Autenticazione PPP utilizzando i comandi ppp chap hostname e ppp authentication chap callin

Sommario

Introduzione

La negoziazione PPP comporta diversi passaggi, ad esempio la negoziazione LCP (Link Control Protocol), l'autenticazione e la negoziazione NCP (Network Control Protocol). Se i due lati non concordano sui parametri corretti, la connessione viene interrotta. Una volta stabilito il collegamento, le due parti si autenticano a vicenda utilizzando il protocollo di autenticazione deciso durante la negoziazione LCP. L'autenticazione deve avere esito positivo prima di avviare la negoziazione NCP.

PPP supporta due protocolli di autenticazione: Protocollo PAP (Password Authentication Protocol) e CHAP (Challenge Handshake Authentication Protocol).

Prerequisiti

Convenzioni

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

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Software Cisco IOS® versione 11.2 o successive

Nozioni di base

L'autenticazione PAP comporta un handshake a due vie in cui il nome utente e la password vengono inviati attraverso il collegamento in formato non crittografato; di conseguenza, l'autenticazione PAP non fornisce alcuna protezione contro la riproduzione e l'analisi della linea.

L'autenticazione CHAP, invece, verifica periodicamente l'identità del nodo remoto utilizzando un handshake a tre vie. Una volta stabilito il collegamento PPP, l'host invia un messaggio di richiesta di verifica al nodo remoto. Il nodo remoto risponde con un valore calcolato utilizzando una funzione hash unidirezionale. L'host confronta la risposta con il proprio calcolo del valore hash previsto. Se i valori corrispondono, l'autenticazione viene riconosciuta; in caso contrario, la connessione viene interrotta.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi di IOS

Configurazione dell'autenticazione CHAP unidirezionale

Quando due dispositivi utilizzano normalmente l'autenticazione CHAP, ciascun dispositivo invia una richiesta di verifica alla quale l'altro dispositivo risponde e viene autenticato dallo sfidante. Ciascun lato autentica l'altro in modo indipendente. Se si desidera utilizzare router non Cisco che non supportano l'autenticazione del router o del dispositivo chiamante, è necessario utilizzare il comando **ppp authentication chap callin**. Se si utilizza il comando **ppp authentication** con la parola chiave **callin**, il server di accesso autenticherà la periferica remota solo se quest'ultima ha iniziato la chiamata (ad esempio, se la periferica remota ha effettuato la chiamata). In questo caso, l'autenticazione viene specificata solo per le chiamate in ingresso (ricevute).

Configurazione di un nome utente diverso dal nome del router

Quando un router Cisco remoto si connette a un router centrale Cisco o non Cisco di un diverso controllo amministrativo, a un provider di servizi Internet (ISP) o a una rotazione di router centrali, è necessario configurare un nome utente di autenticazione diverso dal nome host. In questa situazione, il nome host del router non viene fornito o è diverso in momenti diversi (a rotazione). Inoltre, il nome utente e la password allocati dall'ISP potrebbero non corrispondere al nome host del router remoto. In questa situazione, il comando **ppp chap hostname** viene usato per specificare un nome utente alternativo da usare per l'autenticazione.

Si consideri ad esempio una situazione in cui più dispositivi remoti stanno effettuando la connessione a un sito centrale. Utilizzando la normale autenticazione CHAP, è necessario configurare sul router centrale il nome utente (ovvero il nome host) di ciascun dispositivo remoto e un segreto condiviso. In questo scenario, la configurazione del router centrale può diventare lunga e complessa da gestire; tuttavia, se i dispositivi remoti utilizzano un nome utente diverso dal nome host, è possibile evitare questa condizione. Il sito centrale può essere configurato con un singolo nome utente e un segreto condiviso che possono essere utilizzati per autenticare più client di connessione.

Esempio di rete

Se il router 1 inizia una chiamata al router 2, il router 2 contesta il router 1, ma il router 1 non contesta il router 2. Questo si verifica perché il comando **ppp authentication chap callin** è configurato sul router 1. Questo è un esempio di autenticazione unidirezionale.

In questa configurazione, il comando **ppp chap hostname alias-r1** è configurato sul router 1. Il router 1 utilizza "alias-r1" come nome host per l'autenticazione CHAP anziché "r1". Il nome della mappa del dialer del router 2 deve corrispondere al nome host del protocollo ppp del router 1; in caso contrario, vengono stabiliti due canali B, uno per ciascuna direzione.

