配置和瞭解PPP CHAP身份驗證

目錄

簡介

本檔案介紹質詢握手驗證通訊協定(CHAP)如何透過三次握手驗證對等點的身分。

必要條件

需求

思科建議您瞭解以下主題：

- 如何通過啟用介面上的PPP encapsulation ppp 指令。
- 其 **debug ppp negotiation** 命令輸出。如需詳細資訊，請參閱瞭解debug ppp negotiation輸出。
- 如何在鏈路控制協定(LCP)階段未處於開啟狀態時進行故障排除。這是因為在LCP階段完成並處於開啟狀態之前，PPP身份驗證階段不會開始。如果 debug ppp negotiation命令未指示LCP處於開啟狀態，您需要解決此問題才能繼續。

註：本文檔不介紹MS-CHAP（版本1或版本2）。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

詢問交握驗證通訊協定 (CHAP)（由 RFC 1994 定義）可透過三向式交握，驗證同儕節點的身分。CHAP 執行的一般步驟如下：

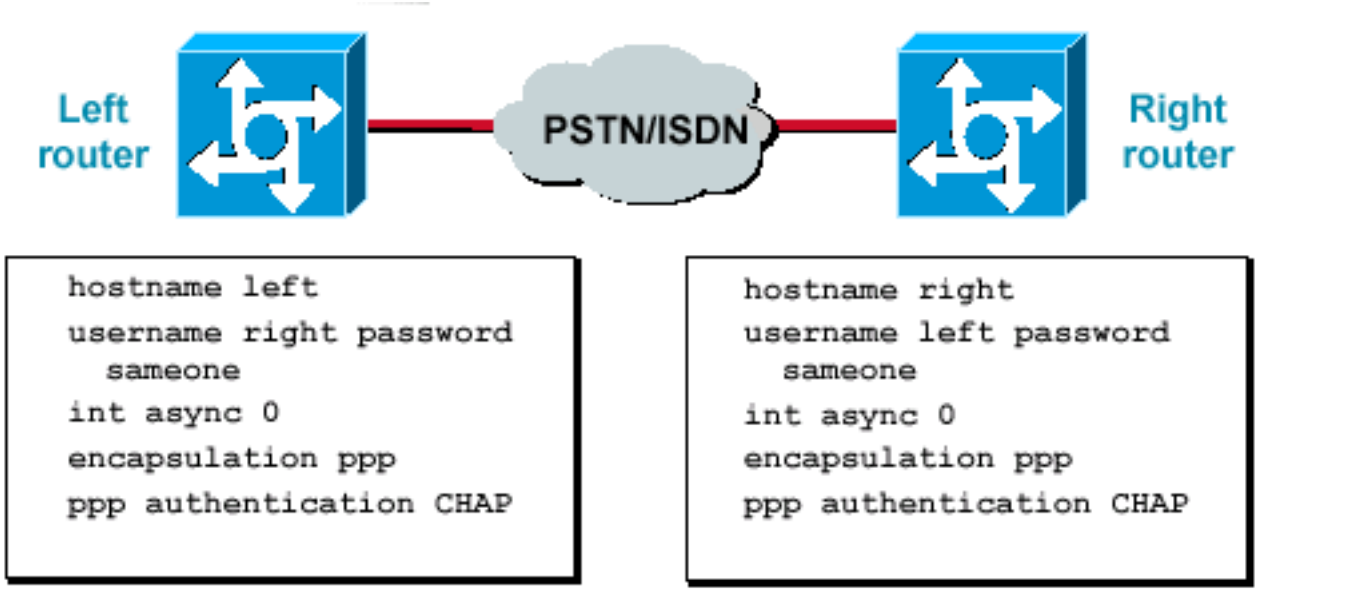
1. 在LCP（鏈路控制協定）階段完成後，兩台裝置之間協商了CHAP後，身份驗證器將向對等裝置傳送質詢消息。
2. 對等體使用通過單向雜湊函式(消息摘要5(MD5))計算出的值進行響應。
3. 驗證器根據自己的預期雜湊值計算來檢查響應。如果值匹配，則身份驗證成功。否則，連線將終止。

