PPP Authentication Using the ppp chap hostname and ppp authentication chap callin Commands

Document ID: 10241

Contents

Introduction

PPP negotiation involves several steps such as Link Control Protocol (LCP) negotiation, Authentication, and Network Control Protocol (NCP) negotiation. If the two sides cannot agree on the correct parameters, then the connection is terminated. Once the link is established, the two sides authenticate each other using the authentication protocol decided on during LCP negotiation. Authentication must be successful prior to starting NCP negotiation.

PPP supports two authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

Prerequisites

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco IOS® Software Release 11.2 or later

Background Theory

PAP authentication involves a two−way handshake where the username and password are sent across the link in clear text; hence, PAP authentication does not provide any protection against playback and line sniffing.

CHAP authentication, on the other hand, periodically verifies the identity of the remote node using a three−way handshake. After the PPP link is established, the host sends a "challenge" message to the remote node. The remote node responds with a value calculated using a one−way hash function. The host checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise, the connection is terminated.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the IOS Command Lookup tool

Configuring Unidirectional CHAP Authentication

When two devices normally use CHAP authentication, each side sends out a challenge to which the other side responds and is authenticated by the challenger. Each sides authenticates one another independently. If you want to operate with non−Cisco routers that do not support authentication by the calling router or device, you must use the **ppp authentication chap callin** command. When using the **ppp authentication** command with the **callin** keyword, the Access Server will only authenticate the remote device if the remote device initiated the call (for example, if the remote device "called in"). In this case, authentication is specified on incoming (received) calls only.

Configuring a Username Different from the Router's Name

When a remote Cisco router connects to either a Cisco or a non−Cisco central router of a different administrative control, an Internet Service Provider (ISP), or a rotary of central routers, it is necessary to configure an authentication username that is different from the hostname. In this situation, the hostname of the router is not provided or is different at different times (rotary). Also, the username and password that is allocated by the ISP may not be the remote router's hostname. In such a situation, the **ppp chap hostname** command is used to specify an alternate username that will be used for authentication.

For example, consider a situation where multiple remote devices are dialing into a central site. Using normal CHAP authentication, the username (which would be the hostname) of each remote device and a shared secret must be configured on the central router. In this scenario, the configuration of the central router can get lengthy and cumbersome to manage; however, if the remote devices use a username that is different from their hostname this can be avoided. The central site can be configured with a single username and shared secret that can be used to authenticate multiple dialin clients.

Network Diagram

If Router 1 initiates a call to Router 2, Router 2 would challenge Router 1, but Router 1 would not challenge Router 2. This occurs because the **ppp authentication chap callin** command is configured on Router 1. This is an example of a unidirectional authentication.

In this setup, the **ppp chap hostname alias−r1** command is configured on Router 1. Router 1 uses "alias−r1" as its hostname for CHAP authentication instead of "r1." The Router 2 dialer map name should match Router

1's ppp chap hostname; otherwise, two B channels are established, one for each direction.