Configurazioni

Router 1

```
!
 isdn switch-type basic-5ess
 !
 hostname r1
 !
 username r2 password 0 cisco
 ! -- Hostname of other router and shared secret !
interface BRI0/0 ip address 20.1.1.1 255.255.255.0 no ip
directed-broadcast encapsulation ppp dialer map ip
20.1.1.2 name r2 broadcast 5772222
  dialer-group 1
  isdn switch-type basic-5ess
  ppp authentication chap callin
 ! -- Authentication on incoming calls only  ppp chap
hostname alias-r1
 ! -- Alternate CHAP hostname ! access-list 101 permit
ip any any dialer-list 1 protocol ip list 101 !
```

Router 2

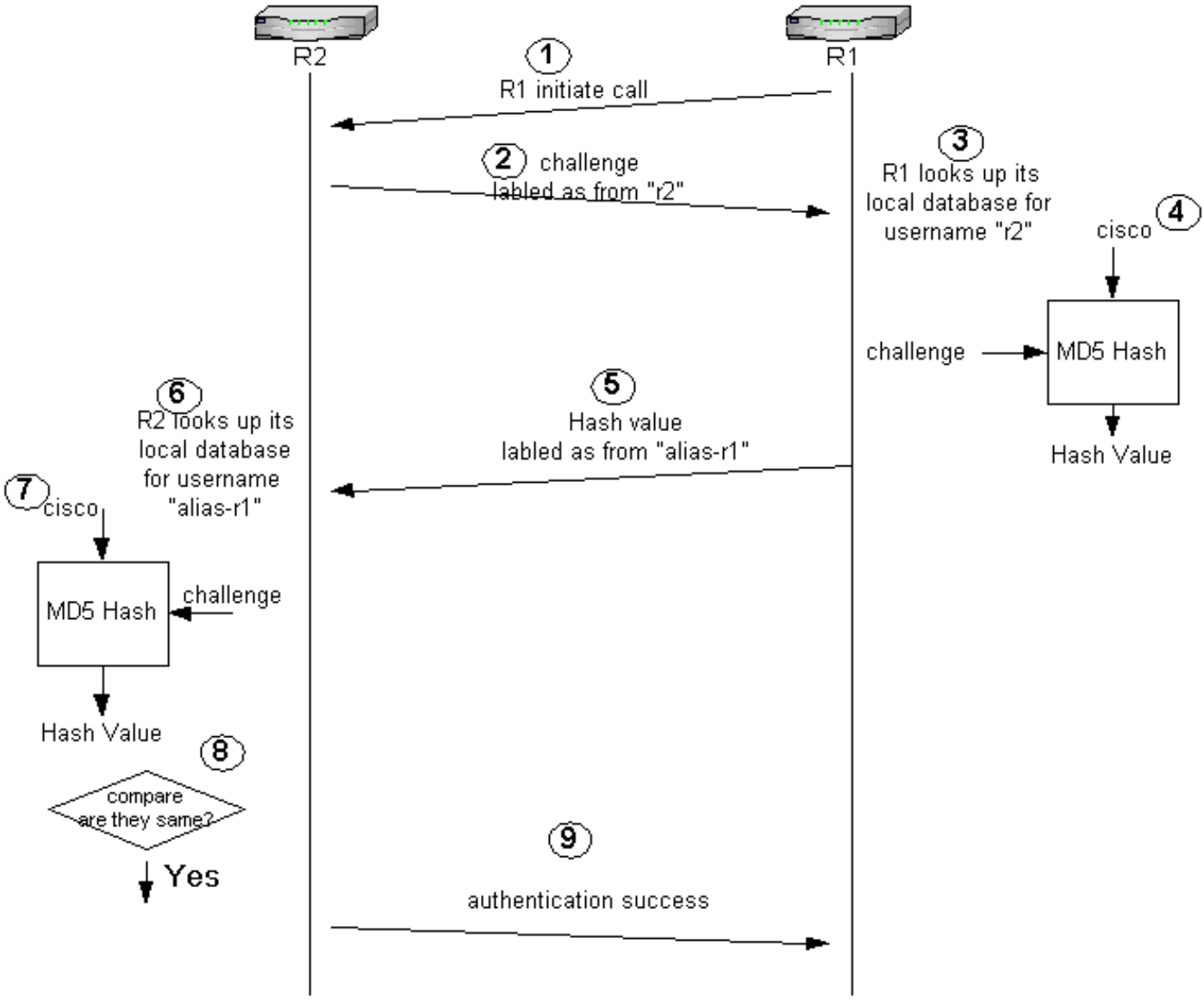
```
!
 isdn switch-type basic-5ess
 !
 hostname r2
```

```
 !
 username alias-r1 password 0 cisco
 ! -- Alternate CHAP hostname and shared secret. ! --
The username must match the one in the ppp chap hostname
! -- command on the remote router.

 !
 interface BRI0/0
  ip address 20.1.1.2 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  dialer map ip 20.1.1.1 name
  alias-r1 broadcast 5771111
  ! -- Dialer map name matches alternate hostname
"alias-r1". dialer-group 1 isdn switch-type basic-5ess
ppp authentication chap ! access-list 101 permit ip any
any dialer-list 1 protocol ip list 101 !
```

