Configurazione e comprensione dell'autenticazione CHAP PPP

Sommario

Introduzione

In questo documento viene descritto come il protocollo CHAP (Challenge Handshake Authentication Protocol) verifica l'identità di un peer tramite un handshake a tre vie.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come abilitare il protocollo PPP sull'interfaccia tramite encapsulation ppp
- OSPF (Open Shortest Path First) **debug ppp negotiation** output del comando. per ulteriori informazioni, fare riferimento a [Descrizione dell'output della negoziazione PPP di debug](#).
- Come risolvere i problemi quando la fase LCP (Link Control Protocol) non è aperta. Questo perché la fase di autenticazione PPP non inizia prima che la fase LCP sia completa e in stato aperto. Se il debug ppp negotiationnon indica che LCP è aperto. È necessario risolvere il problema prima di procedere.

Nota: questo documento non illustra il protocollo MS-CHAP (versione 1 o versione 2).

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Il protocollo CHAP (Challenge Handshake Authentication Protocol) (definito in RFC 1994) verifica l'identità del peer mediante un handshake a tre vie. Di seguito sono riportati i passaggi generali eseguiti nel protocollo CHAP:

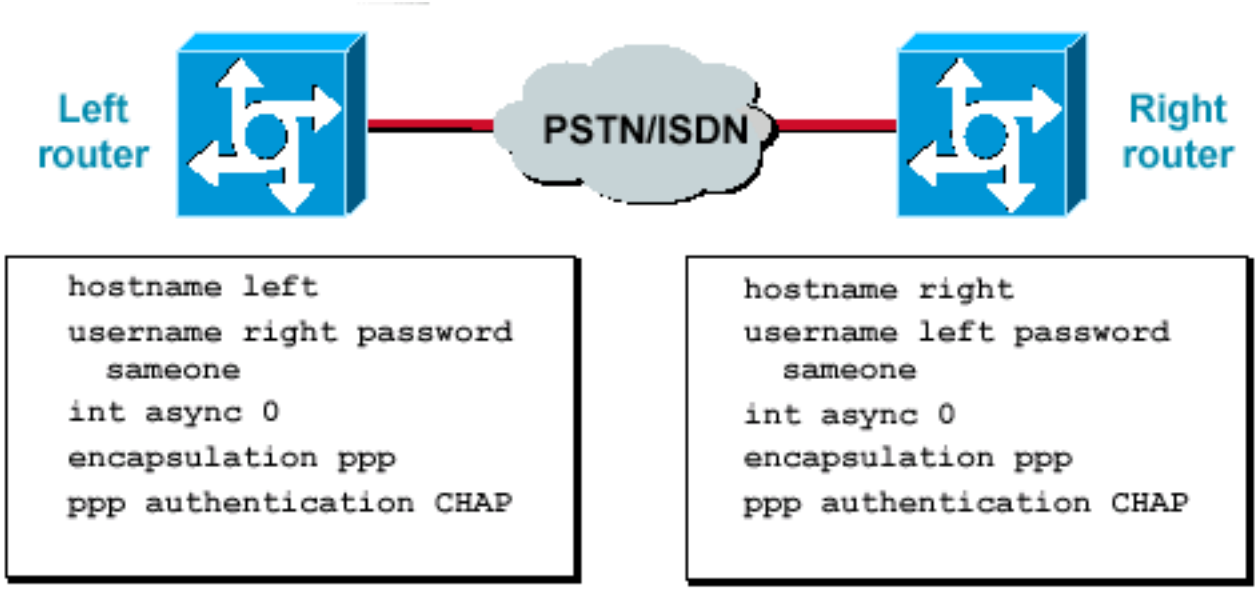
1. Al termine della fase LCP (Link Control Protocol) e dopo la negoziazione del CHAP tra i due dispositivi, il sistema di autenticazione invia un messaggio di verifica al peer.
2. Il peer risponde con un valore calcolato tramite una funzione hash unidirezionale (Message Digest 5 (MD5)).
3. Il sistema di autenticazione verifica la risposta rispetto al proprio calcolo del valore hash previsto. Se i valori corrispondono, l'autenticazione avviene correttamente. In caso contrario, la connessione viene interrotta.

