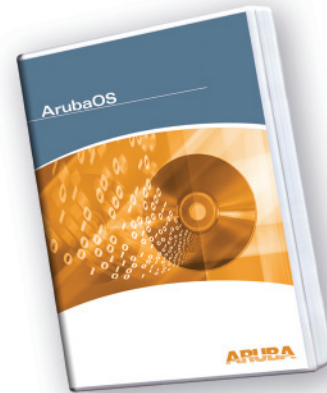


ArubaOS xSec Module

xSec is a highly secure data link layer (Layer 2) protocol that provides a unified framework for securing all wired and wireless connections using strong encryption and authentication. xSec provides greater security than other Layer 2 encryption technologies through the use of longer keys, FIPS (Federal Information Processing Standard)-validated encryption algorithms (AEC-CBC-256 with HMAC-SHA1), and the encryption of Layer 2 header information including MAC addresses. xSec was jointly developed by Aruba Networks and Funk Software.



UNIFIED SECURITY FRAMEWORK

Universal authentication and encryption for wired and wireless users regardless of network access method

FIPS VALIDATED

Meets requirements of U.S. Department of Defense (DoD) directive 8100.2 regarding secure data transmission

LEGACY INVESTMENT PROTECTION

Software-based client solution means legacy wireless access points and NIC cards do not need to be replaced

DESIGNED FOR COMPATIBILITY

Based on IEEE 802.1x framework with support for all secure EAP methods

THE NEED FOR LAYER 2 ENCRYPTION

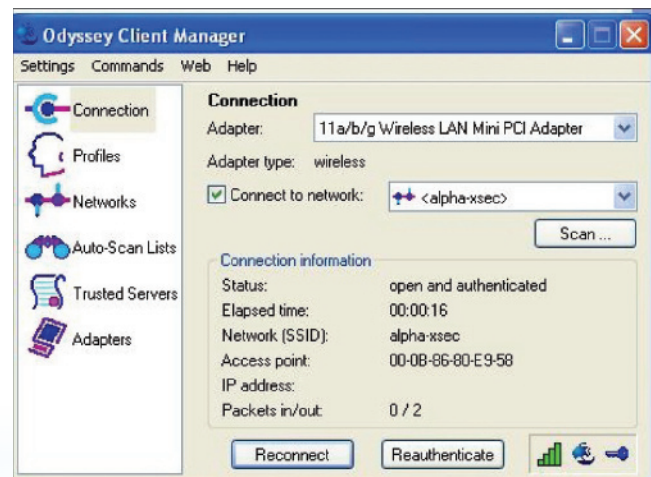
Traditionally, encryption has been performed at Layer 3 (Network Layer) in the form of IPSec. IPSec uses 3DES or AES encryption and can encrypt the IP packet including the source and destination IP addresses in the header.

IPSec provides a commonly accepted, secure method of communication over untrusted networks since the only information left unencrypted are packet headers and pure Layer 2 traffic such as ARP (Address Resolution Protocol) and DHCP (Dynamic Host Configuration Protocol) packets.

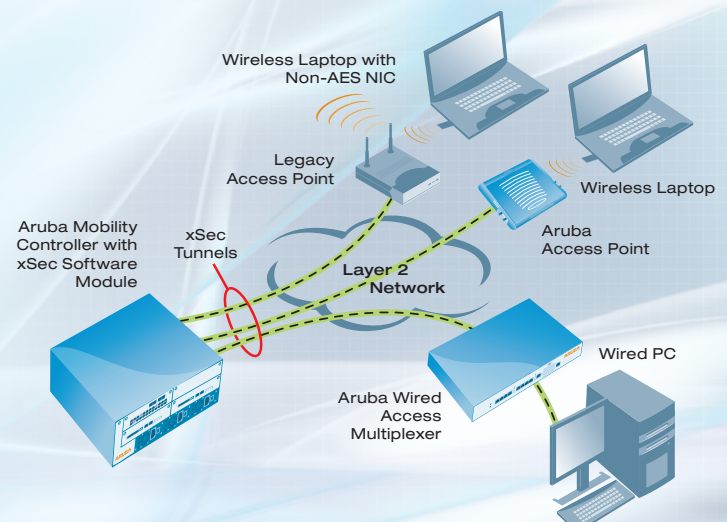
While the confidentiality of IPSec-encrypted data is not in question, the possibility exists that an attacker with direct link-layer access to other devices on a network could carry out attacks against those devices. For example, a wireless network secured with WEP and IPSec could have client devices at risk if an attacker obtains the WEP key and gains Layer 2 access to the network. In addition, there is concern among many security groups that exposure of any packet header information could disclose information that an attacker could use as the basis of an attack.

