Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

2011

Redes Inalámbricas Corporativas

Seguridad integral open source basada en certificados digitales

MAESTRÍA EN SEGURIDAD INFORMÁTICA

CARRERA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

Autor: Ing. Gustavo L. Nakasone

Tutores: Ing. Hugo Pagola

Gabriel Blasco

Cohorte 2010

ÍNDICE

1. Introducción. 5

1.1. Redes corporativas inalámbricas. 5

1.2. Objetivo y alcance del trabajo. 6

1.3. ¿Por qué open source?. 6

2. Redes inalámbricas. 8

2.1. Sus beneficios. 8

2.2. Tipos de redes. 9

3. Seguridad en las redes inalámbricas. 11

3.1. Introducción 11

3.2. IEEE 802.1x – Control de acceso a una red. 11

3.2.1. El estándar. 11

3.2.2. Introducción al protocolo RADIUS. 14

3.2.3. El modelo AAA 15

3.3. IEEE 802.11 – Redes inalámbricas. 16

3.4. IEEE 802.11i – Seguridad en redes inalámbricas. 17

3.4.1. WPA2 17

3.4.2. Jerarquía de claves. 19

3.5. Autenticación 802.1x + RADIUS. 21

4. Solución open source. 24

4.1. La propuesta. 24

4.2. El modelo. 26

4.3. El proceso de autenticación detallado. 28

5. Prueba de concepto. 31

5.1. Software open source 31

5.2. Software adicional. 33

5.3. Maqueta. 33

5.4. Ensayos de laboratorio. 35

5.4.1. Acceso exitoso. 36

5.4.2. Accesos fallidos. 36

6. Recomendaciones. 40

7. Conclusiones finales. 42

ANEXO I - Protocolo RADIUS. 43

A. Introducción. 43

B. Mecanismos de autenticación. 44

C. Proceso de autenticación y autorización. 44

ANEXO II - Certificados digitales. 46

A. Introducción. 46

B. Public Key Infrastructure. 46

B.1. Conceptos. 46

B.2. Emisión de certificados digitales. 48

B.3. Revocación de certificados digitales. 48

ANEXO III - Protocolo LDAP. 50

A. Conceptos generales. 50

ANEXO IV – Protocolo DHCP. 51

A. Conceptos generales. 51

ANEXO V – Configuración del software open source. 53

A. Autoridad Certificante. 53

B. Servidor RADIUS. 54

C. Servidor LDAP. 55

ANEXO VI – Configuración del access point. 57

ANEXO VII - Configuración de la estación inalámbrica. 59

Bibliografía. 61

A. Libros. 61

B. Internet. 61

1. Introducción.

1.1. Redes corporativas inalámbricas.

Hoy en día el acceso inalámbrico a la red corporativa se ha convertido en una necesidad dejando ya de ser simplemente una opción. Por diversas razones (económicas, de espacio, accesibilidad, escalabilidad, practicidad) es muy común ver como las organizaciones habilitan access points en sus edificios a fin de que sus empleados accedan a los recursos informáticos. En muchos casos las notebooks se han convertido en imprescindibles herramientas de trabajo reemplazando a las computadoras de escritorio. Esto plantea indudablemente una pregunta: ¿Qué tan segura es esta clase de conexión?.

Desafortunadamente las redes inalámbricas por sus características particulares presentan evidentes desventajas en materia de seguridad. Muchas veces los mecanismos de seguridad existentes para este tipo de tecnología no son correctamente implementados. Otras veces dichos mecanismos presentan ciertas configuraciones que a pesar de brindar el nivel de seguridad deseable son desestimados por desconocimiento, falta de información o el grado de complejidad que entrañan. Ante este panorama las opciones para lograr una comunicación segura parecen resultar ser siempre las mismas. O adquirir una solución propietaria, solo posible para empresas de cierta envergadura, o conformarse con aquella configuración o arquitectura estándar que resulta poco práctica y/o presenta debilidades por demás conocidas. Pero ésa no es la única salida...

1.2. Objetivo y alcance del trabajo.

El presente trabajo tiene como objetivo desarrollar una solución integral que provea una comunicación inalámbrica segura de bajo costo. Fundamentalmente, la misma estará basada en código open source y en el uso de certificados digitales (instrumentado en una PKI). Con esta solución se pretende cubrir las necesidades de aquellas empresas (pequeñas y medianas) que no pueden costear implementaciones similares pagas. En el informe también se echará luz sobre los métodos y las tecnologías empleadas en cada una de las etapas involucradas durante el establecimiento de este tipo de comunicaciones.

El escrito se iniciará con una introducción a los estándares y las tecnologías de acceso a redes inalámbricas, enfatizando los aspectos relacionados con la seguridad. Se describirán en forma genérica los sistemas que suelen participar en el establecimiento de una comunicación segura y sus posibles configuraciones de seguridad. Luego se hará la presentación formal de una solución integral, describiendo y analizando cada parte de la arquitectura propuesta. Se manejarán conceptos tales como certificados digitales, PKI, autenticación vía RADIUS, servicio DHCP y LDAP, entre otros. Finalmente se cerrará el trabajo con un cuerpo de recomendaciones finales y una conclusión personal de la experiencia y el conocimiento adquirido.

1.3. ¿Por qué open source?.

El concepto subyacente en open source es la de mejora de la calidad del software sustentada por un proceso evolutivo del código, ágil y más participativo (por parte de la extensa comunidad de programadores y desarrolladores). De esta manera el resultado es un producto altamente competitivo y, desde el punto de vista económico, más accesible para aquellas empresas (pequeñas y medianas) que necesitan cubrir necesidades que no pueden costear con implementaciones propietarias similares.

2. Redes inalámbricas.

2.1. Sus beneficios.

La utilización de redes inalámbricas como vías de comunicación digital en los últimos años ha ganado amplio terreno por sobre las cableadas. Algunas razones son ampliamente conocidas, otras solo son visibles por quienes las implementan. Entre las principales no se pueden dejar de mencionar las siguientes:

Beneficio	Descripción
Movilidad	Evidentemente la libertad de movimiento que ofrece a quienes se conectan constituye el principal atractivo. Más aún si su uso está ligado a la actividad laboral, como sucede en un edificio corporativo. Dicha movilidad le permite a una persona desplazarse dentro de un edificio, desempeñe o no allí sus tareas habituales, sin interrumpir el ritmo de trabajo.
Bajo costo	Otra característica que la hace una opción muy recomendada, es que, si bien exige la adquisición de dispositivos y elementos específicos de esta tecnología, al no requerir cableado estructurado permite realizar importantes ahorros. De esta forma se salvan los costos relacionados con la realización de trabajos sobre la misma infraestructura edilicia, que muchas veces se convierte en un obstáculo físico difícil de sortear.
Facilidad y rapidez de implementación	Al no necesitar el típico tendido de cables, la implementación de una red inalámbrica simplifica enormemente los tiempos y el esfuerzo. Incluso por este motivo, muchas veces se opta por este tipo de redes para comunicar dispositivos fijos.
Flexibilidad y escalabilidad	El crecimiento de una red inalámbrica no se encuentra limitado por las características propias del espacio físico que la contiene.
Mantenimiento	Definitivamente, las tareas de mantenimiento de una red inalámbrica resultan menos pesadas debido principalmente a que el medio de transmisión deja de ser un cable para ser reemplazado por el aire.

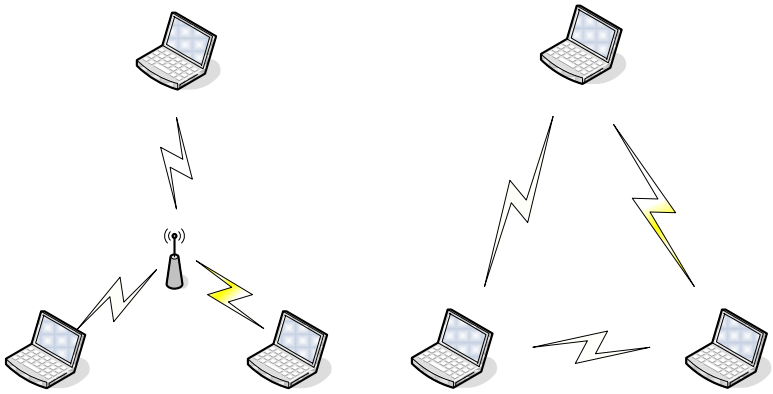
Además, en los últimos años, el crecimiento que ha experimentado la industria electrónica dedicada al desarrollo de dispositivos inalámbricos, y de tecnologías beneficiadas por la existencia de estas redes inalámbricas, ha

sido explosivo. Ya no son solo las notebooks las que cuentan con capacidad para acceder a redes inalámbricas, multiplicidad de dispositivos móviles, como los mismos teléfonos celulares, cuentan con la posibilidad de conectarse a una red de estas características.

2.2. Tipos de redes.

Una red inalámbrica puede ser implementada básicamente en dos modos distintos, a saber:

- Infraestructura: Requiere la presencia de al menos un dispositivo de red, conocido como access point, para permitir la interconexión de los restantes nodos o estaciones. Es decir, que toda comunicación entre dos o más estaciones es establecida a través de un access point.
- Ad hoc: Los nodos/estaciones se conectan entre sí en forma descentralizada, sin la asistencia de ningún equipamiento adicional.



Infraestructura Ad hoc

El presente trabajo ha sido desarrollado específicamente para una red en modo infraestructura. En este modo cada estación debe “asociarse” con un access point para poder comunicarse con otro nodo, sería el equivalente a conectarse físicamente a una red fija. Este proceso es iniciado por la

estación y es el access point quien acepta o no la solicitud. En este contexto, generalmente los access point anuncian su presencia a través de mensajes (beacon), mientras que los dispositivos inalámbricos realizan scaneos en busca de redes activas. Las estaciones también pueden emitir mensajes (probe) requiriendo la contestación de aquellos access points que los escuchen.

3. Seguridad en las redes inalámbricas.

3.1. Introducción.

El talón de Aquiles en cuanto a lo que ha seguridad se refiere reside justamente en su característica distintiva, el medio de transmisión, el aire. Las ondas electromagnéticas que llevan la información no se encuentran protegidas físicamente como lo están en el cableado de una red fija. En redes de este tipo las transmisiones se hallan más expuestas ante posibles accesos no autorizados, incluso frente a interferencias y/o atenuaciones (intencionales o no). Es sabido que las ondas electromagnéticas pueden, dentro de un cierto radio de distancia, ser fácilmente captadas por dispositivos ad-hoc. En pocas palabras, el acceso físico a una red inalámbrica se encuentra menos obstaculizado que al de una red fija y esta es la razón por la cual se hacen necesarios fuertes mecanismos de seguridad. Pero antes de pasar a tratar específicamente este tema, resultará oportuno empezar con un estándar de autenticación conocido como IEEE 802.1x.

3.2. IEEE 802.1x – Control de acceso a una red.

3.2.1. El estándar.

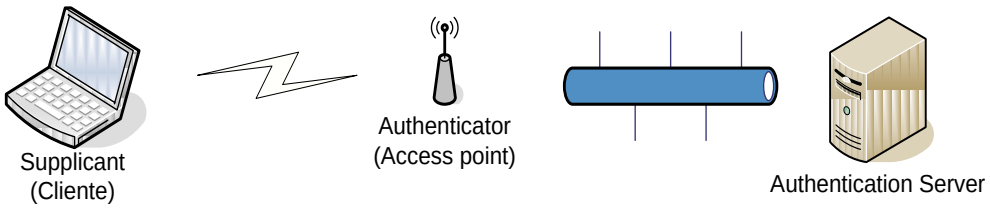
El estándar 802.1x, de la familia IEEE 802, especifica un modelo de autenticación basado en puertos, independientemente se trate de una red inalámbrica o fija. El mismo establece que un dispositivo de red conectado a un puerto, necesita identificarse, de alguna manera, antes de poder comunicarse con otras estaciones. Es decir, la habilitación del puerto (y acceso a la red) dependerá del resultado de la evaluación de la información de autenticación provista por el cliente. Este estándar se encuentra basado

en el protocolo EAP (Extensible Authentication Protocol), diseñado originalmente para conexiones punto a punto. El protocolo se extiende a una red LAN mediante el encapsulado en EAPOL (EAP over LAN) y se encuentra apoyado sobre la capa de enlace del modelo OSI. EAP contempla la utilización de diferentes métodos de autenticación e intercambio de credenciales.