Questo metodo di autenticazione dipende da un "segreto" noto solo al sistema di autenticazione e al peer. Il segreto non viene inviato tramite il collegamento. Sebbene l'autenticazione sia unidirezionale, è possibile negoziare il protocollo CHAP in entrambe le direzioni, con l'aiuto dello stesso segreto impostato per l'autenticazione reciproca.

Per ulteriori informazioni sui vantaggi e gli svantaggi del protocollo CHAP, consultare RFC 1994.

Configurazione CHAP

La procedura per configurare il protocollo CHAP è piuttosto semplice. Si supponga di avere due router, sinistro e destro, connessi attraverso una rete, come mostrato nella Figura 1.



Due router collegati in rete

Figura 1 - Due router collegati in rete

Per configurare l'autenticazione CHAP, attenersi alla seguente procedura:

1. Nell'interfaccia, utilizzare il comando encapsulation ppp.
2. Abilitare l'utilizzo dell'autenticazione CHAP su entrambi i router con **ppp authentication chap**
3. Configurare i nomi utente e le password A tale scopo, utilizzare il comando **username username password password**, dove nomeutente è il nome host del peer. Accertarsi che:Le password siano identiche su entrambi i lati.Il nome e la password del router siano gli stessi, ricordando che si applica la distinzione tra maiuscole e minuscole.

   Nota: per impostazione predefinita, il router utilizza il nome host per identificarsi con il peer. Tuttavia, questo nome utente CHAP può essere modificato tramite ppp chap hostname Per ulteriori informazioni, fare riferimento a Autenticazione PPP con il nome host ppp chap e i comandi di chiamata chap di autenticazione ppp.

Autenticazione unidirezionale e bidirezionale

Il protocollo CHAP è definito come metodo di autenticazione unidirezionale. Tuttavia, si utilizza in entrambe le direzioni per creare un'autenticazione a due vie. Quindi, con il protocollo CHAP a due vie, da ogni lato viene avviato un handshake a tre vie separato.

Nell'implementazione Cisco CHAP, per impostazione predefinita, la parte chiamata deve autenticare la parte chiamante (a meno che l'autenticazione non sia completamente disattivata). Pertanto, l'autenticazione unidirezionale avviata dalla parte chiamata è l'autenticazione minima possibile. Tuttavia, la parte chiamante può anche verificare l'identità della parte chiamata e ciò comporta un'autenticazione a due vie.

Quando ci si connette a dispositivi non Cisco, spesso è necessaria l'autenticazione unidirezionale.

Per l'autenticazione unidirezionale, configurare **ppp authentication chap callin**sul router chiamante.

La Tabella 1 mostra quando configurare l'opzione callin.

Tabella 1: quando configurare l'opzione di chiamata

Tipo di autenticazione	Client (chiamata)	NAS (chiamato)
Una via (unidirezionale)	**ppp authentication chap callin**	**ppp authentication chap**
Due vie (bidirezionale)	**ppp authentication chap**	**ppp authentication chap**

Per ulteriori informazioni, fare riferimento a Autenticazione PPP con il nome host ppp chap e i comandi di chiamata chap di autenticazione ppp.

Comandi e opzioni di configurazione CHAP

Nella Tabella 2 sono elencati i comandi e le opzioni CHAP:

