Configure and Understand the PPP CHAP Authentication

Contents

Introduction

This document describes how the Challenge Handshake Authentication Protocol (CHAP) verifies the identity of a peer by means of a three-way handshake.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- How to enable PPP on the interface through the encapsulation ppp command.
- The **debug ppp negotiation** command output. Refer to [Understand debug ppp negotiation Output](#) for more information.
- How to troubleshoot when the Link Control Protocol (LCP) phase is not in the open state. This is because, the PPP authentication phase does not begin until the LCP phase is complete and is in the open state. If the debug ppp negotiation command does not indicate that LCP is open, you need to troubleshoot this issue before you proceed.

  Note: This document does not address MS-CHAP (Version 1 or Version 2).

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

For more information on document conventions, see the [Cisco Technical Tips Conventions](#).

Background Information

The Challenge Handshake Authentication Protocol (CHAP) (defined in [RFC 1994](#)) verifies the identity of the peer by means of a three-way handshake. These are the general steps performed in CHAP:
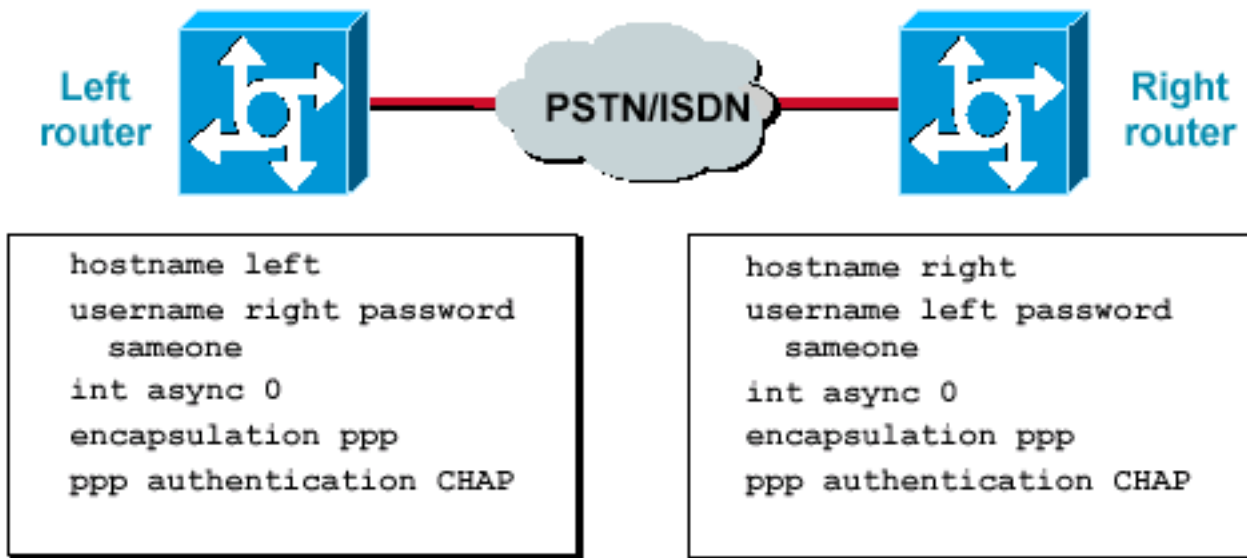
1. After the LCP (Link Control Protocol) phase is complete, and CHAP is negotiated between both devices, the authenticator sends a challenge message to the peer.
2. The peer responds with a value calculated through a one-way hash function (Message Digest 5 (MD5)).
3. The authenticator checks the response 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, you can negotiate CHAP in both directions, with the help of the same secret set for mutual authentication.

For more information on the advantages and disadvantages of CHAP, refer to [RFC 1994](#).

Configure CHAP

The procedure to configure CHAP is fairly straightforward. For example, assume that you have two routers, left and right, connected across a network, as shown in Figure 1.

