PPP CHAP-Authentifizierung verstehen und konfigurieren

Inhalt

Einführung

Das Challenge Handshake Authentication Protocol (CHAP) (definiert in RFC 1994) überprüft die Identität des Peers mithilfe eines Drei-Wege-Handshake. Dies sind die allgemeinen Schritte, die in CHAP durchgeführt werden:

1. Nachdem die LCP-Phase (Link Control Protocol) abgeschlossen und CHAP zwischen beiden Geräten ausgehandelt wurde, sendet der Authentifizierer eine Prüfmeldung an den Peer.
2. Der Peer antwortet mit einem Wert, der durch eine unidirektionale Hash-Funktion berechnet wird (Message Digest 5 (MD5)).
3. Der Authentifizierer überprüft die Antwort anhand seiner eigenen Berechnung des erwarteten Hashwerts. Wenn die Werte übereinstimmen, ist die Authentifizierung erfolgreich. Andernfalls wird die Verbindung beendet.

Diese Authentifizierungsmethode hängt von einem "geheimen" Verfahren ab, das nur dem Authentifizierer und dem Peer bekannt ist. Das Geheimnis wird nicht über den Link übertragen. Obwohl die Authentifizierung nur in eine Richtung erfolgt, können Sie mithilfe desselben geheimen Satzes für die gegenseitige Authentifizierung CHAP in beide Richtungen aushandeln.

Weitere Informationen zu Vor- und Nachteilen von CHAP finden Sie in RFC 1994 .

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten folgende Themen kennen:

- Aktivieren von PPP auf der Schnittstelle mithilfe des Befehls **encapsulation ppp**.
- Die Befehlsausgabe des Befehls **debug ppp negotiation**. Weitere Informationen finden Sie unter Grundlagen der Debug-PPP-Aushandlung.
- Fehlerbehebung, wenn sich die LCP-Phase (Link Control Protocol) nicht im offenen Zustand befindet. Dies liegt daran, dass die PPP-Authentifizierungsphase erst beginnt, wenn die LCP-Phase abgeschlossen ist und sich im offenen Zustand befindet. Wenn der Befehl **debug ppp negotiation** nicht angibt, dass LCP offen ist, müssen Sie dieses Problem beheben, bevor Sie fortfahren.

Hinweis: Dieses Dokument bezieht sich nicht auf MS-CHAP (Version 1 oder Version 2). Weitere Informationen zu MS-CHAP finden Sie in den Dokumenten MS-CHAP Support und MSCHAP Version 2.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

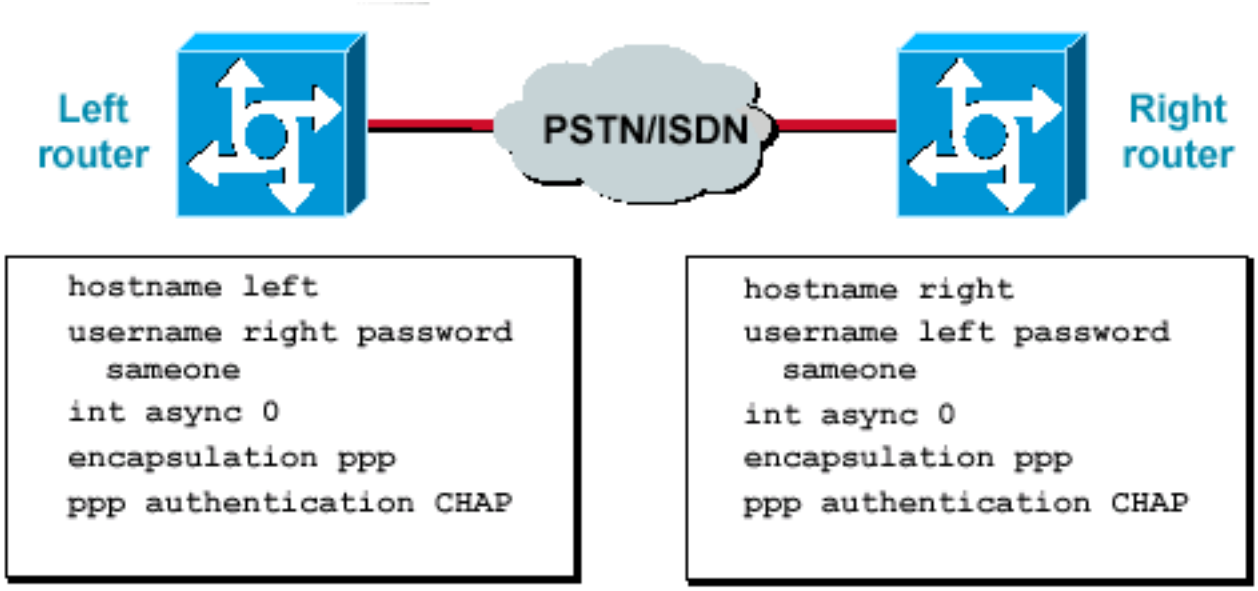
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

