

High Performance Networking and Security



SSHield (SSH1 / SSH2 protocols)

A small-footprint embedded implementation of the Secure Shell (IETF SECSH) protocol. Includes secure copy (scp), secure FTP (sftp and stftp) and built-in modular crypto libraries. Secures any CLI and allows integration with X.509 digital certificates, RADIUS and Kerberos authentication.



SSLimSecure (SSL / TLS protocols)

A small-footprint embedded SSL & TLS implementation. Includes client and server components and a built-in version of modular crypto libraries with APIs for hardware acceleration. Secures web-servers, custom socket applications, and provides transport security at lower layers.



V-IPSecure (IPSec and IKE)

Embedded implementation of network layer security - IPSec and IKE. Supports both tunnel and transport mode ESP and AH, with a wide variety of encryption and hash algorithms. Includes IKE authentication support to allow integration with Kerberos, RADIUS and digital certificates.



NetF1 (High Octane TCP/IP, IPV6, VR)

A high-octane TCP/IP stack for embedded platforms, built for speed and compactness with extensive RFC support, and features for IP backplanes. Includes IPv4 and IPv6 in host and router modes with multi-threaded, multi-instance, Virtual Router (VR) capabilities and DoS protections.



GrandPPPrix (Multi-Class/Multi-Link PPP)

A full-featured embedded PPP stack including a multi-link aggregation of point-to-point links, and multi-class PPP extensions (RFC 2686) to prioritize delay sensitive traffic. Includes support for IPv6 and PPPoE, and provides for external traffic regulation.



ParaDoS (Denial of Service Prevention)

A DoS-hardened network stack with ingress/egress filtering, prioritized traffic functions, and active attack monitoring. It includes built-in protection profiles for common DoS attacks and the flexibility to add new attack patterns and customizable responses based on system alert levels.



X-Calibur (IEEE 802.1X)

An implementation of the Port-based Network Access Control (IEEE 802.1X PNAC) protocol for embedded supplicants and authenticators. It provides a framework to communicate with an authentication server based on Extensible Authentication Protocol (EAP).



ASAP (Access Point Security)

A complete secure WiFi package which includes an 802.11 driver framework, reference drivers and support for WEP, WPA and 802.11i security. Pre-shared key & infrastructure modes (802.1X), and a built-in RADIUS client are included, with support for CCMP and TKIP/Michael.



AuthAgent Kerberos (Kerberos V Agent)

A full-featured implementation of the Kerberos V agent functionality for embedded platforms, which includes functionality to enable Kerberos authentication in network clients and services, based on RFC 1510.



AuthAgent RADIUS (RADIUS Authentication Agent)

A flexible RADIUS client library for embedded environments. It integrates with network security protocols requiring authentication (such as IKE, SSH, 802.1X EAPoL and EAP) and also supports standalone authentication functionality.



AuthAgent X.509 (Digital Certificate Authentication)

A public key and digital certificate authentication framework that includes the ability to revoke certificates (CRL support) and the provision for multiple alternative implementations of X.509 handling.



Switchcraft Merlink (LACP & fail-over)

Managed link aggregation for bundling multiple links for increased effective bandwidth, load-balancing and fail-over capabilities. Includes API-driven link-aggregation library as well as a full implementation of the IEEE 802.3ad LACP and marker protocols.



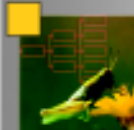
Spantasmic (Spanning Tree Protocols 802.1d/w/s)

An implementation of the STP (802.1d), RSTP (802.1w) and MST (802.1s) variants of the Spanning Tree Protocol for bridges and switches. It includes an optional software bridging framework with built-in forwarding and an address resolution logic-based filtering database.



GNAT (Network Address Translator)

A fast embedded Network Address Translator, sporting a rules-based command interface and full support for bidirectional static and dynamic NAT with NATP, as well as support for popular ALGs.



ClassHopper (Alternate Queuing Discipline)

An alternate queuing discipline framework for QoS enhancements, prioritization and bandwidth limiting. It includes standard queuing models such as Class-Based Queuing, RED and others, as well as a framework to develop custom queuing disciplines.



FireFly (IP Packet Filtering Firewall)

A lean, high performance, packet-filtering embedded firewall. FireFly supports a variety of filtering criteria, and a flexible interface for setting up policies. It also includes hooks for dynamic firewalling and stateful inspection.