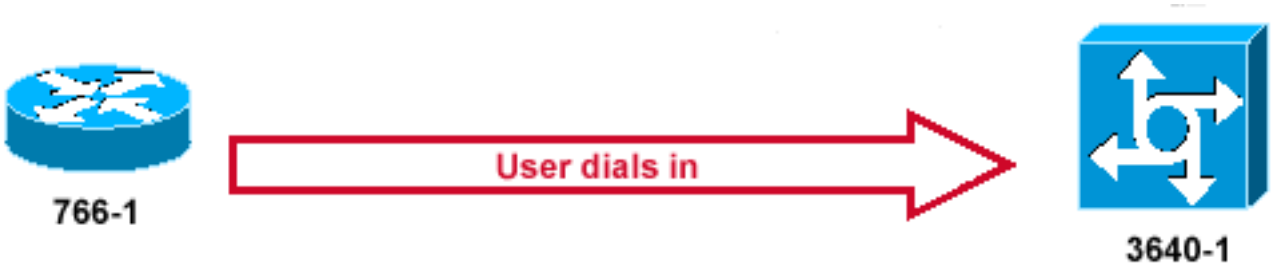
Tabella 2: comandi e opzioni CHAP

Comando	Descrizione
ppp authentication {chap | ms-chap | ms-chap-v2 | eap |pap} [callin]	Questo comando consente l'autenticazione locale del peer PPP remoto con il protocollo specificato.
nomeutente nomehost chap ppp	Questo comando definisce un nome host CHAP specifico per l'interfaccia. Per ulteriori informazioni, fare riferimento a Autenticazione PPP con il nome host ppp chap e i comandi di chiamata chap di autenticazione ppp.
password chap ppp	Questo comando definisce una password CHAP specifica dell'interfaccia.
ppp directioncallin | callout | dedicated	Questo comando forza una direzione di chiamata. Utilizzare questo comando quando nel router non è chiaro se la chiamata è in entrata o in uscita (per esempio, in caso di connessione back-to-back o di connessione tramite linee dedicate e se la Channel Service Unit o Data Service Unit (CSU/DSU) o il Terminal Adapter (TA) ISDN sono configurati per chiamare).
ppp chap refuse [callin]	Questo comando disabilita l'autenticazione remota da parte di un peer (abilitato per impostazione predefinita). Con questo comando, l'autenticazione CHAP è disabilitata per tutte le chiamate, il che significa che tutti i tentativi da parte del peer di forzare l'utente ad eseguire l'autenticazione con l'aiuto del protocollo CHAP vengono rifiutati. L'opzione callin specifica che il router si rifiuta di rispondere alle richieste di autenticazione CHAP ricevute dal peer, ma richiede comunque che il peer risponda a tutte le richieste CHAP inviate dal router.
ppp chap wait	Questo comando specifica che il chiamante deve prima autenticarsi (abilitato per impostazione predefinita). Questo comando specifica che il router non esegue l'autenticazione a un peer che richiede l'autenticazione CHAP fino a quando il peer non si è autenticato sul router.
ppp max-bad-auth value	Questo comando consente di specificare il numero consentito di tentativi di autenticazione (il valore predefinito è 0). Questo comando configura un'interfaccia point-to-point affinché non si resetti immediatamente dopo un errore di autenticazione, ma consenta un numero specificato di tentativi di autenticazione.
ppp chap splitnames	Questo comando nascosto consente nomi host diversi per una richiesta e una risposta CHAP (il valore predefinito è disabilitato).
ppp chap ignoreus	Questo comando nascosto ignora le richieste CHAP con il nome locale (il valore predefinito è abilitato).

Esempio di transazione

Gli schemi riportati in questa sezione illustrano gli eventi che si verificano durante un'autenticazione CHAP tra due router. Questi non rappresentano i messaggi effettivi visualizzati nel debug ppp negotiationoutput del comando. Per ulteriori informazioni, vedere Informazioni sull'output della negoziazione PPP di debug.

