Universidad Autónoma de Baja California

Facultad de Ingeniería Ensenada

"Metodología para implementar mecanismos de autenticación y seguridad en redes inalámbricas"

Tesis
Que para obtener el título de
Maestra en Ingeniería en Computación
Presenta:

Perla Karina Barba Rojo

Ensenada Baja California, Agosto de 2007

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA
UNIDAD ENSENADA

"METODOLOGÍA PARA IMPLEMENTAR MECANISMOS DE AUTENTICACIÓN Y SEGURIDAD EN REDES INALÁMBRICAS"

TESIS

Que para obtener el grado de maestría en ingeniería presenta:

PERLA KARINA BARBA ROJO

Aprobada por:

M.C. Raúl Tamayo Fernández
Director de tesis

Dr. Juan Ivan Nieto Hipolito
Miembro del comité

M.C. Christian X. Navarro Cota
Miembro del comité

M.C. Elitania Jiménez García
Miembro del comité

Ensenada Baja California, México. Agosto 2007

Contenido

Lista de Figuras

Lista de Tablas

I. Introducción

I.1 Antecedentes

En 1997, un comité del Instituto de Ingenieros Eléctricos y Electrónicos [IEEE] desarrolló los estándares IEEE 802.11 como una familia de especificaciones para comunicaciones inalámbricas (Craiger, 2002). El alcance de estos estándares es desarrollar una especificación del control de acceso al medio [MAC] y de la capa física [PHY] (Figura I.1) para ofrecer conectividad inalámbrica a estaciones fijas, portables y en movimiento dentro de un área local (IEEE, 1999). IEEE 802.11 forma parte de la familia de estándares para redes de área local y metropolitana (Figura I.1). Este estándar define las funciones y servicios requeridos por los dispositivos compatibles con IEEE 802.11 (IEEE, 1999). Existen varias especificaciones dentro de la familia de IEEE 802.11 como: IEEE 802.11 (provee 1 ó 2 Mbps de transmisión en la banda de 2.4 GHz), IEEE 802.11a (54 Mbps en la banda de 5 GHz), IEEE 802.11b (11 Mbps en la banda de 2.4 GHz) y IEEE 802.11g (54 Mbps a 2.4 GHz).

I.1.1 Riesgos de Seguridad

Es importante definir algunos de los posibles riesgos de seguridad que las redes inalámbricas con estándar IEEE 802.11 deben de afrontar. Todas las redes, cableadas o inalámbricas están expuestas a dos tipos de ataques: activos (obtienen acceso a la red para destruir o modificar información transmitida) y pasivos (obtienen acceso solo para

"espiar" la información transmitida (Psion-Teklogix, 2003). Las redes inalámbricas IEEE 802.11 envían los datos a través del aire en forma de ondas de radio, y puedes ser accesible desde fuera de los límites físicos de una organización. Son vulnerables a diferentes tipos de ataques como intercepción de datos, capturado de señales de radio, inserción de usuarios y equipos de red no autorizados, interrupción de servicios, entre otros (García-López, 2003)

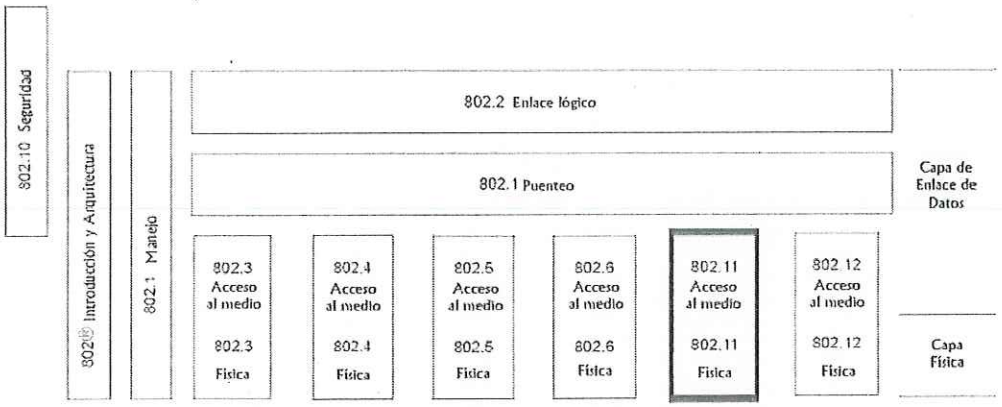


FIGURA I.1 - FAMILIA DE ESTÁNDARES PARA REDES DE ÁREA LOCAL Y METROPOLITANA. (IEEE, 1999)

I.1.2 IEEE 802.11: Mecanismos de Seguridad

Las redes IEEE 802.11, por su tipo de difusión, requieren de mecanismos de seguridad tales como: autenticación de usuarios y protección de la confidencialidad e integridad en la información (Cisco, 2002). Los mecanismos de seguridad que ofrecen los estándares IEEE 802.11 están compuestos por dos métodos de autenticación y un protocolo de cifrado (Cisco, 2002):

- *Autenticación de Sistema Abierto [OSA].* Este protocolo permitirá el acceso a cualquiera que solicite autenticación (Arbaugh *et al.*, 2001). OSA involucra una secuencia de transacción de la autenticación en dos pasos (IEEE, 1999): el primer paso es la petición de autenticación y el segundo paso corresponde a la respuesta de autenticación, en donde el resultado siempre será "Aceptada" (Figura I.2).

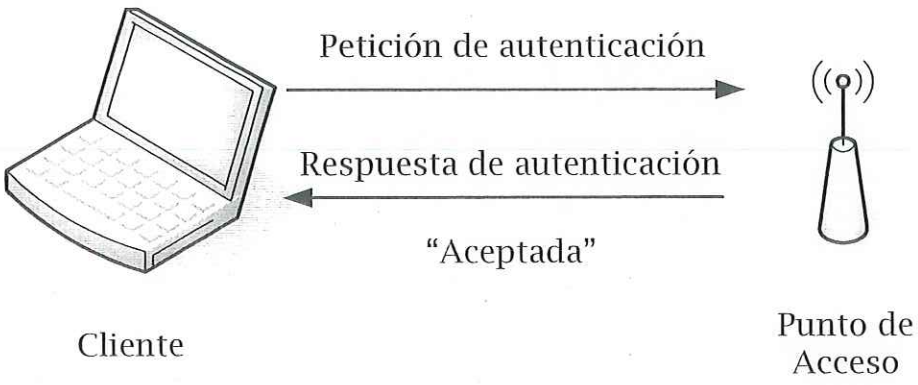


FIGURA I.2 - AUTENTICACIÓN DE SISTEMA ABIERTO.

- *Autenticación de Llave Compartida [SKA].* Requiere que los clientes tengan configurada una llave WEP (Cisco, 2002), la cual deberá ser la misma tanto en el cliente como en el punto de acceso. Este método consiste en cuatro mensajes: petición de autenticación, reto, respuesta al reto (cifrándolo mediante la llave WEP) y aceptación o negación de la autenticación (Figura I.3).

- *Protocolo Equivalente a Privacidad Cableada [WEP].* Diseñado para proveer el mismo nivel de seguridad que una red cableada. Este utiliza el algoritmo de

cifrado simétrico RC4 de *RCA Data Security Inc.* para cifrar y descifrar las transmisiones realizadas por aire. WEP trata de garantizar tres metas principales (Borisov et al., 2001): confidencialidad, control de acceso e integridad de los datos.

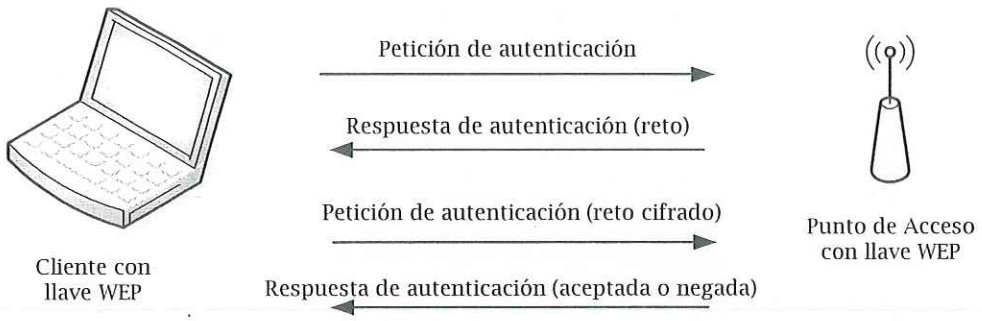


FIGURA I.3- AUTENTICACIÓN DE LLAVE COMPARTIDA.

I.1.3 IEEE 802.11: Vulnerabilidades

La vulnerabilidad de los diferentes métodos de seguridad proporcionados por IEEE 802.11 ha sido expuesta detalladamente en varios artículos y publicaciones tales como:

- Borisov, N., I. Goldberg, y D. Wagner, "*Intercepting Mobile Communications: The Insecurity of 802.11*", 2001 y Scott Fluhrer, Itsik Mantin, Adi Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", 2001. Los cuales muestran las vulnerabilidades del algoritmo de cifrado simétrico RC4 y la forma

en que es usado en WEP, además demuestran como WEP falla en cumplir sus metas de seguridad.

- Arbaugh, W. A., N. Shankar, y Y. C. J. Wan "*Your 802.11 Wireless Network Has No Clothes*", 2001. Describe características de IEEE 802.11 que lo exponen a diferentes ataques. En este artículo los autores se enfocan en presentar las debilidades de los protocolos de autenticación y de control de acceso utilizados por los estándares IEEE 802.11; así mismo proponen métodos para mitigar estas vulnerabilidades. Algunos de los métodos propuestos incluyen un sistema de manejo de llaves para WEP más robusto o el uso de mecanismos de seguridad de nivel más alto como IPsec.

Debido al gran crecimiento en el uso de las redes inalámbricas IEEE 802.11 y las debilidades de sus mecanismos de seguridad, ha sido necesario el desarrollo de nuevos métodos para proteger las transmisiones inalámbricas (Craiger, 2002). Organizaciones como Cisco Systems y Fortress Technologies se han involucrado en el desarrollo de soluciones de seguridad más robustas alrededor de tecnologías basadas en estándares (Psion-Teclogix, 2003). La solución más común de empresas e instituciones como alternativas a WEP ha sido el uso de Redes Privadas Virtuales [VPN], aunque esta tecnología no haya sido específicamente diseñada para el caso de redes inalámbricas y tener como inconveniente la difícil interoperabilidad entre dispositivos de diferentes fabricantes (Sierra et al., 2004).

I.1.4 Introducción a WPA

La Alianza para la Fidelidad Inalámbrica [Wi-Fi Alliance o WFA] en conjunto con la IEEE, han unido esfuerzos para brindar a las redes inalámbricas, mecanismos de seguridad más robustos y que permitan la interoperabilidad entre dispositivos. El resultado de ese esfuerzo es Acceso Protegido a Wi-Fi [WPA] (Wi-Fi-Alliance, 2004a). WPA está basado en el estándar IEEE 802.11i de 2003 (enmienda del estándar IEEE 802.11) antes de ser ratificado por la IEEE (Geier, 2003), y este fue utilizado como una solución provisional a las inseguridades de WEP.

El borrador final del estándar IEEE 802.11i fue ratificado en enero de 2004 y remplazaba las especificaciones de seguridad previas. Wi-Fi Alliance se refiere a su nuevo estándar como WPA2 el cual es su implementación aprobada del IEEE 802.11i.

WPA cuenta con metas tales como ser más robusto, proveer interoperabilidad, ser un reemplazo de WEP, ofrecer actualizaciones de software a los actuales productos certificados por Wi-Fi (Wi-Fi-Alliance, 2004a). Para satisfacer estas metas fue necesario realizar dos perfeccionamientos de seguridad. WPA incluye el Protocolo de Integridad de Llave Temporal [TKIP] y mecanismos IEEE 802.11X, los cuales brindan cifrado de llaves dinámico y autenticación mutua para clientes móviles (Geier, 2003).

- *TKIP*. Ofrece mejoras en el cifrado de la información que incluyen una función de mezclado de llaves por paquete, código de integridad de mensaje [MIC]

conocido como "Michael", un vector de inicialización extendido [IV] con reglas de secuenciado, y un mecanismos para re-generar llaves (Wi-Fi-Alliance, 2004a).

- *Mecanismos IEEE 802.11X.* Para fortalecer la autenticación de usuarios, WPA implementa mecanismos IEEE 802.11X con soporte para el Protocolo de Autenticación Extensible [EAP] o tecnología de Llave Pre-Compartida [PSK] (Vaughan-Nicols, 2003). Esta infraestructura utiliza un servidor de autenticación central como el Servicio de Usuario de Acceso Telefónico de Autenticación Remota [RADIUS], para autenticar usuarios antes de ser aceptados en la red (Wi-Fi-Alliance, 2004a).

I.2 Planteamiento del Problema

Tomando en cuenta las necesidades de las actuales redes inalámbricas, tanto en confidencialidad e integridad de la información transmitida como en el control de acceso, es indispensable el uso de nuevas tecnologías que resuelvan esta problemática. También es importante conocer el funcionamiento, ventajas y desventajas de estos conjuntos de técnicas para seleccionar la más adecuada de acuerdo a los requerimientos exigidos a la red inalámbrica.

I.3 Hipótesis

Es posible generar una metodología que permita la implantación, de manera guiada y sencilla para el administrador de red, de mecanismos de autenticación y seguridad en una red inalámbrica existente.

I.4 Objetivos

I.4.1 Objetivo General

Este trabajo pretende generar una metodología fácil de seguir, que permita la implementación de autenticación y seguridad en una red inalámbrica utilizando la tecnología WPA como herramienta para este fin.

I.4.1 Objetivos Específicos

- Obtener información sobre la metodología utilizada en WPA.
- Analizar los diferentes tipos de autenticación WPA.
- Investigar sobre los componentes necesarios para implementar seguridad en una red inalámbrica con WPA.
- Desarrollar una metodología para implementar autenticación y seguridad en redes inalámbricas.
- Probar la metodología en la red inalámbrica de la Facultad de Ciencias Marinas de la UABC.

I.5 Limitaciones del Estudio

- Sólo se utilizará la tecnología WPA para la metodología propuesta.
- Por no contarse con presupuesto, en la implementación del caso de estudio se llegará hasta la fase del diseño.

II. Conceptos Básicos

II.1 Evolución de las Redes Inalámbricas

Desde sus inicios hasta la actualidad, las redes inalámbricas han ido evolucionando y mejorando las tecnologías de comunicación y de seguridad que ellas operan. Aun así, sigue habiendo problemas tales como ancho de banda, interferencias y seguridad de la información transmitida (Martínez, 2002).

Para observar de una mejor manera el desarrollo de las redes inalámbricas se muestra a continuación un cronograma con los principales hechos que afectaron su evolución, desde una simple idea sobre un sistema de comunicación secreta a través de ondas de radio planteada por un pianista y su esposa.

1942. Una técnica de cifrado de ondas de radio, después llamada tecnología de espectro disperso [SS], fue donada al ejército de Estados Unidos de América por George Antheil (pianista) y Hedy Lamar (actriz).

1958. El ejército de EE.UU. desarrolla el primer chip de computadora para comunicaciones de radio basado en la tecnología clasificada de espectro disperso.

1985. La tecnología de espectro disperso se hace disponible para el comercio.

1989. La FCC (Comisión Federal de Comunicaciones, de EE.UU.) autoriza el uso de la tecnología de espectro disperso en tres bandas de radio.

1990. La IEEE empieza a trabajar en los estándares para la conectividad inalámbrica en las ISM (bandas de frecuencia para uso comercial y sin licencia).

1997.

- La IEEE ratifica el estándar IEEE 802.11, pero no garantiza la interoperabilidad. El mecanismo de seguridad que utiliza es WEP.
- La FCC agrega cuatro bandas sin licencia para uso comercial.

1999

- La IEEE ratifica los estándares IEEE 802.11b y IEEE 802.11a.
- La WECA (Alianza para la Compatibilidad de Ethernet Inalámbrico) se organiza para certificar la interoperabilidad de IEEE 802.11.

2000. La WECA lanza el programa de certificación para productos IEEE 802.11b.

2001

- Los investigadores Scott Fluhrer, Itsik Mantin, y Adi Shamir encuentran vulnerabilidades en el algoritmo RC4 utilizado por WEP.

- Soluciones de seguridad como IPSec o VPN son utilizadas en redes inalámbricas.
- La FCC modifica sus reglas para dar cabida al desarrollo de dispositivos IEEE 802.11g.

2002

- WECA se convierte en la Alianza Wi-Fi (WFA) y empieza las pruebas de certificación de productos IEEE 802.11a.
- IEEE 802.1X es ratificado por la IEEE.
- WFA empieza a desarrollar WPA para ser el reemplazo de WEP.

2003

- La WFA certifica productos WPA.
- La IEEE ratifica el estándar IEEE 802.11g.
- El uso de WPA se hace imperativo como parte del proceso de certificación Wi-Fi.

2004. IEEE 802.11i es ratificado por la IEEE como estándar para proporcionar seguridad en redes inalámbricas. WFA lo reconoce como WPA2.

II.2 Seguridad en las Redes Inalámbricas

Desde el primer estándar para el control de acceso al medio y de la capa física para ofrecer conectividad inalámbrica a estaciones fijas, portables y en movimiento dentro de un área local se ha manejado la idea se ofrecer seguridad en la información transmitida, todo esto garantizando la confidencialidad e integridad de la información, así como la autenticación de usuarios. Este primer estándar (IEEE 802.11) planteaba el uso de SKA para la autenticación y WEP como mecanismo que protegía la integridad y confidencialidad de los datos. Como ya se planteo en la introducción de este documento, WEP demostró ser inseguro al encontrarse en el agujeros de seguridad, los que permitían ataques como: ataques de escucha o monitorización pasiva (eavesdropping), ataques de intercepción-inserción (man-in-the-middle), ataques de denegación de servicio (jamming o DoS), entre otros. En ese momento WEP fue considerado un protocolo roto (*Broken protocol*).

Algunas soluciones provisionales (Wong, 2003) que se adoptaron para remediar la inseguridad descubierta en WEP fueron tecnologías tales como:

- *Llaves WEP Extendidas:* En 1998, la compañía Lucent fue pionera en sacar una llave WEP de 128 bits. Con esta mejora los posibles atacantes tendrían que tomar más tiempo en romper la llave WEP. Aun así, esta solución no fue de mucha ayuda ya que los hoyos de seguridad seguían. US Robotics también saco sus propias llaves WEP, de 152 y 256 bits.

- *Llave WEP dinámica:* Algunas compañías como Cisco ý Microsoft, implementaron puntos de acceso con re-generación de llaves WEP dinámicas. Las llaves tenían un tiempo de vida corto lo que podría resultar en que el atacante no colectara suficiente información para romper la llave WEP.

- *VPN:* En este caso se trataba a la red inalámbrica como una red pública insegura (Earle, 2005), tal como Internet. El cliente de la red inalámbrica debería realizar una sesión VPN con un firewall, gateway o concentrador VPN. La red privada virtual debía utilizar alguna tecnología para proporcionar seguridad. Algunas de las tecnologías utilizadas en las redes inalámbricas VPN son: túneles IPSec, Protocolo de la Asociación de Seguridad de Internet y Manejo de Llaves [ISAKMP], Intercambio de Llaves de Internet [IKE], Encabezado de autenticación IP [AH], entre otras.

Algunas de estas implementaciones logran resolver las vulnerabilidades de WEP, aunque por ser soluciones propietarias no logran una buena interoperabilidad. Para resolver esta problemática la WFA lanza en octubre del 2003 (Wi-Fi-Alliance, 2005) la tecnología WPA o Acceso Protegido a Wi-Fi, basado en el borrador de la especificación IEEE 802.11i, aunque algunas piezas de este como IBSS [Conjunto de Servicios Básicos Independientes], de-autenticación, disasociación, o protocolos avanzados de cifrado como AES - CCMP [Advance Encryption Standar - Counter-Mode/CBC-MAC Protocol] no fueron incluidos (Wi-Fi-Alliance, 2004a). WPA logro resolver las

vulnerabilidades de WEP, además de incluir un método de autenticación de grado empresarial, así como un sistema de distribución de llaves automática y re-generación de llaves. Para el septiembre del siguiente año y ya ratificada la especificación IEEE 802.11i, la WFA lanza el programa WPA2, el cual fue la versión certificada por este grupo, del estándar IEEE 802.11i y que incluía el método de cifrado AES - CCMP. En la Tabla II.1 se muestra un comparativo de las tecnologías utilizadas para cifrado y autenticación de los métodos de seguridad desde el inicio de las redes inalámbricas hasta la fecha. En esta tabla se puede visualizar como la tendencia para mejorar la seguridad del cifrado de llaves es a la generación dinámica de llaves que sea única para cada usuario y para cada paquete. También podemos observar que los métodos de autenticación están dirigidos a usuarios y no a equipos como en WEP. Otra diferencia de los nuevos métodos WPA y WPA2 contra WEP es que estos tienen la posibilidad de trabajar en dos modos, modo empresarial y modo personal. En el modo empresarial utiliza como método de autenticación de IEEE 802.11X/EAP y el modo personal utiliza la llave pre-compartida [PSK].

II.3 WPA

WPA vino a resolver los problemas de seguridad de su antecesor WEP y está diseñado para poder ser usado bajo los equipos WEP existentes actualizando solamente su software. WPA utiliza el protocolo de llave temporal [TKIP] para proporcionar un mejor cifrado de información a través de una función de mezclado de llaves por paquete y del código de integridad de mensaje [MIC], y un vector de inicialización [IV]

asegurado con reglas de secuenciado y un mecanismo de re-generación de llaves (Wi-Fi-Alliance, 2004a). Para fortalecer la autenticación de usuarios, WPA implementa IEEE 802.1X y el Protocolo de Autenticación Extensible [EAP]. Esta infraestructura utiliza un servidor central de autenticación, como RADIUS, para autenticar cada usuario antes de agregarse a la red, también se vale de la "autenticación mutua" para prevenir que algún usuario, accidentalmente sea agregado a una red.

Características	IEEE 802.11	WPA	WPA2
Cifrado			
Algoritmo de Cifrado	WEP (RC4)	TKIP (RC4)/MIC	CCMP (AES)
Longitud	40 bits	128 bits	128, 192 y 256 bits
Generación llave	Estática, la misma para todos los dispositivos.	Dinámica: por usuario, por sesión, por paquete.	Dinámica: por usuario, por sesión, por paquete.
Distribución llave	Manual, en cada dispositivo.	Automática, gestionada por IEEE 802.1X/EAP.	Automática, gestionada por IEEE 802.1X/EAP
Autenticación			
Entorno	Definido por IEEE 802.11	IEEE 802.1X/EAP	IEEE 802.1X/EAP
Método	Abierta/Llave compartida (autentifica el equipo)	EAP-TLS, PEAP, EAP-TTLS (autentifican al usuario) / PSK	EAP-TLS, PEAP, EAP-TTLS (autentifican al usuario) / PSK

TABLA II.1 - COMPARACIÓN DE CARACTERÍSTICAS DE SEGURIDAD PROPORCIONADAS POR IEEE 802.11, WPA Y WPA2

II.3.1 Tipos de WPA

WPA maneja dos modos o tipos, dependiendo del tipo de instalación que se requiera.

- *Modo empresarial.* Basado en un protocolo de autenticación por usuario en combinación con la infraestructura de seguridad IEEE 802.1X, servidor de autenticación, manejo de llaves con TKIP y Michael, dirigido a ambientes empresariales.

Modo Personal o SOHO. Basado en el protocolo de llave pre-compartida en combinación con TKIP y Michael, dirigido para pequeñas oficinas o redes personales.

II.4 Seguridad en Pequeñas Oficinas

Los métodos soportados por EAP necesitan de una cierta infraestructura, fundamentalmente de un servidor RADIUS, lo que puede limitar o dificultar la instalación en una red pequeña. Para resolver o facilitar la instalación de WPA en estos casos, se proporciona la opción de utilizar el modo personal o de pequeña oficina [SOHO], el cual usa la llave pre-compartida [PSK o pre-shared key]. Esto da la posibilidad de configurar TKIP manualmente con una llave en el cliente de la red inalámbrica y el punto de acceso (García-López, 2003).

Las tareas esenciales de este modo son (Takahashi, 2004):

1. Asociación con el punto de acceso.
2. Autenticación y distribución de la llave maestra [PMK].
3. Creación e instalación de la llave derivada [PTK] basada en la PMK.

4. Chequeo de integridad.
5. Sesión satisfactoria usando TKIP.

II.4.1 Vulnerabilidades de PSK

En noviembre de 2003, Robert Moskowitz, director técnico mayor de los laboratorios ICSA, publico el articulo "*Weakness in Passphrase Choice in WPA Interface*", en donde describía como podía ser llevado a cabo un ataque de diccionario a las redes WPA-PSK. Así mismo Takehiro Takahashi, estudiante en Georgia Tech lanzo el "WPA Craker", y Josh Wright, ingeniero de redes, realizó coWPAtty, ambas herramientas para realizar un ataque de diccionario por la fuerza bruta a WPA-PSK (MacMichael, 2005).