此身份驗證方法取決於只有身份驗證器和對等體才知道的「金鑰」。機密資訊不會通過鏈路傳送。雖然身份驗證是單向的，但您可以在兩個方向協商CHAP，使用用於相互身份驗證的相同金鑰集的幫助。

有關CHAP優缺點的詳細資訊，請參閱RFC 1994。

配置CHAP

配置CHAP的過程非常簡單。例如，假設您有兩個路由器（左側和右側）通過網路連線，如圖1所示。



兩台路由器通過網路連線

圖1 — 通過網路連線的兩台路由器

要配置CHAP身份驗證，請完成以下步驟：

1. 在介面上發出encapsulation ppp命令。
2. 在兩台路由器上啟用使用CHAP身份驗證， ppp authentication chap 指令。
3. 配置使用者名稱和密碼。為此，請發出 username username password password命令，其中username是對等體的主機名。確保：兩端的密碼相同。路由器名稱和口令完全相同，因為它們區分大小寫。

   注意：預設情況下，路由器使用其主機名向對等體標識自身。但是，此CHAP使用者名稱可以通過 ppp chap hostname 指令。有關詳細資訊，請參閱使用ppp chap hostname和ppp authentication chap callin命令的PPP身份驗證。

單向與雙向驗證

CHAP被定義為單向身份驗證方法。但是，您可以在兩個方向使用CHAP來建立雙向身份驗證。因此，使用雙向CHAP時，雙方會分別發起三次握手。

在思科CHAP實施中，預設情況下，被叫方必須對主叫方進行身份驗證（除非身份驗證完全關閉）。因此，由被叫方發起的單向身份驗證是最小可能的身份驗證。但是，主叫方也可以驗證被叫方的身份，這將導致雙向身份驗證。

連線到非Cisco裝置時，通常需要單向身份驗證。

對於單向身份驗證，請配置 ppp authentication chap callin呼叫路由器上的命令。

表1顯示了何時配置callin選項。

表1：配置呼入選項的時間

驗證型別	客戶端（呼叫）	NAS（呼叫）
單向（單向）	ppp authentication chap callin	ppp authentication chap
雙向（雙向）	ppp authentication chap	ppp authentication chap

有關詳細資訊，請參閱使用ppp chap hostname和ppp authentication chap callin命令的PPP身份驗證。

CHAP配置命令和選項

表2列出了CHAP命令和選項：

表2:CHAP命令和選項

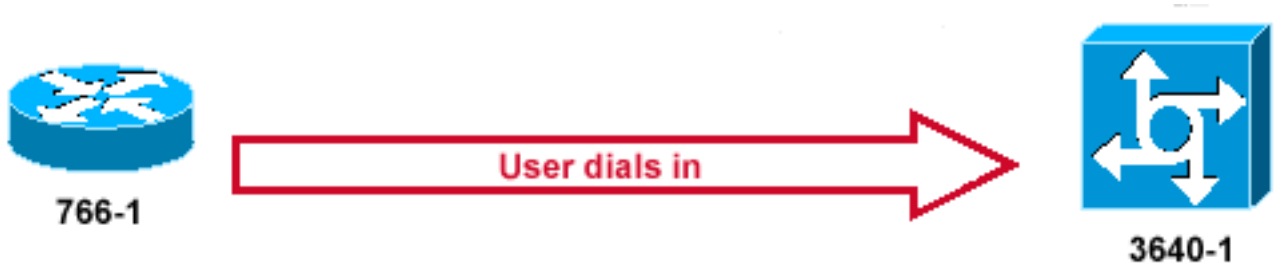
指令	說明
ppp身份驗證{chap | ms-chap | ms-chap-v2 | eap |pap} [callin]	此命令啟用具有指定協定的遠端PPP對等體的本地身份驗證。
ppp chap hostname使用者名	此命令定義介面特定的CHAP主機名。有關詳細資訊，請參閱使用ppp chap hostname和
ppp chap口令口令	此命令定義介面特定的CHAP密碼。
ppp direction callin	此命令強制呼叫方向。當路由器對呼叫是傳入還是傳出感到困惑時(例如，背對背連線或

