



ASAP

Air Secure Access Point

Air Secure Access Point (ASAP) is a comprehensive, secure, managed embedded access point (AP) software package. It integrates the latest wireless security technologies with a flexible driver framework that works with a variety of 802.11 WLAN devices. Besides providing full-featured managed AP functionality, ASAP concurrently supports the many different generations

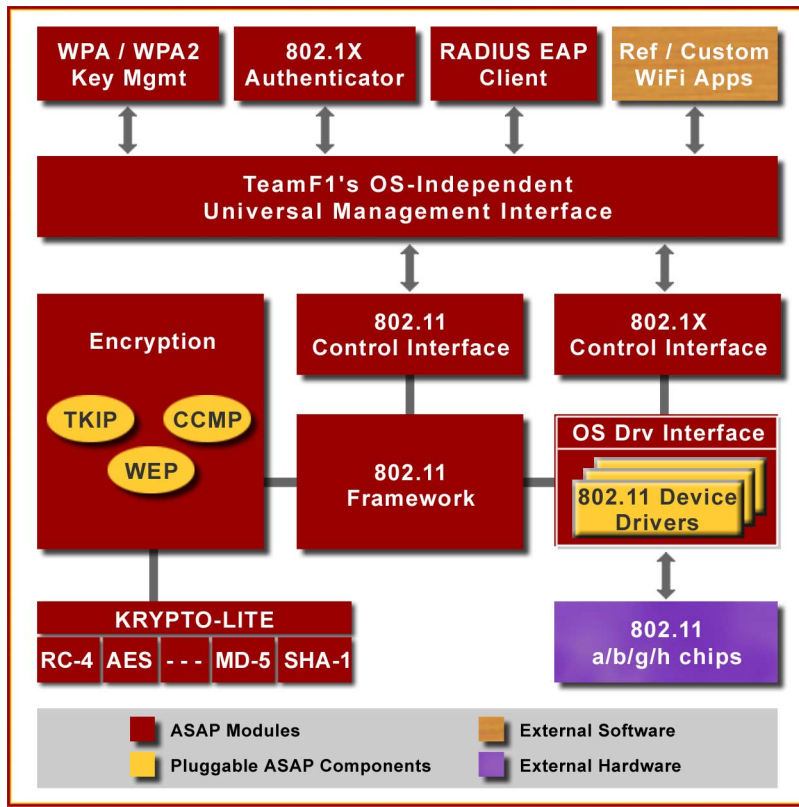
of 802.11 security technology found in today's wireless networks, from WEP through WPA, up to WPA2/ 802.11i, in either Personal (Pre-shared Key) or Enterprise (802.1X) mode.

Rich 802.11 Functionality

ASAP includes comprehensive support for 802.11 - a set of IEEE physical and data link layer standards for radio

Features

- ❖ Complete secure managed access point functionality
- ❖ Support for WEP, WPA, WPA2 / 802.11i
- ❖ CCMP, TKIP + MIChael, WEP-40 and WEP-104 bit cipher support
- ❖ Dynamic WEP re-keying for non-WPA STAs with 802.1X
- ❖ WPA and WPA2/802.11i Key management
- ❖ WPA-Personal (PSK) and WPA Enterprise (802.1X) modes
- ❖ Simultaneous support for non-WPA and WPA/802.11i supplicants
- ❖ Built-in RADIUS client
- ❖ 802.11 framework with QoS (802.11e) and reference drivers
- ❖ Support for multiple CPU types of either endian-ness including PowerPC, MIPS, X86, ARM/Xscale
- ❖ Royalty-free full source distribution



The Security Advantage

ASAP is a complete solution for network devices that require secure access point functionality. ASAP includes Krypto-Lite, TeamF1's FIPS-certified common crypto framework, along with a suite of encryption and integrity components to secure and manage access point traffic. Krypto-Lite also allows the seamless integration of other optional security protocols developed by TeamF1 such as SSL/https, SSH and IPsec/IKE to meet additional security requirements.

frequency communication. ASAP implements the "infrastructure" mode of 802.11 operation which enables a device connected to a wired LAN to act as an access point, allowing wireless stations (STAs) to communicate with it. ASAP includes a template driver for the air interface and an 802.11 framework to ease the development of device drivers for new Wi-Fi@ chips. Besides its integration with various Wi-Fi chipsets, ASAP is seamlessly integrated with leading operating systems. To enable out-of-the-box AP functionality, an optimized 802.11 a/b/g reference driver for Atheros chipsets is also included. In addition, ASAP features an 802.11 MIB, QoS control using 802.11e / WMM™,

and support for multiple radios and SSIDs. Besides facilities for remote configuration and provisioning, such as through a web-interface or a CLI, fine-grain control for **ASAP**'s functionality is also available through developer APIs for use in diagnostics development and custom embedded applications that require programmatic control of the AP.

