PPP CHAP認証の理解および設定

目次

概要

Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）（RFC 1994 で定義）は、スリー ウェイ ハンドシェイクによりピアの身元を確認します。 CHAP では、次の一般的な手順が実行されます。

1. Link Control Protocol（LCP; リンク コントロール プロトコル）フェーズが完了し、両方のデバイス間で CHAP がネゴシエートされた後、認証側はチャレンジ メッセージをピアに送信します。
2. ピアは、一方向ハッシュ関数（Message Digest 5 [MD5]）で計算された値で応答します。
3. 認証側は、その応答が自分の計算した予測ハッシュ値と一致するかどうかをチェックします。 値が一致する場合、認証は成功します。 そうでない場合は、接続が解除されます。

この認証方式は、認証側とピアだけが知る「秘密」に依存します。 この秘密鍵は、リンク上を送信されることはありません。 認証は単方向にすぎませんが、相互認証に同じ秘密鍵セットを使用すると、双方向に CHAP をネゴシエートできます。

CHAP の利点と欠点の詳細は、「RFC 1994」 を参照してください。

前提条件

要件

このドキュメントの読者は次のトピックについて理解している必要があります。

- **encapsulation ppp** コマンドにより、インターフェイスで PPP を有効にする方法
- **debug ppp negotiation** コマンドの出力。 詳細は、『debug ppp negotiation の出力について』を参照してください。
- Link Control Protocol (LCP; リンク制御プロトコル) フェーズがオープン状態ではない場合のトラブルシューティング能力。 これは、PPP 認証フェーズは、LCP フェーズが完了してオープン状態になるまで開始されないためです。 **debug ppp negotiation** コマンドで LCP がオープンであると示されない場合、先に進む前に、この問題のトラブルシューティングを行う必要があります。

注: この文書では、MS-CHAP (バージョン 1 またはバージョン 2) については説明しません。 MS-CHAP の詳細は、『MS-CHAP サポート』および『MSCHAP バージョン 2』を参照してください。

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。

CHAP の設定

CHAP を設定する手順はとても簡単です。 たとえば、図 1 に示すように、left と right という、ネットワークで接続された 2 台のルータがあるとします。

図 1 ネットワークを渡って接続される â 2 ルータ

CHAP 認証を設定するには、次の手順を実行します。

1. インターフェイスで、**encapsulation ppp** コマンドを発行します。
2. 両方のルータで **ppp authentication chap** コマンドを使用して、CHAP 認証の使用を有効にします。
3. ユーザ名とパスワードを設定します。 これには、**username <username>** password **<password>** コマンドを発行します。**<username>** はピアのホスト名です。 次の内容を確認してください。パスワードは、両端で同じである。大文字と小文字が区別されるため、ルータ名とパスワードが完全に同じである。**注:** デフォルトでは、ルータのホスト名は、ピアに対しそれ自体を識別するために使用します。 ただし、この CHAP ユーザ名は、**ppp chap hostname** コマンドで変更できます。 詳細は、『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』を参照してください。

一方向および双方向認証

CHAP は、単方向の認証方式として定義されています。 ただし、双方向認証を作成するには、両方の方向で CHAP を使用します。 したがって、双方向の CHAP では、個別の 3 ウェイ ハンドシェイクがそれぞれの側で開始します。

Cisco の CHAP 実装では、デフォルトでは、（認証が完全にオフにされない限り）着信側が発信側を認証する必要があります。 このため、着信側によって開始される単方向の認証が最低限の認証です。 ただし、発信側も着信側の身元を確認できるため、双方向の認証になります。

単方向認証は、Cisco 以外のデバイスに接続するときに必要になる場合がよくあります。

単方向認証の場合は、発信側ルータで **ppp authentication chap callin** コマンドを設定します。

表 1 に、callin オプションを設定する場合を示します。

いつ表 1 â コールインオプションを設定するか

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

単方向認証を実装する方法の詳細は、『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』を参照してください。