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

Two

Routers Connected Across a Network

Figure 1 — Two Routers Connected Across a Network

To configure CHAP authentication, complete these steps:

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
   username username password password command, where *username* is the hostname of the peer.
   Ensure that:Passwords are identical at both ends.The router name and password are exactly
   the same, because they are case-sensitive.

   Note: By default, the router uses its hostname to identify itself to the peer. However, this
   CHAP username can be changed through the ppp chap hostname command. Refer to PPP
   Authentication with 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, you use CHAP in both directions
to create 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, and this results in a two-way authentication.

One-way authentication is often required when you connect to non-Cisco devices.

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

Table 1 shows when to configure the callin option.

Table 1: 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**

Refer to [PPP Authentication with the ppp chap hostname and ppp authentication chap callin Commands](#) for more information.

CHAP Configuration Commands and Options

Table 2 lists the CHAP commands and options:

Table 2: CHAP Commands and Options

Command	Description
**ppp authentication {chap	ms-chap	ms-chap-v2	eap |pap} [callin]**	This command enables local authentication of the remote PPP peer with the specified protocol.
ppp chap hostnameusername	This command defines an interface-specific CHAP hostname. Refer to [PPP Authentication with the ppp chap hostname and ppp authentication chap callin Commands](#)for more information.
ppp chap passwordpassword	This command defines an interface-specific CHAP password.
**ppp directioncallin	callout	dedicated**	This command forces a call direction. Use this command 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, which means that all attempts by the peer to force the user to authenticate with the help of 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 that the router sends.
ppp chap wait	This command specifies that the caller must authenticate first (default enabled). This command specifies that the router does not authenticate to a peer that requests 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 diagrams in this section 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 negotiationcommand output. For more information, refer to Understand debug ppp negotiation Output.

Call

e Call Comes In   *Th*

Figure 2 — The Call Comes In

Figure 2 displays these steps:

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 how to determine this, refer to Understand debug ppp negotiation Output.
3. A CHAP challenge from 3640-1 to the calling router is required on this call.

Challenge
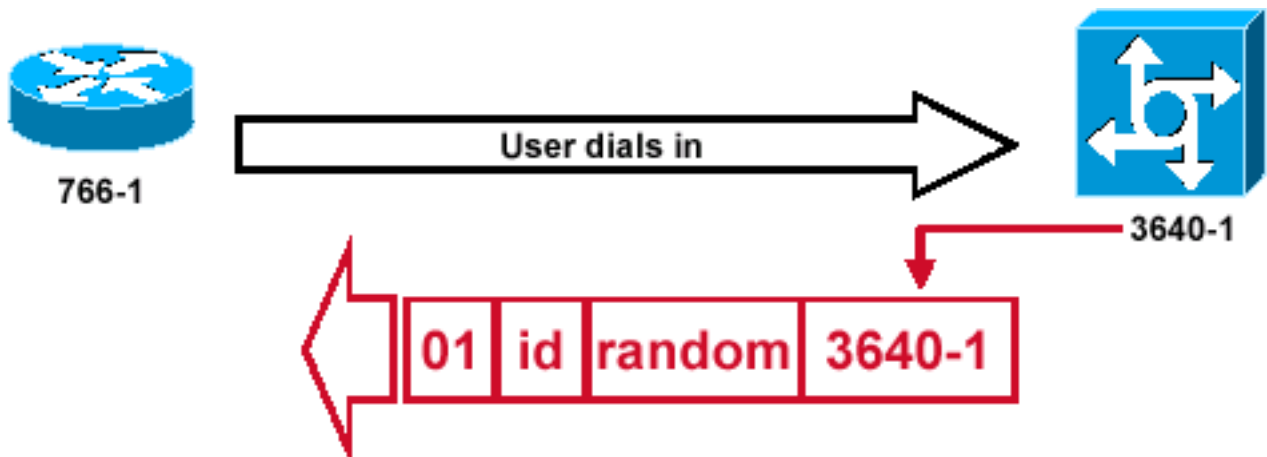
HAP Challenge Packet is Built   *C*