Las partes que intervienen en un proceso de autenticación 802.1x son:

- El supplicant (cliente) es el que intenta tener el acceso a una red.
- El authenticator es el que recibe la petición del cliente y la envía al servidor de autenticación. Actúa como intermediario entre las dos partes. El authenticator es el dispositivo que aloja el port, pudiendo ser un switch o un access point, según sea el caso.
- El authentication server (servidor de autenticación) es el que valida o no las credenciales. Por lo general éste último suele ser un servidor RADIUS (Remote Authentication Dial In User Service).

En una red inalámbrica los roles estarían repartidos de la siguiente manera:

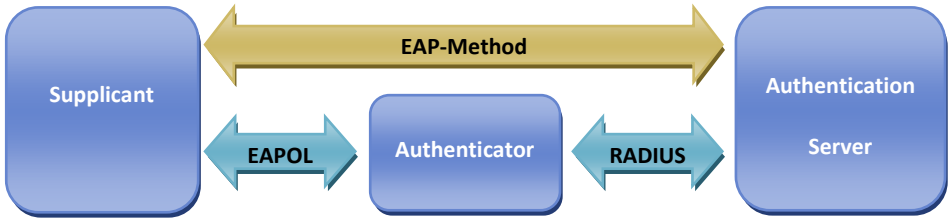


En esta arquitectura, el supplicant solo puede comunicarse físicamente con el authenticator. Este último es quien hace de puente entre el supplicant

y el authentication server. Trabajando de esta forma, el authenticator impide que el supplicant pueda comunicarse con cualquier otro dispositivo de la red, dado que el authenticator solo permite tráfico 802.1x hasta que la autenticación finalice exitosamente (hace un control bidireccional del tráfico).

El protocolo utilizado entre el supplicant y el authenticator es EAPOL y entre el authenticator y el authentication server suele ser RADIUS. El supplicant y el authentication server se comunican empleando mecanismos EAP, denominados EAP-Method`s. Los métodos EAP definen cómo se procede en la autenticación y qué información ha de utilizarse para la validación. En otras palabras, la información y los mensajes de autenticación son intercambiados a través de los EAP-Method, y, a su vez, éstos son encapsulados en el protocolo EAPOL, de un lado, y en el protocolo RADIUS, del otro. Existen diferentes tipos de EAP-Method, los especificados inicialmente son tres: MD5-Challenge, One Time Password (OTP) y Generic Token Card. A los que posteriormente se han sumado otros como EAP-TLS, EAP-TTLS, PEAP y PEAP-FAST.

Resumiendo, durante el proceso de autenticación se pueden distinguir tres comunicaciones:



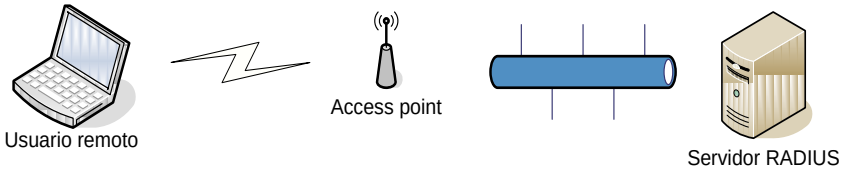
- Entre el supplicant y el authenticator, usan EAPOL (EAP over LAN).
- Entre el authenticator y el authentication server, pueden hablar el protocolo RADIUS.
- Entre el supplicant y el authentication server, emplean EAP-Method.

Es decir, se dan dos comunicaciones físicas, las dos primeras, y una lógica, entre el authentication server y el supplicant.

La solución que se propondrá más adelante en este informe se fundamenta en este estándar (802.1x), empleando EAP-TLS como método de autenticación EAP. EAP-TLS emplea el protocolo TLS (Transport Layer Security) descripto en la RFC 2716. TLS posibilita, a partir del uso de certificados digitales, llevar a cabo una autenticación mutua entre el supplicant y el authentication server, y, además, establecer una sesión segura entre los mismos. Ese proceso de autenticación implica sendas validaciones basadas en la confianza depositada en un tercero, en quien emitió los mencionados certificados. Precisamente PKI (Public Key Infrastructure) define una arquitectura de confianza que vincula identidades con claves públicas, y esto lo logra mediante los certificados digitales. Ya que por sí solas, las claves privadas/públicas no permiten validar la identidad de quien las presenta. Para más detalles ver Anexo II.

3.2.2. Introducción al protocolo RADIUS.

RADIUS (Remote Authentication Dial-In User Service) es un protocolo desarrollado para el control de accesos a los recursos de una red. Permite realizar operaciones de autenticación, autorización y trazabilidad en forma controlada de los usuarios remotos que deseen utilizar recursos (servicios) de uno o varios sistemas. Implementa el denominado modelo AAA de seguridad y funcionalmente cumple con el esquema cliente-servidor. El cliente suele ser un NAS (Network Access Server) que recibe las peticiones del usuario remoto y las redirige al servidor RADIUS, actuando como un interlocutor. Obviamente, en una red inalámbrica el cliente NAS es el access point y el usuario remoto actúa a través del supplicant.



La información de autenticación que es intercambiada entre el supplicant y el authentication server, a través del authenticator, es transmitida en EAP-Methods encapsulados en RADIUS. Las diferentes implementaciones de servidores RADIUS por lo general hablan los EAP-Methods de usos más extendidos. Al final del informe, en el Anexo I, se brinda más información sobre el protocolo RADIUS.

3.2.3. El modelo AAA.

El modelo AAA (siglas para authentication, authorization y accounting) define una arquitectura para el control de accesos que separa las funciones de seguridad en tres servicios fundamentales:

Función	Descripción
Autenticación	Provee métodos para identificar usuarios mediante algún tipo de credencial. Las credenciales más utilizadas son login/password, desafío/respuesta y certificados digitales.
Autorización	Determina si un usuario puede o no hacer uso de un recurso determinado. Por lo general, se toman decisiones sobre una serie de atributos del usuario, resguardados en un repositorio, o en virtud de un conjunto de reglas de acceso definidas para tal fin.
Trazabilidad	Lleva registros de los usuarios sobre sus actividades durante la utilización de los recursos autorizados. La información recolectada posteriormente puede ser utilizada bajo diversos propósitos. Los más comunes son: análisis de seguridad, monitoreo de capacidad, auditoría y facturación.

La aplicación de este modelo permite una mayor flexibilidad y escalabilidad de los controles de accesos. Cabe destacar que RADIUS no es el único protocolo que adopta este modelo, se pueden mencionar además TACACS+ y Diameter.

3.3. IEEE 802.11 – Redes inalámbricas.

Así como la IEEE 802 define el conjunto de estándares IEEE para una LAN (Local Area Network) y una MAN (Metropolitan Area Network) en las dos primeras capas del modelo OSI, la 802.11 es el estándar en el mismo sentido para las redes inalámbricas. La 802.11 define varios aspectos a seguir en el establecimiento de una red inalámbrica, entre ellas, las circunscriptas a la seguridad.

Inicialmente 802.11 provee un mecanismo de seguridad conocido como WEP (Wired Equivalent Privacy). La misma establece el uso de una clave compartida entre la estación cliente y el access point, es decir, un secreto que debe ser configurado en ambos dispositivos, lo que de entrada plantea un dilema, el de cómo distribuirla adecuadamente. Para clarificar esta afirmación se plantean las siguientes situaciones:

- La posibilidad de que el usuario de un dispositivo, con permisos de administrador, tenga acceso a la clave. La confidencialidad de la clave dependerá entonces de muchas personas, no solo de los informáticos, lo que afectará directamente a su privacidad. Puede darse la situación de que uno de los usuarios intente utilizarla para desencriptar la comunicación de otro.
- La administración de claves puede convertirse en una tarea compleja y pesada. Reemplazar y distribuir claves, en una organización que cuenta con un generoso plantel de usuarios habilitados simplemente insumirá considerable tiempo y esfuerzo, además de exigir cierto cuidado en el proceso. Hay que tener en claro que el compromiso de una clave requerirá su reemplazo en todos los dispositivos móviles y access points involucrados.

Antes de continuar vale una aclaración, y es que todo lo referido a la seguridad en 802.11 es para la comunicación entre el cliente inalámbrico y el access point. WEP emplea un mecanismo del tipo desafío-respuesta usando la clave compartida. WEP se implementó sobre el algoritmo de encriptado simétrico RC4 utilizando inicialmente una clave de 64 bits para encriptar el flujo de datos, 24 de los cuales pertenecen al vector de inicialización (IV). Es decir, estamos hablando de una débil clave de sólo 40 bits de longitud, que es utilizada en todas las sesiones (no varía dinámicamente), lo que la torna fácilmente quebrable por fuerza bruta. Actualmente la longitud de esta clave se ha extendido a 128 bits (conservando los 24 del IV), aunque no es una medida ampliamente soportada por los fabricantes. De todas maneras, los principales puntos débiles de WEP son: la reutilización del vector de inicialización, el uso de un método CRC lineal para el chequeo de integridad y el empleo de la misma clave para autenticación y encriptado. Por otro lado, WEP solo cubre el proceso de autenticación, no contempla el manejo de reglas de acceso para permitir o no la utilización de los distintos servicios que una red puede proveer (autorización).

Tiempo después, a WEP lo sucedió WPA (Wi-Fi Protected Access), una solución de transición para resolver solo algunas de las vulnerabilidades. WPA utiliza TKIP (Temporary Key Integrity Protocol) como algoritmo de encriptado, una variante del RC4.

3.4. IEEE 802.11i – Seguridad en redes inalámbricas.

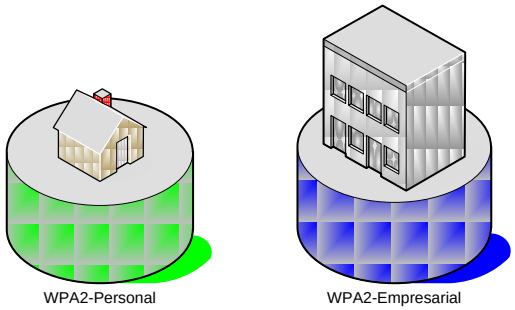
3.4.1. WPA2.

La verdadera solución recién vendría de la mano de WPA2, con resultados realmente satisfactorios. WPA2 surge con el estándar 802.11i que redefine los mecanismos de seguridad de la 802.11. IEEE 802.11i establece un modelo de red inalámbrica bajo el nombre de Robust Security Network

(RSN) a la cual solo se pueden conectar dispositivos que cumplan con una serie de características vinculadas con el denominado nuevo concepto de contexto de seguridad (Security Context). Principalmente, estas palabras conllevan la idea de que logrado una autenticación exitosa se inicia un contexto de seguridad, de duración finita, durante el cual se autoriza el uso de determinados recursos. Otra idea subyacente, es el manejo por separado de los procesos de autenticación y de protección de los mensajes (integridad y privacidad). Una mejora importante introducida por este estándar, es la creación y utilización de un conjunto de claves temporales (o de sesión) para la encripción del tráfico entre el cliente y el access point dentro del contexto de seguridad, ordenadas en una jerarquía dada; más adelante se entrará en detalle. Estas claves temporales son generadas a partir de una clave fija o clave maestra.

WPA2 utiliza CCMP como algoritmo de cifrado, derivado del AES (Advanced Encryption Standard), el actual estándar de la NIST para cifrado simétrico. Además utiliza una versión mejorada del código de chequeo de integridad empleado por WPA, el MIC (Message Integrity Code), conocido como Michael.

WPA2 admite dos versiones, la WPA2-Personal y la WPA2-Empresarial, WPA también lo hacía, las diferencias básicamente residen en el proceso de autenticación. La primera, por su simplicidad, está orientada al uso hogareño, ya que cubre satisfactoriamente sus expectativas de seguridad, mientras que la segunda está pensada para entornos más exigentes como lo es una corporación.

