UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA

DISEÑO Y PRUEBAS DE UN SISTEMA DE CONTROL DE ACCESO A WLAN MEDIANTE EAP Y RADIUS

Presentado por:

Ing. Giovanni D. Mazzei P

TRABAJO DE GRADO PRESENTADO ANTE LA ILUSTRE UNIVERSIDAD CENTRAL DE VENEZUELA PARA OPTAR AL TITULO DE ESPECIALISTA EN COMUNICACIONES Y REDES DE COMUNICACIONES DE DATOS

Tutor Académico:

Ing. Vincenzo Mendillo

Caracas, Enero 2012

AGRADECIMIENTO

Realicé un sueño, culminé una meta que implicó
dedicación, lucha, desvelo y el apoyo de cada uno de ustedes;
en muestra de gratitud le agradezco en estas cortas líneas:
A Dios ante todo, por iluminarme y guiarme en todos los aspectos de la vida.
A mi familia y a mi novia, por su apoyo constante e incondicional y alentarme
a culminar esta etapa profesional.
A todos los profesores, por la gran labor desarrollada de impartir
educación, por permitirnos peregrinar en sus aulas, por ser nuestro pilar
fundamental en este nuevo futuro. En especial a mi tutor el Prof. Vincenzo Mendillo,
por su aporte intelectual y apoyo en la realización del presente proyecto y ser una
gran persona y amigo.
A todas las personas que de una manera u otra, contribuyeron
En la ejecución del presente proyecto.
A todos.

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA

POSTGRADO EN ESPECIALIZACIÓN EN COMUNICACIONES Y REDES DE COMUNICACIÓN DE DATOS

DISEÑO Y PRUEBAS DE UN SISTEMA DE CONTROL DE ACCESO A WLAN MEDIANTE EAP Y RADIUS

Autor: Ing. Giovanni D. Mazzei P **Tutor**: Prof. Vincenzo Mendillo

RESUMEN

El presente Trabajo Especial de Grado está basado en el diseño y pruebas de un sistema de control de acceso a WLAN mediante EAP y RADIUS. Su desarrollo se basó en la investigación bajo la modalidad de proyecto factible. Se realizó el estudio del protocolo de seguridad RADIUS y se utilizó la aplicación FreeRADIUS para analizar su comportamiento en redes inalámbricas, con la finalidad de implantarlo como mecanismo avanzado de control de acceso en redes empresariales.

En los últimos años las redes de área local inalámbricas (WLAN, Wireless Local Area Network) han ido ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios el acceso a información y recursos en tiempo real sin necesidad de estar físicamente conectados a una red. Unas de las características menos entendida de esta tecnología, es el aspecto de la seguridad, lo que representa un serio problema, ya que se pone en riesgo la confidencialidad, integridad y disponibilidad de la información. Partiendo de este hecho, se consideró conveniente

diseñar, probar y evaluar un sistema de control de acceso a WLAN mediante el protocolo EAP en conjunto con un sistema de autenticación basado en RADIUS. Luego de realizar una investigación, se eligió la herramienta open source, llamada FreeRADIUS, operando sobre una plataforma GNU/Linux. La utilización de tecnologías basadas en código libre, ha permitido abrir una gama de posibilidades, la cual va más allá de la parte económica y de los costos que se pueden ahorrar, sino en la libertad de modificar, optimizar y conocer el funcionamiento de estas aplicaciones.

Se utilizaron como base teórica los conceptos de un sistema AAA. Se estudiaron las estructuras básicas del protocolo EAP y los diferentes métodos o mecanismos de autenticación. Se realizó una revisión del funcionamiento y desglose del protocolo RADIUS, su formato como paquetes y la secuencia de autenticación.

Las bondades de esta solución fueron probadas en ambientes de laboratorio, utilizando máquinas virtuales, como lo fueron VirtualBox y VMWare.

Luego de realizar las pruebas, se recomienda la implementación de RADIUS como protocolo de autenticación, a través de las herramientas open source FreeRADIUS y ZeroShell sobre plataformas virtualizadas, ya que de esta manera se obtiene un alto desempeño, una alta disponibilidad y una buena relación costo/prestaciones.

ÍNDICE GENERAL

LISTA DE FIGURAS

FIGURAS Pág.

LISTA DE TABLAS.

INTRODUCCIÓN

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy. Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red alambrada.

La popularidad de estas redes ha crecido a tal punto que los fabricantes de computadores y motherboards están integrando dispositivos para acceso a WLAN en sus equipos; tal es el caso de Intel, que fabrica el chipset Centrino para computadores portátiles.

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Cualquier equipo que se encuentre cerca de un punto de acceso, podría tener acceso a la red inalámbrica. Por ejemplo, si varias empresas tienen sede en un mismo edificio, y todas ellas poseen red inalámbrica, el equipo de un empleado podría encontrarse en cierto momento en el área de cobertura de dos o más redes diferentes, y dicho empleado podría conectarse (intencionalmente o no) a la red de una compañía que no es la suya. Aún peor, como las ondas de radio pueden salir del edificio, cualquier persona que posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a la red de la empresa.

Lo grave de esta situación es que muchos administradores de redes parecen no haberse dado cuenta de las implicaciones negativas de poseer puntos de acceso inalámbrico en la red de una empresa. Es muy común encontrar redes en las que el acceso a Internet se protege adecuadamente con un firewall bien configurado, pero al interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos e irradiando señal hacia el exterior del edificio. Cualquier persona que desde el exterior capte la señal del punto de acceso, tendrá acceso a la red de la compañía, con la posibilidad de navegar gratis en la Internet, emplear la red de la compañía como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software y/o información, introducir virus o software maligno, entre muchas otras cosas.

Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la compañía.

La mala configuración de un acceso inalámbrico es, desgraciadamente, una cosa muy común. Un estudio publicado en 2003 por RSA Security Inc.4 encontró que de 328 puntos de acceso inalámbricos que se detectaron en el centro de Londres, casi las dos terceras partes no tenían habilitado el cifrado mediante WEP (Wired Equivalent Protocol). Además, cien de estos puntos de acceso estaban divulgando información que permitía identificar la empresa a la que pertenecían, y 208 tenían la configuración con la que vienen de fábrica.

Como se mencionó anteriormente, los mecanismos de seguridad poseen debilidades y algunas veces no ofrecen los niveles de seguridad esperados. Por ende, es importante realizar un análisis de los mecanismos de seguridad existentes y del sistema de control de acceso que va hacer motivo de nuestro estudio.

El presente trabajo se encuentra estructurado por 5 capítulos, los cuales poseen objetivos determinados que se mencionan en forma breve a continuación:

Capítulo I. El Problema

En él se presentan los aspectos introductorios a la investigación, en su contenido se hace referencia al planteamiento del problema, también se describen: la justificación, alcances, limitaciones que intervienen en el desarrollo del proyecto, las cuales plantean de forma detallada su estudio y permiten la inicialización de la primera etapa del proyecto.

El Capítulo II. Marco Metodológico

Está constituido por el Marco Metodológico en el cual se describe el diseño de la investigación, las técnicas e instrumentos de recolección de datos, indispensables en la recopilación de la información requerida y por último, la metodología utilizada para el análisis y diseño del sistema.

El Capítulo III. Marco Teórico

El Marco Teórico esta integrado por los antecedentes relacionados a la investigación que se presenta, se incluyen también las bases teóricas que sustentan a la investigación tanto en un nivel operativo como en un nivel técnico.

El Capítulo IV. Pruebas y Resultados.

Este capítulo se presenta los resultados obtenidos en la investigación realizada, el estudio de factibilidad del proyecto y el proceso de cómo fue llevado a cabo el estudio metodológico en la investigación.

Consta de la explicación clara y precisa de cada uno de los pasos que se realizaron para el desarrollo del sistema de Control de Acceso a WLAN, mediante EAP y RADIUS.

El Capítulo V. Conclusiones y Recomendaciones

Se concretan los resultados del trabajo de investigación así como el desarrollo del sistema, también se presentan la conclusiones y recomendaciones necesarias, las cuales deben ser tomadas en consideración para el sistema. Culmina este capítulo con la Bibliografía y los Anexos correspondientes a la investigación.

Al estructurar los cinco capítulos de esta forma, se tiene como objetivo principal, proporcionar a los lectores de este Trabajo Especial de Grado, la organización secuencial de los diversos puntos ubicados en este contexto.

CAPÍTULO I

1.1 PLANTEAMIENTO DEL PROBLEMA

La irrupción de la nueva tecnología de comunicación basada en redes inalámbricas ha proporcionado nuevas expectativas en el futuro para el desarrollo de sistemas de comunicación, así como nuevos riesgos. La flexibilidad y la movilidad que nos proporcionan las nuevas redes inalámbricas han hecho que la utilización de estas redes haya aumentado en estos años, siendo la mejor manera de realizar conectividad de datos en edificios sin necesidad de cablearlos. Pero como todas las nuevas tecnologías en evolución, presenta unos riesgos debido al optimismo inicial y en la adopción de la nueva tecnología sin observar los riesgos inherentes a la utilización de un medio de transmisión tan observable como lo son las ondas de radio.

El presente trabajo pretende dar una visión global del estado actual de la seguridad en las redes inalámbricas, desde los riegos existentes en las implementaciones de los estándares actuales, hasta las mejores propuestas para subsanar dichos riesgos pasando por consideraciones recomendadas en cuanto al diseño de redes inalámbricas.

Ahora bien, en la actualidad es muy común observar a una gran cantidad de personas localizando y conectándose a una gran cantidad de redes tanto privadas como publicas, ya sea para buscar información o comunicarse entre ellos mismos. Por tal motivo se requiere el uso de un buen sistema de control de acceso para impedir el ingreso de personas ajenas a estas redes.

Cuando se maneja un gran numero de usuarios como entornos empresariales, el control de acceso puede hacerse más eficazmente, centralizando las funciones AAA, en servidores, también llamados servidores de autenticación, para tal fin utilizaremos una herramienta denominada Zeroshell. Es una distribución Linux para servidores y dispositivos embebidos, que provee servicios de red. Es esencialmente un firewall open source, que posee las características de los equipos más complejos de seguridad; éste nos permitirá configurar el servidor de autenticación con el protocolo que va a ser estudiado en este trabajo de grado, como lo es RADIUS.

Remote Authentication Dial In User Service, es un protocolo AAA (Autenticación, Autorización y Administración) para aplicaciones como acceso a redes o movilidad IP.

Luego de evaluar las alternativas para desarrollar un innovador sistema de control de acceso frente al menú de opciones tecnológicas existentes se escogió RADIUS, las razones que justifican esta selección son:

- ✓ Facilita una administración centralizada de usuarios.
- ✓ Permite una gran cantidad de almacenamiento
- ✓ Es altamente flexible y configurable.

También lo que se plantea en este trabajo es la de romper los paradigmas de que usar redes inalámbricas es inseguro, ya que con las herramientas necesarias y tomando en cuenta las mejores practicas para su configuración se tendrá una red confiable y segura.

1.2 Objetivos

1.2.1 Objetivo General

Diseñar y probar un sistema de control de acceso a WLAN mediante EAP y RADIUS

1.2.2 Objetivos Específicos

- Investigar los distintos protocolos de autenticación y autorización disponible bajo código abierto.
- Comparar los distintos protocolos de autenticación y autorización disponible bajo código abierto.
- Analizar teórica y técnicamente el funcionamiento del protocolo de autenticación y autorización (RADIUS) en redes inalámbricas y sus principales ventajas.
- Diseñar un esquema de seguridad que garantice autenticidad y autorización en la red, mediante el uso del protocolo RADIUS.
- Realizar pruebas funcionales de conexiones inalámbricas conjuntamente con el protocolo de autenticación recomendada, a fin de establecer características funcionales de la solución.
- Culminar con conclusiones y recomendaciones.

1.3 Justificación

Las redes inalámbricas se diferencian de las redes cableadas, en la naturaleza del medio que emplean para transmitir sus datos, el aire El acceso a los elementos cableados es físicamente complicado por que se encuentran protegidos por paredes y

puertas .Sin embargo, el limitar el acceso por el medio de transmisión inalámbrico es más complicado, lo que conlleva que se hayan convertido en objetivos interesante de posibles ataques. Estos problemas de seguridad son de especial relevancia en empresas o entornos empresariales por la confidencialidad de la información utilizada en los mismos. Por esta razón las redes inalámbricas necesitan mecanismos de seguridad adicionales para garantizar un nivel adecuado de seguridad.

1.4 Alcance

El proyecto se basará en el estudio del protocolo de seguridad en redes inalámbricas, RADIUS, con la utilización de software de redes Open Source, como lo son ZeroShell, VirtualBox, y FreeRADIUS, entre otros con el objetivo de realizar un análisis detallado del mismo, para estudiar su comportamiento en redes inalámbricas, con la finalidad de implantarlo.

CAPÍTULO II

2 METODOLOGÍA DE LA INVESTIGACIÓN

En base a las distintas características que presenta esta investigación y los objetivos planteados, se puede considerar como un Proyecto Factible que, como lo señala la Universidad Pedagógica Experimental Libertador (UPEL, 2006).”El Proyecto Factible consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. El proyecto debe tener apoyo en una investigación de tipo documental, de campo o un diseño que cumpla ambas modalidades.”(p.21).

El Proyecto Factible comprende las siguientes etapas generales: diagnostico, planteamiento y fundamentación teórica de la propuesta; procedimiento metodológico, actividades y recursos necesarios para su ejecución; análisis y conclusiones sobre la viabilidad y realización del Proyecto; y en caso de su desarrollo, la ejecución de la propuesta y la evaluación tanto del proceso como de sus resultados.(p.21).

2.1 Revisión Teórica

Para la revisión teórica se realizaron consultas a varias fuentes de investigación, como lo fueron libros, material electrónico (CD-DVD), consultas vía email, sitios Web, etc.

La realización de la revisión teórica está enfocada en determinar los siguientes puntos:

- ✓ Determinar las características principales de los sistemas de autenticación AAA (Autenticación, Autorización y Contabilización).
- ✓ Comparación de los sistemas de autenticación, como TACACS, RADIUS, Diameter, etc.
- ✓ Funcionamiento del protocolo RADIUS, a través de la herramienta open source freeRADIUS la cual se base nuestra investigación.
- ✓ Explicar las características de la autenticación EAP en redes inalámbricas.
- ✓ El funcionamiento del estándar 802.1X en las redes inalámbricas.
- ✓ Las características y el funcionamiento del protocolo de autenticación y cifrado en redes inalámbricas.
- ✓ La utilización de herramientas basadas en código abierto (Linux)
- ✓ Buenas prácticas en el diseño, configuración e instalación de la solución estudiada en redes inalámbricas.
- ✓ Impacto de la seguridad que se debe considerar a la hora de implantar un sistema de autenticación basado en el protocolo RADIUS en redes inalámbricas.

2.2 Plantear el objetivo de la investigación

Una vez realizado la revisión teórica se procede a realizar el planteamiento de los objetivos de la investigación en su máxima expresión.

Los puntos importantes de esta fase de investigación, es considerar los siguientes aspectos:

- ✓ Conocer los diferentes sistemas de autenticación existentes.
- ✓ Selección del sistema de autenticación RADIUS.
- ✓ Utilizar herramientas basadas en Linux
- ✓ Estudiar la seguridad en las redes inalámbricas

.

2.3 Realización de Pruebas y Evaluaciones

En esta fase se realizan las pruebas funcionales de un sistema de control de acceso a WLAN mediante EAP y RADIUS, para lo cual se debe generar las condiciones necesarias para las mismas.

- ✓ Establecer las pruebas funcionales a realizar.
- ✓ Implantar el ambiente de laboratorio necesario para la realización de las pruebas previstas.
- ✓ Instalar y configurar las soluciones el sistema de control de acceso a WLAN mediante EAP y RADIUS.
- ✓ Realizar las pruebas funcionales bajo las herramientas de software libre seleccionadas.
- ✓ Detectar y solucionar fallas y/o errores comunes que pudieran afectar el adecuado funcionamiento en el ambiente de laboratorio.
- ✓ Documentar experiencias de las pruebas efectuadas sobre el protocolo de autenticación RADIUS, basada en herramientas de software libre.

.

2.4 Establecer Recomendaciones

En esta fase de la metodología se analizan los resultados recolectados de las pruebas y evaluaciones a fin de formular recomendaciones respecto al diseño de un sistema de control de acceso a WLAN mediante EAP y RADIUS

También en esta fase se recomienda la arquitectura a implantar en la solución al diseño de un sistema de control de acceso

CAPÍTULO III

3 MARCO TEÓRICO

3.1 Sistemas AAA.

En el mundo actual la identificación de las personas se ha convertido en una importantísima necesidad en cualquier ámbito. Para poder identificarnos ante otra persona utilizamos los documentos de identidad aceptados (Cédula de Identidad, pasaporte, tarjetas, etc.), presentándolos ante quien nos los solicita. Sin embargo, en muchas situaciones esto ya no es suficiente, ya que no existe una persona física ante nosotros, encargada de comprobar la autenticidad de nuestro documento, sino un sistema (computadora, red, etc.) que precisa saber quiénes somos sin posibilidad de duda, para ofrecernos un servicio concreto. La cantidad de situaciones donde se produce esto en la vida real es muy elevada y aumenta cada día. Muchas veces no percibimos el gran alcance de estas situaciones, ya que lo hacemos de forma automática, sin plantearnos la importancia de esta seguridad.

El número de servicios que precisan de información es cada día más numeroso. La forma de realizar esta identificación suele ser especifica para cada uno de esos servicios ofrecidos, con lo que la lista de identificadores y contraseñas que debemos manejar es cada vez mayor, y por tanto más complicada para los usuarios. En el caso de una identificación física como la de la cédula de identidad tradicional, ésta nos sirve para presentarlo en una gran variedad de situaciones y servicios (pagar con tarjeta de crédito, retirar dinero, etc.).

Cada día aumenta el numero de proveedores de servicios que nos solicita identificación para todo tipo de funciones que, teóricamente, nos facilitan la vida: acceso público o privado a Internet, telefonía móvil, acceso al banco, compra por Internet, servicios y tramites legales o gubernamentales, servicios universitarios, voto por Internet, etc. El problema del manejo de tantas credenciales es tan grave que se venden programas para el archivado seguro o cifrado de todos los nombres de usuarios, contraseñas, secretos compartidos, etc., con lo que tenemos que lidiar día a día.

Desde el punto de vista del usuario que se identifica ante un sistema, también es de vital importancia que el sistema que nos identifica sea el que suponemos que tiene que ser. Por ejemplo, cuando nos conectamos a nuestro banco, éste nos identifica para asegurarse que ofrece sus servicios a la persona que los ha contratado, y no a una persona que hace uso fraudulento de ellos. Pero igualmente cuando realizamos esta conexión deberíamos asegurarnos que quien nos pide ser identificados sea realmente el banco al que pretendemos acceder y no una entidad fraudulenta. Por ello debemos identificar al identificador.

Lo que hay detrás de todos y cada uno de estos servicios es una infraestructura de sistemas basados en la autenticación, que gestionan todos nuestros datos de forma segura y eficiente. Estas infraestructuras pueden ser muy sencillas o extremadamente complejas, según el número de usuarios y localizaciones que manejan y según sus niveles de garantía de seguridad.

Debemos comprender que finalmente es y debe ser el propio usuario el responsable de solicitar o exigir unos niveles determinados y adecuados de seguridad a los propios proveedores de servicios, aunque en muchas ocasiones la seguridad vaya en sentido contrario de la comodidad.

3.2.1 Las Tres “A”: AAA

Siempre que se habla de sistemas basados en la autenticación se habla de RADIUS como principal alternativa. RADIUS es un protocolo que existe antes que AAA y que, cumple todas las normas del estándar AAA. Esto se debe a que el desarrollo de RADIUS es anterior a AAA y que libremente prestó sus códigos y conocimientos al grupo de trabajo que comenzó a diseñar las bases de AAA. Las personas que formaron los grupos de diseño de RADIUS y AAA fueron en muchos casos los mismos.

AAA es un estándar para el diseño de sistemas basados en la autenticación. No es un sistema en si, sino una colección y definición de normas (un marco) para la creación de sistemas.

AAA son las siglas en ingles de Authenticaction + Authorization +Acconting, que en castellano se traduce como Autenticación +Autorización + Arqueo. Esta ultima traducción (Arqueo) también se denomina "Contabilidad". La fusión de estos tres componentes nos permite crear un sistema de gestión completa de usuarios que controle todos los aspectos relativos a su identificación (a partir de aquí: autenticación), gestión de recursos o servicios permitidos para su uso (autorización) y gestión de reportes y estadísticas para el control de su utilización (arqueo). Este sistema íntegramente aplicado es de una grandísima potencia para gestionar cualquier tipo de servicio, desde los más simples hasta los más complejos y seguros.

Antes de la existencia de este estándar, la autenticación era un proceso independiente, al igual que la autorización y el arqueo. Para acceder a un servicio concreto, dependiendo del fabricante y del servicio, había que configurar manualmente en cada uno de los equipos de acceso los protocolos y las bases de datos de autenticación necesarias. El hecho de estandarizar este proceso facilitó la vida de muchos administradores de redes que tenían que hacer grandes esfuerzos

para unificar y administrar sus sistemas. En los primeros años de implantación de Internet, ya comenzó a ser una importantísima necesidad el encontrar un sistema o protocolo para que los ISPs (Internet Service Providers) pudieran facilitar y garantizar la entrada a sus clientes.

Si agrupáramos muchos de estos sistemas basados en la autenticación, podríamos crear un único tipo de identificación para autenticarnos de forma idéntica en cualquiera de los servicios en los que nos hubiéramos previamente registrado. Esto simplificaría la labor del usuario, evitando mantener diferentes tipos de credenciales para todos los sistemas. Pero para que esto no resulte demasiado arriesgado para el usuario, debe tener una gran confianza en las entidades que gestionan sus credenciales y además debe poder tener el control completo sobre la revocación o retirada de su confianza en cualquier momento.

AAA no queda simplemente en unas normas que permiten regular la implantación y desarrollo de RADIUS, sino que se desvincula de RADIUS, permitiendo la coexistencia de otros productos basados en las mismas normas como Diameter. A Diameter se le pudo considerar un producto de futuro que desbancaría a RADIUS en los años 90. Su nombre (Diámetro) proviene de "el doble de RADIUS" o como dicen sus desarrolladores de "twice as good as RADIUS" (dos veces tan bueno como RADIUS). Diameter prometía mejorar todos los problemas de escalabilidad y seguridad de RADIUS, actualizando sus limitaciones hasta lo necesario para su futuro cercano. Otros sistemas basados en el Standard AAA son TACACS (Terminal Acces Controller Access Control System).

3.1.1.1 Orígenes, Descripción y Regulación.

Para la creación de AAA se forma un grupo de trabajo en la IETF (Internet Enginerin Task Force) dedicado al estudio y desarrollo de un estándar que desvincule a RADIUS como único producto de las tecnologías basadas en la autenticación. Con el fin de que se puedan crear otros productos que mejoren este sistema y que regulen su funcionamiento, se parte del código fuente de RADIUS y se mejoran sus propiedades. Como suele ser habitual en el caso de los estándares, se anticipa la aparición de nuevos productos comerciales a la finalización de los RFC (Request for Changes), como paso con RADIUS. Pero el grupo de trabajo de AAA continúa creando las bases de funcionamiento de los productos basadas en la autenticación hasta hoy, a fin de desarrollar productos cada vez más seguros y estables. Sin embargo, RADIUS cumplió las normas del estándar AAA desde el primer día hasta sus últimos desarrollos, y eso es porque fue precursor de todos estos estándares. Pero RADIUS no era la finalidad de AAA, ya que este grupo fue más lejos, adelantándose al método existente para crear otros sistemas más avanzados como Diameter y otros que queden por llegar. Por esto, cuando se habla de AAA se piensa en primer lugar en RADIUS, pero puede ser que en unos años se hable de otros productos similares.

En el caso de RADIUS, el producto apareció por la necesidad que planteaba el mercado y después se fue mejorando y estudiando en los grupos de trabajo creados para tal fin. Antes de que estos grupos dieran sus frutos, su implantación ya era muy importante. Esta es otra forma de poner un producto como este en circulación. De esta manera ha sido AAA el grupo que ha ido posteriormente sentando las bases de actualización del mismo, permitiendo que no quede en un producto propietario para unos pocos fabricantes y pueda ser ampliamente implantado por cualquier fabricante. Los esfuerzos de este grupo de trabajo sientan las bases para el beneficio común de todos los usuarios que acaban utilizando de forma transparente estos productos.

Las metas que se planteó el grupo de trabajo AAA son:

- Buscar la claridad sobre las normas de funcionamiento de un modelo basado en la autenticación, que pueda ser interconectable con otros.
- Organizar los tipos de mensajes que necesita este tipo de sistema para desempeñar óptimamente su servicio, informando de todas las incidencias que se produzcan.
- Introducción de soporte para el nuevo protocolo IPv6
- Independencia del tipo de transporte, definiendo un método principal de transporte y dejando abiertas otras futuras posibilites.
- Soporte completo para proxy y control de carga.
- Mantenimiento de la compatibilidad con el protocolo RADIUS.
- Reforzamiento de la seguridad en todos los procesos procurando no sobrecargar el tráfico.
- Posibilidad de implementación en los equipos existentes (legacy) y futuros.
- Definición de MIB para IP tanto en su versión 4 como 6, para su uso sobre el protocolo SNMP.

El modelo de arquitectura que plantea AAA es en origen un modelo cliente-servidor, aunque en su posterior desarrollo contempla protocolos de red tipo peer to peer. En la arquitectura cliente-servidor un sistema cliente solicita los servicios de un sistema servidor, pero el sistema servidor nunca solicita servicios del sistema cliente. Así se puede controlar toda la infraestructura de este sistema que permite controlar los anchos de banda y flujos de información, permitiendo redundancia y balanceo de carga hacia otros sistemas paralelos de servidores.

