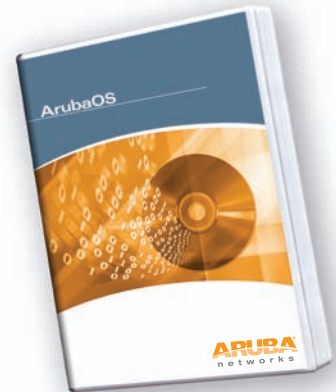




## MÓDULO XSEC ARUBAOS

xSec es un protocolo extremadamente seguro de capa de enlace de datos (capa 2) que proporciona un entorno de trabajo unificado para asegurar todas las conexiones conectadas por cable e inalámbricas mediante un cifrado y una autenticación muy potentes. xSec ofrece un mecanismo conforme con el estándar FIPS (Federal Information Processing Standard) para conferir una seguridad basada en identidad a las agencias gubernamentales y a las entidades comerciales que transmiten información altamente sensible a través de redes inalámbricas. xSec aporta más seguridad que otras tecnologías de cifrado de capa 2, porque utiliza claves más largas, algoritmos de cifrado validados por FIPS (AES-CBC-256 con HMAC-SHA1) y cifrado de la información de cabecera de capa 2, incluyendo las direcciones MAC. xSec ha sido desarrollado conjuntamente por Aruba Networks y Funk Software, una división de Juniper Networks.



### MARCO DE SEGURIDAD UNIFICADO

- Autenticación y cifrado universales para usuarios conectados por cable e inalámbricos, con independencia del método de acceso a la red

### VALIDACIÓN FIPS

- Conformidad y certificación FIPS 140-2

### PROTECCIÓN DE LA INVERSIÓN ANTERIOR

- La solución de cliente basada en software significa que no es necesario reemplazar los puntos de acceso inalámbricos anteriores ni las tarjetas NIC

### DISEÑADO PARA LA COMPATIBILIDAD

- Basado en el marco IEEE 802.1x con soporte de todos los métodos EAP seguros

### PROTECCIÓN CONTRA AP MALICIOSOS

- Detección, localización y contención automática de los AP maliciosos

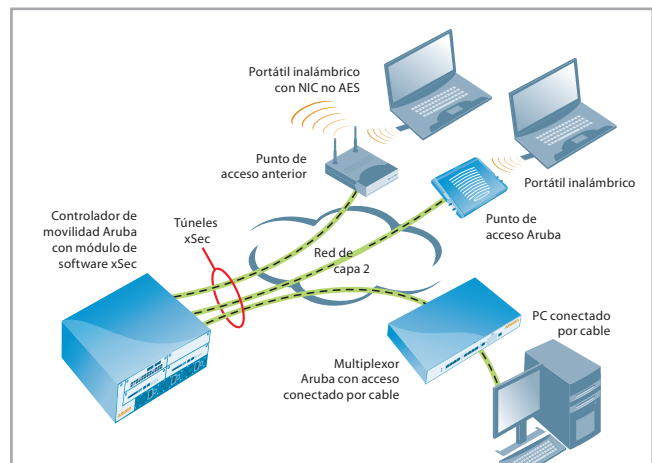
### LA NECESIDAD DEL CIFRADO DE CAPA 2

Tradicionalmente, el cifrado se ha efectuado en la capa 3 (capa de red) en forma de IPsec. El IPsec utiliza el cifrado 3DES o AES y puede cifrar el paquete IP, incluyendo las direcciones IP fuente y destino de la cabecera. El IPsec supone un método de comunicación seguro y ampliamente aceptado a través de redes que no son de confianza, puesto que la única información que no se cifra son las cabeceras de los paquetes y el tráfico puro de capa 2, como es el caso de los paquetes ARP (Address Resolution Protocol) y DHCP (Dynamic Host Configuration Protocol).

Si bien no se cuestiona la confidencialidad de los datos cifrados con IPsec, existe la posibilidad de que un atacante con acceso directo a la capa de enlace de los otros dispositivos de la red pudiera efectuar ataques contra dichos dispositivos. Por ejemplo, una red inalámbrica asegurada con WEP e IPsec podría poner en riesgo los dispositivos cliente, si un atacante obtiene la clave WEP y consigue el acceso de capa 2 para acceder a la red. Asimismo, a muchos colectivos dedicados a la seguridad les preocupa el hecho de que la

información de cabecera del paquete quede expuesta, porque podría utilizarse como la base para un ataque.

