PPP CHAP認証の設定と理解

内容

概要

このドキュメントでは、Challenge Handshake Authentication Protocol（CHAP；チャレンジハンドシェイク認証プロトコル）が3ウェイハンドシェイクを使用してピアのIDを確認する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- インターフェイスでPPPを有効にする方法 encapsulation ppp コマンドが表示されない場合もあります。
- 「 **debug ppp negotiation** コマンド出力.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)フェーズがオープン状態でない場合のトラブルシューティング方法これは、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。If the debug ppp negotiationコマンドはLCPが開いていることを示しません。続行する前にこの問題をトラブルシューティングする必要があります。

注：このドキュメントでは、MS-CHAP（バージョン1またはバージョン2）については説明していません。

使用するコンポーネント

このドキュメントの内容は、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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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

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 で実行される一般的なステップを次に示します。

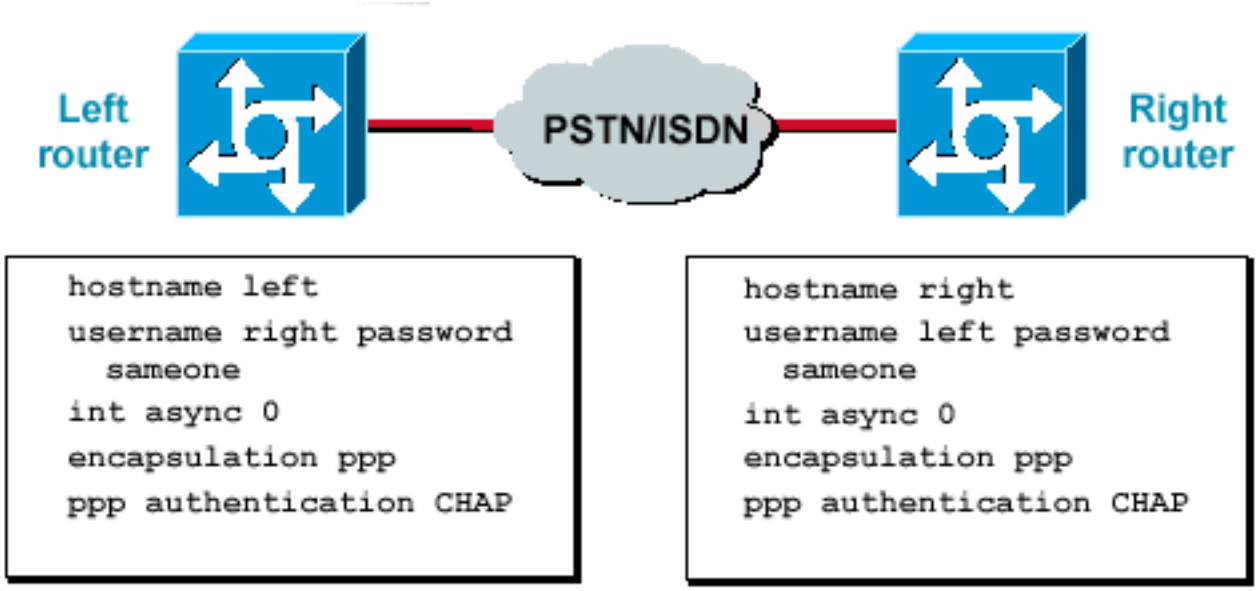
1. Link Control Protocol（LCP; リンク コントロール プロトコル）フェーズが完了し、両方のデバイス間で CHAP がネゴシエートされた後、認証側はチャレンジ メッセージをピアに送信します。
2. ピアは、一方向ハッシュ関数（Message Digest 5 [MD5]）で計算された値で応答します。
3. 認証側は、その応答が自分の計算した予測ハッシュ値と一致するかどうかをチェックします。値が一致する場合、認証は成功します。そうでない場合は、接続が解除されます。

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。

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、ネットワークを介して左右に接続された2台のルータがあるとします。