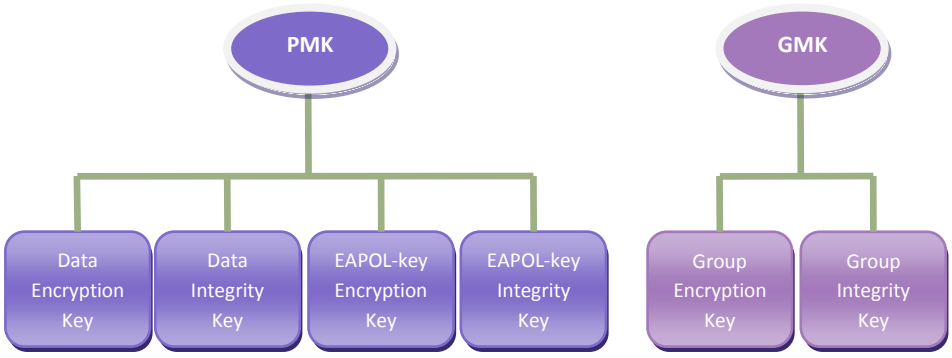


WPA2-Personal, o WPA2-PSK, utiliza una clave PSK (pre-shared key), que en forma similar a WEP, debe ser configurada en el cliente y en el access point. Es la clave maestra. WPA2-PSK admite claves de 8 a 63 caracteres alfanuméricos, y como no involucra mayor complejidad, es la configuración más usada y, a su vez, la más insegura, ya que una clave débil potencia los ataques por fuerza bruta. Probado son los ataques de este tipo que valiéndose de software dedicado, como Aircrack-ng (http://www.aircrack-ng.org), obtienen resultados exitosos mediante la captura de paquetes y la asistencia de herramientas de crackeo de passwords que usan bases o diccionarios de hashes. En síntesis, la seguridad depende fuertemente de la robustez de una clave. A esto se debe sumar el problema de la distribución de claves que, como sucede con WEP, trae aparejado varios inconvenientes a los administradores.

La otra versión, WPA2-Empresarial, permite el uso de certificados digitales que combinado con métodos de autenticación más sofisticados, constituirá el fundamento de este trabajo. Desde luego, una implementación de este tipo exige mayor conocimiento de tecnologías y protocolos de comunicación, así como también, otros recursos informáticos.

3.4.2. Jerarquía de claves.

802.11i establece el uso de claves de pares (pairwise keys) y grupales (group keys), todas temporales. Las primeras son las que se emplean para cifrado y chequeo de integridad de la comunicación entre cada dispositivo móvil y el access point (unicast), y las segundas son utilizadas dentro de un grupo de estaciones y el access point (multicast o broadcast). A su vez, cada tipo engloba una serie de claves reunidas en una jerarquía ordenada, es decir, existe una jerarquía de claves de pares y otra de claves grupales.



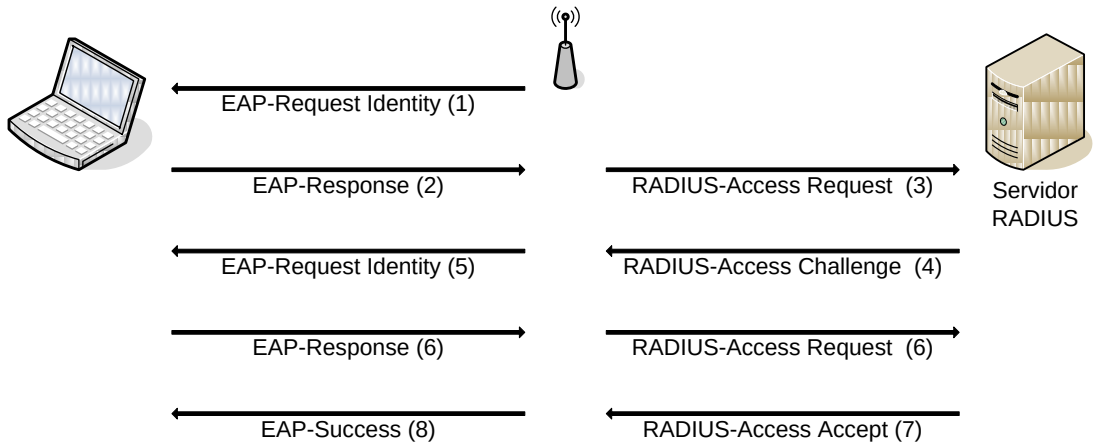
En la jerarquía de claves de pares la posición más alta es ocupada por la PMK (Pairwise Master Key) de 256 bits, que puede ser la clave pre-compartida, como en WPA2-PSK, o generada durante el proceso de autenticación entre el supplicant y el authentication server (conocida como server-key). Como un adelanto, el mecanismo EAP-TLS permite generar la PMK durante el proceso de autenticación. Esta PMK no es utilizada para asegurar la comunicación sino que a partir de ella, el authenticator y el supplicant generan las claves de sesión. Obviamente, en EAP-TLS, el authentication server antes debe transferirla al authenticator, y esto lo puede hacer utilizando el protocolo RADIUS. De la PMK, el supplicant y el authenticator, derivarán 4 claves, 2 para proteger los datos (una para encriptado y otra para integridad) y 2 para proteger el handshake inicial EAPOL (encriptado e integridad). Las 4 claves (Data Encryption key, Data Integrity key, EAPOL-Key Encryption key y EAPOL-Key Integrity key) son temporales de 128 bits, y son referenciadas como PTK (Pairwise Transient Key).

En el caso de las claves grupales, el access point es quien genera la GMK (Group Master Key) de 256 bits, el nodo principal de la jerarquía, del cual deriva 2 claves temporales (para encriptado e integridad) de 128 bits que luego envía a cada estación. En una arquitectura de red inalámbrica de tipo infraestructura, el access point es el único que hace multicast/broadcast (las estaciones no lo pueden hacer directamente). Las claves temporales

(Group Encryption key y Group Integrity key) conforman la GTK. Por razones lógicas de seguridad, la GTK debe regenerarse cada vez que una estación se desconecta, pero esta no es una tarea compleja gracias a que el access point comparte con cada estación las correspondientes PTK, por lo que puede enviar (la GTK) en forma segura.

3.5. Autenticación 802.1x + RADIUS.

A esta altura, están dadas las condiciones para describir el proceso de autenticación 802.1x estándar:



Proceso de autenticación 802.1x exitoso

(1) El authenticator detecta link en un port (capa 2) y envía un EAP-Request Identity (un paquete EAP) al supplicant para su identificación. Si no obtiene respuesta puede hacer reenvíos del request. Para el caso de una red inalámbrica la detección de link sería el símil al proceso de asociación. Es decir que un cliente puede estar asociado pero no autenticado. Si el authenticator no recibe el EAP-Response esperado, mantiene el puerto en estado no autorizado y envía un EAP-Failure al supplicant. También puede configurarse el access point para que ubique el port en una VLAN (Guest VLAN) para aquellos dispositivos que no hablen 802.1x, no hay que descartar esta situación.

(2) Si se trata de un supplicant 802.1x, una vez recibido el EAP-Request Identity envía su EAP-Response para identificarse.

(3) El authenticator reencapsula la respuesta y se la envía al authentication server para su validación (un RADIUS-Access Request). Como ya se explicó, entre el authenticator y el authentication server comparten una password (shared secret) que es empleada para la autenticación mutua (el authentication server además puede chequear la ip del authenticator) y el encriptado de parte del tráfico intercambiado.

(4) El authentication server, una vez validada las credenciales del authenticator, le envía un RADIUS-Access Challenge en el cual propone el EAP-Method a usar (dirigido al supplicant). Si la ip del authenticator no está autorizada descarta los RADIUS-Access Request, en cambio, si el password resulta incorrecto envía un RADIUS-Access Reject.

(5) El authenticator pasa el RADIUS-Access Challenge al supplicant. El supplicant aceptará o propondrá otro EAP-Method que soporte al authentication server.

(6) En esta instancia, entre el supplicant y el authentication server tratarán de negociar el método de autenticación, el proceso puede implicar el intercambio de varios paquetes. En caso de no lograr acuerdo el authentication server enviará al authenticator un Failure, quién lo reenviará al supplicant (EAP-Failure). Nuevamente, esta acción según sea la configuración del authentication server puede significar el seteo de una Guest VLAN.

(7) Si la autenticación se lleva a cabo exitosamente el authentication server le envía información al authenticator de la validación (RADIUS-Access Accept) y sobre cómo debe proceder con el puerto (especificando la VLAN que ha de configurar, por ejemplo).

(9) El authenticator permite al supplicant el acceso a la red (EAP-Success).

Posteriormente el supplicant y el authenticator, siguiendo el estándar 802.11i, utilizan EAPOL para la generación de las claves de pares y grupales. La forma en que se procede en este paso depende del método EAP utilizado. Más adelante, al momento de presentar la propuesta se detallará el proceso de autenticación específico para el método EAP-TLS.

Luego de la autenticación, se ejecuta periódicamente un proceso de reautenticación. El supplicant también puede ser configurado para que inicie el proceso de autenticación 802.1x. En este caso, si el supplicant no recibe un EAP-Request Identity enviará un EAPOL-Start a tal efecto. Algunas veces el mismo puerto no está configurado en 802.1x, para prevenir esta situación es posible indicarle al supplicant que empiece a transmitir normalmente si no ha obtenido respuesta a sus mensajes EAPOL-Start.

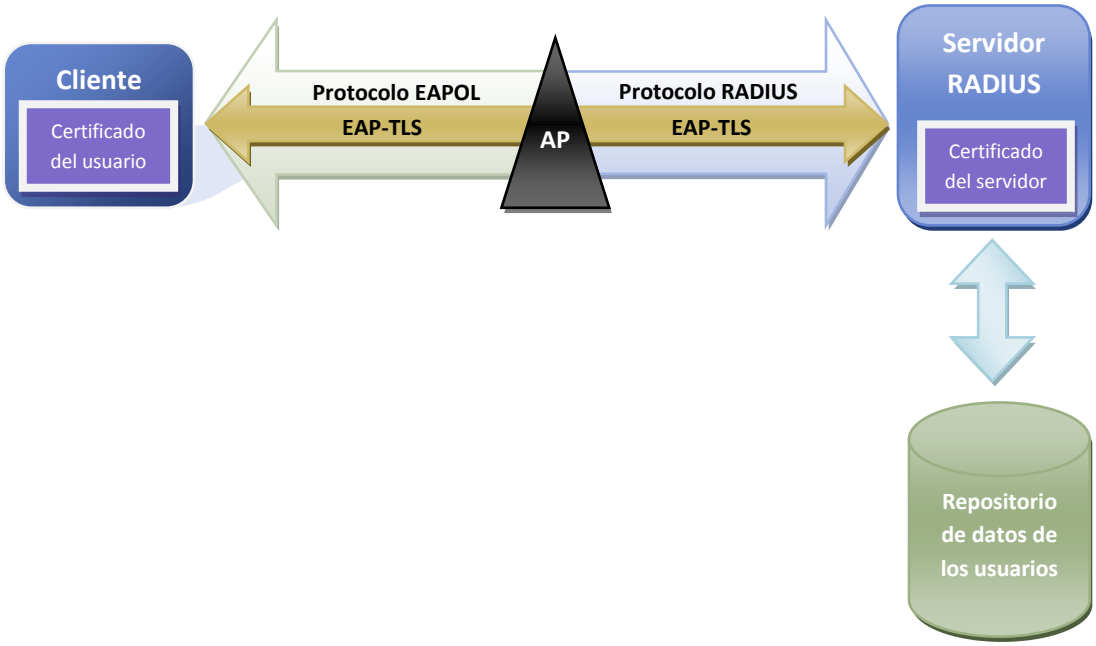
La seguridad en la comunicación entre el authenticator y el authentication server se fundamenta sobre tres pilares:

- La mutua autenticación basada en ips conocidas.
- La encripción de los datos (en este caso mensajes EAP-Method) utilizando una password compartida.
- El método de encripción seleccionado por el mismo EAP-Method.

4. Solución open source.

4.1. La propuesta.

En las unidades anteriores se expuso en forma clara y precisa los estándares y las tecnologías disponibles para abordar los requerimientos de seguridad de las redes inalámbricas. A partir de ellos, se ha diseñado una solución de seguridad integral **open source** para una red inalámbrica corporativa de tipo **infraestructura** basado en el estándar de autenticación **802.1x**, enmarcado en el modelo **AAA** (con participación del protocolo **RADIUS**). A fin de contribuir a un mayor nivel de seguridad se decidió incorporar certificados digitales a la ecuación, brindando robustez a la autenticación (**WPA2-Empresarial**) y a la generación de claves de sesión (**EAP-TLS**), las cuales serán utilizadas para la encriptación y el chequeo de integridad durante la comunicación inalámbrica entre el cliente y el access point.



