

Configurando e Troubleshooting de PPP Password Authentication Protocol (PAP)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Autenticação unidirecional vs bidirecional](#)

[Comandos de configuração](#)

[ppp authentication pap \[callin\]](#)

[username <nome do usuário> password <senha>](#)

[PPP pap sent-username <nome do usuário> password <senha>](#)

[Exemplo de configuração](#)

[Chamando a configuração do lado \(cliente\)](#)

[Configuração do lado de recepção \(servidor\)](#)

[Saídas de depuração](#)

[Chamando a depuração do lado \(cliente\) para uma autenticação de PAP de sentido único bem-sucedida](#)

[Depuração do lado chamado \(servidor\) para uma autenticação PAP unidirecional bem-sucedida](#)

[Troubleshooting de PAP](#)

[Os dois lados não concordam com o PAP como o protocolo de autenticação](#)

[A autenticação de PAP não teve êxito](#)

[Informações Relacionadas](#)

Introduction

O Protocolo de Autenticação (PPP) oferece suporte a dois Protocolos de Autenticação: Protocolo de autenticação de senha (PAP) e Protocolo de autenticação de handshake de desafio (CHAP). Ambos são especificados em RFC 1334 e são suportados em interfaces síncronas e assíncronas.

- O PAP fornece um método simples para um nó remoto estabelecer sua identidade utilizando um handshake bidirecional. Após a conclusão da fase de estabelecimento do enlace PPP, um par com o nome de usuário e a senha é enviado repetidamente pelo nó remoto através do enlace link (em texto sem formatação) até que a autenticação seja reconhecida ou até que a conexão seja encerrada.
- PAP não é um protocolo de autenticação seguro. As senhas são enviadas pelo link em texto claro e não há proteção contra ataques de reprodução ou tentativa e erro. O nó remoto controla a frequência e o tempo das tentativas de logon.

Para obter mais informações sobre como solucionar problemas de autenticação PPP (usando PAP ou CHAP), consulte [Troubleshooting de Autenticação PPP \(CHAP ou PAP\)](#) para obter um fluxograma completo, passo a passo para Troubleshooting da fase de autenticação PPP. Para obter mais informações sobre como solucionar problemas de todas as fases do PPP (LCP, Autenticação, NCP), consulte o documento [Fluxograma de Troubleshooting do PPP](#) para obter um fluxograma completo para a solução passo a passo de problemas de todas as fases do PPP relacionadas e parâmetros negociados.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Informações de Apoio

O CHAP é considerado mais seguro porque a senha do usuário nunca é enviada pela conexão. Para obter mais informações sobre CHAP, consulte [Entendendo e configurando a autenticação CHAP PPP](#).

Apesar das falhas, PAP pode ser usado nos seguintes ambientes:

- Uma grande base instalada de aplicativos clientes que não suportam CHAP
- Incompatibilidades entre as implementações de diferentes fornecedores de CHAP
- Situações nas quais uma senha de texto simples deve estar disponível para simular um logon no host remoto

Autenticação unidirecional vs bidirecional

Como ocorre com a maioria dos tipos de autenticação, o PAP oferece suporte a autenticação bidirecional (duas direções) e unidirecional (uma direção). Com autenticação unidirecional, somente o lado recebendo a chamada (NAS) autentica o lado remoto (cliente). O cliente remoto não autentica o servidor.

Com a autenticação bidirecional, cada lado envia independentemente um Authenticate-Request (AUTH-REQ) e recebe um Authenticate-Acknowledge (AUTH-ACK) ou Authenticate-Not Acknowledged (AUTH-NAK). Eles podem ser vistos com o comando [debug ppp authentication](#). Um exemplo dessa depuração no cliente é mostrado a seguir:

```
*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.
```

Na saída de depuração acima, a autenticação foi bidirecional. Entretanto, se a autenticação unidirecional tivesse sido configurada, veríamos apenas as duas primeiras linhas da depuração.

Comandos de configuração

Existem três comandos necessários para autenticação PAP regular, descritos abaixo:

ppp authentication pap [callin]

O roteador em que o comando `ppp authentication pap` está configurado utilizará PAP para verificar a identidade de outro lado (peer). Isso significa que o outro lado (peer) deve apresentar seu nome de usuário/senha ao dispositivo local para verificação.

A opção `callin` diz que o roteador no qual o comando [ppp authentication pap callin está configurado autenticará apenas o outro lado durante uma chamada recebida](#). Para uma chamada efetuada, não autenticará o outro lado. Isso significa que o roteador que inicia a chamada não requer uma requisição para autenticação (AUTH-REQ) a partir do outro lado

A tabela a seguir mostra quando a opção `callin` deve ser configurada:

Tipo de autenticação	Cliente (chamando)	NAS (chamado)
Unidirecional	<code>ppp authentication pap callin</code>	<code>ppp authentication pap</code>
Bidirecional	<code>ppp authentication pap</code>	<code>ppp authentication pap</code>

username <nome do usuário> password <senha>

Este é o nome de usuário e senha utilizados pelo roteador local para autenticar o peer de PPP. Quando o peer envia seu nome de usuário e senha de PAP, o roteador local verifica se aquele nome de usuário e senha estão configurados localmente. Se houver uma correspondência bem-sucedida, o peer será autenticado.

Observação: a função do comando `username` para PAP é diferente de sua função para CHAP. Com o CHAP, o nome de usuário e a senha são utilizados para gerar a resposta ao desafio, mas o PAP só os utiliza para verificar se um nome de usuário e uma senha de entrada são válidos.

Para autenticação unidirecional, esse comando somente é necessário no roteador chamado. Para autenticações bidirecionais, esse comando é necessário nos dois lados.

