Table of Contents

Understanding and Configuring PPP CHAP Authentication

Introduction

The Challenge Handshake Authentication Protocol (CHAP) (defined in RFC 1994) verifies the identity of the peer using a three−way handshake. The following general steps are performed in CHAP:

1. After the link establishment phase is complete, the authenticator sends a challenge message to the peer.
2. The peer responds with a value calculated using a one−way hash function (Message Digest 5 (MD5)).
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is successful. Otherwise, the connection is terminated.

This authentication method depends on a "secret" known only to the authenticator and the peer. The secret is not sent over the link. Although the authentication is only one−way, by negotiating CHAP in both directions, you can use the same secret set for mutual authentication.

For more information on the advantages and disadvantages of CHAP, refer to RFC 1994 .

Before You Begin

Conventions

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

Prerequisites

Readers of this document should be knowledgeable of the following:

- Enable PPP on the interface using the command **encapsulation ppp**.

- You must be able to read and understand the **debug ppp negotiation** command output. Refer to Understanding debug ppp negotiation Output for more information.
- The PPP authentication phase does not begin until the Link Control Protocol (LCP) phase is complete and is in the open state. If the **debug ppp negotiation** command does not indicate that LCP is open, troubleshoot this issue before proceeding.

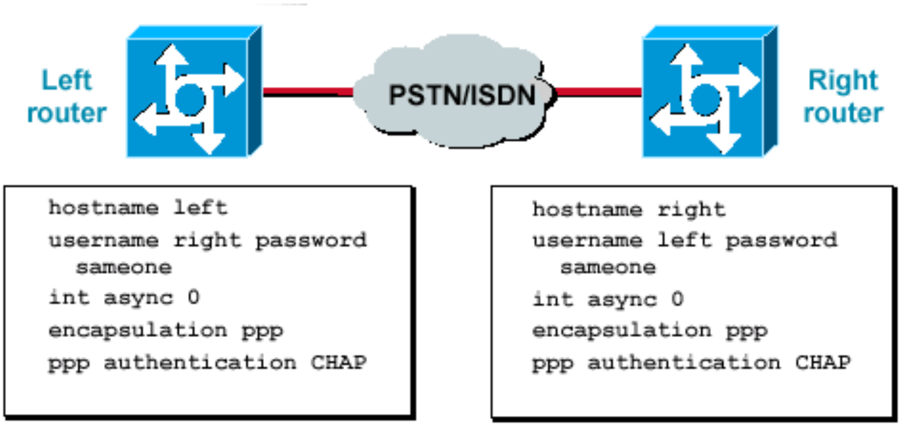
Note: This document does not address MS−CHAP (Version 1 or Version 2). For more information on MS−CHAP, refer to the documents MS−CHAP Support and MSCHAP Version 2.

Components Used

This document is not restricted to specific software and hardware versions.

Configuring CHAP

Configuring CHAP is fairly straightforward. For example, say you have two routers, left and right, connected across a network, as shown in the example below.



```
hostname left
username right password
  sameone
int async 0
encapsulation ppp
ppp authentication CHAP
```

```
hostname right
username left password
  sameone
int async 0
encapsulation ppp
ppp authentication CHAP
```

Use the following steps as a guide to configure CHAP authentication:

1. On the interface, issue the **encapsulation ppp** command.
2. Enable the use of CHAP authentication on both routers with the **ppp authentication chap** command.
3. Configure the usernames and passwords. To do so, issue the command **username *username* password *password*** , where *username* is the hostname of the peer.

   ♦ Passwords must be identical at both ends.
   ♦ The router name and password are casesensitive.

   Note: By default, the router uses its hostname to identify itself to the peer. However, this CHAP username can be changed using the command **ppp chap hostname**. Refer to PPP Authentication Using the ppp chap hostname and ppp authentication chap callin Commands for more information.

One−Way and Two−Way Authentication

CHAP is defined as a one−way authentication method. However, using CHAP in both direction creates a two−way authentication. Hence, with two−way CHAP, a separate three−way handshake is initiated by each side.

In the Cisco CHAP implementation, by default, the called party must authenticate the calling party (unless authentication is completely turned off). Therefore, a one−way authentication initiated by the called party is the minimum possible authentication. However, the calling party can also verify the identity of the called party, resulting in a two−way authentication.

One−way authentication is often required when connecting to non−Cisco devices.

For one−way authentication, configure the command **ppp authentication chap callin** on the calling router.

The following table shows when to configure the callin option:

Authentication Type	Client (calling)	NAS (called)
One−way (unidirectional)	**ppp authentication chap callin**	**ppp authentication chap**
Two−way (bidirectional)	**ppp authentication chap**	**ppp authentication chap**

For more information on implementing one−way authentication, refer to PPP Authentication Using the ppp chap hostname and ppp authentication chap callin Commands.