AAA permite la existencia de servidores proxy para descentralizar peticiones hacia otros servidores, con lo que una petición de autenticación, autorización o arqueo podrá ser transferida a otro servidor secundario por el servidor principal. Todo este proceso de proxy es independiente para cada una de las tres "A", por lo que se pueden construir redes complejas que gestionen independientemente la autenticación hacia un servidor, la autorización hacia otro u otros y el arqueo hacia otros. Todo esto proporciona las características de redundancia, descentralización y balanceo de carga. Esta descentralización no es iniciada por el cliente, sino por el equipo autenticador (NAS) o por el servidor de autenticación.

En un esquema clásico cliente-servidor, el cliente es el equipo o usuario que solicitaría la autenticación o la entrada al sistema, y el servidor es el recurso que nos provee servicios. En el caso de AAA, no se debe utilizar esta definición de cliente y servidor, ya que esto nos podría llevar a equívocos, puesto que estos conceptos "cliente/servidor" son más ambiguos. En esta cadena de participantes existen diferentes componentes que la hacen un poco más compleja:

- El equipo o usuario que solicita autenticación o entrada se llama suplicante, y no es obligatoriamente quien inicia la secuencia de autenticación.

- El equipo de red que hace de puerta de entrada física a la red, llamado NAS (Network Access Server) o servidor de acceso a la red, es el que permite la entrada física a la red y tramita nuestra autenticación. Puede ser una pila de modems, un switch de red, un punto de acceso (AP), un router, etc. Este equipo suele ser quien inicia la secuencia de autenticación al detectar una conexión activa en una de sus puertas, por ello se le denomina autenticador. Su labor es la de hacer de intermediario entre el suplicante y el servidor de autenticación. En AAA también se le denomina "equipo de servicio" o Service Equipment. El NAS es en la realidad el centro de todo de este sistema

AAA, ya que es el responsable de abrir o limitar las características reales de funcionamiento de la infraestructura.

- El Servidor de Autenticación que puede ser RADIUS, TACACS, Diameter u otros y es el que dirige todo el proceso de autenticación, autorización y arqueo de los equipos y usuarios que solicitan acceso. Por supuesto en AAA se le conoce como “Servidor AAA”.

- El servidor de Autenticación o servidor AAA puede hacer el papel de proxy, elevando las consultas a otros servidores AAA. De esta manera un Servidor AAA que hace de Proxy AAA se convierte en cliente de otro servidor.

- El servidor de directorio o servidor de bases de datos de usuarios y credenciales, al cual el servidor de autenticación va a solicitar los datos de autenticación de los solicitantes de acceso. Éste pudiera ser la misma màquina que el servidor de autenticación, aunque en instalaciones reales no suela serlo. Puede ser un servidor de AD (Active Directory) de LDAP (Lightweight Directory Access Protocol), una base de datos SQL (MySQL, Microsoft SQL Server, Oracle, etc.), o un servidor Unix con credenciales de usuario.

- El servidor de recursos y servicios que necesita el usuario para realizar su cometido en la red. Puede ser un servidor de almacenamiento de datos, un servidor Web, etc.

- El Proveedor de Servicios (Service Provide) en el modelo AAA es el propietario de la infraestructura de acceso a la que se conecta el usuario y por lo tanto es el propietario del servidor AAA y del equipo de servicio o NAS. Puede haber varios proveedores de servicio que colaboren entre sí. Si esto ocurre, y existen varios proveedores en colaboración para prestar un servicio,

el servidor contractual del usuario se denomina UHO (User Home Organization).

Es por esta secuencia que se hace difícil definir de forma general en el estándar AAA quién es el cliente y quién es el servidor. En la terminología que utiliza AAA, el cliente es aquel que envía paquetes con estructura AAA a un servidor AAA. Pero esto lo puede hacer el suplicante, así como el equipo NAS o el propio servidor, por lo que dependería del contexto el poder utilizar el término cliente. Para evitar confusiones hablaremos de: suplicante, NAS o autenticador y Servidor de Autenticación. En líneas generales en el proceso de configuración de RADIUS, se habla de clientes para definir a los NAS.

Las tres "A" proporcionan respuesta a las tres preguntas necesarias para acceder a un servicio que se presta a un solicitante:

- Autenticación: ¿Quién es el solicitante?
- Autorización: ¿A qué servicios le voy a permitir acceder?
- Arqueo: ¿Qué hace el cliente con los servicios que presto?

3.1.1.2 Autenticación.

La autenticación o "authentication" en inglés debe dar respuesta inequívoca a la pregunta: ¿Quién o que entidad pretende acceder a los servicios que presto?

"Autenticación" es la más importante de las tres "A", y en la que se basan no solo las dos restantes, sino todo el sistema completo. Si buscamos la palabra "autenticar", la definición que encontramos es:

(I) Autorizar o legalizar algo.

(II) Dar fe de la verdad de un hecho o documento con autoridad legal.

Los primeros sistemas basados en la autenticación utilizan una estructura simple de nombre de usuario y contraseña en texto en claro, basando todo este sistema en estos dos datos, que podrían ser interceptados o robados por otra persona. Con el tiempo este sistema se fue mejorando mediante el acceso a través de desafío (challenge) mediante el cual no hay intercambio de contraseñas durante el transporte de la autenticación, sino la encriptación de mensajes mediante una misma clave y un mismo algoritmo, evitando el transporte de la contraseña en sí. Posteriormente se implantaron otros métodos, como el acceso a través de equipos telefónicos con identificador (número de teléfono o numero de serie), el generador de contraseñas portátil (token), tarjetas de acceso, sistemas biométricos, etc.; hasta llegar en la actualidad a un sistema muy seguro basados en certificados (PKI).

En cualquier caso, lo importante es siempre la solicitud de la presentación de una prueba fehaciente de identidad. La autenticación no consiste únicamente en la identificación de personas físicas, sino también de equipos (computadores, PDA, teléfonos, etc.) que acceden a una red. Además se pueden autenticar otro tipo de características, como las profesiones, los estados civiles, etc. Si necesitáramos gestionar el acceso de policías a un sistema de consulta de identidad, podríamos basar la entrada en un certificado que se conceda únicamente desde la jefatura a estos profesionales, garantizando el acceso a este sistema sólo a los poseedores de este certificado y de las credenciales necesarias.

Cuando se accede a Internet a través de una línea xDSL, existe un proceso de autenticación durante el acceso, y aunque pensemos que este acceso utiliza simplemente un usuario y contraseña común para todos los clientes, en realidad se produce una autenticación física mediante la línea telefónica y puerto de acceso utilizados, por lo que este acceso queda relacionado a esos datos. Se puede también gestionar la autenticación mediante dirección MAC de la tarjeta de red (NIC) de un

router de entrada o de un equipo, aunque al ser ésta fácilmente falsificable, no se puede garantizar la seguridad por este método.

Durante el proceso de autenticación de un usuario para acceder a una red, no es el suplicante quien habla lenguaje AAA con el servidor de Autenticación, sino que el suplicante habla con el NAS o autenticador, y es éste quien traduce y encamina los paquetes hacia el servidor de autenticación. De esta manera no existe un camino abierto entre el suplicante y el servidor de autenticación, con lo que se garantiza bastante la seguridad del servidor de autenticación contra ataques directos, ya que un atacante tendría que estar en el interior de la infraestructura.

AAA es muy versátil, porque no provee de un único método de autenticación, sino que es considerado un protocolo extensible porque permite cualquier tipo de autenticación que se integre o adapte a su formato.

En la fase de autenticación se produce un mensaje inicial de solicitud de acceso desde el equipo NAS al servidor de autenticación en forma de:

- **Access – Request** (Solicitud de Acceso). El suplicante envía el nombre de usuario y la contraseña cifrada, si procede hacia el NAS. Éste envía entonces al servidor de autenticación el mensaje de Acces-Request solicitando además el puerto de acceso para el suplicante.

En algunos casos, como en las comunicaciones de dial up (marcado por modems) al solicitar el acceso a la red a través de un dispositivo PPP o similar, no se produce una solicitud de identidad al suplicante, ya que este dato es intrínsico al puerto de conexión (PAE Port Access Entity) que conoce algún dato como el Caller-Id (identificador de llamada) o dirección MAC del suplicante.

3.1.1.3 Autorización.

La autorización o "Authorization" contesta a la pregunta: ¿A que servicios voy a permitir acceder al solicitante, una vez autenticado? y está intrínsicamente unida a la autenticación. Otra definición aceptable explica que la autorización es el acto de determinar si podemos confiar un derecho a un solicitante.

Tras el traspaso de credenciales para la autenticación se produce la consulta del servidor de autenticación a la base de datos de usuarios, centrándose en la información del usuario que solicita acceso. En los registros relacionados con este usuario, se podrá consultar todo tipo de derechos y deberes relacionados con él. De esta manera el servidor conocerá detalles como: si el solicitante está autorizado a acceder a la red en este momento, si le debe asignar una dirección IP concreta, ai habrà que configurarle parámetros específicos para su conexión, si deberá concederle un ancho de banda determinado, si debe solicitar otro tipo de credenciales, o simplemente si deberá denegar su acceso. Todas estas reglas son definidas para cada usuario en concreto, para un grupo de usuarios o para todos los usuarios por defecto.

Si tras buscar las credenciales del usuario no se encontraran en ninguno de los directorios y bases de datos designados, se le negaría el acceso, siempre que no se haya definido algún perfil predeterminado para los usuarios no autenticados.

Existe multitud de reglas o campos configurables en los sistemas AAA. Estos campos o parámetros se conocen como atributos o AVP (Attribute Value Pair) en AAA. El sistema de diseño de este estándar es totalmente modularizable, ya que todo el intercambio de información entre los equipos y usuarios se basa en estos atributos. Unos atributos están definidos en los RFCs comunes y otros son específicos de cada fabricante de equipos. Todos estos atributos se almacenan en lo que se conoce como

diccionarios de atributos (dictionary); si son atributos estándar se almacenan en el diccionario estándar y si son atributos de fabricante en los diccionarios de fabricantes.

Por ejemplo: una contraseña de un usuario es un atributo, el tipo de autenticación que usa es un atributo, su dirección IP es otro atributo, cualquier parámetro es un atributo. Fabricantes como CISCO, 3COM, etc. disponen de sus diccionarios de atributos para configurar sus equipos NAS en respuesta a una solicitud concreta. Gran parte del intercambio de estos atributos se produce en la fase de autorización.

En esta fase el servidor de autenticación, tras conocer todos los atributos necesarios para el solicitante, responderá a su solicitud de autenticación mediante un mensaje estándar enviado al equipo NAS para permitir, denegar o volver a preguntar sobre su acceso:

- **Access – Accept** (Aceptación del Acceso). El fin mismo de la solicitud de autenticación es la aceptación del acceso. Si el mecanismo de acceso ha sido correcto, se le envía este mensaje al NAS con los atributos necesarios para regular el acceso del suplicante de forma personalizada.
- **Access – Reject** (Denegación del acceso). Debido a las circunstancias que puedan no permitir el acceso de un usuario, como por ejemplo: usuario inexistente, contraseña incorrecta, derechos revocados, etc. se le deniega de forma incondicional el acceso a este solicitante. Se puede incluir en este mensaje el motivo de la denegación del servicio. El NAS que recibe este mensaje no permite el acceso al suplicante, enviando un mensaje (si se incluye) al solicitante o suplicante.
- **Access – Challenge** (Solicitud de información adicional para el acceso). Se le solicita al solicitante o suplicante información adicional, como contraclave, tarjeta de acceso, PIN de acceso, o cualquier otro método alternativo o

adicional de acceso. El NAS trasmite la solicitud al suplicante. Este mensaje puede ser intercambiado en múltiples ocasiones dependiendo del tipo de autenticación y de la información que se precisa.

Tras este intercambio de mensajes el suplicante esta autorizado o no a utilizar los recursos de la red, a la cual desea acceder. Si lo estuviera estaría regulado por los derechos u obligaciones asignados durante este proceso, como duración máxima de la conexión, máximo flujo de datos, VLANs de acceso, etc.

3.1.1.4 Contabilidad

Una vez realizado el proceso de autorización se produce la fase de arqueo o "Accounting". Ésta es iniciada por el autenticador o NAS tras autorizar el acceso al suplicante. El arqueo es la fase estadística y de recolección de datos sobre la conexión. Se produce de forma de contadores o logs de conexión y se suelen almacenar en bases de datos SQL relacionadas con el usuario o en archivos tipo log. Estos datos correctamente manejados y gestionados nos permiten tomar decisiones en cuanto al uso de los recaros por parte de los usuarios, con el fin de denegar conexiones, cambiar los anchos de banda mediante QoS (Calidad de Servicio), impedir descargas, etc. La fase de arqueo esta limitada por la capacidad del equipo NAS de registrar información de sesiones.

La contabilidad de la conexión permite a los buenos administradores mediante estadísticas gestionar la futura demanda de crecimiento de sus sistemas para planificar sus ampliaciones. También como debe suceder en los sistemas de seguridad o IDS se deberían generar avisos por intentos reiterados o denegados de conexiones infructuosas para tomar decisiones basadas en la seguridad, si bien la mayor parte de los equipos y servidores no proveen este tipo de información.

Durante la fase de arqueo se producen los siguientes mensajes:

- **Accounting – Request [Start]** (Solicitud de inicio de arqueo). Es una solicitud de inicio enviada desde el equipo NAS al servidor, para indicar que ha comenzado la fase de arqueo, y se comienzan a registrar los datos de la sesión del usuario.
- **Accounting – Response [Start]** (Respuesta de asentimiento al inicio del arqueo). El servidor de autenticación responde a la solicitud inicial, registrando la información de inicio y enviando este paquete al NAS para mostrar su conformidad.
- **Accounting - Request [Stop]** (Solicitud de final de arqueo). El NAS comprueba la desconexión del usuario y envía al servidor un mensaje de final de la fase de arqueo con los siguientes datos de la sesión del usuario:

Delay time (tiempo de intento de envío de este mensaje)
Input octets (número de bytes recibidos por el usuario)
Output octets (número de bytes enviados por el usuario)
Session time (duración en segundos de la sesión del usuario)
Input packets (número de paquetes recibidos por el usuario)
Out packets (número de paquetes enviados por el usuario)
Reason (motivo de la desconexión de la sesión del usuario)

- **Accounting – Response [Stop]** (Respuesta de asentimiento al final de arqueo). El servidor tras almacenar la información anterior, envía el NAS su conformidad al final de la fase de arqueo, admitiendo haber recibido correctamente toda la información de la sesión.

RADIUS no es un protocolo que mantenga un control fiable de la recepción de paquetes por parte del servidor, (aunque si se contempla retrasmisiones), por lo que se podría llegar a peder la información de accounting enviada al servidor a la finalización de su sesión, con el perjuicio económico que tendría

sobre un operador que facture como consumo. Para evitar este tipo de problemas se crearon en RADIUS unas nuevas extensiones llamadas “Interim accounting updates” que fuerzan el traspaso de la información de accountig de una sesión activa cada n segundos, minimizando así el impacto económico causado por la perdida de información de arqueo. Uno de los atributos nuevos incluidos es:

Acct-Interim-Interval

2.1.1.5 Auditoria, la cuarta “A”

Las RFC de AAA o de RADIUS no contemplan el control o registro de los intentos fallidos de autenticación o cualquier otra información relacionada con la seguridad, si bien cualquier sistema moderno debe permitir el registro de estos intentos para mantener un registro completo de los intentos de conexión infructuosa o de otros datos relevantes de seguridad. Los servidores de autenticación registran durante la fase de arqueo toda la información relacionada con el consumo de recursos o tarificación, pero no suele controlar esa información relacionada con la seguridad, por eso coloquialmente se suele definir el uso de esta tecnología en los sistemas de autenticación como AAAA.

Un administrador eficiente podrá y deberá comprobar diariamente estos logs para detectar intentos reiterados de intrusión o problemas de configuración o funcionamiento. Un sistema completo de auditoria debería registrar los siguientes tipos de información sobre la autenticación de usuarios:

- Intentos de acceso con resultados Accept y Reject.
- Intentos de uso de certificados revocados.
- Existencia de autenticadores de mensajes incorrectos

- Solicitudes de acceso invalidas por pertenecer a clientes (NAS u otros servidores RADIUS) no autorizados.
- Paquetes no RADIUS o paquetes RADIUS mal construidos, con direcciones MAC incorrectos, etc.
- Entradas autorizadas con credenciales denunciadas como robadas o de usuarios dados de baja.
- Cambios en los archivos de configuración.

Este tipo de registros se debe revisar concienzuda y diariamente, como los logs de un IDS, ya que si no se hace, la utilidad de estos es indiscutible. En algunos sistemas operativos, como Windows o como Linux (mediante librerías como AppArmor oSELinux), se puede auditar también el acceso o modificación de los archivos de configuración o registro.

3.1.2 Marco de Autorización AAA

Todo el modelo AAA queda perfectamente explicado en los siguientes documentos de la IETF:

- RFC 2903 - Arquitectura genérica AAA.
- RFC 2905 – Marco de autorización AAA.
- RFC 2905 – Ejemplos de aplicación de autorización AAA.
- RFC 2906 – Requerimientos para la autorización AAA.

Estos documentos son la mejor base para explicar en su totalidad la infraestructura de los sistemas AAA. Específicamente el documento RFC 2905 explica en profundidad el marco de desarrollo del estándar y las relaciones de confianza entre los diferentes componentes de la infraestructura.

Basándonos en los tipos de relaciones que se pueden establecer entre los componentes de una relación de confianza en AAA, podemos distinguir tres tipos de relaciones de autorización o secuencias de autorización:

- Secuencia de agente o **Agent Sequence**: en esta secuencia de autorización el usuario solicita un servicio al servidor AAA, que decide si prestar el servicio al usuario y notifica al equipo de servicio que se preste el servicio, si así lo decide. El equipo de servicio notifica al servidor AAA si se produce la prestación del servicio.

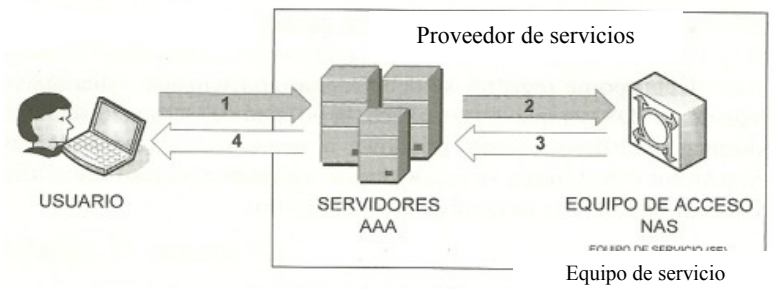

Figura 3.1. Secuencia de agente (Agent).
Fuente: Hansen, Fernandez Yago, 2008

Ejemplo: Un usuario solicita un acceso de 10 Mb/s de ancho de banda al servidor. El servidor solicita al router una conexión de 10 Mb/s para el usuario y el router, si la soporta, se la concede y notifica al servidor la prestación del servicio de acceso.

- Secuencia de tiro o Pull Sequence: es la secuencia clásica de protocolos de marcación o de Servidores de Autenticación como RADIUS. El usuario solicita el acceso al equipo (NAS), y éste en comunicación interna con el Servidor de Autenticación tramita la solicitud. Si el servidor la considera

correcta, éste se la comunica al NAS, que abrirá el canal y notificará a un servidor.

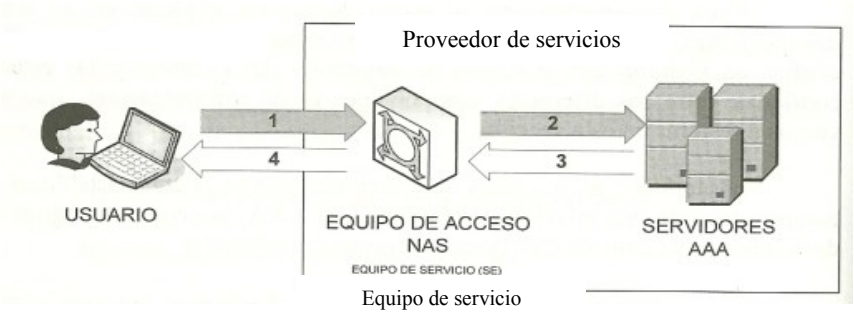

Figura 3.2. Secuencia de tiro (Pull).
Fuente: Hansen, Fernandez Yago, 2008

Ejemplo: un usuario solicita un acceso a su proveedor de ADSL local a través de sus enrutadores de acceso. Los enrutadores envían las credenciales del usuario, además de los datos de identificador de llamante y otros. El servidor de autenticación (si el cliente tiene concentrado el servicio) permite el acceso y notifica al router que preste el servicio. El router que actúa como NAS, notifica la prestación al servidor de Autenticación.

- Secuencia de empuje o **Push Sequence:** en este caso, el usuario realiza una solicitud de servicio al Servidor AAA en forma de ticket de servicio o certificado. Este ticket regula el servicio que prestará, mediante el mismo tiempo (tiempo de prestación, características, etc.). En el siguiente paso, el usuario solo debe presentar el ticket al equipo NAS, que conocerá por sus características, y prestará el servicio al usuario. No se produce una comunicación directa entre el equipo prestador del servicio o NAS y el servidor de autenticación.

Proveedor de servicios Proveedor de servicios

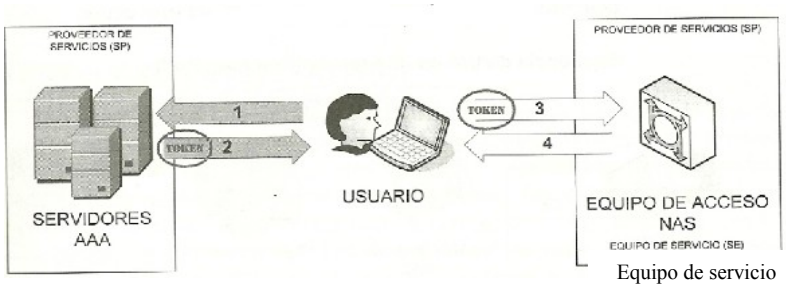

Figura 3.3. Secuencia de empuje (Push).
Fuente: Hansen, Fernandez Yago, 2008

Ejemplo: un usuario contacta con el servidor AAA y solicita un acceso por tiempo limitado (1 semana) con un ancho de banda determinado (10 Mb/s). El servidor le concede su solicitud y le entrega un certificado con esas características. Cuando desea conectarse, para comenzar a recibir el servicio, el usuario contacta con el equipo prestador del servicio y le entrega el certificado. El NAS conoce el certificado y sus características y comienza a prestar de forma automática el servicio y a registrar el uso del certificado de usuario hasta su finalización.

Estas secuencias y relaciones entre componentes se pueden complicar mucho más si partimos de una base de subcontratación de prestación de servicios entre varios proveedores, permitiendo incluso la itinerancia (roaming) del usuario entre diferentes proveedores. En este caso, no existe un solo equipo NAS, un solo servidor AAA, aunque sí un solo usuario.

- Secuencia de tiro de itinerancia o **Roaming Pull Sequence**: este tipo de secuencia es similar a la secuencia de tiro, pero contempla dos proveedores de servicio.El usuario puede contratar su acceso a través de otros proveedores (se define en AAA como UHO o User Home Provider) o a través del propio propietario. Si lo hace a traves de otro proveedor,(a través de sus equipos

NAS y servidores de acceso en forma de Proxy) la solicitud a los servidores AAA del proveedor del usuario, que autorizan a los equipos de prestación o NAS a prestar finalmente el servicio contratado por el usuario. El propietario tendrá algún tipo de acuerdo de facturación por servicios con el proveedor.

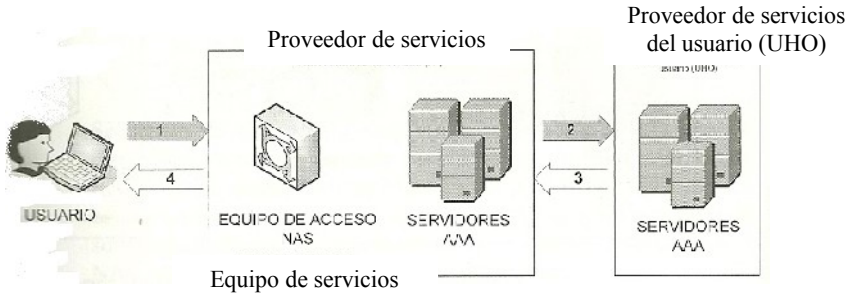

Figura 3.4. Secuencia de tiro en itinerancia (Roaming Pull).
Fuente: Hansen, Fernandez Yago, 2008

- Secuencia de agente de itinerancia o **Roaming Agent Sequence**: el usuario solicita el acceso directamente al servidor AAA del propietario del acceso, que pasa en forma de Proxy su solicitud al proveedor local (UHO) del usuario. Finalmente los equipos NAS del propietario prestan el servicio qu ha sido solicitado al proveedor local.
- Secuencia de empuje de itinerancia o **Roaming Push Sequence**. El usuario solicita un ticket (token) o certificado a su proveedor local (UHO). Una vez concedido ese ticket, se le envía al usuario solicitante. El usuario utiliza su ticket, entregándoselo al equipo o NAS del proveedor de acceso, que le concederá el acceso.

3.1.3 Otros Protocolos AAA.

Como veíamos con anterioridad, RADIUS es el mayor conocido de la serie de protocolos que cumplen con los estándares AAA, si bien, aunque fue el primero no será el ultimo ni el principal. El camino de AAA ha seguido un tiempo

paralelo al de RADIUS, pero AAA ha despegado para buscar las mejores en todos los mecanismos relacionados con la autenticación, autorización y arqueo. Para ello ha estudiado los puntos débiles de RADIUS, así como las necesidades de mejora, escribiendo una serie de normas para la construcción de un estándar mejor. Durante todo este camino, otros protocolos han ido apareciendo de forma paralela o derivada. De entre ellos destacan los que referenciamos a continuación.

