Fusion Embedded™ PPP

With the explosive growth over the last decade of dial-up Internet connectivity, the Point-to-Point Protocol (PPP) has become the standard protocol for connecting to the Internet over serial links.

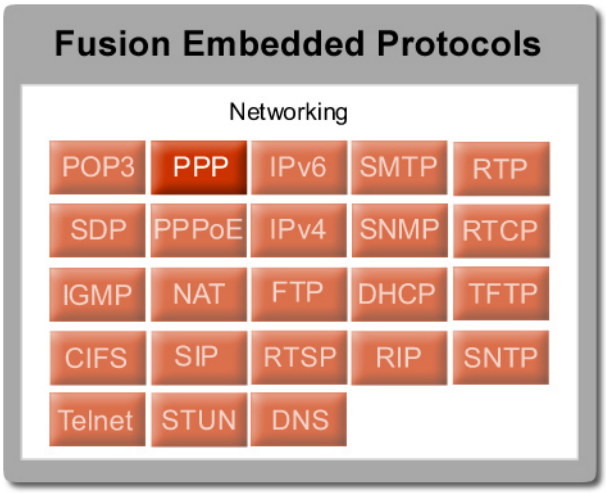
The success of PPP is due largely to its ability to automatically configure a serial communication link without human intervention. In particular, it allows a remote access server to automatically assign an IP address, a default IP gateway, and name server (DNS) addresses to a dial-up client (a home PC, for example) without human intervention. This auto-configuration capability was the main design goal of PPP. It has proven to be enormously successful, especially in the home market where it has been instrumental in enabling the Internet revolution by making it simple for home PCs to connect to the Internet via dial-up modem connections to Internet Service Providers.

Also critical to the success of PPP is its integral support for authentication. Via PPP negotiations, a PPP client and server can agree on an authentication protocol to use to authenticate each end of the link. Internet Service Providers use this authentication to limit access to their networks to paying subscribers, and to implement billing and accounting. In this scenario, typically only the dial-up PPP client (PC) authenticates itself to the server. However, PPP supports authentication in either or both directions, so that for added security both ends of the link can be authenticated. This capability is exploited, for example, when two Internet routers connect to one another via a PPP link. Using Fusion Embedded PPP, these same capabilities can be extended to embedded platforms.

Serial links remain the most cost-effective approach to adding TCP/IP network connectivity to low-cost embedded platforms. Direct connections (null modems) can be used for local connectivity, while dial-up connections via standard modems enable low-cost remote connectivity for a wide range of devices – from vending machines to set-top boxes, security systems to remote seismic equipment.

Product Overview

Fusion Embedded PPP is standards-compliant and provides all of the features expected of a mature and robust PPP implementation for embedded systems. It can be anywhere from the simplest, single-interface PPP clients, to more complex Remote Access Server (RAS) devices with multiple interfaces and routing requirements. It integrates seamlessly with Fusion Embedded TCP/IP stack.



- Robust, 100% RFC 1661 compliant Finite-State-Machine (FSM) ensures reliability and interoperability
- Fully re-entrant code supports multiple concurrent PPP sessions
- Simple interface to serial device drivers for bringing links up and down, and sending and receiving packets
- Use as a PPP client or server, individually configurable per-interface
- Built-in support for PPP over asynchronous links, including HDLC framing and character transparency
  stuffing/ removal
- Link Configuration Protocol (LCP) for configuring the serial link (character stuffing, authentication protocol, etc.)
- Internet Control Protocol (IPCP) for autoconfiguration of client and server IP addresses, default gateway addresses and Domain Name
- Server (DNS) addresses Van Jacobsen (VJ) compression included for reduction of TCP/IP overhead on slow links
- Support for bi-directional authentication using the two most popular authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Protocol (CHAP).
- Both protocols are included at no additional cost.