Antes de pasar a la descripción general y detallada del modelo, resultará muy útil volver a justificar brevemente los conceptos resaltados en el párrafo previo. A saber:

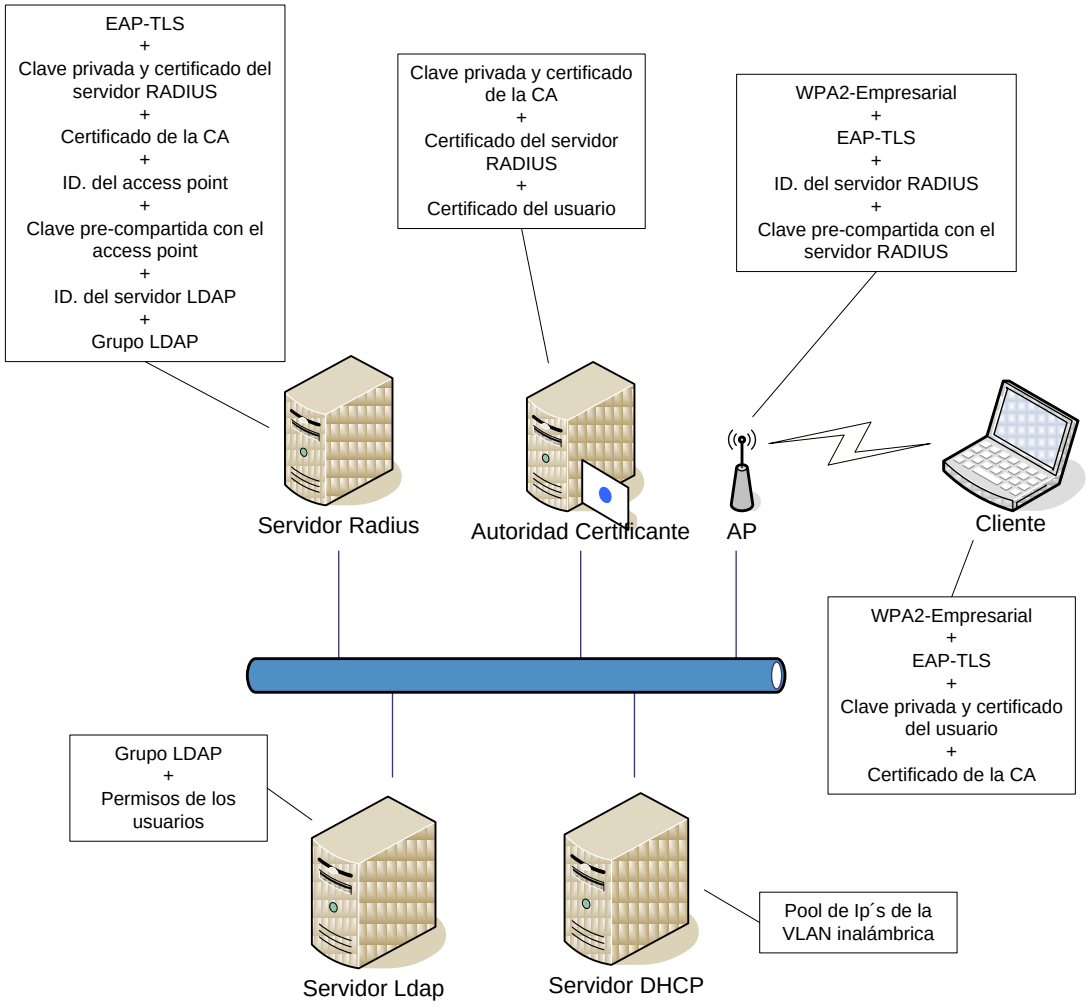
- ✓ Software **open source**: Brinda soluciones de calidad a bajo costo, destinadas a aquellas empresas (medianas a chicas) incapaces de afrontar los precios elevados que insumen tecnologías propietarias.
- ✓ Modo **infraestructura**: Obliga a todas las estaciones/clientes a conectarse a través de los access points facilitando la aplicación de controles y la administración de los mismos.
- ✓ Estándar **802.1x**: Impide que cualquiera de los clientes pueda comunicarse con otro nodo hasta que se encuentre debidamente autenticado. El único tráfico posible es el vinculado con el proceso de autenticación.
- ✓ Modelo **AAA**: Separa las funciones de seguridad en autenticación, autorización y trazabilidad permitiendo un mejor control y manejo de las mismas.
- ✓ Protocolo **RADIUS**: Permite cristalizar en una implementación el modelo AAA en forma segura y eficiente.
- ✓ **Certificados digitales**: En el contexto de una PKI, permite incorporar los beneficios derivados del uso de criptografía asimétrica para validación de identidades (en base a la confianza depositada en una CA) y la concreción de una sesión TLS (para el método EAP-TLS). De todas maneras, para implementar esta solución no es necesario recurrir a una verdadera autoridad certificante, operación que insumiría cierto costo monetario, basta con crear una propia, cubriendo las expectativas y necesidades con holgura.
- ✓ Modo **WPA2**: Provee mayores niveles de seguridad en cuanto a encripción y control de integridad que las alternativas anteriores (WEP y WAP).

- ✓ Modo **WAP2-Empresarial**: Permite el uso de certificados digitales en el proceso de autenticación, eliminando el problema de tener que pre-compartir claves.
- ✓ Método **EAP-TLS**: Establece una sesión TLS, usando certificados digitales, para que el supplicant y el authentication server puedan establecer una comunicación segura y generen la clave maestra.

Para el resguardo de los datos de los usuarios a autenticar y a autorizar por el servidor RADIUS se emplea un repositorio LDAP (Lightweight Directory Access Protocol). Este protocolo define un servicio de directorio optimizado para lecturas y búsquedas, implementado en forma distribuida. Por un lado, favorece una correcta y segura administración, y por el otro, este servicio es ampliamente utilizado para gestionar los permisos de accesos a diversos recursos informáticos, por lo que resulta un componente de integración ideal. Ver Anexo III.

Otro servicio muy utilizado en las redes inalámbricas es el basado en el protocolo DHCP. Si bien en la prueba de concepto no se incluyó este elemento, existen buenas razones que lo convierten en una opción interesante. DHCP (Dynamic Host Configuration Protocol) permite una adecuada administración de las direcciones IP, manejando eficientemente aquellas situaciones en las que los dispositivos se conectan transitoriamente a una red o viajan de una red a otra, como suele suceder en las redes inalámbricas. Ver Anexo IV.

4.2. El modelo.



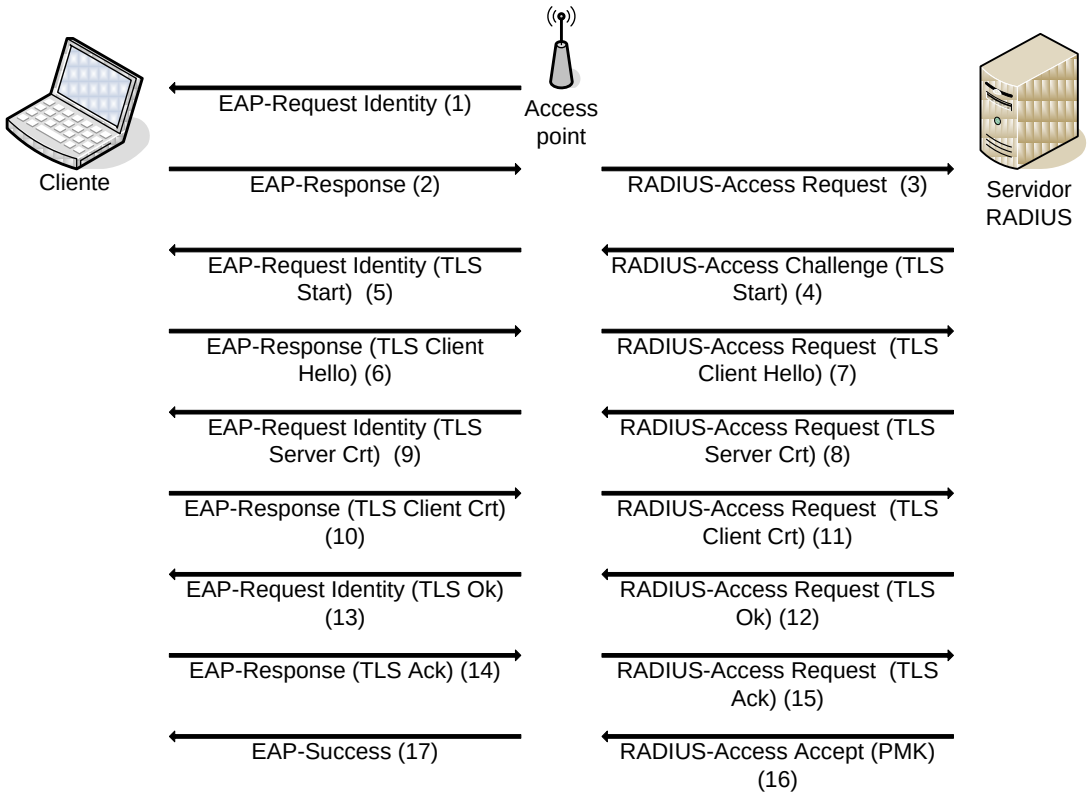
En los bloques de texto se pueden apreciar a grandes rasgos la configuración y/o archivos adicionales presentes en cada componente.

En líneas generales, el proceso de autenticación comienza cuando la estación o cliente intenta acceder a la red corporativa. El access point, mientras el usuario no esté autenticado, solo permite el tráfico entre el cliente y el servidor RADIUS. Estos últimos proceden a validarse empleando los correspondientes certificados, es importante aclarar que, en realidad, del lado del cliente se utiliza el certificado emitido al usuario (no se encuentra asociado a la estación). Pasada esta etapa, la de autenticación propiamente dicha, se procede a la autorización por parte de RADIUS, es decir, el usuario debe pertenecer al Grupo LDAP y tener los permisos necesarios (en el

repositorio LDAP). Si la autorización sucede, el servidor RADIUS y el cliente negocian el establecimiento de una sesión TLS con los mismos certificados utilizados durante la autenticación. Durante esa sesión generan la PMK o clave maestra. Para terminar el servidor RADIUS le indica al access point el resultado exitoso de la autenticación y la autorización y le envía la PMK. El access point le habilita el puerto al cliente luego de derivar entre ambos las claves de sesión. Como último paso, el cliente le requiere al servidor DHCP los parámetros para configurar su placa de red y lograr de esta manera conectividad a nivel de red.

4.3. El proceso de autenticación detallado.

A continuación se detallará el proceso de autenticación utilizado en la implementación, objeto de este trabajo.



(1) El authenticator detecta “link” en un port (capa 2) y envía un EAP-Request Identity (un paquete EAP) al supplicant para su identificación. Si no obtiene respuesta puede hacer reenvíos del request. Si el authenticator no recibe el EAP-Response esperado mantiene el puerto en estado no autorizado y envía un EAP-Failure al supplicant. También puede configurarse el access point para que ubique el port en una VLAN (Guest VLAN) para aquellos dispositivos que no hablen 802.1x, no hay que descartar esta situación.

(2) Si se trata de un supplicant 802.1x, una vez recibido el EAP-Request Identity envía su EAP-Response para identificarse.

(3) El authenticator reencapsula la respuesta y se la envía al authentication server para su validación (un RADIUS-Access Request). Como ya se explicó, entre el authenticator y el authentication server comparten una password (shared secret) que es empleada para la autenticación mutua (el authentication server además puede chequear la ip del authenticator) y el encriptado de parte del tráfico intercambiado.

(4) El authentication server procede a la validación de las credenciales del authenticator. Si la ip del authenticator no está autorizada descarta los RADIUS-Access Request, en cambio, si el password resulta incorrecto envía un RADIUS-Access Reject. Ante una validación positiva, le envía un RADIUS-Access Challenge en el cual propone el EAP-Method a usar (dirigido al supplicant). En este caso envía un Start-TLS.

(5) El authenticator pasa el RADIUS-Access Challenge al supplicant, recordemos que lo reencapsula en EAPOL.

(6) El supplicant aceptará o, si no soporta EAP-TLS, propondrá otro EAP-Method al authentication server. El authentication server está configurado para usar solamente EAP-TLS, de no ser posible este método enviará al authenticator un Failure, quién lo reenviará al supplicant (EAP-Failure). Nuevamente, esta acción según sea la configuración del authentication server puede significar el seteo de una Guest VLAN. Si el suppllicant acepta responderá con un EAP-Response con un TLS Client Hello.

(7) El authenticator reencapsula el EAP-Response y envía un RADIUS-Access Request al authentication server.

(8) El authentication server responde con otro RADIUS-Access Challenge conteniendo su certificado TLS.

(9) El authenticator lo reencapsula y lo envía al supplicant bajo la forma de un EAP-Request Identity.