Router 1 — ISDN/PPP — Router 2

Configurations

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
```
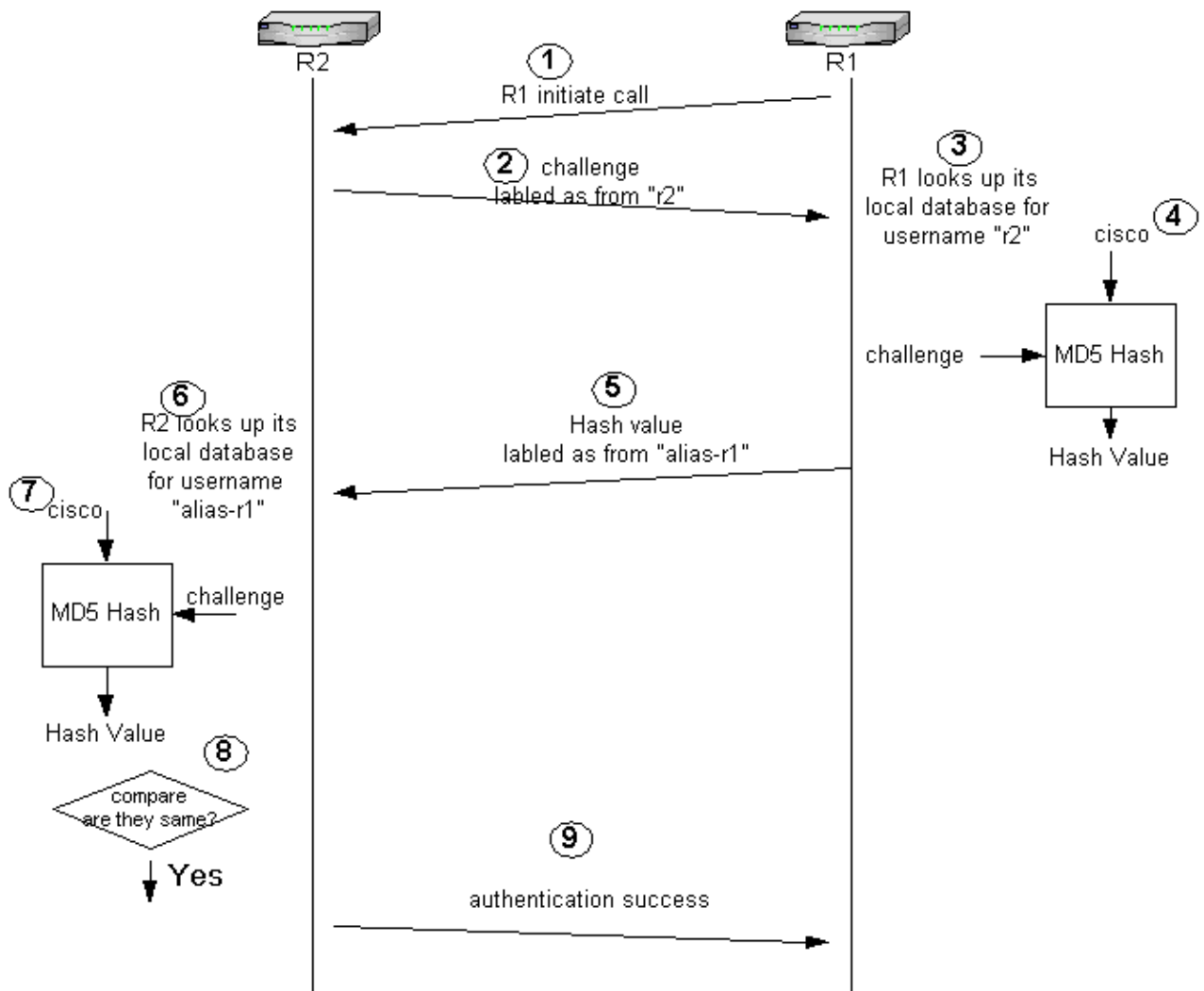
```
! -- Dialer map name matches alternate hostname "alias-r1".

 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
!
```

Configuration Explanation

Please refer to the numbers below this graphic for explanations:

1. In this example, Router 1 initiates the call. Since Router 1 is configured with the **ppp authentication chap callin** command, it does not challenge the calling party, which is Router 2.
2. When Router 2 receives the call, it challenges Router 1 for authentication. By default for this authentication, the hostname of the router is used to identify itself. If the **ppp chap hostname** *name* command is configured, a router uses the name in place of the hostname to identify itself. In this example, the challenge is labeled as it is coming from "r2."
3. Router 1 receives Router 2's challenge and looks in its local database for username "r2."
4. Router 1 finds the "r2" password, which is "cisco." Router 1 uses this password and the challenge from Router 2 as input parameters of the MD5 hash function. The hash value is generated.

5. Router 1 sends the hash output value to Router 2. Here, since the **ppp chap hostname** command is configured as "alias−r1," the reply is labeled as coming from "alias−r1."
6. Router 2 receives the reply and looks for the "alias−r1" username in its local database for the password.
7. Router 2 finds that the password for "alias−r1" is "cisco." Router 2 uses the password and the challenge sent out earlier to Router 1 as input parameters for the MD5 hash function. The hash function generates a hash value.
8. Router 2 compares the hash value it generated and the one it receives from Router 1.
9. Since the input parameters (challenge and password) are identical, the hash value is same resulting in a successful authentication.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Before attempting any of the debug commands, please see Important Information on Debug Commands

Sample Debug Output

Following is sample output from the **debug ppp authentication** command:

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
```

Related Information

- **PPP Commands for Wide-Area Networking**
- **Configuring PPP and Authentication**
- **Understanding PPP and PPP Authentication**
- **ISDN Debug Information**

Updated: Sep 09, 2005   Document ID: 10241