ネットワーク経由で接続された2台のルータ

図1：ネットワーク経由で接続された2台のルータ

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CHAP認証の使用を有効にするには、 ppp authentication chap コマンドが表示されない場合もあります。
3. ユーザ名とパスワードを設定します。これを行うには、 username username password passwordコマンドを発行します。ここで、usernameはピアのホスト名です。次の点を確認します。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、ルータは自身のホスト名を使用してピアに対して自身を識別します。ただし、このCHAPユーザ名は、 ppp chap hostname コマンドが表示されない場合もあります。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、 ppp authentication chap callinコマンドを発信側ルータで発行します。

表 1 に、callin オプションを設定する場合を示します。

表1: Callinオプションを設定する場合

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

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

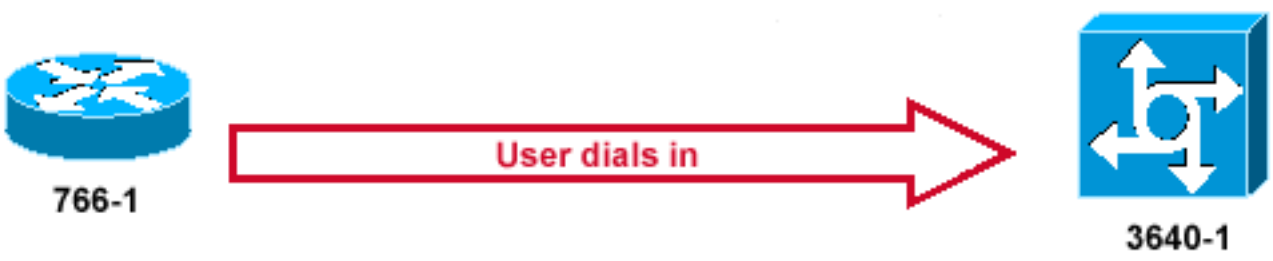
表 2 に、CHAP コマンドとオプションをリストします。

表2: CHAPのコマンドとオプション

コマンド	説明
ppp authentication {chap | ms-chap | ms-chap-v2 | eap |pap} [callin]	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
ppp chap hostnameusername	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 passwordpassword	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 directioncallin |コールアウト |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 Data Service Unit [CSU/DSU] または ISDN Terminal Adapter [TA; ターミナル アダプ
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）。 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 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
ppp max-bad-auth value	このコマンドは、認証のリトライの許容回数を指定します（デフォルト値は 0）。こ 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
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。これらのメッセージは、Cisco IOSソフトウェアリリース12.1以降で表示される debug ppp negotiationコマンド出力.詳細は、『debug ppp negotiationの出力について』を参照してください。