CHAP konfigurieren

Die Vorgehensweise zum Konfigurieren von CHAP ist relativ einfach. Nehmen Sie beispielsweise an, dass zwei Router (links und rechts) über ein Netzwerk verbunden sind (siehe Abbildung 1).

Abbildung 1: zwei Router, die über ein Netzwerk verbunden sind



Gehen Sie wie folgt vor, um die CHAP-Authentifizierung zu konfigurieren:

1. Geben Sie auf der Schnittstelle den Befehl **encapsulation ppp ein**.
2. Aktivieren Sie die Verwendung der CHAP-Authentifizierung auf beiden Routern mit dem Befehl **ppp authentication chap**.
3. Konfigurieren Sie die Benutzernamen und Kennwörter. Geben Sie dazu den Befehl **username *username* password** ein, wobei *Benutzername* der Hostname des Peers ist. Stellen Sie sicher, dassKennwörter sind an beiden Enden identisch.Der Router-Name und das Kennwort sind identisch, da zwischen Groß- und Kleinschreibung unterschieden wird.**Hinweis:** Standardmäßig identifiziert sich der Router anhand seines Hostnamens für den Peer. Der CHAP-Benutzername kann jedoch über den Befehl **ppp chap hostname** geändert werden. Weitere Informationen finden Sie unter Befehle für PPP-Authentifizierung mithilfe des PPP-chap-Hostnamens und des ppp-Authentifizierungskopfs.

One-Way- und Two-Way-Authentifizierung

CHAP wird als unidirektionale Authentifizierungsmethode definiert. Sie verwenden jedoch CHAP in beide Richtungen, um eine Zwei-Wege-Authentifizierung zu erstellen. Daher wird bei einem bidirektionalen CHAP von jeder Seite ein separater Drei-Wege-Handshake initiiert.

In der Cisco CHAP-Implementierung muss der Angerufene standardmäßig den anrufenden Teilnehmer authentifizieren (es sei denn, die Authentifizierung ist komplett deaktiviert). Aus diesem Grund ist eine vom angerufenen Teilnehmer initiierte unidirektionale Authentifizierung die minimale mögliche Authentifizierung. Der anrufende Teilnehmer kann jedoch auch die Identität des angerufenen Teilnehmers überprüfen, was zu einer Zwei-Wege-Authentifizierung führt.

Eine unidirektionale Authentifizierung ist häufig erforderlich, wenn Sie eine Verbindung mit Geräten von Drittanbietern herstellen.

Konfigurieren Sie für die unidirektionale Authentifizierung den Befehl **ppp authentication chap callin** auf dem anrufenden Router.

Tabelle 1 zeigt, wann die Anrufoption konfiguriert werden muss.

Tabelle 1 - Wann wird die Callin-Option konfiguriert?

Authentifizierungstyp	Client (anrufen)	NAS (genannt)
unidirektional (unidirektional)	PPP-Authentifizierungs-Chap-Callin	PPP-Authentifizierungsschap
Zweiwege (bidirektional)	PPP-Authentifizierungsschap	PPP-Authentifizierungsschap

Weitere Informationen zum Implementieren der unidirektionalen Authentifizierung finden Sie unter PPP-Authentifizierung mithilfe des PPP-chap-Hostnamens und ppp-Authentifizierungsschap-Callin-Befehle.

