目次

概要

Point-to-Point Protocol（PPP）は現在 2 種類の認証プロトコルをサポートしています。 パスワード認証プロトコル（PAP）および Challenge Handshake 認証プロトコル（CHAP）です。 これらの認証プロトコルはどちらも RFC 1334 で規定されており、同期および非同期インターフェイスでサポートされています。

- PAP は、リモート ノードが双方向ハンドシェイクを使用して自身の身元を明らかにするための単純な方法を提供します。 PPP リンク確立フェーズが完了した後、ユーザ名とパスワードのペアがリンクを通じて（クリア テキストで）繰り返し送信されます。これは、認証が確認応答されるか、または接続が終了するまで続きます。
- PAP は安全な認証プロトコルではありません。 パスワードはクリアテキストのリンクを渡って送信され、再生またはトライアル アンド エラー攻撃から保護がありません。 リモート ノードによってログイン試行の回数とタイミングが管理されます。

（PAP または CHAP を使用した）PPP 認証のトラブルシューティングについては、PPP 認証フェーズをトラブルシューティングするための順を追った網羅的なフローチャートである『トラブルシューティング：PPP（CHAP または PAP）認証』を参照してください。 すべての PPP フェーズ（LCP、認証、NCP）のトラブルシューティングについては、すべての関連 PPP フェーズとネゴシエーションされるパラメータに関する順を追ったトラブルシューティングの網羅的なフローチャートである『PPP のトラブルシューティング フローチャート』のドキュメントを参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

CHAP ではユーザ パスワードが接続を通じて送信されないため、PAP よりも安全であると見なされています。 CHAP についての詳細は、『PPP CHAP 認証の説明と設定』を参照してください。

安全な認証プロトコルではないにもかかわらず、次の環境では PAP が使用される場合があります。

- クライアント アプリケーションの大規模なインストール ベースで、CHAP がサポートされていない場合
- CHAP の実装がベンダー間で異なり、互換性がない場合
- リモート ホストでログインをシミュレートするために、プレーンテキストのパスワードが必要な場合

単方向認証と双方向認証

ほとんどの認証タイプと同様に、PAP は双方向認証と単方向認証をサポートします。 単方向認証では、コールを受信する側（NAS）のみがリモート サイド（クライアント）を認証します。 リモート クライアントはサーバを認証しません。

双方向認証では、各サイドが個別に Authenticate-Request（AUTH-REQ）を送信し、Authenticate-Acknowledge（AUTH-ACK）または Authenticate-Not Acknowledged（AUTH-NAK）を受信します。 **これは debug ppp authentication コマンドを使用して確認できます。** クライアントでの、このデバッグの例を次に示します。

```
*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.
```
上記のデバッグ出力では、認証が双方向でした。 単方向認証が設定されている場合は、デバッグの最初の 2 行のみが表示されます。

設定コマンド

通常の PAP 認証には、次に示す 3 つのコマンドが必要です。

ppp authentication pap [callin]

ppp authentication pap コマンドが設定されているルータでは、PAP を使用して相手側（ピア）の識別情報を確認します。 つまり、相手側（ピア）は確認のために ローカル デバイスに対して自身のユーザ名/パスワードを提示する必要があります。

callin オプションを指定した場合、ppp authentication pap callin コマンドが設定されているルータでは、着信コール時のみ相手側を認証します。 発信コールの場合は相手側を認証しません。 つまり、コールを開始するルータは相手側からの認証要求（AUTH-REQ）を必要としません。

次の表は、callin オプションをどの場合に設定すればよいかを示しています。

認証タイプ	クライアント（発信側）	NAS（着信側）
単方向	ppp authentication pap callin	ppp authentication pap
双方向	ppp authentication pap	ppp authentication pap

username <username> password <password>

これは、PPP ピアを認証するために ローカル ルータで使用されるユーザ名とパスワードです。 ピアが自身の PAP ユーザ名とパスワードを送信してくると、ローカル ルータはそのユーザ名とパスワードがローカルに設定されているかどうかをチェックします。 一致すれば、ピアは認証されます。

注PAP の username コマンドの機能は CHAP の機能とは異なります。 CHAP では、このユーザ名とパスワードを使用して身元証明要求への応答が生成されますが、PAP はこれを着信ユーザ名とパスワードの有効性を確認するためだけに使用します。

単方向認証では、このコマンドは着信側ルータにのみ必要です。 双方向認証では、このコマンドは両方の側に必要です。

PPP pap sent-username <username> password <password>

発信 PAP 認証を有効にします。 ローカル ルータでは ppp pap sent-username コマンドで指定されたユーザ名とパスワードにより、リモート デバイスに対して自身を認証します。 相手側のルータでは、上記の username コマンドを使用して、この同じユーザ名/パスワードが設定されている必要があります。