|標註 |專用
ppp chap拒絕 [callin]	此命令禁用對等體的遠端身份驗證（預設啟用）。使用此命令，將禁用所有呼叫的CHA
ppp chap wait	此命令指定呼叫方必須首先進行身份驗證（預設啟用）。此命令指定路由器不會向請求
ppp max-bad-auth value	此命令指定允許的身份驗證重試次數（預設值為0）。此命令將點對點介面配置為在身
ppp chap拆分名稱	此隱藏命令允許CHAP質詢和響應使用不同的主機名（預設值為禁用）。
ppp chap ignoreus	此隱藏命令將忽略本地名稱的CHAP質詢（預設值已啟用）。

事務性示例

本節中的圖示顯示了兩台路由器之間的CHAP身份驗證期間發生的一系列事件。這些並不代表在debug ppp negotiation命令輸出。如需詳細資訊，請參閱瞭解debug ppp negotiation輸出。

通話



來

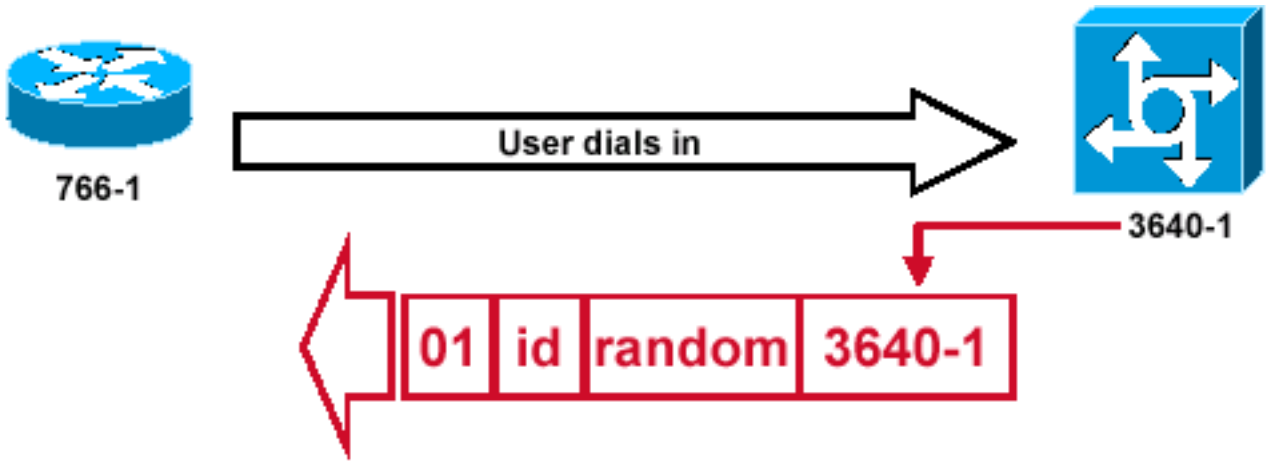
電進入

圖2 — 呼叫進入

圖2 顯示了以下步驟：

1. 電話是撥打3640-1。傳入介面配置有 ppp authentication chap 指令。
2. LCP會協商CHAP和MD5。有關如何確定此情況的詳細資訊，請參閱瞭解debug ppp negotiation輸出。
3. 此呼叫需要從3640-1到呼叫路由器的CHAP質詢。