Chiamate



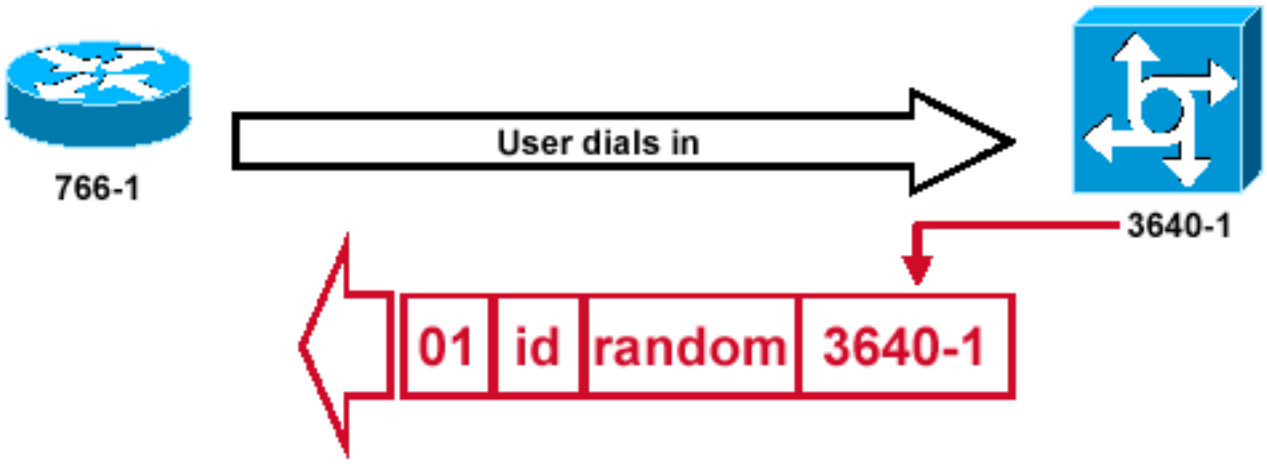
Arriva La Chiamata

Figura 2 - Arriva la chiamata

La figura 2 mostra i seguenti passaggi:

1. La chiamata arriva al numero 3640-1. L'interfaccia in ingresso è configurata con ppp authentication chap
2. LCP negozia CHAP e MD5. Per ulteriori informazioni su come determinare questa condizione, vedere Informazioni sull'output della negoziazione PPP di debug.
3. In questa chiamata è necessaria una richiesta CHAP da 3640-1 al router chiamante.

Richiesta



Il pacchetto di richiesta di verifica CHAP è stato creato

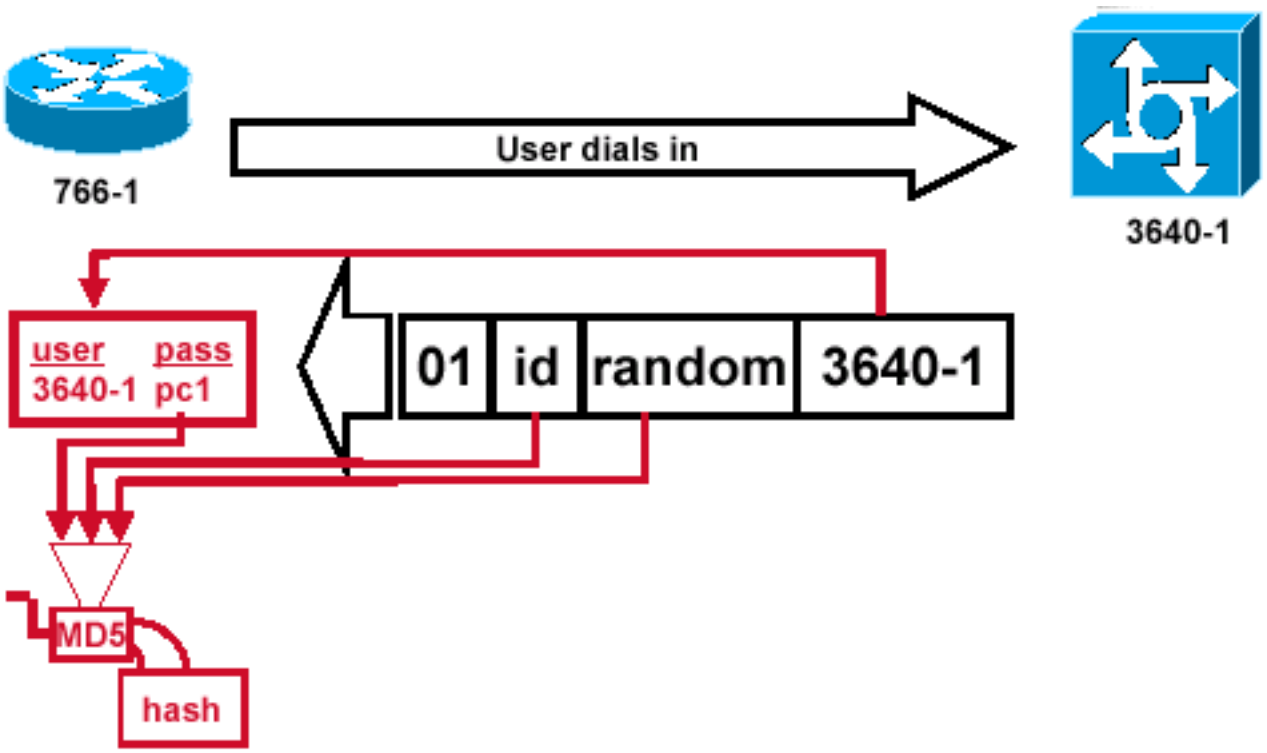
Figura 3 - Creazione di un pacchetto CHAP Challenge