CHAP-Konfigurationsbefehle und -optionen

In Tabelle 2 sind die Befehle und Optionen des CHAP aufgeführt:

Tabelle 2 - CHAP-Befehle und -Optionen

Befehl	Beschreibung
ppp-Authentifizierung {*chap	ms-chap	ms-chap-v2	Seife |pap*} [*callin*]	Dieser Befehl aktiviert die lokale Authentifizierung des Remote-PPP-Peers mit dem angegebenen Protokoll.
ppp chap Hostname *Benutzername*	Dieser Befehl definiert einen schnittstellenspezifischen CHAP-Hostnamen. Weitere Informationen finden Sie unter Befehle für PPP-Authentifizierung mithilfe des PPP-chap-Hostnamens und des ppp-Authentifizierungskopfs.
ppp chap Kennwort *Kennwort*	Dieser Befehl definiert ein schnittstellenspezifisches CHAP-Kennwort.
Anruf **in** *ppp-Richtung*	*Callout*	Dieser Befehl erzwingt eine Anrufrichtung. Verwenden Sie diesen Befehl, wenn ein Router verwirrt ist, ob der Anruf ein- oder ausgeht (z. B. wenn er mit einer Back-to-Back-Verbindung verbunden ist oder über Mietleitungen verbunden ist und die Channel Service Unit oder Data Service Unit (CSU/DSU) oder der ISDN Terminal Adapter (TA) für die Wählfunktion konfiguriert sind).
ppp chap Müll [*Callin*]	Dieser Befehl deaktiviert die Remote-Authentifizierung durch einen Peer (standardmäßig aktiviert). Mit diesem Befehl

	wird die CHAP-Authentifizierung für alle Anrufe deaktiviert. Das bedeutet, dass alle Versuche des Peers, den Benutzer mithilfe von CHAP zu zwingen, sich zu authentifizieren, abgelehnt werden. Die Anrufoption gibt an, dass der Router sich weigert, die vom Peer empfangenen CHAP-Authentifizierungsprobleme zu beantworten, aber trotzdem den Peer benötigt, um alle vom Router gesendeten CHAP-Herausforderungen zu bewältigen.
ppp chap Warten	Dieser Befehl gibt an, dass sich der Anrufer zuerst authentifizieren muss (standardmäßig aktiviert). Dieser Befehl gibt an, dass sich der Router erst dann bei einem Peer authentifiziert, der eine CHAP-Authentifizierung anfordert, wenn sich der Peer beim Router authentifiziert hat.
ppp max-bad-auth-*Wert*	Dieser Befehl gibt die zulässige Anzahl von Wiederholungsversuchen für die Authentifizierung an (der Standardwert ist 0). Mit diesem Befehl wird eine Point-to-Point-Schnittstelle so konfiguriert, dass sie sich nicht sofort nach einem Authentifizierungsfehler zurücksetzt, sondern stattdessen eine angegebene Anzahl von Authentifizierungsversuchen zulässt.
ppp chap Splitnamen	Dieser ausgeblendete Befehl ermöglicht verschiedene Hostnamen für eine CHAP-Herausforderung und -Antwort (der Standardwert ist deaktiviert).
PPP CHAP ignoriert	Dieser ausgeblendete Befehl ignoriert CHAP-Herausforderungen mit dem lokalen Namen (der Standardwert ist aktiviert).

Transaktionsbeispiel

Die Diagramme in diesem Abschnitt zeigen die Ereignisreihen, die während einer CHAP-Authentifizierung zwischen zwei Routern auftreten. Diese stellen nicht die tatsächlichen Meldungen dar, die in der Befehlsausgabe des Befehls **debug ppp negotiation** angezeigt werden. Weitere Informationen finden Sie unter Understanding debug ppp negotiation Output.

Anruf

Abbildung 2 - der Anruf kommt ein

Abbildung 2 zeigt folgende Schritte:

1. Der Anruf geht an 3640-1. Die eingehende Schnittstelle wird mit dem Befehl **ppp authentication chap** konfiguriert.
2. LCP handelt CHAP und MD5 aus. Weitere Informationen zum Ermitteln dieser Methode finden Sie unter Grundlagen der Ausgabe der Debugging-PPP-Aushandlung.
3. Für diesen Anruf ist eine CHAP-Herausforderung von 3640-1 an den anrufenden Router erforderlich.