II.5 Cifrado: TKIP

TKIP o Protocolo de Integridad de Llave Temporal es un protocolo de encriptación que intenta corregir los problemas de WEP sin realizar cambios en el hardware (únicamente sería necesario una actualización del firmware). Fue desarrollado por los mismos investigadores que encontraron las vulnerabilidades en el uso del algoritmo RC4 (InformIT, 2005), y fue inicialmente llamado WEP2 (Gast, 2005), pero fue cambiado para que no ser asociado con la seguridad de WEP. Algunas de las técnicas utilizadas para remediar esas vulnerabilidades incluyen una función de mezclado por paquete, un vector de inicialización extendido [IV] con reglas de secuenciado y un código de integridad de mensaje [MIC].

II.5.1 Mejoras de TKIP contra WEP

A continuación se muestra las vulnerabilidades de WEP y como TKIP lo soluciona (Microsoft-TechNet, 2004):

- *IV demasiado corto.* TKIP utiliza un IV del doble de tamaño que WEP (48 bits).
- *Integridad de la información débil (CRC-32).* Remplaza CRC-32 con el algoritmo Michael. Este calcula un código de integridad de mensaje [MIC] de 64 bits, el cual es cifrado en TKIP.

- *Uso de la llave maestra en lugar de la derivada.* TKIP y Michael usan un conjunto de llaves temporales derivadas de la llave maestra y otros valores. La llave maestra es derivada de EAP-TLS o PEAP. Además, la parte secreta de la entrada a RC4 Pseudo Generador de Números Aleatorios [PRNG] es cambiada en cada trama a través de una función de mezclado de paquetes.

- *No existe la re-generación de llaves.* Automáticamente re-genera las llaves para obtener un nuevo grupo de llaves temporales.

- *No tiene protección contra replay.* TKIP usa el vector de inicialización IV para proporcionar protección contra el ataque de replay.

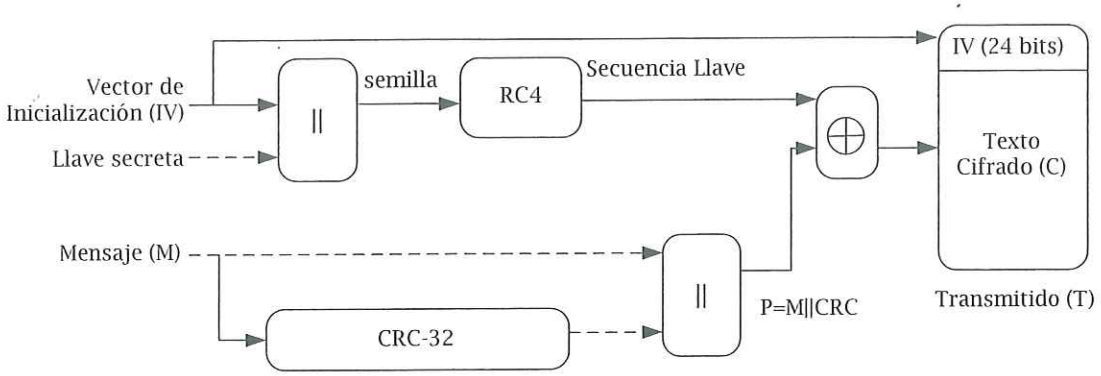


FIGURA II.1 - PROCESO DE CIFRADO CON WEP.

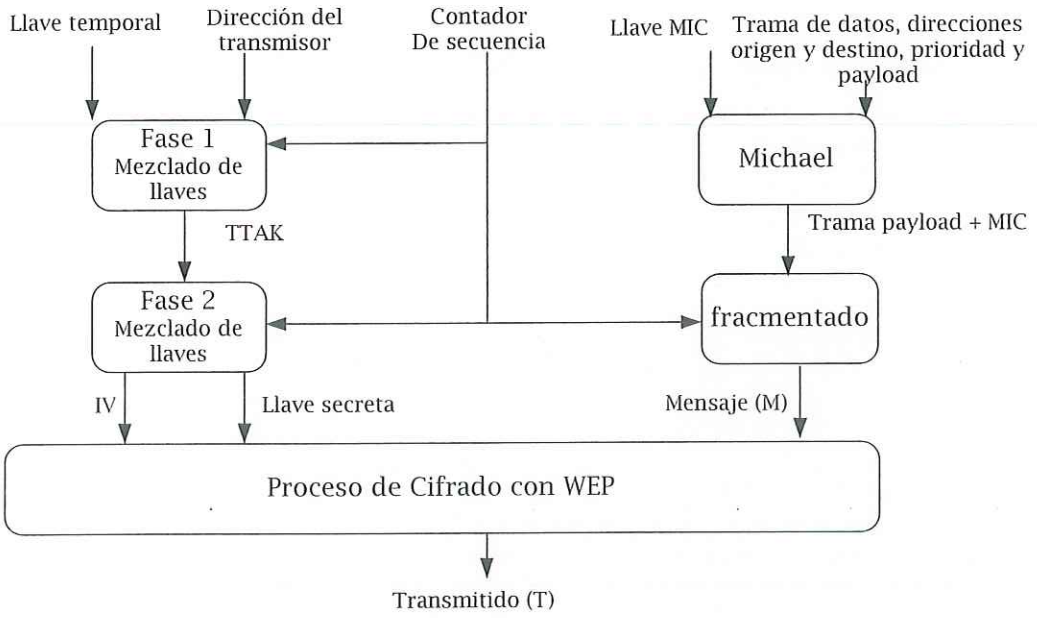


FIGURA II.2 - PROCESO DE CIFRADO CON TKIP.

Al igual que WEP, TKIP proporciona soporte para cifrado y protección de la integridad de la información como parte del mismo proceso (Figuras II.1 y II.2). Los datos de entrada de TKIP son (Gast, 2005): la trama de datos en claro, la llave MIC que en conjunto con Michael son usados para proteger el contenido de la trama de datos, la

dirección del transmisor, un contador de secuencia y la llave temporal usada para cifrar la trama de datos.

El mezclado de llaves consiste en la generación de una llave única para cada trama de datos transmitida [PPK]. Esta llave es derivada del vector de inicialización (contador de secuencia), la dirección del transmisor y la llave temporal. La salida de esta función es una llave WEP de 128 bits, en la cual 24 bits son derivados de IV. El mezclado de llaves es un proceso que consta de dos fases (Moen, 2004). En la fase 1 consiste en simples operaciones ('o' exclusivo, adiciones, cambios de bits) lo que reduce la carga al procesador y se obtiene un valor de 80 bits (TTAK), esta fase solo es realizada en una de cada 65,536 tramas de datos (Gast, 2005). La fase 2 del mezclado de llaves debe realizarse para cada trama de datos. Esta recibe el resultado de la fase 1, así como la llave temporal y los 16 últimos bits del contador de secuencia. La salida de esta fase es una llave RC4 de 128 bits, en donde los últimos 16 bits son usados como IV del proceso de cifrado WEP.

El punto más vulnerable en WEP era la protección de la integridad de la información (Gast, 2005), el cual aseguraba que el mensaje no había sufrido algún cambio durante la transmisión. WEP trataba de resolver ese problema mediante un chequeo de redundancia cíclica [CRC] el cual fue probado, encontrando en el, deficiencias en la resolución de tal problema. TKIP utiliza la función Michael (algoritmo diseñado por el ingeniero en criptografía Niels Ferguson) para ofrecer un mejor resultado en la protección de la integridad de la información transmitida (Ferguson,

2002). Esta función toma como entrada (Moen, 2004): una llave MIC, direcciones del destino y origen, y el mensaje (Figuras II.2); la salida de la función es el mensaje concatenado con la etiqueta MIC, si es necesario es fragmentada antes de entrar al proceso de WEP.

II.6 Autenticación: IEEE 802.1X

IEEE 802.1X (IEEE, 2001) es un estándar para autenticación basado en puertos (Port-Based Network Access Control), lo que significa que trabaja en la capa dos. Puede ser utilizado en cualquier red IEEE 802, incluyendo Ethernet, Token Ring, y redes inalámbricas IEEE 802.11 (Congdon, et al., 2003). IEEE 802.1X brinda un diseño modular, escalable y centralizado de control de acceso a la red basado en puertos (Haryanto, 2004), el cual mantiene los puertos de los servicios de red deshabilitados hasta que la autenticación se realiza satisfactoriamente (Figuras II.3 y II.4).

El estándar IEEE 802.1X es una adaptación IEEE del Protocolo de Autenticación Extensible [EAP], originalmente especificado in el RFC 2284 y actualizado por el RFC 3748. EAP es un protocolo de infraestructura que soporta múltiples métodos de autenticación, por lo que en lugar de especificar como autenticar usuarios, EAP permite a los diseñadores crear su propio método o subprotocolo que realice la autenticación (Gast, 2005).

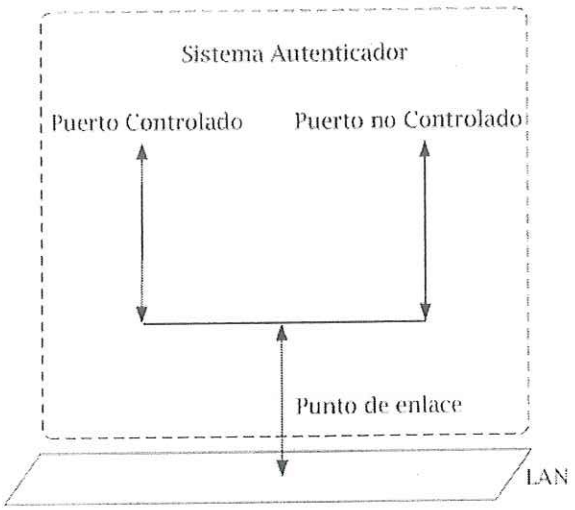


FIGURA II.3 - PUERTOS CONTROLADOS Y NO CONTROLADOS (IEEE, 2001).

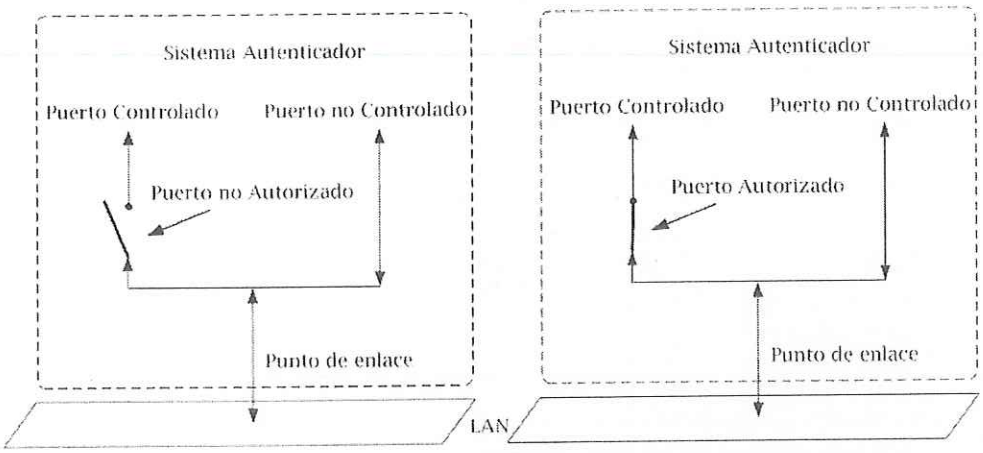


FIGURA II.4 - EFECTO DEL ESTADO DE AUTORIZACIÓN EN LOS PUERTOS CONTROLADOS (IEEE, 2001).

II.6.1 Componentes de IEEE 802.1X

Para poder describir el proceso de autenticación de IEEE 802.1X es necesario conocer las definiciones de los diferentes componentes que utiliza. Estos son, un suplicante, un autenticador y un servidor de autenticación, tal como se muestran en la Figura II.5.

Suplicante o solicitante. Es la aplicación cliente que reside en la estación y que proporciona la información de las credenciales al autenticador (García-López, 2003). Es definido por la IEEE como el puerto que desea acceder a los servicios que ofrece el sistema autenticador (IEEE, 2001). Algunos ejemplos de suplicantes son: la infraestructura EAP para Microsoft Windows [incluida en Windows XP y Windows 2000], la infraestructura de EAP para Apple OS X [incluida en Mac OS X 10.3+], SecureW2, Funk Odyssey, Meetinghouse AEGIS, wpa_supplicant, Xsupplicant y Wire1x.

Autenticador. Es el dispositivo de red que toma la información proporcionada por el suplicante, y la traslada en el formato necesario por el servidor de autenticación. Es definido por la IEEE como el puerto que obliga a realizar la autenticación antes de permitir el acceso a los servicios que ofrece el sistema autenticador (IEEE, 2001). Este rol es desempeñado por un punto de acceso.

Servidor de Autenticación. Es definido por la IEEE como el servidor que realiza la función de autenticación necesaria para verificar si las credenciales proporcionadas por el usuario e indica si el suplicante es autorizado o no, a acceder a los servicio ofrecidos por el sistema autenticador (IEEE, 2001). El ejemplo más común para un servidor de autenticación es RADIUS, aunque existen otros como TACACS, TACACS+, o DIAMETER (Haryanto, 2004).

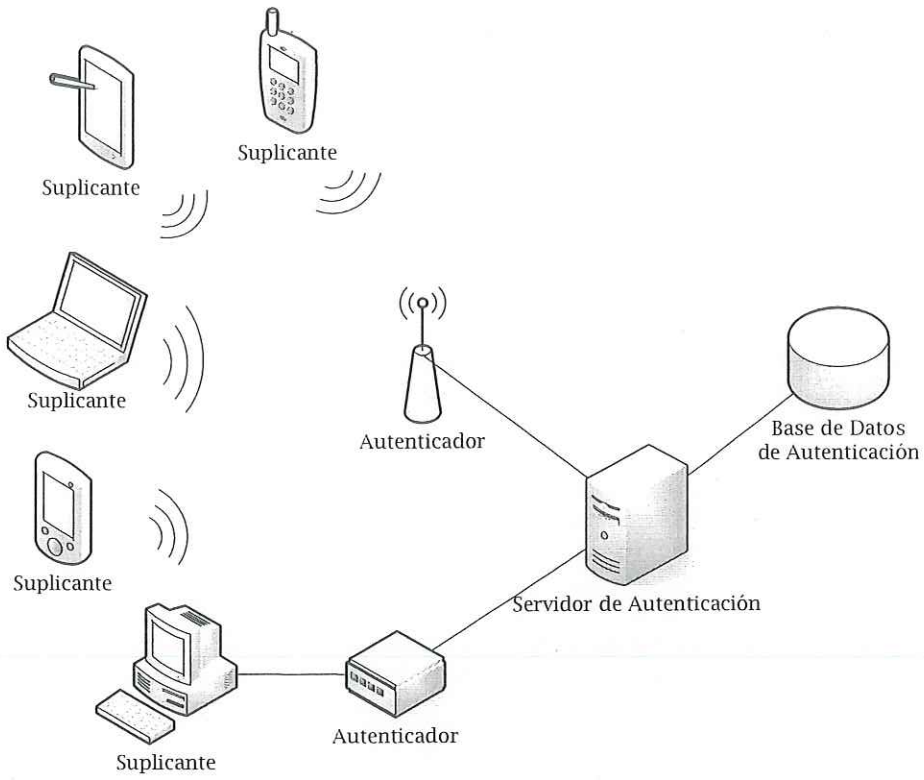


FIGURA II.5 - COMPONENTES DE IEEE 802.1X

Entidad de Acceso al Puerto [PAE]. Es el componente lógico de IEEE 802.1X que se encuentra en el suplicante y el autenticador para el intercambio de mensajes EAP.

II.6.2 EAP e EAP Sobre LANs [EAPoL]

La infraestructura EAP típicamente es ejecutada sobre la capa de enlace de datos (Figura II.6) tal como en el Protocolo de Punto a Punto [PPP] o IEEE 802, en los que no es necesario un IP (RFC 3748, 2004). Puede ser usadó sobre enlaces dedicados, así como circuitos intercambiados, y tanto en redes cableadas como en inalámbricas. Uno de los avances de la arquitectura EAP es su flexibilidad ya que puede soportar múltiples

mecanismos de autenticación tales como contraseñas, respuestas de retós [challenge response], contraseña de una sola vez [OTP o One Time Pasword], Generic Token Card [GTC], y certificados de infraestructura de llave pública (Haryanto, 2004).

Cada paquete EAP (Figura II.7) puede ser transportado en diferentes tramas. Los campos son código, identificador, longitud y datos (RFC 3748, 2004).

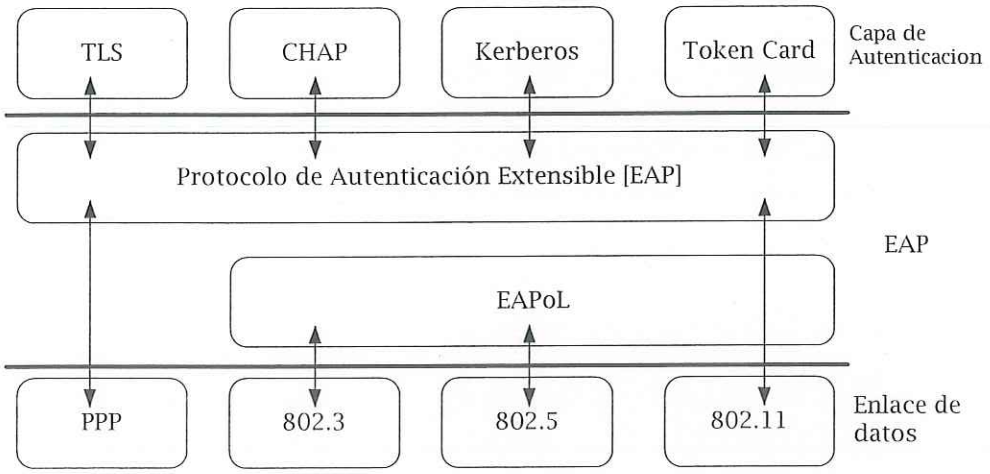


FIGURA II.6 - ARQUITECTURA EAP

- *Código.* Es el primer campo del paquete, su longitud es de un byte e identifica el tipo de paquete EAP. Es usado para interpretar el campo datos. Existen cuatro tipos de paquetes: Petición [Request], Respuesta [Response], Éxito [Success] o Falla [Failure].
- *Identificador.* De longitud de un byte. Contiene un entero sin signo utilizado para unir la petición con la respuesta. La retransmisión usa el mismo identificador.
- *Longitud.* De dos bytes y corresponde al número complete de bytes del paquete.

- *Datos.* El tamaño de este campo depende del tipo de paquete, y su contenido es determinado por el campo código.

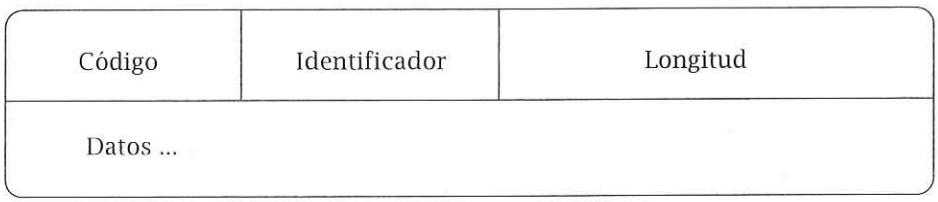


FIGURA II.7 - FORMATO DEL PAQUETE EAP

II.6.3 Proceso de Autenticación de IEEE 802.1X: EAPoL

Una vez terminada la configuración de los dispositivos (clientes y servidores) para trabajar con IEEE 802.1X, el proceso de autenticación puede ser realizado (James, 2002). Antes de la autenticación y para asegurar que ningún tráfico no autorizado sea transmitido, el PAE del autenticador debe ser configurado como no-controlado. Lo que significa que solamente los mensajes EAP de petición o request, serán aceptados y enviados al servidor de autenticación (Figura II.8).

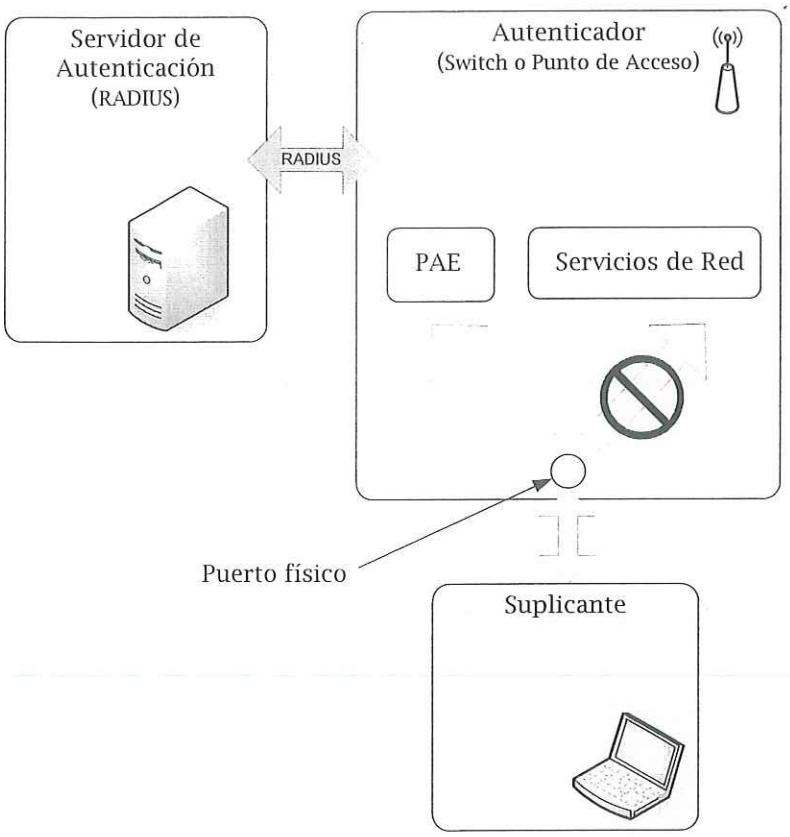


FIGURA II.8 - ESTADO DE LOS PUERTOS ANTES DE LA AUTENTICACIÓN

El proceso de autenticación EAP (Figura II.9) consta de diez pasos principales, en los que intervienen el autenticador, servidor de autenticación y el suplicante (RFC 3748; Snynder, 2002):

1. El autenticador manda un mensaje EAP de Petición [Request/Identity] para autenticar al cliente o suplicante.
2. El suplicante manda el paquete EAP de Respuesta [Response/Identity].

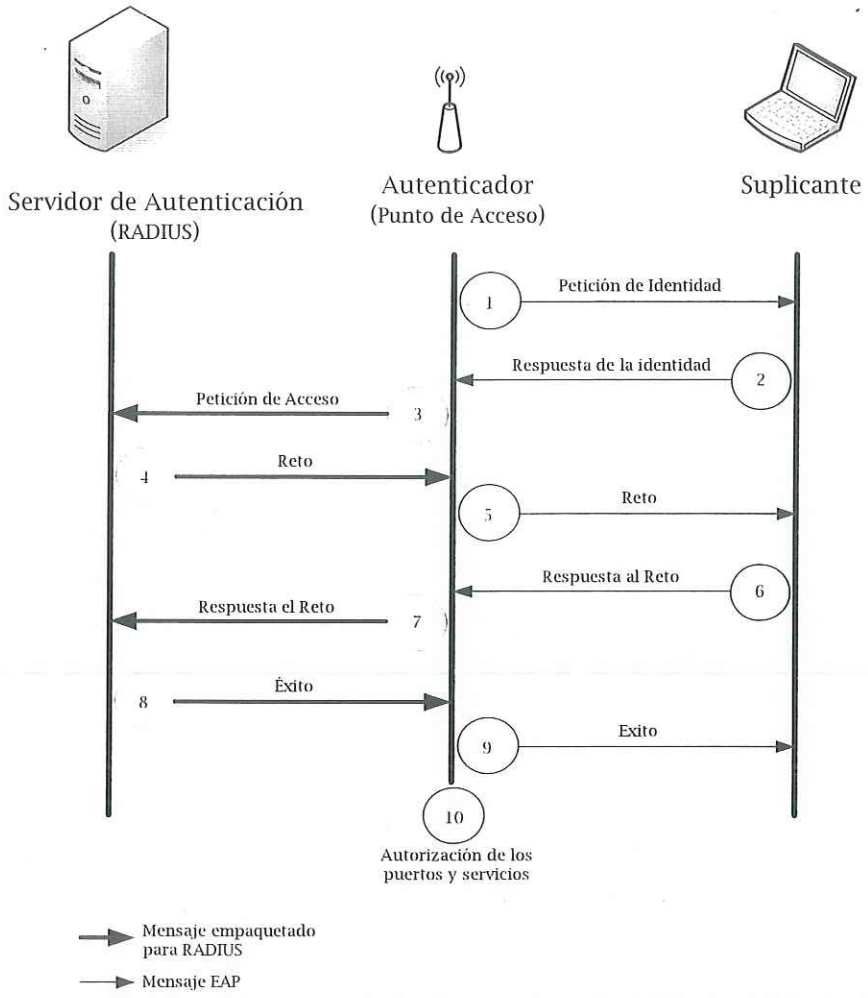


FIGURA II.9 - PROCESO DE AUTENTICACIÓN

3. El mensaje es pasado al servidor de autenticación (comúnmente RADIUS).
4. El servidor de autenticación manda un reto al autenticador. Este lo desempaqueta de IP, lo reempaqueta en un mensaje EAPoL.
5. Este paquete es enviado al suplicante.
6. El suplicante responde al reto a través del autenticador, el cual redirige el mensaje hacia el servidor de autenticación.