3.1.3.1 TACACS, TACACS+

Durante los años de la gran expansión de las redes ARPANET y MILNET, se crearon los protocolos TAC (Terminal Access Controller). Estos protocolos eran utilizados en la red de Milnet para permitir el acceso de los equipos remotos mediante MÓDEM, gestionando su autenticación y posterior acceso a la red. Este primer protocolo TAC, utilizado por Milnet en sus nodos de acceso a la red, como YUMA-TAC se pasó a llamar TACACS (Access Control System). TACACS permitió que las credenciales de usuario no se almacenaran en el equipo TAC y se pudiera descentralizar las bases de datos de credenciales hacia equipos que la almacenaban. El TACACS original fue desarrollado por el Ministerio de Defensa de EE.UU., y la empresa privada BBN Planet Corp. El diseño original de este protocolo consistía en un esquema simple de usuario y contraseña. TACACS se basó en UNIX y al servidor se le llama TACACSSD o TACACS daemon y utiliza como puertos de autenticación el 49 tanto en TCP como en UDP indistintamente. TACACS no incorpora seguridad ni encriptación en sus transmisiones, con lo que simplemente interceptando el tráfico se puede recopilar todas las credenciales. Es un protocolo modelo cliente-servidor, donde el NAS envía una solicitud al servidor y éste responde afirmativamente o negativamente.

En 1990, CISCO adoptó este protocolo pasándose a llamar XTACACS e incorporando el arqueo o contabilidad y la auditoría. Posteriormente desarrolló TACACS+, realizando importantes aportaciones y mejoras en el mismo pero separándolo de sus antecesores, de tal manera que fuera incompatible. CISCO lo convirtió en un protocolo extensible aceptando plugins de autenticación: como tarjeta inteligente y otros sistemas basados en challege o desafío, además de añadir encriptación en las comunicaciones entre cliente y servidor. Se modularizó, basándose en AAA. TACACS+ es un protocolo de segunda generación basado en AAA, y que habita principalmente en equipos de CISCO, ya que es un protocolo propietario de CISCO y no esta abierto a otros fabricantes. Algunas características de TACACS+ son:

- TACACS+ usa TCP como protocolo de transporte.
- TACACS+ encripta el cuerpo entero del mensaje.
- TACACS+ separa el proceso de autenticación, permitiendo utilizar sólo la autorización y el accounting de forma independiente. De esa manera puede utilizar otros protocolos de autenticación como Kerberos.
- TACACS+ da soporte a los siguientes protocolos: Netbios, x25, Appletalk, Novell NASI.
- TACACS+ controla la configuración de seguridad del acceso a routers.

Los RFC que tratan sobre TACACS son el RFC 1492 de 1993 (“Un protocolo de control de acceso, a veces llamado TACACS”), RFC 927 (“Opción de Telnet para TACACS”) y RFC 2975 de 2000 (“Introducción a la gestión de contabilidad o arqueo”).

3.1.3.2 Diameter.

Tras la creación del grupo de trabajo en la IETF en 1995 dedicado a crear el RFC correspondiente a RADIUS, se pensó en crear un nuevo código limpio y mejorado de RADIUS que se llamaría RADIUS v.2. Pero la IETF no permitió esta maniobra, debido a que RADIUS todavía no había sido ratificado en una RFC funcional y corregida, y no se debía crear otro estándar hasta que el primero hubiera sido publicado. Por ello, el nombre que recibió este nuevo estándar no pudo ser RADIUS v2 y se optó por Diameter (dos veces el radio o como definieron sus creadores "twice as good as RADIUS" o "dos veces tan bueno como RADIUS"). Diameter fue diseñado en 1996 por Pat Calhoun de la compañía Black Storm Networks.

El RFC que regula Diameter paso a ser el RFC-2588 ("Diameter Base Protocol"), y posteriormente se han ido creando diferentes RFC que regulan su aplicación en MobileIP, EAP, etc.

Según (Hansen, Fernandez Yago, 2008). Diameter es un protocolo de segunda generación, cien por cien basado en AAA, que como posible sucesor de RADIUS pretendía mejorar todas sus carencias puntos débiles. Unas de las premisas más importantes en su diseño fue que tenía que ser compatible con RADIUS ("legacy compatible") para que pudiera asumir todas las instalaciones en forma de migración. Por eso cada vez que se modifica un RFC relacionado con RADIUS es necesario modificar esas nuevas características en Diameter para seguir permitiendo mantener ese principio de compatibilidad entre ambos sistemas. Algunas de las mejoras que incorpora son: la sustitución de UDP por TCP y SCTP mejorando el control de errores en la transmisión, el uso de túneles mediante IPSec o TLS, y su cambio de modelo hacia peer to peer en vez de cliente-servidor, con lo que un servidor puede realizar consultas hacia un cliente, permitiendo sesiones dinámicas.

Diameter mejora RADIUS en muchos aspectos como la gestión de las comunicaciones mediante SCTP, previendo de una forma muy adecuada el timeout

en los envíos de mensaje y en la búsqueda de rutas alternativas hacia el servidor o servidores. Diameter firma los mensajes mediante un código de tiempo, que impide duplicidades en la recepción de respuestas simultáneas, además de ser usar cifrado basado en certificados y firma digital. Diameter se apoya en un modulo criptográfico llamado CMS (Criptographic Message Syntax) integrado en su plataforma, que se encarga del cifrado de todos los mensajes. Diameter da soporte al nuevo estándar de gestión de NAS llamado NASREQ.

Otro aspecto que mejora Diameter es el de la comunicación entre servidores de autenticación (Diameter), permitiendo definir cadenas de proxy para los envíos de mensajes e implantando mejores modelos de confianza que RADIUS. Todos estos ingredientes de Diameter es la de roaming que permite crear grandes redes distribuídas.

Con los años RADIUS fue creciendo y mejorando, con lo que muchas de las motivaciones que instaron a la creación de Diameter se sumieron en lo innecesario, por eso RADIUS ha seguido manteniéndose como un gran estándar en la actualidad.

Sin embargo Diameter continúa su proceso de expansión y comienza a implantarse en sectores como la telefonía móvil o la VoIP debido a todos esos ingredientes que incorpora, que lo convierten en un producto ideal para este tipo de instalaciones de gran nivel.

3.2 RADIUS, EAP, Wi-Fi.

3.2.1 Introducción a RADIUS.

RADIUS son las siglas de Remote Authentication Dial-up Server, que significa Servidor de Autenticación Remota para Sistemas de marcado Telefónico a Redes. Este nombre proviene de sus comienzos, donde su único uso era el acceso a redes a través de MÓDEM, pero actualmente su funcionalidad es mucho más amplia.

El motivo por el cual RADIUS es el protocolo AAA hegemónico en la actualidad no es solamente porque haya sido el primero, ni porque haya tenido tanto marketing para alcanzar su globalización, sino porque ha ido creciendo y mejorando desde sus comienzos hasta el día de hoy. A pesar de algunas de sus limitaciones, ha ido adoptando una serie de mejoras que le han llegado a permitir a gestionar desde pequeñas redes seguras de pequeñas y medianas empresas hasta redes de alto nivel.

3.2.1.1 Orígenes.

RADIUS es un producto creado para satisfacer una necesidad de mercado durante los años 90. En aquel momento, debido al empuje de redes de cada vez mayor tamaño, se hacia muy difícil el control de acceso a éstas. Las universidades creaban redes de intercambio de información para los investigadores, profesores y estudiantes. Estas redes de acceso más o menos público fueron las precursoras de la actual Internet. Algunas de ellas incluso estaban ya basadas en el protocolo IP y otras utilizaban protocolos propietarios. Esta maraña de redes universitarias necesitaba ir interconectándose, por lo que tenían que ir unificando criterios y protocolos para lograrlo. Una de las principales dificultades consistía en gestionar el acceso de los usuarios, por lo que cada fabricante de sistemas de acceso remoto telefónico (dial-up) utilizaba sus sistemas propietarios de control de acceso. Cuando un usuario necesitaba entrar en varias de estas redes, había que administrar un perfil diferente en cada una de ellas para ese usuario. Esto hacia que la administración de estos sistemas fuera muy compleja y tediosa, lo que llevo a una empresa llamada Merit, que gestionaba lo accesos a varias de estas redes en California, a buscar una solución para desarrollar un mecanismo de autenticación común para todas las pilas de modems de

acceso que tenía distribuída. Para ello, Merit lanzó en 1991 una RFI (Request for Information) a las principales empresas de networking que existían en su segmento. Una de las empresas que respondió a esa solicitud fue Livingston Enterprises (después Lucent). Steve Willens de Livingston respondió con una clara descripción de lo que posteriormente paso a llamarse RADIUS.

Tras la incorporación de este desarrollo a los servidores de acceso remoto de Livingston (Portmaster Servers), su funcionamiento fue ejemplar y Merit continuo mejorándolo, incorporando nuevas funciones como un sistema Proxy y otro de autenticación distribuida. De esa manera se creó el servidor RADIUS de Merit, cuyo código inicial había sido totalmente reescrito por el equipo de Merit. Tras un tiempo se convirtió en el servidor RADIUS RAD-Series de la empresa Interlink derivada de Merit, que sigue desarrollando su servidor a día de hoy.

Los pasos que surgieron a continuación fueron los que permitieron la expansión que tuvo lugar de este servidor RADIUS, y que fue necesaria para evitar que quedara relegado a otro software propietario. En 1992 se formó en la IETF un grupo de trabajo llamado NASREQ (encargado de gestionar los requerimientos de los equipos de acceso a redes o NAS) para buscar un estándar que recogiera los requisitos técnicos y características necesarias para la futura gestión de equipos NAS. En la mesa se sentaron componentes de Merit (Al Rubens y John Vollbrecht) entre otros, para discutir sobre las posibles soluciones de futuro que se necesitaban. En 1994 Livingston (Steve Willens y Carl Rigney) cedió el código fuente de RADIUS a este grupo de trabajo, abriendo de esta manera RADIUS a todos los fabricantes que deseasen incorporar o mejorar este código. De esa manera era mucho más fácil mejorar el servidor, ya que si no estuviera disponible ese código cada empresa que quisiera hacer mejoras debería comenzar de nuevo, volviendo a reprogramar todo el trabajo ya realizado. NASREQ sigue trabajando en conjunción con Diameter, funcionando como una puerta de enlace entre los dos protocolos.

Debido a la gran demanda del mercado, muchos fabricantes fueron incorporando RADIUS a sus productos de Hardware y Software por lo que su extensión fue increíble, casi cualquier equipo debe soportarlo. Mientras tanto, se seguía debatiendo en el grupo NASREQ si RADIUS era la mejor solución o no, y si cumplía todos los requerimientos y la seguridad necesaria. Debido a la presión de muchos fabricantes en 1995 se crea un grupo de trabajo para estudiar y documentar RADIUS a fin de limpiar el código de todos los procesos a los que se le había sumido. En 1997 aparece el primer RFC (Request for Comments) oficial de RADIUS (RFC 2039) que fue posteriormente sustituido por el (RFC 2865) en el año 2002 que prevalece hasta hoy. En 2007 se publico el texto definitivo del RFC 5080, un documento que trata algunos de los problemas de implementación de RADIUS y sugiere algunas soluciones al respecto.

3.2.1.2 Descripción del protocolo.

RADIUS es un servicio o daemon que se ejecuta en una de las múltiples plataformas que permite (Unix, GNU/Linux, Windows, Solaris, etc.) y que permanece de forma pasiva a la escucha de autenticación hasta que estas se producen. Para ello utiliza el protocolo UDP (y no TCP o SCTP) que permitiría mayor control y seguridad en el transporte y permanece a la escucha en los puertos 1812 o 1645 para la autenticación y 1813 o 1646 para el arqueo. En un principio se utilizaban los puertos 1645 y 1646 para RADIUS, pero tras la publicación de la RFC 2865 se utilizan por acuerdo 1812 y 1813 debido a que el 1645 estaba siendo utilizado por otro servicio denominado “datametrics”. Algunos servidores como FreeRadius utilizan el puerto UDP 1814 para la escucha de respuestas Proxy RADIUS de otros servidores, pero esto no esta contemplado en ningún RFC, y esta en conflicto con el puerto utilizado por TDP Suite (Telocator Data Protocol), protocolo para comunicaciones para localizadores o buscapersonas.

RADIUS esta basado en un modelo cliente-servidor, ya que RADIUS escucha y espera de forma pasiva las solicitudes de sus clientes o NAS, a las que responderá de forma inmediata. En este modelo el cliente es el responsable del envío y de la correcta recepción de las solicitudes de acceso, y es el servidor RADIUS el responsable de verificar las credenciales del usuario y de ser correctas, de enviar al NAS los parámetros de conexión necesarios para prestar el servicio.

El motivo por el cual RADIUS justifica el uso de UDP sobre TCP en su RFC es por el aprovechamiento de la normativa del protocolo UDP, que mantiene una copia del paquete de solicitud sobre la capa de transporte a fin de poder recuperarlo para reenviarlo, si fuera necesario, a otro servidor RADIUS si el primero no estuviera disponible. De esa manera se simplifica el diseño del protocolo, evitando tener que hacerse cargo del control de llegada de esos paquetes a su destino. Para aprovechar esta simplicidad se utiliza las características de UDP de ser "stateless" o "connectionless". Las retransmisiones se pueden hacer más rápidamente hacia otros servidores, ya que el puerto no quedará colapsado por el control de la conexión, evitándose las esperas necesarias en el protocolo TCP.

El servidor RADIUS puede actuar como servidor proxy, elevando las solicitudes de un cliente hacia otro servidor de autenticación RADIUS, o de otro tipo.

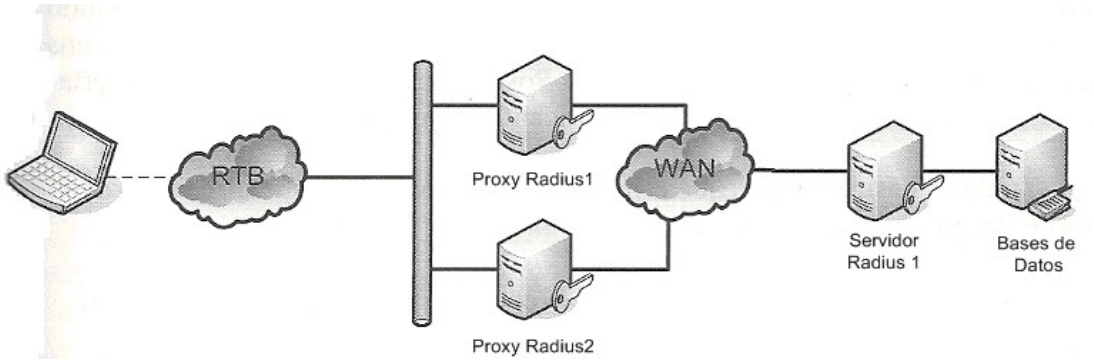

Figura 3.5. Sistema de Proxy RADIUS.
Fuente: Hansen, Fernandez Yago, 2008

RADIUS dispone de una muy extensa variedad de módulos de autenticación, encargados de completar un proceso de autenticación con todo lo que ello conlleva. En una comunicación RADIUS nunca se envían las contraseñas en texto claro, incluso en sus versiones más antiguas se utilizaba un sistema de cifrado, aunque este sistema primitivo ha quedado ya obsoleto. Estos módulos de autenticación se han ido desarrollando a medida que el mercado ha ido demandando nuevos sistemas más seguros y fiables para la autenticación. La idea predominante es la de sustituir los métodos que se van quedando obsoletos por vulnerabilidades o problemas de seguridad por otros más actuales que ofrezcan más confianza y más probabilidades de servicio.

RADIUS es un protocolo extensible, por lo que permite la introducción mediante su sistema de atributos o variables definibles (AVP) de cualquier adaptación a cualquier nuevo equipo de cualquier fabricante. Este sistema se funcionamiento mediante atributos es uno de los principales pilares de este protocolo, ya que toda su estructura modular se basa en ellos como veremos mas adelante.

3.2.1.3 Especificaciones de RADIUS.

En esta sección, se pretende explicar cuales son las principales especificaciones que hay que tener en cuenta sobre RADIUS a la hora de decidir su adquisición.

¿Qué especificaciones mínimas debe ofrecer un servidor RADIUS propicio para la aplicación a la que va a ir destinado?

- Cumplir la función para la cual se va adquirir.

- Incluir todas las tecnologías necesarias para que pueda cubrir las necesidades del usuario final de la autenticación, a través de cualquier sistema operativo y/o plataforma de forma segura.
- Soportar o ser soportado por todas las plataformas de hardware que utilicemos en la infraestructura de red, como equipos de electrónica de Red, NAS, Plataformas AAA, ADSL, GSM, Wi-Fi, Wi-Max, enrutadores, etc.
- Soportar el sistema o sistemas de bases de datos o servicio de directorio que hayamos elegido para la gestión de usuario y de arqueo de cuentas.
- Disponer de la arquitectura adecuada para la instalación en la plataforma servidora elegida.
- Disponer de las librerías de programación adecuadas para la personalización de sistemas como PHP, Java, Pearl, Python, etc.
- Ser fácilmente configurable y administrable.
- Cumplir unos niveles adecuados de seguridad en su parte de cliente y de proveedor de seguridad.
- Fidelidad a los estándares y RFC, que los regulan.
- Ser transportable y migrables a otros entornos.
- Ser abierto con otros sistemas, a la hora de intercambio de información.
- Si fuera necesario, disponer de un sistema de gestión centralizado de servidores.
- Si precisamos de ellos, disponer de la redundancia y escalabilidad necesarias para una gran instalación. Disponer de control de carga y de calidad de servicio.
- Proveer de sistemas de control de sesiones de usuarios activas o cambios dinámicos en la autorización.
- Ser preciso y concienzudo en el registro de información sobre sesiones para ofrecer estadísticas y registros adecuados. Es necesario en algunos casos que sea capaz de manejar SNMP o información syslog.

- Incluir técnicas de troubleshooting y depuración para localizar fácilmente la causa de los problemas que se detecten.
- Posibilidad de enlazar el accounting contra sistemas de tarificación si se precisa de ellos.
- Ser un producto actualizable y adaptable a los cambios que se produzcan, tanto en el cliente como en el mercado.
- Ofrecer garantías de servicio. Ofrecer soporte técnico adecuado a las necesidades

Todas estas características, dependiendo del tipo de implementación que necesitaremos, son las que definen a RADIUS o a cualquier servidor AAA.

3.2.1.4 Multiplataforma (GNU-Linux, Windows, Solaris, etc.).

Como es habitual en este tipo de protocolos clásicos, fueron desarrollados en sistemas basados en Unix y algunos posteriormente trasladados o migrados a sistemas basados en Windows. Por tanto los primeros servidores basados en RADIUS fueron compilados para Unix y funcionan perfectamente en GNU/Linux o sistemas similares.

Con el paso del tiempo, de forma inexplicable muchos de estos servidores han ido migrando hacia Windows, encontrándose en este sistema hoy por hoy a los fabricantes de mayor renombre, aunque muchos de ellos siguen manteniendo versiones en varias plataformas.

Otra solución para algunas organizaciones consiste en la adquisición de appliances (combinación de hardware y software en forma de equipos electrónicos), las cuales podemos gestionar desde consolas de administración y son transparentes al sistema operativo que llevan integrado.

En las plataformas basadas en Unix como GNU/Linux podemos encontrar soluciones RADIUS de código abierto. El problema que presentan estas implantaciones de código abierto como FreeRADIUS para algunos administradores es la falta de comodidad en la administración por medio de consolas graficas o GUI. Muchos administradores actuales se han formado en cómodos sistemas gráficos de ventanas y eluden cualquier sistema de administración basado en la consola de texto. Pero el resto de características que incorporan y la fidelidad a todos los RFCs y a las nuevas aportaciones son formidables.

Independientemente de si el software elegido ha sido desarrollado por una organización no lucrativa o por una firma comercial, esta la elección de la plataforma o sistemas operativo que la adoptara. Un servidor RADIUS debe trabajar sobre una plataforma potente y sobre un sistema operativo ligero como sea posible, para ceder los recursos al servicio. También dependerá de si estamos instalando un servidor de autenticación para diez, cien, mil o millones de usuarios, pero GNU/Linux utiliza mucho menos recursos y deja menos puertas abiertas que un servidor base de Windows.

3.2.2 Métodos de Autenticación.

Los métodos de autenticación son paquetes de software o módulos de software sobre los que se basa el proceso de autenticación de usuario una plataforma de RADIUS. Estos módulos son realmente complejas cajas matemáticas encargadas de realizar el cifrado, descifrado y empaquetado de todos los procesos complejos de autenticación. Desde el método nativo de RADIUS que es el PAP hasta los más actuales como algunos tipos nuevos de EAP, la evolución en cuanto a seguridad ha sido notable. Cuando RADIUS recibe una solicitud de acceso, va pasándola por cada uno de los módulos de autenticación que tenga activado en su configuración, hasta que algunos de esos módulos reconozcan sus algoritmos o las credenciales del usuario y se encargue de validar la autenticación.

- **PAP** (Password Authentication Protocol o protocolo de autenticación mediante contraseña). Es el sistema más sencillo de autenticación, y por lo tanto el más vulnerable. Se basa simplemente en la transmisión del nombre de usuario y contraseña almacenado en texto en claro o ASCII. Por si alguien no lo ha notado, no se debe usar si no es enviado por túnel.

- **CHAP** (Challenger Handshake Authenticaction Protocol o protocolo de desafío mutuo). Se le supuso como una actualización a PAP, para incrementar la seguridad de este protocolo. Es un método del tipo de secreto compartido, ya que ambos sistemas comparten el conocimiento de una contraseña o hash. El suplicante o usuario conoce su contraseña en texto en claro y el servidor tiene también que conocer la contraseña. En el momento de la autenticación el servidor envía una frase aleatoria (desafío) para que el suplicante la pase junto con su contraseña por una función MD5 y se la reenvíe. Al recibir el servidor, que ya conoce su valor calculado, la compara con su resultado recibido y, si es correcto, permite la entrada del suplicante a la red. Ese desafío se puede repetir en varias ocasiones durante la sesión del usuario, pero con frases de desafío diferentes.

- **MS-CHAPv1**. Es la primera versión del protocolo CHAP basado en desafío por el sistema Microsoft. Ya no esta incluída en Windows Vista. La mejora de MS-CHAP sobre CHAP es que ni el servidor ni el cliente deben almacenar la contraseña de usuario en texto claro, ya que tanto al procesar el desafío por parte del cliente como parte del servidor, ambos utilizan el valor hash de la contraseña y no la contraseña en sí. Aunque hoy, romper una contraseña calculada mediante algoritmo MD5, no es demasiado difícil.
- **MS-CHAPv2.** Es la versión actual de CHAP de Microsoft, que tiene soporte en todos sus SO desde Windows 2000 y que es incompatible con la

v1.Permite soporte para cambios de contraseña y mensajes de respuesta con estados.

- **Unix**. Se pueden utilizar simplemente los nombres de usuarios y contraseñas existentes en un sistema Unix/Linux que se encuentran almacenados en el directorio *etc* de Unixen el archivo passwd o mediante la función shadow.

- **HTTP Digest**. Es también un protocolo de autenticación por desafío para clientes de servidores Web con autenticación RADIUS; para evitar los ataques de repetición usa también frases precomputadas únicas. También utiliza MD5 como algoritmo, aunque maneja otros como SHA-1.

Métodos EAP.

- **EAP-MD5.** Es un método simple e inseguro de autenticación que utiliza el algoritmo MD5 para calcular el hash de una contraseña. Este protocolo es fácilmente violable, ya que todo el proceso circula en texto claro. Se puede capturar el hash y forzarlo off-line, por lo que es vulnerable si no se utiliza algún tipo de envío por túnel de las comunicaciones.

- **EAP-OTC**. (One Time Password). Es un método similar a MD5 pero basado en un sistema portátil de generación de claves instantáneas. Las opciones capaces de generar la contraseña de un sólo uso son programas de software, llaveros con algoritmos programados, PDA con software apropiado, etc.

- **EAP-GTC**. Generic Token Card. Es un sistema simple para el uso de algunas tarjetas smatcard (criptográficas) sobre protocolo EAP. Requiere que el usuario teclee su PIN para finalizar la autenticación. También se

utiliza este método con dispositivos tipo token mediante interfaz USB, serial o paralelo.

- **EAP-MS-CHAP.** Es la aplicación de la versión 1 del protocolo CHAP de Microsoft transportado por EAP, que es la versión Microsoft del sistema de desafío o Challenger de contraseña. Es vulnerable si no lleva cifrado o por vía túnel de las comunicaciones.

- **EAP-MS-CHAPv2.** Versión 2 del protocolo MS-CHAP. Tampoco es muy recomendable usarlo sin túnel.

- **EAP-SIM.** Versión de EAP para autenticación de los equipos de telefonía móvil GSM mediante tarjeta SIM, aunque también se puede utilizar como método de autenticación en cualquier tipo de equipo mediante un lector de tarjetas SIM.

- **EAP-AKA.** Authenticaction and Key Agreement (Autenticación y aceptación de clave). Utilizada en servicios UMTS (Universal Mobile Telecommunications System), se basa en el uso de la criptografía simétrica para canalizar la autenticación y la distribución de claves de sesión. Proporciona privacidad de usuario y mecanismos de reconexión rápida.

Métodos de EAP propietarios de CISCO.

- **EAP –LEAP.** Protocolo propietario de CISCO que es muy similar a EAP-MD5 pero utilizando un sistema de rotación dinámica de claves. Es otro método que debe ya abandonar por las vulnerabilidades que ofrece, demostrado por el autor del programa ASLEAP que obtiene las claves LEAP de forma muy sencilla y rápida.