挑戰



C

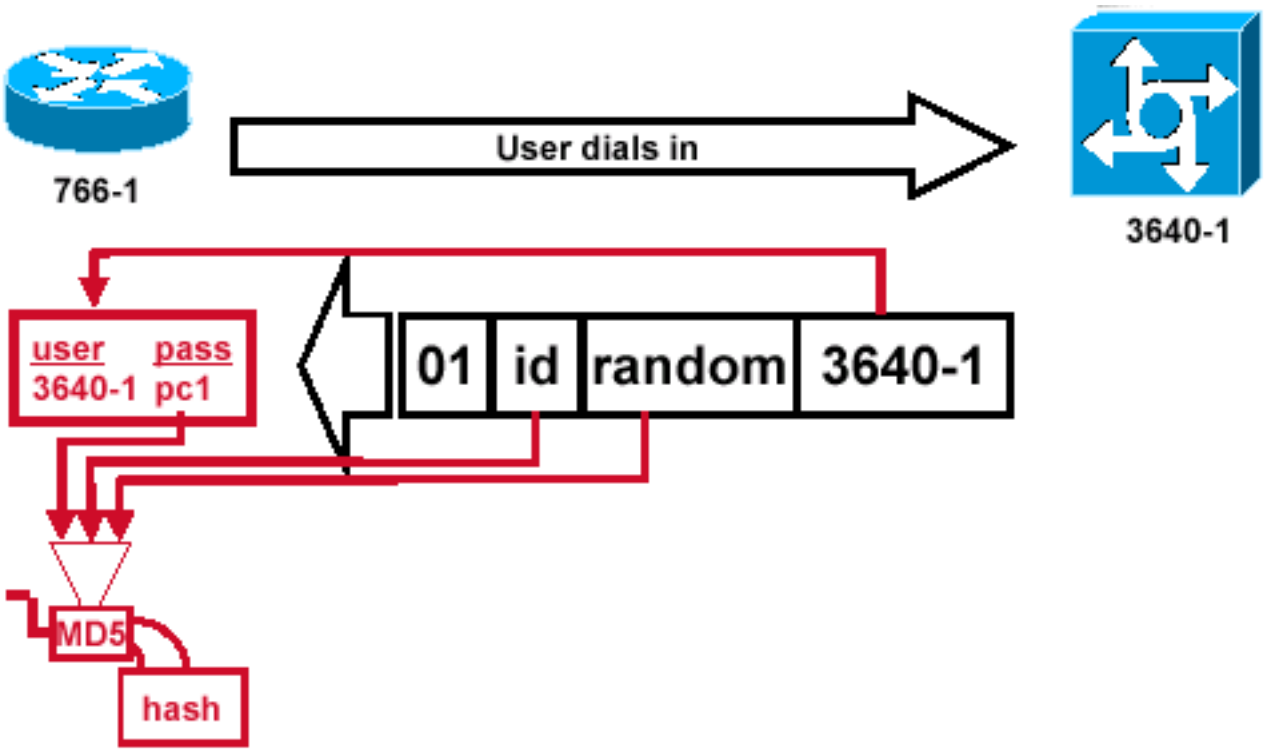
HAP質詢資料包已生成

圖3 - CHAP質詢資料包已生成

圖3說明了兩台路由器之間的CHAP身份驗證中的以下步驟：

1. 構建的CHAP質詢資料包具有以下特性：01 =質詢資料包型別識別符號。ID =標識質詢的序列號。random =路由器生成的合理隨機數。3640-1 =挑戰者的身份驗證名稱。
2. ID和隨機值儲存在被呼叫的路由器上。
3. 質詢資料包被傳送到呼叫路由器。保留一份未解決的挑戰清單。