Herausforderung

Abbildung 3: ein CHAP-Challenge-Paket erstellt

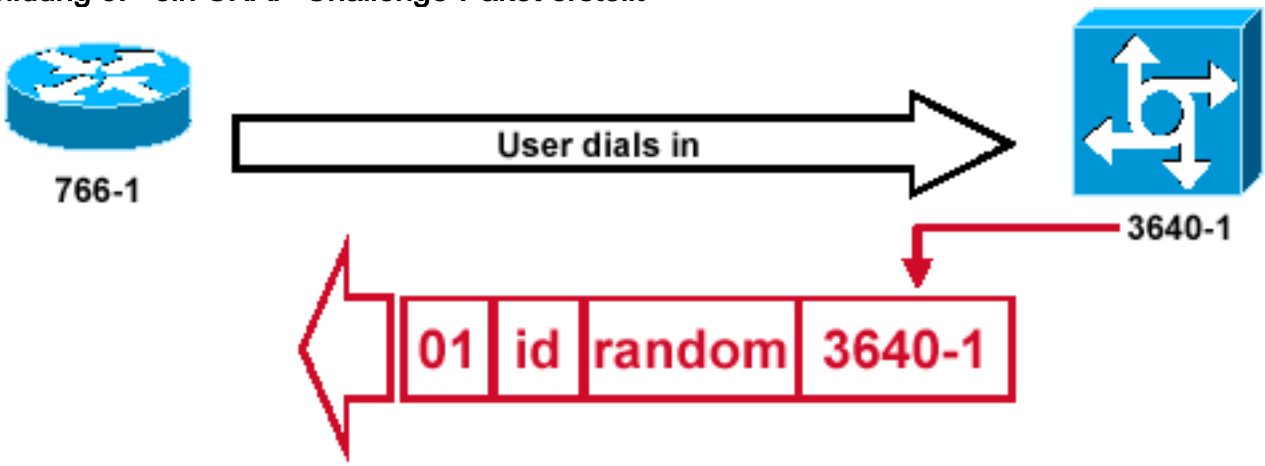


Abbildung 3 veranschaulicht diese Schritte bei der CHAP-Authentifizierung zwischen den beiden Routern:

1. Ein CHAP-Challenge-Paket baut auf folgenden Eigenschaften auf:01 = herausfordernde Pakettyp-Kennung.ID = sequenzielle Nummer zur Identifizierung der Herausforderung.random = eine nach dem Zufallsprinzip vom Router generierte Zahl.3640-1 = der Authentifizierungsname des Herausforderers.
2. Die ID und Zufallswerte werden auf dem angerufenen Router beibehalten.
3. Das Challenge-Paket wird an den anrufenden Router gesendet. Es wird eine Liste der noch offenen Herausforderungen geführt.

