# ppp chap hostname および ppp authentication chap callin コマンドを使用した PPP 認証

## 内容

[概要](#)
[前提条件](#)
[表記法](#)
[要件](#)
[使用するコンポーネント](#)
[背景理論](#)
[設定](#)
[単一方向 CHAP 認証の設定](#)
[ルータ名と異なるユーザ名の設定](#)
[ネットワーク図](#)
[設定](#)
[設定に関する説明](#)
[確認](#)
[トラブルシュート](#)
[debug 出力例](#)
[関連情報](#)

## 概要

PPP ネゴシエーションには、Link Control Protocol（LCP; リンク コントロール プロトコル）ネゴシエーション、認証、および Network Control Protocol（NCP; ネットワーク コントロール プロトコル）ネゴシエーションのような複数の段階があります。両サイドが適切なパラメータで同意できない場合、接続は終了されます。リンクが確立されると、双方は LCP ネゴシエーション中に決定された認証プロトコルを使用して、相互認証を行います。認証は、NCP ネゴシエーションを開始する前に成立していなければなりません。

PPP は次の 2 つの認証プロトコルをサポートします。パスワード認証プロトコル（PAP）および Challenge Handshake 認証プロトコル（CHAP）です。

## 前提条件

### 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。

### 要件

このドキュメントに関しては個別の前提条件はありません。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS(R) ソフトウェア リリース 11.2 以降

## 背景理論

PAP 認証では、リンク上でユーザ名とパスワードをクリア テキストで送信する 2 ウェイ ハンドシェイクが行われます。そのため、プレイバックおよびライン探知に対する保護機能はありません。

一方、CHAP 認証では、スリーウェイ ハンドシェイクを使用して、定期的にリモート ノードのアイデンティティが検証されます。PPP リンクが確立されると、ホストから「チャレンジ」メッセージがリモート ノードに送信されます。リモート ノードでは、1 ウェイのハッシュ計算機能を使用して計算された値を応答します。ホストではこの応答を、自身で算出したハッシュ期待値と照らし合わせて検証します。値が一致する場合、認証は確認応答されます。一致しない場合、接続が終了します。

# 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

**注：このド**キュメントで使用されているコマンドの詳細を調べるには、IOS Command Lookupツールを使用してください

## 単一方向 CHAP 認証の設定

通常、2 つのデバイスが CHAP 認証を使用する場合、双方がチャレンジを送信し、これに対して相手側が応答して、チャレンジ送信側で認証が行われます。各側での相手側の認証は別々に行われます。シスコルータ以外で、認証をサポートできないルータまたはデバイスを発呼側にを使用する場合は、ppp authentication chap callin コマンドを使用してください。ppp authentication コマンドを callin キーワードを付けて使用すると、アクセス サーバでは、リモート デバイスがコールを発信した場合 ( たとえば、リモート デバイスが「コールイン」した場合 ) のリモート デバイスだけを認証します。 この場合、認証は着信 ( 受信 ) コールのみに指定されます。

## ルータ名と異なるユーザ名の設定

管理制御様式の異なるシスコまたはシスコ製品以外のセントラル ルータ、インターネット サービス プロバイダ ( ISP ) 、またはセントラル ルータのロータリーのいずれかに、リモートシスコルータが接続する場合、ホスト名と異なる認証ユーザ名を設定する必要があります。このような状況では、ルータのホスト名は、提供されていないか、場合によって異なる場合があります ( ロータリー ) 。 また、ISP によって割り振られたユーザ名およびパスワードが、リモート ルータのホスト名とは異なる場合もあります。このような場合には、ppp chap hostname コマンドを使用し、認証に使用する代替ユーザ名を指定します。

たとえば、複数のリモート デバイスがセントラル サイトにダイヤルインしている状況を考えてく

ださい。通常の CHAP 認証を使用する場合、各リモート デバイスの ( ホスト名となるはずの ) ユーザ名および共有の秘密事項をセントラル ルータで設定する必要があります。このシナリオでは、中央ルータの設定の管理に時間がかかり、煩雑になることがあります。ただし、リモート デバイスがホスト名と異なるユーザ名を使用すれば、これを回避することができます。複数のダイヤルイン クライアントの認証に使用できる単一のユーザ名と共有秘密で中央サイトを設定できます。

## ネットワーク図

ルータ1がルータ2へのコールを開始すると、ルータ2はルータ1にチャレンジしますが、ルータ1はルータ2にチャレンジしません。これは、ルータ1で**ppp authentication chap callinコマンドが設定されているためです。これは単方向認証の例です。**

この設定では、ppp chap hostname alias-r1 コマンドがルータ 1 に設定されています。ルータ 1 は、CHAP 認証ホスト名として "r1" の代わりに "alias-r1" を使用します。 ルータ2のダイヤラマップ名は、ルータ1のppp chap hostnameと一致している必要があります。そうしないと、2 つの B-channel が 1 方向につき 1 つずつ確立されてしまいます。