(10) El supplicant responde con un EAP-Response con su certificado TLS (el del usuario).

(11) El authenticator lo reencapsula y lo envía al authentication server.

(12) Si el certificado es válido, el authentication server responde con un ok para la transacción TLS y los algoritmos criptográficos soportados.

(13) El authenticator lo reencapsula y lo envía al supplicant.

(14) El supplicant confirma con una respuesta EAP-Response.

(15) El authenticator lo reencapsula y lo envía al authentication server.

(16) El authentication server responde con un RADIUS-Access Accept y le envía la clave maestra al authenticator (PMK). Durante la negociación SSL entre el supplicant y el authentication server, ambas partes intercambian los valores que les permitirán computar separadamente la misma

clave maestra (PMK). El authentication server le transmite la PMK al authenticator, utilizando el protocolo RADIUS.

(17) El authenticator habilita el puerto para que la estación acceda a la red y envía un EAP-Success al supplicant. Entre el authenticator y el supplicant derivan las claves de pares, posteriormente el authenticator le transmite al supplicant las claves grupales que creó.

5. Prueba de concepto.

5.1. Software open source.

Los programas open source utilizados en la prueba de concepto se detallan en el siguiente cuadro:

Open source (versión)	Descripción general	Características
FreeRADIUS (2.1.10)	Desarrollado por The FreeRADIUS Project (http://freeradius.org). Es una de las implementaciones de servidor RADIUS más utilizada. Según encuestas propias, en el 2006 estimaron que cerca de 100.000.000 usuarios eran autenticados por servidores FreeRADIUS. Compitiendo directamente, en igual porcentaje, con los productos de Cisco (Access Control Server) y Microsoft (Internet Authentication Service). Es usado por ISP's Tier 1.y empresas listadas en Fortune 500 (http://www.fortune.com/500).	▪ Modular. ▪ Escalable. ▪ Multiplataforma. ▪ Dispone de diccionarios (de atributos-valores) para muchos dispositivos propietarios. ▪ Puede trabajar con distintos tipos de repositorios (LDAP, SQL, archivos de textos). ▪ Soporta VMPS (VLAN Management Policy Server) para asignar VLANs según la MAC address de la estación.
OpenSSL (0.9.8)	Desarrollado por el OpenSSL Project (http://www.openssl.org). Provee un conjunto de herramientas para desarrollar implementaciones sobre SSL v2/v3 (Secure Sockets Layer) y TLS v1 (Transport Layer Security), además cuenta con varias librerías criptográficas. El proyecto creó el módulo OpenSSL FIPS Object Module (compatible con OpenSSL) que permite que los productos que usen OpenSSL API puedan utilizar criptografía validada según la FIPS 140-2. La FIPS 140-2 es el estándar de seguridad de la NIST (National Institute of Standards and Technology) del Departamento de Comercio de los Estados Unidos para la	▪ Multiplataforma. ▪ Soporta un amplio espectro de algoritmos criptográficos estándares. ▪ Provee un entorno auto-suficiente para la creación y administración de una CA (PKI). ▪ OpenSSL FIPS Object Module.

	acreditación de módulos criptográficos con el objeto de ser utilizados por ese gobierno o grandes corporaciones que requieren manejar altos niveles de seguridad.	
OpenLDAP (2.3.43)	Desarrollado por el OpenLDAP Project (http://www.openldap.org). Es una implementación de LDAP que comprende un servidor LDAP, varios clientes, librerías y herramientas relacionadas con el servicio.	▪ Multiplataforma. ▪ Modular. ▪ Escalable. ▪ Puede interactuar con diferentes formatos de repositorios de datos. ▪ Maneja reglas de acceso. ▪ Soporta negociaciones SSL/TLS. ▪ Contempla distintos métodos de autenticación. ▪ Posee un mecanismo de replicación.

Otro software open source interesante, pero que no fue utilizado porque en realidad introduce mejoras administrativas es OpenCA. OpenCA provee un framework para la administración de una CA basado en las herramientas de OpenSSL.

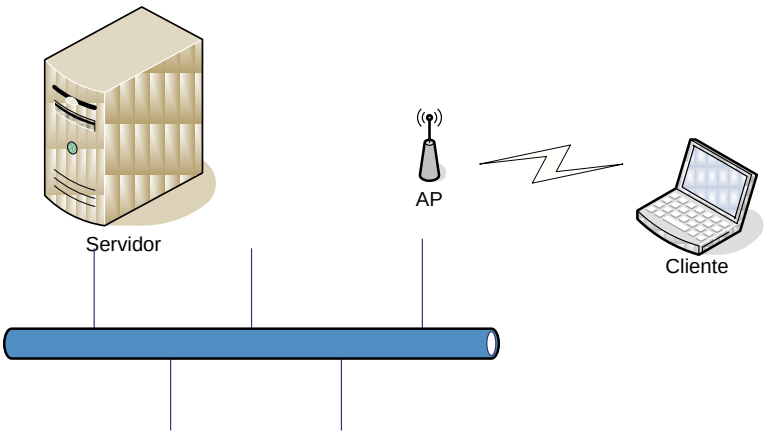
Open source	Descripción general	Características
OpenCA	Desarrollado por el OpenCA PKI Research Labs, anteriormente conocido como el OpenCA Project (http://www.openca.org). Es un framework para PKI. El Proyecto también se aboca a otros desarrollos relacionados, como por ejemplo: ▪ Librerías para desarrollar aplicaciones PKI (LibPKI). ▪ Un servidor de OCSPD (OpenCA OCSPD). OCSPD (Online Certificate Status Protocol) es un protocolo diseñado para el chequeo online de certificados revocados.	▪ Utiliza las herramientas desarrolladas por OpenSSL. ▪ Provee una interfaz web amigable para la administración de una CA.

5.2. Software adicional.

Además del software open source mencionado en el punto anterior también se empleó VMware Workstation (versión 7.1.2), un producto de VMware (http://www.vmware.com) para virtualizar la pc que alojó a los servidores RADIUS y LDAP. La razón de esta decisión responde a la necesidad de movilidad para realizar las demostraciones que resultaran pertinentes.

5.3. Maqueta.

Teniendo en consideración los aspectos descriptos en los puntos anteriores, la solución de seguridad integral open source para una red inalámbrica corporativa se vio materializada a través de la siguiente maqueta de laboratorio:



Donde los principales componentes puestos en juego fueron:

Componente	Función	Hardware	Sistema operativo
HP d325 Microtower	▪ **Cliente (Supplicant)**.	▪ AMD Athlon XP 2600+.	▪ Microsoft Windows XP Profesional (Versión

		▪ CPU de 1,91 GHz. ▪ RAM de 256 MB. ▪ Disco rígido de 40 GB. ▪ Placa de red inalámbrica.	2002). ▪ Service Pack 2.
Cisco 1130AG Series Access Point	▪ **Access point (Authenticator).**		▪ Cisco Internetwork Operating System. ▪ Versión 12.4(10b)JDA3.
HP Compaq dc 7600 Convertible Minitower	▪ **Servidor (VMware Host).**	▪ Intel(R) Pentium(R) 4. ▪ CPU de 3.20GHz. ▪ RAM de 1 GB. ▪ Disco rígido de 80 GB.	▪ Microsoft Windows XP Profesional (Versión 2002). ▪ Service Pack 3.
Workstation virtual (VMware Guest)	▪ **Servidor RADIUS (Authentication server).** ▪ **Servidor LDAP.**	▪ Intel(R) Pentium(R) 4. ▪ CPU de 3.20GHz. ▪ RAM de 512 MB. ▪ Disco rígido de 4 GB.	▪ Red Hat Enterprise Linux Server Release 5.3 (Tikanga). ▪ Kernel 2.6.18.

Las tareas realizadas para el desarrollo del modelo de implementación fueron las siguientes:

1. Puesta a punto del servidor RADIUS.
   - 1.1 Instalación.
   - 1.2 Configuración general.
   - 1.3 Puesta en marcha del servicio.
2. Puesta a punto del servidor LDAP.
   - 2.1 Instalación.
   - 2.2 Configuración general.
   - 2.3 Creación del grupo y los usuarios a partir del esquema indicado por RADIUS (ver Anexo V).
   - 2.4 Puesta en marcha del servicio.
3. Creación de los certificados (ver Anexo V).

3.1 Creación de la CA (y su certificado).
3.2 Creación de la clave privada del servidor RADIUS.
3.3 Creación de las claves privadas de los usuarios de prueba.
3.4 Generación de los certificados del servidor RADIUS y de los de los usuarios de prueba.

4. Configuración definitiva del servidor RADIUS (Anexo V).
   4.1 Configuración del EAP-Method para autenticación: EAP-TLS.
   4.2 Definición del grupo habilitado para acceder a la red (Grupo LDAP).
   4.3 Configuración de los parámetros para su interacción con el servidor LDAP (autorización).
   4.4 Incorporación de la clave privada y el certificado del servidor RADIUS y del certificado de la CA.
   4.5 Habilitación del access point como authenticator (IP y clave compartida).
5. Configuración del access point (ver Anexo VI).
   5.1 Configuración general.
   5.2 Configuración de los parámetros de WPA2 y EAP.
   5.3 Configuración del servidor RADIUS (IP y clave compartida).
6. Configuración de la estación cliente (ver Anexo VII).
   6.1 Configuración de los parámetros WPA2 y EAP en la placa de red.
   6.2 Carga del certificado de la CA y la clave privada y el certificado del usuario.

Previamente a todas estas tareas se instaló y configuró la máquina virtual (VMware) utilizada para alojar a los servidores RADIUS y LDAP.

5.4. Ensayos de laboratorio.

Las pruebas de conexión llevadas a cabo a fin de corroborar el efectivo y adecuado funcionamiento del modelo de autenticación propuesto serán listadas más abajo. A cada intento se anexa los logs originados por el servidor RADIUS (authentication server).

Observación:

Los usuarios autorizados para acceder a la red inalámbrica deben tener una entrada en el repositorio LDAP, en donde, consten mínimamente, estos dos atributos:

- radiusGroupName
- dialupAccess

En donde el valor del primero debe ser “WPA2Corporativo” (grupo LDAP definido en el servidor RADIUS) y el del último ha de coincidir con el cn del certificado digital emitido al usuario (ver Anexo V, Servidor RADIUS).

5.4.1. Acceso exitoso.

- Cliente con certificado (del usuario) válido y usuario con valores correctos de dialupAccess y radiusGroupName en el LDAP.

Logs:

Tue Feb 15 20:15:17 2011 : Info: Ready to process requests.
Tue Feb 15 20:15:48 2011 : Auth: Login OK: [Gustavo Nakasone/<via Auth-Type = EAP>] (from client msiap port 259 cli 0008.549a.ec93)

5.4.2. Accesos fallidos.

- Cliente sin certificado.

Logs:

El servidor RADIUS no generó los debido a que el access point no recibió la credencial esperada de parte del cliente. El sistema operativo del cliente (Microsoft Windows XP Profesional) exhibió el siguiente mensaje:

- Cliente con certificado emitido por otra CA.

Logs:

Tue Feb 15 20:23:21 2011 : Info: Ready to process requests.
Tue Feb 15 20:23:24 2011 : Error: rlm_eap: No EAP session matching the State variable.
Tue Feb 15 20:23:24 2011 : Auth: Login incorrect: [Gustavo Nakasone/<via Auth-Type = EAP>] (from client msiap port 277 cli 0008.549a.ec93)
Tue Feb 15 20:23:41 2011 : Error: --> verify error:num=20:unable to get local issuer certificate
Tue Feb 15 20:23:41 2011 : Error: TLS Alert write:fatal:unknown CA
Tue Feb 15 20:23:41 2011 : Error: TLS_accept: error in SSLv3 read client certificate B
Tue Feb 15 20:23:41 2011 : Error: rlm_eap: SSL error error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned
Tue Feb 15 20:23:41 2011 : Error: SSL: SSL_read failed in a system call (-1), TLS session fails.

- Cliente con certificado expirado.

Logs:

Fri Jul 15 19:02:22 2011 : Info: Ready to process requests.
Fri Jul 15 19:02:33 2011 : Error: --> verify error:num=10:certificate has expired
Fri Jul 15 19:02:33 2011 : Error: TLS Alert write:fatal:certificate expired
Fri Jul 15 19:02:33 2011 : Error: TLS_accept: error in SSLv3 read client certificate B
Fri Jul 15 19:02:33 2011 : Error: rlm_eap: SSL error error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned
Fri Jul 15 19:02:33 2011 : Error: SSL: SSL_read failed in a system call (-1), TLS session fails.
Fri Jul 15 19:02:33 2011 : Auth: Login incorrect (certificate has expired): [Gustavo L Nakasone/<via Auth-Type = EAP>] (from client msiap port 269 cli 0008.549a.ec93)

- Cliente con certificado válido pero usuario sin entrada en el LDAP.