Por este motivo, numerosas agencias gubernamentales y entidades comerciales obligan a desplegar potentes tecnologías de cifrado de capa 2 para garantizar la confidencialidad absoluta de los datos. Muchas agencias de defensa requieren que todos los datos transmitidos a través de dispositivos inalámbricos comerciales estén cifrados en la capa 2. Los motores criptográficos utilizados en todas las comunicaciones sensibles del gobierno de los Estados Unidos de-



Conectividad de dispositivos conectados por cable e inalámbricos mediante xSec

ben estar validados conforme cumplen los requisitos del estándar FIPS 140-2. En este sentido, xSec se ha diseñado pensando específicamente en dicho requisito, pero además ofrece un gran número de ventajas adicionales.

### MARCO DE SEGURIDAD UNIFICADO

xSec habilita la autenticación y el cifrado universales, con independencia del método de acceso. Todos los clientes que se conectan a la red, ya sea inalámbrica o conectada por cable, pueden autenticarse en un controlador de movilidad Aruba mediante un cliente xSec. La autenticación dentro del proto-

## MÓDULO XSEC ARUBAOS

colo xSec se lleva a cabo con el protocolo 802.1x EAP (Extensible Authentication Protocol) estándar y con un servidor RADIUS estándar que se encargan de validar las credenciales. xSec soporta autenticación mediante contraseñas, certificados, tarjetas inteligentes, tarjetas token y otras credenciales compatibles con el tipo de EAP seleccionado.

### VALIDACIÓN FIPS

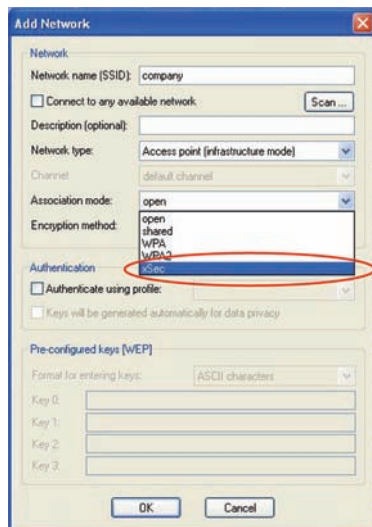
Puesto que en el cifrado utiliza el AES-CBC con una clave de 256 bits, xSec ofrece el único protocolo COTS (Commercial Off-the-Shelf) de capa 2 con validación FIPS. Por consiguiente, xSec es la solución perfecta para las aplicaciones sensibles a la seguridad de los mercados gubernamentales, financieros y sanitarios. FIPS es un estándar de seguridad más riguroso que los que se necesitan en el sector comercial y, por tanto, resulta más adecuado para conseguir la conformidad con las normativas comerciales como HIPAA y GLBA.

### PROTECCIÓN DE LA INVERSIÓN ANTERIOR

La mayoría del equipamiento anterior no se puede actualizar para soportar los estándares de seguridad más recientes como 802.11i y WPA2. No obstante, el cifrado xSec se realiza por hardware en el controlador de movilidad Aruba y en software, a nivel de cliente, por lo que sí es posible actualizar la red existente para que soporte la tecnología de seguridad más novedosa sin tener que reemplazar los puntos de acceso anteriores o las NIC (network interface cards) inalámbricas.

### DISEÑO PARA LA COMPATIBILIDAD

xSec se basa en el estándar de seguridad IEEE 802.1x. Los métodos EAP seguros soportados son EAP-TLS, TTLS y PEAP, por lo que xSec es compatible con los mecanismos de seguridad existentes como los tokens RSA y los certificados PKI. El diseño del xSec es transparente para la infraestructura de capa 2 y el módulo puede operar a través de una red Ethernet conmutada sin correr el riesgo de que las tramas EAP sean interceptadas por los conmutadores Ethernet con reconocimiento de 802.1x. Odyssey Client de Juniper Networks con soporte de xSec está disponible para Windows 2000, Windows XP y Windows Mobile.



Configuración del cliente para utilizar el cifrado xSec en el SSID "company"



Odyssey Client conectado al SSID "alpha-xsec" mediante el protocolo xSec

### ESCENARIOS DE DESPLIEGUE

xSec se despliega con la activación de la licencia de software xSec en un controlador de movilidad Aruba y con la instalación del Odyssey Client de Juniper Networks en un PC conectado por cable o inalámbrico. xSec sirve para asegurar el tráfico entre un controlador de movilidad Aruba y un cliente inalámbrico, entre un controlador de movilidad y un cliente conectado por cable o bien entre dos controladores de movilidad de la misma VLAN.



[WWW.ARUBANETWORKS.COM](http://WWW.ARUBANETWORKS.COM)

1322 Crossman Avenue, Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550