Antwort

Abbildung 4: des Empfangs und MD5-Verarbeitung des Challenge-Pakets vom Peer

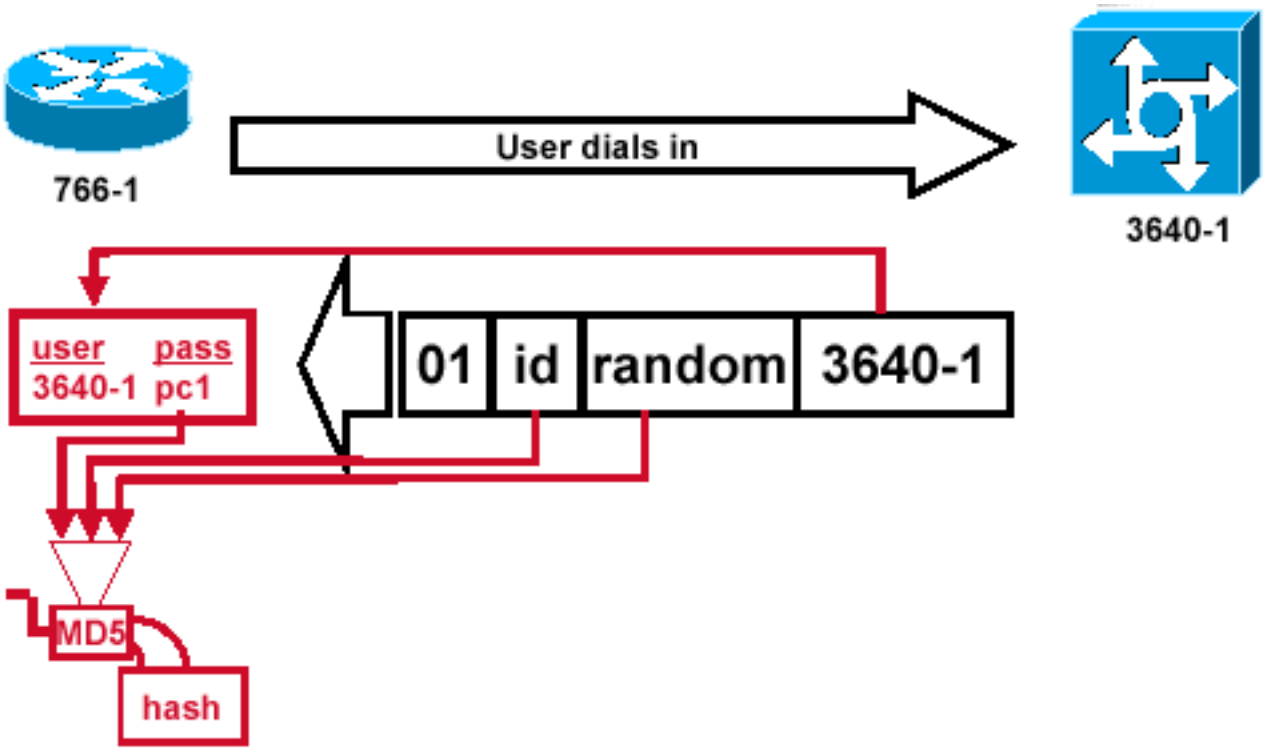


Abbildung 4 veranschaulicht, wie das Challenge-Paket vom Peer empfangen und verarbeitet wird (MD5). Der Router verarbeitet das eingehende CHAP-Challenge-Paket folgendermaßen:

1. Der ID-Wert wird in den MD5-Hash-Generator eingespeist.
2. Der Zufallswert wird in den MD5-Hash-Generator eingespeist.
3. Der Name 3640-1 wird zum Nachschlagen des Kennworts verwendet. Der Router sucht nach einem Eintrag, der mit dem Benutzernamen der Herausforderung übereinstimmt. In diesem Beispiel wird Folgendes gesucht:
   ```
   username 3640-1 password pc1
   ```
4. Das Kennwort wird in den MD5-Hash-Generator eingegeben.Das Ergebnis ist die unidirektionale MD5-Hash-CHAP-Herausforderung, die in der CHAP-Antwort zurückgesendet wird.

Antwort (Fortsetzung)

Abbildung 5 - Das an den Authentifizierer gesendete CHAP-Antwortpaket ist erstellt.