Logs:

Tue Feb 15 20:28:17 2011 : Info: Ready to process requests.
Tue Feb 15 20:28:18 2011 : Auth: Login incorrect ([ldap] User not found): [Gustavo Luis Nakasone/<via Auth-Type = Reject>] (from client msiap port 316 cli 0008.549a.ec93)

- Cliente con certificado válido pero usuario con incorrecto valor de dialupaccess en el LDAP.

Logs:

Tue Feb 15 20:37:55 2011 : Info: Ready to process requests.
Tue Feb 15 20:37:59 2011 : Auth: Login incorrect ([ldap] User not found): [Gustavo Luis Nakasone/<via Auth-Type = Reject>] (from client msiap port 373 cli 0008.549a.ec93)

- Cliente con certificado válido pero usuario con incorrecto valor de radiusGroupName en el LDAP.

Logs:

Tue Feb 15 20:40:55 2011 : Info: Ready to process requests.
Tue Feb 15 20:40:56 2011 : Auth: Login incorrect ([ldap] User not found): [Gustavo Nakasone/<via Auth-Type = Reject>] (from client msiap port 383 cli 0008.549a.ec93)

6. Recomendaciones.

Dejando de lado las consabidas medidas de seguridad aplicables a la implementación de una red inalámbrica y a la puesta en producción y mantenimiento de un sistema informático, se cree oportuno incluir en esta sección del informe algunas recomendaciones que hacen a la adecuada y segura cristalización de la propuesta. En cuanto a las conocidas medidas se está aludiendo, por ejemplo, a aquellas relacionadas con la ubicación física de los access points para evitar interferencias, hardening de servidores, configuraciones genéricas, parches y actualizaciones de programas y sistemas operativos, alta disponibilidad en sus distintos niveles, etc.

La primera recomendación se refiere al equipo de software elegido para la solución. Las razones expuestas en el capítulo 5 (sección 5.1) bastan para destacar a FreeRADIUS, OpenSSL y OpenLDAP de entre las producciones similares existentes actualmente en el mundo open source. El uso masivo de los mismos es un indicativo de la aceptación generalizada que han logrado. Estos programas además cuentan con características y funcionalidades que no han sido utilizadas por estar fuera del objetivo y alcance del trabajo pero que pueden llegar a resultar muy interesantes. Entre ellas podemos considerar la trazabilidad que permite FreeRADIUS sobre la actividad de los usuarios (siguiendo el modelo AAA) y los mecanismos de seguridad provistos por OpenLDAP para su administración.

Por otra parte, también se considera una decisión inteligente la de contemplar además de una VLAN para la red inalámbrica, una VLAN para invitados, destinada a los dispositivos que no logren terminar una autenticación exitosamente. De esta manera se daría conectividad a aquellos dispositivos que no hablan 802.1x o a equipos móviles de personas que no pertenecen al plantel de la empresa. Desde luego, a la VLAN para invitados hay que aplicar reglas de acceso más restrictivas ya que

posiblemente las estaciones en cuestión no pertenezcan a la corporación y, por lo tanto, no cumplan con sus estándares de seguridad.

En lo referente a las claves privadas, siguiendo los lineamientos de la NIST Special Publication 800-57, Recommendation for Key Management, es aconsejable utilizar el algoritmo de encriptado RSA con claves de 2048 bits.

En cuanto a la PKI, dado el rol importante que juega la CA en el esquema de autenticación utilizado, se aconseja tener especiales cuidados al respecto. Como se adelantó, no es necesario acudir a una CA real para la emisión de certificados, pero la puesta en producción de una CA propia exige tomar ciertos recaudos. Esto significa, no solamente tener un servidor dedicado específicamente para la institución de la CA, es decir, aislado físicamente, sino también restringir el acceso a su administración tanto como sea posible. Una correcta decisión es la de adoptar un circuito de backup cifrado paralelo en donde la información respaldada no comparta el mismo soporte físico con el resto de los demás servidores.

Para terminar, en pos de la seguridad es importante no descuidar el factor humano. Primero, negándole al usuario los permisos de administrador de la estación inalámbrica asignada, cuando sea posible, y luego a través de su concientización, entrenamiento y educación en el uso de la misma y en el manejo de su clave privada y certificado. Por ejemplo, es muy importante que el usuario sea consciente de los riesgos a los que expone la información manejada por él y la organización al no reportar el compromiso de su clave privada.

7. Conclusiones finales.

El presente desarrollo demuestra que se pueden lograr niveles más que aceptables de seguridad en una red inalámbrica empleando software open source. Si bien requiere un mayor esfuerzo dirigido a resolver aspectos de integración, la complejidad aparente que entraña se disipa a medida que crece el conocimiento de las herramientas empleadas.

Entonces, es posible afirmar que existen al alcance de la mano caminos alternativos a las recetas corporativas pagas que permiten implementar soluciones de seguridad de bajo costo e igual de robustas, basadas en los mismos estándares y protocolos. A esto hay que sumar que el software utilizado permite distintas variantes, ajustables con poco esfuerzo a las necesidades y requerimientos imperantes.

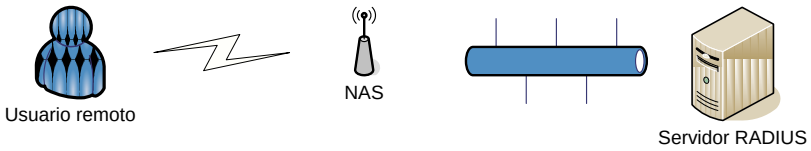
El resultado logrado también pone de manifiesto la cantidad de elementos que han de conjugarse para brindar seguridad a un sistema, seguridad que desde luego nunca será perfecta. Viéndose claramente, cómo el factor humano sigue siendo una de las variables a considerar para que todo cierre. Y, por lo tanto, cuán relevante es el rol que ocupa la concientización en la planificación de la SI de una organización.

Finalmente, en lo personal, el trabajo significó un proceso de aprendizaje y de profundización e integración de conocimientos ya que la elaboración del mismo implicó la coordinación de distintos conceptos, estándares, protocolos y servicios vistos durante la cursada del primer año de la Maestría en SI, especialmente en la materia Seguridad en Redes I.

ANEXO I - Protocolo RADIUS.

A. Introducción.

RADIUS (Remote Authentication Dial-In User Service) es un protocolo desarrollado para el control de accesos a los recursos de una red. Permite realizar operaciones de autenticación, autorización y trazabilidad de usuarios remotos que deseen utilizar recursos (servicios) de uno o varios sistemas. Implementa el modelo AAA de seguridad y funcionalmente cumple con el esquema cliente-servidor. Donde el cliente, suele ser un NAS (Network Access Server), que recibe las peticiones del usuario remoto y las redirige al servidor RADIUS.



Los servidores RADIUS trabajan con un conjunto de políticas a partir de las cuales toman la decisión de autenticar o no a un usuario. La información de los usuarios suele permanecer almacenada en algún tipo de repositorio de datos (una base de datos, un archivo de texto, un servidor LDAP, etc.). A su vez, los servidores pueden decidir específicamente qué recursos el usuario puede utilizar en función de su identidad. Otra característica importante que provee RADIUS, que completa el modelo AAA, es la posibilidad de recolectar información valiosa sobre la actividad de los usuarios. Los servidores RADIUS suelen emplear claves compartidas (shared secrets) con los el clientes NAS destinadas a una mutua validación.

La comunicación entre el server RADIUS y el cliente involucra la transmisión de pares atributos-valores. El protocolo permite una amplia variedad de atributos y tipos de valores, permitiendo incluso la incorporación

de atributos definidos por terceras partes, una opción muy utilizada por fabricantes de dispositivos de red. Para poder manejar esos atributos los servidores RADIUS deben contar con diccionarios en los cuales se encuentren las definiciones y características de los mismos. Diccionarios que pueden ser modificados o extendidos para integrar atributos de terceros.

B. Mecanismos de autenticación.

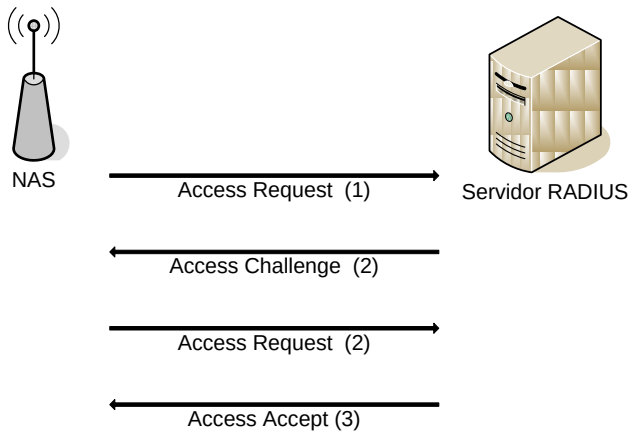
RADIUS soporta diferentes mecanismos de autenticación. Los más empleados son:

- El usuario remoto se contacta con el servidor RADIUS, si éste lo autentica y autoriza, lo comunica con el servidor proveedor del servicio, a quien informa de la habilitación exitosa.
- El usuario remoto se contacta directamente con el servidor de servicio, y éste es quien consulta sobre sus permisos con el servidor RADIUS.
- El usuario se contacta con el servidor RADIUS, si éste lo autentica y autoriza le devuelve un token. El usuario a partir de entonces, presentará este token al servidor del servicio para acceder al recurso deseado.

Existe también un modelo de roaming que permite a los usuarios acceder a servicios provistos por servidores administrados por otra organización.

C. Proceso de autenticación y autorización.

El proceso de autenticación y autorización basado en el protocolo RADIUS comprende los siguientes pasos:



(1) El cliente NAS envía un paquete de Access-Request al servidor RADIUS requiriendo el acceso a un servicio de red determinado. Este paquete contiene información del usuario (incluidas las credenciales), del dispositivo de red del interesado y del servicio requerido.

(2) Si el servidor recibe información no satisfactoria puede requerir más información respondiendo con un Access-Challenge. El cliente deberá responder con un Access-Request con la información solicitada.

(3) Finalmente, si el usuario es identificado exitosamente, el servidor responde con un Access-Accept, que puede devolver información adicional sobre el servicio autorizado. En caso contrario envía un Access-Reject, comunicando la negación del servicio. Los motivos para responder con un Access-Reject pueden ser desde credenciales incorrectas o insuficientes privilegios hasta políticas del sistema.

ANEXO II - Certificados digitales.

A. Introducción.

Como es sabido el uso de claves públicas para cifrar un mensaje, habilita a quien posea la correspondiente clave privada a descifrar el mismo. Asimismo, el uso de claves privadas para cifrar el resultado de aplicar un algoritmo de hash sobre un mensaje permite determinar la integridad de un mensaje. Pero en ninguno de los dos casos se puede establecer fehacientemente la identidad del supuesto emisor. Una forma de resolver este problema es que un tercero en quien tengamos confianza certifique que la clave pública pertenece a quien dice ser. Y justamente esto es lo que ofrece PKI.

B. Public Key Infrastructure.

B.1. Conceptos.

PKI se basa en el uso de certificados, instrumentos digitales emitidos por entidades de reconocimiento comprobable que permiten asociar una clave pública con una identidad. Dicho certificado además contiene información extra relativa a la identidad del dueño de la clave pública y a la entidad que emitió dicho certificado, así como también sobre su propósito y período de validez.

El procedimiento es relativamente sencillo. El interesado en validar su identidad hace la solicitud de un certificado en base a su clave privada a una autoridad de una insfraestructra PKI. Es importante que la autoridad seleccionada sea considerada de confianza por quienes constituirán la contraparte en el proceso de identificación, de lo contrario el certificado

pierde su utilidad. La autoridad luego de verificar la identidad del interesado y la autenticidad de la solicitud procederá a emitir el correspondiente certificado firmándolo con su propia clave privada. El emisor del certificado por lo tanto deberá implementar los mecanismos más adecuados para corroborar la identidad de quien lo solicita. Este procedimiento suele implicar el uso de documentación probatoria. La validación del certificado emitido se lleva a cabo utilizando el certificado autofirmado de la CA.