7. El servidor utiliza un algoritmo de autenticación específico para verificar la integridad del cliente. Esto puede ser a través del uso de certificados digitales o cualquier otro tipo de autenticación EAP. El número de mensajes reto-respuesta dependerá el tipo de método EAP que se esté utilizando. Algunos de estos métodos pueden soportar autenticación mutua, es decir, el servidor autentica al cliente y viceversa.
8. En el caso de que el suplicante proporcione una identidad apropiada, el servidor de autenticación responderá con un mensaje EAP de Éxito [Success], de ser errónea la identidad proporcionada por el suplicante, el servidor de autenticación responderá con un mensaje EAP de Error [Failure].
9. Cualquiera de estos dos mensajes será enviado al suplicante.
10. En el caso de que el mensaje sea de Éxito, el autenticador dará acceso a los puertos y servicios del sistema autenticador (Figura II.10).

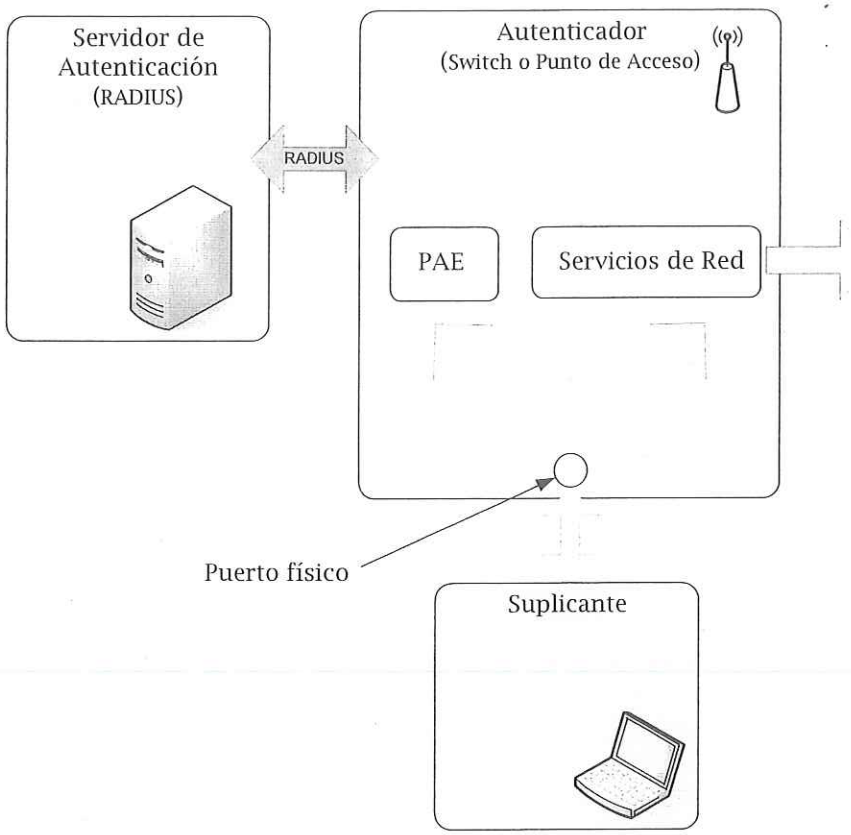


FIGURA II.10 - ESTADO DE LOS PUERTOS DESPUÉS DE UNA AUTENTICACIÓN EXITOSA

II.7 Métodos de Autenticación EAP

Los métodos EAP pueden tener diferentes metas, y por lo tanto el uso de distintos métodos de autenticación de usuarios dependerá de los requerimientos de la situación particular.

Hoy en día la implementación de redes inalámbricas IEEE 802.11 están basadas en estos métodos de autenticación, incluyendo EAP-TLS, EAP-TTLS, PEAP, LEAP y

EAP-MD5. Estos métodos soportan credenciales de autenticación que incluyen: certificados digitales, nombres y contraseñas de usuarios y tokens seguros [RFC 4017, 2005].

II.7.1 EAP en Redes Inalámbricas

Los requerimientos para el desarrollo de métodos EAP utilizados en redes inalámbricas IEEE 802.11 están especificados en el documento "*Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs - RFC 4017* ", de autores D. Stanley, J.Walker, B. Aboba. En este se dividen los requerimientos de los métodos en cuatros tipos generales: tipos de credenciales, requerimientos mandatarios, requerimientos recomendados y características opcionales; así mismo, define consideraciones de seguridad para estos métodos.

Tipos de Credenciales. En la implementación de las redes inalámbricas IEEE 802.11 se espera el uso de diferentes tipos de credenciales, tales como: certificados digitales, nombres y contraseñas de usuarios, tokens seguros y certificados de red móvil (como GSM o UMTS secretas). Otros tipos de credenciales que pueden ser usados, incluyen llaves publicas/privadas y soporte para credenciales asimétricas.

Requerimientos Mandatarios. Los métodos de autenticación EAP para uso en redes inalámbricas IEEE 802.11 deben satisfacer los siguientes criterios:

1. Proporcionar material para la generación de llaves.

2. Fortaleza de las llaves (128 bits).
3. Soporte para autenticación mutua.
4. Equivalencia de estado compartido.
5. Resistencia a ataques de diccionario.
6. Protección contra ataques de man-in-the-middle.
7. Negociación ciphersuite protegida.

Requerimientos Recomendados.

8. Fragmentación.
9. Identidad de usuario final escondida.

Características Opcionales.

10. Channel binding.
11. Reconexión Rápida.

Consideraciones de Seguridad. Las consideraciones de seguridad descritas en el RFC 4017son las siguientes:

1. Independencia del algoritmo.
2. Sesión de llaves fuerte y fresca.
3. Protección de replay.
4. Autenticación.
5. Autorización.
6. Sesión de llaves.

7. Negociación de ciphersuite.
8. Nombrado único.
9. Efecto domino.
10. Key binding.

II.7.2 EAP-MD5

EAP-MD5 [Extensible Authentication Protocol - Message-Digest Algorithm 5] es el más sencillo de los métodos EAP. Este está basado en la autenticación con usuario y contraseña utilizando el algoritmo de hashing MD5. Los pasos que sigue este método son:

1. El cliente se identifica a sí mismo con el servidor mediante su nombre de usuario.
2. El servidor genera aleatoriamente una cadena "reto o challenge" la cual es enviada al cliente.
3. El cliente calcula la respuesta del reto mediante la combinación de la contraseña y reto con el algoritmo MD5 y lo manda al servidor.
4. El servidor realiza el mismo procedimiento con el reto y la contraseña de su base de datos.
5. El resultado de los últimos dos puntos es comparado, si coinciden la autenticación es exitosa, de lo contrario es fallida.

Este método no cumple con los requerimientos especificados en el RFC 4017 ya que ofrece una seguridad mínima, además de ser vulnerable a ataques de diccionario y no soportar llaves dinámicas.

II.7.3 LEAP

LEAP [Lightweight Extensible Authentication Protocol] es un método EAP propietario de Cisco Systems (Intermec, 2005). Es básicamente una mejora del método EAP-MD5 la cual soporta el manejo de llaves dinámicas y la autenticación mutua. Ya que utiliza CHAP MD5, LEAP es susceptible a ataques de diccionario, aunque Cisco Systems asegura que el uso de contraseñas largas y complejas mitiga en gran parte esta vulnerabilidad.

Al ser propietario, solo puede ser utilizado con puntos de acceso Cisco como autenticador, por lo que es una limitante al momento de escoger el método EAP apropiado para proporcionar seguridad a alguna red inalámbrica.

II.7.4 EAP-TLS

EAP-TLS [Extensible Authentication Protocol – Transport Layer Security], fue desarrollado por Microsoft y está basado en el RFC 2716 de la IETF. Es el método que más se está utilizando en estos últimos tiempos debido a que Windows utiliza este método en gran cantidad de ocasiones. Este método realiza la autenticación mediante certificados X.509, creados por una autoridad de certificación de confianza.

La autenticación es mutua, es decir, se autentifica tanto el cliente como el servidor (Figura II.11). Además, permite la asignación dinámica de llaves WEP, aumentando enormemente la seguridad. Otra característica de este método, es que no es necesario acceder a bases de datos. Esto puede suponer un problema en algunos casos en los que interese tener un control de acceso basado en bases de datos.

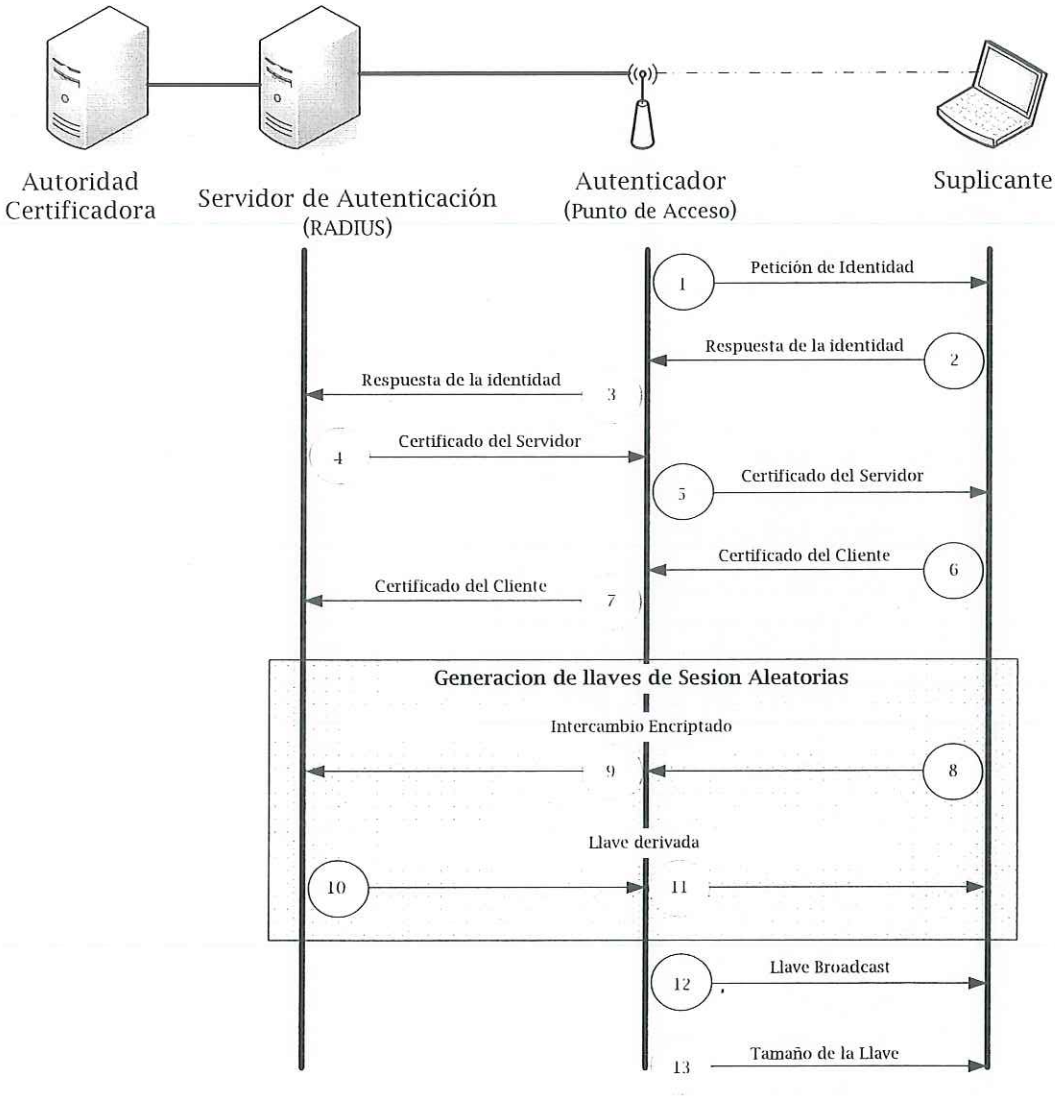


FIGURA II.11 - PROCESO DE AUTENTICACIÓN CON EAP-TLS

II.7.5 EAP-TTLS

EAP-TTLS [Extensible Authentication Protocol – Tunnel Transport Layer Security], es un estándar desarrollado como alternativa para EAP-TLS por Funk Software y Certicom. En este caso, solo es necesario el certificado del sistema o del servidor. Una vez realizada la autenticación del servidor, se realiza un túnel TLS por donde se realiza el resto de la autenticación, que consiste en una autenticación de segundo orden que se utiliza para autenticar al cliente. En esta segunda fase de la autenticación se puede utilizar un amplio número de métodos de autenticación, que utilicen nombre de usuario y contraseña; estos pueden ser métodos tales como MD5, CHAP, MS-CHAP, entre otros.

El hecho de que EAP-TTLS utiliza una autenticación del cliente basada en usuario y contraseña, permite utilizar este método con las infraestructuras de bases de datos existentes actualmente. Además, simplifica el proceso ya que no hay que obtener certificados para el cliente, por lo que no es necesario que haya un servidor de certificados. Soporta también asignación dinámica de llaves WEP. Todas estas características hacen de EAP-TTLS un método bastante seguro que a su vez, permite la autenticación basada en usuario y contraseña de una manera bastante sencilla.

II.7.6 PEAP

PEAP [Protected Extensible Authentication Protocol] fue desarrollado por Microsoft, Cisco y RSA Security (Madrid-Molina, 2003) como un protocolo abierto.

Funciona de manera similar a EAP-TTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador. Otra ventaja que ofrece PEAP es la reconexión rápida, esto que debe a que cuenta con la capacidad de reconexión a un punto de acceso inalámbrico mediante llaves de sesión almacenadas en la caché, lo que permite moverse rápidamente entre puntos de acceso inalámbrico.

El proceso de autenticación con PEAP consta de dos fases principales (Fig. 2.12):

Autenticación de servidor y creación de un túnel de cifrado de TLS. El servidor se identifica ante un cliente proporcionando a éste información del certificado. Una vez que el cliente comprueba la identidad del servidor, se genera un secreto maestro. A continuación, las llaves de sesión obtenidas del secreto maestro se utilizan para crear un canal de cifrado de TLS que cifra toda la comunicación posterior entre el servidor y cliente inalámbrico.

Conversación de EAP y autenticación de usuario y de equipo cliente. Mediante el canal de cifrado de TLS se encapsula una conversación de EAP completa entre el cliente y el servidor. Con PEAP puede utilizarse cualquiera de los diversos métodos de autenticación de EAP, como contraseñas, tarjetas inteligentes y certificados, para autenticar al usuario y al equipo cliente.

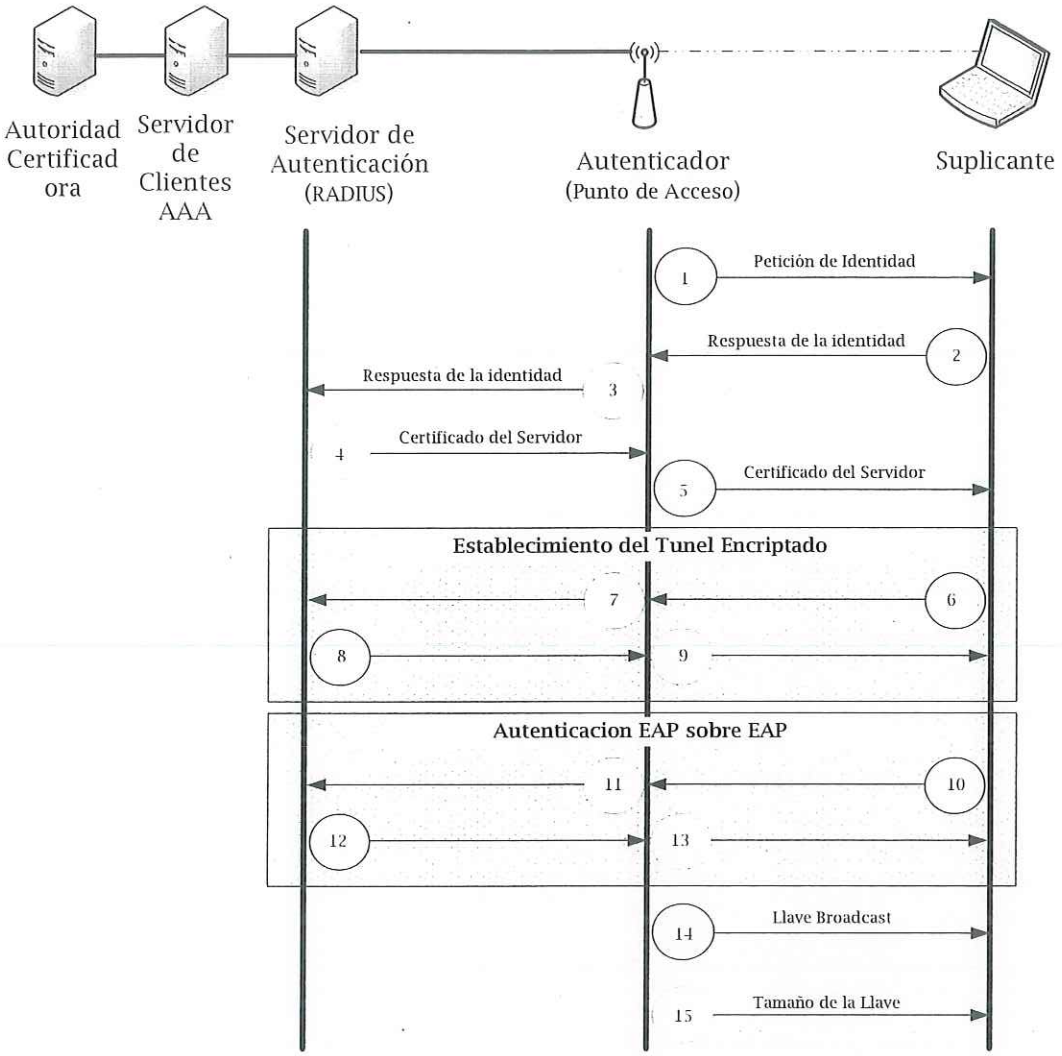


FIGURA II.12 - PROCESO DE AUTENTICACIÓN CON PEAP

Después de una autenticación exitosa, el material para la generación de llaves dinámicas es proporcionado por el servidor de autenticación al autenticador. Este utiliza el material de generación de llaves para crear las llaves necesarias de protección de la información.

Existen dos subtipos de métodos PEAP certificados por WPA y WPA2. Estos son: PEAPv0/EAP-MSCHAPv2 y PEAPv1/EAP-GTC.

PEAPv0/EAP-MSCHAPv2. Este término técnico es el más comúnmente utilizado para referirse a PEAP. Después de EAP-TLS, EAP-MSCHAPv2 es el método con más soporte en el mundo. Existen implementaciones de clientes y servidores de marcas como Microsoft, Cisco, Apple, Linux y de sistemas abiertos.

PEAPv1/EAP-GTC. Fue creado por Cisco como una alternativa a PEAPv0/EAP-MSCHAPv2. Este método ofrece soporte para el uso de las tarjetas GTC (Generic Token Card).

La principal diferencia entre estos dos tipos de PEAP radica en que EAP-GTC manda la contraseña en claro a través del túnel TLS, mientras que EAP-MSCHAPv2 solo puede ser usado en instancias donde la lista de contraseñas es almacenada en un formato Microsoft-password-NT-hash o en texto simple, de tal forma que el servidor de autenticación pueda calcular el hash.

II.7.7 Otros Métodos EAP

Otros métodos de autenticación EAP menos populares son:

EAP-FAST [EAP-Flexible Authentication vía Secure Tunneling] fue creado por Cisco System para solucionar las debilidades de LEAP.

EAP-AKA [EAP for Universal Mobile Telecommunications System Authentication and Key Agreement] es un mecanismo de autenticación y distribución de llaves de sesión del USIM o modulo de identidad de subscriptor de UMTS [Universal Mobile Telecommunications System].

EAP-SIM [Extensible Authentication Protocol Method for GSM Subscriber Identity] es un mecanismo de autenticación y distribución de llaves de sesión del SIM o modulo de identidad de subscriptor de GSM [Global System for Mobile Communications].

EAP-SPEKE [Extensible Authentication Protocol – Simple Password-authenticated Exponential Key Exchange] es un método que permite verificar que tanto el cliente como el servidor de autenticación comparten una contraseña a través de un medio seguro.

Además de los antes mencionados, existen métodos como: EAP-IKEv2, EAP-GPRS y EAP-Archie, aunque estos son menos populares.

II.8 RADIUS

RADIUS es un protocolo de control de acceso que verifica y autentifica a los usuarios basándose en el método de Reto/Respuesta (Challenge / Response) (Hassell, 2002). Fue originalmente desarrollado por Livingston Enterprises.

Muchos servidores RADIUS existen actualmente, algunos comerciales y otros de código abierto, todos con características que pueden varían, aunque la mayoría pueden usar archivos de texto, servidores LDAP o algunas bases de datos para autenticar usuarios. RADIUS es un protocolo de autenticación comúnmente utilizado por el estándar 802.1X. Aunque originalmente no fuera diseñado para ser utilizado como un método autenticación para redes inalámbricas.

II.8.1 AAA

El marco alrededor de construcción de RADIUS se conoce como el proceso del AAA [Authentication, Authorization, and Accounting - Autenticación, Autorización y Manejo de Cuentas], este consiste en la autenticación, autorización, y uso de cuentas. Mientras que no hay nada específico sobre RADIUS en el modelo del AAA, un fondo general es necesario para justificar el comportamiento de éste. El protocolo RADIUS fue creado antes de que el modelo del AAA fuera desarrollado, pero era el primer protocolo AAA-basado verdadero que exhibía la funcionalidad del AAA para ganar la aceptación de la industria y uso extenso. Sin embargo, eso no quiere decir que no hay otros protocolos que satisfacen los requisitos de la arquitectura (Hassell, 2002).

II.8.2 Características

Las características principales de RADIUS son (RFC 2865, 2000):

- *Modelo Cliente – Servidor.* Un servidor de acceso a la red [NAS] opera como cliente para RADIUS. El cliente es responsable de enviar la información al servidor RADIUS designado, para después actuar a la respuesta que es regresada. El servidor RADIUS es responsable de recibir la petición de conexión del usuario, autenticar al usuario y regresar toda la información de la configuración necesaria para que el cliente provea el servicio al usuario.
- *Seguridad de Red.* Las transacciones entre el cliente y el servidor RADIUS son manejadas a través del uso de una llave secreta, la cual no es enviada sobre la red. Además, todas las contraseñas de usuarios son enviadas de manera cifrada.
- *Mecanismo de Autenticación Flexible*. El servidor puede soportar varios métodos de autenticación.
- *Protocolo Extensible*. Nuevos valores de atributos pueden ser agregados sin dañar la implementación actual del protocolo.

II.8.3 UDP

Una característica interesante del servidor RADIUS es que en principio utiliza segmentos UDP en lugar de TCP. Esto se debe a que RADIUS tiene algunas propiedades propias de los segmentos UDP. RADIUS requiere que las consultas fallidas

hacia un servidor sean redirigidas a un segundo servidor, y para hacer esto, una copia del pedido original debe existir sobre la capa de transporte del modelo OSI. Esto, obliga a usar tiempo de retransmisión. RADIUS usa el puerto UDP 1812 para la autenticación y el puerto 1813 para el manejo de cuentas; anteriormente usaba los puertos 1645 y 1646, estos fueron remplazados por causar conflictos con el servicio "datametriscs" (RFC 2865, 2000).

II.8.4 Formato de Paquete

El protocolo RADUS usa paquetes UDP para la transmisión entre el cliente y el servidor. En la Figura II.13 se muestra el paquete de datos de RADIUS. La trama se divide en cinco regiones, las cuales se describen a continuación (Hassell, 2002).

