

Compatible Systems Tech Notes: Authentication of PPP Connections

Document ID: 17666

- Introduction**
- Prerequisites**
 - Requirements
- Affected Products**
- Affected Versions**
- More Information**
- Related Information**

Introduction

This document defines three methods of PPP authentication called Chat Script, PAP, and CHAP.

Prerequisites

Requirements

There are no specific requirements for this document.

Affected Products

900i, 1200i, 1220i, 1250i, 1270i, 2600i, 2900i, 2200R, 2220R, 2250R, 2270R, 3500R, 3800R, VSR-2, and VSR-8

Affected Versions

All versions

More Information

There are three methods of Authentication used by Compatible routers to authenticate WAN PPP connections.

Chat Script Authentication involves the chat script answering terminal server type prompts from the far side that ask for login and password in plain text. Here is an example of a generic Chat script with authentication:

```
send ATDT 9,1,800-356-0283
expect CONNECT
expect ogin:
send username
expect sword:
send password
```

The "login:" and "password:" prompts are cut off because the router is trying to match the text exactly with what the far end is sending before moving on. When you leave off letters, it allows for differences in

capitalization. Ensure that the text sent from the far end matches exactly what the chat script expects. You can check in the device log at "debug level" to see if each of the lines in your chat script are used and accepted. For every "expect" you see, it should have an "expect matched" later on. If you see an "expect timeout" that means the router never saw what was expected. Check that you really do use this authentication method and that the far end sends exactly what you expect. If you do not use this method of authentication, then leave these extra lines off of the chat script so that you only have the send ATDT and expect CONNECT lines. If this type of authentication fails, then remove it and configure both CHAP and PAP. CHAP and PAP are on demand and it does not hurt to have them both on to respond to the other side.

PAP Authentication is Password Authentication Protocol. This is where the far end challenges the router for PAP authentication and the router sends across in plain text its username and password. In the log you see something like "Authentication Phase" and see your username and password. It also tells you whether the authentication was successful. If it was not, then the PPP connection does not establish and the negotiation shuts down.

CHAP Authentication is Challenge Handshake Authentication Protocol. This is a more secure method of authentication similar to PAP, but it uses encryption to hide its username and password. The log is similar, but says CHAP instead of PAP.

Ensure that when you use PAP and CHAP that you only "Allow" or "Respond" to requests. If you accidentally use "Both" or "Request" the router queries the far side for their password and most likely they are not prepared for it and the negotiation fails.

In order to configure CHAP and PAP, refer to the online manuals under PPP.

Related Information

- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jun 19, 2007

Document ID: 17666
