CoVPN

Protocol Suite

Product overview

Virtual Private Networking (VPN) permits the establishment and maintenance of secure, private end-to-end "tunnels" between geographically distributed network devices. As defined by the IETF, the Layer 2 Tunneling Protocol (L2TP) allows encapsulated data to be securely transmitted over the Internet or an Intranet, ensuring the integrity and authenticity of data. A L2TP tunnel consists of two end-points:

- A remote user connected through a Network Access Server, known as a L2TP Access Concentrator (LAC).
- A "network gateway" L2TP Network Server (LNS).

CoVPN allows developers to rapidly integrate and deploy L2TP LAC/LNS and RADIUS Client services. The CoVPN software suite includes the following components:

- **CoPPP-ML,** a complete implementation of PPP and MultiLink PPP (see separate data sheet).
- **CoL2TP,** an implementation of LAC and LNS protocols, composed of a client task that interacts with a UDP/IP stack through a socket library and an API for controlling tunnel establishment, payload messaging, "keep alive" mechanisms, flow control and other features.
- **CoRADIUS,** a client implementation of the Remote Authentication Dial-In User Service (RADIUS) protocol, composed of a client task and an API library.

Interaction between the L2TP client, RADIUS client, and other applications is managed via Interprocess Communications (IPC) mechanisms and a UDP socket interface.

In a typical L2TP session, the PPP Link Control Protocol (LCP) on the LAC and the PPP Network Control Protocol (NCP) on the LNS negotiate a connection, conduct authentication (via RADIUS or a similar protocol), and then use a virtual PPP port to exchange encapsulated frames and data. This is illustrated in Fig. 1.

PN tunnels can also serve as a platform for the Multi-node MultiLink Protocol, allowing individual links within a MultiLink PPP bundle to be terminated on different dial-up servers. Multiple tunnels between an LAC and LNS might also support multiple physical media types with different Quality of Service (QoS) attributes.

Available for VxWORKS, pSOS and other real-time operating systems, CoVPN supports the following industry standards:

- RFC 2661/PPP Working Group, L2TP and L2TP Accounting Procedures.
- RFC 2138 - Remote Authentication Dial-In User Service (RADIUS).
- RFC 2139 - RADIUS Accounting Procedures.
- IETF Draft / PPP Working Group, RADIUS Tunneling.

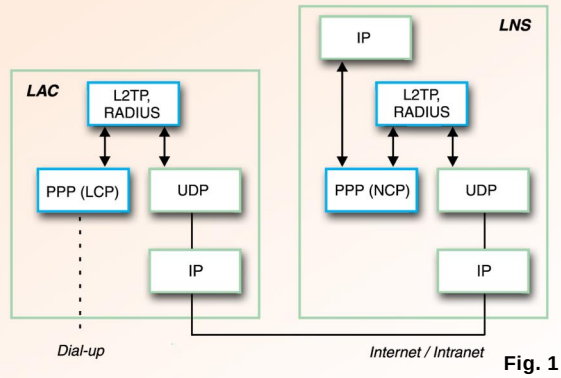

Fig. 1

- Seamless integration with CoPPP-ML (PPP/MultiLink PPP), CoFRelay (Frame Relay) and CoISDN (BRI and PRI) stacks.

CoVPN will provide support for evolving standards in upcoming releases (call for availability). Examples include:

Standards

- L2TP Tunnel Authentication at LAC and LNS.
- Internet Key Exchange Protocol (IKE).
- Multiprotocol over ATM.
- PAP, CHAP, and MS-CHAP Proxy Authentication at LNS.

Drafts

- L2TP over AAL5 and FUNI.
- L2TP Security Extensions for non-IP Networks.
- L2TP MIB.
- Multi-node/MultiLink Support (call bundling in tunnels).
- RADIUS Compulsory Tunnel Extensions.
- Accounting Interim Record Extensions.
- RADIUS Extensible Authentication Protocol (EAP).
- RADIUS Modifications for Tunnel Protocol Support.
- RADIUS Authentication Client MIB.

An overview of the CoVPN architecture is illustrated in Fig. 2.

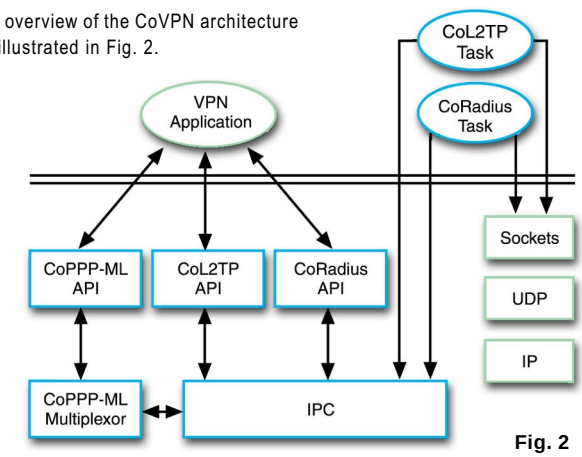

Fig. 2

CoSystems Networking & Communication Technologies
1263 Oakmead Parkway, Sunnyvale, CA 94085, USA.
Ph: + 1 (408) 522 0500. Fax: + 1 (408) 720 9114.
www.cosystems.com