- **EAP-FAST**. Protocolo propietario de CISCO que pretende sustituir a LEAP por sus vulnerabilidades, tutelando el transporte de la autenticación sin el uso de certificados mediante el sistema PAC (Credencial de acceso protegido) que genera en el servidor una clave única por usuario que será distribuida a la creación del usuario de manera manual o automática. Pero esto no garantiza de una manera seria la seguridad. Como lo hace el sistema de generación de certificados por PKI, además conlleva ciertas desventajas a la hora de distribuir las claves.

Métodos EAP basados en PKI

- **EAP-TLS** (Transport Layer Security).
- **EAP-TTLS** (Tuneled Transport Layer Security)
- **EAP-PEAP.**

Otros métodos.

- **Biometría.** Se comienzan a desarrollar sistemas biométricos que trabajen sobre RADIUS, y concretamente sobre EAP. Esta es una buena alternativa al sistema convencional y esta todavía por desarrollar. Entre las opciones biométricas se considera la huella dactilar, el iris ocular, la forma del rostro, la voz, etc.

3.2.2.1 Autenticación simple y autenticación mutua.

La importancia de la autenticación mutua sobre la simple no ha sido siempre tenida en cuenta. Los ataques ingeniados por algunos hackers y la mejora de la

seguridad ha sido la principal causa que ha propiciado la importancia que se merece este concepto.

La autenticación simple, que es el modelo clásico, se basa en que el sistema suplicante (usuario) solicita la autenticación al servidor de autenticación, presuponiendo que éste sea el servidor lícito al que se quiere conectar, y por ello le entrega sus credenciales para ser autenticado.

Mediante la autenticación mutua, basada en la desconfianza mutua, el suplicante que se conecta al servidor de autenticación verifica primero la identidad del servidor al que va posteriormente a enviar sus credenciales.

En los casos de autenticación mutua mediante certificados, como en los protocolos EAP, enviado por túnel mediante TLS, antes de que se produzca el intercambio de credenciales vía túnel entre suplicante y servidor, ambos pasan por un proceso de verificación de identidades, normalmente mediante el uso de un certificado de cliente y otro de servidor. Los protocolos EAP-TLS, EAP-TTLS, EAP-PEAP y algunos otros se basan en la autenticación mutua, bien sea mediante certificados de cliente y de servidor o por combinación de certificados de servidor y credenciales de usuario.

3.2.2.2 PAP, CHAP, MS-CHAP.

PAP (utilizado anteriormente en el protocolo PPP) y CHAP son los métodos nativos de autenticación incluidos en los primeros servidores RADIUS y por ese motivo son también los mas antiguos y menos fiables. Todas las versiones de RADIUS tienen soporte nativo para los módulos PAP y CHAP.

PAP (Password Authentication Protocol) se basa en el envío del nombre de usuario y contraseña, o sea las credenciales, desde texto en claro sin cifrado ni

ocultación. Si bien PAP no tiene soporte para cifrado, RADIUS oculta siempre las contraseñas durante el transporte entre el NAS y el Servidor, aunque por el tramo entre el suplicante y el NAS quedan descubiertas. El suplicante se las envía al servidor de autenticación a través del autenticador o NAS. El NAS intercepta este mensaje que proviene normalmente de otro protocolo como PPP o EAP y lo traduce a RADIUS, encriptando el atributo User-Password (atributo de contraseña por defecto en RADIUS) mediante una función MD5 basada en el shared secret que comparte con el servidor y otros operadores. Por eso se dice siempre que RADIUS no envía contraseñas sin ocultarlas, y aunque cierto, no por ello menos inseguro. A pesar de esta simplicidad de PAP, es el sistema ideal por su simpleza para ser utilizado por otros métodos como tokens y generadores de contraseña que por diseño generan contrastes de un solo uso. También podemos utilizar funciones matemáticas como MD5 para el procesamiento de las contraseñas y evitar su almacenamiento en texto en plano.

CHAP es la actualización propuesta a PAP (RFC 1334 y 1994), y no hay que quitar mérito a su desarrollo, que en su momento fue muy importante. CHAP se basa en un sistema de desafío-respuesta, que implica que el servidor solicite la respuesta correctamente codificada a una frase aleatoria que ha planteado al suplicante. La principal ventaja de CHAP es que no se produce el trasporte de las contraseñas en sí, ya que lo que se traspasa es el resultado de aplicar la contraseña a una función MD5 contra la frase propuesta. No obstante este método está ya hoy en día demasiado obsoleto. El principal inconveniente de CHAP es que, a pesar de mejorar la seguridad en el transporte, obliga a bajar la seguridad en la base de datos de usuarios, ya que precisa de una contraseña almacenada en texto claro, cosa que por seguridad ya no hace actualmente ningún sistema. Si se comprometiera una base de datos de organización, y esto es más importante que comprometer una contraseña.

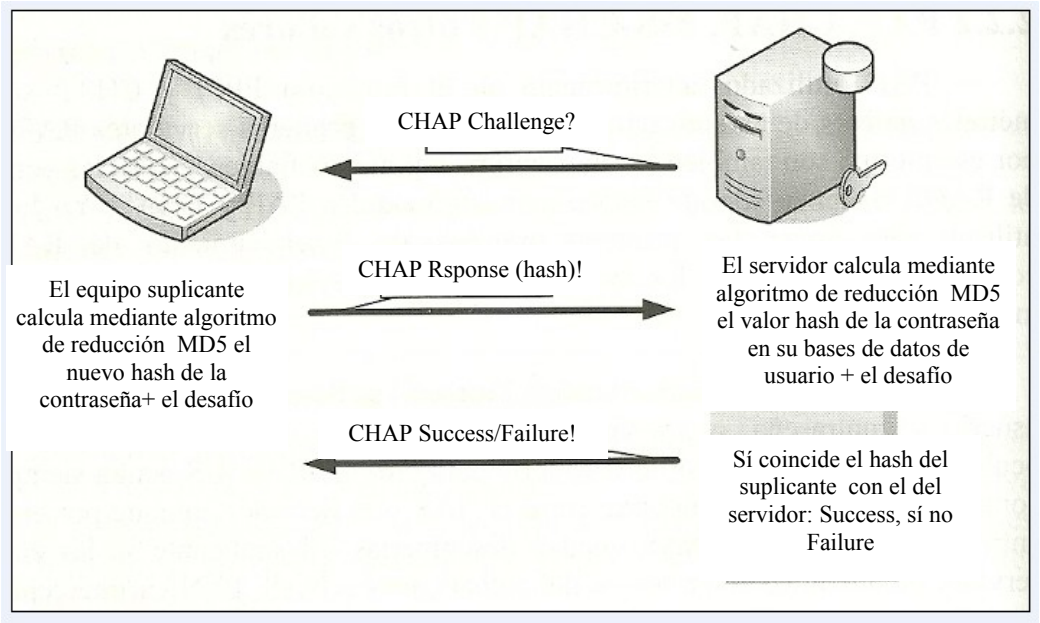

Figura 3.6. Secuencia de Autenticación CHAP.
Fuente: Hansen, Fernandez Yago, 2008

Futuras versiones de CHAP aparecieron desarrolladas de la mano de Microsoft como MS-CHAPv1 y MS-CHAPv2 que mejoran algunos atributos de mensajería además de evitar el almacenamiento de contraseñas en texto en claro tanto en el lado del servidor, como en el lado del suplicante. Además permitía negociar los cambios de contraseña ante la caducidad de la misma. MS-CHAPv1 utiliza, a diferencia de CHAP, el hash de NT o de LM para el calculo del Challenger response y no la contraseña en texto en claro. MS-CHAPv2 elimina el uso del hash de LanManager (LM) por problemas de seguridad y añade autenticación mutua contra el equipo NAS. Sin embargo MS-CHAP tiene hoy en día muchas vulnerabilidades y problemas de seguridad, ya que la entropía de su sistema de encriptación DES es insuficiente (56 bits) y el sistema de cambio de contraseña puede comprometer más aún su seguridad.

Comparación ente PAP y CHAP

- **PAP.** Se pueden almacenar las contraseñas cifradas. La contraseña viaja descubierta desde el suplicante hasta el NAS. El riesgo de interceptación de la contraseña (difícil en líneas telefónicas o xDSL) afecta a una sola contraseña.

- **CHAP.** Obliga a almacenar las contraseñas sin encriptar. La contraseña en sí no viaja desde el suplicante hasta la NAS. El riesgo de seguridad afecta a la base de datos de contraseñas.

Hoy en día se siguen usando estos métodos de autenticación, aunque en entornos controlados donde la autenticación no es tan importante, como en conexiones ADSL donde existen otros datos de identificación como el puerto del módem, el identificador de llamada o la dirección MAC del router. También se suelen usar estos métodos en conexiones por túnel mediante TLS como EAP-PEAP o EAP-TTLS.

3.2.2.3 EAP (Extensible Authentication Protocol).

Extensible Authentication Protocol o EAP es la extensión de autenticación que ha permitido que RADIUS resurja, y es porque cuando ya los demás métodos de autenticación estaban en seria duda de seguridad, se precisaba de un nuevo método que pudiera extender la autenticación hacia un futuro a medio plazo.

Un error que se comete habitualmente es considerar a EAP como un protocolo de autenticación, ya que en realidad no lo es. EAP es un protocolo encargado del transporte, encapsulado y seguridad de la autenticación, y en su interior se encuentran

los métodos de autenticación que se desea utilizar. Por ello cuando hablemos de autenticación EAP, siempre incluimos un sufijo como MD5, MSCHAP, etc. quedando el método de autenticación como EAP-MD5 o EAP-MSCHAP. Existen más de cuarenta métodos de autenticación sobre EAP, lo que lo hace muy versátiles para cualquier tipo de implementación a cualquier escala. La verdadera potencia de EAP es que puede trabajar de forma independiente como protocolo de transporte sobre la capa dos de OSI (cap de enlace), prescindiendo de la dependencia hacia otros protocolos como IP o PPP. Al ser EAP un protocolo de transporte como PPP, dispone de sus propios sistemas de entrega, retransmisión y de integridad de paquete.

Lo interesante del modelo EAP es que es un protocolo de autenticación de tipo "pass-through", lo que significa que el NAS o autenticador sólo tiene que iniciar el proceso de autenticación mediante un paquete EAP-Request y a partir de ese momento reencamina todo el proceso de autenticación hacia un servidor de autenticación como RADIUS. Haciéndolo de esta manera, el NAS no tiene por que realizar el papel de autenticador, sino que lo deriva hacia el servidor de autenticación que es el que soportará el tipo de autenticación solicitada. De esa manera la única función del NAS en la conversación es encapsular los paquetes de tipo EAP en paquetes RADIUS. El protocolo RADIUS se encarga de forma transparente del transporte de esos paquetes entre el autenticador y el servidor de autenticación. En condiciones normales, el servidor de métodos de autenticación de EAP reside en el mismo sistema que el autenticador y suele ser el propio RADIUS. La labor que realiza RADIUS es encapsular los paquetes EAP en sus mensajes estándar de Access-Request, Access-Challenge, Access-Accept y Access-Reject. Este encapsulamiento se produce de forma muy sencilla, introduciendo los paquetes EAP en forma de atributos EAP-Message-Authenticator. Esta forma de encapsulamiento funciona de forma muy adecuada, excepto en algunas configuraciones de proxy RADIUS en las que puede tener algunos inconvenientes.

Existen innumerables métodos de autenticación que funcionan sobre EAP, entre los más comunes CHAP (MD5), PAP, TLS, TTLS, PEAP, SIM, AKA, o incluso Kerberos. Algunos de estos tipos de EAP, como EAP-SIM, se utilizan en la telefonía móvil porque implementan soporte para nuevas tecnologías de movilidad como el roaming o el protocolo MobileIP. Podemos agrupar tres tipos principales de métodos de autenticación sobre EAP.

- **Métodos basados en claves compartidas**. Los métodos basados en claves compartidas han existido siempre y seguirán existiendo por mucho tiempo más. El problema de ellos consiste en la forma de distribución, transporte o almacenamiento de las credenciales. Dando por hecho que cada usuario debe tener bien guardada su clave en sitio seguro. Algunos métodos basados en claves compartidas son PAP, CHAP, EAP-MD5, EAP-MSCHAPv2, EAP-FAST, EAP-SIM, EAP-AKA.

- **Métodos basados en certificados u otros sistemas de claves no compartidas.** Estos son los métodos más adecuados para una buena implantación de seguridad, pero también son los más duros de implantar. Los sistemas basados en la generación de una clave inmediata como los token son más fiables que los anteriores, pero los certificados PKI o las tarjetas criptográficas ofrecen soluciones más complejas de implementar pero muchos más cómodos y adecuados, una vez funcionales. Algunos de estos métodos son EAP-TLS, EAP-TTLS, EAP-PEAP.

- **Métodos basados en características físicas.** En la actualidad están apareciendo nuevas implementaciones de seguridad basadas en EAP que utilizan nuestras características biométricas como medio de identidad.

También se pueden clasificar los métodos de autenticación sobre EAP en otros dos tipos, basándonos en su sistema de seguridad:

- **Métodos no vía túnel**. Los primeros tipos de autenticación sobre EAP, como EAP-MD5, EAP-MSCHAPv2, EAP-SIM, etc., no son por "túnel". El tráfico EAP completo no es cifrado por el suplicante, autenticador y servidor de autenticación. Sólo la información de contraseñas de usuario y algunos otros paquetes delicados se cifran en el interior de los paquetes que circulan por la red. Si se interceptan los paquetes que se generan en el proceso de autenticación, se pueden capturar los hashes para así poder obtener las credenciales de los usuarios. Existen otros tipos de EAP no vía túnel como EAP-OTP y EAP-GTC que utilizan sistemas tokens generadores de claves instantáneas de un solo uso.

- **Métodos vía túnel**. El sistema por túnel de EAP es principalmente EAP-TLS y sus sucesores que utilizan un sistema criptográfico simétrico/asimétrico para la encriptación completa del tráfico durante el proceso de autenticación, autorización y arqueo. Este cifrado asimétrico se sustenta de certificados X.509 que son intercambiados entre el servidor y el suplicante y utiliza un túnel similar a SSL. De esta manera se incrementa la seguridad del canal de forma bastante robusta contra la interceptación de tráfico o los ataques de MiTM. Algunos de estos métodos son EAP-PEAP y EAP-TTLS.

Cada uno de los tipos de EAP dispone de un identificador de tipo de EAP para establecer el método en las conversaciones EAP. El RFC base que define EAP es el RFC 3748.

3.2.2.3.1 EAP-MD5.

EAP-MD5 es la primera versión, la más simple y, por tanto, la más insegura de EAP. El método utilizado fue desarrollado por RSA es análogo a CHAP. Como su nombre lo indica, utiliza el algoritmo MD5, para obtener un hash de la contraseña de usuario, lo que lo hace muy vulnerable a ataques de fuerza bruta o a ataques mediante Rainbow Tables. Es un método de autenticación de una sola dirección (el servidor autentica al cliente pero no viceversa). Se considera el más inseguro de los tipos de EAP, ya que no incorpora ningún sistema de encriptación de los paquetes, que circulan en texto en claro. No incorpora la característica de generar claves de sesión para el cifrado de protocolos como WEP o WPA como lo hagan TLS, TTLS o PEAP. Solo se debe utilizar en canales de autenticación difíciles de interpretar como 802.1X para redes cableadas y con mucha precaución.

3.2.2.3.2 EAP-TLS.

Estos métodos, además de utilizar los seguros certificados para la identificación de las partes y el establecimiento de las partes y el establecimiento del túnel, pueden utilizar claves precompartidas (PAP, CHAP…) en el interior del canal cifrado, por lo que su seguridad es doble. El sistema criptográfico utilizado se basa en PKI (Public Key Infraestructure o Infraestructura de clave pública).

Desde la aparición de los sistemas inalámbricos el confort de la seguridad en la que se basan muchos proveedores de servicios tuvo que cambiar. A pesar de que muchos protocolos como EAP-MD5, LEAP y otros anteriores a éste ya tenían importantes vulnerabilidades demostradas, muchos proveedores se sentían poco amenazados, porque la “privacidad” del cable les mantenía “protegidos”. Pero la aparición de estos sistemas inalámbricos que permitían escuchar todos los procesos de las comunicaciones (entre los que está el proceso de asociación y autenticación),

les comenzó alarmar. A partir de ese momento comenzó a acelerarse la finalización de los trabajos sobre este tipo de nuevos protocolos de autenticación como EAP-TLS, EAP-PEAP, EAP-TTLS, etc.

3.2.2.3.3 Métodos EAP basados en TLS.

Los métodos de EAP basados en TLS se apoyan en PKI (Public Key Infraestructure o infraestructura de clave pública) para el uso de certificados X.509. Tras el intercambio y la comprobación de los certificados de confianza, se establece un túnel TLS (*outer-tunnel*) para el envío al suplicante de una clave de cifrado que se utilizara en las consecutivas comunicaciones. Este primer intercambio de credenciales para el establecimiento del túnel TLS se conoce como *outer-tunnel* y produce un flujo de paquetes entre el servidor y el suplicante. Apoyándose en la seguridad proporcionada por este sistema de certificados, se puede utilizar con bastante tranquilidad dentro de este túnel (*inner-tunnel*) cualquier otro sistema de autenticación más inseguro como CHAP, PAP u otros similares. Este segundo intercambio produce un segundo flujo de paquetes entre el servidor y el suplicante. Podemos simplemente entender que se producen dos procesos de autenticación independientes entre el servidor de autenticación y el suplicante, y así lo gestionan algunos servidores como FreeRADIUS. Por esto, como ejemplo, cuando se produce una autenticación como PEAP basada en MSCHAPv2, se produce una primera fase de autenticación basada en certificados (TLS) y posteriormente en su interior se produce una autenticación basada en EAP-MSCHAPv2.

Al enviar un suplicante al servidor la solicitud de acceso con su nombre de usuario (que en algunos tipos como TTLS puede, y debe, ser anónimo), el servidor responde enviando su certificado de servidor para que el suplicante lo verifique. Tras esa comprobación de la confianza sobre el servidor, el suplicante realiza el envío de su certificado de cliente al servidor.

Pasado ese primer proceso de verificaciones, se establece un canal seguro mediante TLS (SSL) para que, si procede, se intercambien credenciales u otros métodos de autenticación y para finalmente acabar entregando al suplicante y al equipo NAS una clave única a fin de que pueda establecer una sesión segura de comunicaciones, como es el caso de WPA2 en redes inalámbricas. TLS y SSL funcionan en capas diferentes del modelo OSI, TLS trabaja en la capa 2 (enlace) y SSL sobre la capa 5, pero su modelo basado en PKI es muy similar.

EAP-TLS es un método de autenticación muy seguro, pero que requiere de una infraestructura medianamente compleja para su puesta en funcionamiento, por ese motivo seguramente su difusión está resultando algo lento. Este protocolo es un protocolo de autenticación mutua, lo que significa, como ya explicamos, que tanto el suplicante debe autenticarse contra el servidor como el servidor contra el suplicante. Esto hace que se necesite de dos certificados X.509, uno para el servidor de autenticación y otro para el suplicante. De esa manera se evitan los ataques del tipo MITM (hombre en medio) que pueden provocar que un suplicante entregue sus credenciales a un falso servidor. EAP-TLS necesita que se almacenen los certificados de cliente en el equipo donde reside el suplicante. Esto puede también conllevar problemas de seguridad, ya que la parte principal de ese certificado, que es la clave privada, podría ser robada del equipo en cuestión si no se almacena cifrada, y esto suele ser así en algunas implementaciones. Para evitar esto, se puede utilizar smartcards o tarjetas criptográficas que protegen mediante un procesador de cifrado y un pin, la clave privada del cliente. La única posibilidad de robar la identidad del usuario es robar su tarjeta y conocer su PIN pero aun así el sistema PKI se apoya en la revocación de certificados y al denunciar por parte del usuario la perdida del certificado de su tarjeta, éste puede ser inmediatamente revocado y la tarjeta quedará inservible para esta red. Otra opción sería que los propios programas suplicantes cifran los certificados al guardarlos y/o solicitaran un PIN al utilizarlos.

EAP-TLS está soportado por la mayor parte de suplicantes del mercado, incluyendo los de los propios SO como Windows que lo soporta desde la versión 2000 SP4, por lo que su implantación resulta muy apropiada para instalaciones como las redes inalámbricas.

Un fallo de seguridad intrínseco al EAP-TLS es la forma en la que se intercambian los datos de identidad (User-Name) en texto en claro, previamente al intercambio de certificados, de tal manera que interceptando este tráfico se pueden recopilar los nombres de usuario, de aquellos que se estén autenticando. Si bien los nombres de usuario no bastan para realizar un ataque contra la red, es un dato que ayudará bastante en la enumeración del sistema.

EAP-TLS no permitía la reconexión rápida mediante recuperación del túnel TLS, aunque en el último RFC 5216 de marzo de 2008 ya se comienza a implementar. EAP-TLS es un estándar abierto (no propietario) y el RFC que lo define es el RFC 5216 que deja obsoleto al RFC 2716 de IETF.

3.2.2.3.4 EAP-TTLS.

EAP-TTLS es una extensión de EAP-TLS, desarrollado por Funk y Certicom para simplificar la implantación de EAP-TLS. Su identificador de tipo EAP es 21. Este método no se basa en la autenticación mutua previa mediante dos certificados, ya que solo el servidor debe disponer de un certificado X.509. Esto dificulta igualmente que se produzca un ataque MITM, puesto que el suplicante estará igualmente seguro de la identidad del servidor contra el que se autentica. No obstante, en TTLS el cliente puede utilizar opcionalmente un certificado X.509 si lo prefiere.

El sistema TTLS implementa un sistema de creación de dos túneles de seguridad respectivamente. El primer túnel TLS se crea para el intercambio de credenciales y el segundo para el traspaso de la clave de cifrado de sesión, con la que

equipos NAS como AP cifran el tráfico con la estación que se conecta. Todo el tráfico circula encriptada, incluso los mensajes de EAP Succee y Failure (Autenticación exitosa o fallida).

La secuencia comienza una vez que el cliente comprueba el certificado del servidor, con lo que se inicia un túnel o canal cifrado para el traspaso de las credenciales del cliente al servidor de forma segura. Utilizando este canal seguro podemos, ya dentro del túnel, utilizar otros medios de autenticación más primitivos como PAP, CHAP, MS-CHAP u otros que decidamos, y esto no supondrá un riesgo. Este es un sistema de autenticación mixta, porque se basa en la autenticación mutua pero utiliza claves compartidas.

Esta autenticación inicial basada en un solo certificado de servidor, simplifica de forma importante la implementación de esta seguridad al no tener que generar certificados para cada cliente nuevo que desee conectarse a la red y por tanto no nos obliga a disponer de una Infraestructura de Clave Pública o PKI activa.

Otra ventaja de TTLS es que se utiliza un sistema de atributos similar al nativo de RADIUS llamado AVP (Attribute Value Pair o par de atributo/valor), con una notación parecida a la de RADIUS. El intercambio de atributos y valores se realiza en el canal cifrado TLS. Su principal valor es el de poder extender el protocolo mediante nuevas implementaciones de atributos, a diferencia de EAP-PEAP que no utiliza el sistema AVP sino un intercambio de mensajes EAP.

En cuanto al fallo de seguridad de EAP-TLS (captura de nombres de usuario), también queda solucionado al enviarse un nombre de usuario anónimo al inicio de la autenticación, diferente al nombre de usuario real que se utiliza en el traspaso de credenciales CHAP, PAP… para el acceso. Por ello su seguridad es muy robusta. El trafico de una sesión de autenticación EAP es importante, si se debe reautenticar a un suplicante cada poco tiempo se genera demasiado trafico. Por eso EAP-TTLS permite

la reconexión rápida mediante el parámetro "TLS session resume" que continúa la ultima sesión por túnel TLS evitando una gran cantidad de trafico. EAP-TLS no dispone inicialmente de la función Fast reconnect. La función fast reconnect usando el "TLS resume" puede causar problemas en infraestructuras con varios servidores RADIUS, ya que la clave TLS en caché para esa conexión no estaría disponible si la validación se realizara contra otro servidor de la cadena, por disponer de roaming o control dinámico del trafico. Se discute también sobre si el uso de este parámetro puede permitir ataques MiTM.

Microsoft no da soporte nativo a EAP-TTLS que se puede implantar mediante suplicantes ajeno como SecureW2, WAP_Supplicant u otros de pago.

3.2.2.3.5 EAP-PEAP.

EAP-PEAP (Protected Extensible Protocol) fue desarrollado por CISCO, Microsoft y RSA y por eso se encuentra en los productos de estos fabricantes de forma más o menos nativa.

EAP-PEAP se basa en un solo certificado de servidor como TTLS y soporta como métodos de autenticación MS-CHAPv2 y GTC (Generic Token Card). Si empleamos el método MS-CHAPv2 se le conoce como PEAPv0 que es prácticamente el único incluido en los sistemas operativo como Windows y si utilizamos GTC se le conoce como PEAPv1 que no tiene soporte nativo en ningún SO. Es por esto, y por intereses comerciales, que Microsoft conoce a PEAPv0 como PEAP simplemente y tras la salida al mercado del estándar EAP-TTLS no tiene pensado dar soporte a la v1.

Lo que para algunos administradores puede suponer una ventaja de PEAP es que al haber sido en parte desarrollado por Microsoft posee nativo para su sistema operativo a partir de Windows XP. Este soporte nativo, que forma parte de Windows Server 2003, incluye a PEAP en sus políticas de grupo, facilitando la divulgación de

certificados y de confianzas de forma automatizada para toda la red basada en AD. Lo que puede ser una ventaja para la implementación de PEAP en sistemas Microsoft y Cisco puede ser una desventaja para otros sistemas por la falta de soporte que tiene PEAP en ellos. Hay una larga discusión sobre si es mejor utilizar TTLS o PEAP. Ambos son dos productos con un nivel de seguridad muy adecuado y con el tiempo y los hackers se ira viendo cual es más seguro o apropiado.