コ

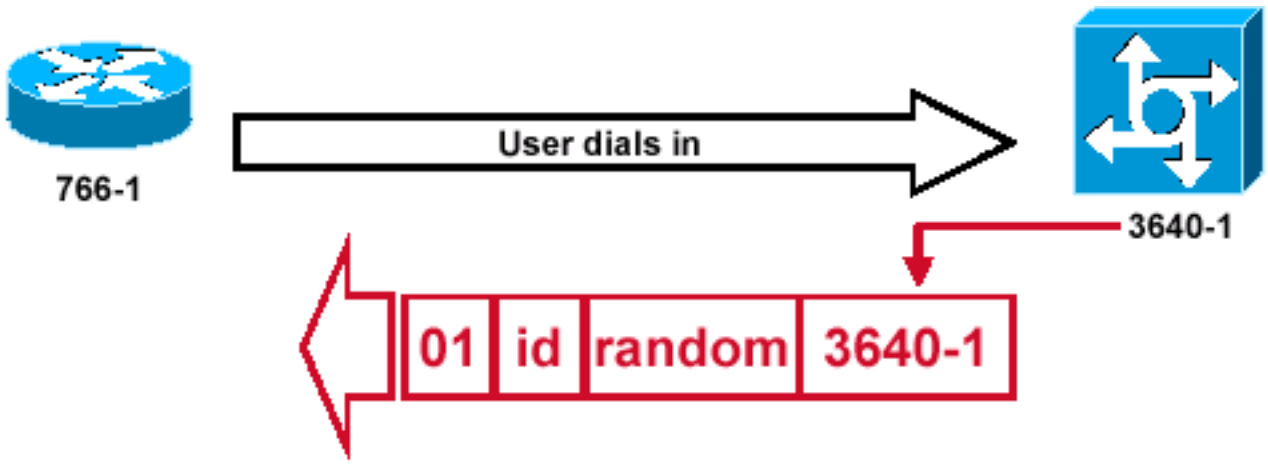
ールが着信します

図2：コールの着信

図2は、次の手順を示しています。

1. コールは3640-1に着信します。着信インターフェイスは、 ppp authentication chap コマンドが表示されない場合もあります。
2. LCP は CHAP および MD5 をネゴシエートします。これを判別する方法の詳細は、『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。

CHALLENGE



C

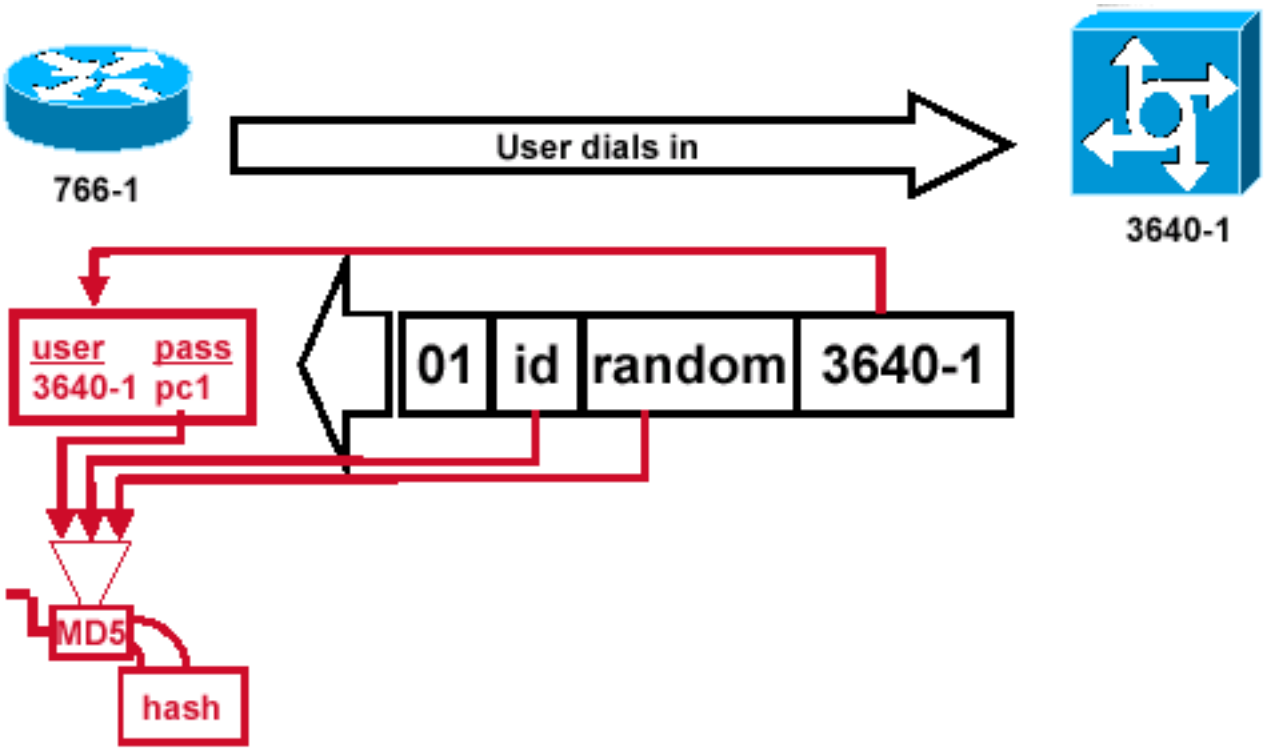
HAPチャレンジパケットの作成

図3:CHAPチャレンジパケットの作成

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。

応答



ピアから のチャレンジパケットの受信とMD5処理

図4：ピアからのチャレンジパケットの受信およびMD5処理

図4は、チャレンジパケットがピアから受信され、処理される方法(MD5)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。