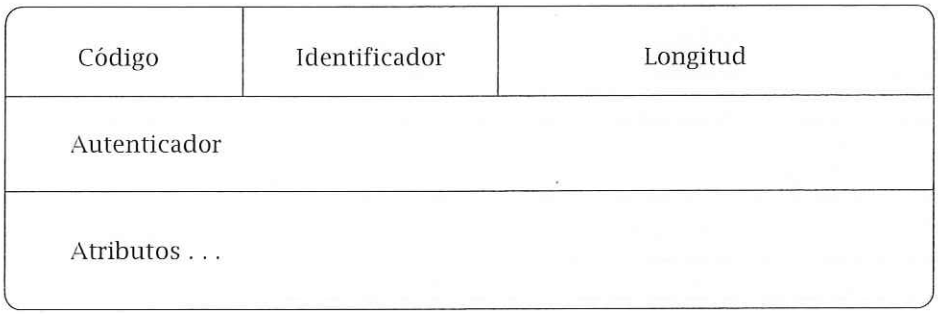


FIGURA II.13 - PAQUETE RADIUS

- *Código.* Un octeto de largo que sirve para distinguir el tipo de mensaje. Códigos validos son:

  1 Access-Request
  2 Access-Accept
  3 Access-Reject

4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

- *Identificador.* El identificador tiene una longitud de un byte y es usado para hacer "threading" (secuencias), o enlace automático de los pedidos iniciales y contestaciones subsecuentes. El servidor RADIUS generalmente puede interceptar mensajes duplicados con examinar factores como el origen de la dirección IP, el origen del puerto UDP, la duración entre los mensajes sospechosos, y el campo de identificación.
- *Longitud.* La región de longitud es de dos bytes y se usa para especificar el tamaño del mensaje RADIUS. El valor en este campo se calcula al analizar los campos de: código, identificador, longitud, autenticador, y haciendo la suma de sus atributos. El campo de longitud se checa cuando el servidor RADIUS recibe un paquete para asegurar la integridad de los datos. El rango de tamaño válido está entre los 20 y 4096. Si el servidor recibe un paquete más grande o chico del rango permitido, este ignora todos los datos y pasa al punto final designado en el campo de longitud.
- *Autenticador.* La región de autentificación tiene una longitud por los regular de 16 bytes, este es el campo en que la integridad de la carga útil del mensaje se inspecciona y verifica. En este campo el más importante byte es transmitido antes que cualquier otro –el valor usado para

autentificar es contestado por el servidor RADIUS. Este valor también es usado en el mecanismo para conceder contraseñas. Hay dos tipos específicos de valores de autenticación: los valores de petición y respuesta. Los de petición son usados con los paquetes de *Authentification-Request* y *Accounting-Request*. El valor de pedido es de 16 bytes y es generado aleatoriamente para prevenir cualquier ataque. El autenticador de respuesta es usado en los paquetes *Acces-Accept*, *Acces-Reject*, y *Acces-Challenge*. El valor es calculado con una función hash generada por los valores en las regiones del paquete: código, identificador, longitud, y la región de autenticador de pedido, seguido por la carga útil del paquete y el secreto compartido.

- *Atributos.* Esta sección del paquete es donde se guardan un número arbitrario de campos de atributos.

II.8.5 Métodos de Autenticación

RADIUS soporta una variedad de protocolos para la transmisión de datos de usuarios desde el servidor de autenticación. Los más comúnmente utilizados son: el Protocolo de Autenticación de Contraseña [Password Authentication Protocol, PAP] y el Protocolo de Autenticación de Reto Mutuo [Challenge-Handshake Authentication Protocol, CHAP] (Hassell, 2002).

- *PAP.* El atributo de "*contraseña del usuario*" en un paquete solicitado señala al servidor RADIUS que el protocolo PAP va a ser usado para la

transacción. Es importante observar que el único campo óbligatorio en este caso es el la "*contraseña del usuario*". El campo de "*nombre de usuario*" no tiene que ser necesariamente incluido en el paquete solicitado, y es posible que el servidor RADIUS a lo largo de la cadena Proxy cambie el valor del campo de este campo.

- *CHAP.* está basado en la premisa de que la contraseña nunca debe ser enviado en ningún paquete a través de la red. CHAP cifra dinámicamente el identificador y la clave solicitados. La máquina del usuario pasa al procedimiento de conexión, después de haber obtenido la llave del equipo del cliente RADIUS. El cliente entonces utiliza una función "hash" para la llave, enviando de regreso un identificador CHAP, una respuesta CHAP, y el nombre de usuario al cliente RADIUS. El cliente RADIUS, al haber recibido todo lo anterior, coloco el campo del identificador CHAP en un lugar apropiado del atributo del *CHAP-Password* y envía una respuesta. El valor del desafío obtenido se coloca en el atributo *CHAP-Challenge* o en el campo de autentificación en el encabezado.

III. Metodología

En este capítulo se describirá la metodología propuesta para llevar a cabo la implementación de seguridad en una red inalámbrica, se incluirán las fases de análisis de requerimientos, planeación, instalación, pruebas y mantenimiento. (Figura III.1).

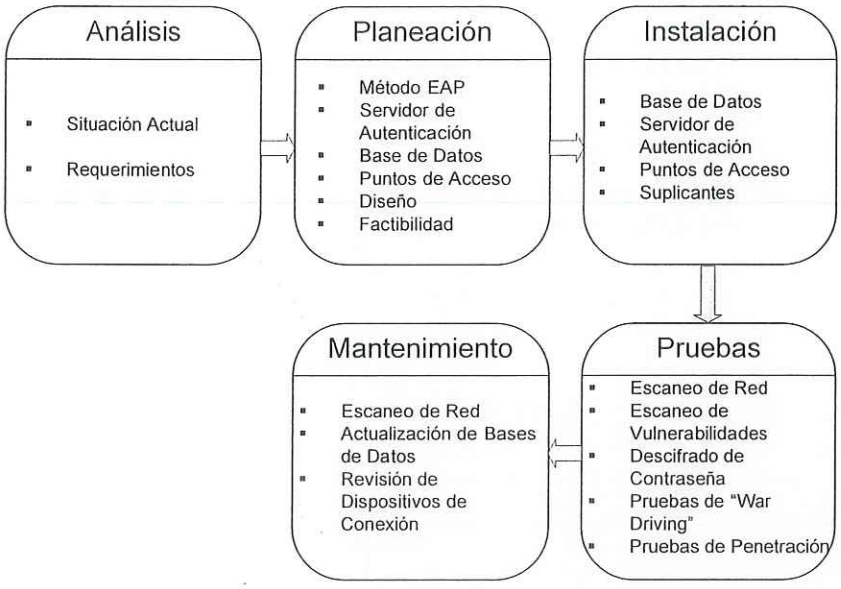


FIGURA III.1 - DIAGRAMA DE FLUJO DE LA IMPLEMENTACIÓN DE SEGURIDAD EN UNA RED INALÁMBRICA

III.1 Análisis de Requerimientos

Antes de la implementación de autenticación y seguridad en una red inalámbrica es necesario recolectar información sobre la situación actual de esta, además de establecer una estrategia para su instalación y utilización. Esta estrategia deberá abarcar áreas tales como las necesidades de los usuarios, políticas actuales de las redes cableadas, situación y ubicación de los dispositivos de red cableada e inalámbrica.

- Determinar las motivaciones y las necesidades de los usuarios de la red e identificar claramente los objetivos, además de asegurarse de que los beneficios superen a los riesgos.
- Integrar las políticas de las redes inalámbricas a las actuales políticas de las redes cableadas tomando en cuenta que las soluciones inalámbricas son una extensión de la red cableada.
- Definir claramente la propiedad de las redes inalámbricas y con ello garantizar el control al identificar las amenazas a la seguridad.
- Proteger la infraestructura existente dando importancia a la ubicación de los dispositivos inalámbricos no quedando estos directamente en la red interna, sino implementar una red inalámbrica separada con gateways muy controlados a la red principal.
- Educar a los usuarios sobre las políticas de seguridad en la red inalámbricas que incluyan la instrucción a los empleados en la configuración de sus dispositivos para que tengan acceso de manera segura a la red.

III.1.1 Situación Actual de la Red Inalámbrica

La información necesaria sobre de la situación de la red actual, abarcando interrogantes tales como:

- ¿Se cuenta con red inalámbrica?
- ¿Cuáles son los dispositivos utilizados en la red actual?

- ¿Estos dispositivos son capaces de proporcionar mecánismos de seguridad?
- ¿Qué mecanismos de seguridad proporcionan?
- ¿El firmware de estos dispositivos puede ser actualizado para soportar mecanismos de seguridad más efectivos?
- ¿Se cuentan con servidores de autenticación tales como RADIUS o TACACS?
- ¿Cuál es el número de usuarios de la organización?
- ¿Cuál es el número de equipos a conectar en la organización?
- ¿Qué sistemas operativos utilizan los usuarios de la red?

Otros documentos importantes que ayudan en el desarrollo de un plan de implementación de seguridad en una red inalámbrica son los diagramas de red que muestren su topología y que tengan información detallada de los dispositivos de conexión y su ubicación física, así como el listado de computadoras y dispositivos conectados a la red que contengan las direcciones IP asignadas a cada una, su dirección MAC, su propietario y contacto.

III.1.2 Requerimientos

Además de la situación actual de la red, se deberá hacer un análisis y especificación de los requerimientos de la red inalámbrica, según las necesidades y características de la organización. Una de las características que deberá tomarse en

cuenta es el tamaño de la organización, es decir el número de máquinas y usuarios de la misma, la preferencia en el método de autenticación de la organización, ya sea con certificados o con contraseñas, la vulnerabilidad a un ataque pasivo o activo que presenta el área de cobertura de la red inalámbrica de la organización, la restricción de enlace, como el tiempo máximo de conexión, entre otras políticas de seguridad con que cuente la organización.

De este análisis se obtendrá un documento que mostrará detalladamente las características que deberá tener la red inalámbrica para satisfacer a las necesidades de seguridad de la organización. Este documento definirá los siguientes puntos:

- *Usuarios.* Especificar el número de usuarios y ubicar el lugar donde estarán trabajando.
- *Conexiones.* Mostrar los diagramas de red que muestren su topología y que tengan información detallada de los dispositivos de conexión.
- *Instalaciones.* En esta sección se deberá mostrar un mapa de las instalaciones, así como la ubicación de los puntos de acceso en el caso que ya exista una red inalámbrica o en su caso la posible ubicación donde podrán ser montados los puntos de acceso.
- *Área de cobertura.* Identificar las áreas de cobertura que se tienen en la red inalámbrica actual, o si es el caso identificar las áreas de cobertura que se desean implementar.

- *Aplicación.* Definir el tipo de aplicación que los usuarios deberán manejar, como navegadores, correo electrónico, transferencia de archivos entre otros.
- *Seguridad.* Se describe en esta área del documento la privacidad de la información almacenada en servidores o transmitida través de la red inalámbrica, tal como numero de cuentas bancarias, contraseñas u otros documentos e información confidenciales.
- *Plataforma de clientes.* Enlistar las plataformas, sistemas operativos y demás especificaciones de los equipos de los clientes.
- *Políticas.* Describir las políticas de seguridad actuales en la organización.

III.2 Planeación

En base al análisis y especificación de los requerimientos se podrá comenzar con la planeación y el diseño de seguridad en la red inalámbrica que deberán satisfacer las necesidades de la organización. En esta sección de la implementación se necesitarán realizar tareas tales como: selección de los métodos de seguridad, selección de los dispositivos de conexión, en el caso de no existir una red inalámbrica o que los dispositivos actuales no tengan la capacidad de soportar los métodos de seguridad seleccionados, selección de bases de datos de usuarios, determinación de los clientes soportados.

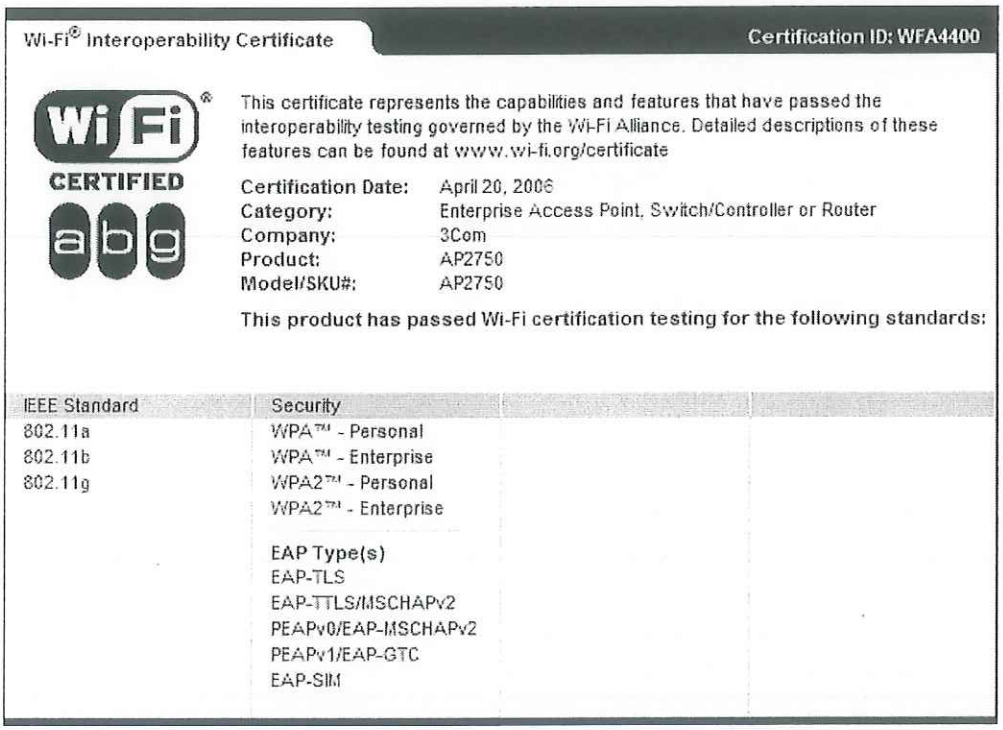
III.2.1 Determinación del Método EAP más Adecuando

El siguiente paso en la planeación es el de escoger el método EAP más adecuado para el caso, tomando en cuenta los requerimientos de seguridad descritos en el análisis; también se deberán tomar en cuenta para esta selección, los clientes soportados. Deberá optarse por soluciones no propietarias, es decir aquellas que no requieran características de hardware y software de clientes y dispositivos de conexión de una marca específica.

Existen varios métodos EAP y cada uno de ellos proporciona un enfoque distinto a la autenticación, aunque utilizan el mismo esquema y protocolo. De los cuales solo cinco de esos métodos han sido probados por la Wi-Fi Alliance (Phifer, 2006), estos son: EAP-TLS, EAP-TTLS, PEAPv0, PEAPv1 y EAP-SIM. Para determinar que método EAP es soportado por algún dispositivo en particular, se deberá examinar la página de "Productos Certificados por Wi-Fi Alliance" (Figura III.2). De cualquier modo, algunos dispositivos no certificados por esta organización pueden ser funcionar en conjunto con dispositivos certificados.

La mejor manera de elegir el método adecuado, es revisar las características de los diferentes métodos y buscar el que mejor satisfaga las necesidades de seguridad de la organización. Para observar mejor las diferencias entre los métodos de autenticación EAP más comúnmente utilizados, podemos ver la siguiente tabla (Tabla III.1), la cual muestra algunas características importantes en la toma de decisión del método EAP.

Otras características que deberán ser tomadas en cuenta son la compatibilidad con software y dispositivos de diferentes marcas, ya que algunos de estos métodos son propietarios (Tablas III.2 y III.3). Estas tablas nos permiten observar la interoperabilidad entre los diferentes métodos y los servidores de autenticación y suplicantes existentes.



Wi-Fi® Interoperability Certificate — Certification ID: WFA4400

Wi-Fi® CERTIFIED a b g

This certificate represents the capabilities and features that have passed the interoperability testing governed by the Wi-Fi Alliance. Detailed descriptions of these features can be found at www.wi-fi.org/certificate

Certification Date:	April 20, 2006
Category:	Enterprise Access Point, Switch/Controller or Router
Company:	3Com
Product:	AP2750
Model/SKU#:	AP2750

This product has passed Wi-Fi certification testing for the following standards:

IEEE Standard	Security
802.11a	WPA™ - Personal
802.11b	WPA™ - Enterprise
802.11g	WPA2™ - Personal
	WPA2™ - Enterprise
	EAP Type(s)
	EAP-TLS
	EAP-TTLS/MSCHAPv2
	PEAPv0/EAP-MSCHAPv2
	PEAPv1/EAP-GTC
	EAP-SIM

FIGURA III.2 - CERTIFICACIÓN WI-FI DE INTEROPERABILIDAD EN DISPOSITIVOS DE CONEXIÓN (HTTP://CERTIFICATIONS.WI-FI.ORG/)

Características	MD5	LEAP	TLS	TTLS	PEAP
Atributos de Autenticación	solo autentifica al cliente	mutua	mutua	mutua	mutua
Generación de llaves WEP	utiliza claves estáticas	si	Generada durante la autenticación y actualizada a intervalos regulares.	Generada durante la autenticación y actualizada a intervalos regulares.	Generada durante la autenticación y actualizada a intervalos regulares
Dificultad de implementación	sencilla	sencilla	difícil	moderada	moderada
Seguridad	pobre	buena, con contraseñas complejas	muy buena	muy buena	Puede utilizar autenticación segura de contraseñas o certificados digitales.
Protección de credenciales de usuario	no	no	no	Autenticación basada en certificados protegida por túnel de Transport Layer Security (TLS).	Protegido por túnel de Transport Layer Security (TLS).
Certificados del cliente	requerida	requerida	requerido	requerido	requerido
Certificados del Servidor	no	requerida	requerido	opcional	opcional
Reconexión Rápida	no	no	no	si	si

TABLA III.1 - COMPARACIÓN DE CARACTERÍSTICAS DE LOS PRINCIPALES MÉTODOS DE AUTENTICACIÓN EAP (GAST, 2002)

Marca	Métodos EAP soportados
Funk Software	MD5,LEAP, TLS,TTLS,PEAP
InfoBlox	MD5,LEAP, TLS,TTLS,PEAP
Hewlett-Packard	MD5,LEAP, TLS,TTLS,PEAP
Microsoft	MD5, TLS, PEAP
Meetinghouse	MD5,TLS, TTLS
Cisco Systems	MD5,LEAP, TLS,PEAP,EAP-FAST
FreeRadius	MD5,TLS, TTLS, PEAP

TABLA III.2 - INTEROPERABILIDAD ENTRE LOS SERVIDORES DE AUTENTICACIÓN Y LOS MÉTODOS EAP. (INTEROPNET, 2004).

Marca	Sistemas operativos soportados	Métodos EAP soportados
Microsoft	2000/XP	MD5,TLS, PEAP
Meetinghouse	98/ME/NT/2000/XP;MacOS X;Linux	MD5,TLS, PEAP, TTLS
Funk	98/ME/2000/XP	MD5,TLS, PEAP, TTLS
Free1X.ORG	Linux/BSD(Xsupplicant)	MD5,TLS, PEAP, TTLS
MacOSX	MacOS	MD5,TLS, PEAP, TTLS
Cisco	95/98/NT/2000/XP;MacOS;Linux	MD5,TLS, PEAP, LEAP

TABLA III.3 - INTEROPERABILIDAD ENTRE LOS CLIENTES O SUPLICANTES Y LOS MÉTODOS EAP. (INTEROPNET, 2004).

III.2.2 Selección del Servidor de Autenticación

Esta tarea es sencilla de realizar, ya que solo existen unos pocos servidores de autenticación que soporten métodos EAP. Lo primero que debemos de revisar es si ya se cuenta con algún servidor de autenticación dentro de la organización y si este es interoperable con el método de autenticación que ya se seleccionó (Tabla III.2). De no contar con ningún servidor de autenticación ya instalado, se puede escoger uno de todos los existentes, tomando en cuenta características como la interoperabilidad con el método seleccionado, costos y el conocimiento del administrador de red sobre el uso del mismo.

Una solución de bajo costo es el uso de un servidor de autenticación FreeRADIUS. Este que es un servidor de RADIUS instalable en plataformas Unix, es de código abierto con licencia GNU. FreeRADIUS puede realizar autenticación vía PAP, CHAP, MS-CHAP, EAP-MD5, EAP-GTC, EAP-TLS, EAP-TTLS, PEAPv0, LEAP, EAP-SIM.

Otra solución es la compra de servidores de marcas como: CISCO, Microsoft, Funk, entre otros; todos ellos con el soporte de estas compañías.

III.2.3 Selección de la Base de Datos para Autenticación

La base de datos de usuarios será necesaria en el caso de haber elegido un método que utilice contraseñas para la autenticación de usuarios. La mayoría de los servidores de autenticación RADIUS soportan las siguientes fuentes de datos (Tauno-Williams, 2006):

- Archivos
  - Texto
  - DB / DBM
- LDAP
  - OpenLDAP
  - Novell NDS
  - Sun One
  - LDAPv3
- Ejecutable Local
- Script en Perl
- Script en Python
- Bases de datos de SQL
  - Oracle
  - PostgreSQL
  - Sybase

- IBM DB2
- MySQL
- ODBC
  - iODBC
  - uniXODBC

El caso ideal es usar una base de datos que ya exista en la organización y que cuente con los usuarios y contraseñas necesarios. De no ser así, se tendrá que implementar alguna de entre la lista de bases de datos compatibles con los servidores RADIUS.

Algunos puntos que deben tomarse en cuenta para la selección de la base de datos de autenticación, en el caso de no existir una dentro de la organización, serán: costos, conocimiento del uso por parte del administrador y compatibilidad con el servidor de autenticación seleccionado. Una solución bajo costo es el uso de bases de datos con licencia pública como MySQL u OpenLDAP.

III.2.4 Selección de los Puntos de Acceso

Otra parte de la planeación es la selección y señalamiento de la ubicación de los puntos de acceso, estos pueden ser:

Comerciales. En el caso de seleccionar un punto de acceso comercial se deberá tomar en cuenta que en las especificaciones del punto de acceso se defina la capacidad

de proveer seguridad con WPA con el método EAP seleccionado, esto se puede verificar en la página "Productos Certificados por Wi-Fi Alliance" (Figura III.1). De existir ya una red inalámbrica en la organización y esta cuente con puntos de accesos comerciales, se deberá verificar que se cumpla lo anterior o en su defecto investigar sobre la posible actualización del firmware del dispositivo para que la pueda ofrecer.

Comerciales con software libre. Para este caso se deberá realizar las mismas verificaciones que en los puntos de acceso comerciales.

"Caseros". Otra opción es la instalación de un punto de acceso utilizando una computadora con sistema operativo Linux instalado, que tenga una tarjeta de red inalámbrica. Esta opción ofrece ventajas tales como (Garaizar-Sagarminaga, 2005):

- Un PC es mucho más potente que un AP, muchas posibilidades (filtrados, mejoras de seguridad, enrutamiento, DHCP, entre otras).
- Reciclaje de equipos obsoletos lo cual genera puntos de acceso de bajo costo.

Además de seleccionar los dispositivos que servirán como puntos de acceso se deberá determinar la ubicación de estos, para proporcionar la cobertura marcada en los requerimientos. Para esta tarea se deberá revisar bibliografía que describa el diseño de redes inalámbricas, de forma que permita hacer una implementación que logre una mayor cobertura, que no se vea tan afectada por el ruido y la interferencia de ondas de radio frecuencia, tipos de antenas más apropiadas, etc.

III.2.5 Diseño del Proyecto

Para terminar la planeación, el resultado que genera es un documento que reúne la información obtenida en el análisis y que describe claramente los dispositivos y tecnologías que se usarán en la implementación de la seguridad. Además deberá mostrar la arquitectura de seguridad de la red inalámbrica mediante un diagrama mostrando los componentes de la red (Figura III.3). Este documento servirá de plataforma para la implementación de la seguridad en la red inalámbrica o en su defecto la implementación total de una red inalámbrica en una organización.