PEAP también es un protocolo muy recomendado para la seguridad de redes inalámbricas como Wi-Fi y esta extensamente soportado por la mayoría de los fabricantes de equipos compatibles con 802.1X y 802.11i. EAP-PEAP dispone también de la función Fast reconnect para el establecimiento de sesiones TLS. Ambos protocolos permiten el intercambio dinámico de claves como las que se precisan en Wi-Fi o VPN.

3.2.2.3.6 Tabla Comparativa de Tipos de EAP.

Tabla 3.1 Tabla Comparativa de Tipos de EAP

	EAP-MD5	**LEAP**	**EAP-TLS**	**EAP-TTLS**	**EAP-PEAP**	**EAP-FAST**
Certificado de Servidor	No	Challenge	Si	Si	Si	No PKI Shared Secret
Certificado de Cliente	No (Nombre de usuario y contraseña mediante Challenge)	No (Nombre de usuario y contraseña mediante Challenge)	Obligatorio (Posible Smartcard)	Opcional (credenciales de usuario)	Opcional (credenciales de usuario)	PAC No PKI
Validación de certificados	No	No	OCSP TLS	OCSP TLS	OCSP TLS	No
Credenciales soportables	MD5 hash	Hash similar a MS-CHAP	Certificados de cliente	CHAP, PAP, MS-CHAPv1 y v2	EAP-MSCHAPv2 EAP-GTC y otros tipos de EAP	PAC

Soporta cambio de contraseña	No	No	No	Si	Si	Si
Autenticación Mutua	No (solo cliente)	Si (Challenge)	Si	Si	Si	Si
Tunelamiento	No	No	Si, TLS	Si, TLS	Si, TLS	Si, TLS
Entrega de claves dinámicas	No	Si	Si	Si	Si	Si
Reconexión rápida	No	No	Si (a partir de RFC5216)	Si	Si	Si
Bases de Datos de Autenticación	SQL, en formato MD5	AD, NTLM	AD, NTLM, Token, LDAP, Novell NDS, OTP	AD, NTLM, Token, LDAP	AD, NTLM, Novell NDS Token.	AD, NTLMM LDAP
Desarrollador	Estándar	Solo Cisco	Microsoft	Funk y Certicom	Microsoft, Cisco y RSA	Cisco
Suplicantes que lo soportan	Microsoft WPA Supplicant MacOs	Propietarios MacOS Linux	Propietarios MacOS Linux	Junip. Oddissey SecureW2 WAP Supplicant MacOS	Propietarios MacOS Linux	Cisco
Muestra nombres de usuario	Si	Si	Si	Anónimo en la fase 1	Anónimo en la fase 1	Si
Vulnerable MiTM	Si	Si	No	No	No	No
Vulnerable actualmente	Si Diccionario	Si	No	No	No	No
Usos Recomendados	Solo redes cableadas 802.1X	No recomendado	802.1X Alámbrica e inalámbrica Smartcards	802.1X Alámbrica e inalámbrica	802.1X Alámbrica e inalámbrica	Redes con equipos Cisco propietario

La decisión sobre los tipos de EAP que debemos introducir se determina varios factores como, por ejemplo:

- **El medio de conexión**: alámbrica o inalámbrica. Si fuera alámbrica contra un switch 802.1X, el nivel de seguridad en la autenticación puede quedar en segundo plano si tenemos en cuenta que cada puerto de conexión está en teoría físicamente aislado. Si elegimos una instalación inalámbrica el nivel de privacidad en la autenticación y posterior funcionamiento debe ser muy alto.

- **La complejidad de la implantación**. Si resulta demasiado problemático implementar certificado de servidor y de cliente (infraestructura completa PKI) podemos elegir un sistema como PEAP o EAP-TTLS que nos evita gran parte de la infraestructura PKI.

- **La plataforma de producción que vamos a utilizar**. Tanto los servidores como los clientes pueden ser Windows, PocketPC, Linux, MacOS, etc. Debemos intentar buscar alternativas si vamos a trabajar en múltiples plataformas. Debemos asegurarnos que cada plataforma soporte el suplicante elegido.

- **Intercambio dinámico de claves de sesión.** Si pretendemos cifrar o tutelar el tráfico de red tras la autenticación, el estándar de autenticación elegido debe permitir el transporte o intercambio de claves de cifrado y caducidad de sesión.

3.2.3 Shared Secret (Secreto Compartido).

El shared secret o secreto compartido de RADIUS es lo que se conocía como RADIUS key o RADIUS secret. Es una contraseña con formato alfanumérico de hasta 128 bytes (depende de las versiones), que se define en los dos extremos de un canal RADIUS entre el cliente y el servidor, o sea, entre el NAS y el servidor RADIUS. Se pueden y se deben usar contraseñas o secretos diferentes para cada uno de los equipos NAS que actúa contra un servidor. También hay que definir estos

secretos en las comunicaciones entre un servidor y un Proxy de RADIUS, ya que como hemos visto un cliente RADIUS, puede ser un NAS, un servidor de autenticación, una librería, servidor Web o un Proxy RADIUS. Para cada uno de estos participantes, su paso anterior es un cliente.

Este secreto se utiliza para encriptar las comunicaciones entre el cliente y el servidor RADIUS, ya que de no hacerlo, se podría interceptar y examinar todo el tráfico de texto claro entre clientes y servidor RADIUS. Utilizando la autenticación simple PAP el servidor generará un mensaje de Access-Reject sí el secreto compartido no es correcto debido a que el atributo User-Password se cifra utilizando el shared secret, mediante cualquier otro tipo de autenticación el servidor simplemente descarta la solicitud de forma silenciosa.

El funcionamiento del shared secret (secreto compartido) es muy similar al del sistema de desafío o Challenger utilizado en muchos protocolos de autenticación como CHAP o NTLM, Muchos de ellos están dejando de utilizarse o utilizan algoritmos de reducción diferentes a MD5 que es el que utiliza RADIUS.

MD5 es un algoritmo de reducción del mensaje, no de cifrado de mensaje, y se utiliza para no tener que transportar una clave en texto en claro. Esa clave se pasa por una función MD5 que la procesa en una frase generada o hash que es irreversible; no se debe poder obtener la clave inicial a través de ese hash

En una autenticación mediante RADIUS, el cliente o NAS comparte el mismo secreto que el servidor, por eso se llama secreto compartido. Cuando se produce una solicitud de acceso (Access-Request) el NAS envía esta petición en texto claro, cifrando solamente el campo de password o contraseña de usuario. Para ello el NAS genera una frase de 16 bytes de código aleatorio que se denomina Request Authenticator, y que incluye en el paquete de solicitud. Esta frase se concatena con el secreto compartido y se pasa el resultado para una función MD5 que crea un hash de 16

bytes, al que se le aplica la función XOR con los primeros 16 bytes de la contraseña del usuario. Si la contraseña midiera más de 16 bytes se repetiría la misma formula tantas veces como segmentos de 16 bytes tuviera la contraseña, excepto porque la concatenación de la función MD5 se realiza usando en vez del Request Authenticator el resultado de la primera fase cifrada.

fc [1] = p [16b] . XOR MD5 (ss + ra)

fc [2] = p [16b] . XOR MD5 (ss + fc [1])

fc = fc [1] + fc [2]

Donde: **fc** (frase cifrada), **p [16b]** (segmento de 16 bytes de la contraseña de usuario), **ss** (shared secret), **ra** (Request Authenticator). El símbolo más (+) representa concatenación. En el ejemplo anterior se reduce un password de usuario de un máximo de 32 bytes.

Figura 3.7. Shared Secrets (secreto compartido).
Fuente: Hansen, Fernandez Yago, 2008

Como medidas de seguridad se recomienda usar shared secrets (secreto compartido) de un mínimo de 32 bytes no basados en diccionario y respetando las normas de seguridad de cualquier contraseña aceptable, como utilizar símbolos, números, letras, mayúsculas y minúsculas. Aun haciéndolo así el valor de posibles claves por byte pasa de 256 si usaramos notación hexadecimal a 94 usando un teclado americano.

Y la verdad es que muy pocos servidores RADIUS permiten shared secrets (secreto compartido) utilizando notación hexadecimal. Este es uno de los puntos débiles de las comunicaciones de RADIUS, ya que la administración de diferentes secretos compartidos en diferentes equipos es un punto de riesgo de seguridad.

Recomiendo en utilizar diferentes shared secrets (secreto compartido) para cada uno de los componentes de la cadena, ya que utilizar el mismo para cada uno comporta un alto riesgo de seguridad. Con las tecnologías actuales de haching, conociendo el secreto compartido, se puede simplemente descifrar las claves de usuario.

3.2.4 Estructura de las comunicaciones RADIUS.

En esta sección explicaremos la estructura de un paquete de RADIUS estándar y mostraremos la secuencia de un proceso completo de autenticación.

3.2.4.1 Formato de mensaje RADIUS. Paquetes de datos.

Vamos a diseccionar un paquete de datos en formato RADIUS para conocer un poco mejor su estructura y la de cada uno de los campos que lo forman. Debemos tener en cuenta que el formato de paquete que se muestra a continuación viene encapsulado dentro de un paquete UDP estándar.

Paquete UDP:

Figura 3.8 Paquete UDP.
Fuente: Hansen, Fernandez Yago, 2008

Paquete RADIUS:

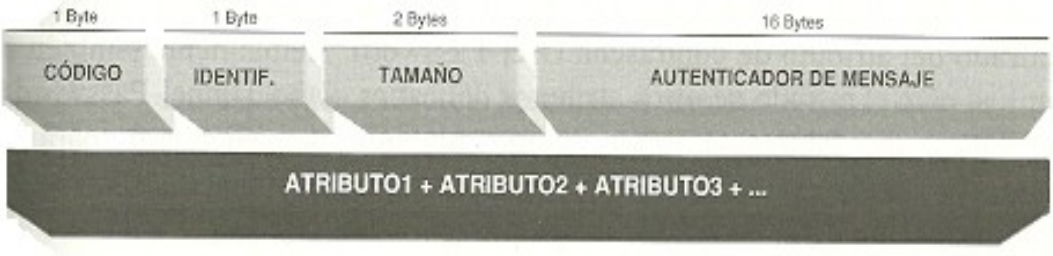

Figura 3.9 Paquete RADIUS
Fuente: Hansen, Fernandez Yago, 2008

- **Identificador** – Es un campo utilizado para relacionar los paquetes que conforman una conversación (solicitud y respuesta, etc.) (1 byte).
- **Tamaño** – Tamaño del paquete completo (entre 20 y 4096 bytes), incluyendo cabecera y atributos (2 bytes).
- **Autenticador de mensaje** (16 bytes) – Es un campo generado pseudoaleatoriamente, utilizado para validar la legitimidad del servidor RADIUS con el que estamos conversando. Se utiliza desde los comienzos para el cifrado del atributo de la contraseña User-Password. Actualmente también se utiliza para el cifrado de otros atributos delicados como Túnel-Password y atributos de fabricante VSA, como algunos de Microsoft para el intercambio de claves mediante MS-CHAP. Es también un sistema de comprobación de la integridad del paquete.
- **Atributos estándar** – El verdadero contenido del paquete RADIUS, con todos los AVP necesarios para el funcionamiento de todo el proceso AAA. El paquete de atributo tiene las siguientes estructura:

Figura 3.10 Atributo Estándar de Paquete RADIUS
Fuente: Hansen, Fernandez Yago, 2008

- **Código**. (1 byte). Representa el código de atributo que se incluye, ya que no se utiliza el nombre real del atributo. Se debe utilizar el diccionario estándar o de fabricante para la traducción de código a nombre de atributo. Por ejemplo: el atributo User-Password aparecerá como código 2.
- **Tamaño**. (1 byte). Muestra el tamaño del atributo, incluyendo su cabecera (código + tamaño) y su cuerpo (valor). Si no corresponde el valor de este campo con el tamaño real del paquete, se descartará.
- **Valor**. Incluye los datos que conforman el contenido o el valor del atributo que se incluye. Su tipo de datos y tamaño dependerá del atributo específico que se incluya.

- **Atributos de Fabricante o VSA** – El otro tipo de atributo que se puede incluir en el mensaje es el atributo de fabricante. El diccionario del fabricante debe ser incluido en el servidor RADIUS para su traducción. Su formato es un poco diferente:

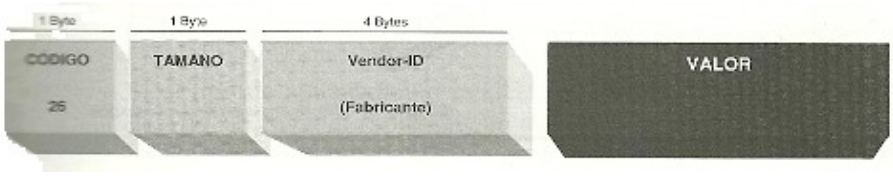

Figura 3.11 Atributo Atributos de Fabricante o VSA
Fuente: Hansen, Fernandez Yago, 2008

- **Código**. (1 byte). En el caso de atributo propio de fabricante o VSA se utiliza el número de atributo 26 (1x1A hexadecimal) cuya traducción en el diccionario estandar es Vendor-Specific.
- **Tamaño**. (1 byte). Muestra el tamaño del atributo, incluyendo su cabecera (código + Vendor-ID + tamaño) y su cuerpo (valor). Si no

corresponde el valor de este campo con el tamaño real del paquete, se descartará

- **Vendor-ID**. (4 bytes). Es el atributo que define código de fabricante utilizando 3 bytes (el primer byte se pone a 0x00) en el formato SMI (Structure and Identificaction of Management Information – code of vendor).

Figura 3.12 Vendor-ID
Fuente: Hansen, Fernandez Yago, 2008

- **Valor**. Incluye los datos que conforman el contenido o el valor del atributo que se incluye. Cada uno de los diferentes atributos incluidos conlleva un formato más o menos fijo de datos.

Esto representa la estructura típica de un mensaje de datos RADIUS y su estructura básica de un paquete de datos.

3.2.4.2 Secuencia de Autenticación de RADIUS.

Las secuencias no son siempre idénticas; durante un proceso de autenticación hay varios factores que pueden variar, como el método de autenticación, los reintentos u otros factores.

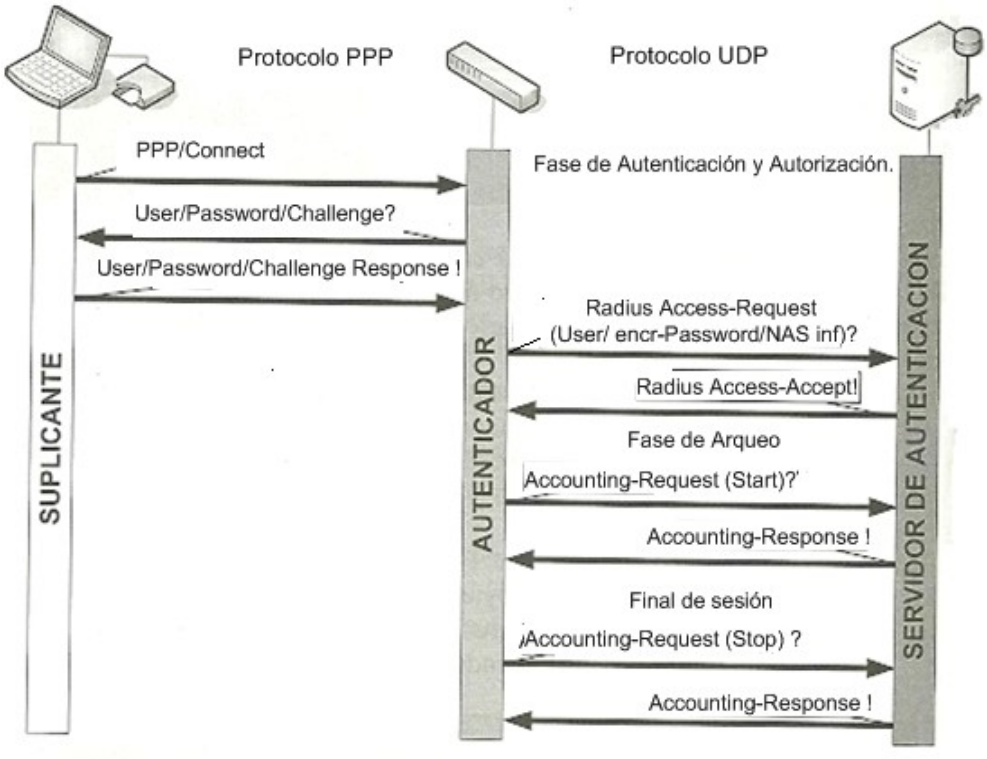

Figura 3.13 Secuencia AAA de RADIUS.
Fuente: Hansen, Fernandez Yago, 2008

- El proceso suele comenzar por un Access-Request. La solicitud de acceso es un mensaje que contiene atributos como el nombre de usuario, la contraseña (en caso de PAP) el número de puerto NAS y el ID de cliente. El NAS envía esta solicitud al primer servidor RADIUS que tenga preestablecido en su lista de servidores. Si no recibe respuesta en un tiempo a determinar, reintentará el envió un número de veces designado a ese o a otros servidores RADIUS de la red.

- El servidor RADIUS que recibe la solicitud comprueba si proviene de un equipo NAS autorizado; si no es así la descarta silenciosamente (silently discard). Si el cliente esta en su lista y el shared secret es el correcto, comprueba en la/s bases de datos de usuarios el nombre y la contraseña. Si

este registro fuera acompañado de otros atributos de servicio (dirección IP, ancho de banda asignado, etc.) se los enviaría al cliente o NAS para que los gestione. Podría ocurrir en este paso que el servidor esté directamente configurado como Proxy o que en el nombre de usuario exista un realm al que debe reencaminar las solicitudes; si es así, reenviará el mensaje al servidor designado, y si tuviera configurado para ello añadiría algunos atributos a la solicitud.

- Si el tipo de autenticación es CHAP o cualquier otra basada en el desafío, se envía al suplicante un mensaje de Access-Challenge con la frase aleatoria que debe calcular. En algunos métodos basados en desafío como OTP (One Time Password o contraseña de un solo uso) como Token, dispositivos de cifrado USB, etc. se solicita en este momento al usuario un PIN, contraseña, la introducción de una tarjeta o dispositivo de cifrado USB, etc. para volver a enviar un Access-Request con los nuevos datos calculados. Este proceso se puede volver a repetir varias veces dependiendo del método de autenticación utilizado.

- Tras comprobar todos estos datos de autorización y la base de datos de credenciales, decidirá si acepta o deniega la solicitud, enviando un mensaje de Access- Accept o Access-Reject al NAS con los atributos necesarios para activar o denegar el servicio.

- En ese momento el NAS abrirá el puerto solicitando con los atributos designados, y enviará un mensaje de Accounting-Request [Start] al servidor RADIUS indicando que ha comenzado a registrar los datos de arqueo de la sesión de usuario y pasándole los datos del inicio de sesión. Algunos equipos NAS no soportan el arqueo de cuentas, y se saltan este proceso.

- El servidor RADIUS ratifica la recepción del inicio de sesión, devolviendo al NAS un mensaje Accounting-Response [Start], y guardando en su base de datos o archivo log los datos de inicio de sesión del usuario. Si el servidor no envía este mensaje puede que se deba a que no ha recibido la solicitud de inicio, por lo que el NAS deberá reenviar a este o a otro servidor su solicitud de inicio de arqueo.

- Al desconectar el suplicante o finalizar la sesión por cualquier causa, el NAS envía un mensaje de Accounting-Request [Stop] al servidor para indicarle el fin de la sesión del usuario, y enviarle los datos de consumo del usuario.

- El servidor ratifica la recepción de esos datos mediante un mensaje Accounting-Reponse [Stop] que envía al NAS. Si no se produce este mensaje el NAS deberá seguir intentando enviar a este o a otro servidor de arqueo su solicitud de fin de sesión con los datos de la misma. La pérdida de esta información suele conllevar un perjuicio económico, por lo que debe ser tratada con la adecuada atención.

3.2.5 Ámbito de Utilización y Escalabilidad.

Existen multitud de situaciones en la que se puede utilizar o se utiliza un servidor RADIUS de Autenticación. El primer uso que tuvieron fue el de controlar el acceso de los usuarios de módem a redes como Milnet o finalmente a Internet. En ese primer momento RADIUS era muy popular y se utilizaba como puerta de entrada a muchos sistemas que requerían de autenticación mediante los métodos de los que se disponía como PAP o CHAP. Todavía siguen existiendo conexiones a Internet por módem o enrutador xDSL que utilizan este protocolo de la misma manera que lo hacían antes.

- Servidor de conexiones Dialup a Internet o RAS.

- Servidor de Acceso remoto o VPN.
- Servidor de Web privado o de comercio electrónico.
- Servidor Web de banca o de trámites administrativos.
- Conexión de VoIP inalámbrica o alámbrica. El servidor de autenticación se utiliza para verificar las credenciales de un Terminal contra un registrador SIP utilizando autenticación por Digest. Se utilizan aquí también las funciones de accounting del servidor para poder facturar el consumo.
- Conexión celular GSM o de banda ancha móvil UMTS (3G).

Estos son sólo algunos de los ejemplos que puede encontrar en los que se aplica una instalación basada en RADIUS.

3.2.5.1 Modelos de Implantación.

En esta sección se demostró de forma simple cual es el modelo típico de implantación de un servidor RADIUS y sus clientes, aplicando lo que hemos aprendido hasta el momento.

En el diseño que se encuentra a continuación, podemos observar una zona segura de la red interna donde se sitúan el servidor de autenticación RADIUS y el Servidor de Base de Datos o de directorio. Esta zona esta protegida para los usuarios externos, ya que para llegar hasta ella, se deben autenticar previamente mediante los equipos de acceso o NAS que son los únicos que tienen acceso directo a la zona segura.

Cualquiera de los equipos que pretenda tener acceso a la red deberá solicitar previamente el acceso al AP o al Conmutador Ethernet, que lo gestionará a través del servidor RADIUS1. Este a su vez consultará el directorio o DB de credenciales y permitirá o no el acceso del usuario.

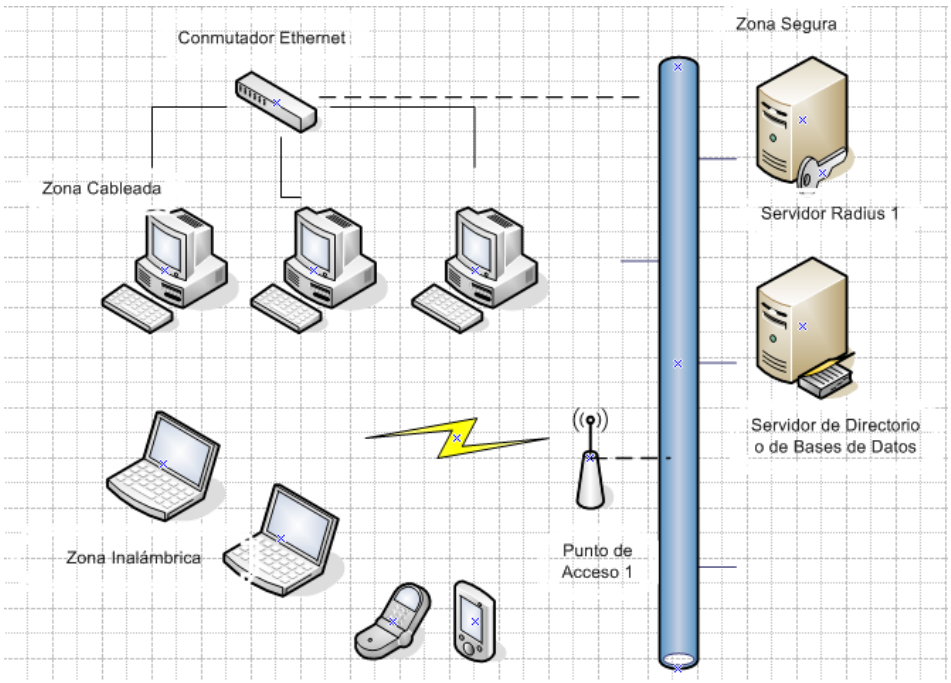

Figura 3.14 Infraestructura Simple RADIUS.
Fuente: Hansen, Fernandez Yago, 2008

3.2.6 Estadísticas y Logs.

Cualquier servidor que presta un servicio tan vital como es AAA, debe mantener constantemente informado de los recursos que está utilizando en cada momento. Estos recursos se componen de porcentaje de procesador/es, ancho de banda utilizado, solicitudes por período (minuto/hora/día/semana...), memoria utilizada, disco utilizado, etc. Si bien, muchos de estos datos nos los ofrecen administradores de servidores en forma de software, los propios de RADIUS nos los debe ofrecer el propio servidor RADIUS que hayamos seleccionado.

Este servidor RADIUS debe grabar y/o trasmitir extensos y detallados logs de todo lo que esta haciendo, para poder depurar y auditar todos los procesos relacionados.

Se deben incorporar administradores remotos, para la revisión de todas estas estadísticas y logs, además de poder monitorizar el servidor en tiempo real, bien sea mediante shells remotas, consolas de administración remotas o mediante el uso de un servidor Web que centralice todos esos datos de uno o más servidores. Además de los datos relativos a AAA se tienen que poder administrar las opciones de configuración y de seguridad remotamente, utilizando cualquiera de estas herramientas.