For this reason, many government agencies and commercial entities that transmit highly sensitive information over wireless networks mandate that strong Layer 2 encryption technologies be deployed to ensure absolute data privacy. U.S. DoD Directive 8100.2 requires that all data transmitted using commercial wireless devices be encrypted at Layer 2 or Layer 3. The U.S. Navy and Army are acquiring Layer 2 encryption, and cryptographic engines used for all sensitive government communications must be validated as meeting FIPS 140-2 requirements.

xSec has been designed to address this requirement and provide a number of additional benefits.



Odyssey Client connected to SSID "alpha-xsec" using xSec protocol



Wired and Wireless Device Connectivity Using xSec

UNIFIED SECURITY FRAMEWORK

xSec enables universal authentication and encryption regardless of access method. Every client that connects to the network, wired or wireless, can authenticate to an Aruba mobility controller using an xSec client. Authentication inside the xSec protocol is accomplished using standard 802.1x EAP (Extensible Authentication Protocol) and utilizes a standard RADIUS server to validate credentials. xSec supports authentication using passwords, certificates, smart cards, token cards, and other credentials supported by the chosen EAP type.

FIPS VALIDATED

Through the use of AES-CBC with a 256-bit key length for encryption, xSec provides the only COTS (Commercial Off-the-Shelf) Layer 2 protocol that is FIPS validated.

As a result, xSec is an ideal solution for security-sensitive applications in the government, finance, and healthcare markets. FIPS validated is a more stringent security standard than those required in the commercial sector, assuring compliance with commercial regulations such as HIPAA and GLBA.

LEGACY INVESTMENT PROTECTION

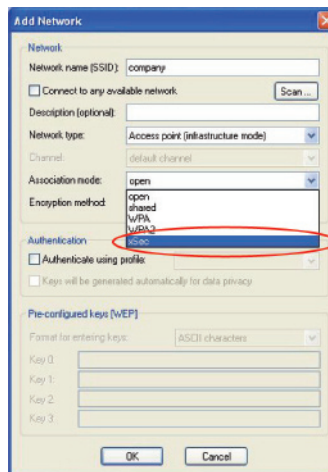
Most legacy equipment cannot be upgraded to support the latest security standards such as 802.11i and WPA2. xSec encryption, however, is performed in hardware by the Aruba mobility controller, and in software at the client level. This means that an existing network can be upgraded to support the latest security technology without the need to replace older access points or wireless NICs (network interface cards).

DESIGNED FOR COMPATIBILITY

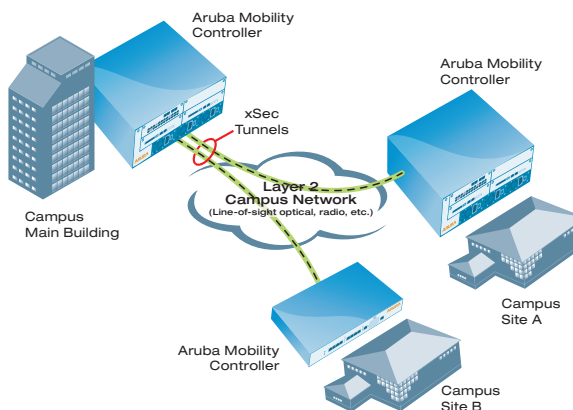
xSec is based on the IEEE security standard 802.1x. Secure EAP methods supported include EAP-TLS, TTLS and PEAP, allowing compatibility with existing security mechanisms such as RSA Tokens and PKI certificates. xSec is designed to be transparent to the Layer 2 infrastructure and can operate through a switched Ethernet network without the risk of EAP frames being intercepted by 802.1x-aware Ethernet switches. Funk Software's Odyssey Client with xSec support is available for Windows 2000 and Windows XP.

DEPLOYMENT SCENARIOS

xSec is deployed by activating the xSec software license on an Aruba mobility controller and by installing Funk Software's Odyssey Client on a wired or wireless PC. xSec can be used to secure traffic between an Aruba mobility controller and a wireless client, between an Aruba mobility controller and a wired client, or between two Aruba mobility controllers on the same VLAN.



Configuring client to use xSec encryption on SSID "company"



xSec-Secured Site-to-Site Connectivity on the Same VLAN

FEATURE

BENEFIT

Multicast Support

- Supports group keys and sends only one packet when performing multicast; Minimizes unnecessary "chatter" on the network and improves network performance.

Path MTU (Maximum Transmission Unit) Discovery

- Includes MTU discovery as part of the protocol operating at Layer 2; Important in wireless networks where large packet fragments can be more problematic.

Built-In Keepalive

- Provides a method of determining if a device has left the network that is more reliable and accurate than ICMP, especially with personal firewalls.

Built-In Redundancy Methods

- Offers a clean method of handling multicast discovery protocols with redundancy; way of interacting with two switches that respond to one multicast discovery probe.

Built-In Out-of-Order Packet Delivery Mechanism

- Encrypts packet fragmentation information, thereby stopping a malicious user from intercepting and replaying packets in the wrong order to mount a denial of service (DoS) attack.