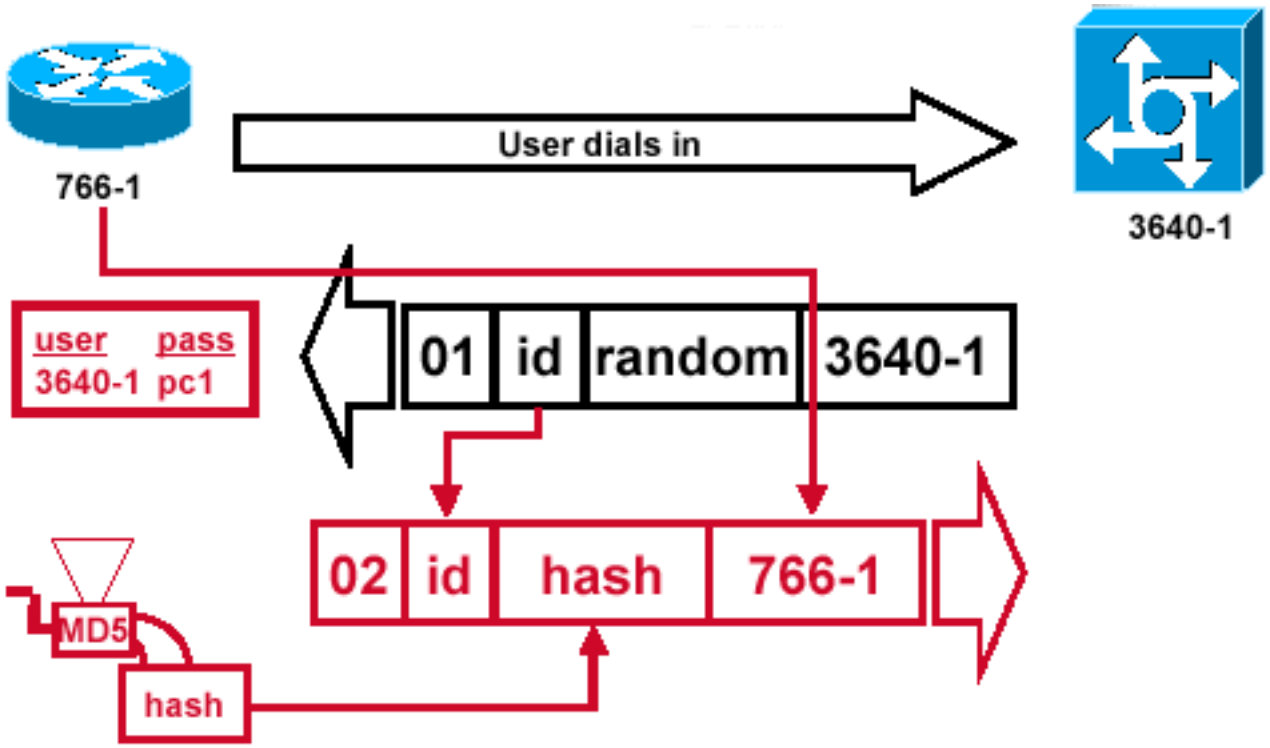


Abbildung 5 veranschaulicht, wie das an den Authentifizierer gesendete CHAP-Antwortpaket erstellt wird. Dieses Diagramm zeigt die folgenden Schritte:

1. Das Antwortpaket wird aus den folgenden Komponenten zusammengestellt:02 = CHAP-Antwortpakettypkennung.ID = aus dem Challenge-Paket kopiert.hash = die Ausgabe des MD5-Hash-Generators (die Hashinformationen aus dem Chassis-Paket).766-1 = der Authentifizierungsname des Geräts. Dies ist erforderlich, damit der Peer den Benutzernamen und das Kennwort nachschlagen kann, die zur Überprüfung der Identität erforderlich sind (dies wird im Abschnitt CHAP überprüfen genauer erläutert).
2. Das Response-Paket wird dann an den Herausforderer gesendet.

CHAP überprüfen

Dieser Abschnitt enthält Tipps zur Überprüfung Ihrer Konfiguration.