単方向認証を使用している場合、このコマンドはコールを開始するルータにのみ必要です。 双方

向認証では、このコマンドは両側に設定する必要があります。

設定例

次の設定のセクションでは、単方向認証シナリオで必要な PAP コマンドを示しています。

注設定の関連セクションだけ示されています。

発信側（クライアント）の設定

```
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.
```

受信側（サーバ）の設定

```
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.
```

デバッグ出力

PPP PAP 問題のデバッグを行うには、debug ppp negotiation コマンドと debug ppp authentication コマンドを使用します。 次の 2 つの点に注意してください。

1. 両側が認証方式として PAP に一致しているか。
2. 一致している場合、PAP 認証が成功するか。

これらの質問に正しく回答する方法については、次のデバッグを参照してください。 また、PPP 認証などの異なる PPP フェーズにおけるさまざまなデバッグ行のすべてと関連する意味の説明については、『debug ppp negotiation の出力について』も参照してください。 このドキュメントは、PPP ネゴシエーションの失敗原因をすばやく判断するのに役立ちます。（PAP または CHAP を使用した）PPP 認証のトラブルシューティングについては、PPP 認証フェーズをトラブルシューティングするための順を追った網羅的なフローチャートである『トラブルシューティング：PPP（CHAP または PAP）認証』を参照してください。

単方向 PAP 認証が成功した場合の発信側（クライアント）のデバッグ

```
maui-soho-01#show debugPPP:  PPP authentication debugging is on  PPP protocol negotiation debugging is onmaui-soho-01#ping 172.22.53.144Type 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.*

単方向 PAP 認証が成功した場合の着信側（サーバ）のデバッグ

maui-nas-06#**show debug**PPP: PPP authentication debugging is on PPP protocol negotiation debugging is onmaui-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.*

PAP のトラブルシューティング

PAP のトラブルシューティングを行うときは、「デバッグ出力」の項にあるのと同じ質問に答えます。

1. 両側が認証方式として PAP に一致しているか。
2. 一致している場合、PAP 認証が成功するか。

（PAP または CHAP を使用した）PPP 認証のトラブルシューティングについては、PPP 認証フェーズをトラブルシューティングするための順を追った網羅的なフローチャートである『トラブルシューティング：PPP（CHAP または PAP）認証』を参照してください。

双方は認証プロトコルとして PAP に同意しません

設定によっては、PAP を使用するにもかかわらず、両方の側が認証プロトコルとして PAP に一致せず、代わりに CHAP に一致する場合があります。 このような問題のトラブルシューティングを行うには、次のステップに従います。

1. コールを受信しているルータに次の認証コマンドのいずれかが設定されていることを確認します。**ppp authentication pap** or **ppp authentication pap chap** or **ppp authentication chap pap**
2. **コールを発信しているルータに ppp authentication pap callin コマンドが設定されていることを確認します。**
3. **発信側にコマンド ppp pap sent-username username password password が正しく設定されていることを確認します。ユーザ名とパスワードは受信側ルータに設定されているものと一致する必要があります。**
4. **発信側ルータのインターフェイス設定モードでコマンド ppp chap refuse を設定します。** Cisco ルータは、デフォルトでは認証プロトコルとして CHAP を受け入れます。 **クライアントが PAP を希望しているものの、アクセス サーバで PAP と CHAP がどちらも実行できる（ppp authentication chap pap が設定されている）状況では、ppp chap refuse コマンドを使用して、クライアントに認証プロトコルとして強制的に PAP を受け入れさせることができます。**
```
maui-soho-01(config)#interface BRI 0maui-soho-01(config-if)#ppp chap refuse
```

PAP 認証が失敗する

両側が認証プロトコルとして PAP に合意しているにもかかわらず PAP 接続が失敗する場合、最も可能性が高いのはユーザ名/パスワードの問題です。

1. 発信側にコマンド **ppp pap sent-username username** password **password** が正しく設定されていることを確認します。ユーザ名とパスワードは受信側ルータに設定されているものと一致する必要があります。
2. 双方向認証の場合は、受信側にコマンド **ppp pap sent-username username** password **password** が正しく設定されていることを確認します。ユーザ名とパスワードは発信側ルータに設定されているものと一致する必要があります。双方向認証を行っている場合に、受信側ルータにコマンド **ppp pap sent-username username** password **password** が設定されておらず、なおかつ PPP クライアントがサーバにリモートでの認証を要求しようとしたときは、**debug ppp negotiation**（または **debug ppp authentication**）の出力に次のように表示されます。
```
maui-soho-01(config)#interface BRI 0maui-soho-01(config-if)#ppp chap refuse
```
この エラー メッセージは設定上の問題を示すもので、必ずしもセキュリティ侵犯とは限りません。
3. 3. ユーザ名とパスワードが、ピアでコマンド **ppp pap sent-username username** password **password** によって設定されているものと一致することを確認します。それらが一致するこのメッセージが表示されます:
```
*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.
```

関連情報

- **認証の設定**
- **PPP のトラブルシューティング フローチャート**

- PPP (CHAP または PAP) 認証に関するトラブルシューティング
- debug ppp negotiation の出力について
- ppp chap hostname コマンドおよび ppp authentication chap callin コマンドを使用する PPP 認証
- ダイヤルアップ技術：
- テクニカルサポートとドキュメント - Cisco Systems