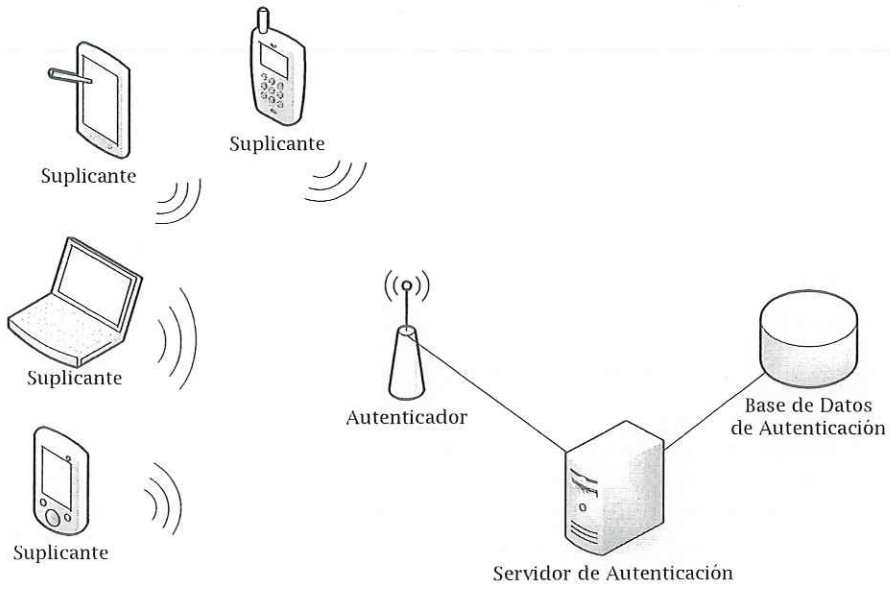


FIGURA III.3 - ARQUITECTURA DE SEGURIDAD DE LA RED INALÁMBRICA.

III.2.6 Factibilidad del Proyecto

Una vez conocidos los requerimientos y el diseño se podrá realizar un análisis de la factibilidad del proyecto. Con esto se pretende identificar los beneficios y determinar

si los costos de la implementación tendrán un efecto positivo como resultado de la inversión (Geier, 2002). Los aspectos que deberán ser tomados en cuenta son aquellos que muestren los costos y complicaciones de esta implementación; y por otro lado los costos e inconvenientes que implicaría el no instalar seguridad en la red inalámbrica, como perdida, modificación o robo de información, o la disminución del ancho de banda en el caso de usuarios no autorizados.

III.3 Instalación

En este subcapítulo se describirá todo lo relacionado a la instalación del sistema de seguridad en la red inalámbrica. Si el diseño se realizó de manera efectiva, este proceso se llevará a cabo con mayor facilidad. Se asumirá que la infraestructura de la red inalámbrica está completa, esto es, lo referente a la instalación de los puntos de acceso en los lugares indicados en el documento de diseño, así como las antenas y el cableado necesarios.

Si el diseño define el uso de puntos de acceso "caseros" se podrá revisar el Anexo E, en la cual se incluyen los manuales para la instalación de un punto de acceso utilizando una computadora con sistema operativo Linux, que incluyen características como: servidor DHCP, enrutamiento de paquetes y capacidad para ser configurado con algún método EAP.

III.3.4 Bases de datos de usuarios

El primer paso para la instalación de la autenticación en una red inalámbrica es la verificación de la fuente de datos para la autenticación de usuarios. En esta sección se describirán a los más comúnmente utilizados.

Archivos de Unix (shadow, passwd, group). Usuarios, contraseñas y grupos de un servidor Unix. Si la organización cuenta con algún servidor Unix y este tiene agregados a los usuarios no es necesaria ninguna instalación extra.

OpenLDAP. Es una iniciativa para desarrollar el protocolo LDAP [Protocolo de Acceso Ligero a Directorio - Lightweight Directory Access Protocol] de código abierto. En el caso de no existir algún servidor OpenLDAP en la organización podrá instalarse uno siguiendo el manual correspondiente. (Ver Anexo A).

MySQL. Es un servidor de base de datos SQL [Lenguaje de Petición Estructurada - Structured Query Language]. En este servidor puede agregarse una base de datos que aloje la información para la autenticación y contabilidad de los usuarios. (Ver Anexo C).

III.3.5 Instalación del servidor de autenticación

El siguiente paso es la instalación del servidor RADIUS y conforme al diseño podrán utilizarse servidores comerciales y de libre distribución. Al igual que en la sección anterior, solamente se describirán los más comúnmente utilizados.

FreeRADIUS. Servidor de RADIUS instalable en plataformas Unix, es de código abierto con licencia GNU. Ver el Anexo B, donde se muestra el manual para la instalación y configuración de este.

Radiator. Servidor comercial que cuenta con una amplia interopérabilidad con una gran cantidad de fuentes de datos y métodos EAP. Distribuido por la compañía Open System Consultants. Se podrá visitar la página 'http://www.open.com.au/radiator/' la cual muestra en su sección de documentación, manuales de instalación en diferentes sistemas operativos, y manuales de configuración para su uso con diferentes fuentes de datos y métodos EAP.

Microsoft IAS [Internet Authentication Service]. Otro servidor RADIUS de la compañía Microsoft, instalable solo en servidores de esa misma compañía; Soporta solo unos pocos métodos EAP. Su configuración puede ser revisada en la página de Microsoft.

Cisco ACS [Secure Access Control Server]. Instalable en sistemas operativos Windows o Unix; también puede conseguirse como un dispositivo dedicado (módulo de red, del tamaño de un switch). Ofrece soporte de autenticación de usuarios con fuentes de datos como LDAP o bases de datos ODBC [Open Database Connectivity – Conectividad Abierta de Bases de Datos]. Los manuales de instalación y configuración están incluidos en la compra de este servidor.

Steel-Belted Radius. De marca Funk Software (actualmente esta compañía fue adquirida por Juniper Networks). Instalable en varios sistemas operativos (Windows, Solaris, Linux). Los manuales de instalación se encuentran en la página Web 'http://www.juniper.net'.

HP-UX AAA Server. Servidor de autenticación de la compañía Hewlett-Packard, ofrece soporte de autenticación para diferentes métodos EAP tales como TLS, TTLS,

MD5, PEAP, LEAP y GTC. Toda la documentación necesaria para su instalación y configuración viene incluida.

InfoBlox. Tiene un diseño modular. Soporta un gran número de métodos de autenticación. Puede utilizar una base de datos interna en el servidor o conectarse a "Microsoft Active Directory" mediante el uso de de un agente replicador.

III.3.6 Configuración de Puntos de Acceso

El punto de acceso se deberá configurar con la dirección IP que coincida con el de uno de los clientes del servidor RADIUS para que este lo identifique. Además deberá seleccionarse WPA como modo de seguridad (Figura III.4) y escoger uno de los métodos de cifrado (Figura III.5). Por último deberá configurarse la dirección IP del servidor RADIUS. Así como el puerto de conexión y el secreto compartido (Figura III.6).

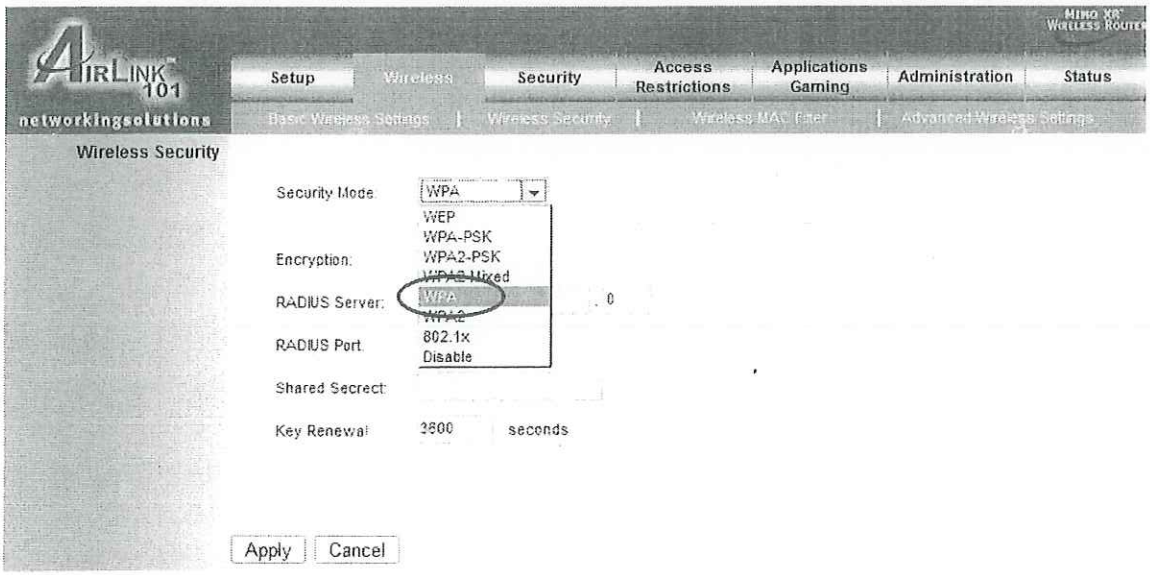


FIGURA III.4 - SELECCIÓN DEL MODO DE SEGURIDAD WPA

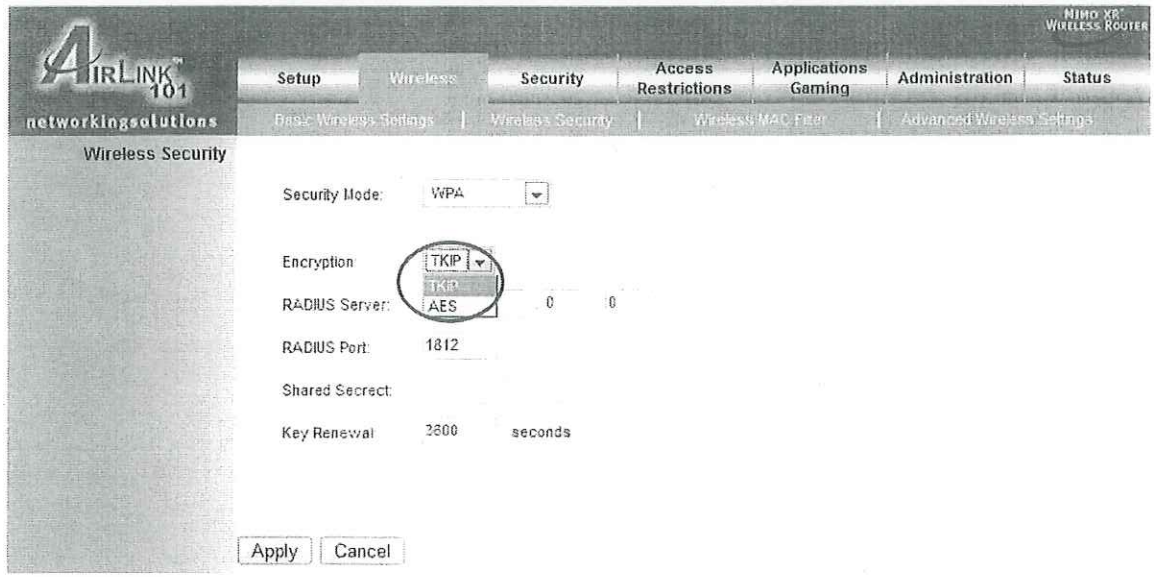


FIGURA III.5 - SELECCIÓN DEL MÉTODO DE CIFRADO

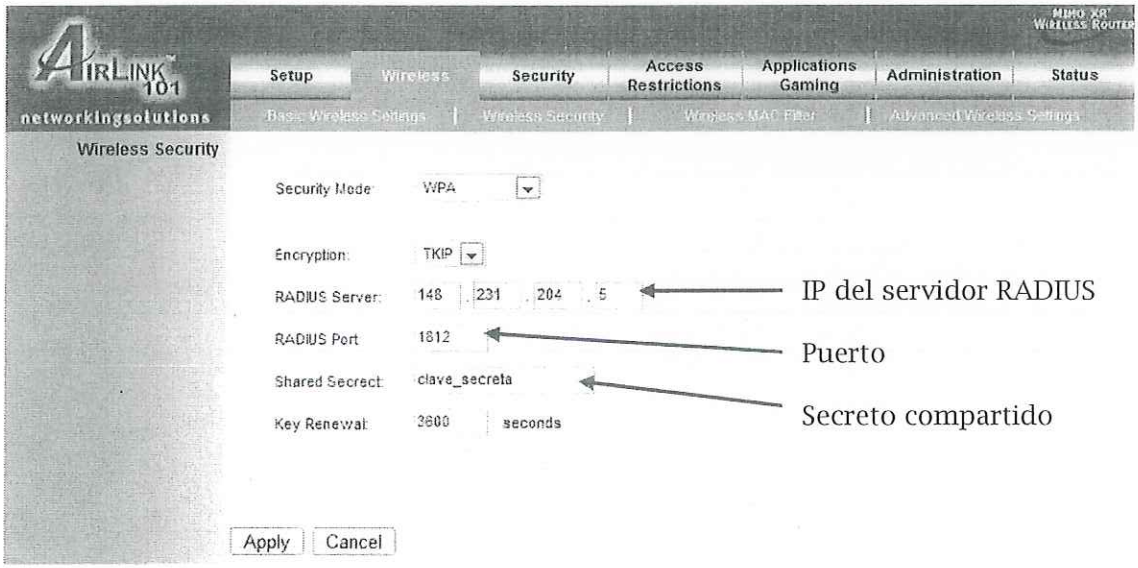


FIGURA III.6 - CONFIGURACIÓN DEL SERVIDOR RADIUS Y DEL SECRETO COMPARTIDO

III.3.5 Configuración de los clientes

Por último, para terminar la instalación se configurarán los suplicantes o clientes. A continuación se muestran los más comúnmente utilizados: Windows, Mac OS X, XSupplicant, Cisco Secure Services Client, Odissey, SecureW2 y WPA_suplicant. En general la configuración se basa en la selección del método de autenticación, credenciales e indicación del usuario y la contraseña.

III.4 Pruebas

Las pruebas que se deberán realizar involucran la evaluación de la seguridad en la red inalámbrica de la organización. Estas puedes realizarse antes de la implementación como método para valorar los riesgos y después de esta para probar la efectividad del sistema de seguridad recién instalado. Existen diferentes técnicas para realizar pruebas de seguridad en una red de cómputo en general, estas se describen detalladamente en el documento (Wack, et al., 2003). Estas técnicas van desde las primordialmente manuales, en las que es necesario de un individuo para realizarlas, hasta las totalmente automatizadas. En este subcapítulo se describirán algunas de esas técnicas, descartando aquellas que no se apliquen en redes inalámbricas. Usualmente se usan más de una de estas técnicas para asegurar para que el resultado sea más completo.

III.4.1 Escaneo de Red

Esta técnica involucra el uso de paquetería de escaneo de puertos para identificar a los nodos potencialmente conectados a la red de la organización, así como los servicios que ofrecen estos nodos (FTP o HTTP). El resultado de este escaneo es una lista de los nodos activos y los servicios que ofrecen. Esta lista podrá ser revisada por el realizador de la prueba para verificar lo siguiente:

- Nodos no autorizados conectados a la red.
- Identificación de servicios vulnerables.
- Identificación de desviaciones de servicios permitidos, definidos en las políticas e seguridad de la organización.
- Preparación para utilizar la prueba de penetración.
- Ayudar en la configuración de un sistema de detección de intrusos.
- Recolección de evidencia forense.

Una vez identificadas las situaciones deberán hacerse las correcciones necesarias, como la desconexión de nodos no autorizados, o la eliminación de servicios innecesarios.

III.4.2 Escaneo de Vulnerabilidades

El software para el escaneo de vulnerabilidades toma el escaneo de puertos y agrega la interpretación de las vulnerabilidades asociadas a cada servicio; este trabajo que en el escaneo de red se dejaba al individuo que realizaba la prueba, ahora se realiza de manera automatizada (Ver Anexo F).

III.4.3 Descifrado de Contraseña

Otra prueba que puede realizarse es la de descifrado de contraseñas. Esto utilizando paquetería que identifica contraseñas débiles. (Ver Anexo F).

III.4.4 Pruebas de "War Driving"

Esta técnica está diseñada para ser utilizada en redes inalámbricas y consiste en convertirse en el atacante de esa red mediante el uso de computadoras portátiles con conexión inalámbrica y herramientas de prueba para detectar redes inalámbricas (ver Anexo F). La frecuencia para realizar esta prueba dependerá de circunstancias tales como:

- Ubicación de la organización.
- Nivel de amenaza de la organización.
- Control organizacional sobre recursos de red.
- El uso de técnicas de seguridad robustas.
- Sensibilidad de la información.

III.4.5 Pruebas de Penetración

En esta técnica el evaluador intenta penetrar la seguridad de la organización. El objetivo de esta técnica es identificar los métodos y obtener el acceso al sistema utilizando herramientas comunes y técnicas utilizadas por atacantes; el ataque puede realizarse desde dentro de la organización o fuera de ella. Estas evaluaciones deben

realizarse con el consentimiento de la organización. La técnica de penetráción consiste en cuatro fases (Figura III.7).

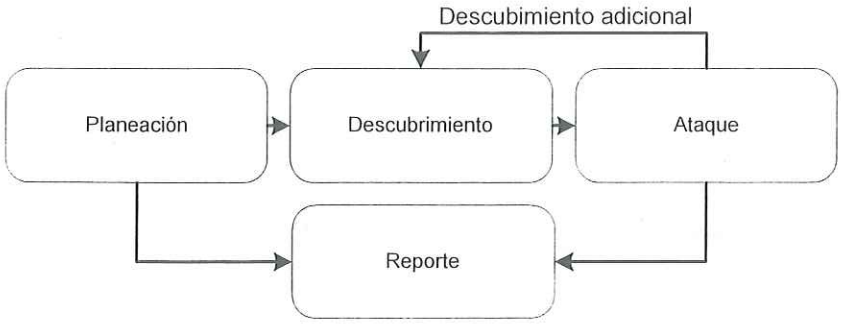


FIGURA III.7 - FASES DE LA PRUEBA DE PENETRACIÓN

En la fase de planeación se establecen las metas y se instituyen las bases para un buen ataque.

En la fase de descubrimiento se realiza un escaneo de puertos para identificar a los posibles blancos. Además del escaneo de puertos se realizan técnicas comúnmente utilizadas para obtener información como:

- Uso de "whois"
- Búsqueda en los servidores Web.
- Búsqueda de LDAP
- Captura de paquetes

La segunda parte de la fase de descubrimiento es el análisis de vulnerabilidades. Una vez detectadas las vulnerabilidades se procede al ataque, en el que se ganará acceso

y se escalará en privilegios. Es aquí donde se realiza un ciclo con la fase de descubrimiento y el ataque; para así ir ganando privilegios.

La fase de reporte ocurre simultáneamente con las demás fases de la prueba.

III.5 Mantenimiento

Durante la etapa de mantenimiento se deberán llevar a cabo las siguientes tareas: escaneo de red, actualización de bases de datos de usuarios y revisión de dispositivos de conexión.

III.5.1 Escaneo de Red

Del mismo modo que en la fase de pruebas, se deberán llevar a cabo escaneos periódicos de los dispositivos conectados a la red, para verificar que no existan nodos no autorizados, identificar servicios vulnerables en los nodos e identificar la desviación de servicios permitidos. Esta información servirá para recolectar evidencia forense en caso de algún ataque, además de ayudar en la configuración de un sistema de detección de intrusos. Una vez identificadas las situaciones deberán hacerse las correcciones necesarias, como la desconexión de nodos no autorizados, o la eliminación de servicios innecesarios. Algunas herramientas para el escaneo de red pueden examinarse en el Anexo F.

III.5.2 Actualización de Bases de Datos

En la tarea de actualización de bases de datos, se deberán eliminar a los usuarios que ya no tengan derechos para utilizar la red inalámbrica, ya sea por haber sido sancionados o porque ya no pertenezcan a la organización. Además deberán agregarse los nuevos usuarios con derecho de conexión a la red inalámbrica.

III.5.3 Revisión de Dispositivos de Conexión

De manera periódica, deberán revisarse los dispositivos de conexión para su buen funcionamiento. Esto es:

- *Revisión de puntos de acceso y su configuración.* Verificar que los puntos de acceso se encuentre configurados de acuerdo a la implementación. Además de realizar el mantenimiento físico preventivo de los equipos y cableado (para evitar la acumulación de polvo y posible deterioro de las conexiones por efecto de la oxidación).
- *Monitoreo de los servidores de autenticación.* Mantener actualizados los sistemas operativos y firmwares de los servidores para evitar agujeros de seguridad. Además de identificar intentos y ataques a los servidores de autenticación. Una vez identificados los posibles ataques se deberán realizar las tareas necesarias para evitar más en un futuro.

IV. Caso de Estudio

La aplicación de la metodología se llevó a cabo en la red inalámbrica de la Facultad de Ciencias Marinas de la UABC [RI-FCM], la información se obtuvo de la unidad de administración de red de esa Facultad.

IV.1 Análisis de Requerimientos

La RI-FCM surgió como resultado de las necesidades de los profesores y alumnos de esta facultad de tener conexión a Internet y a la red interna de la UABC dentro de las aulas y áreas verdes.

La configuración de los clientes corre a cuenta del administrador de red, el cual asigna una dirección IP a cada computadora; todo esto con el fin de cumplir con la políticas de "solo conexión a alumnos tesistas, alumnos de posgrado y profesores de la facultad". De esto surge la motivación de instalar un sistema de autenticación que haga de esta tarea algo más sencillo para el cliente y el administrador de red; además de evitar el robo de direcciones IP.

La información que viaja a través de la red inalámbrica puede ser desde una simple conversación con algún mensajero, hasta documentos como publicaciones o tesis, los cuales por sus características deben de guardar cierto grado de confidencialidad hasta

su publicación. De esta situación nace la necesidad de brindar seguridad a la información transmitida por la RI-FCM.

IV.1.1 Situación Actual de la Red Inalámbrica

La FCM está compuesta por 11 edificios enumerados del E12 al E20, además los edificios E27 y E41 (Figura IV.1); de los cuales, a excepción de los edificios 41 y 27, todos cuentan con red cableada. Debido a que la red cableada se limita a los cubículos de profesores y a algunos laboratorios, se dio a la tarea de instalar red inalámbrica que diera cobertura a las áreas verdes de la facultad, además de las aulas de clases; todo esto para satisfacer las necesidades de conexión de los profesores en sus clases y de los alumnos de posgrado y tesistas.

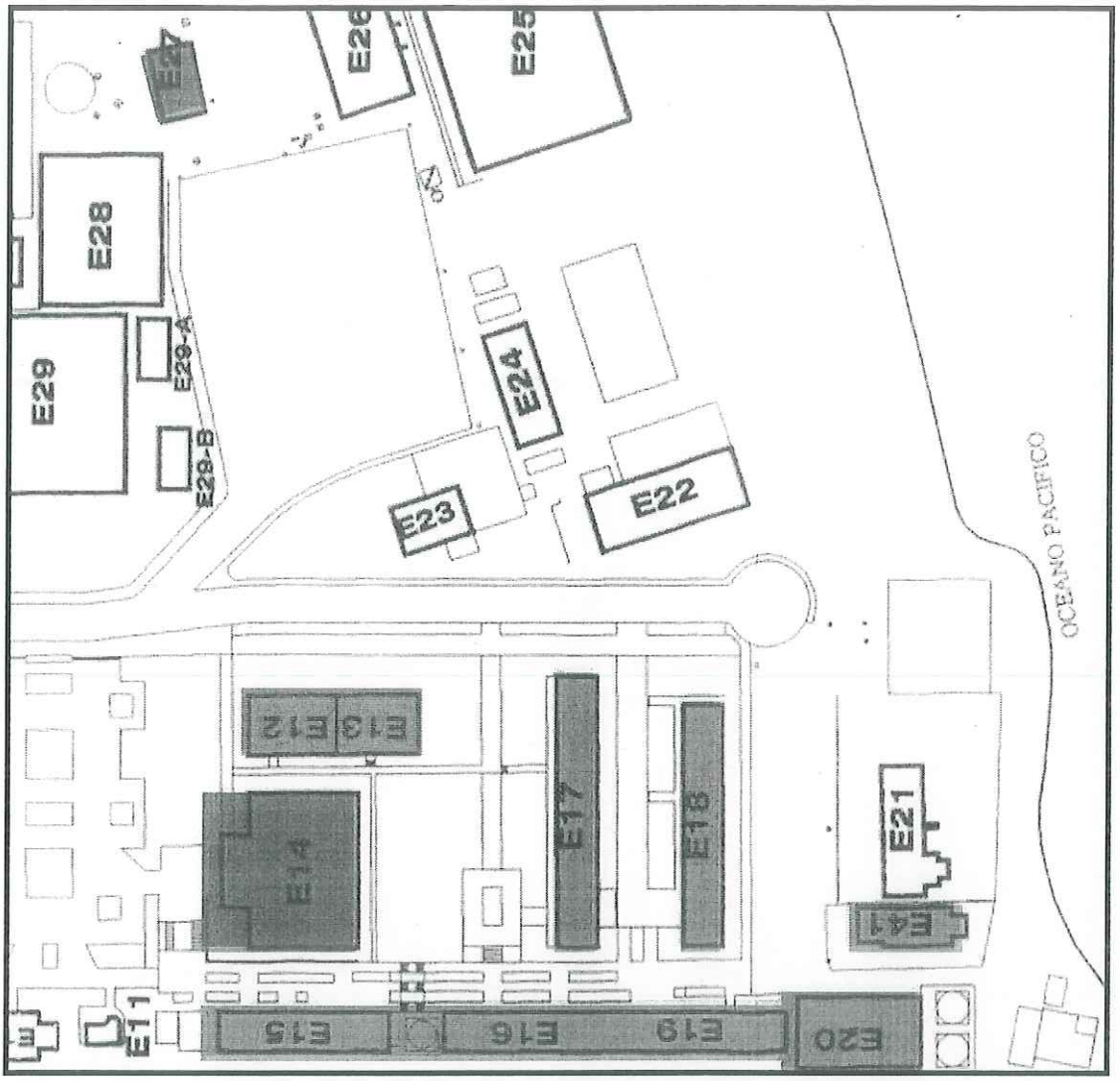


FIGURA IV.1 - EDIFICIOS DE LA FCM

IV.1.2 Requerimientos

- *Usuarios.* Los usuarios se dividen en los siguientes grupos:
    - *Académicos*. Actualmente hay 61 académicos de medio tiempo y tiempo completo en la facultad. La red inalámbrica es usada por los académicos en las aulas de clases.

