MECANISMOS DE SEGURIDAD

WEP (Wired Equivalent Protocol)

El protocolo WEP es un sistema de encriptación estándar propuesto por el

comité 802.11, implementada en la capa MAC y soportada por la mayoría de

vendedores de soluciones inalámbricas. En ningún caso es comparable con IPSec. WEP

comprime y cifra los datos que se envían a través de las ondas de radio.

Con WEP, la tarjeta de red encripta el cuerpo y el CRC de cada trama 802.11

antes de la transmisión utilizando el algoritmo de encriptación RC4 proporcionado por

RSA Security. La estación receptora, sea un punto de acceso o una estación cliente es la

encargada de desencriptar la trama.

OSA (Open System Authentication)

Es otro mecanismo de autenticación definido por el estándar 802.11 para

autentificar todas las peticiones que recibe. El principal problema que tiene es que no

realiza ninguna comprobación de la estación cliente, además las tramas de gestión son

enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable.

3.3 ACL (Access Control List)

Este mecanismo de seguridad es soportado por la mayoría de los productos

comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada

estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de

Control de Acceso.

3.4 CNAC (Closed Network Access Control)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo

solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID)

actuando este como contraseña.