Email: info@unicoi.com **Phone**: +1 (678) 208-2250

- Run-time configurable embedded authentication database enables creation of a pool of IP addresses for assignment on an asneeded basis to client devices
- API provided for interfacing to an external authentication database. Fully integrated with the state machine, it enables the use of a file hsystem or even a remote authentication server, such as RADIUS for authenticating peers.
- API for runtime configuration of LCP and IPCP negotiations individually for each PPP interface

For LCP

- Address/Control Field Compression enable/disable
- Protocol Field Compression enable/disable
- Silent mode: wait passively for peer to send the first

LCP configure request

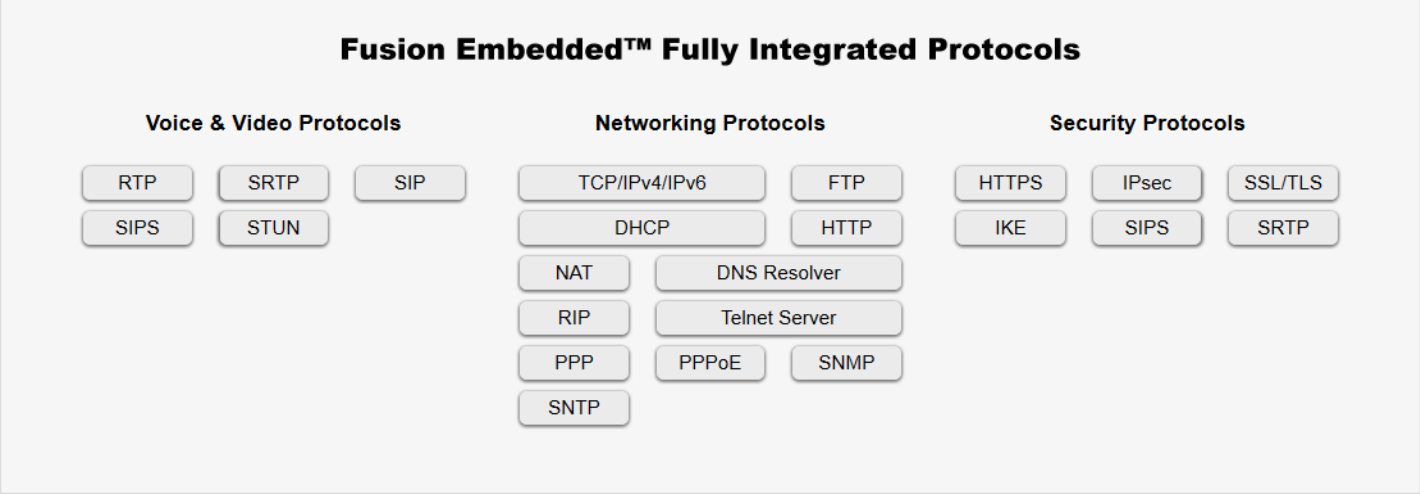
- Persist mode: automatically attempt to establish link when it terminates (normally used with silent mode f or server applications)
- Refuse CHAP authentication: refuse to be authenticated by a server with (CHAP)
- Configure Maximum Receive Unit (MRU)
- For IPCP:
- Enable/disable acceptance of local (Fusion) PPP
- session IP address from peer (server's) IP address (provide an IP address to the peer if disabled)
- Provide the peer with DNS and/or NBNS server addresses, including API call to configure addresses

PPP Features

- Client and server included
- Powerful API for runtime configuration
- Call-back functions for status and progress
- Multiple concurrent PPP sessions
- Encapsulates datagrams over serial links
- Link Control Protocol (LCP) for establishing,
- configuring and testing data-link connection
- IPCP for automatic configuration of IP addressing, including DNS and gateways
- Supports Van Jacobsen (VJ) header compression
- State machine architecture for accurate, robust performance
- Mature code deployed in a wide range of applications and backed by many years of embedded networking experience
- DSP and microprocessor support

RFC Compliance

- RFC 1144
- RFC 1321
- RFC 1332
- RFC 1334
- RFC 1661
- RFC 1662
- RFC 1994



Email: info@unicoi.com **Phone**: +1 (678) 208-2250