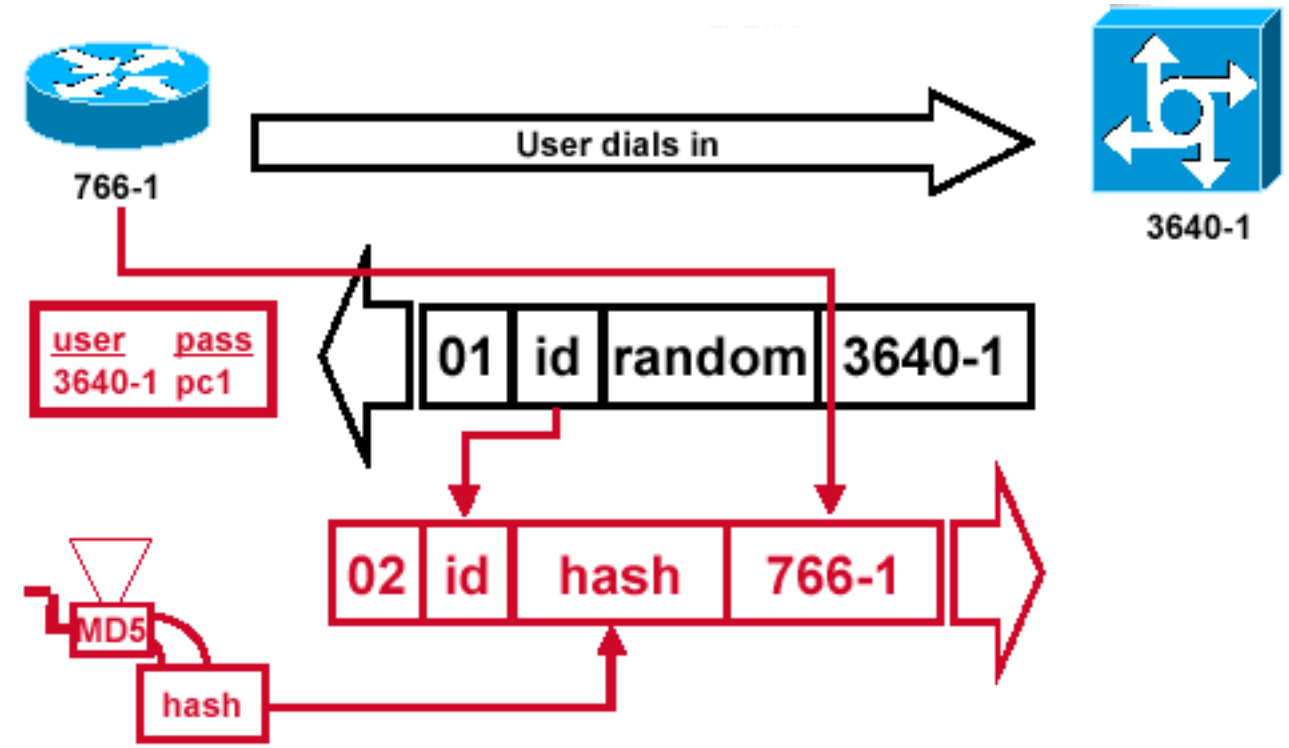
1. ID 値が MD5 ハッシュ ジェネレータに入力されます。
2. random 値が MD5 ハッシュ ジェネレータに入力されます。
3. 名前 3640-1 が、パスワードの参照に使用されます。ルータは、チャレンジ内のユーザ名に一致するエントリを検索します。この例で検索される内容は、次のとおりです。

```
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）



オーセン

ティケータに送信されるCHAP応答パケットが作成される

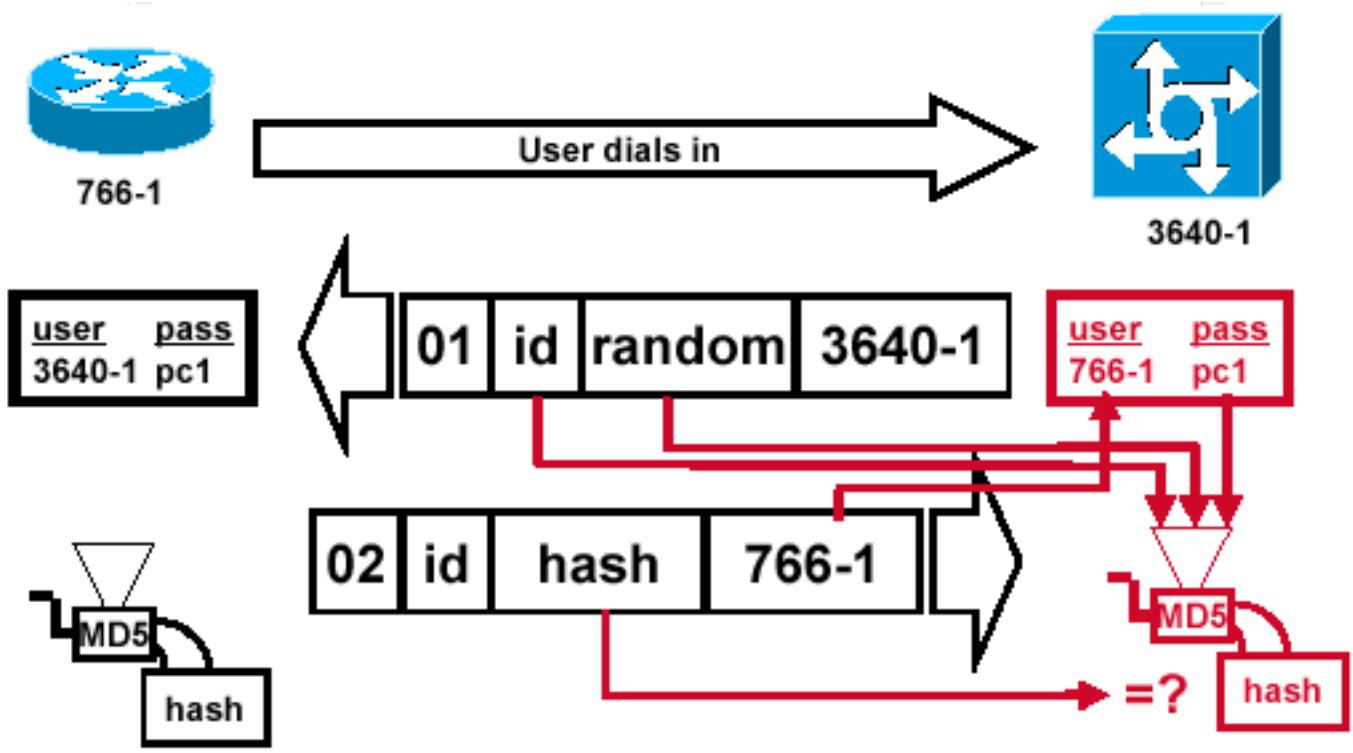
図5：オーセンティケータに送信されるCHAP応答パケットが作成される

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。