Spiegazione della configurazione

Per ulteriori informazioni, fare riferimento ai numeri riportati di seguito:



1. Nell'esempio, il router 1 avvia la chiamata. Poiché il router 1 è configurato con il comando **ppp authentication chap callin**, non contesta la parte chiamante, ossia il router 2.

2. Quando il router 2 riceve la chiamata, contesta l'autenticazione al router 1. Per impostazione predefinita, il nome host del router viene utilizzato per identificarsi. Se il comando **ppp chap hostname** *name* è stato configurato, un router utilizza il nome al posto del nome host per identificarsi. In questo esempio, la sfida viene etichettata come proveniente da "r2".
3. Il router 1 riceve la richiesta di verifica del router 2 e cerca il nome utente "r2" nel database locale.
4. Il router 1 trova la password "r2", ossia "cisco". Il router 1 utilizza questa password e la richiesta di verifica del router 2 come parametri di input della funzione hash MD5. Viene generato il valore hash.
5. Il router 1 invia il valore di output dell'hash al router 2. In questo caso, poiché il comando **ppp chap hostname** è configurato come "alias-r1", la risposta viene etichettata come proveniente da "alias-r1".
6. Il router 2 riceve la risposta e cerca la password nel nome utente "alias-r1" nel database locale.
7. Il router 2 rileva che la password per "alias-r1" è "cisco". Il router 2 utilizza la password e la richiesta di verifica inviata in precedenza al router 1 come parametri di input per la funzione hash MD5. La funzione hash genera un valore hash.
8. Il router 2 confronta il valore hash generato e quello ricevuto dal router 1.
9. Poiché i parametri di input (verifica e password) sono identici, il valore hash è lo stesso e l'autenticazione ha esito positivo.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Prima di usare i comandi di debug, consultare le informazioni importanti sui comandi di debug

Output di esempio del comando debug

Di seguito viene riportato un output di esempio del comando **debug ppp authentication**:

Router 1

```
r1#ping 20.1.1.2

 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 20.1.1.2, timeout is 2 seconds:

  *Mar 1 20:06:27.179: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
  *Mar 1 20:06:27.183: %ISDN-6-CONNECT:
  Interface BRI0/0:1 is now connected to 5772222
  *Mar 1 20:06:27.187: BR0/0:1 PPP: Treating connection as a callout
  *Mar 1 20:06:27.223: BR0/0:1 CHAP: I CHALLENGE id 57 len 23 from "r2"
```

```
   ! -- Received a CHAP challenge from other router (r2) *Mar 1 20:06:27.223: BR0/0:1 CHAP:
Using alternate hostname alias-r1
  ! -- Using alternate hostname configured with ! -- ppp chap hostname command *Mar 1
20:06:27.223: BR0/0:1 CHAP: O RESPONSE id 57 Len 29 from "alias-r1" ! -- Sending response from
"alias-r1" ! -- which is the alternate hostname for r1 *Mar 1 20:06:27.243: BR0/0:1 CHAP: I
SUCCESS id 57 Len 4 ! -- Received CHAP authentication is successful ! -- Note that r1 is not
challenging r2 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 36/38/40 ms r1#
*Mar 1 20:06:28.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to
up r1# *Mar 1 20:06:33.187: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5772222 r2
```

Router 2

```
r2#

  20:05:20: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
  20:05:20: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5771111
  20:05:20: BR0/0:1 PPP: Treating connection as a callin
  20:05:21: BR0/0:1 CHAP: O CHALLENGE id 57 Len 23 from "r2"
  ! -- r2 is sending out a challenge 20:05:21: BR0/0:1 CHAP: I RESPONSE id 57 Len 29 from
"alias-r1"
 ! -- Received a response from alias-r1, ! -- which is the alternate hostname on r1 20:05:21:
BR0/0:1 CHAP: O SUCCESS id 57 Len 4 ! -- Sending out CHAP authentication is successful 20:05:22:
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to up 20:05:26: %ISDN-6-
CONNECT: Interface BRI0/0:1 is now connected to 5771111 alias-r1
```

Informazioni correlate

- Comandi PPP per reti WAN
- Informazioni sull'autenticazione PPP e PPP
- Informazioni di debug ISDN