- *Estudiantes de posgrado*. El número de alumnos de posgrado que solicita el uso de la red inalámbrica, varía de 40, a 50. Utilizan la RI-FCM en las áreas verdes y dentro de algunos laboratorios.
- *Tesistas de Licenciatura*. Existen solo unos pocos tesistas de licenciatura que solicitan tener conexión a la red inalámbrica en las áreas verdes y laboratorios.

La Facultad no cuenta con servidores de autenticación de usuarios. Las bases de datos de usuarios están almacenadas en archivos de los servidores Linux con el servicio SAMBA (smbpasswd), aunque solo el grupo de profesores y alumnos de posgrado están incluidos.

Descripción	Modelo
Switch	Enterasys Vertical Horizon VH-2402S2
Punto de Acceso	Enterasys Networks Access Point, Roam About R2 Access Platform / RBTR2-A
2 Tarjetas de red	Enterasys Networks RoamAbout 802.11b DS High Rate CSIBD-AA-128
2 Antenas	Cisco Aironet Omnidireccional

TABLA IV.1 - DESCRIPCIÓN DE DISPOSITIVOS DE RED DE LA RI-FCM

- *Conexiones.* La topología de la RI-FCM se muestra en la figura IV.2 y su ubicación dentro de la topología de la red de la Facultad en la figura IV.3.

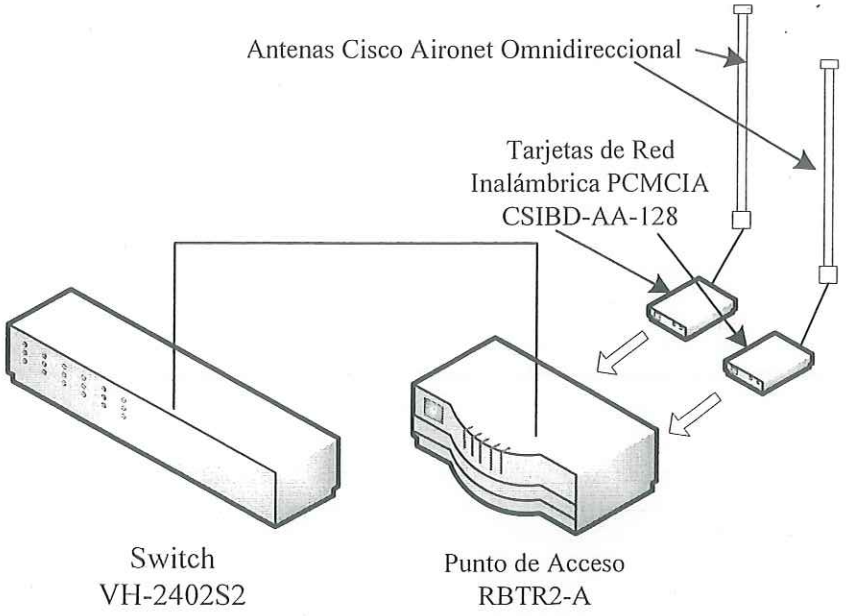


FIGURA IV.2 - CONEXIONES DE LOS DISPOSITIVOS DE LA RI-FCM

- *Instalaciones.* La RI-FCM cuenta con dos antenas y un punto de acceso con tarjetas de red marca Enterasys ubicados en el edificio E17, estos dispositivos están conectados a la red cableada mediante un cable UTP acoplado a un switch de la misma marca (Tabla IV.1).
- *Área de cobertura.* La red inalámbrica da servicio a las áreas verdes entre los edificios 14, 17 y 18; además de los salones de clases ubicados dentro del edificio 18, laboratorios en los edificios 15,16 y 19 y el almacén situado en el edificio 13 (Figura IV.4). En el área de cubículos y aulas del edificio 17 es muy la baja señal de la red inalámbrica, esto causado por el concreto con que están hechos los techos y paredes de este edificio.

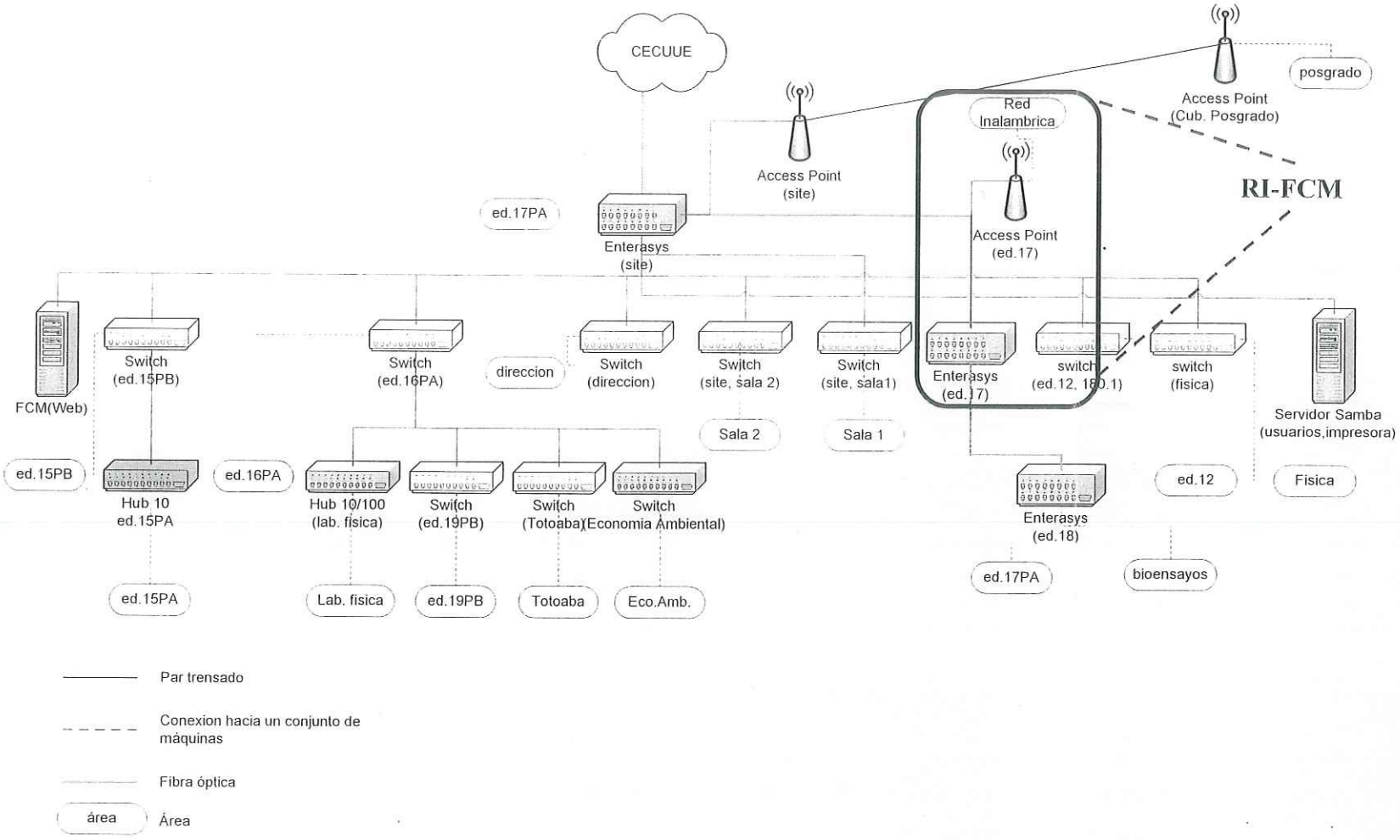


FIGURA IV.3 - TOPOLOGÍA DE LA RED DE LA FCM Y UBICACIÓN DE LA RI-FCM.

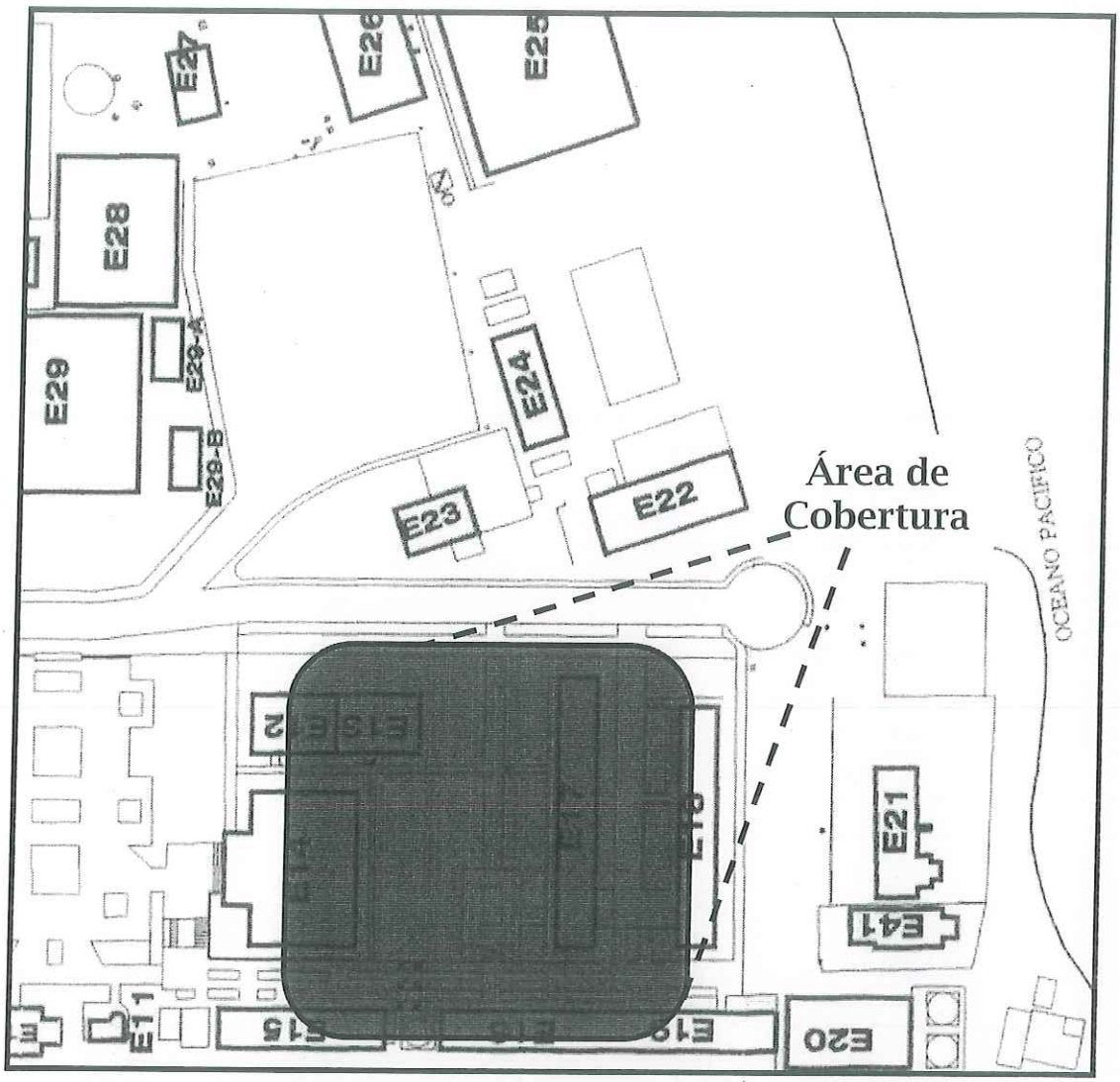


FIGURA IV.4 - ÁREA DE COBERTURA DE LA RED INALÁMBRICA

- *Aplicación.* Las aplicaciones que los usuarios manejan en la RI-FCM son: navegadores, correo electrónico, transferencia de archivos y mensajeros.
- *Seguridad.* La información enviada a través de la RI-FCM y almacenada en los servidores de la facultad puede llegar a ser documentos como: tesis, publicaciones, información y datos de proyectos de la facultad, entre otros; todos estos con un carácter de confidencialidad.

- *Plataforma de clientes.* Las computadoras de los usuarios tienen en su mayoría sistemas operativos Windows XP, aunque existen algunos pocos con Windows Vista y Mac OS.
- *Políticas.* La única política que se aplica en la red inalámbrica es la que permite la conexión a la RI-FCM a los alumnos de posgrado, tesistas de licenciatura y profesores de la facultad, exclusivamente. Aunque hereda políticas de seguridad de la red de cómputo de la UABC, establecidas por el área de seguridad en cómputo del Departamento de Información Académica [DIA].

IV.2 Planeación

IV.2.1 Determinación del Método EAP más Adecuando

Se examinó la página de Wi-Fi Alliance para verificar los certificados de interoperabilidad Wi-Fi de los dispositivos de la RI-FCM (Figuras IV.5, y IV.6) y se encontró que ninguno de ellos tiene capacidad de proveer seguridad WPA, ni de utilizar algún método EAP. También se buscó información sobre posibles actualizaciones de los firmwares para poder soportar WPA, pero no se encontró ninguna información al respecto. Con esta información, se llego a la conclusión de buscar el método EPA más adecuado tomando en cuenta solo los requerimientos de seguridad de la red inalámbrica y las características de cada método.

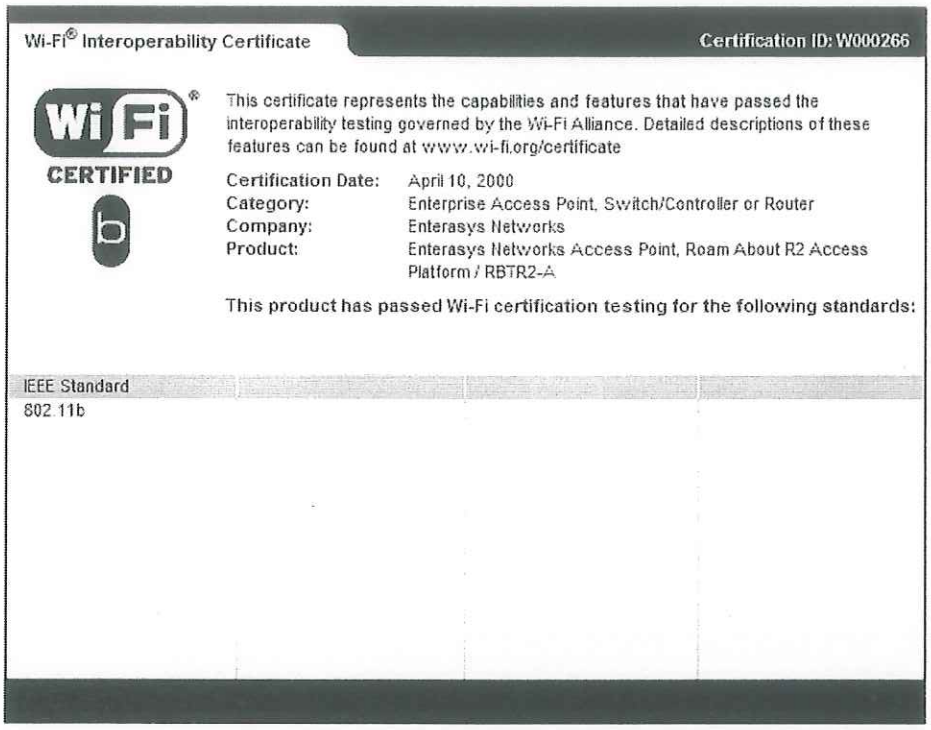


FIGURA IV.5 - CERTIFICACIÓN WI-FI DEL PUNTO DE ACCESO MODELO ROAM ABOUT R2

FIGURA IV.6 - CERTIFICACIÓN WI-FI DE LAS TARJETAS DE RED INALÁMBRICAS MODELO ROAM ABOUT 802.11B DS HIGH RATE

Se requiere de un método que ofrezca una gran seguridad en la transferencia de la información y que además autentifique al usuario por medio de contraseñas; Además que pueda ser configurado con facilidad en equipos con Windows XP, Vista, y MacOS. No se seleccionó MD5 por contar con una seguridad bastante baja. LEAP también fue descartado, aunque ofrece buena seguridad, usa contraseñas y es sencillo de implementar, es un método propietario y requiere de la instalación de un suplicante en todos los clientes. De los tres restantes, TLS implica una difícil implementación y TTLS requiere al igual que LEAP de la instalación de un suplicante en sistemas operativos Windows XP. La opción elegida y que cumple con los requerimientos de seguridad y de compatibilidad es PEAP, ya que puede ser instalado en clientes Windows y MacOs sin necesidad de ningún software extra, es de moderada dificultad en la implementación, puede utilizar contraseñas y ofrece una gran seguridad en la información transmitida.

IV.2.2 Selección del Servidor de Autenticación

La mayoría de los servidores de autenticación, comerciales y de distribución libre, ofrecen interoperabilidad con el método seleccionado. Se eligió FreeRADIUS por ser solución de bajo costo y no tener una gran complejidad en la instalación y configuración.

IV.2.3 Selección de la Base de Datos para Autenticación

La selección de la base de datos de usuarios fue una tarea sencilla de realizar, ya que la organización ya cuenta con una. La fuente de datos elegida fueron los archivos de texto de su servidor Linux (passwd, shadow y group), en el cual ya se han agregado a la mayoría de los usuarios y esta ordenado por grupos. La tarea que deberá de realizarse durante la implementación será la de agregar a los usuarios faltantes.

IV.2.4 Selección de los Puntos de Acceso

No se puede seleccionar una marca y modelo específicos de puntos de acceso pero si se pueden señalar las características que debes de cumplir estos dispositivos. Estas características son: proporcionar seguridad con WPA y tener capacidad de utilizar el método PEAP; además de ofrecer conexión para una o más antenas omnidireccionales. En el caso de tener una sola conexión para antenas se deberán contemplar dos puntos de acceso para poder satisfacer la misma área de cobertura. Algunos ejemplos de posibles puntos de acceso para esta solución son:

- Cisco Aironet 1300 Series AIR-BR1310G
- RoamAbout AP 4102 de Enterasys

Observando las características de estos dos puntos de acceso (Anexo G) se puede notar que los dos cumplen perfectamente con los requerimientos establecidos, la diferencia más grande radica en que el punto de acceso de marca Cisco cuenta con

antenas integradas y tiene un costo mayor. El punto de acceso marca Enterasys ofrece conexión para dos antenas externas, lo que permitirá usar la instalación de las antenas actuales.

IV.2.5 Diseño del Proyecto

Para terminar la fase de planeación se realizó el diseño, en el que se incluyeron la especificación de los componentes a utilizar, la arquitectura del sistema, las conexiones de los dispositivos antes y después de la implementación, así como los pasos a seguir para la instalación.

La arquitectura del sistema, los componentes a utilizar en esta implementación, así como el rol que tendrá cada uno, se muestra en la figura IV.7

Componentes de la arquitectura:

- *Suplicantes.* No es necesaria la instalación de clientes, ya que los sistemas operativos de los usuarios ya cuentan con el suplicante necesario para conectarse utilizando el método EAP seleccionado. Los clientes contemplados en esta implementación son los que cuentan con sistemas operativos Windows XP, Windows Vista y MacOS.

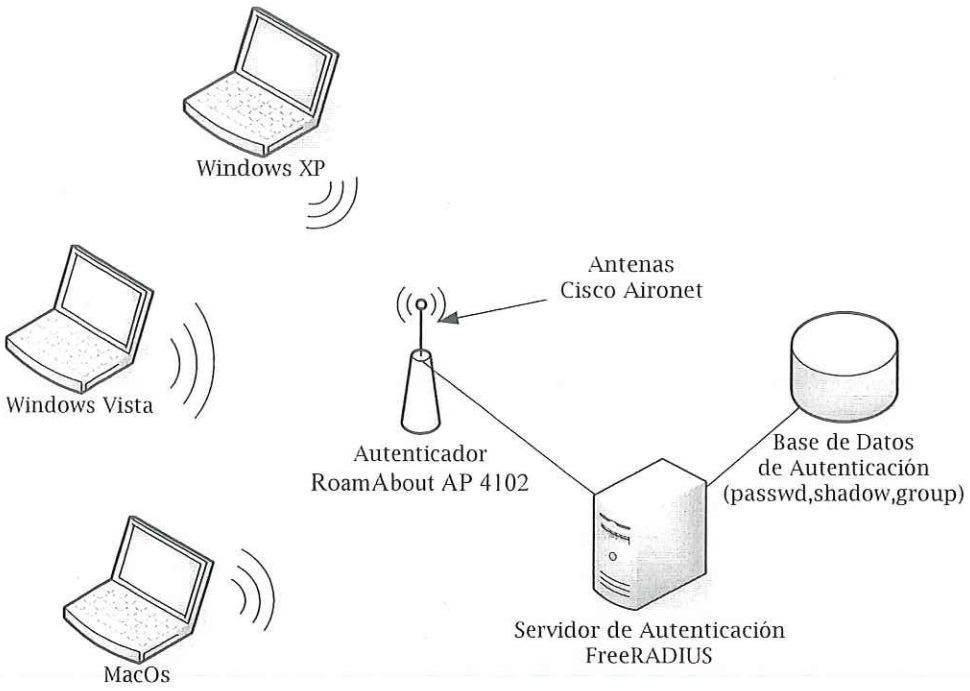


FIGURA IV.7 - ARQUITECTURA DE SEGURIDAD DE LA RI-FCM.

- *Autenticador.* El punto de acceso seleccionado es RoamAbout AP 4102 de Enterasys, cuenta con capacidad de conexión para dos antenas externas utilizando conectores RP-SMA y una conexión hacia la red cableada a través de un puerto RJ-45. Este punto de acceso podrá remplazar al actual, utilizado la misma ubicación y conexiones a la red cableada y antenas.
- *Servidor de Autenticación.* El servidor de autenticación a utilizar es un FreeRADIUS, el cual tendrá que ser instalado durante la fase de implementación. Deberá ser configurado para autenticar usuarios de los archivos passwd, shadow y group del servidor de usuarios de la facultad.

- *Bases de Datos de Autenticación.* Se utilizaran los archivos passwd, shadow y group del servidor de usuarios de la facultad y solo se agregaran los usuarios faltantes.
- *Antenas.* Se utilizarán las antenas con que actualmente cuenta la RI-FCM, solo será necesaria la instalación de un conector RP-SMA para unirlas al punto de acceso seleccionado.
- *Método EAP.* Se utilizará PEAP como método de autenticación.

Conexión de dispositivos antes y después de la implementación:

- *Antes.* Las antenas Cisco Aironet están conectadas a dos tarjetas de red inalámbrica CSIBD-AA-128 acopladas al punto de acceso Enterasys RoamAbout RBTR2-A. El punto de acceso se conecta a la red cableada a través de un cable UTP con puntas RJ-45 enchufadas al switch Enterasys VH-2402S2 (Figura IV.8).
- *Después.* Las antenas Cisco Aironet están conectadas al punto de acceso Enterasys RoamAbout AP 4102. El punto de acceso se conecta a la red cableada a través de un cable UTP con puntas RJ-45 enchufadas al switch Enterasys VH-2402S2 (Figura IV.8).