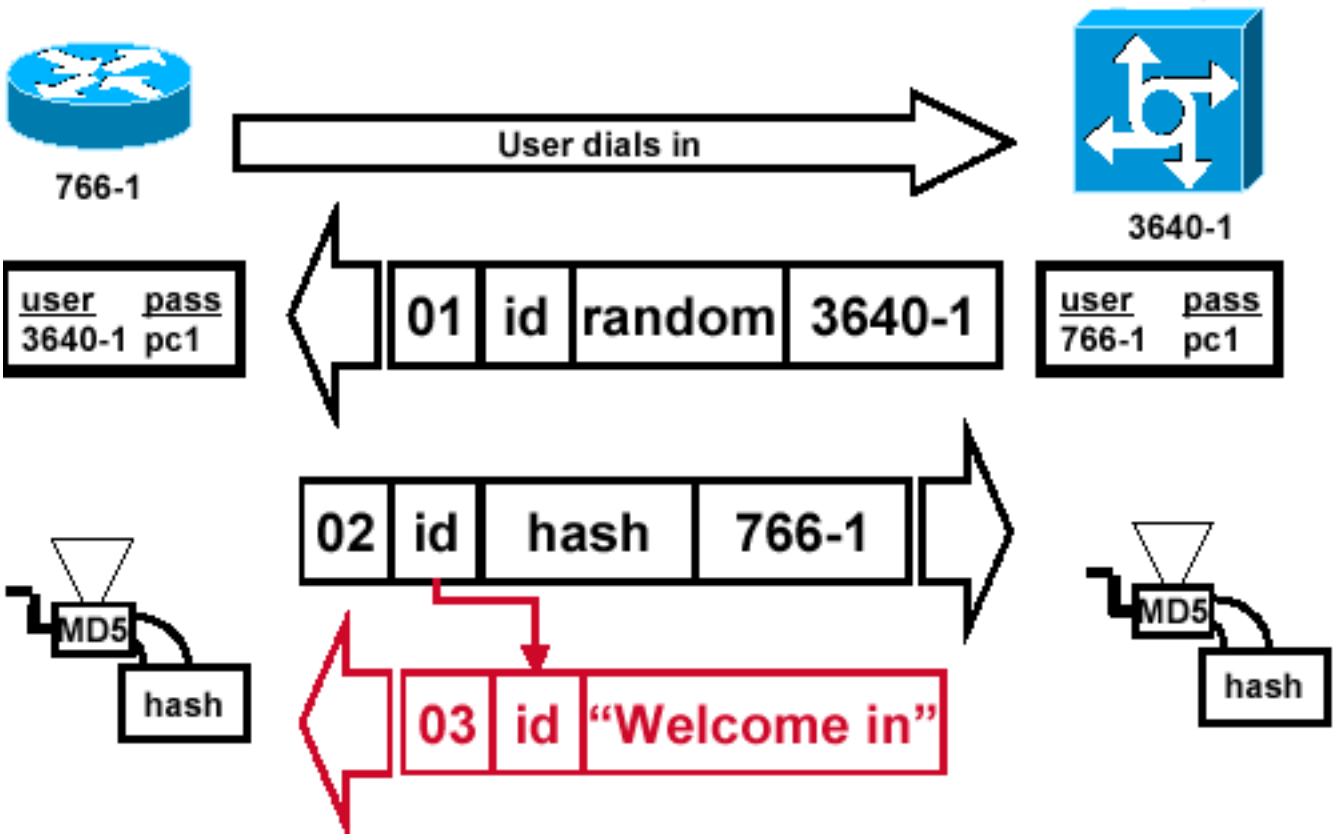
チャレンジャが応答パケットを処理する

図6：チャレンジャが応答パケットを処理する

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は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



成功メッセージが発信側ルータに送信される

図7：成功メッセージが発信側ルータに送信される

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。これには、次の手順が含まれます。

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。「Welcome in」は、ユーザが読み取り可能な説明を提供する単なるテキストメッセージです。
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。「Authentication failure」または他のテキストメッセージ。ユーザが読み取り可能な説明を提供します。
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：この例では、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は、『PPP（CHAPまたはPAP）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 chap hostnameコマンドとppp authentication chap callinコマンドを使用したPPP認証
- シスコテクニカルサポートおよびダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。