CHAP 設定コマンドとオプション

表 2 に、CHAP コマンドとオプションをリストします。

表 2 â Chap コマンドおよびオプション

コマンド	説明
PPP 認証 {*chap* | *mschap* | *ms-chap-v2* | *eap* |*pap*}	このコマンドは、リモート PPP ピアのローカル認証を、指定したプロトコルで有効にします。

[*callin*]	
ppp chap hostname username	このコマンドは、インターフェイス固有の CHAP ホスト名を定義します。 詳細は、『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』を参照してください。
ppp chap password password	このコマンドは、インターフェイス固有の CHAP パスワードを定義します。
ppp 方向 *callin | 引き出し | 専用*	このコマンドは、コールの方向を強制的に設定します。 このコマンドは、コールが着信か発信かに関してルータが混乱している場合（たとえば、バックツーバックで接続されていたり、リース回線で接続され、Channel Service Unit or Data Service Unit [CSU/DSU] または ISDN Terminal Adapter [TA; ターミナル アダプタ] がダイヤル接続用に設定されている場合）に使用します。
ppp chap refuse [callin]	このコマンドは、ピアによるリモート認証を無効にします（デフォルトでは有効）。 このコマンドにより、CHAP 認証がすべてのコールに対して無効にされます。つまり、すべてのユーザに CHAP を使用して認証させようとするピアによる試みがすべて拒否されることを意味します。 callin オプションにより、ルータはピアから受信する CHAP 認証チャレンジへの応答を拒否するけれど、ピアに対しては、ルータの送信する CHAP チャレンジへの応答をまだ要求することが指定されます。
ppp chap wait	このコマンドは、発信側が最初に認証する必要があることを指定します（デフォルトで有効）。 このコマンドは、ピアがルータに対して自身を認証するまで、ルータは CHAP 認証を要求するピアに対して認証を行わないことを指定します。
pp	このコマンドは、認証のリトライの許容回数を指定

ppp max-bad-auth value	します（デフォルト値は 0）。 このコマンドは、認証が失敗した直後に自身をリセットするのではなく、指定した回数認証をリトライできるように、ポイントツーポイント インターフェイスを設定します。
ppp chap splitnames	この隠しコマンドを使用すると、CHAP チャレンジと応答に対して異なるホスト名を使用できます（デフォルト値は無効）。
ppp chap ignoreus	この隠しコマンドは、ローカル名を持つ CHAP チャレンジを無視します（デフォルト値は有効）。

トランザクションの例

このセクションの図は、2 台のルータ間の CHAP 認証中に起きる一連のイベントを示しています。 これらは、**debug ppp negotiation** コマンドの出力に実際に表示されるメッセージを表しているわけではありません。 詳細は、『debug ppp negotiation の出力について』を参照してください。

図 2 â はコール入ります
図 2 に、これらの手順を示します。

1. コールは 3640-1 に入ります。 着信インターフェイスは **ppp authentication chap コマンド**で設定されます。
2. LCP は CHAP および MD5 をネゴシエートします。 これを決定する方法の詳細は、『debug ppp negotiation の出力について』を参照してください。
3. 3640-1 から発信側ルータへの CHAP チャレンジが、このコールで必要になります。

チャレンジ

図 3 â は CHAP チャレンジパケット構築されます
図 3 は、2 台のルータ間の CHAP 認証における次の手順を示しています。

1. CHAP チャレンジ パケットが次の特性で作成されます。01 = チャレンジ パケット タイプの識別子。ID = チャレンジを識別するシーケンシャル番号。random = ルータによって生成される適宜ランダム番号。3640-1 = チャレンジャの認証名。
2. id 値と random 値は、着信側ルータで保持されます。

3. チャレンジ パケットが発信側ルータに送信されます。 未解決のチャレンジのリストが維持されます。

シスコの対応

図 4 ピアからのチャレンジパケットの â 受信および MD5 処理
図 4 は、どのようにピアからチャレンジ パケットが受信され、処理（MD5）されるかを示しています。 ルータは、着信 CHAP チャレンジ パケットを次のように処理します。

