PPP Configuration Options

Cisco routers using PPP encapsulation include the LCP options shown in the following table.

Feature	How It Operates	Protocol
Authentication	Requires a password; performs challenge handshake	PAP CHAP
Compression	Compresses data at source; reproduces data at destination	Stacker or protocol
Error detection	Monitors data dropped on link; avoids frame looping	Magic Number
Multilink	Load balancing across multiple links	Multilink Protocol (MP)

- Authentication options are Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).
- Compression options increase the effective throughput on PPP connections.
- For error detection, the quality and magic number options help ensure a reliable, loop-free data link.
- Multilink is available in Cisco IOS Release 11.1 and later. It improves throughput and reduces latency between peer routers.
- PPP callback is available in Cisco IOS Release 11.1. It offers enhanced security. After making the initial DDR call, the router requests that it be called back and then terminates its call.

Establishing a PPP Session

The three phases of PPP session establishment are link establishment, authentication, and network protocol.

- **Link establishment—**Each PPP device sends LCP packets to configure and test the data link. Options such as maximum receive unit, compression, and link authentication are negotiated here. Default values are assumed when no figures are present.
- **Authentication (optional)—**After the link is established, the peer can be authenticated.
- **Network layer protocol—**NCP packets are used to select and configure network layer protocols. After they are configured, the network layer protocols can begin sending datagrams over the link.

PPP Authentication Protocols

PPP Authentication Protocol is a simple two-way handshake that's used to establish a remote node's identity. It takes place after the PPP link is established. The remote node repeatedly sends its username and password to the router until authentication is acknowledged or the connection is terminated.

CHAP is a three-way handshake that takes place at link startup and periodically throughout the session to verify the remote node's identity. After the PPP link is established, the local router sends a challenge message to the remote node. The remote node responds with a calculated value (typically, an MD5 function is used). The local router checks the response against its own calculated value. If the values match, the authentication is acknowledged. Otherwise, the connection is terminated immediately.

How Secure Is PAP/CHAP?

With PAP, passwords are sent across the link without encryption or protection against trial-and-error attacks. This level of security is usually sufficient for token-type passwords that change with each authentication.

CHAP uses unpredictable challenge values, which limit exposure to attacks. Local router or authentication servers (TACACS) control the challenges' frequency and timing.

PPP Encapsulation and Authentication Overview

You must do the following before enabling PAP or CHAP:

- Enable PPP protocol encapsulation on each router.
- Assign a host name to each router.
- Define a remote username and password for each router to accept the authentication process.

Here's a CHAP configuration example:

```
RouterA>enable
RouterA#configterm
RouterA(config)#hostname flanders
RouterA(config)#username ned password maude
RouterA(config)#interface serial 0
RouterA(config-if)#encapsulation ppp
```