CHAP Configuration Commands and Options

The following table lists the CHAP commands and options:

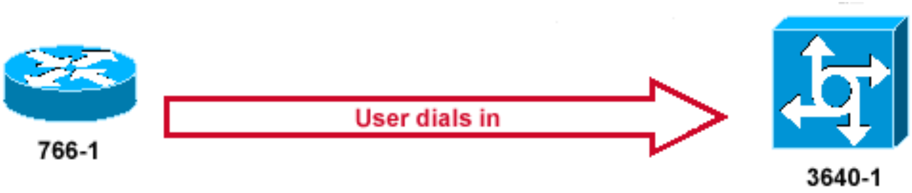
Command	Description
ppp authentication {*chap* | *ms−chap* | *pap*} [*callin* | *default*]	This command enables local authentication of the remote PPP peer with the specified protocol.
ppp chap hostname *username*	This command defines an interface−specific CHAP hostname. Refer to the document PPP Authentication Using the ppp chap hostname and ppp authentication chap callin Commands for more information.
ppp chap password *password*	This command defines an interface−specific CHAP password.
ppp direction *callin* | *callout* | *dedicated*	This command forces a call direction. The command is used when a router is confused as to whether the call is incoming or outgoing (for example, when connected back−to−back or connected by leased lines and the Channel Service Unit or Data Service Unit (CSU/DSU) or

	ISDN Terminal Adapter (TA) are configured to dial).
ppp chap refuse [*callin*]	This command disables remote authentication by a peer (default enabled). With this command, CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP are refused. The callin option specifies that the router refuses to answer CHAP authentication challenges received from the peer, but still requires the peer to answer any CHAP challenges the router sends.
ppp chap wait	This command specifies that the caller must authenticate first (default enabled). This command specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.
ppp max−bad−auth *value*	This command specifies the allowed number of authentication retries (the default value is 0). This command configures a point−to−point interface not to reset itself immediately after an authentication failure, but instead to allow a specified number of authentication retries.
ppp chap splitnames	This hidden command allows different hostnames for a CHAP challenge and response (the default value is disabled).
ppp chap ignoreus	This hidden command ignores CHAP challenges with the local name (the default value is enabled).

Transactional Example

The following diagrams show the series of events that occur during a CHAP authentication between two routers. These do not represent the actual messages seen in the **debug ppp negotiation** command output. For more information, refer to Understanding debug ppp negotiation Output.

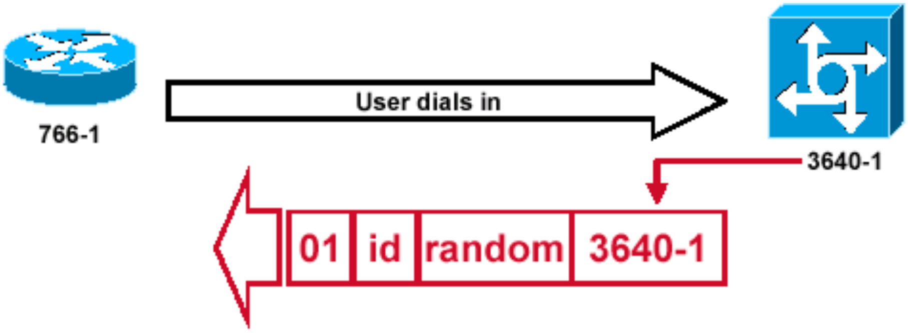
Call



The following steps are shown in this diagram:

1. The call comes in to 3640−1. The incoming interface is configured with the **ppp authentication chap** command.
2. LCP negotiates CHAP and MD5. For more information on determining this, refer to Understanding the debug ppp negotiation Output.
3. A CHAP challenge from 3640−1 to the calling router is required on this call.