En PKI, quien se encarga de la emisión de certificados recibe el nombre de autoridad certificante o CA (Certification Authority), un ente privado o público especializado en el tema. Dicha entidad se encarga de administrar los certificados emitidos, que son identificados a través de un número de serie (serial). Dada la importancia de la tarea, los requisitos legales y técnicos para realizar dicha actividad son muy exigentes, esto resulta muy necesario ya que el organismo ocupa el principal lugar en esta cadena de confianza. Una CA debe ser altamente confiable especialmente si se trata de una root CA, la que firma su propio certificado. También existen las cadenas de certificados, en donde un certificado con determinadas características puede ser utilizado por otra CA para emitir sus propios certificados. En tal caso si hubiera un certificado inválido la cadena deja de ser confiable desde el nivel que ha sido comprometido.

Un certificado puede ser emitido para usos tan específicos como:

- Firma de correo electrónico.
- Identidad de web servers.
- Transacciones comerciales electrónicas.

Los certificados respetan un formato definido por el estándar X.509. La última versión, la 3, contempla el soporte de extensiones que permiten la incorporación de más datos, que ordenados en una serie de campos, pueden ser utilizados para múltiples propósitos.

B.2. Emisión de certificados digitales.

El proceso para la emisión de certificados se puede sintetizar en los siguientes pasos:

1) Establecida la finalidad del certificado, el interesado a través de un programa o herramienta dedicada genera su clave privada y un request asociado a dicha clave. El request servirá para solicitar a la autoridad certificante respectiva la emisión de un certificado. Alternativamente el interesado puede crear solo un request, para que la autoridad certificante se encargue de la creación de su clave privada y el certificado.
2) El interesado envía el request a la autoridad certificante.
3) La autoridad certificante le requiere al solicitante documentación o información probatoria que permita validar su identidad.
4) Si el punto anterior se cumple en forma exitosa, la autoridad certificante emite el certificado o una clave privada más el certificado, según sea el caso.
5) La autoridad certificante envía el certificado o la clave privada más el certificado al interesado. Existen diferentes estándares de archivos para cumplimentar tal acción conocidos como PKCS (Public-Key Cryptography Standards), en especial, si se trata de incluir una clave privada se recurre a un formato encriptado.

B.3. Revocación de certificados digitales.

PKI contempla además la revocación de certificados, es decir, los mismos pueden quedar inválidos antes de que expiren, a solicitud del involucrado. Para atender este caso existe un mecanismo de lista de revocación cuyo fin es informar qué certificados están comprometidos y por lo tanto han dejado de ser válidos, es decir, han dejado de ser confiables. La llamada CRL (Certificate Revocation List) es una lista de los certificados

revocados que suele ser periódicamente actualizada y publicada por la CA para evitar la circulación peligrosa de certificados inválidos como válidos. Existen diversos métodos para publicar CRL`s: parcialmente, por incrementos, a través de repositorios de consulta e inclusive existe un protocolo, el OSCP (Online Certificate Status Protocol) que incorpora a la infraestructura un agente de validación (OSCP responder).

ANEXO III - Protocolo LDAP.

A. Conceptos generales.

LDAP (Lightweight Directory Access Protocol) es un protocolo que define un servicio de directorio optimizado para lecturas y búsquedas, implementado en forma distribuida.

LDAP nació como un protocolo “liviano”, más sencillo, para comunicarse con el servicio de directorio X.500 como backend, en una arquitectura cliente-servidor, sobre el protocolo TCP/IP. X.500 es un servicio de directorio diseñado sobre el modelo OSI lo que implica cierto overhead en los mensajes que lo hacía “pesado”. LDAP no contempla muchas de las operaciones soportadas por X.500 que fueron descartadas por considerarse de poco uso. Vale decir que muchas soluciones LDAP que se pueden conseguir en internet, en realidad no disponen de un X.500 como backend.

La información en un directorio LDAP está estructurada en un modelo de árbol DIT (Directory Information Tree) en donde cada nodo constituye una entrada. Cada una de esas entradas contiene información asociada a una o más clases de datos, donde cada clase reúne una serie de atributos obligatorios y/u opcionales. Cada nodo puede ser unívocamente referenciado vía un identificador conocido como distinguished name (DN).

LDAP también puede contemplar mecanismos de autenticación para que un cliente pueda acceder a la información almacenada en forma segura.

ANEXO IV – Protocolo DHCP.

A. Conceptos generales.

DHCP (Dynamic Host Configuration Protocol) es un protocolo que provee un mecanismo de configuración automática de los dispositivos de red basada en el estándar TCP/IP. De esta manera facilita a los administradores la muchas veces tediosa tarea de asignar direcciones de red, dependiendo de la arquitectura y la envergadura de la red. Evitando así, asignaciones incorrectas, derroche de direcciones (originados por dispositivos que ya no las usan por baja) o duplicaciones, producto del error humano o de un deficiente y/o desactualizado sistema de registro, lo que inevitablemente es fuente de problemas de conectividad.

Basado en el modelo cliente/servidor, mediante este protocolo un cliente se conecta al servidor DHCP para recibir los parámetros necesarios a fin de configurar su interfaz de red (en principio, su dirección IP, red y máscara). A través de este servicio se pueden asignar direcciones tanto estática como dinámicamente (en base a un rango de IP disponibles). Claramente son apreciables las ventajas que ofrece el mismo en cuanto a la administración de direcciones IP en una red inalámbrica donde los dispositivos que se conectan lo hacen a veces a distintas VLANs o de forma ocasional y transitoria. Los access points por lo general tiene integrado un servidor DHCP configurable para proveer el servicio. Como beneficio adicional, desliga al propio usuario, en el caso de no contar con suficiente personal técnico, de tener que lidiar con la configuración de red de su estación de trabajo.

La asignación de IP`s es realizada por un período de tiempo determinado (address leasing), antes de que expire el plazo el cliente debe renovar el uso de la IP para no perder conectividad. En la práctica, los

clientes continúan usando la IP asignada mientras intentan renovar su uso. El address leasing permite que el DHCP server pueda reutilizar (reasignar) las IP`s que han dejado de ser utilizadas.

ANEXO V – Configuración del software open source.

En el presente anexo se detallarán las operaciones llevadas a cabo para implementar el software open source seleccionado. Esta sección no intenta ser un tutorial de configuración e instalación de esas herramientas, sólo se describirán aquellas acciones relacionadas específica y directamente con el modelo de autenticación propuesto.

A. Autoridad Certificante.

Para crear la propia autoridad certificante (CA), los pares de claves privadas/públicas de los usuarios y sus correspondientes certificados se utilizó un script provisto por el software FreeRADIUS. El mismo se vale de la herramienta OpenSSL. Dicho script (llamado bootstrap) se encuentra en el directorio …/raddb/certs (directorio de instalación). El script se alimenta de los archivos de configuración ca.cnf (para la CA), server.cnf (para el servidor RADIUS) y client.cnf (para los clientes). La corrida genera, en el directorio …/certs, las claves privadas (.key), los requests (.csr) y los certificados (.pem) más un archivo conteniendo el próximo serial number a asignar.

Los únicos archivos que necesita el servidor RADIUS son su clave privada, su certificado y el certificado de la autoridad certificante. Por razones de seguridad, la clave privada de la autoridad certificante debe resguardarse en un repositorio aislado de los demás circuitos existentes. Para llevar la clave privada y el certificado al cliente, ver ANEXO VII, se utilizó el estándar PKCS#12, que define el uso de un contenedor encriptado, también se debe enviar el certificado de la autoridad certificante.

A continuación se listarán algunos comandos OpenSSL utilizados durante el desarrollo de la prueba de concepto y otros que resultan muy útiles para administrar certificados:

Operación	Comando OpenSSL
Ver una clave privada	openssl rsa -text -noout -in
Ver el request de un certificado	openssl req -in [request] –text
Ver un certificado	openssl x509 -text -noout -in [certificado]
Probar un certificado	openssl s_server -cert [certificado] -key [clave privada] –www
Crear un contenedor para una clave privada y su certificado	openssl pkcs12 -export -clcerts -in [certificado] -inkey [clave privada] -out [p12]
Revocar un certificado	openssl ca -config ./ca.cnf -revoke [certificado comprometido]
Crear una lista de certificados revocados	openssl ca -config ./ca.cnf -gencrl -out [lista]
Ver lista de certificados revocados.	openssl crl -in [lista] -text –noout

B. Servidor RADIUS.

En el archivo de configuración “eap.conf”, ubicado en el directorio de instalación …/raddb, se determina:

- El EAP-Method, en este caso EAP-TLS (“default_eap_type = tls”).
- La ubicación de la clave privada y del certificado del servidor y del certificado de la autoridad certificante.

En el archivo de configuración “clients.conf”, también en …/raddb, se declaran los clientes (access points) habilitados para comunicarse con el servidor. Se indica la IP del access point, un identificador (para que aparezca en los logs) y la password compartida para la autenticación mutua.

En el archivo “users”, directorio …/raddb, se listan los usuarios que tienen permitido algún tipo de acceso. Dicha lista es procesada en orden de aparición y, por lo general, la búsqueda se detiene con el primer matcheo. Allí se establece el grupo de usuarios permitidos, en este caso “Ldap-Group”, que es el valor dado al atributo “radiusGroupName” de cada usuario en el repositorio LDAP.

En el archivo “ldap”, directorio …/raddb/modules, se indica la dirección del servidor LDAP y los parámetros del filtro para realizar la búsqueda en ese repositorio. Los parámetros son:

```
filter = "(&(dialupAccess=%u)(cn=%u))"
groupmembership_filter = (cn=%u)
groupname_attribute = radiusGroupName
groupmembership_attribute = radiusGroupName
```

Las dos primeras líneas determinan el filtro de búsqueda en el repositorio LDAP: el usuario debe tener su entrada con los permisos de acceso correctos (atributo dialupAccess) y además pertenecer al grupo habilitado (atributo radiusGroupName). Las restantes establecen que el atributo radiusGroupName es el que debe contener como valor el nombre del grupo definido en el servidor RADIUS (archivo “users”).

En el archiva “default”, directorio …/raddb/sites-available, se determina la incorporación del servicio LDAP al mecanismo de autorización (descomentando la palabra “ldap” en el módulo “authorize”).

C. Servidor LDAP.

En el archivo de configuración “slapd.conf”, ubicado en el directorio de instalación …/openldap, se incorpora el esquema de la clase de objeto RADIUS (openldap.schema) provisto por el software FreeRADIUS.

Las entradas en el repositorio LDAP se definen de la siguiente manera:

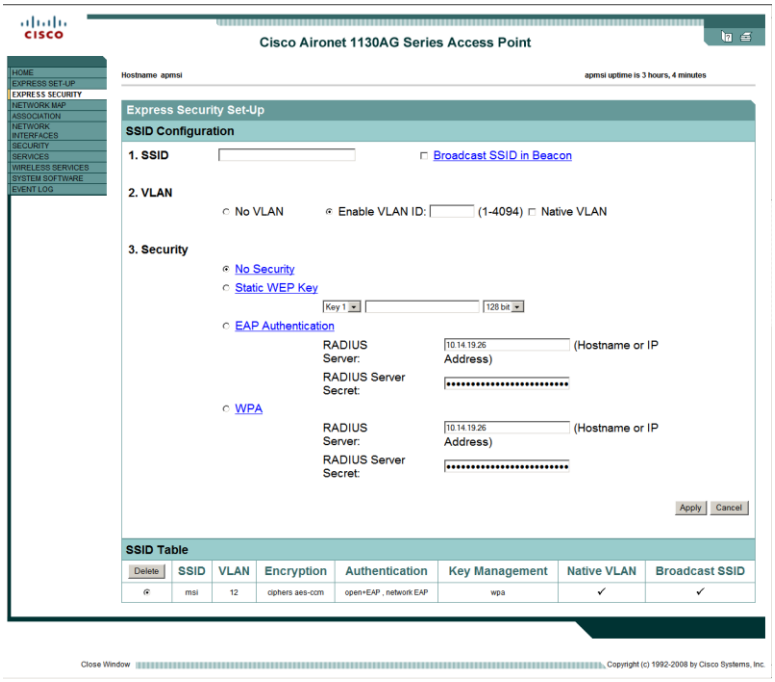
Entrada	Atributos
Grupo de usuarios	dn: ou=[GRUPO],dc=[DOMINIO] objectclass:organizationalunit ou: [GRUPO] description: [DESCRIPCION]
Usuario	dn: cn=[IDENTIFICADOR],ou=[GRUPO],dc=[DOMINIO] objectclass: person objectclass: radiusprofile cn: [NOMBRE] sn: [APELLIDO] dialupAccess: [IDENTIFICADOR] radiusGroupName: [GRUPO RADIUS]

Los dos últimos atributos (dialupAccess y radiusGroupName) son los utilizados durante la etapa de autorización y se encuentran definidos en el esquema provisto por FreeRADIUS. El primero, “dialupAccess”, debe coincidir con el cn del certificado del usuario y el segundo, “radiusGroupName”, establece el grupo LDAP aceptado por el servidor RADIUS.