響應



從對等方接收質詢資料包並進行MD5處理

圖4 — 從對等方接收質詢資料包並進行MD5處理

圖4說明了如何從對等裝置接收和處理質詢資料包(MD5)。路由器通過以下方式處理傳入的CHAP質詢資料包：

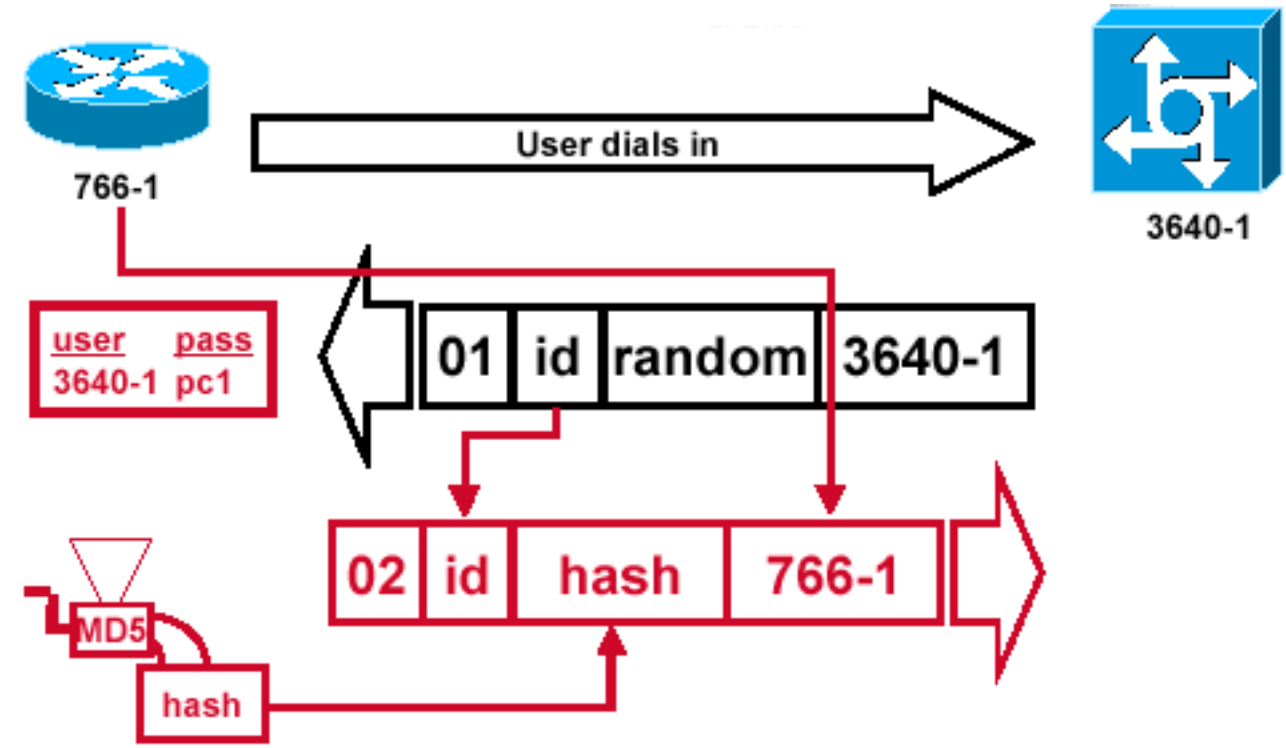
1. 該ID值將饋入MD5雜湊生成器。
2. 隨機值被饋入MD5雜湊生成器。
3. 名稱3640-1用於查詢密碼。路由器會尋找與挑戰賽中的使用者名稱相符的專案。在此範例中，會尋找：

```
username 3640-1 password pc1
```