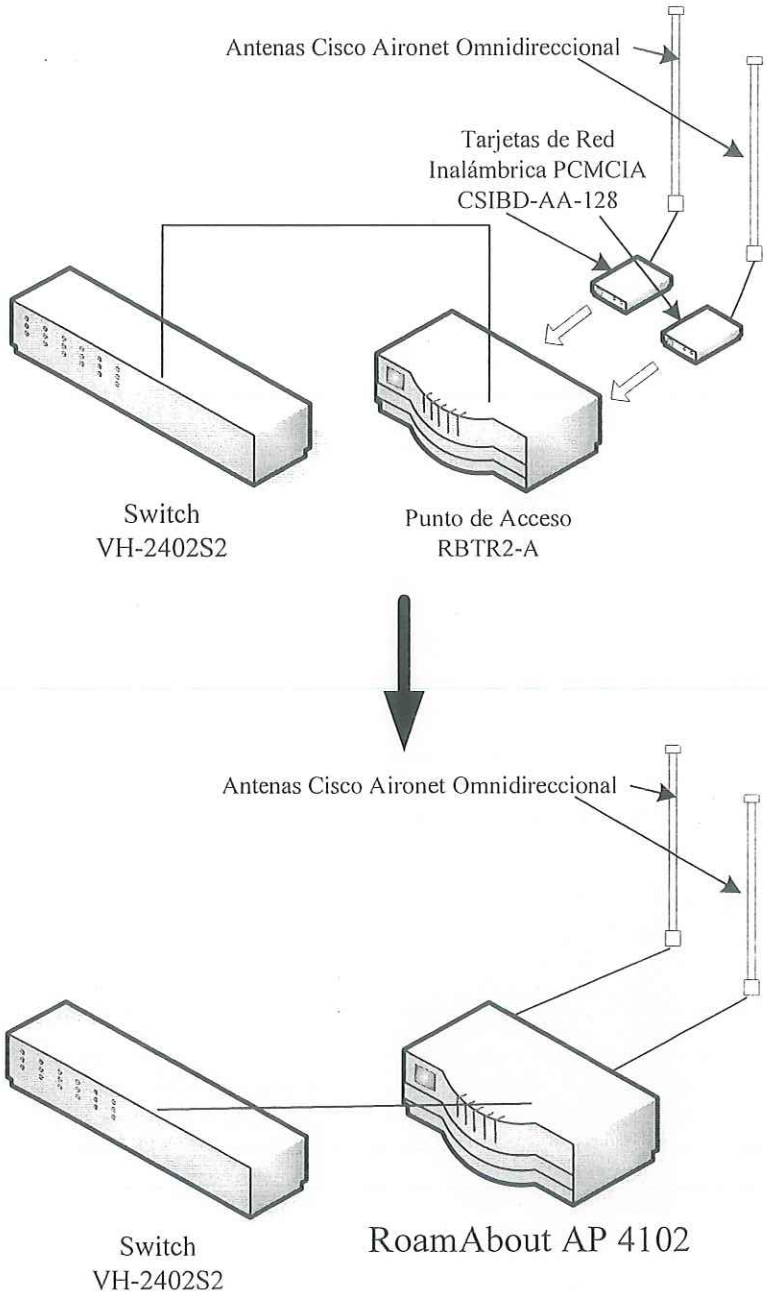


FIGURA IV.8 - CONEXIONES DE LOS DISPOSITIVOS DE LA RI-FCM ANTES Y DESPUÉS DE LA IMPLEMENTACIÓN

Pasos a realizar durante la instalación:

- *Base de Datos de Autenticación.* Agregar a los usuarios faltantes.

- *Servidor FreeRADIUS.* Instalar el servidor de autenticación FreeRADIUS siguiendo los pasos del Anexo C. Además de configurarlo para autenticar usuarios en la base de datos seleccionada.
- *Punto de Acceso.* Realizar la instalación física del punto de acceso y la configuración del mismo para utilizar el servidor de autenticación y método EAP seleccionado.
- *Suplicantes.* Configurar suplicantes o realizar manuales de instalación para cada sistema operativo, lo que facilitará la administración y configuración de los clientes.
- *Pruebas.* Realizar pruebas de descifrado de contraseñas y de penetración a la red inalámbrica para examinar alguna posible vulnerabilidad en la instalación.

IV.2.6 Factibilidad del Proyecto

Los costos de la implementación y tiempos de instalación (ver Tabla IV.2), así como la seguridad que impondrá en la red inalámbrica comparada con la que cuenta actualmente, hacen de este proyecto una tarea necesaria con pocos puntos en contra y muchas ventajas (ver Tabla IV.3), por lo que la factibilidad de realizar este proyecto es muy alta.

Dispositivo	Descripción	Costo	Tiempo de Instalación
Switch	Enterasys Vertical Horizon VH-2402S2	$0 m.n. (existente)	0 min.
Punto de Acceso	Enterasys Networks Access Point, Roam About AP 4102	Entre $4000 y $5000 m.n.	5 horas
2 Antenas	Cisco Aironet Omnidireccional	$0 m.n. (existentes)	20 min. (Solo para la conexión)
Servidor de Autenticación	FreeRADIUS	$0 m.n. (PC existente, servidor de distribución libre)	5 horas
Base de Datos de Usuarios	archivos passwd, shadow y group	$0 m.n. (existente)	0 min.
Mano de obra	-	$0 m.n. (personal actual capacitado)	-
Total		**Entre $4000 y $5000 m.n**	**10 horas con 20 minutos como máximo**

TABLA IV.2 – COSTOS Y TIEMPOS DE IMPLEMENTACIÓN DEL PROYECTO PROPUESTO

Ventajas	Desventajas
• Autenticación de usuarios	• Tener control de otro servidor más en la Facultad
• Mayor seguridad en la transmisión de datos	• Clientes con sistemas operativos diferentes a los soportados, deberán instalar un suplicante para el método EAP.
• Facilidad para agregar nuevos usuarios	
• Fácil instalación	

TABLA IV.3 – VENTAJAS Y DESVENTAJAS DE LA IMPLEMENTACIÓN PROPUESTA

V. Conclusiones

Hoy en día, en la mayoría de las organizaciones, la entidad más importante es la información. En las redes inalámbricas, la información usa como medio físico de transporte al aire, por lo que la vulnerabilidad a sufrir algún ataque es más alta que en las redes cableadas; es por eso que es de gran importancia implantar un sistema de seguridad en toda red inalámbrica, ya que esto permitirá no solo que la información transmitida no sea "observada" por terceros (privacidad), ni sea alterada durante su transmisión (integridad), sino que también se logrará conocer y limitar a los usuarios que podrán conectarse a esa red inalámbrica (autenticación).

Este trabajo de investigación involucró la recolección, análisis y depuración de un gran acervo de información, lo cual permitió sintetizar y obtener una metodología para la implementación de autenticación y seguridad en redes inalámbricas. Esta metodología es de gran ayuda en la selección de los métodos y componentes necesarios para el propósito especificado, además de servir como guía para las tareas que deberán realizarse durante la implementación. La importancia de esta metodología radica en que desglosa y facilita la labor de instalar o agregar autenticación y seguridad a una red inalámbrica.

Con el caso de estudio desarrollado, se pudo corroborar que la metodología obtenida permite al administrador de red obtener un sistema de seguridad para redes

inalámbricas de manera sencilla y guiada, basándose en la información y situación actual de la red y la organización.

V.1 Trabajo Futuro

Como trabajo futuro, se recomienda unir una metodología para la implementación de redes inalámbricas con esta metodología para implantar seguridad, para así ofrecer una herramienta completa, que sirva a los administradores de red en las decisiones que deberán tomarse durante el diseño y la instalación de una red inalámbrica.

Además, podrán agregarse nuevos métodos de seguridad a la metodología, incluyendo sus descripciones, características y guías de instalación, de tal manera que el administrador de red tenga un amplio espectro de posibilidades para proporcionar seguridad a su red inalámbrica.

Definición de Términos

Autenticación. El servicio usado para establecer la identidad de una estación como miembro de de un grupo de estaciones autorizadas para asociarse con otra estación.

Cifrar. Proceso de codificar información a una forma secreta.

Confidencialidad. Propiedad de la información que la hace no accesible a individuos, entidades o procesos no autorizados.

Control de acceso. Prevención del uso no autorizado de recursos.

Descifrar. Proceso de decodificar información cifrada.

DIAMETER. Es un protocolo de red para la autentificación, autorización y control (AAA) para aplicaciones tales como acceso de red o movilidad IP. El concepto básico es proporcionar un protocolo base que pueda ser extendido para proporcionar servicios AAA a nuevas tecnologías de acceso. Diameter está diseñado para trabajar en local y con roaming de AAA.

Eavesdropping. Termino inglés que traducido al español significa escuchar secretamente, se ha utilizado tradicionalmente en ámbitos relacionados con la seguridad.

Firewall. Es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

Gateway. Es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior.

Integridad. Propiedad de la información que no permite sea modificada por individuos,

entidades o procesos no autorizados.

Interoperabilidad. Dispositivos de diferentes marcas y modelos trabajando en conjunto.

Punto de acceso. Entidad que tenga que proporcione acceso a los servicios a través de un medio inalámbrico.

Abreviaturas y Acrónimos

AAA. Autenticación, Autorización y Manejo de Cuentas (Authentication, Authorization and Accounting)

AES. Estándar de Cifrado Avanzado (Advanced Encryption Standard)

AH. Encabezado de autenticación IP

CCMP. Siglas en ingles. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

DHCP. Protocolo de Configuración Dinámica de Servidor.

EAP. Protocolo de Autenticación Extensible.

EAP-TLS. EAP de Transporte de Capa de Seguridad (EAP-Transport Layer Security)

EAP-TTLS. EAP de Transporte de Capa de Seguridad sobre Tunel (EAP-Tunneled Transport Layer Security)

GTC. Tarjeta de Símbolo Genérico (Generic Token Card)

IBSS. Conjunto de Servicios Básicos Independientes o Independent Basic Service Set.

IEEE. Instituto de Ingenieros Eléctricos y Electrónicos.

IKE. Intercambio de Llaves de Internet

IPsec. Seguridad del Protocolo de Internet.

ISAKMP. Protocolo de la Asociación de Seguridad de Internet y Manejo de Llaves.

ISM. Espectro Industrial, Científico y Medico.

MAC. Control de Acceso al Medio.

MIC. Código de Integridad de Mensaje.

OSA. Autenticación de Sistema Abierto.

OSI. Interconexión de Sistemas Abiertos.

OTP. One time password o contraseña de una sola vez

PEAP. Protocolo de Autenticación Extensible Protegido.

PHY. Capa física del modelo OSI.

PMK. Llave Maestra en Pares (Pairwise Master Key)

PPK. Llave Por Paquete (Per-Packet Key)

PRNG. Ron's Code 4 Pseudo Random Number Generator

PSK. Llave Pre-Compartida.

PTK. Llave Transitoria en Pares (Pairwise Transient Key)

RADIUS. Servicio de Usuario de Acceso Telefónico de Autenticación Remota.

RC4. Siglas en inlges. Rivest Cipher 4 ó Ron's Code 4

SKA. Autenticación de Llave Compartida.

SS. Espectro Disperso (Spread Spectrum)

TACACS. Sistema De Control De Acceso Del Controlador De Acceso A Terminales (Terminal Access Controller Access-Control System)

TACACS+. Sistema De Control De Acceso Del Controlador De Acceso A Terminales + (Terminal Access Controller Access-Control System Plus)

TKIP. Protocolo de Integridad de Llave Temporal.

VPN. Redes Privadas Virtuales.

WECA. Alianza para la Compatibilidad de Ethernet Inalámbrico

WEP. Protocolo Equivalente a Privacidad Cableada.

Wi-Fi. Fidelidad Inalámbrica.

WPA. Acceso Protegido a Wi-Fi.

WPA2. Acceso Protegido a Wi-Fi 2.

Referencias

Arbaugh et al., 2001 — Arbaugh, W. A., Shankar N., y Wan Y. C. J. "*Your 802.11 Wireless Network Has No Clothes*", 2001.

Bartlett, 2005 — Bartlett Scott, "*FreeRadius and MySQL*", 2005.

Borisov et al., 2001 — Borisov, N., Goldberg I., y Wagner D., "*Intercepting Mobile Communications: The Insecurity of 802.11*", 2001.

Cisco, 2002 — CISCO, "*A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite*", 2002.

Congdon, et al., 2003 — Congdon P., Abada B, Smith A., Zorn G., Roese J., "*RFC 3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*", 2003.

Craiger, 2002 — Craiger J. Philip, "*802.11, 802.1X, and Wireless Security*", SANS Institute, 2002.

Earle, 2005 — Aaron E. Earle, "*Wireless Security Handbook*", 2005, Cap. 15 pag. 267-298.

Ferguson, 2002 — Ferguson Niels, "*Michael: an improved MIC for 802.11 WEP*", 2002.

Fluhrer, 2001 — Scott Fluhrer, Itsik Mantin, Adi Shamir, "*Weaknesses in the Key Scheduling Algorithm of RC4*", 2001.

Garaizar-Sagarminaga, 2005 — Garaizar Sagarminaga Pablo, "*Seguridad en redes Wi-Fi*", III Xornadas sobre o Sistema Operativo Linux en Ordes, Galicia 2005.

García-López, 2003 — García López Francisco, "*WPA, Seguridad en Redes Inalámbricas*", 2003.

Gast, 2002 — Gast Matteew, "*A Technical Comparison of TTLS and PEAP*", 2002.

Gast, 2005 — Gast Matteew, "*802.11 Wireless Network: The Definitive Guide*", 2005, O'Reilly, cap. 6 y 7.

Geier, 2002 — Geiger Jim, "*Wireless LAN Deployment Steps*", http://www.wi-fiplanet.com/tutorials/article.php/1377551, 2002.

Geier, 2003 Geiger Jim, "*WPA plugs holes in WEP*", Network Work, 2003.

Haryanto, 2004 Haryanto Ronny, "*802.1X*", 2004.

Hassell, 2002 Jonathan Hassell, "*RADIUS*", 2002, O'Reilly.

Hill, 2001 Joshua Hill, "*An Analysis of the RADIUS Authentication Protocol*", InfoGard Laboratories, 2001.

IEEE, 1999 IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

IEEE, 2001 IEEE, "*Port-Based Network Access Control*", 2001.

InformIT, 2005 Pearson Education, Inc. InformIT, "*Security: Temporal Key Integrity Protocol (TKIP)*", 2005.

Intermec, 2005 Intermec Technologies Corporation, "*Choosing the Right EAP Type for Wireless LAN Security*", 2005.

InteropNet, 2004 LAN Access Security Interoperability Lab, "*Cooking up 802.1X Successfully*", 2004.

James, 2002 Anthon James, "*Using IEEE 802.1X to Enhance Network Security*", Foundry Networks, 2002.

MacMichael, 2005 John L. MacMichael, "*Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key*", 2005.

Madrid-Molina, 2003 Juan Manuel Madrid Molina, "*Seguridad en Redes Inalámbricas 802.11*", 2003.

Martínez, 2002 Evelio Martínez, "*Estándares WLAN*", revista RED, 2002.

Microsoft, 2004 Microsoft Corporation, "*The Advantages of Protected Extensible Authentication Protocol (PEAP): A Standard Approach to User Authentication for IEEE 802.11 Wireless Network Access*", 2004.

Microsoft-TechNet, 2004 The Cable Guy - Microsoft TechNet, "*Wi-Fi Protected Access Data Encryption and Integrity*", 2004.

Moen, 2004 Moen Vebjorn, Raddum Harvard, Hole Kjell J., "*Weakness in the Temporal Key Hash of WPA*", 2004.

Phifer, 2006 Phifer Lisa, "*Choosing the right flavor of 802.1X*", SearchSecurity.com, 2006.

Psion-Teklogix, 2003 — Psion-Teklogix, "*802.11 WLAN security*", 2003.

RFC 2865, 2000 — C. Rigney, S. Willens, A. Rubens, W. Simpson, "*Remote Authentication Dial In User Service (RADIUS) – RFC 2865*", Network working Group, 2000.

RFC 3748, 2004 — B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, "*Extensible Authentication Protocol (EAP) – RFC 3748*", Network working Group, 2004.

RFC 4017, 2005 — D. Stanley, J.Walker, B. Aboba, "*Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs – RFC 4017*", Network working Group, 2005.

Sierra et al., 2004 — Sierra J., Maya M y Betancur L., "*Protocolo de Seguridad WEP*", 2004, http://www.monografias.com.

Snynder, 2002 — Joel Snyder, "*What is 802.1X?*", Network World Global Test Alliance, 2002.

Takahashi, 2004 — Takehiro Takahashi, "*WPA Passive Dictionary Attack Overview*", 2004.

Tauno-Williams, 2006 — Adam Tauno Williams, "*Wireless Alphabet Soup*", 2006. http://www.whitemiceconsulting.com

Villarroel et al., 2004 — Villarroel G. Carlos, Rodríguez P. Angie, Valle P. Julio, "*Diseño De Una Red De Área Local Inalámbrica*", 2004. XII Congreso Internacional de Telecomunicaciones y II Muestra de Tecnología.

Vaughan-Nicols, 2003 — Vaughan-Nicols Steven J, "*Making the WPA Upgrade*", 2003.

Wack et al., 2003 — Wack John, Tracy Miles, Souppaya Murugiah, "*Guideline on Network Security Testing Recommendations of the National Institute of Standards and Technology*", 2003, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8930.

Wi-Fi-Alliance, 2004a — Wi-Fi-Alliance, "*Wi-Fi Protected Access*", 2004.

Wi-Fi-Alliance, 2004b — Wi-Fi-Alliance, "*WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks*", 2004.

Wi-Fi-Alliance, 2005 — Wi-Fi-Alliance, "*Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise*", 2005.

Wong, 2003 Stanley Wong, "*The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards*", 2003.

Anexos

A) Manual para la instalación y configuración de un servidor OpenLDAP (Calzada-Pradas, 2000)

Instalación de OpenLDAP. Para instalar el servidor de directorio OpenLDAP hace falta seguir los siguientes pasos:

- Copiar el software en el servidor. Este software esta públicamente accesible en http://www.openldap.org. Habitualmente hay dos versiones, la distribución release, es la distribución original, la distribución stable, tiene corregidos los errores que se han podido detectar en la versión release.

- Descomprimir y desempaquetar la distribución.

```
#gzip –dc openldap-stable.tgz | tar xvf
ldap/
ldap/doc/
ldap/doc/man/
ldap/doc/man/Makefile.in
ldap/doc/man/man1/
...
```

- Ejecutar el comando configure con las opciones necesarias. Para ello es aconsejable ejecutarlo primero con la opción –help.

```
# ./configure –help
```

- Una vez configurado, se comprueban las dependencias y se procede a compilar el servidor.

```
# make depend
# make
```

- Tras la compilación del servidor, procederemos a comprobar que los programas generados funcionan de modo correcto.

```
# cd tests
# make
```

- Si todo ha ido correctamente, se puede proceder a la instalación del servidor.

```
# su
Password:
# make install
```

Para más información pueden consultarse los ficheros README e INSTALL que acompañan a la distribución y la documentación sobre el proceso de instalación en el servidor Web del proyecto OpenLDAP (http://www.openldap.org).

Configuración de OpenLDAP. La configuración del servidor OpenLDAP se almacena en el fichero <directorio_instalacion>/etc/openldap/slapd.conf. Este fichero contiene información para el servidor slapd, pero también es utilizado por slurpd, programa encargado de las réplicas, y por los programas de indexación LDBM (ldif2ldbm, ldif2index, ldif2id2entry y ldif2id2children.

El fichero slapd.conf contiene una serie de directivas globales, que se aplican al servidor slapd y todas las bases de datos definidas, seguidas de definiciones de bases de datos específicas.

El formato general del fichero tiene el siguiente aspecto:

```
# comment - these options apply to every database
<global configuration options>
# first database definition & configuration options
database <backend 1 type>
<configuration options specific to backend 1>
# subsequent database definitions & configuration options
...
```

Pueden incluirse tantas secciones específicas para bases de datos como sean necesarias. Las opciones incluidas en estas secciones tienen prioridad sobre las opciones generales. Las líneas en blanco y las que comiencen por # son tratadas como comentarios. Las líneas que comiencen con un espacio en blanco son tratadas como continuación de la línea anterior.

Opciones globales de configuración. Las opciones descritas en esta sección se aplican a todos los servicios de base de datos, salvo que sean redefinidas en una definición específica.

```
access to <what> [ by <who> <accesslevel> ]+
```

Esta opción permite el acceso (especificado en <accesslevel>) al conjunto de entradas y/o atributos (especificados en <what>) por los solicitantes (especificados en <who>).

```
attribute <name> [<name2>] { bin | ces | cis | tel | dn }
```

Esta opción asocia una sintaxis con un nombre de atributo. Por defecto se asume que la sintaxis de un atributo es cis.

```
defaultaccess { none | compare | search | read | write }
```

Esta opción especifica los permisos que se asignan cuando no hay ninguna coincidencia en las listas de control de accesos. Un determinado nivel de acceso contiene los niveles inferiores. Por defecto es read.

```
include <filename>
```

Esta opción permite indicar a slapd que debe leer el fichero especificado como parte de la configuración. Esta opción suele emplearse para incluir los ficheros slapd.at.conf y slapd.oc.conf, que contienen las especificaciones de los tipos de datos de los atributos (utilizando la opción attribute) y las definiciones de las reglas del esquema (utilizando la opción objectclass)

```
Loglevel <integer>
```

Esta opción permite indicar el nivel de traza que se desea (utilizando el programa syslogd y la utilidad LOG_LOCAL4).

```
objectclass <name> [ requires <attrs> ] [ allows <attrs> ]
```

Esta opción define las reglas del esquema para la clase definida. Esta opción se utiliza en conjunción con la opción schemacheck.

```
referral <url>
```

Esta opción permite especificar la referencia a devolver a un cliente cuando slapd no pueda localizar una base de datos local para completar la petición.

```
schemacheck { on | off }
```

Esta opción activa el control de las operaciones de actualización para que los resultados sean conformes al esquema. Por defecto esta desactivada (off).

```
sizelimit <integer>
```

Esta opción permite limitar el número máximo de entradas que el servidor slapd devolverá en una operación de búsqueda. Por defecto es 500.

```
timelimit <integer>
```

Esta opción específica el tiempo máximo en segundos (en tiempo real) que el servidor slapd empleará para responder a una petición. Si no ha completado la petición, devolverá un mensaje indicando que el tiempo máximo ha sido excedido.

B) Manual para la instalación de un servidor FreeRADIUS

FreeRADIUS es un servidor de autenticación de libre distribución muy completo y eficiente. Actualmente viene incluido en los discos de instalación de la mayoría de las distribuciones del sistema operativo Linux. De ser así, se puede instalar fácilmente, utilizando la herramienta para la instalación de paquetes RPM que se incluye en el sistema operativo, o mediante la siguiente instrucción que puede ser ejecutada como "superusuario" (usuario root):

```
#rpm –ivh freeradius-X.X.X-X.XXX.rpm
```

De no existir el paquete RPM o en caso de que se use otro sistema operativo basado en Unix, se puede buscar el archivo de instalación para ser compilado en la página web de FreeRADIUS y se sigue los pasos que se muestran a continuación:

- Descarga el archivo comprimido de instalación de la página www.freeradius .org
- Extrae el contenido del archivo tar.

```
tar -zxvf freeradius.tar.gz
```

- Ejecutar en el directorio que contenga los archivos de instalación (usuario root):

```
# ./configure.
# make.
#  make install.
```

Configuración. Para configurar el servidor FreeRADIUS se edita los archivos de configuración de la carpeta principal del software llamada raddb, la ubicación de esta carpeta dentro de un entorno Unix/Linux es en la mayoría de los casos en: /etc/raddb/. Los archivos de configuración son: radius.conf, client.conf, users e eap.conf.

users

Archivo donde se especifican las credenciales de los usuarios de la red. En este ejemplo definimos el usuario test con la clave test. Estas credenciales tendremos que ingresar cuando intentemos conectarnos a la red inalámbrica.

```
test Auth-Type := Local , User-Password == "test"
```

clients.conf

Descripción y credenciales de los diferentes dispositivos que consultan al RADIUS (ejemplo: Puntos de Accesos).

```
client 192.168.13.91 {
secret = testing123
shortname = AP-RADIUS
}
```

eap.conf

Archivo de configuración de las directivas EAP a utilizar.

```
Archivo de configuración de las directivas EAP a utilizar.
eap {
default_eap_type = tls
timer_expire = 60
ignore_unknown_eap_types = no
cisco_accounting_username_bug = no
# Supported EAP-types
# EAP-TLS
tls {
private_key_password = laclave
private_key_file = ${raddbdir}/certs/servidor-prueba.key
certificate_file = ${raddbdir}/certs/servidor-prueba.crt
CA_file = ${raddbdir}/certs/demoCA/cacert.pem
dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
fragment_size = 1024
include_length = yes
}
```

```
peap {
default_eap_type = mschapv2
}
mschapv2 {
}
```

radius.conf

Archivo general de configuración de FreeRADIUS.

```
prefix = /usr/local
exec_prefix = ${prefix}
sysconfdir = ${prefix}/etc
localstatedir = ${prefix}/var
sbindir = ${exec_prefix}/sbin
logdir = ${localstatedir}/log/radius
raddbdir = ${sysconfdir}/raddb
radacctdir = ${logdir}/radacct
# Location of config and logfiles.
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/radiusd
#
log_file = ${logdir}/radius.log
#
libdir = ${exec_prefix}/lib
#
pidfile = ${run_dir}/radiusd.pid
#
max_request_time = 30
#
delete_blocked_requests = no
#
cleanup_delay = 5
#
max_requests = 1024
#
bind_address = *
#
port = 0
#
hostname_lookups = no
#
allow_core_dumps = no
#
regular_expressions = yes
extended_expressions = yes
#
log_stripped_names = yes
#
log_auth = yes
#
```

```
log_auth_badpass = yes
log_auth_goodpass = yes
#
usercollide = no
#
lower_user = no
lower_pass = no
#
nospace_user = no
nospace_pass = no
#
checkrad = ${sbindir}/checkrad
# SECURITY CONFIGURATION
security {
max_attributes = 200
reject_delay = 1
status_server = no
}
# PROXY CONFIGURATION
proxy_requests = no
# CLIENTS CONFIGURATION
$INCLUDE ${confdir}/clients.conf
# SNMP CONFIGURATION
snmp = no
# THREAD POOL CONFIGURATION
thread pool {
start_servers = 5
max_servers = 32
min_spare_servers = 3
max_spare_servers = 10
max_requests_per_server = 0
}
# MODULE CONFIGURATION
modules {
$INCLUDE ${confdir}/eap.conf
mschap {
authtype = MS-CHAP
}
files {
usersfile = ${confdir}/users
acctusersfile = ${confdir}/acct_users
preproxy_usersfile = ${confdir}/preproxy_users
compat = no
}
}
# Instantiation
instantiate {
}
#
authorize {
files
mschap
eap
```

```
}
# Authentication.
authenticate {
Auth-Type MS-CHAP {
mschap
}
eap
}
#
preacct {
}
#
accounting {
}
#
session {
}
#
post-auth {
}
#
pre-proxy {
}
#
post-proxy {
}
```

Arrancar FreeRADIUS. Para arrancar el servicio ejecutamos:

```
# /usr/local/sbin/radiusd -f -X

...
Listening on authentication *:1812
Listening on accounting *:1813
Ready to process requests.
```

C) Manual para la implementación de la base de datos para autenticación con FreeRADIUS (Bartlett, 2005).