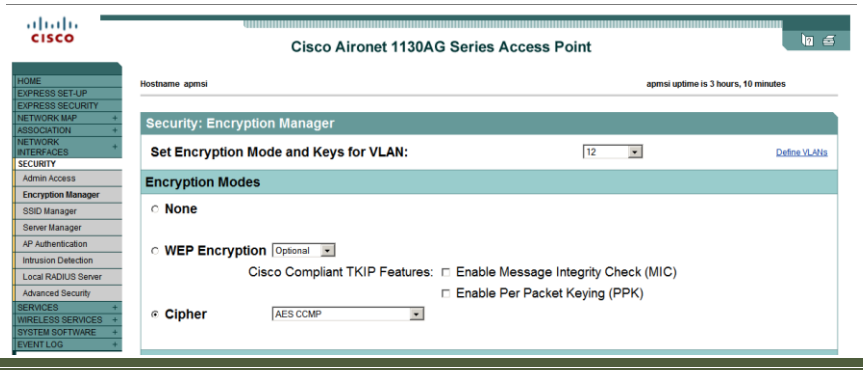
ANEXO VI – Configuración del access point.

El access point utilizado es un Cisco Aironet 1130 AG. La configuración se realizó vía el servidor http con el que cuenta dicho dispositivo. A la configuración de base hay que añadir los parámetros de WPA, EAP y RADIUS. A continuación, las principales capturas de la configuración efectuada:

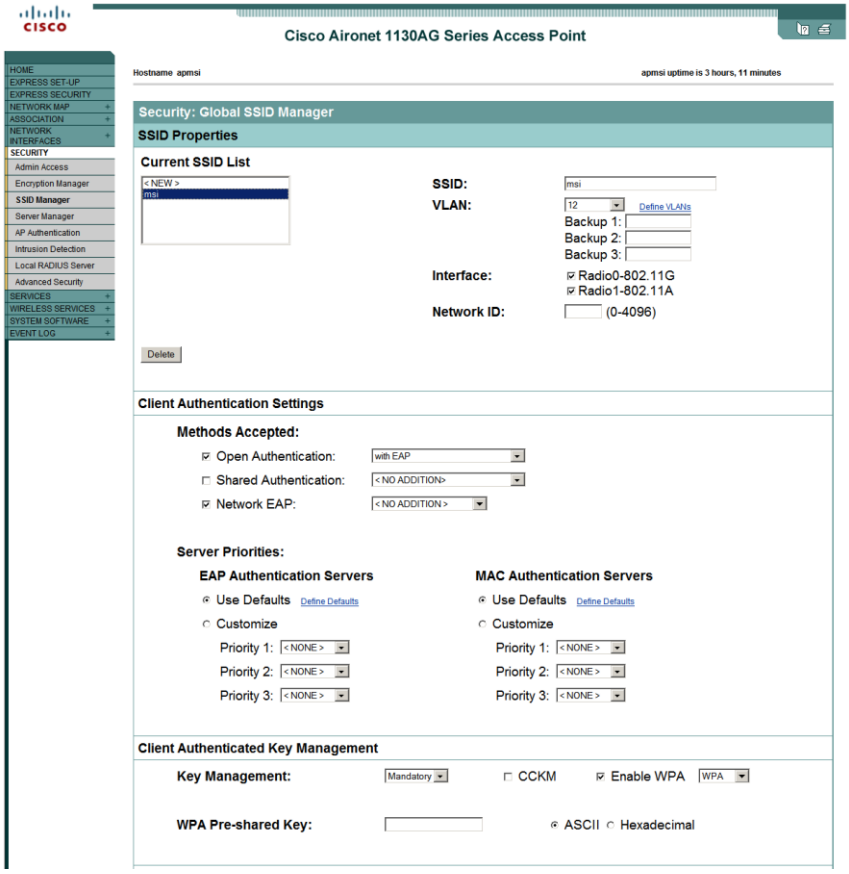
- Configuración general.



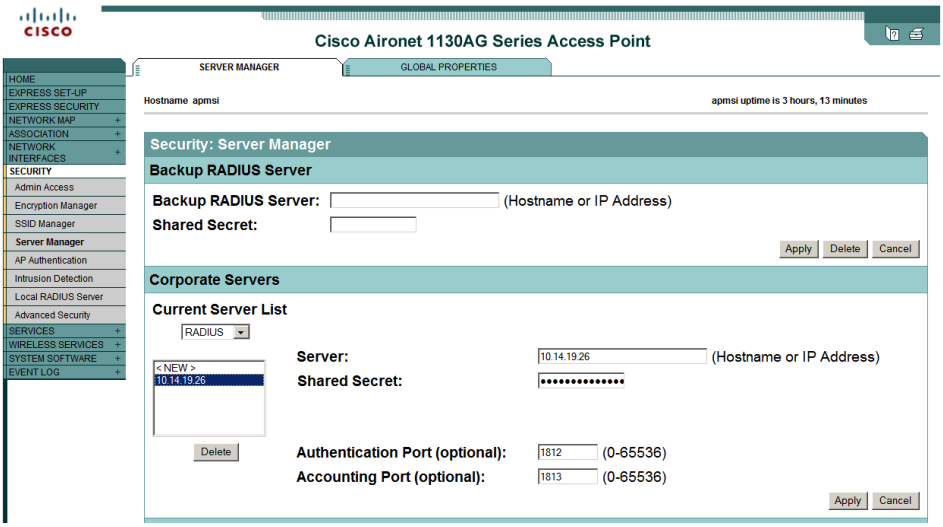
- Elección del algoritmo de cifrado: CCMP (AES).



- Configuración del método de autenticación utilizado con el cliente.



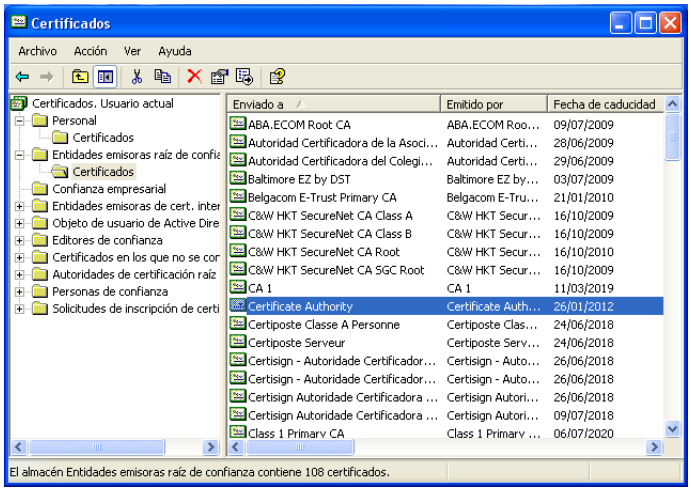
- Configuración del servidor RADIUS, incluyendo la clave pre-compartida.



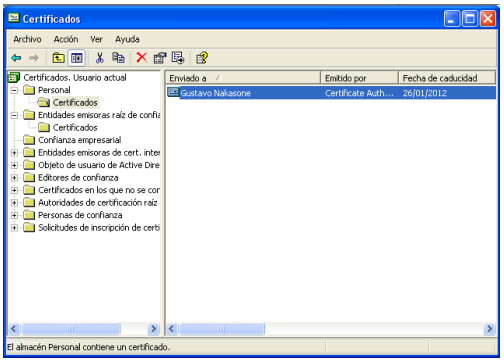
ANEXO VII - Configuración de la estación inalámbrica.

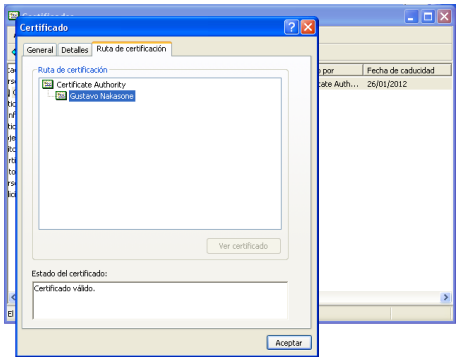
La configuración comprende dos tareas bien diferenciadas. Una es la carga de la clave privada del usuario y los correspondientes certificados emitidos por la CA, y la otra, es la configuración adecuada de la placa de red inalámbrica.

La primera tarea se realiza a través de herramienta MMC (Microsoft Management Console) de Windows, que provee la aplicación certmgr.msc. Este anexo no pretende ser un tutorial sobre la mencionada herramienta, por lo que solamente se mostrarán las capturas que muestran el resultado de la operación realizada.



Certificado de la CA

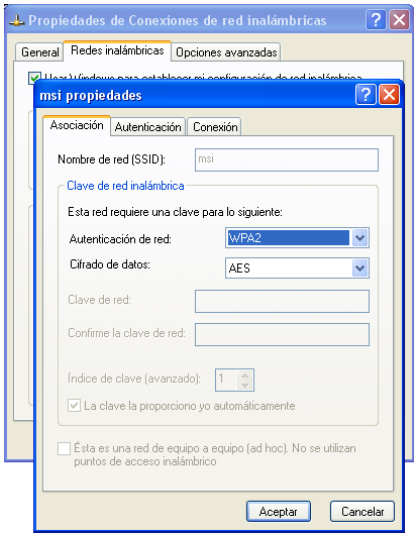




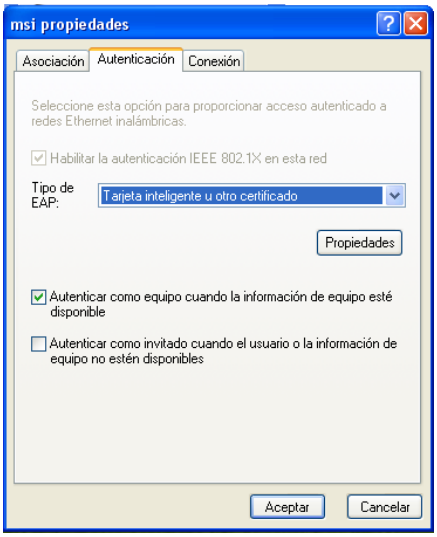
Clave privada del usuario y su certificado

Ruta del certificado

- En la configuración de la placa de red inalámbrica se debe ajustar el modo a WPA2 y el método EAP con certificados.

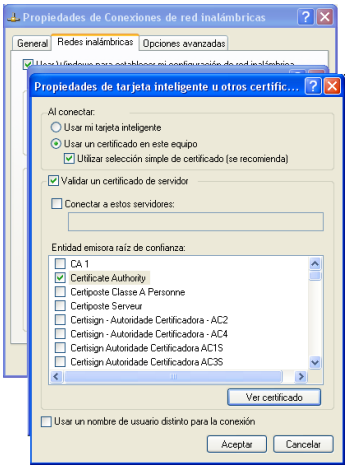


WPA2



EAP con certificados.

- Para terminar, es importante indicar la CA seleccionada.



Bibliografía.

A. Libros.

- Bruce Potter & Bob Fleck, 802.11 Security, O'Reilly Media, 2002.
- Matthew Gast, 802.11 Wireless Networks: The Definitive Guide, Second Edition, O'Reilly Media, 2005.
- Edwin Lyle Brown, 802.1X Port-Based Authentication, First Edition, Auerbach Publications, 2007.
- Gerald Carter, LDAP System Administration, O'Reilly Media, 2003.
- John Viega, Matt Messier & Pravir Chandra, Network Security with OpenSSL, First Edition, O'Reilly Media, 2002.
- Jonathan Hassell , RADIUS, O'Reilly Media, 2002.
- Jon Edney, William A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison Wesley, 2003.
- Ralph Droms & Ted Lemon, The dhcp handbook, Second Edition, Sams, 2003.

B. Internet.

- http://freeradius.org, The FreeRADIUS Project, marzo 2011.
- http://www.openca.org, OpenCA PKI Research Labs (anteriormente OpenCA Project), marzo 2011.
- http://www.openldap.org, The OpenLDAP Project, marzo 2011.
- http://www.openssl.org, OpenSSL Project, marzo 2011.