Figure 3 — A CHAP Challenge Packet is Built

Figure 3illustrates these steps in the CHAP authentication between the two routers:

1. A CHAP challenge packet is built with these 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
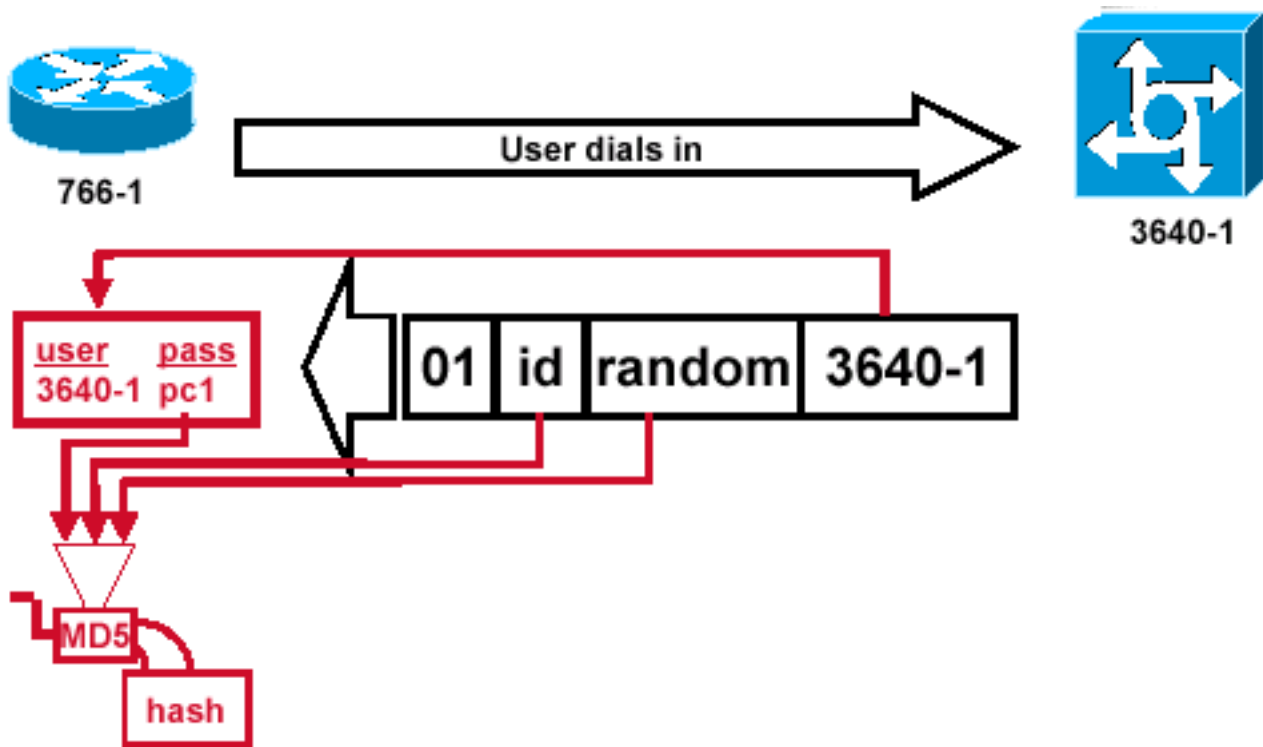
Receipt and MD5 Processing of the Challenge Packet from the Peer

Figure 4 — Receipt and MD5 Processing of the Challenge Packet from the Peer

Figure 4 illustrates the how the challenge packet is received from the peer, and processed (MD5). The router processes the incoming CHAP challenge packet in this way:

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 that matches 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 is sent back in the CHAP response.