4.將密碼輸入到MD5雜湊生成器。

結果是在CHAP響應中傳送回的單向MD5雜湊CHAP質詢。

回應（續）



傳送到身份驗證器的CHAP響應資料包已生成

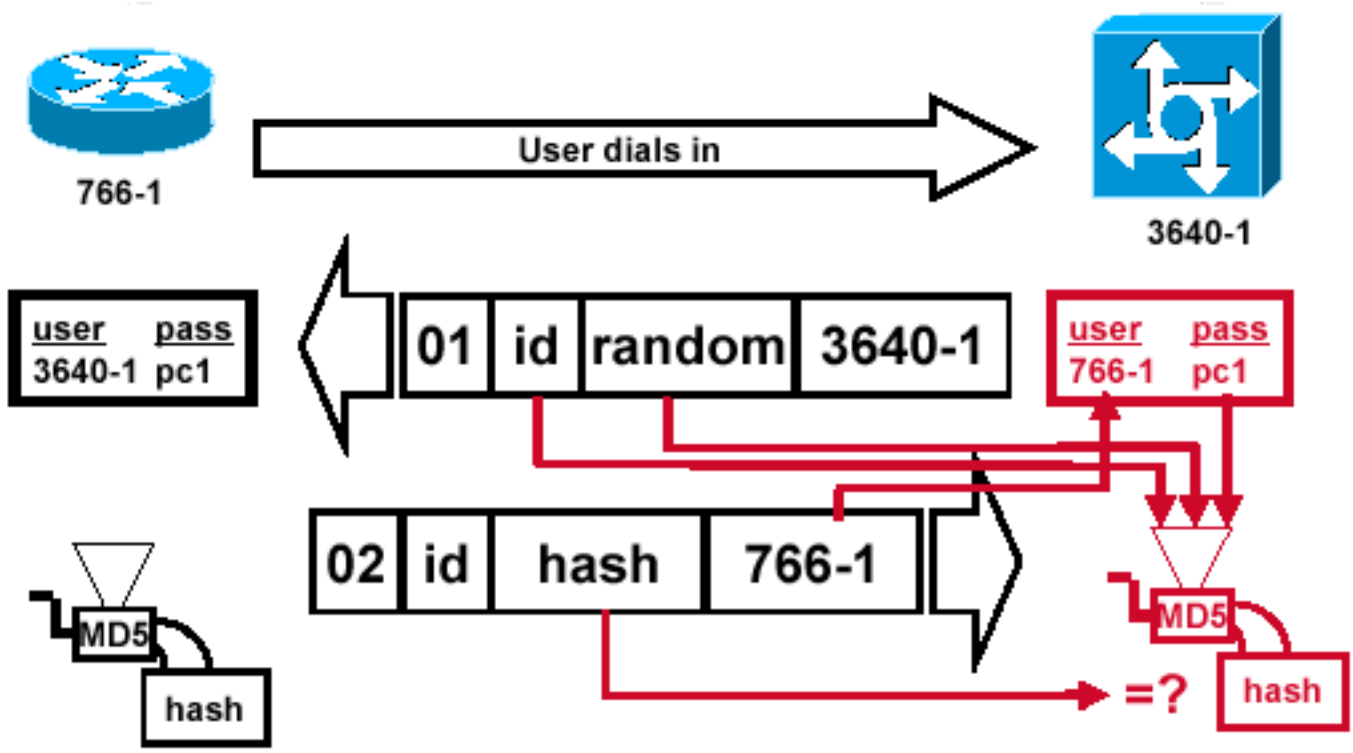
圖5 — 傳送到身份驗證器的CHAP響應資料包已生成

圖5說明了如何構建傳送到身份驗證器的CHAP響應資料包。此圖顯示以下步驟：

1. 響應資料包由以下元件組合而成：02 = CHAP響應資料包型別識別符號。ID =從質詢資料包複製。雜湊= MD5雜湊生成器的輸出（來自質詢資料包的雜湊資訊）。766-1 =此裝置的身份驗證名稱。對等體需要執行此操作來查詢驗證身份所需的使用者名稱和密碼條目(驗證CHAP部分將對此進行更詳細的說明)。
2. 然後將響應資料包傳送到挑戰者。