## 設定

**ルータ 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 !
```

**ルータ 2**

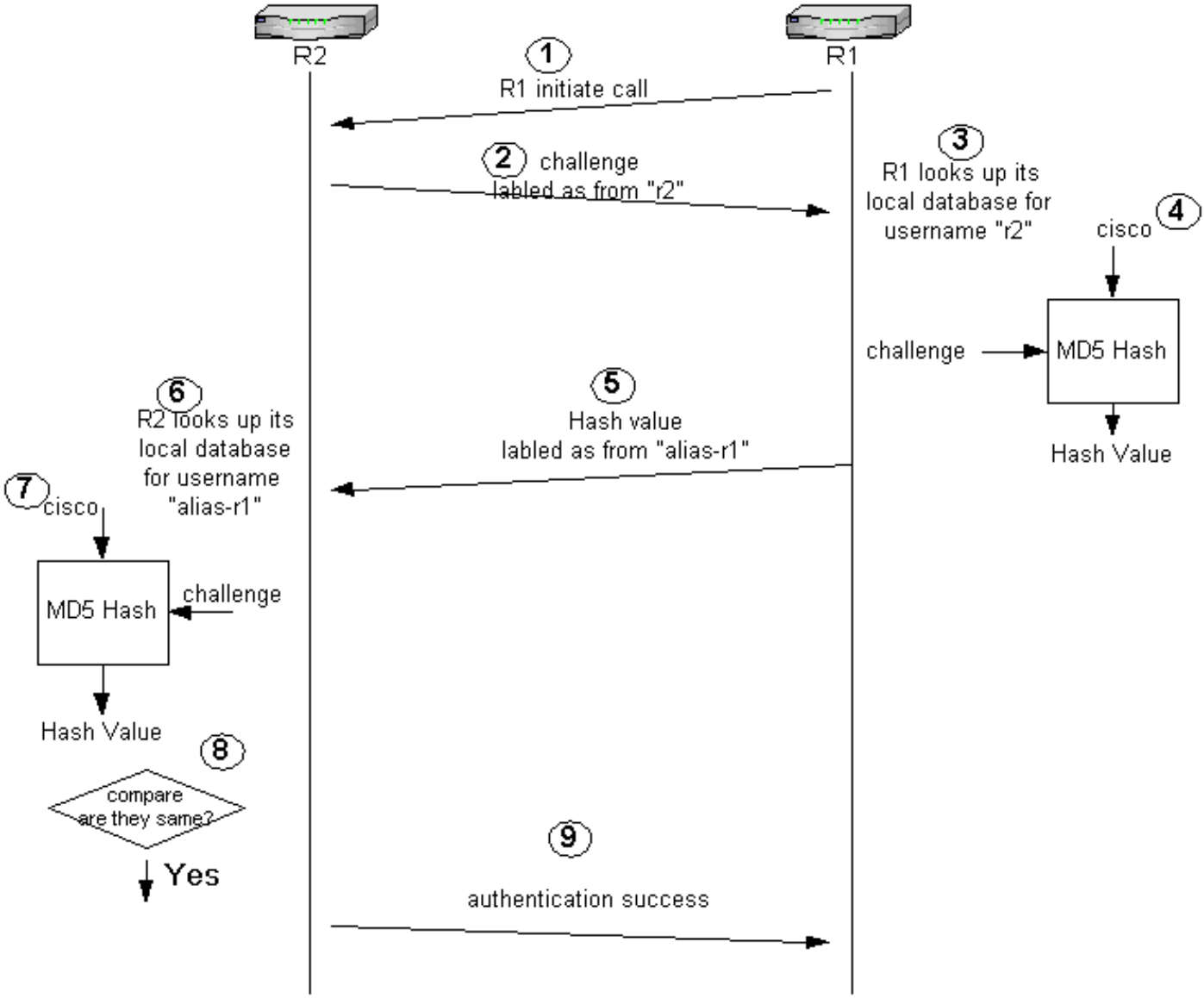
```
!
 isdn switch-type basic-5ess
 !
 hostname r2
 !
 username alias-r1 password 0 cisco
```

```
 ! -- 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 !
```

## 設定に関する説明

説明は、図の下の数字を参照してください。




1. この例では、ルータ 1 からコールを開始しています。ルータ 1 は 、ルータ 2 を発呼側としてppp authentication chap callin コマンドで設定しているため、ルータ 2 の身元証明を要求しません。
2. ルータ 2 がコールを受信すると、ルータ2は認証を行うためルータ 1の身元証明を要求しま

す。この認証において、デフォルトでは、ルータのホスト名がそのルータ自体を識別するために使用されます。ppp chap hostname name コマンドが設定されている場合、ルータはホスト名のかわりにその名前を使って、そのルータ自体を識別します。この例では、身元証明要求は "r2" から着信したものとして、ラベルが付けられます。

3. ルータ 1 はルータ 2 の身元証明要求を受けとり、ユーザ名 "r2" のローカル データベースを調べます。
4. Router 1 が「r2」のパスワードを見つけます。これは「cisco」となっています。 Router 1 では、MD5 ハッシュ関数の入力パラメータとして、このパスワードと Router 2 からのチャレンジを使用します。そのハッシュ計算値が生成されます。
5. ルータ1はハッシュ出力値をルータ2に送信します。ここで、**ppp chap hostnameコマンド**は「alias-r1」として設定されているため、「alias-r1」からの応答としてラベルが付けられます。
6. ルータ 2 は返信応答を受け取り、パスワードのローカル データベースにある "alias-r1" ユーザ名を検索します。
7. Router 2 は、「alias-r1」のパスワードが「cisco」であることを見つけます。 Router 2 では、MD5 ハッシュ関数の入力パラメータとして、このパスワードと以前に Router 1 に送信されたチャレンジを使用します。ハッシュ計算機能がハッシュ計算値を生成します。
8. ルータ 2 は、自身で生成したハッシュ計算値と、ルータ 1 から受け取ったハッシュ計算値を比較します。
9. 入力パラメータ（身元証明要求およびパスワード）が同一であれば、ハッシュ計算値も同じになるので、認証が成功します。

## 確認

現在、この設定に使用できる確認手順はありません。

## トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

debug コマンドを試行する前に、『デバッグ コマンドの重要な情報 』を参照してください。

### debug 出力例

次は、debug ppp authentication コマンドからの出力例です。

**ルータ 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
```

### ルータ 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
```

## 関連情報

- WAN 用の PPP コマンド
- PPP と PPP 認証について
- ISDN デバッグ情報