Nella figura 3 vengono illustrati i seguenti passaggi dell'autenticazione CHAP tra i due router:

1. Viene creato un pacchetto richiesta CHAP con le seguenti caratteristiche:01 = identificativo del tipo di pacchetto richiesta.ID = numero progressivo che identifica la richiesta.random =

numero casuale generato dal router.3640-1 = nome di autenticazione del richiedente.
2. L'ID e i valori casuali vengono mantenuti sul router chiamato.
3. Il pacchetto di richiesta inviato al router chiamante. Viene mantenuto un elenco delle richieste ancora in sospeso.

Risposta



Ricezione ed elaborazione MD5 del pacchetto di verifica dal peer

Figura 4 — Ricezione ed elaborazione MD5 del pacchetto di verifica dal peer

La Figura 4 illustra il modo in cui il peer riceve ed elabora il pacchetto di richiesta (MD5). Il router elabora il pacchetto di richiesta CHAP in arrivo nel modo seguente:

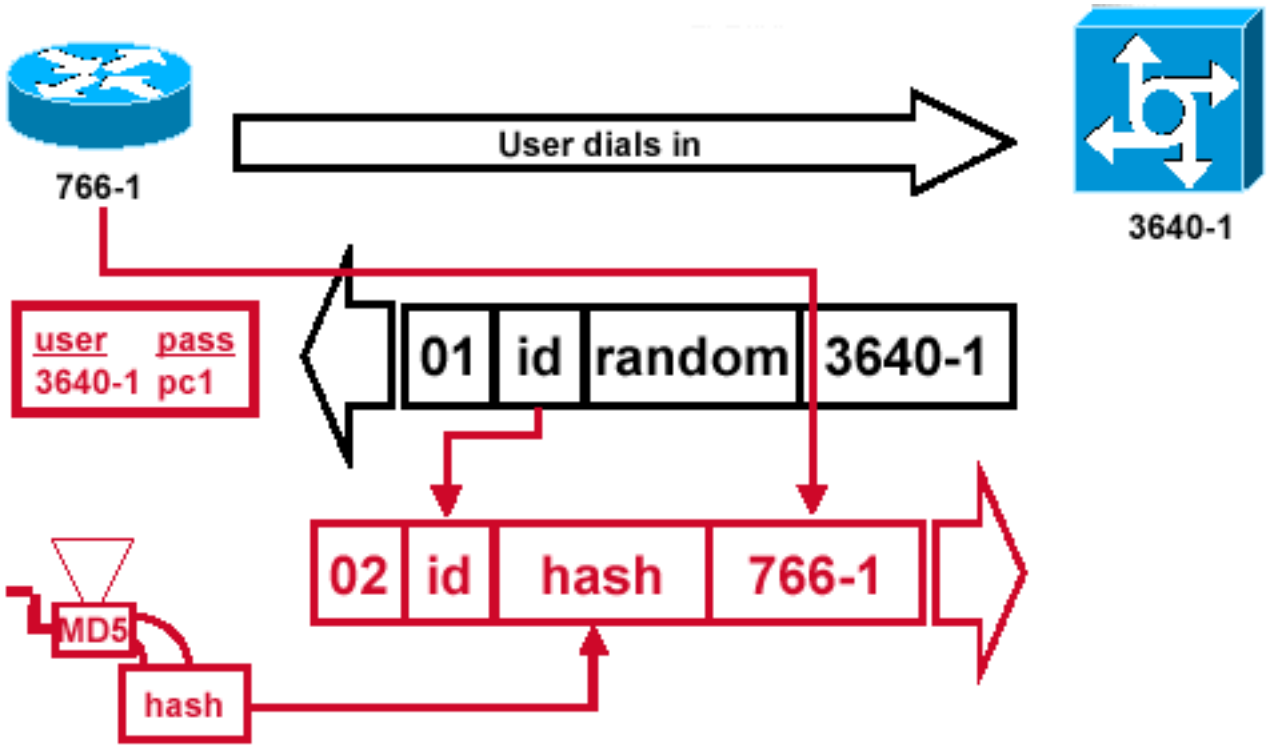
1. Il valore ID viene immesso nel generatore di hash MD5.
2. Il valore casuale viene immesso nel generatore di hash MD5.
3. Il nome 3640-1 viene utilizzato per cercare la password. Il router cerca una voce corrispondente al nome utente della richiesta. In questo esempio, cerca:

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

4. La password viene inserita nel generatore di hash MD5.

Il risultato è la richiesta CHAP con hash MD5 unidirezionale che viene inviata nella risposta CHAP.

Risposta (continua)



Il pacchetto di risposta CHAP inviato all'autenticatore è compilato

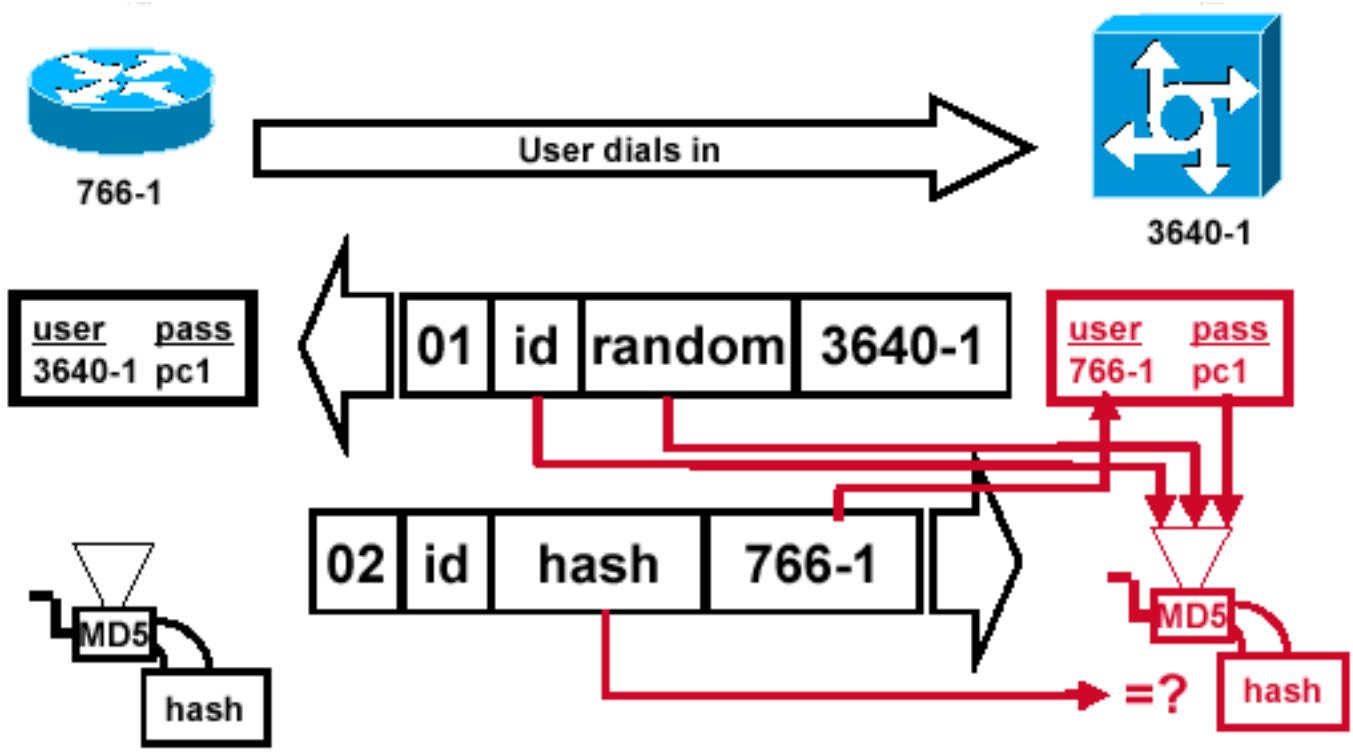
Figura 5 - Viene creato il pacchetto di risposta CHAP inviato all'autenticatore