1. ID 値が MD5 ハッシュ ジェネレータに入力されます。
2. random 値が MD5 ハッシュ ジェネレータに入力されます。
3. 名前 3640-1 が、パスワードの参照に使用されます。 ルータは、チャレンジ内のユーザ名に一致するエントリを検索します。 この例で検索される内容は、次のとおりです。`username 3640-1 password pc1`
4. パスワードが MD5 ハッシュ ジェネレータに入力されます。結果は、MD5 ハッシュ処理済みの単方向の CHAP チャレンジとなり、CHAP 応答で返送されます。

応答（続き）

図 5 â はオーセンティケータに送られる CHAP レスポンスパケット構築されます。
図 5 は、認証者に送信される CHAP 応答パケットがどのように作成されるかを示しています。この図に、これらの手順を示します。

1. 応答パケットは、次の構成要素で構成されます。02 = CHAP 応答パケット タイプの識別子。ID = チャレンジ パケットからコピーされた ID。hash = MD5 ハッシュ ジェネレータからの出力（チャレンジ パケットからハッシュ処理された情報）。766-1 = このデバイスの認証名。 これは、ピアが身元の確認に必要なユーザ名およびパスワードのエントリを検索するために必要です（詳細は「CHAP の確認」セクションで説明されています）。
2. 次に、応答パケットがチャレンジャに送信されます。

CHAP の確認

このセクションでは、設定の確認方法に関するヒントを説明します。

図 6 â は挑戦者レスポンスパケットを処理します
図 6 は、チャレンジャが応答パケットを処理する方法を示しています。 CHAP 応答パケットが（認証側で）処理される際に行われる手順を次に示します。

1. ID は、元のチャレンジ パケットを検索するために使用されます。
2. ID が MD5 ハッシュ ジェネレータに入力されます。
3. 元のチャレンジによるランダムな値が、MD5 ハッシュ ジェネレータに入力されます。
4. 名前 766-1 は、次のソースのうちの 1 つからパスワードを検索するために使用されます。ローカル ユーザ名およびパスワードのデータベース。RADIUS サーバまたは TACACS+ サーバ。
5. パスワードが MD5 ハッシュ ジェネレータに入力されます。
6. 応答パケットで受信されたハッシュ値は、MD5 ハッシュの計算値と比較されます。 計算されたハッシュ値と受信されたハッシュ値が等しい場合、CHAP 認証は成功します。

結果

図 7 â 成功 メッセージはコーリングルータに送信 されます
図 7 は、発信側ルータに送信される成功メッセージを示しています。 この手順には、次のステップが含まれています。

1. 認証が成功した場合、CHAP 成功パケットが次の構成要素から作成されます。03 = CHAP 成功メッセージ タイプ。ID = 応答パケットからコピーされた ID。â 歓迎 inâ はユーザが読みやすい説明を提供するテキストメッセージ単にです。
2. 認証が失敗した場合、CHAP 失敗パケットが次の構成要素から作成されます。04 = CHAP 失敗メッセージ タイプ。ID = 応答パケットからコピーされた ID。â 認証 failureâ か他のテキストメッセージは、それユーザが読みやすい説明を提供します。
3. 次に、成功または失敗パケットが、発信側ルータに送信されます。**注:** この例は、単方向認証を示しています。 双方向認証では、この処理全体が繰り返されます。 ただし、発信側ルータが最初のチャレンジを開始します。

CHAP のトラブルシューティング

問題のトラブルシューティング方法についての詳細は、『PPP 認証のトラブルシューティング』を参照してください。

関連情報

- debug ppp negotiation の出力について
- PPP 認証のトラブルシューティング
- 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
- アクセス テクノロジーに関するサポート ページ
- テクニカルサポート - Cisco Systems