Response (Continued)
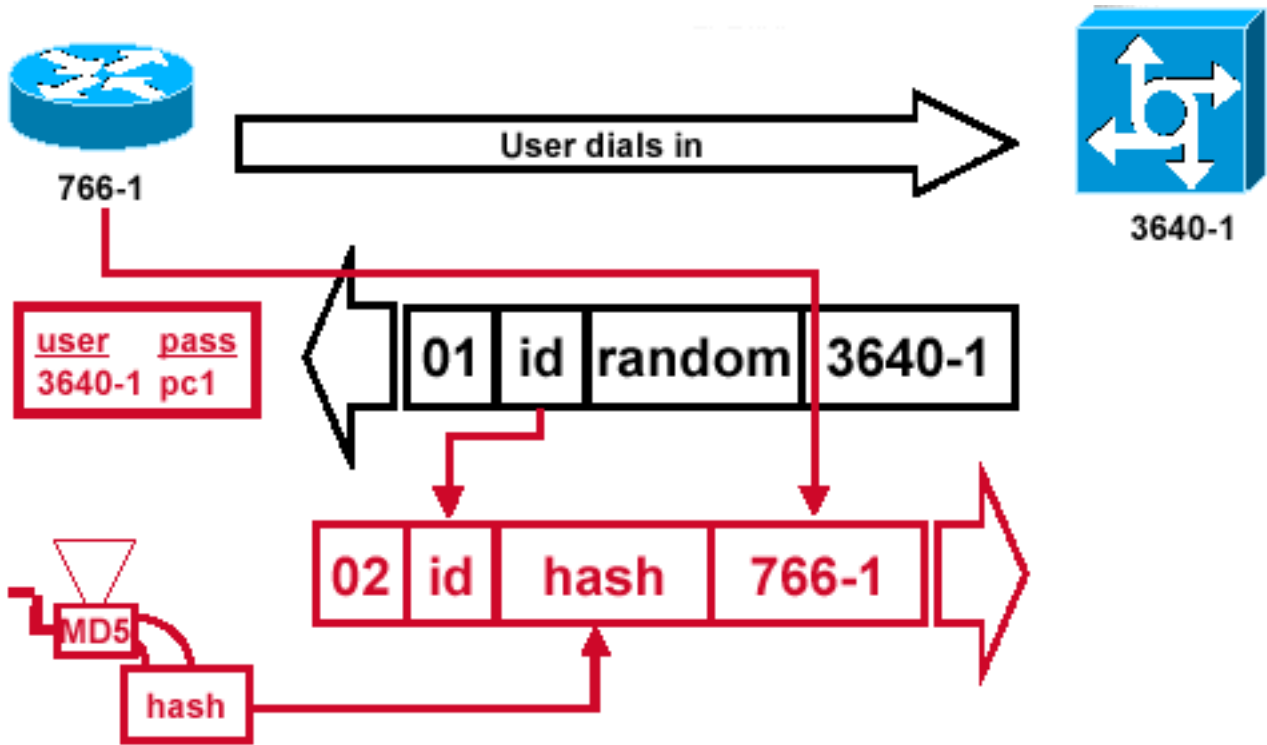
Response Packet Sent to the Authenticator is Built

Figure 5 — The CHAP Response Packet Sent to the Authenticator is Built

Figure 5 illustrates how the CHAP response packet sent to the authenticator is built. This diagram shows these steps:

1. The response packet is assembled from these 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 in the Verify CHAP section).
2. The response packet is then sent to the challenger.