PPP pap sent-username <nome do usuário> password <senha>

Ativa autenticação de PAP de saída. O roteador local usa o nome de usuário e a senha especificados pelo comando [ppp pap sent-username](#) para se autenticar em um dispositivo remoto. O outro roteador deve ter esse mesmo nome de usuário/senha configurado usando o comando `username` descrito acima.

Se você estiver usando a autenticação de sentido único, esse comando só será necessário no roteador que inicia a chamada. Em autenticações de duas vias, este comando deve ser configurado em ambos os lados.

Exemplo de configuração

As seções de configuração a seguir mostram os comandos de PAP necessários para um cenário de autenticação de sentido único.

Observação: somente as seções relevantes da configuração são mostradas.

Chamando a configuração do lado (cliente)

```
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
```

```
! --- 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.
```

Configuração do lado de recepção (servidor)

```
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.
```

Saídas de depuração

Para depurar um problema PPP PAP, use os comandos `debug ppp negotiation` e `debug ppp authentication`. Há dois problemas principais sobre os quais você deve estar atento:

1. Ambos os lados concordam que PAP é o método de autenticação?
2. Em caso afirmativo, a autenticação PAP aconteceu?

Consulte as depurações abaixo para obter informações sobre como responder adequadamente a essas perguntas. Além disso, consulte [Entendendo a saída da negociação de ppp de depuração](#) para obter uma explicação de todas as diferentes linhas de depuração com seu significado relativo durante as diferentes fases do PPP, incluindo a autenticação PPP. Este documento é útil para determinar rapidamente a causa das falhas de negociação do PPP. Para obter mais informações sobre como solucionar problemas de autenticação PPP (usando PAP ou CHAP), consulte [Troubleshooting de Autenticação PPP \(CHAP ou PAP\)](#) para obter um fluxograma completo, passo a passo para Troubleshooting da fase de autenticação PPP.

Chamando a depuração do lado (cliente) para uma autenticação de PAP de sentido único bem-sucedida

```
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 (0x05062F1A7C63) *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.
```

Depuração do lado chamado (servidor) para uma autenticação PAP unidirecional bem-sucedida

```
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 de PAP

Ao Troubleshoot o PAP, responda às mesmas perguntas mostradas na Seção de Saída de Depuração:

1. Ambos os lados concordam que PAP é o método de autenticação?
2. Em caso afirmativo, a autenticação PAP aconteceu?

Para obter mais informações sobre como solucionar problemas de autenticação PPP (usando PAP ou CHAP), consulte [Troubleshooting de Autenticação PPP \(CHAP ou PAP\)](#) para obter um fluxograma completo, passo a passo para Troubleshooting da fase de autenticação PPP.

Os dois lados não concordam com o PAP como o protocolo de autenticação

Em determinadas configurações, é possível observar que os dois lados não concordam em relação ao PAP como o protocolo de autenticação ou, então, concordam em relação ao CHAP (quando você desejava PAP). Use os seguintes passos para fazer Troubleshooting desses problemas:

1. Verifique se o roteador que recebe a chamada tem um dos seguintes comandos de autenticação

```
ppp authentication pap
```

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

2. Verifique se o roteador que está fazendo a chamada tem o comando `ppp authentication pap callin` configurado.
3. Verifique se o lado da chamada tem o comando `ppp pap sent-username username password password` configurado corretamente, em que o nome do usuário e a senha correspondem àqueles configurados no roteador de recebimento.
4. Configure o comando [ppp chap reject](#) no modo de configuração de interface do roteador de chamada. Os roteadores Cisco, por padrão, aceitarão o CHAP como protocolo de autenticação. Em uma situação em que o cliente deseja fazer PAP, mas o servidor de acesso pode fazer PAP ou CHAP ([ppp authentication chap pap](#) configurado), o comando `ppp chap reject` pode ser usado para forçar o cliente a aceitar PAP como o protocolo de autenticação.

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

A autenticação de PAP não teve êxito

Se os dois lados concordarem em PAP como o protocolo de autenticação, mas a conexão PAP falhar, é muito provável que seja um problema de nome de usuário/senha.

1. Verifique se o lado da chamada tem o comando `ppp pap sent-username username password password` configurado corretamente, em que o nome do usuário e a senha correspondem àqueles configurados no roteador de recebimento.
2. Para autenticação bidirecional, verifique se o comando `ppp pap sent-username username password password` está configurado corretamente no lado de recepção, com o nome do usuário e a senha correspondendo àqueles configurados no roteador de recebimento. Ao fazer a autenticação bidirecional, se o comando `ppp pap sent-username username password password` não estiver presente no roteador de recebimento e o cliente PPP tentar forçar o servidor a fazer a autenticação remotamente, a saída do comando `debug ppp negotiation` (ou `debug ppp authentication`) deverá indicar
3. Verifique se o nome de usuário e a senha correspondem àquela configurada no comando `ppp pap sent-username username password password` no peer. Se não corresponderem, você verá esta mensagem:

```
*Jan  3 16:47:20.259: Se0:1 PAP: Failed request for PAP credentials.  Username maui-nas-06
*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.

Informações Relacionadas

- [Configurando a autenticação](#)
- [Fluxograma de Troubleshooting de PPP](#)
- [Troubleshooting de Autenticação de PPP \(CHAP ou PAP\)](#)
- [Entendendo a saída de negociação de debug ppp](#)
- [Autenticação PPP Usando os Comandos ppp chap hostname e ppp authentication chap callin](#)
- [Tecnologia dialup: Visões gerais e explicações](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)