Flexible & Secure

With the introduction of **ASAP**, the embedded designer can now leverage the significant benefits offered by wireless communication to networked devices without the security problems that would otherwise result from the use of difficult-to-protect airwaves with no well-defined physical boundary. Compromised security on a WLAN could take the shape of unauthorized clients or even unauthorized access-points (inadvertent or deliberate "evil-twin" APs) that join the network. **ASAP**'s ability to turn off SSID broadcast and features for rogue AP detection and MAC address based filtering thwart many of these spoofing attacks. Further, data interception and monitoring attacks such as session-hijacking are also some problems in an inherently insecure medium. 802.11's legacy Wired

Equivalence Privacy (WEP) has several deficiencies but is still commonly used. Industry standards such as Wi-Fi Protected Access (WPA™) and the newer WPA2™ & IEEE 802.11i standards provide much stronger security. **ASAP** supports WPA's Temporal Key Integrity Protocol (TKIP) for data confidentiality and the "MIChael" message integrity code for data integrity. **ASAP** also supports the Counter with CBC-MAC Protocol (CCMP) based on the AES algorithm which is part of the 802.11i specification. Further, **ASAP** includes an enhanced implementation of the legacy WEP protocol, with dynamic keys using 802.1x as the delivery mechanism to improve its security characteristics. **ASAP** includes support for concurrently connecting to a mix of 802.11i, WPA and WEP clients which is useful in networks that are transitioning from one generation of security technology to the next. **ASAP** also includes WPA/802.11i key management and multiple "dot11" profiles to store interface independent WPA and other settings that can be individually enabled.

802.1X & RADIUS Support

ASAP relies on 802.1X for enterprise-mode authentication and includes a full implementation of the Port-based Network Access Control state machine defined by IEEE 802.1X. In 802.1X mode, **ASAP** allows the AP to act as an authenticator to the network, while using its built-in RADIUS client functionality to authenticate Wi-Fi clients with the Extensible Authentication Protocol (EAP). When in non-enterprise mode, **ASAP** also allows the use of pre-shared keys in environments where RADIUS servers are not available.

Also Available

- ❖ **S Secure Family**
Security protocols (SSL, SSH, IPsec/IKE)
- ❖ **AuthAgents**
Authentication agents: Kerberos, RADIUS, X.509
- ❖ **INSECTS**
Firewall, NAT and QoS disciplines

Custom Solutions

TeamF1's professional services can provide the resources and expertise to build customized applications with **ASAP** including support for hardware acceleration, and **ASAP** device driver development.

OS and Hardware Support

ASAP is a drop-in access point solution offering a lean yet full featured set of standards-based communication and security features packaged as a coherent, easy to use framework. It has been extensively validated on a variety of CPU architectures including PowerPC, MIPS, X86 and ARM/XScale, which minimizes development and integration efforts. **ASAP** accelerates the addition of optimized and secure embedded wireless services into your next design by taking advantage of the unique features presented by popular operating systems. **ASAP** is available with optimized editions for *VxWorks®* and *Linux®* with support for the native network driver model, enhanced memory management. Designed specifically with embedded constraints in mind, and with an emphasis on strong security and leading-edge standards support, **ASAP** can be the building block to add secure wireless AP capabilities to any embedded device.

Standards Support

IEEE 802.11 a/b/g
IEEE 802.11d
IEEE 802.11e / WMM
IEEE 802.11i

Interoperability

WPA2 Personal
WPA2 Enterprise
WPA Key Management
Dynamic WEP re-keying for non-WPA STAs with 802.1X

Email: sales@TeamF1.com
Web: www.TeamF1.com
Ph: 510-505-9931 ext. 5
Fax: (510) 505-9941



© 2003-2005 TeamF1, Inc.