Verify CHAP

This section provides tips on how to verify your configuration.
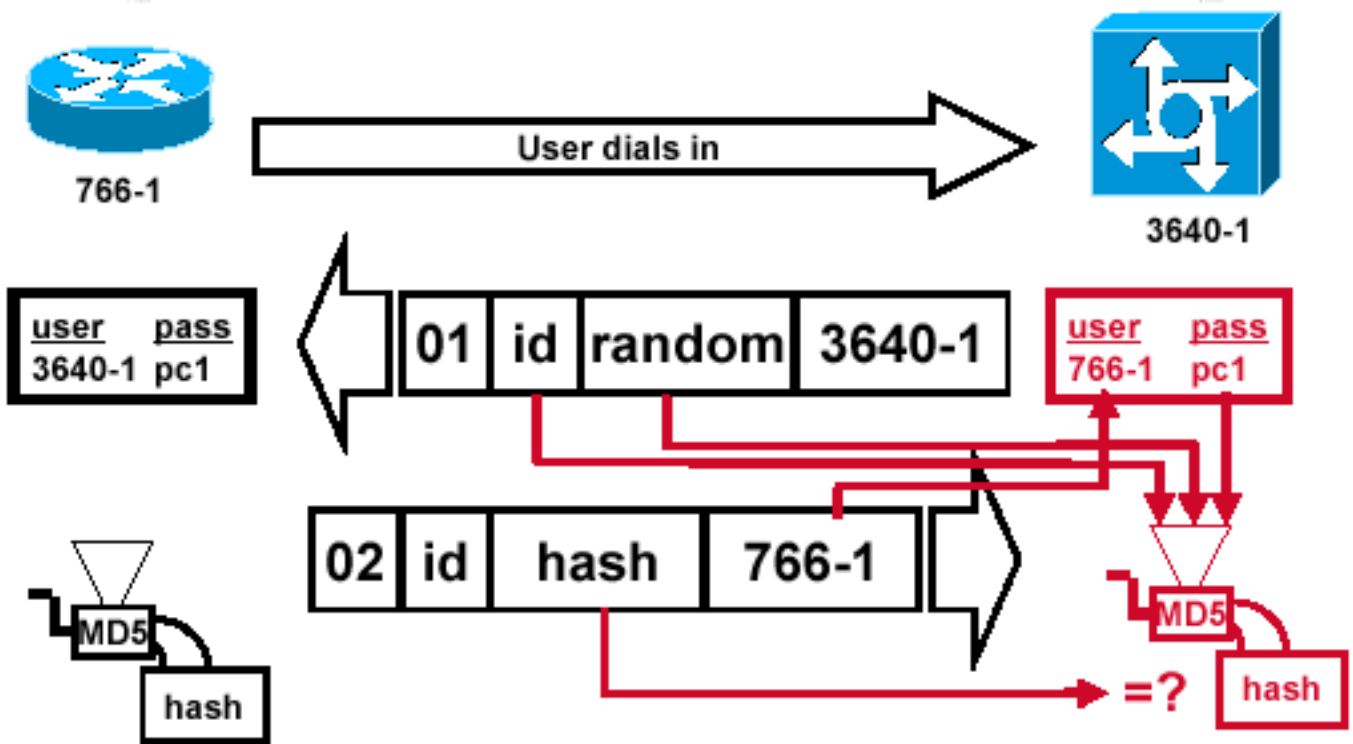
Challenger Processes the Response Packet

Figure 6 — The Challenger Processes the Response Packet

Figure 6 shows how the challenger processes the response packet. Here are the steps involved when the CHAP response packet is processed (on the authenticator):

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 these 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 with the calculated MD5 hash value. CHAP authentication succeeds if the calculated and the received hash values are equal.