Mediante el uso del protocolo SNMP y de los administradores adecuados, el servidor RADIUS debe poder enviar datos y estados a syslogs remotos. En el caso de Linux puede comunicarse a través del propio Kernel con servidores syslog que filtren y registren toda esa información. En el caso de SNMP, se registra y analiza esa información desde herramientas apropiadas. Muchas organizaciones de alto nivel utilizan sistemas recopiladores de eventos centralizados, que mantienen documentados todos los procesos de protección de datos y seguridad. Implementaciones como Sentinel de Novell recopilan y archivan todos los eventos de miles de estaciones y servidores de una organización y toman decisiones basadas en los eventos que se producen en tiempo real. Por estos y otros motivos es por lo que resulta imprescindible que el software que conforma un servidor RADIUS registre y publique la mayor cantidad de eventos mediante SNMP, syslog, visor de sucesos (WMI) o logs. Las estructuras de almacenamiento de SNMP en RADIUS están reguladas por la RFC 4668 a RFC 4671 que implementan las MIB de RADIUS.

Para la revisión de logs, se debe referir a los archivos que están situados en la ruta *(/usr/log/freeradius/freeradius.log)*.

Uno de los archivos de log configurables desde servidores como FreeRADIUS es el archivo *radutmp* (proviene del archivo Unix *utmp*) que mantiene un registro de los usuarios autenticados. Este archivo puede ser consultado mediante un editor como *radutmped* o mediante la utilidad *raswho*, ya que su formato es binario. Estos

archivos de log se mantienen actualizados (mediante la información de arqueo) cuando se recibe un paquete de Accounting-Request y no a la autenticación, cosa que hay que tener claro a la hora de consultarlo, ya que si estuvieran vacíos es que no se estaría actualizando la información de Accounting desde el equipo de servicio. Además del archivo *radutmp* existen otros como *radwtmp* que mantiene las sesiones actuales que se pueden consultar mediante la utilidad *radlast*. Estos archivos están situados en la ruta */var/log/freeradius/*.

3.2.7 Extensiones de Autorización Dinámica.

Una de las principales carencias o limitaciones de RADIUS fue siempre que su modelo cliente-servidor no le permitía al servidor de autenticación iniciar una conversación con un cliente o NAS. De esta forma era muy complicado o imposible hacer cambios en la configuración de los clientes en tiempo real o simplemente desconectar a un cliente o suplicante. En el año 2003 se publica la RFC 3576 (Extensiones de Autorización Dinámica para RADIUS) que propone una nueva serie de comandos que el servidor puede enviar al NAS. Estos comandos se utilizaran para proveer soporte de desconexión de sesiones abiertas de usuarios, y de mensajes para realizar cambios en la Autorización de forma dinámica. Estas nuevas extensiones regulan definitivamente lo que se denomina CoA (Change of Authorization), que establece un mecanismo para realizar cambios en las sesiones activas de usuarios.

A partir de ese momento los equipos deberán comenzar, si los fabricantes los desean, a ser compatibles con este RFC para dar soporte a estas normas. Se crean una serie de atributos y mensajes RADIUS que pueden ser enviados desde el servidor RADIUS al equipo NAS, concretamente al puerto 3799 UDO (aunque algunos equipos propietarios utilizan otros como el 1700), incluyendo información de la sesión de usuario y del puerto físico del NAS que se desea desconectar o modificar. Estos nuevos mensajes que se regulan en este RFC son Disconnect-Request, Disconnect.Response, Disconnect-ACK, CoA-Request, CoA-ACK y Coa-NAK.

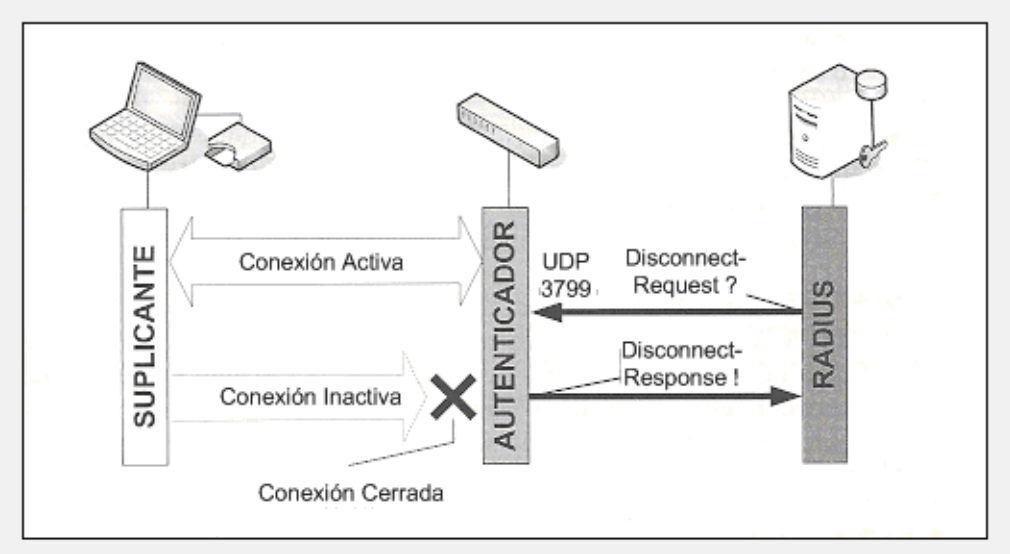

Figura 3.15 Desconexión de Usuarios.
Fuente: Hansen, Fernandez Yago, 2008

3.2.8 Limitaciones de RADIUS.

Muchas de las limitaciones de RADIUS son o han sido temporales, debido a que RADIUS siempre ha sido un producto vivo, que se actualiza cada día. Durante los últimos años, esas limitaciones que favorecían a otros protocolos se han ido corrigiendo hasta ponerse a su altura. (Hansen, Fernandez Yago, 2008)

- Cuando se realizan modificaciones de configuración en el servidor RADIUS, por norma general hay que reiniciar el servicio para aplicar esas configuraciones. Otro problema relacionado es que RADIUS no mantiene estados, es un protocolo "stateless" que si se para el servicio, no recuerda el estado anterior, perdiendo las transacciones pendientes, configuraciones de usuarios, arqueo, etc.

- Uno de los principales puntos débiles de RADIUS está en el sistema de proxying, que obliga a un paquete RADIUS que es reenviado a otros servidores Proxy a volver por el mismo camino hacia el suplicante, pasando por todos los hops (saltos) que haya recorrido hasta llegar al suplicante. Esto implica retardos en el transporte y una débil seguridad pasando por toda la información por cada uno de los servidores Proxy que podría capturarla. Por eso es muy importante que se mantenga muy bien controlada toda la cadena de confianzas e incluso utilizar túnel como VPN entre cada nodo y el siguiente. También se puede enviar por túnel la relación entre un NAS y un servidor, si el NAS puede actuar como cliente o servidor VPN.

- Desde sus inicios se ha comentado que el diseño de RADIUS tiene problemas de crecimiento para instalaciones muy grandes, donde sufre de degradación de rendimiento y pérdida de paquetes por no disponer de sistemas de control de la congestión de la red.

- A diferencia de protocolos como Diameter, RADIUS trabaja en modo cliente-servidor y no peer-to-peer (par a par) lo que incapacita al servidor para iniciar conversaciones con el cliente, por ejemplo para rescindir un servicio del que el usuario está siendo uso. Aunque las extensiones de autorización dinámica solventan bastaste este problema.

3.2.9.1 El Estándar 802.1X.

808.1X no es un protocolo de comunicaciones, sino una extensión del sistema de autenticación RADIUS, a las capas más bajas de una red. 802.1X es una gran novedad en la implementación de redes. Cuando hablamos de seguridad en las capas más bajas de la red, hablamos de la capa 2 o capa de enlace. El campo de actuación de 802.1X es la capa de enlace en redes cableadas o inalámbricas, para asegurar la

conexión de dispositivos a la infraestructura de red de la organización. El procedimiento de conexión utilizado por este estándar se basa en la provisión de un sistema de autenticación por puertos en los que se establece un canal o puerto blindado de comunicación entre el suplicante y el NAS a fin de permitir únicamente su autenticación.

3.2.9.2 Estándar 802.1X.

Hasta la creación de este estándar, cuando un intruso ganaba acceso al cable de conexión de una red de datos o en la cobertura de la red inalámbrica, todas nuestras infraestructuras de red quedaban en situación de riesgo. A partir de esa conexión al cable de red o a la red inalámbrica de nuestra organización, el intruso o hacker tenía grandes posibilidades de interceptar todo tipo de información relacionada con la organización. Muchos administradores de red, en la práctica, basan su seguridad en el perímetro de la red, pero una vez dentro la preocupación de blindar cada uno de los equipos interiores no les preocupaba tanto.

La seguridad de las redes se basa en los siguientes conceptos:

- **Control de Acceso o Control de Admisión.** La seguridad en el acceso a la red es un punto de gran importancia, debiéndose denegar totalmente el acceso a la red, a cualquiera que no esté autorizado a acceder. El control de acceso a la red debe igualmente ser muy restrictivo con los servicios a los que esté autorizado a utilizar el usuario o equipo solicitante.
- **Privacidad**: La privacidad es otro punto vital para evitar la interceptación de los datos trasmitidos por un usuario o equipo, que esté utilizando como medio de transporte una red de datos. Gran parte de la información que viaja por la red se transmite en texto en claro, a pesar de ser información privada y sensible. La privacidad siempre se debe basar en la encriptación o cifrado de las comunicaciones en las capas 2 y 3 del modelo OSI.

- **Autenticación y Autorización**: La autenticación y autorización son el motor que va a permitir llevar a cabo, de forma íntegra, los dos puntos anteriores. La autenticación debe asegurar los medios para si propia integridad, impidiendo la interceptación de la credenciales o lo intentos de penetración no autorizados. La autorización se ocupará de limitar el uso del canal y de los recursos por parte del equipo o usuario.

La seguridad de una red Ethernet, siempre ha comenzado en las capas superiores, desde la capa 7 y descendiendo. Cuando entramos en el correo o en una pagina http nos autenticamos en la capa de aplicación, al igual que cuando establecemos una sesión SSL. El gran invento de las VPN, que nos dan un gran soporte de seguridad en las comunicaciones punto a punto, es permitir que trabajen en la capa tres (red). Los protocoles mas comunes que trabajan sobre esta capa son IPSec, PPTP, etc. Su implantación es también bastante compleja. El problema de trabajar sobre sistemas VPN como IPSec es que sólo garantizan la seguridad sobre el protocolo IP en la capa tres y superiores, dejando abierto el tráfico de otros protocolos de la capa tres y de los protocolos de autenticación, que actúan sobre la capa dos.

802.1x, estándar necesario para garantizar la seguridad a partir de la capa dos del modelo OSI. La importancia de denegar el acceso a la capa de enlace (y a la red en sí misma) si no se ha cumplido previamente con el proceso de autenticación, es algo que se va a presenciar en el transcurso del tiempo. La seguridad en la capa de enlace provee de los mecanismos necesarios para viabilizar los procesos de autenticación y envíos de trama de control. Todo esto es lo que se conoce como la seguridad en la capa de enlace (Link Layer Security) que además expande esa seguridad a todas las capas superiores. Si aplicamos la

seguridad 802.1x a las tecnologías inalámbricas, conseguiremos unas redes WLAN seguras y blindadas.

A la 802.1x se le llama comúnmente ESPOL (Extensible Authentication Protocolo over Lan) o EAP sobre Ethernet. Si lo aplicamos a tecnologías inalámbricas se suele llamar EAPoW (EAP over Wireless). EAP es el protocolo de transporte de la autenticación nativo de 802.1x, ya que trabaja contra servidores de autenticación sobre tramas Ethernet, lo que permite trabajar en la capa dos del modelo OSI (Capa de enlace de datos o capa MAC). También se define como un sistema de autenticación basado en puertos puesto que el control de admisión se realiza a través de puertos virtuales LAN.

Un equipo NAS que trabaje sobre 802.1x emplea un sistema virtual de dividir cada puerto físico LAN (PAE Port Access Entity) en dos puertos virtuales, un puerto controlado y un puerto incontrolado (controlled port & uncontrolled port). Desde el momento de la conexión de un dispositivo al puerto físicos LAN hasta el momento en el que se produzca una autenticación exitosa, sólo el puerto virtual incontrolado esta abierto. Y este puerto incontrolado solamente permite el paso de paquetes del tipo ESPOL a fin de permitir el proceso de autenticación del suplicante.

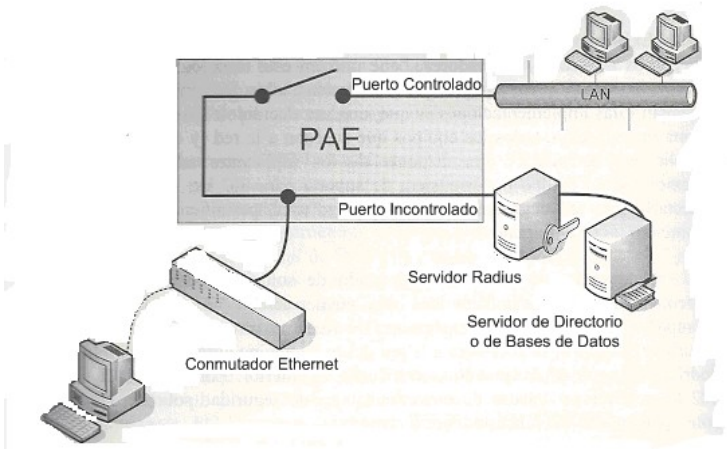

Figura 3.16 Estado de Puerto 802.1X
Fuente: Hansen, Fernandez Yago, 2008

Una vez que el suplicante se haya autenticado exitosamente, el puerto pasa a un estado autorizado o "controlado" y se abre para ese dispositivo. Cuando está abierto, el equipo autorizado puede pasar simplemente a hacer uso de la red, de forma normal. A través del proceso de autorización, que gestiona el servidor RADIUS, se le pueden asignar al suplicante características como una dirección IP estática/dinámica de un ámbito definido, o simplemente dejar a ese equipo en una red virtual (VLAN), segmentando la red en diferentes partes para diferentes usos. Por ejemplo: un equipo de recepción de un hotel que acaba de arrancarse se conecta automáticamente mediante su suplicante al switch de la red (compatible 802.1x) y tras el proceso de autenticación contra RADIUS, se le asigna una dirección IP reservada para él y se le abre el puerto, aislándola en una VLAN del departamento de recepción, en la que solo coexisten los equipos de recepción y la puerta de enlace para conectarse a Internet. Las redes VLAN trabajan en la capa 2 y 3 de OSI y necesitan enrutamiento IP. La Fig. 3.17 muestra la configuración para un usuario, al que vamos a asignar una VLAN en el momento de la conexión:

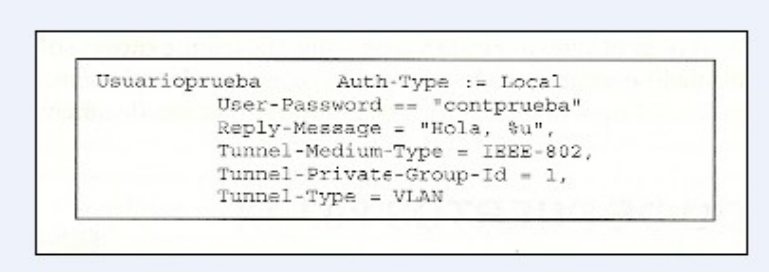

Figura 3.17 Configuración de usuario.
Fuente: Hansen, Fernandez Yago, 2008

Existe una gran variedad de modelos de equipos de NAS como switches de red, puntos de acceso, enrutadores… que utilizan esta tecnología para su propio acceso a la red o el de los equipos que se conecten a ellos. Si bien, un problema que presentan estas implementaciones es que, una vez decidido el uso de este estándar en una organización, todos los equipos que accedan a la red deben cumplir este estándar, o sea disponer de los suplicantes adecuados para su conexión. Si un equipo no

dispusiera de soporte para 802.1x, y tuviéramos que conectarlo a la red degradaríamos la seguridad total, permitiendo su acceso.

Este estándar puede ir acompañado de soluciones de encriptación de trafico, en caso de redes inalámbricas como puede ser WPA2 o similares. Si no va acompañado de encriptación en la capa de Red, no ofrece el cien por cien de seguridad, ya que si se accediera a la red desde un equipo autorizado para hacerlo, podríamos seguir interceptando el tráfico en su interior. Por lo tanto el uso de 802.1x no excluye del uso de otras soluciones de seguridad sobre la capa tres, como puede ser VPN de tipo IPsec o similares.

Las nuevas tecnologías Wi-Fi recomiendan el uso del protocolo 802.1x en las redes corporativas. Para ello utilizan un estándar conocido como 802.11i, que definitivamente mejora el concepto de seguridad en Wi-Fi y que la Wi-Fi Alliance certifica como "WPA2 Enterprise". El intercambio de contraseñas de autenticación y el posterior proceso de cifrado del canal de trasmisión hacen por fin a estas redes lo suficientemente robustas para evitar la intrusión o interceptación de datos.

Lo que hay detrás de las tecnologías 802.1x no es sino un servidor de autenticación, en la mayor parte de los casos RADIUS, que gestiona todo el sistema AAA contra los suplicantes, a través del equipo NAS. Esta autenticación se realiza de forma muy segura, utilizando sistemas vía túneles basados en certificados PKI, como EAP-TLS, EAP-PEAP u otros. Se puede, aunque no se recomienda, utilizar versiones más débiles de EAP como EAP-MD5, ya que esto descendería el nivel de seguridad general. De esa manera el incremento de seguridad es máximo, creando un sistema de autenticación bidireccional (mutua) donde el servidor identifica al cliente y el cliente identifica al servidor. Así se evitan graves riesgos de seguridad, como la posible existencia de *rogue-AP* actuando como MiTM (Man in The Middle). Este tipo de autenticación además de autenticar al usuario puede hacer lo mismo con el equipo, por lo que se puede disponer de un certificado de equipo para poder entrar en la red.

RADIUS utiliza en este caso una tecnología que proporciona autenticación, integridad de datos y privacidad, a través del protocolo 802.1x.

Esto ha sido cambiado en los últimos años el concepto que se tenía de la seguridad, ya que ahora se busca la seguridad en el control de acceso al medio y los cortafuegos suben la seguridad hacia las capas más altas (capa 7), cuando antes se basaban en el filtrado de puertos en las capas mas bajas.

Una infraestructura 802.1x basada en PKI puede disponer de x equipos que se conectan a la red, que disponen de x certificados de equipos. Además cada usuario dispone de las credenciales necesarias para autenticarse contra la red. La administración de estas infraestructuras es un poco más tediosa, pero el resultado incrementa la seguridad general de forma notable. Quizás el hecho de que su implantación sea un poco más compleja es lo que haya causado que, desde su publicación, su implantación en el mercado esté siendo más lenta de lo provisto.

Otro motivo que ha dificultado la extensión de 802.1x ha sido la falta de disponibilidad de programas suplicantes adecuados y robustos. Microsoft dispone de un suplicante 802.1x en sus versiones Windows XP y 2000 SP4 pero tiene algunos problemas de diseño. Uno de esos problemas es la necesidad de activar el servicio WXCS (servicio de configuración inalámbrica rápida) para disponer de la autenticación 802.1x, aunque sea para una tarjeta Ethernet LAN y no WLAN. Este servicio suele gustar a pocos administradores, y muchos suplicantes para tarjetas inalámbricas tienden a deshabilitarlo, con lo que se deshabilita también el suplicante para redes cableadas. Otro de esos problemas es el propio diseño de las fases de autenticación entre el suplicante 802.1x y el propio sistema de login de Windows hacia un servidor de dominio Kerberos o de directorio activo. Windows pretende autenticarse contra su servidor de dominio, antes de hacerlo contra la red 802.1x, pero su servidor de dominio no estaría disponible hasta que la red estuviera disponible, todo un caos de intentos infructuosos de registro. Para evitar este caos de

autenticación, las soluciones pasan por hacer disponible al servidor de dominio en una red virtual VLAN abierta, con los graves problemas de seguridad que eso conlleva; también se puede cambiar un suplicante de otro fabricante, libre o de pago.

El estándar 802.1x se recoge en el RFC 3580 (IEEE 802.1x RADIUS Usage Guidelines) el estándar IEEE 802.11i ratificado en 2004 está incluido en el RFC 4017.

3.2.1.0 Estructura de las Comunicaciones EAP.

A continuación se presentará la estructura de un paquete de datos EAP, similar a la estructura de un paquete RADIUS, y la forma en la que se establece una comunicación completa sobre este protocolo.

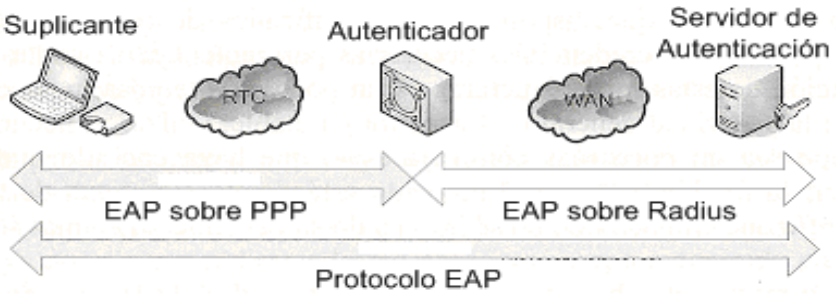

Figura 3.18 EAPOL y EAP sobre RADIUS.
Fuente: Hansen, Fernandez Yago, 2008

3.2.10.1 Formato de mensaje EAP. Paquete de datos.

La Fig.3.19 se muestra una estructura genérica correspondiente a un paquete EAPOL sobre 802.3/Ethernet.

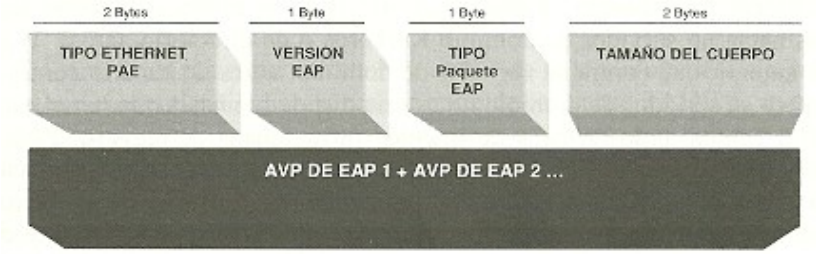

Figura 3.19 Paquete EAPOL sobre 802.3/Ethernet.
Fuente: Hansen, Fernandez Yago, 2008

- **Tipo Ethernet de PAE (Port Access Entity Ethernet Type)** (2 byte) – Es un campo utilizado para describir el tipo de protocolo Ethernet que utiliza el puerto del NAS implicado.

- **Versión de EAP (Protocol Versión)** (1 byte) – Un número positivo en formato binario que representa el método de autenticación EAP que se está utilizando.

- **Tipo de paquete EAP** (1 byte) – Un número positivo en formato binario que representa el tipo de mensaje EAP incluido. Sus valores pueden ser:

    - **EAP-packet** (Paquete de intercambio de datos del protocolo EAP)

    - **EAPOL-Start** (Inicio de las comunicaciones EAP, estímulo, desde el suplicante al NAS)

    - **EAPOL-Logoff** (Desconexión, el suplicante desea desconectar y envía al NAS este mensaje)

- **EAPOL-Key** (Para el intercambio de claves de cifrado en sesiones posteriores de protocolos que requieren cifrado como WPA o vía túnel VPN).

- **EAPOL-Encapsulated-ASF-Alert** (Para el intercambio de alertas en protocolos como SNMP).

- **Tamaño del cuerpo (2 bytes)** – Valor entero sin signo que representa el tamaño en bytes del cuerpo del paquete, donde se incluyen los valores.

- **Cuerpo del Mensaje**. En el cuerpo del mensaje se incluyen los valores y atributos de tipo EAP. Este campo sólo estará presente en los mensajes de EAP tipo: EAP-Packet, EAPOL-Key y EAP-Encapsulated-ASF-Alert. El formato de los atributos de EAP es muy similar a los de RADIUS:

    - **Código** (1 byte). El código o tipo de atributo EAP.

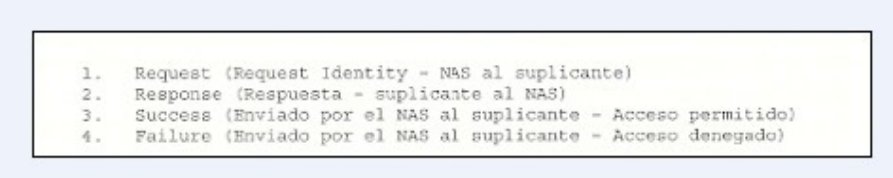

Figura 3.20 Atributo EAP.
Fuente: Hansen, Fernandez Yago, 2008

    - **Identificador** (1Byte). Al igual que en un paquete RADIUS, el identificador se utiliza para relacionar los paquetes y las sesiones entre sí.

    - **Tamaño** (2 Bytes). Señala el tamaño total del paquete EAP, incluyendo todos los campos de cabecera y cuerpo de mensaje.

- **Tipo de EAP** (1 Byte). Indica el tipo de autenticación EAP que se utiliza en la conversación. Muestro unos ejemplos entre ellos.

1. Identity (Intercambio de identidad)
2. Notification
3. NAK
4. MD5-Challenge
5. One Time password
6. Generic Token Card
13. TLS
21. TTLS
25. PEAP
29. MSCHAPV2

Figura 3.21 Tipo de autenticación EAP
Fuente: Hansen, Fernandez Yago, 2008

- **Datos del Paquete** (Tamaño – 5 bytes). El valor de datos que se está transmitiendo, que depende del tipo de EAP que se utilice.