La Figura 5 illustra la modalità di creazione del pacchetto di risposta CHAP inviato al sistema di autenticazione. Questo schema mostra i seguenti passaggi:

1. Il pacchetto di risposta è costituito da questi componenti:02 = identificatore del tipo di pacchetto di risposta CHAP.ID = copiato dal pacchetto di richiesta.hash = output del generatore di hash MD5 (le informazioni hash del pacchetto di richiesta).766-1 = nome di autenticazione del dispositivo. Tutto questo serve al peer per cercare il nome utente e la password necessari per verificare l'identità (questo punto è spiegato in dettaglio nella sezione Verifica CHAP).
2. Il pacchetto di risposta viene quindi inviato al richiedente.

Verifica CHAP

Questa sezione indica come verificare la configurazione.



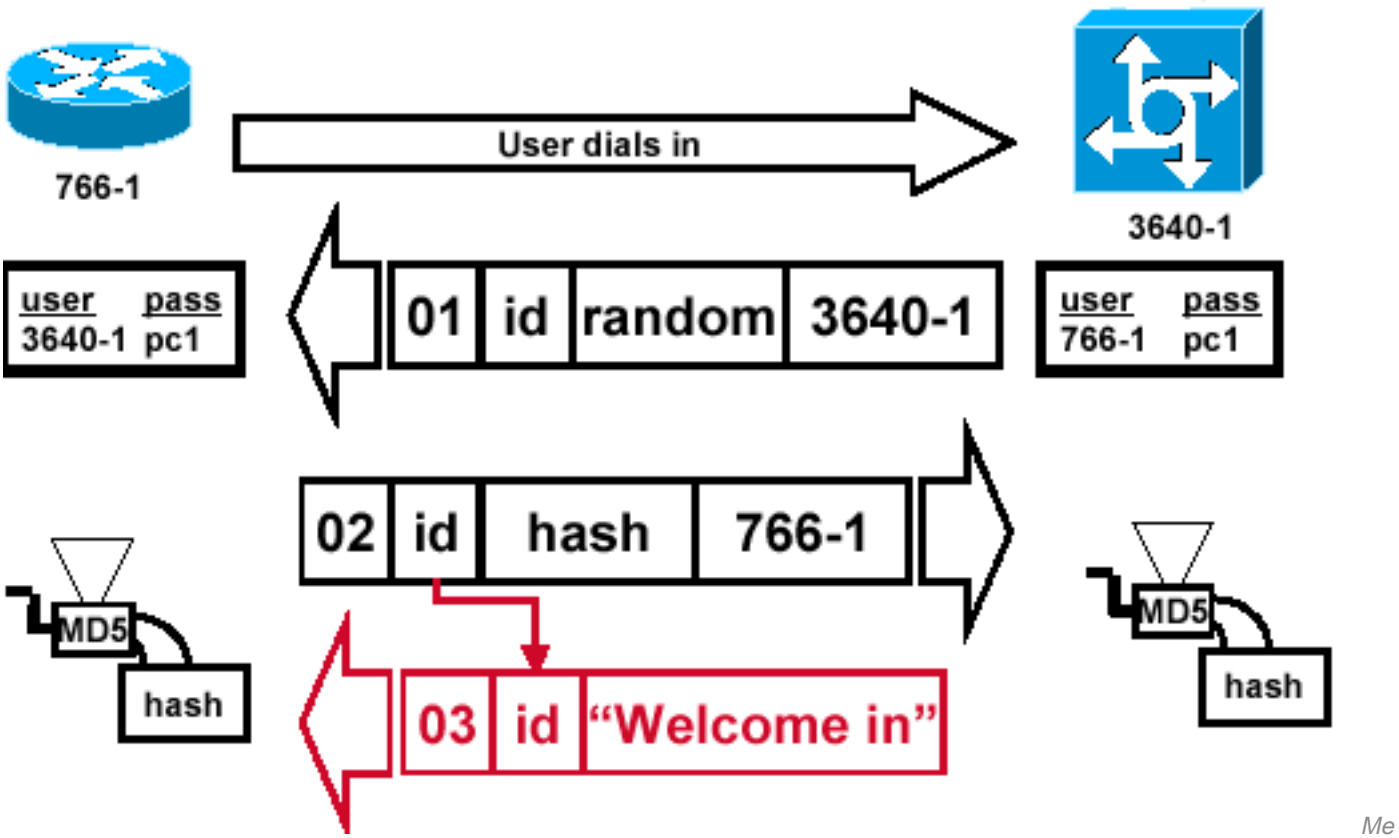
Challenger elabora il pacchetto di risposta