Abbildung 6 - Der Challenger verarbeitet das Response-Paket

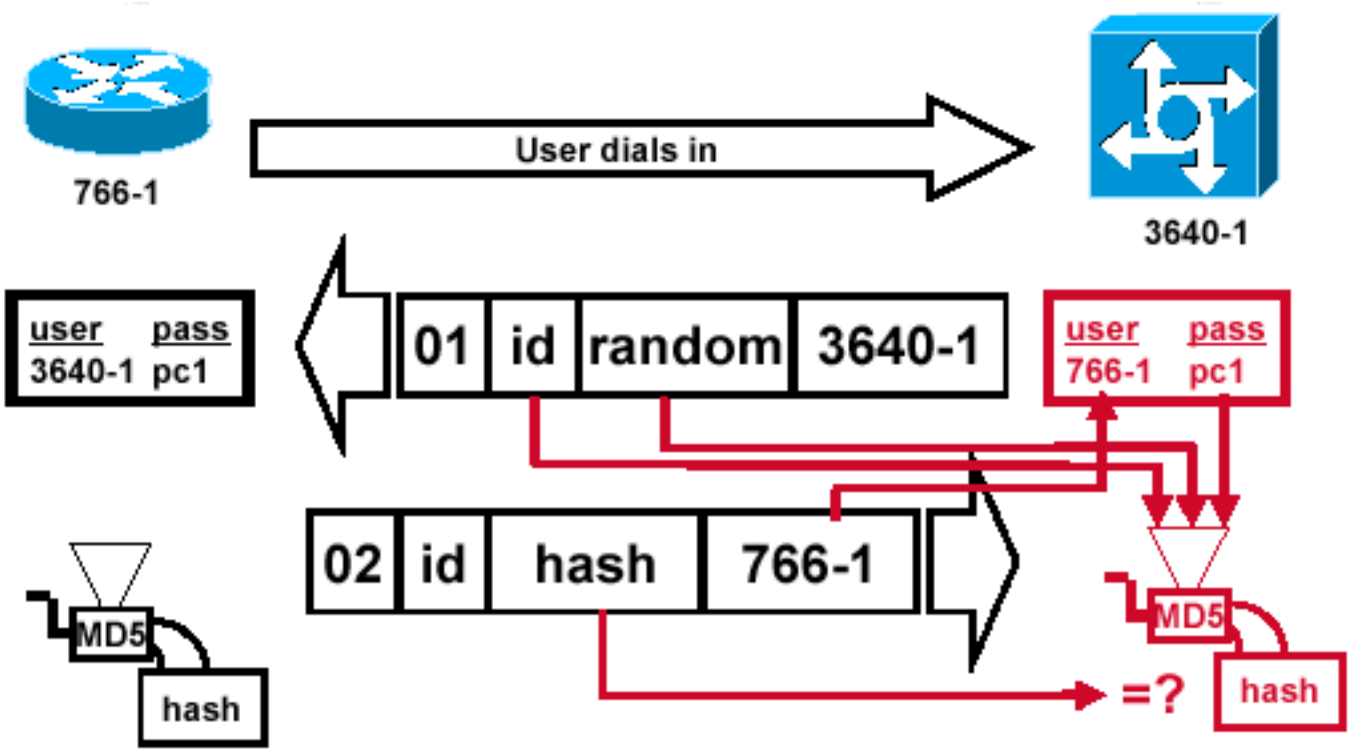


Abbildung 6 zeigt, wie der Herausforderer das Antwortpaket verarbeitet. Im Folgenden sind die Schritte aufgeführt, die bei der Verarbeitung des CHAP-Antwortpakets (auf dem Authentifizierer) erforderlich sind:

1. Die ID wird verwendet, um das ursprüngliche Challenge-Paket zu finden.
2. Die ID wird in den MD5-Hash-Generator eingespeist.
3. Der ursprüngliche Zufallswert der Herausforderung wird in den MD5-Hash-Generator eingespeist.
4. Der Name 766-1 wird verwendet, um aus einer der folgenden Quellen nach dem Kennwort zu suchen:Lokale Datenbank mit Benutzernamen und Kennwort.RADIUS- oder TACACS+-Server.
5. Das Kennwort wird in den MD5-Hash-Generator eingegeben.
6. Der im Antwortpaket empfangene Hashwert wird dann mit dem berechneten MD5-Hashwert verglichen. Die CHAP-Authentifizierung ist erfolgreich, wenn die berechneten und die empfangenen Hash-Werte gleich sind.