Agregar la base de datos RADIUS a MySQL. Lo primero es generar una base de datos vacía con el nombre de 'radius' en MySQL y proporcionar los usuarios y permisos necesarios para manejarla.

El siguiente paso es generar el esquema para la base de datos. Para esto existe un archivo que lo describe, este archivo es un script SQL y se encuentra /src/modules/rlm_sql/drivers/rlm_sql_mysql/db_mysql.sql dentro del directorio de FreeRadius. Este script puede ser ejecutado de diferentes maneras, una de ellas es ejecutarlo localmente usando el siguiente comando:

```
mysql -u{root} -p{rootpass} radius < db_mysql.sql
```

Donde 'root' y 'rootpass' son los previamente configurados para el manejo de esta base de datos.

Configurar FreeRADIUS para trabajar con MySQL. Editar el archivo /usr/local/etc/raddb/sql.conf introduciendo el nombre del servidor, usuario y contraseña para conectarse al servidor MySQL y la base de datos de RADIUS. La base de datos y los nombres de las tablas deberán dejarse sin modificar en el caso de usar el esquema por defecto.

Editar tambien el archivo /usr/local/etc/raddb/radiusd.conf agregando la línea 'sql'a la sección de 'authorize{}', justo antes de 'files'.

Además agregar la línea 'sql' a la sección de 'accounting{}', en medio de 'unix' y 'radutmp'.

El final del archivo radius.conf deberá lucir así:

```
authorize {
        preprocess
        chap
        mschap
        #counter
        #attr_filter
        #eap
        suffix
        sql
        #files
```

```
        #etc_smbpasswd
}

authenticate {
        authtype PAP {
                pap
        }
        authtype CHAP {
                chap
        }
        authtype MS-CHAP{
                mschap
        }
        #pam
        #unix
        #authtype LDAP {
        #       ldap
        #}
}

preacct {
        preprocess
        suffix
        #files
}

accounting {
        acct_unique
        detail
        #counter
        unix
        sql
        radutmp
        #sradutmp
}

session {
        radutmp
}
```

Llenar la base de datos. Ahora se deberá agregar usuarios a la base de datos para poder realizar una prueba. La información deberá quedar de la siguiente manera:

- En 'usergroup' se ponen todos los usuarios, cada uno con el grupo asignado.
- En 'radcheck' se agregan todos los usuarios, incluyendo la contraseña y el atributo de la contraseña. Se deberá dejar en blanco el campo 'op'.
- En 'radreply' se agregan los atributos específicos que deberán regresar y a que usuario.
- En 'radgroupreply' se crean los atributos a ser regresados para cada grupo.

Continuación se muestra un ejemplo de cómo quedarían las tablas en la base de datos 'radius':

usergroup

ID	UserName	GroupName
1	Jhassell	Dialin
2	Rneis	Staticdial
3	Bgrossman	Suspended
4	Awatson	dialin

radcheck

ID	UserName	Attribute	Value	Op
1	Jhassell	Password	Changeme	==
2	Rneis	Password	Thewb	==
3	Bgrossman	Password	Sarah	==
4	Awatson	Password	Moo	==

radreply

ID	UserName	Attribute	Value
1	Rneis	Framed-IP-Address	66.26.224.46
2	Bgrossman	Auth-Type	Reject

radgroupreply

ID	GroupName	Attribute	Value	Op
34	Dialin	Framed-Compression	Van-Jacobsen-TCP-IP	==
33	Dialin	Framed-Protocol	PPP	==
32	Dialin	Service-Type	Framed-User	==
31	Dialin	Auth-Type	Local	:=
35	Dialin	Framed-MTU	1500	==
36	Staticdialin	Auth-Type	Local	:=
37	Staticdialin	Framed-Protocol	PPP	==
38	Staticdialin	Service-Type	Framed-User	==
39	Staticdialin	Framed-Compression	Van-Jacobsen-TCP-IP	==

Probar instalación. Con la configuración complete se deberá reiniciar FreeRADIUS y probar la instalación usando 'radtest' (o NTradPing); el usuario podrá autenticar y se mostrara una salida de retroalimentación mostrando la comunicación entre FreeRADIUS y MySQL.

D) Manual para la instalación un servidor de DHCP

Descripción. DHCP [Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Nodos] es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuánto tiempo la ha tenido, a quien se la ha asignado después.

Instalación. Existe una implementación del protocolo DHCP programada y mantenida por el ISC [Internet Systems Consortium]. El software puede descargarse de su página web, aunque la gran mayoría de las distribuciones de Linux han compilado un paquete que incluye la versión de DHCP del ISC. Se puede instalar fácilmente, utilizando la herramienta para la instalación de paquetes RPM que se incluye en el sistema operativo, o mediante la siguiente instrucción que puede ser ejecutada como "superusuario" (usuario root):

```
#rpm –ivh dhcpd-X.X.X-X.XXX.rpm
```

Otra opción para instalarse es mediante el uso de los archivos sin compilar. Para estos de deberá realizar los siguientes pasos:

- Descarga el archivo comprimido de instalación de la página www.isc.org
- Extrae el contenido del archivo tar.

```
tar -zxvf dhcp-X.X.X.tar.gz
```

- Ejecutar en el directorio que contenga los archivos de instalación (usuario root):

```
# ./configure.
# make.
#  make install.
```

Configuración. Una vez instalado el servidor, es necesario configurarlo mediante la edición del archivo "dhcpd.conf" localizado en el folder "/etc". Un ejemplo sencillo de configuración quedaría de la siguiente manera:

```
option domain-name "ens.uabc.mx";
option domain-name-servers 148.231.192.6;
option routers 192.168.0.1;
default-lease-time 14400;
ddns-update-style none;
subnet 192.168.0.0 netmask 255.255.255.0 {
 range 192.168.0.2 192.168.0.30;
 default-lease-time 14400;
 max-lease-time 172800;
}
```

Esta configuración asigna direcciones IP de entre el rango de 192.168.0.2 al 30, con su máscara, Gateway y DNS.

E) Manual para la instalación de un punto de acceso utilizando una computadora con sistema operativo Linux

Para instalar un punto de acceso con el uso de una computadora con sistema operativo Linux es necesario instalar el servidor HostAPD, el cual implementa el manejo de puntos de acceso 802.11, Autenticadores IEEE 802.1X/WPA/WPA2/EAP, cliente de RADIUS, servidor EAP, y servidor de autenticación RADIUS.

Los pasos que deberán llevarse a cabo para la instalación son: instalación de la tarjeta de red inalámbrica, instalación del servidor de DHCP, instalación del sistema de enrutamiento de paquetes a través de la red cableada y la red inalámbrica, y por último la instalación del servidor HostAPD.

Instalación de la tarjeta de red inalámbrica. La tarjeta de red debe de poder ser configurada como punto de acceso o modo "master", esto puede ser revisado en las características de la tarjeta como tipos de modo de trabajo (nodo, ad hoc ó master).

Si el sistema operativo Linux no ha detectado la tarjeta de red inalámbrica, se deberán conseguir los drivers para el chipset indicado. Existen solo dos chipsets que pueden ser utilizados para la instalación de HostAPD; estos son:

- Atheros. Sus drivers pueden ser obtenidos de la página: http://madwifi.org
- Prism. Existen actualmente dos drivers para este chipset y pueden ser obtenidos en: http://hostap.epitest.fi/ y http://prism54.org/

La instalación de estos drivers es sencilla, para el caso de Atheros con drivers MadWifi los driver pueden conseguirse en la forma de archivos para compilar en varias distribuciones de Linux. Los pasos para la instalación del driver MadWifi son:

Remover modulos antiguos. Para este pasos de deberá acceder como usuario **root**, y se apagaran todos los dispositivos de red con chipset de Atheros:¶

```
#ifconfig ath0 down
#ifconfig wifi0 down
```

Asumiendo que nos encontramos dentro del directorio de MadWifi, de deberá ejecutar los que sigue para remover los módulos actuales de la memoria del sistema:

```
cd scripts
./madwifi-unload.bash
./find-madwifi-modules.sh $(uname -r)
```

Compilar MadWifi. Ejecutar lo que sigue dentro del directorio de instalación:¶

```
#make
#make install
```

Cargar el modulo MadWifi. Este paso cargará el driver MadWifi dentro del sistema.

```
modprobe ath_pci
```

En el caso de tener una tarjeta de red inalámbrica con chipset Prism, los drivers pueden ser instalados al mismo tiempo que el servidor HostAPD

Instalación del servidor DHCP. Se deberá instalar un servidor de DHCP el cual permitirá la autoconfiguración de red de los equipos conectados. En el Anexo D se muestra a detalle la instalación y configuración de este servidor.

Instalador del sistema de enrutamiento de paquetes a través de la red cableada y la red inalámbrica. Se deberá generar un script para el enrutamiento de paquetes entre la red cableada y la red inalámbrica. Este podrá ser agregado como tarea a realizar al iniciar la el servidor.

```
#!/bin/bash
#### /etc/init.d/nat.sh

# Interfaces
IF_EXT="eth0"
IF_INT="ath0"

# Puertos
P_WEB="8080"
P_FTP="2121"

# IPs
IP_INT="192.168.0.1"

# Modulos
modprobe iptable_nat ip_conntrack_ftp ip_nat_ftp \
ip_conntrack_irc ip_nat_irc iptable_filter \
ipt_MASQUERADE ipt_state ip_tables

# Reglas por defecto
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -t nat -F
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

```
# Reglas de router (SNAT)
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o $IF_EXT -j MASQUERADE
iptables -t nat -A POSTROUTING -s 127.0.0.0/24 -o $IF_EXT -j MASQUERADE

# Reglas de servidores (DNAT)
iptables -A PREROUTING -t nat -p tcp -i $IF_EXT --destination-port $P_WEB \
-j DNAT --to $IP_INT:80
iptables -A PREROUTING -t nat -p tcp -i $IF_EXT --destination-port $P_FTP \
-j DNAT --to $IP_INT:21

# Filtrado de paquetes
iptables -A INPUT -i $IF_EXT -p tcp --destination-port 80 -j ACCEPT
iptables -A INPUT -i $IF_EXT -p tcp --destination-port 21 -j ACCEPT
iptables -A INPUT -i $IF_EXT -m state --state NEW,INVALID -j DROP
iptables -A FORWARD -i $IF_EXT -p tcp --destination-port 80 -j ACCEPT
iptables -A FORWARD -i $IF_EXT -p tcp --destination-port 21 -j ACCEPT
iptables -A FORWARD -i $IF_EXT -m state --state NEW,INVALID -j DROP

# Reenvio de IP
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Instalación del servidor HostAPD.

El primero paso es revisar que las librerías necesarias se encuentren instaladas, estas son: '**openssl**' y '**openssl-devel**'.

Se debe buscar el archivo de instalación para ser compilado en la página web de http://hostap.epitest.fi/hostapd/ y se sigue los pasos que se muestran a continuación:

- Descarga el archivo comprimido de instalación de la página http://hostap.epitest.fi/hostapd/
- Extrae el contenido del archivo tar.

```
tar -zxvf hostapd-X.X.X.tar.gz
```

- Generar el archivo de configuración '.config' dentro del directorio que contenga los archivos de instalación (usuario root):

```
# Example hostapd build time configuration
#
# This file lists the configuration options that are used when building the
# hostapd binary. All lines starting with # are ignored. Configuration option
# lines must be commented out complete, if they are not to be included, i.e.,
# just setting VARIABLE=n is not disabling that variable.
#
# This file is included in Makefile, so variables like CFLAGS and LIBS can also
```

```
# be modified from here. In most cass, these lines should use += in order not
# to override previous values of the variables.

# Driver interface for Host AP driver
CONFIG_DRIVER_HOSTAP=y

# Driver interface for wired authenticator
CONFIG_DRIVER_WIRED=y

# Driver interface for madwifi driver
CONFIG_DRIVER_MADWIFI=y
CFLAGS += -I/home/pkbr/Desktop/madwifi-0.9.2/madwifi-0.9.2 # change to reflect local setup
directory
# for madwifi src

# Driver interface for Prism54 driver
#CONFIG_DRIVER_PRISM54=y

# Driver interface for FreeBSD net80211 layer (e.g., Atheros driver)
#CONFIG_DRIVER_BSD=y
#CFLAGS += -I/usr/local/include
#LIBS += -L/usr/local/lib

# IEEE 802.11F/IAPP
#CONFIG_IAPP=y

# WPA2/IEEE 802.11i RSN pre-authentication
#CONFIG_RSN_PREAUTH=y

# Integrated EAP server
CONFIG_EAP=y

# EAP-MD5 for the integrated EAP server
#CONFIG_EAP_MD5=y

# EAP-TLS for the integrated EAP server
#CONFIG_EAP_TLS=y

# EAP-MSCHAPv2 for the integrated EAP server
#CONFIG_EAP_MSCHAPV2=y

# EAP-PEAP for the integrated EAP server
CONFIG_EAP_PEAP=y

# EAP-GTC for the integrated EAP server
#CONFIG_EAP_GTC=y

# EAP-TTLS for the integrated EAP server
#CONFIG_EAP_TTLS=y

# EAP-SIM for the integrated EAP server
#CONFIG_EAP_SIM=y
```

```
# EAP-PAX for the integrated EAP server
#CONFIG_EAP_PAX=y

# EAP-PSK for the integrated EAP server (this is _not_ needed for WPA-PSK)
#CONFIG_EAP_PSK=y

# PKCS#12 (PFX) support (used to read private key and certificate file from
# a file that usually has extension .p12 or .pfx)
#CONFIG_PKCS12=y

# RADIUS authentication server. This provides access to the integrated EAP
# server from external hosts using RADIUS.
CONFIG_RADIUS_SERVER=y

# Build IPv6 support for RADIUS operations
#CONFIG_IPV6=y
```

- Realizar la instalación:

```
# make.
```

Una vez terminada la instalación, de deberá configurar el archive **'hostapd.conf'** para que coincida con las características deseadas, como el método EAP, la interfaz de red inalámbrica, el servidor RADIUS, entre otras características.

F) Herramientas para realizar pruebas de seguridad en redes

'Sniffers' de Red

Herramienta	Habilidad	Página Web	Plataforma		Costo
			Linux/ Unix	Win 32	
Dsniff	Sniffer para Unix	http://www.monkey.org/~dugsong/dsniff/	✓		Gratuito
Ethereal	sniffer con ambiente grafico (Unix/Windows)	http://www.ethereal.com/	✓	✓	Gratuito
Sniffit	Sniffer para Unix	http://reptile.rug.ac.be/~coder/sniffit/sniffit.html http://www.symbolic.it/Prodotti/sniffit.html (Windows)	✓	✓	Gratuito
Snort	Sniffer para Unix	http://www.snort.org	✓	✓	Gratuito
TCPDump	Sniffer para Unix	http://www-nrg.ee.lbl.gov/	✓		Gratuito
WinDump	Sniffer para Windows	http://netgroup-serv.polito.it/windump/	✓		Gratuito

Herramientas de Escaneo de Red

Herramienta	Habilidad	Página Web	Plataforma		Costo
			Linux / Unix	Win 32	
DUMPSec	Herramienta de enumeración para Windows	http://www.systemtools.com		✓	Gratuito
Firewalk	Mapeo de reglas de filtrado de firewalls	http://www.packetfactory.net/firewalk/	✓		Gratuito
Fscan	Escaneo de puertos	http://www.foundstone.com/		✓	Gratuito
LANguard Network Scanner	Escaneo de puertos, detección de Sistema Operativo	http://www.gfi.com/languard/lanscan.htm		✓	Gratuito
NDS Snoop	Herramienta de enumeración para Novell	http://www.novell.com/coolsolutions/		✓	Gratuito
Nmap	Escaneo de puertos, detección de Sistema Operativo	http://www.insecure.org/nmap/	✓	✓	Gratuito
Solarwinds	Herramienta de enumeración	http://www.solarwinds.net/		✓	A la venta
SuperScan	Escaneo de puertos, detección de Sistema Operativo	http://www.foundstone.com/		✓	Gratuito

Herramientas de Escaneo de Vulnerabilidades

Herramienta	Habilidad	Página Web	Plataforma		Costo
			Linux / Unix	Win 32	
CyberCop Scanner	Escaneo de Vulnerabilidades	http://www.pgp.com/products/	✓	✓	A la venta
ISS Internet Scanner	Escaneo de Vulnerabilidades	http://www.iss.net/		✓	A la venta
Nessus	Escaneo de Vulnerabilidades	http://www.nessus.org/	✓	✓	Gratuito
SecureScanNX	Escaneo de Vulnerabilidades	http://www.vigilante.com/securescan/		✓	A la venta
SAINT	Escaneo de Vulnerabilidades	http://www.wwdsi.com/saint/	✓		A la venta
SARA	Escaneo de Vulnerabilidades	http://www-arc.com/sara/	✓		Gratuito
SATAN	Escaneo de Vulnerabilidades	http://www.fish.com/satan/	✓		Gratuito

Descifrado de Contraseña

Herramienta	Habilidad	Página Web	Plataforma		Costo
			Linux / Unix	Win 32	
Crack 5	Descifrador de contraseñas (Unix)	http://www.crypticide.org/users/alecm/	✓		Gratuito
IMP 2.0	Descifrador de contraseñas Novell Netware	http://www.wastelands.gen.nz		✓	Gratuito
John the Ripper	Descifrador de contraseñas Windows y Unix	http://www.openwall.com/john/	✓	✓	Gratuito
L0pht Crack	Descifrador de contraseñas Windows	http://www.securityfocus.com/tools/1005		✓	A la venta
Nwpcrack	Descifrador de contraseñas Novell Netware	http://ftp.cerias.purdue.edu/pub/tools/novell/		✓	Gratuito

Herramientas para Redes Inalámbricas

Herramienta	Habilidad	Página Web	Plataforma		Costo
			Linux / Unix	Win 32	
Aerosol	Sniffer para Redes Inalámbricas	http://www.sec33.com/sniph/aerosol.php		✓	Gratuito
AirSnort	Sniffer para Redes Inalámbricas	http://airsnort.shmoo.com/	✓		Gratuito
Kismet	Sniffer para Redes Inalámbricas	http://www.kismetwireless.net/	✓		Gratuito

Netstumbler	Sniffer para Redes Inalámbricas	http://www.netstumbler.com		✓	Gratuito
Sniffer Wireless	Sniffer para Redes Inalámbricas	http://www.sniffer.com/		✓	Gratuito
WEPCrack	Descifrador de llaves WEP	http://sourceforge.net/projects/wepcrack/	✓		Gratuito
WaveStumbler	Mapeo de Redes Inalámbricas	http://www.cqure.net/tools08.html	✓		Gratuito

G) Especificación de posibles Puntos de Accesos para el diseño de la RI-FCM.

RoamAbout AP 4102 de Enterasys

General

- Tipo de dispositivo: Punto de acceso inalámbrico
- Anchura: 13.7 cm
- Profundidad: 3.3 cm
- Altura: 21.8 cm
- Peso: 0.8 kg

Conexión de redes

- Factor de forma: Externo
- Tecnología de conectividad: Inalámbrico
- Velocidad de transferencia de datos: 54 Mbps
- Formato código de línea: DBPSK, DQPSK, CCK, 64 QAM, BPSK, QPSK, 16 QAM
- Protocolo de interconexión de datos: IEEE 802.11b, IEEE 802.11g
- Método de espectro expandido: OFDM, DSSS
- Protocolo de gestión remota: Telnet, SNMP 3, HTTP
- Banda de frecuencia: 2.4 GHz
- Características: Alimentación mediante Ethernet (PoE), negociación automática, soporte VLAN, activable
- Algoritmo de cifrado: AES, WEP de 128 bits, WPA, WPA2
- Método de autentificación: Identificación de conjunto de servicios de radio (SSID)
- Cumplimiento de normas: IEEE 802.11b, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x, IEEE 802.11h

Antena

- Antena: Externa desmontable con conector RP-SMA
- Cantidad de antenas: 2

Descripción del fabricante sobre el producto

Enterasys Networks es el proveedor líder en el mundo de infraestructuras de comunicaciones para los clientes empresariales. El hardware y software para redes de Enterasys brinda innovadoras soluciones de seguridad, disponibilidad y movilidad requeridas por las organizaciones más importantes del mundo, complementadas con el servicio y soporte más fuerte de la industria.

Expansión / conectividad

- Interfaces:
  - 1 x red / energía - Ethernet 10Base-T/100Base-TX - RJ-45
  - 2 x red - Radio-Ethernet
  - 1 x gestión - RS-232 - D-Sub de 9 espigas (DB-9)

Diverso

- Cumplimiento de normas: ETSI, CSA, VCCI, EN 60950, EN55022, IEC 60950, EN55024, UL 60950, EN 300.328, UL 2043, FCC

Alimentación

- Dispositivo de alimentación: Adaptador de corriente - externa
- Voltaje necesario: CA 120/230 V

Parámetros de entorno

- Temperatura mínima de funcionamiento: 0 °C
- Temperatura máxima de funcionamiento: 55 °C
- Ámbito de humedad de funcionamiento: 5 - 95%

Ciao

- Incluido en Ciao desde : 31/05/2006

Costo

- 450 dólares

Cisco Aironet 1300 Series AIR-BR1310G

General

- Marca: Cisco Systems, Inc
- Numero de parte: AIR-BR1310G-A-K9-T
- Sitio Web: www.cisco.com
- Línea: Aironet
- Serie: 1300

- Tipo: Puente inalámbrico.
- Modelo: AIR-BR1310G

Especificaciones Inalámbricas

- Tecnología inalámbrica: IEEE 802.11b/g
- Antena: 13dBi Antena Direccional Integrada
- Rango de antena:
  - 1.3 Mile@ 54Mbps Punto a punto IEEE 802.11g
  - 9 Mile@ 11Mbps Punto a punto IEEE 802.11b
  - 1.1 Mile@ 54Mbps Punto a multipunto IEEE 802.11g
  - 8 Mile@ 11Mbps Punto a multipunto IEEE 802.11b
- Banda de Frecuencia: 2.412 GHz to 2.462 GHz IEEE 802.11b/g
- Canales
  - 11 Channel(s)Operating Americas
  - 3 Channel(s)Non-overlapping
- Velocidad de Transmisión: 54Mbps
- Seguridad Inalambrica:
  - IEEE 802.11i
  - IEEE 802.1x
  - TKIP
  - AES
  - WPA
  - WPA2
  - LEAP
  - PEAP-GTC
  - PEAP-MSCHAPv2
  - EAP-TLS
  - EAP-TTLS
  - EAP-SIM
  - EAP-FAST
  - Modulación

Interfaces/Puertos:

- Interfaces/Puertos 1 x F-Type Connector LAN

Administración y Protocolos

- DHCP
- SNMP
- SSH
- SSL
- Telnet

- HTTP
- FTP
- TFTP
- RADIUS
- MIC

Características Físicas

- Dimensiones 3.12" de Altura x 8.1" de Ancho x 8" de Profundidad
- Peso 2.5 lb

Costo

- 990 dólares