Result

Success Message is Sent to the Calling Router
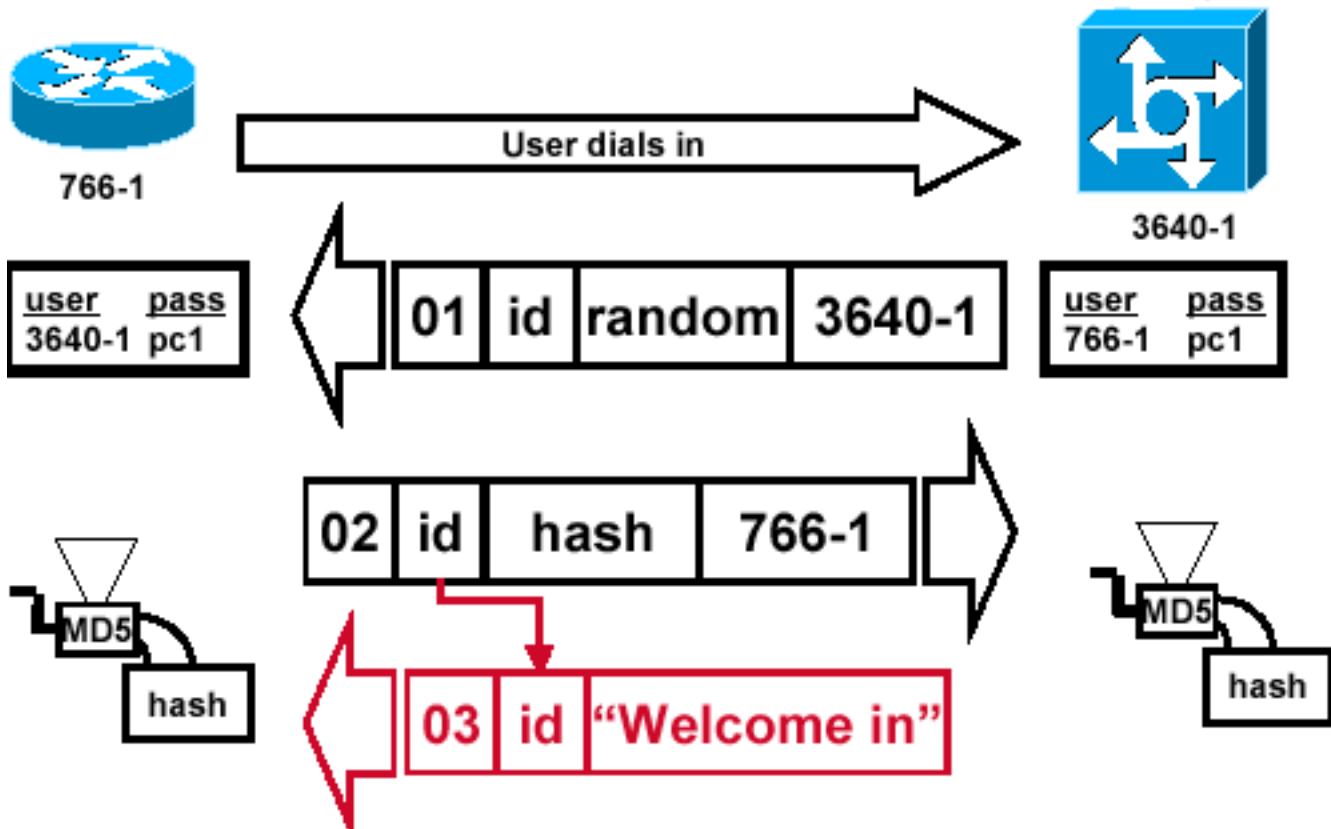
ccess Message is Sent to the Calling Router

Figure 7 — Success Message is Sent to the Calling Router

Figure 7 illustrates the success message sent to the calling router. This involves these steps:

1. If authentication is successful, a CHAP success packet is built from these components:03 = CHAP success message type.ID = copied from the response packet."Welcome in" is simply a text message that provides a user-readable explanation.
2. If authentication fails, a CHAP failure packet is built from these components:04 = CHAP failure message type.ID = copied from the response packet."Authentication failure" or other text message, that provides 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.

Troubleshoot CHAP

Refer to [Troubleshoot PPP (CHAP or PAP) Authentication](#) for information on how to troubleshoot any issues.

Related Information

- **[Understand debug ppp negotiation Output](#)**
- **[PPP Authentication with the ppp chap hostname and ppp authentication chap callin Commands](#)**
- **[Cisco Technical Support & Downloads](#)**