3.2.10.2 Secuencias de autenticación EAP.

Es importante conocer la forma en la que se desarrolla una secuencia completa AAA basada en el protocolo de transporte EAP. No hay una formula universal para realizar esta secuencia, ya que dependerá de ciertos factores variables, como por ejemplo el tipo de EAP utilizado o de la capacidad de iniciar la conversación o no por parte del equipo NAS. En el caso de un conmutador que haga de autenticador, será este quien detecte que un equipo se conecta a uno de sus puertos, o que un equipo acaba de activarse o encenderse; pero en el caso de un AP inalámbrico que no tiene puertos físicos, el suplicante debe iniciar la conversación tras asociarse con el punto

de acceso mediante un mensaje EAPOL-Start, ya que el AP no es capaz de detectar al nuevo cliente de otra manera.

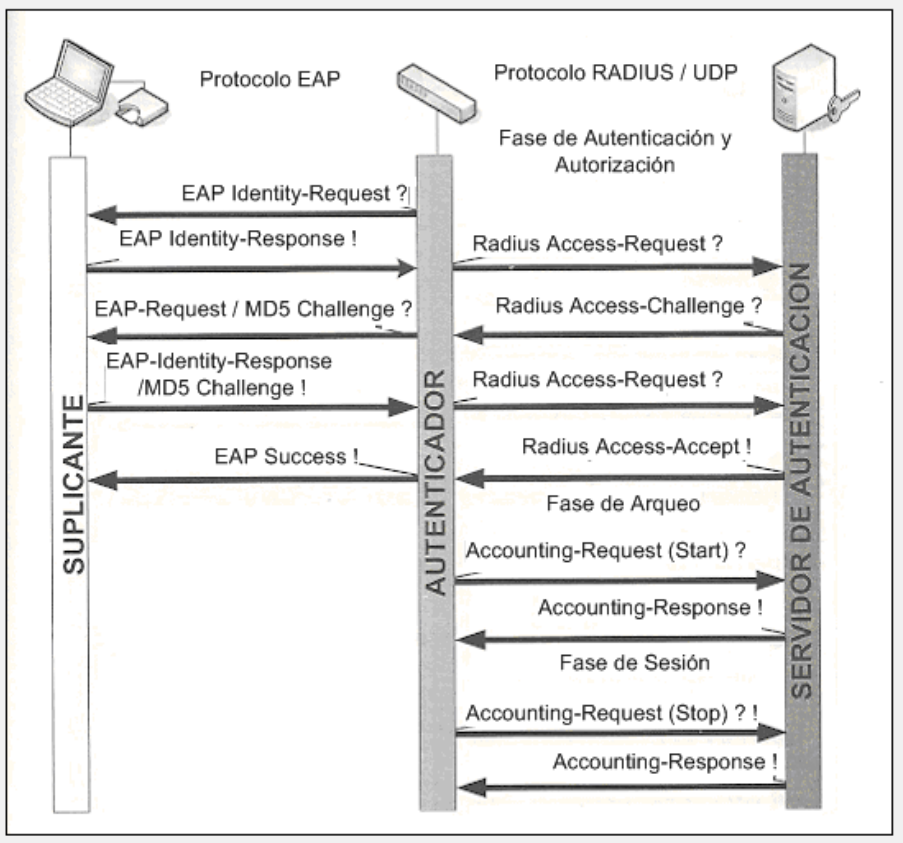

Figura 3.22 Secuencia de Autenticación EAP/MD5.
Fuente: Hansen, Fernandez Yago, 2008

En la ilustración anterior podemos ver una secuencia de autenticación estándar sobre el tipo de autenticación sobre EAP más básico: EAP-MD5. Lo podemos comparar con el método CHAP sobre RADIUS. Ninguno de estos tipos básicos de autenticación debe de ser utilizado, por motivos de seguridad, a no ser en entornos muy cerrados o blindados, como en el interior de un canal de comunicación por módem o cualquier otro canal enviado por túnel de alguna forma.

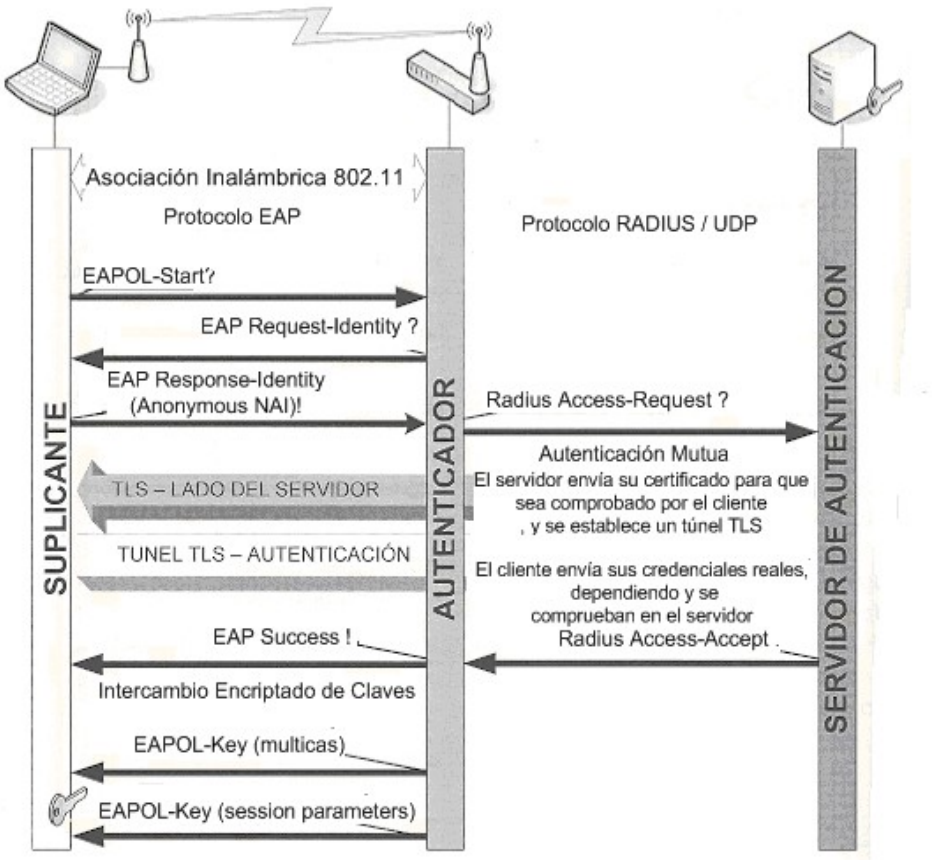

Figura 3.23 Secuencia de Autenticación EAP-PEAP-MS-CHAPv2

Detalle de la secuencia EAP-PEAP-MS-Chapv2:

0. Cuando el suplicante o el NAS se han detectado, la secuencia suele comenzar por un paquete EAPOL-Start, para indicar que se desea iniciar una conversación EAP.

1. Cuando el NAS (autenticador) detecta un paquete EAPOL-Start, cuando detecta la actividad del suplicante conectándose a uno de sus puertos, o

asociándose a 802.11, envía un paquete EAP tipo “EAP-Request/Identity” al suplicante.

2. El suplicante responde mediante un paquete de tipo “EAP-Response/Identity” con su identidad (en PEAP debe ser anónima en esta fase). El NAS envía este paquete EAP encapsulado en forma de atributo EAP-Message dentro de un paquete UDP estándar de RADIUS.

3. El servidor RADIUS solicita un desafío o challenge al NAS, dependiendo del método de autenticación EAP demandado y disponible. El NAS realiza su misión de desencapsular y encapsular los mensajes tipo RADIUS a EAP y se lo envía al suplicante. Se producen intercambios de paquetes Challenge, dependiendo del método EAP y del tipo de autenticación mutua.

4. El suplicante responde a los mensajes Challenge a través del NAS, que siempre encapsula todos los mensajes EAP en formato RADIUS y se los envía al servidor RADIUS.

5. Tras los procesos necesarios para la creación del túnel e intercambios de identidades y si además cada uno de los procesos de autenticación, dentro y fuera del túnel, se ha superado correctamente, el servidor RADIUS responderá con un mensaje Access-Accept enviado al NAS con todos los parámetros necesarios de autorización para permitir el acceso del puerto del cliente. El NAS responderá al suplicante con un mensaje EAP-Success.

6. Se produce (en caso de VPN o red inalámbrica Wi-Fi) el intercambio de las claves de sesión necesarias para que se establezca un correcto cifrado durante la consiguiente sesión segura del usuario a la red.

Estos procesos descritos anteriormente pueden variar ligeramente o drásticamente, dependiendo del tipo de EAP que se decida implantar; pero la teoría es la misma para cualquiera de los intercambios de paquetes entre los diferentes componentes.

3.2.10.3 Modelos de implantación.

Se muestra en la Fig.3.24 un modelo típico y simple de implantación de una infraestructura basada en 802.1x, mediante certificados autofirmados. En la zona segura de la red se encuentra el servidor de autenticación RADIUS, el servidor de Directorio (LDAP, Active Directory, Base de Datos, etc.), el servidor de certificación (OpenSSL, Microsoft Certificate Server, etc) y un servidor para el acceso remoto por VPN. Esta zona de la red está protegida y a ella solo tienen acceso los equipos NAS y los administradores. Como equipo NAS, podemos ver un swtich o conmutador Ethernet compatible 802.1x para los usuarios cableados y un punto de acceso 802.11i que autentica contra RADIUS y certificados PKI. El servidor VPN también autentica contra el servidor RADIUS. En ambos ejemplos podemos ver un servidor RADIUS manteniendo toda la infraestructura basada en la autenticación AAA.

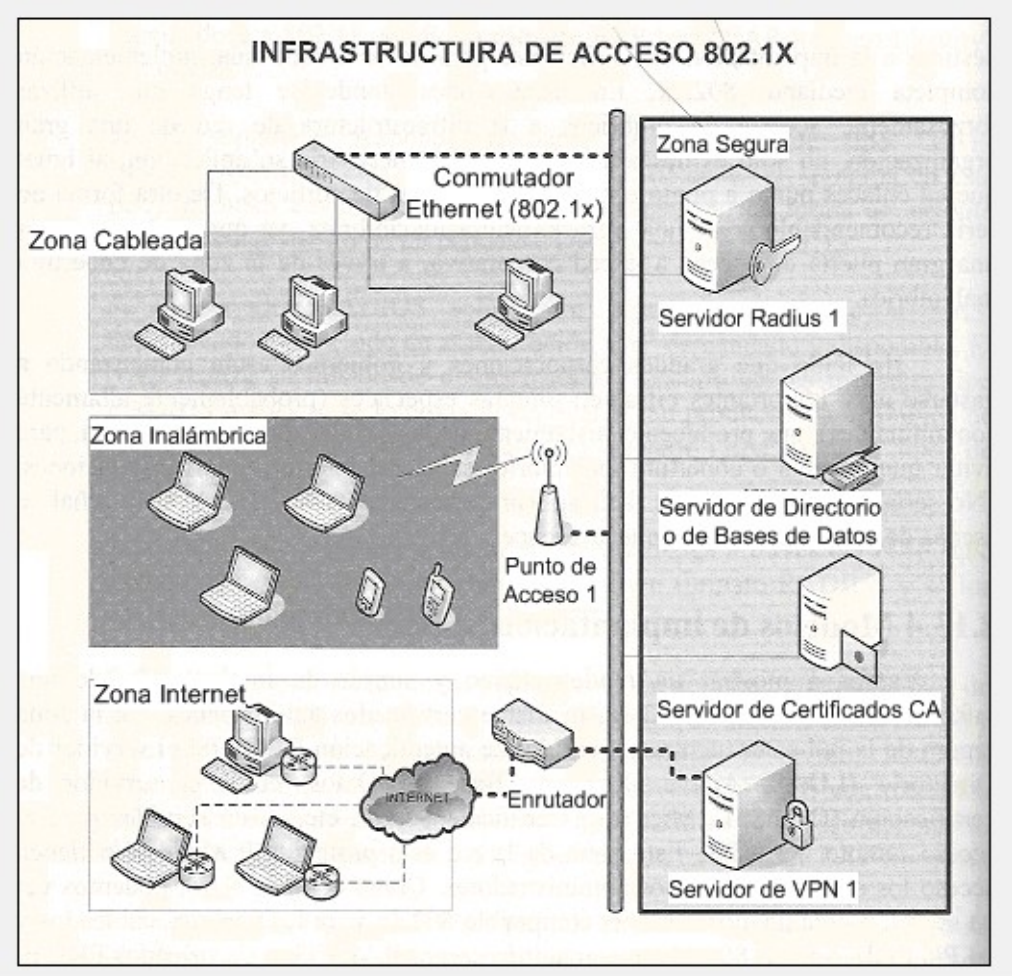

Figura 3.24 Infraestructura de acceso 802.1X.
Fuente: Hansen, Fernandez Yago, 2008

3.2.11 Wi-Fi

Uno de los motivos por lo que RADIUS está progresando de forma importante en estos últimos años es la gran implantación que está teniendo Wi-Fi y los aspectos de seguridad relacionados con esta tecnología. Las tecnologías inalámbricas, que han dado lugar a lo que hoy se conoce como Wi-Fi (Wireless Fidelity), se fueron desarrollando y cobrando popularidad en la década de los años 90. Wi-Fi es un conjunto de estándares certificados por una alianza independiente llamada Wi-Fi Alliance. Esta alianza se encarga de certificar a los fabricantes y a sus productos para

que se consideren homologados para esta norma. Loa estándares sobre los que trabaja Wi-Fi forman parte de la serie 802.11 del grupo IEEE y actúan sobre las capas uno y dos del modelo OSI.

La demanda tan grande que han tenido las redes Wi-Fi se basa en la comodidad y en la dificultad en muchos tipos de infraestructuras de utilizar redes basadas en el cable. Sustituir de forma taxativa el cable por la red inalámbrica no es factible, ya que cada tipo de red tiene su aplicación, además de sus ventajas e inconvenientes. A pesar de los atractivos números que venden los fabricantes de redes inalámbricas como índices de velocidad y de ancho de banda, cabe decir que estos equipos no cumplen ni de lejos las medidas ofrecidas, y que las medidas reales serán compartidas entre el número de equipos conectados.

Wi-Fi ha luchado con y contra el mercado comercial, viéndose obligada en muchas ocasiones a publicar partes de normativas o borradores antes de estar totalmente desarrollados y publicados. Esta excesiva premura en la utilización de normativas que suponen mejoras de velocidad y seguridad han llevado en ocasiones a crear un cierto caos en las especificaciones. A este tipo de normas se les suele llamar pre-draft.

No obstante, el estado actual de las redes inalámbricas a fecha de hoy ofrece un nivel muy adecuado de salud y seguridad. El problema que podemos encontrar en la actualidad no se debe tanto a un problema de capacidades de seguridad, sino que esta causado por deficiencias de instalación por parte de las compañías, proveedores y administradores. Podemos achacar estos problemas a la falta de formación, a la dejadez y a las carencias de servicio de todos estos participantes.

3.2.11.1 Conceptos de Wi-Fi.

Para lograr entender los conceptos y el lenguaje particular que utilizan las tecnologías Wi-Fi, se explica, su modo de funcionamiento.

- **AP. Punto de Acceso o Access Point**. Es el equipo de red (NAS), capaz de trabajar sobre una red de radiofrecuencia, que se utiliza para hacer de intermediario en las comunicaciones inalámbricas entre equipos o para convertir una red cableada en inalámbrica.

- **SSID**. El SSID (Service Set Identifier) es el nombre que se le asigna a una celda de red. Es un nombre de red para definir la red a la que nos vamos a conectar. Si la red es entre equipos (peer to peer) y no se produce intermediación de un equipo AP, se le denomina BSSID y si es una red de tipo infraestructura conectada a un punto de acceso se le llama ESSID. Este nombre de red se divulga por parte del AP mediante unos pequeños paquetes que se envían (unos 250 por minuto) con los datos de la red y sus características. Estos paquetes balizas se utilizan para localizar la red a la que queremos conectarnos y para medir su nivel de señal respecto a nosotros, además de para mostrar sus características.

- **Canal**. Dependiendo del tipo de red Wi-Fi y de su normativa, el espectro o espacio radioeléctrico asignado para el desempeño de estas redes se divide en canales. En el caso de redes 802.11b/g se divide en 14 canales, el uso de los cuales varía según las normativas légales de cada país. Estos canales fijan unas frecuencias fijas de trabajo para los equipos que los utilizan. Si bien existen hasta 14 canales, esto no significa que esos 14 canales permitan crear 14 redes simultáneas. Debido a la forma de funcionamiento de estas

tecnologías inalámbricas se puede utilizar hasta 3 ó 4 canales sin solapamiento.

- **Potencia** o cantidad de señal. El nivel de potencia de una señal se expresa usualmente en dBm (decibelios relativos a 1 mW). Cada uno de los componentes en la transmisión suma o resta potencia a la misma. Si el AP trasmite a una potencia de n dBm, hay que restar a su potencia inicial las atenuaciones causadas por el cable, los conectores y el medio (aire) que crean esas pérdidas.

- **Cobertura.** El área o la zona de cobertura de una estación (AP o cliente) lo determina la potencia de transmisión del equipo (medida normalizada por la legislación) y el tipo de antena que se va a utilizar, además de otros factores externos como las estructuras de las construcciones, el clima, etc. La cobertura se va reduciendo desde el trasmisor y a lo largo de la línea de transmisión hasta llegar casi a desaparecer o hacerse imperceptible. El control de la cobertura en el diseño de las infraestructuras inalámbricas es una de las tareas más complejas y duras, pero más importante para su estable funcionamiento.

- **Antenas**. Cada antena tiene un diseño diferente, existiendo gran variedad de diseños y tipos. La ganancia de una antena se considera pasiva, ya que no agrega potencia a la señal, sino que la dirige en mayor grado hacia un ángulo concreto. Según la direccionalidad de la antena ésta se puede clasificar en varios grupos:

    - **Isotrópica**. No es un diseño real de antena, sino simplemente teórico. Es la antena perfecta que transmite a igual potencia en todos los ángulos, creando una proyección en forma de esfera. De ella parte el

valor dBi que especifican todas las antenas. Este valor significa decibelios en relación a una antena isotrópica.

- **Omnidireccional**. Sería el diseño más parecido a una antena isotrópica. Transmite en horizontal o vertical hacia todos los ángulos. Su proyección tiene forma de dona, aunque puede variar su altura con respecto a su distancia de cobertura.

- **Direccional**. Enfocan mayoritariamente la señal hacia ángulos más concretos, evitando que se disperse hacia todas partes. Dependiendo del ángulo de enfoque pueden ser semi direccionales o de alta direccionalidad como las antenas de tipo yagui o parabólicas.

- **Velocidad y ancho de banda**. Si bien la velocidad a aumentado considerablemente desde sus primeros diseños y sus técnicas de trasmisión y recepción son muy avanzadas, los números, que pueden impresionar bastante, no tienen una estrecha relación con la realidad. El ancho de banda de una red es el valor de cantidad de datos contenidos (y no de balizamiento y control) transmitidos por segundo.

- **Seguridad**. En redes inalámbricas no hablamos directamente de algoritmos de encriptación y cifrado a la hora de configurarlas, ya que lo que se utiliza son kits de seguridad (que incluyen todas las técnicas necesarias para crear una conexión segura), como WEP o WPA.

3.2.12.2 Secuencia de conexión Wi-Fi.

Resulta indispensable conocer la secuencia de intercambios que se produce en la conexión de una estación con un punto de acceso, para poder entender su configuración y la depuración de los errores que puedan surgir.

En la secuencia siguiente se puede observar cada uno de los pasos que se producen durante la conexión de una estación a un AP. Dependiendo del tipo de autenticación y asociación utilizada, la secuencia puede variar de forma importante. Pero en ella se muestran los dos principales estados que puede tener un cliente con respecto a un punto de acceso: autenticado y asociado. Esto dos procesos son independientes el uno del otro, ya que se pueden producir situaciones donde una estación esté asociada pero no autenticada o autenticada pero no asociada. O incluso si la autenticación y la asociación son abiertas, la estación podría estar autenticada y asociada pero, por no conocer su clave de cifrado, no podría comunicarse de forma inteligible con el AP.

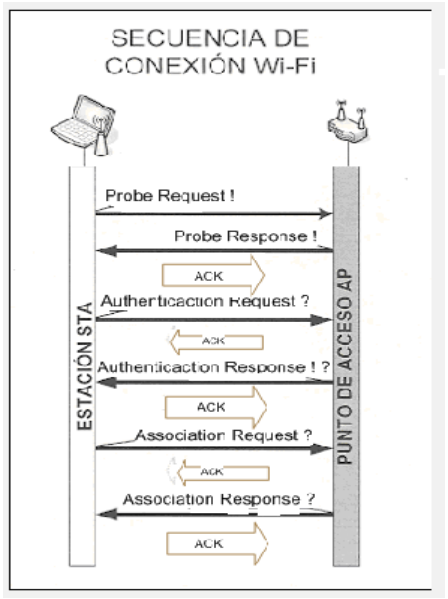

Figura 3.25 Secuencia de Conexión Wi-Fi.
Fuente: Hansen, Fernandez Yago, 2008

3.2.11.3 Estructura de una red Wi-Fi.

Las redes Wi-Fi definen varios modelos de estructura dependiendo de su diseño y topología:

- **BSS**. Basic Service Set, llamado también celda. Es una modalidad de infraestructura, ya que esta basada en una red centralizada sobre un punto de acceso. El punto de acceso (AP) hace de mediador en todas las comunicaciones. En la Fig. 3.26 cada una de las tres estaciones (STA1, STA2 y STA3) sería incapaz de comunicarse con cualquiera de las restantes ya que no esta en su rango de cobertura directa. Sin embargo al hacer el punto de acceso de intermediario en las comunicaciones (que sí esta en el rango de las tres estaciones) se pueden establecer correctamente las comunicaciones entre todos los componentes. Normalmente el AP está conectado con la red cableada y las comunicaciones hacia la red cableada pasan por uno o más puertos Ethernet de los que dispone.

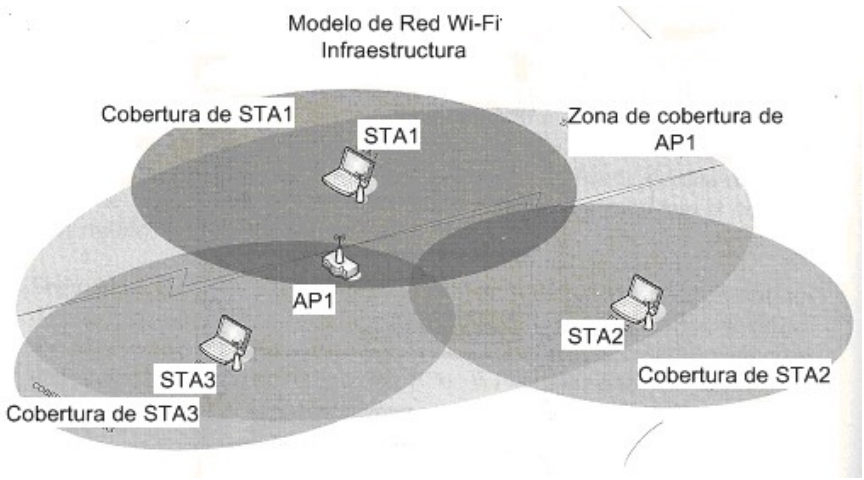

Figura 3.26 Modelo de Red Wi-Fi Infraestructura.
Fuente: Hansen, Fernandez Yago, 2008

- **ESS**. Extended Service Set. El ESS es el diseño que se utiliza en infraestructuras mayores. No solamente existe un AP, sino dos o más que están conectados entre sí mediante red cableada, aunque pudieran estar conectados mediante puentes inalámbricos. Las estaciones pueden realizar itinerancia (roaming) por la red, decidiendo en cada caso a qué AP se conectan dependiendo del nivel de la señal. Los AP pueden utilizar ESSID distinto o iguales, aunque lo habitual es que sean iguales para permitir el roaming. Se utilizan canales distintos para los diferentes AP.

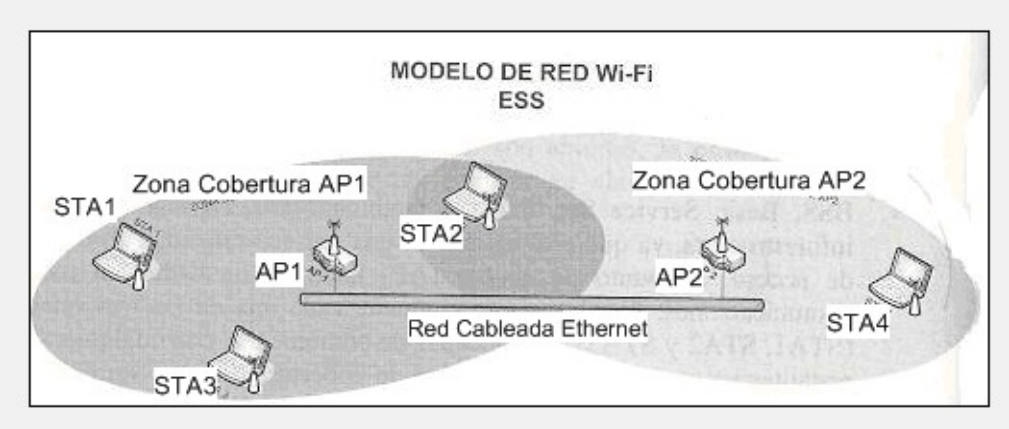

Figura 3.27 Modelo de Red Wi-Fi ESS.
Fuente: Hansen, Fernandez Yago, 2008

- **IBSS**. Independent Basic Service Set. El tipo más sencillo, pero también el menos utilizado, es el tipo ad-hoc (peer to peer) en el que cada uno de los componentes o estaciones (STA) se comunica con el que desea contactar de forma directa. Este diseño utiliza el mismo canal de radio para todas las estaciones. Existen muchos inconvenientes en este tipo de redes, pero el más habitual es la cobertura de las tarjetas inalámbricas, que no permite demasiada distancia entre los equipos. La comunicación se mantiene viva mediante el envío de beacons entre los equipos.