驗證CHAP

本節提供有關如何驗證配置的提示。



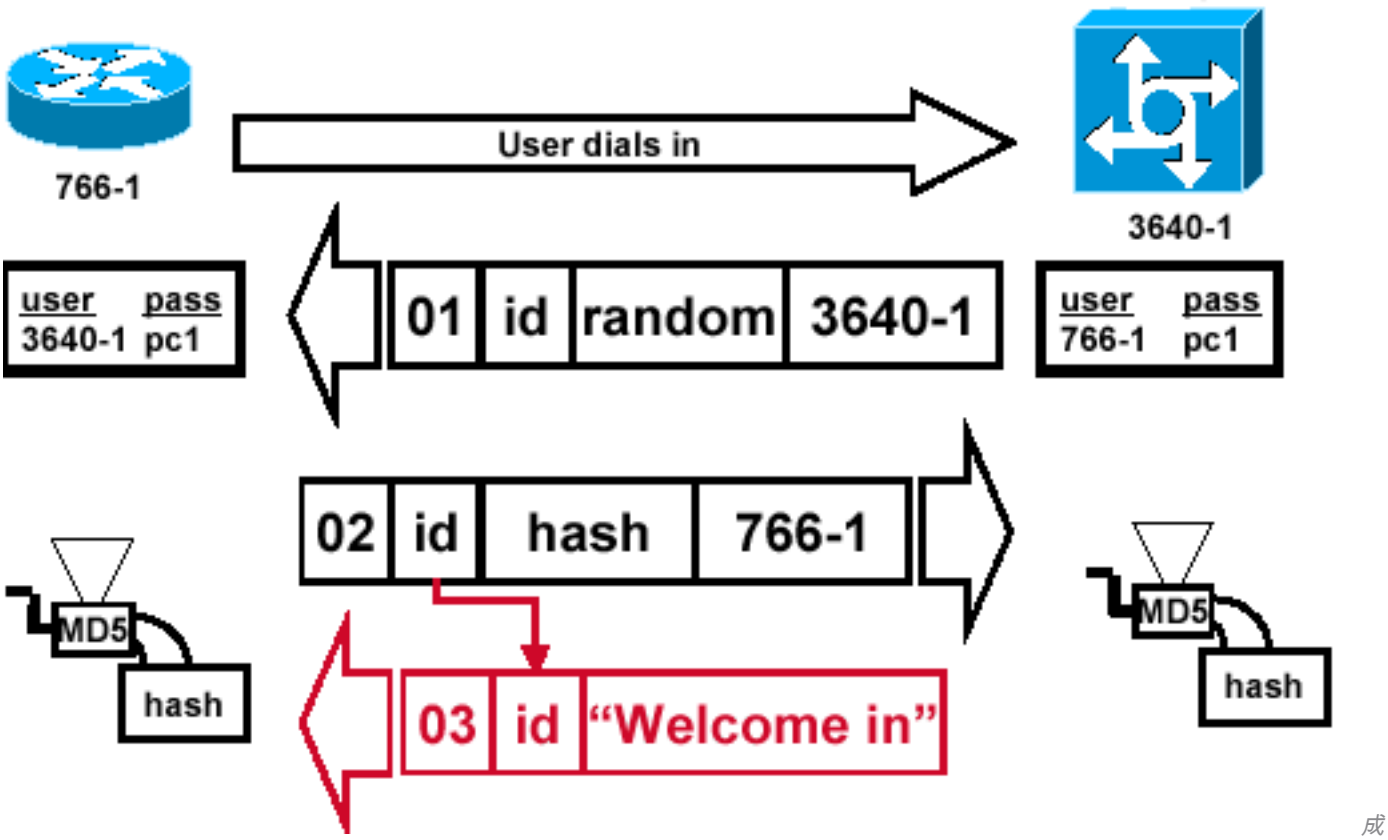
Challenger處理響應資料包

圖6 — 挑戰者處理響應資料包

圖6顯示了挑戰者如何處理響應資料包。以下是處理CHAP響應資料包（在身份驗證器上）時涉及的步驟：

1. 該ID用於查詢原始質詢資料包。
2. 該ID被饋入MD5雜湊生成器。
3. 原始的詢問隨機值被輸入到MD5雜湊生成器。
4. 名稱766-1用於從以下來源之一查詢密碼：本地使用者名稱和密碼資料庫。RADIUS或TACACS+伺服器。
5. 密碼被輸入到MD5雜湊生成器。
6. 然後將響應資料包中接收的雜湊值與計算的MD5雜湊值進行比較。如果計算的雜湊值和收到的雜湊值相等，則CHAP身份驗證成功。

結果



成功消息被傳送到呼叫路由器

圖7 — 成功消息傳送到呼叫路由器

圖7顯示了傳送至呼叫路由器的成功消息。這涉及以下步驟：

1. 如果驗證成功，則會使用以下元件構建CHAP成功資料包：03 = CHAP成功消息型別。ID =從響應資料包複製。「歡迎加入」只是提供使用者可讀說明的文本消息。
2. 如果身份驗證失敗，則會從以下元件生成CHAP失敗資料包：04 = CHAP失敗消息型別。ID =從響應資料包複製。「身份驗證失敗」或其他文本消息，提供使用者可讀的解釋。
3. 然後，成功或失敗資料包被傳送到呼叫路由器。

註：此範例說明單向驗證。在雙向驗證中，會重複整個過程。但是，呼叫路由器發起初始質詢。

CHAP故障排除

有關如何排除任何問題的資訊，請參閱排除PPP（CHAP或PAP）身份驗證故障。

相關資訊

- 瞭解debug ppp negotiation輸出
- 使用ppp chap hostname和ppp authentication chap callin命令進行PPP身份驗證
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。