**



Updated: Oct 30, 2002 Document ID: 10313