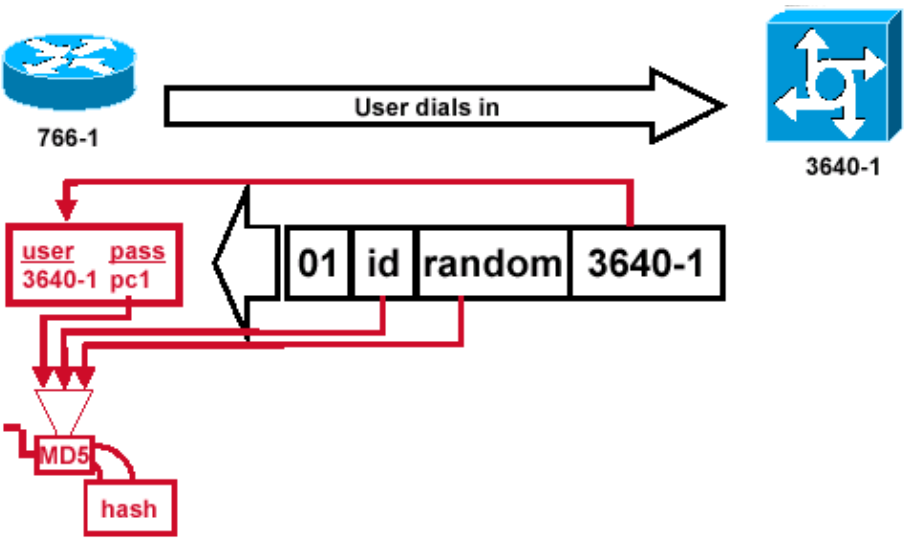
Challenge



This figure illustrates the following steps in the CHAP authentication between the two routers:

1. A CHAP challenge packet is built with the following characteristics:
   - 01 = challenge packet type identifier.
   - ID = sequential number that identifies the challenge.
   - random = a reasonably random number generated by the router.
   - 3640−1 = the authentication name of the challenger.
2. The ID and random values are kept on the called router.
3. The challenge packet is sent to the calling router. A list of outstanding challenges is maintained.

Response



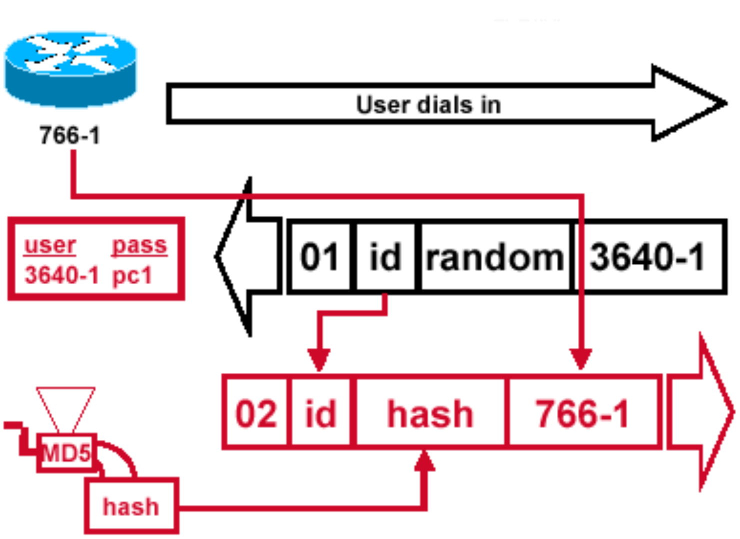
This diagram illustrates the receipt and MD5 processing of the challenge packet from the peer. The router processes the incoming CHAP challenge packet in the following manner:

1. The ID value is fed into the MD5 hash generator.
2. The random value is fed into the MD5 hash generator.
3. The name 3640−1 is used to look up the password. The router looks for an entry matching the username in the challenge. In this example, it looks for:

   ```
   username 3640−1 password pc1
   ```
4. The password is fed into the MD5 hash generator.

   The result is the one−way MD5−hashed CHAP challenge that will be sent back in the CHAP response.

Response (continued)

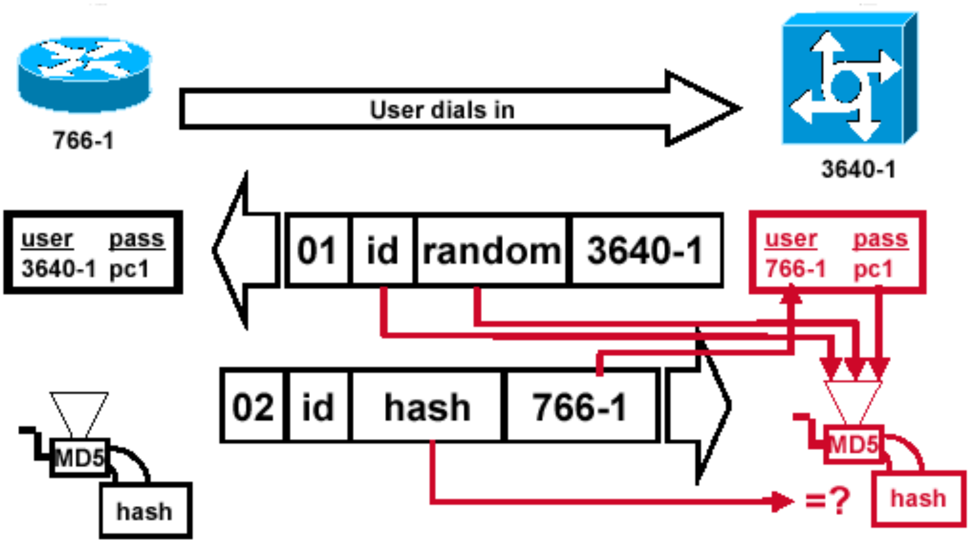


This diagram illustrates how the CHAP response packet sent to the authenticator is built. The following steps are shown in this figure:

1. The response packet is assembled from the following components:

    - ♦ 02 = CHAP response packet type identifier.
    - ♦ ID = copied from the challenge packet.
    - ♦ hash = the output from the MD5 hash generator (the hashed information from the challenge packet).
    - ♦ 766−1 = the authentication name of this device. This is needed for the peer to look up the username and password entry needed to verify identity (this is explained in more detail below).
2. The response packet is then sent to the challenger.

Verification

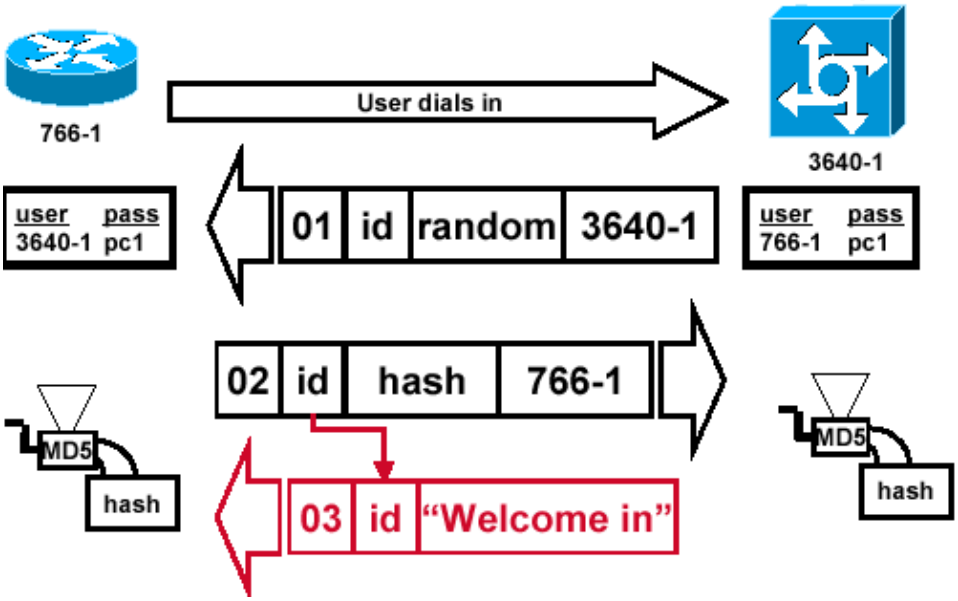


This diagram shows how the challenger processes the response packet. The CHAP response packet is processed (on the authenticator) in the following manner:

1. The ID is used to find the original challenge packet.
2. The ID is fed into the MD5 hash generator.
3. The original challenge random value is fed into the MD5 hash generator.
4. The name 766−1 is used to look up the password from one of the following sources:

    - ♦ Local username and password database.
    - ♦ RADIUS or TACACS+ server.
5. The password is fed into the MD5 hash generator.
6. The hash value received in the response packet is then compared to the calculated MD5 hash value. CHAP authentication succeeds if the calculated and the received hash values are equal.

Result



This diagram illustrates the success message being sent to the calling router.

1. If authentication is successful, a CHAP success packet is built from the following components:
   - 03 = CHAP success message type.
   - ID = copied from the response packet.
   - Welcome in is simply a text message providing a user−readable explanation.
2. If authentication fails, a CHAP failure packet is built from the following components:
   - 04 = CHAP failure message type.
   - ID = copied from the response packet.
   - Authentication failure or other text message, providing a user−readable explanation.
3. The success or failure packet is then sent to the calling router.

   Note: This example depicts a one−way authentication. In a two−way authentication, this entire process is repeated, however the calling router initiates the initial challenge.

Troubleshooting CHAP

Refer to Troubleshooting PPP Authentication for troubleshooting information.

Related Information

- **Understanding debug ppp negotiation Output**
- **Troubleshooting PPP Authentication**
- **PPP Authentication Using the ppp chap hostname and ppp authentication chap callin Commands**
- **Access Technology Support Pages**
- **Tools and Utilities − Cisco Systems**
- **Technical Support − Cisco Systems**