Ergebnis

Abbildung 7 - Erfolgsmeldung wird an den anrufenden Router gesendet

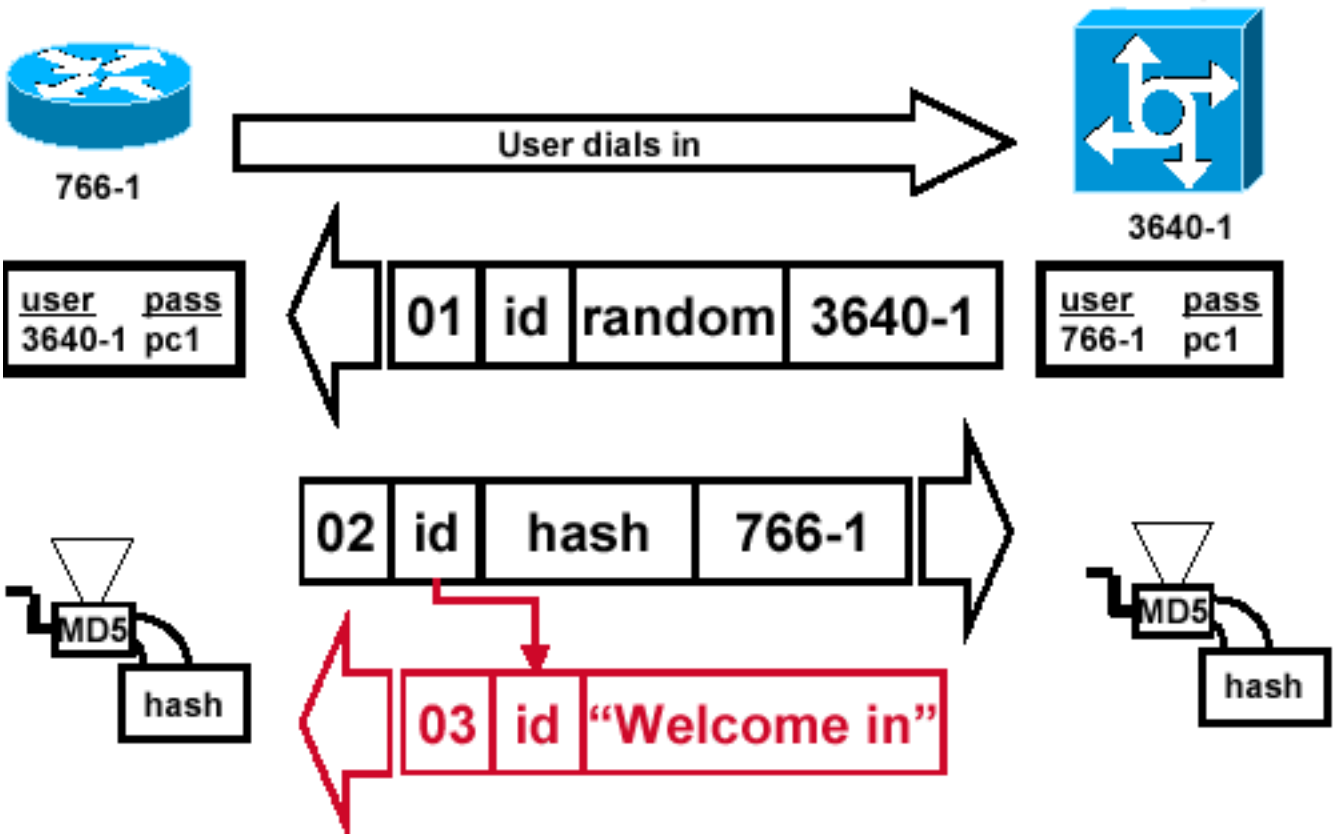


Abbildung 7 zeigt die Erfolgsmeldung, die an den anrufenden Router gesendet wurde. Es umfasst folgende Schritte:

1. Wenn die Authentifizierung erfolgreich ist, wird ein CHAP-Erfolgspaket aus folgenden Komponenten erstellt:03 = CHAP-Erfolgsmeldungstyp.ID = aus dem Antwortpaket kopiert.â Welcome inâ ist einfach eine Textnachricht, die eine anwenderlesbare Erklärung liefert.
2. Wenn die Authentifizierung fehlschlägt, wird ein CHAP-Fehlerpaket aus den folgenden Komponenten erstellt:04 = CHAP-Fehlermeldungstyp.ID = aus dem Antwortpaket kopiert.â Authentication Failureâ oder andere Textnachrichten, die eine vom Benutzer lesbare Erklärung liefern.
3. Das Erfolgs- oder Fehlerpaket wird dann an den anrufenden Router gesendet.**Hinweis:** Dieses Beispiel zeigt eine unidirektionale Authentifizierung. Bei einer Zwei-Wege-Authentifizierung wird dieser gesamte Prozess wiederholt. Der anrufende Router initiiert jedoch die erste Herausforderung.

Fehlerbehebung CHAP

Informationen zur Fehlerbehebung finden Sie unter Fehlerbehebung bei der PPP-Authentifizierung.

Zugehörige Informationen

- Debugging-PPP-Aushandlung
- Fehlerbehebung: PPP-Authentifizierung
- PPP-Authentifizierung mit dem PPP-chap-Hostnamen und den ppp-Authentifizierungschap-Callin-Befehlen

- Support-Seiten für Technologien aufrufen
- Technischer Support - Cisco Systems