Figura 6 - Il Challenger elabora il pacchetto di risposta

La Figura 6 mostra il modo in cui il richiedente elabora il pacchetto risposta. Passaggi necessari per l'elaborazione del pacchetto risposta CHAP (sul sistema di autenticazione):

1. L'ID viene utilizzato per trovare il pacchetto di richiesta originale.
2. L'ID viene immesso nel generatore di hash MD5.
3. Il valore casuale della richiesta originale viene immesso nel generatore di hash MD5.
4. Il nome 766-1 viene utilizzato per cercare la password da una di queste origini:Database locale con nome utente e password.Server RADIUS o TACACS+.
5. La password viene immessa nel generatore di hash MD5.
6. Il valore hash ricevuto nel pacchetto di risposta viene quindi confrontato con il valore hash MD5 calcolato. L'autenticazione CHAP ha esito positivo se i valori hash calcolati e ricevuti sono uguali.

Risultato



Me ssaggio di operazione riuscita inviato al router chiamante

Figura 7 - Messaggio di operazione riuscita inviato al router chiamante

La Figura 7 illustra il messaggio di operazione riuscita inviato al router chiamante. Questa operazione prevede le seguenti fasi:

1. Se l'autenticazione avviene correttamente, viene creato un pacchetto di operazione riuscita CHAP usando questi componenti:03 = tipo di messaggio CHAP completato.ID = copiato dal pacchetto di risposta."Benvenuto in" è semplicemente un messaggio di testo che fornisce una spiegazione leggibile dall'utente.
2. Se l'autenticazione non avviene, viene creato un pacchetto di errore CHAP usando questi componenti:04 = tipo di messaggio di errore CHAP.ID = copiato dal pacchetto di risposta."Errore di autenticazione" o altro messaggio di testo che fornisce una spiegazione leggibile dall'utente.
3. Il pacchetto operazione riuscita o non riuscita viene quindi inviato al router chiamante.

Nota: in questo esempio viene illustrata un'autenticazione unidirezionale. In un'autenticazione a due vie, l'intero processo viene ripetuto. Tuttavia, il router chiamante avvia la richiesta iniziale.

Risoluzione dei problemi CHAP

Per informazioni su come risolvere eventuali problemi, fare riferimento a Risoluzione dei problemi di autenticazione PPP (CHAP o PAP).

Informazioni correlate

- Informazioni sull'output della negoziazione PPP di debug
- Autenticazione PPP con i comandi nome host e chiamata chap di autenticazione ppp
- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).