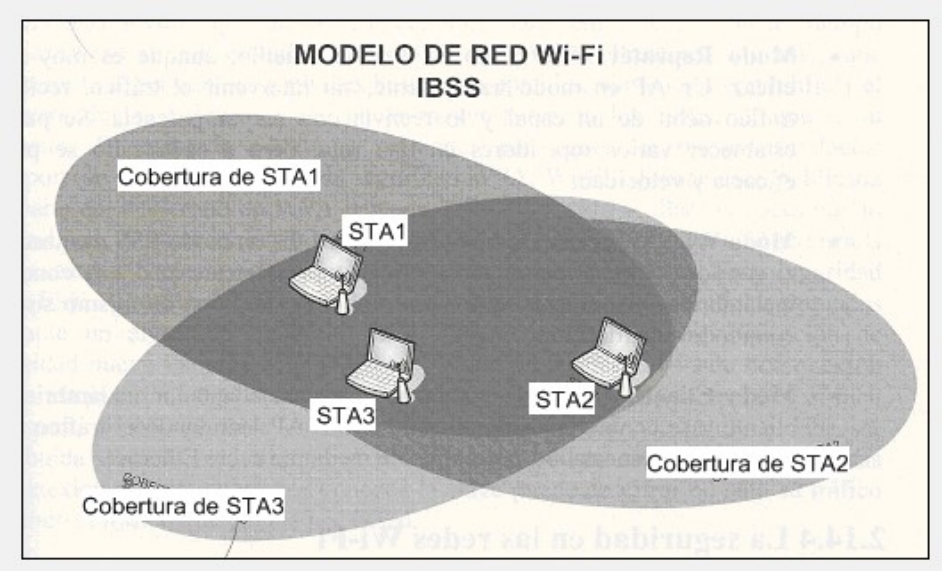

Figura 3.28 Modelo de Red Wi-Fi IBSS.
Fuente: Hansen, Fernandez Yago, 2008

Existen otros modos avanzados de operación del AP, que dependen del modelo de AP y de su gama. Inicialmente un equipo que funcionara como Bridge se denomina Bridge inalámbrico, al igual que un repetidor era un repeater inalámbrico, y no se llamaban AP, pero actualmente la tecnología y el firmware de los equipos permiten que el mismo pueda desarrollar diferentes funciones mediante cambios en su configuración.

- **Modo Bridge**. Es un modo puente en el que se conectan dos AP (ambos conectados a la red inalámbrica) y trasladan todo el trafico de una red cableada a la otra mediante un enlace inalámbrico transparente. Se suele utilizar para conexiones punto a punto o multipunto inalámbricos en enlaces entre diferentes edificios o zonas.

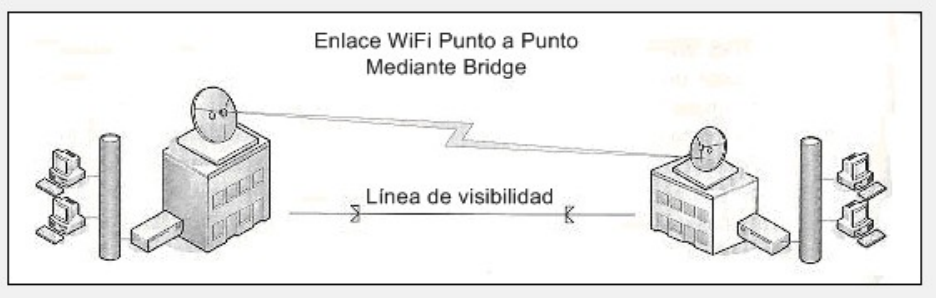

Figura 3.29 Enlace Wi-Fi Punto a Punto mediante Bridge.
Fuente: Hansen, Fernandez Yago, 2008

- **Modo Repeater**. Este modo es el más sencillo, aunque es muy poco eficaz. Un AP en modo transparente, sin intervenir el tráfico, recibe el tráfico débil de una canal y lo reenvía con mayor potencia. Se pueden establecer varios repetidores en una ruta, pero a cada salto se pierde eficacia y velocidad.

- **Modo WDS** (Wireless Distribution System). Es un modo ESS avanzado en el que los AP están conectados entre sí (normalmente mediante conexión inalámbrica) y son capaces de crear una única red con un mismo sistema común de autenticación.

- **Modo Cliente**. El AP se comporta como un adaptador inalámbrico de cliente y se convierte en un cliente de otro AP, enrutado el tráfico a los ordenadores conectados, normalmente mediante cable Ethernet.

3.2.11.4 Seguridad en las redes Wi-Fi.

Las primeras redes inalámbricas carecían totalmente de seguridad. No existía una preocupación por aspectos como la escucha, espionaje o interceptación de datos. Cuando ya estaban bastante extendidas, con el consiguiente desconocimiento de esta nueva tecnología por parte de los usuarios, se empezó a extender, su falta completa de

seguridad. Por ello, se produjo un importante descenso en las ventas e instalaciones, alegando graves problemas de seguridad.

A partir de ese momento, surge el estándar de seguridad WEP (Wire Equivalent Privacy), que se conocía como privacidad equivalente a las redes cableadas, incorporando la autenticación del usuario y la encriptación posterior de las sesiones. A lo largo de los siguientes años, en relativamente muy poco tiempo WEP (que utiliza el algoritmo de encriptación RC4) fue atacado y roto por parte de los hackers. Cada día que pasaba se encontraba métodos más veloces y eficaces para su ruptura, por lo que volvió a ser bastante ineficaz y se precisaba de otros métodos más fiables. La implantación de WEP ha sido tan extensa que actualmente todavía queda un amplio porcentaje de redes inalámbrico que utiliza este sistema.

Tras demostrar sus vulnerabilidades, WEP tenía que claudicar ante un sistema más seguro, que debería aparecer inmediatamente. Se llevaba un tiempo trabajando sobre un estándar llamado WPA (Wi-Fi Protected Access), que mejoraría la seguridad hasta niveles bastante aceptables, sin tener que modificar el hardware de la tarjeta de red en la mayor parte de los casos, aunque sí su firmware. El mercado volvió a presionar para que los nuevos productos incorporaran el nuevo estándar de seguridad WPA. Wi-Fi Alliance sacó publicada una parte del desarrollo de WPA llamada WPA-PSK para acallar las voces que lo demandaban, aunque el estándar completo debía incorporar seguridad avanzada para entornos corporativos y ésta todavía no estaba terminada. Esta seguridad WPA-PSK (Pre-Shared Key) incorpora unos niveles de cifrado apropiados mediante un algoritmo mejorado RC4 dinámico (TKIP), una verificación de integridad nueva llamada MIC (Michael) y una protección mediante desconexión contra ataques. Este tipo de seguridad basada en una clave pre-compartida, si bien es segura, no es aceptable en un entorno empresarial, donde la clave debe ser distribuida y puede ser comprometida fácilmente, ya que ésta es igual para todas las conexiones. Cualquiera que conozca la clave puede descifrar no solo su tráfico sino todo el tráfico que circula por la red.

Cuando estuvo totalmente finalizado el estudio (2004) se publicó la norma 802.11i que significaba la aplicación completa de la norma 802.1x para Wi-Fi, además de otros tipos de cifrado como CCMP sobre bloques de AES y la norma PMK (Pairwise Master Key) para facilitar el roaming entre puntos de acceso. A esto se le llamó WPA2, que separa dos tipos de infraestructuras: WPA2-Personal basada en PSK y WPA2-Enterprise basada en 802.1x. La inclusión de esta norma en los equipos fabricados desde su publicación es obligatoria si desean estar certificados por Wi-Fi Alliance. Actualmente la implementación de esta norma de forma adecuada y correcta garantiza al completo la seguridad de los datos enviados y recibidos por una red local. Esta nueva implantación completa de seguridad implantada por 802.11i se conoce como RSN (Robust Security Network).

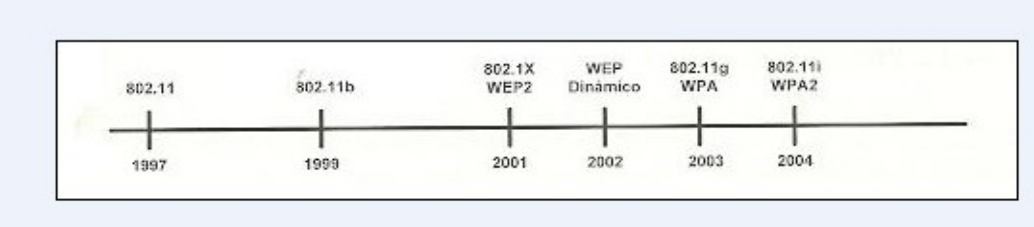

Figura 3.30 Evolución en el tiempo de la seguridad en redes inalámbricas. Fuente: Hansen, Fernandez Yago, 2008

No obstante cabe remarcar que muchas de estas implementaciones de seguridad han ido apareciendo de forma anticipada y muchos fabricantes han implementado las normas provisionales o incluso sus propios desarrollos, con lo cual es muy fácil ver tipos de cifrado y encriptación que no corresponden a un modelo de seguridad como WPA con AES, WEP Dinámico o WEP+ u otros tipos híbridos.

3.2.11.4.1 Hacking WI-FI.

Actualmente existen muchas técnicas y programas especializados en extraer información o averiguar las claves de acceso de las redes inalámbricas. La cultura de

obtener banda ancha gratis desde la casa, se ha ido propagando por todo el territorio, creándose técnicas muy sencillas para conseguir acceder a redes ajenas.

Muchas personas e incluso empresas responden a esto que el problema consiste en la pérdida de ancho de banda, pero nada más lejos de la realidad. Utilizar una red ajena para el acceso limpio a Internet no interfiere demasiado la actividad de la empresa, pero si el uso que se está haciendo de Internet es fraudulento o ilegal, todas las operaciones realizadas quedarán registradas con la marca de la dirección IP pública que está utilizando la organización o individuo.

Esto, sin contar con que una vez que el hacker haya accedido a la red Wi-Fi, significa de igual manera que ha accedido a la red cableada y por tanto está en el interior de la organización, con la capacidad de interceptar todo tipo de información privada y de claves de acceso. Resulta necesario, en todos los casos, evaluar los riesgos que conlleva un acceso ilícito al interior de la empresa.

3.2.11.4.2 Protegiendo WI-FI.

Proteger una red Wi-Fi es una tarea simple, si se respetan todas las reglas del juego. Para un usuario doméstico, quizás sea más complejo llegar a un óptimo nivel de seguridad que para una organización.

Para crear esa red de tamaño medio/alto completamente segura debemos implementar un sistema basado en la autenticación AAA, mediante un servidor RADIUS y una base de datos de usuarios.

Como medida de seguridad, las organizaciones deben evitar el uso de algoritmos generadores de claves y credenciales, como los que usan algunas compañías de servicios de acceso para sus clientes y equipos.

3.3 CA. Autoridad Certificadora.

La autoridad certificadora es la entidad responsable y capaz de la emisión de certificados y del mantenimiento de toda la infraestructura PKI. Esta entidad debe generar la confianza necesaria para resultar suficientemente confiable para todos los participantes en el proceso. Para que esta resulte confiable, su infraestructura debe ser lo suficientemente segura para que no pueda ser comprometida. A partir de la emisión de un certificado, el motor que mueve todo el sistema se basa en la confianza hacia la entidad emisora de ese certificado. Los clientes de PKI (usuarios, equipos, etc) mantendrán a esa entidad CA en sus listas de confianza. Para el uso de la infraestructura PKI es necesario que las confianzas entre todos sus participantes sean recíprocas.

Su misión consiste en el mantenimiento y gestión de la infraestructura necesaria para realizar sin riesgo todas las labores de PKI. Para ello CA es la responsable de la emisión de los certificados firmados, de su registro y control de caducidad y renovación, además de su revocación en caso necesario. Para ello los certificados emitidos se almacenan en los almacenes o repositorios de certificados que pueden ser directorios, o bases de datos. Si bien los repositorios de certificados deben ser accesibles por cualquiera que desee consultar sus datos a fin de poder hacer uso de una clave pública de alguien para poder enviar datos o comprobar una firma, esto choca en cierta medida con las actuales leyes de protección de datos, por lo que la consulta y almacenamiento de esta información estarán regulados por estas leyes.

En los casos de pequeñas organizaciones, una CA puede estar desconectada del resto de la red, emitiendo y gestionando certificados en modo off-line. Sin embargo el problema se produce cuando se precisa de un mecanismo de control para

la revocación de certificados comprometidos; en este caso se debe disponer de una lista de revocación de certificados en línea para su comprobación. En otros casos, una CA corporativa se encentra en modo on-line para la emisión, comprobación y revocación de certificados.

Los certificados emitidos por una CA contienen la clave pública de la CA, y están firmados digitalmente por esta CA mediante su clave privada de entidad emisora. Esa clave pública de CA está disponible públicamente para que pueda ser comprobada por aquellos que realicen operaciones con ese certificado. Una de las finalidades principales del certificado y de su proceso de emisión es la de ligar la clave pública creada a un sujeto o entidad. Cuando se desea confiar en una CA, se debe descargar su clave pública raíz en nuestros repositorios de entidades emisoras de confianza, para que pueda ser utilizada por el sistema para la comprobación de cualquier certificado emitido por ella.

La emisión de un certificado suele partir de una solicitud por parte del usuario, equipo, etc, que es enviada a la CA para su comprobación y posterior emisión. Esta solicitud de certificado se denomina CSR (Certificate Signing Request o solicitud de firma de certificado). Esa solicitud de firma incorpora los datos necesarios del solicitante, además del par de claves públicas/privada que puede generar el propio solicitante o la CA. Loa certificados pueden ser emitidos como válidos o como revocados (hasta que sean comprobados los datos del solicitante). Un certificado pre-revocado, a pesar de introducir datos correctos y firmados por la CA, no es válido hasta que se retire su revocación por parte de la entidad validadora.

El proceso completo de certificación o creación de certificados se apoya en los siguientes pasos:

- Generación por parte del solicitante o de la CA del par de claves pública y privada del sujeto o entidad.

- Inclusión de los datos necesarios para el certificado, como nombre de entidad, correo electrónico, datos del solicitante, etc.
- Solicitud del certificado mediante la creación de un pre-certificado o CSR (Certificate Signing Request).
- Verificación física de los datos del certificado por parte de la RA (Registration Authority).
- Firma de la solicitud por parte de la CA son su clave privada y creación del certificado en los formatos necesarios para su uso.
- Publicación y distribución del certificado al solicitante.

Estos son básicamente los pasos necesarios para la creación de un certificado de usuario, auque puede variar según el tipo de CA y su infraestructura.

3.3.1 PKI (Public Key Infrastructure).

PKI es un esquema que permite establecer soluciones de certificación electrónica y sobre las que se fundamentan la prestación de servicios de certificación. Es la combinación de hardware, software, políticas y procedimientos que provee la seguridad requerida para llevar a cabo intercambios electrónicos de datos (EDI), debido a que cumple con los componentes de seguridad básicos, como los son: confidencialidad, autenticidad, integridad y no-repudio.

Para un buen funcionamiento de una PKI son importantes las siguientes características:

- Transparencia: El usuario no necesita conocer los mecanismos de gestión de claves y certificados que utiliza la PKI para poder utilizar los servicios que ésta ofrece.
- Escalabilidad: La adición de nuevos usuarios a la PKI no supone decrementos importantes en las prestaciones de la misma.
- Compatibilidad: La implementación de la PKI es independiente del software que se utiliza a nivel de usuario (por ejemplo, navegadores o programa de correo).

- Seguridad: La PKI debe implementar mecanismos que permitan a los usuarios confiar en las operaciones realizadas utilizando sus servicios.
- Eficiencia: La interacción de los usuarios con la PKI debe realizarse con tiempos de respuesta cortos.
- Disponibilidad: Se debe garantizar que la PKI siempre se encuentre operativa.

Las funciones principales que tiene la infraestructura de clave pública son las siguientes:

a) Generación de certificados de clave pública, que enlacen la identidad del titular del certificado con su clave pública.
b) Acceso a la política de certificación bajo la cual un certificado ha sido emitido.
c) Servicio de revocación de certificados rápido y seguro.
d) Acceso directo o indirecto a la lista de los certificados revocados de una forma confiable y con máxima disponibilidad.
e) Responsabilidad legal sobre el funcionamiento del sistema.

Componentes de PKI

a) Autoridad de certificación (CA): es el núcleo de la infraestructura de clave pública. Se encarga de la emisión de certificados. Los certificados son firmados por la autoridad de certificación y por ende toda la confianza dentro de la infraestructura depende de ella.
b) Autoridad de Registro (RA): establece las relaciones entre los usuarios y las CA. Es la que se encarga del registro de los usuarios, de la confirmación y validación de la identidad de los usuarios.
c) Políticas de Seguridad: establecen y definen los niveles máximos de seguridad de la información para una organización, así como los procedimientos a utilizar. Por lo general, incluye:

- Una clasificación de los usuarios que solicitan el certificado.

- Los procedimientos: método de registro, renovación de certificados, revocación de certificados.
- Los controles técnicos de seguridad: controles de ciclo de vida, seguridad física, compatibilidad con estándares.
- Cuestiones de responsabilidad, obligaciones y leyes.
- Limitaciones referentes al uso de certificados y claves asociadas.

d) Sistema de Distribución de Certificados: los certificados se pueden distribuir de varias formas, dependiendo de la estructura del entorno PKI. Se pueden distribuir, por ejemplo, manualmente (usuario-usuario), a través de un servicio de directorios o por vía e-mail.

e) Aplicaciones de PKI: son aquéllas que están habilitadas para el uso de PKI. Algunos ejemplos de éstas aplicaciones pueden ser:

- Comunicaciones entre servidores y browsers de Internet.
- Correo electrónico.
- Intercambio electrónico de datos (EDI).
- Transacciones con tarjeta de crédito en Internet.
- Redes privadas virtuales (VPN).

3.3.2 Tipos de entidades participantes en PKI.

La autoridad certificadora (CA) es el principal componente de un sistema de certificación basado en PKI, y aunque no tenga por qué ser el único componente de esta infraestructura, sí que podría realizar todas las funciones necesarias para el mantenimiento de esta infraestructura.

Para la emisión de un certificado confiable, lo datos del solicitante deben ser corroborados mediante la acción de una persona que los compruebe físicamente o mediante un sistema que garantice de forma fehaciente la veracidad de los mismos. Este filtro que comprueba los datos del solicitante los acepta como válidos y autoriza

la emisión de ese certificado por parte de la CA, se llama entidad de registro o autoridad de registro (RA). Esta Autoridad de Registro, es en muchos casos, la responsable de verificar los datos de una solicitud CSR y, por tanto, de autorizar su emisión. En el caso que el certificado haya sido emitido como implícitamente revocado, será RA la encargada de la comprobación de sus datos y de la retirada de esa revocación. Para la comprobación de los datos del solicitante se utilizan técnicas de comprobación de identidad cara a cara, o remotas como la comprobación de la titularidad de un dominio o e-mail. En la mayor parte de los casos se firman las condiciones o normas de la CA para el uso de un certificado, por requerimiento de la RA.

Otra entidad que participa en toda esta infraestructura es la Autoridad de Validación o VA (Validation Authority), responsable de la comprobación de los certificados emitidos. La Autoridad de Sellado de Tiempo o TSA (Time –Stamp Authority) se utiliza para la firma o sellado de documentos mediante estampación de la fecha y hora de realización de una operación. Su utilidad es la de dar fe de la realización de una operación en un punto o espacio temporal determinado.

3.3.3 Organismos Privados.

Todo este sistema, que forma una infraestructura PKI, puede ser empleado para la gestión de sistemas seguros en organizaciones privadas o en operaciones realizadas con la administración publica. A pesar de ello su finalidad no suele tener relación directa con el origen público o privado de esa infraestructura emisora de certificados. Una infraestructura CA pública puede emitir certificados que pueden ser utilizados para operaciones privadas y públicas. En caso contrario, en el que una CA privada emite un certificado, este certificado no se utiliza para fines públicos sino privados.

Los certificados emitidos por estas CA privadas tienen un precio determinado, que ha de pagarse a la emisión y en su renovación. El coste de estos certificados depende de la entidad emisora, aunque su coste puede ser elevado para el mantenimiento de una infraestructura empresarial de un tamaño medio.

Estas entidades privadas disponen de medios de tramitación al alcance de cualquier solicitante, mediante páginas Web en Internet que permiten realizar y controlar todo el proceso de principio a fin. Para la comprobación de esas solicitudes de certificados, utilizan su propia Autoridad de Registro que comprueba los datos del solicitante. En este caso, además, la RA se encarga de la verificación del pago del certificado, además de la comprobación de los datos.

3.3.4 Organismos Públicos.

En el caso de organismos públicos, la infraestructuras necesarias para la emisión de certificados y todos sus procesos relacionados están creados y mantenidos por organismos o administraciones públicas de los gobiernos de países Para crear una CA pública, es necesario que el organismo público se adapte a las normas del estándar, pero también que se adapte la legislación a las normas de funcionamiento de PKI.

3.3.5 Certificados Auto firmados.

La alternativa a este costoso sistema de certificados emitidos por CA privadas son los certificados auto firmados, o la creación de nuestra propia CA para el uso interno en nuestra organización. El problema que nos encontramos ante el uso de certificados emitidos por nuestra organización es la generación de confianza sobre nuestros certificados. Si emitimos certificados a nivel interno, para proteger los accesos a nuestra Intranet y no divulgamos externamente los certificados, no tenemos

mayor problema que implantar el certificado de nuestra CA raíz en los repositorios de entidades emisoras de confianza de cada uno de los usuarios de nuestra red. Pero si la idea consiste en que los visitantes confíen en una página Web en la que damos servicio, debemos acudir a certificados emitidos por CA privadas de confianza como Verisign u otras incluidas en la confianza de sistemas operativos como Windows.

Existen varias aplicaciones en el mercado capaces de generar certificados auto firmado, tanto para Windows como para otras plataformas. Pero la más recomendable, si deseamos trabajar con certificados, es instalar una pequeña CA que cumpla todos los requerimientos, tanto sobre Windows como Linux.

3.3.6 CA Gratuitas.

Se están creando otros tipos de CA como Web of Trust, SPKI, Cacert o RobotCA que procuran hacer más asequible este mundo de los certificados y la firma digital. La proliferación de entidades emisoras de certificados gratuitas está siendo muy importante, aunque debemos recordar que un sistema PKI se basa principalmente en la confianza que generan las entidades emisoras de certificados y por lo tanto en los certificados emitidos por ellas

3.3.7 Formatos y Tipos de Certificados.

El modelo actual de certificado utilizado habitualmente en PKI es el certificado digital en formato X.509 versión 3, descrito en el RFC 3280. La sintaxis utilizada para la construcción de un certificado se conoce como ANSI.1 (Abstract Syntax Notation 1), un estándar que precisa la sintaxis a utilizar (similar a la de XML) y que se ocupa de definir un estándar de notación en formato de texto o binario. Las normas de codificación binarias se definen en el documento X.690. Aunque X.509 no define un tipo de criptografía determinada para la incrustación de claves en los certificados, hoy en día el tipo más común es RSA. No obstante, debemos recordar que un

certificado es un documento público (que sólo suele incluir la clave pública) por lo que no precisa de encriptación para su almacenamiento.

La principal diferencia entre las versiones 1, 2 y 3 del modo X.509 es la nueva introducción de las extensiones es la versión 3, así como la ampliación de algunos campos. Estas extensiones se dividen en tres categorías:

- **Políticas de uso y claves.** La versión 1 y 2 no permite definir prácticas de uso para la implantación de políticas de seguridad similares a las utilizadas en el protocolo IPsec. Se definen los ciclos de vida de cada una de las claves (públicas y privada), así como los propósitos de cada una de ellas.

- **Restricciones de uso del certificado.** El propio certificado puede restringir su uso para alguna actividad relacionada. Por ejemplo: puede restringir el uso de certificado para la emisión de certificados (CA), el espacio de nombres a utilizar o la cadena de certificación.

- **Atributos del emisor y del sujeto.** Mediante la introducción de parejas de atributos/valores (AVP), se permite el uso de datos que no están incluidos de forma nativa en el estándar, para la incrustación de todo tipo de informaciones, como fotografías, datos biométricos, nombre alternativos, etc.

Prácticamente, todos los certificados que están actualmente en uso utilizan la versión 3, ya que la mayoría de las aplicaciones actuales precisan del uso de estas extensiones.

Los datos de los que está compuesto un certificado son básicamente:

- La información del titular **(subjet)** en formato X.509 Distinguished Name o DN. Este campo conocido como asunto del certificado es el que define los datos únicos del titular. Puede incluir un nombre alternativo del sujeto para el uso con aplicaciones como correo electrónico, IPsec, etc., además de cualquier dato del tipo X.500 como datos específicos de LDAP o Active Directory.

- El certificado puede contener otra información del sujeto, como una fotografía, huella dactilar, otros datos biométricos, profesión, domicilio, etc.

- La información del emisor o CA emisora. Se suele incluir la ubicación de la CA y de la CRL mediante dirección Web, además de una dirección de correo electrónico para consultas de soporte. También puede incluir un nombre alternativo.

- La información del certificado, como su versión (1,2,3), extensiones (en la versión 3) o usos permitidos, período de validez, nombre alternativo, etc.

- Un número de serie único para cada certificado en la CA que define el identificador del certificado para su búsqueda o revocación.

- La clave pública del certificado y su algoritmo de creación. Una buena definición de un certificado lo define como un documento que relaciona una clave pública con un titular.
- La firma de los datos del certificado mediante los campos de algoritmo de firma, la huella y la propia firma digital de la CA, realizada mediante su clave privada. Esto garantiza la integridad del certificado y facilita su comprobación mediante la clave pública de la CA.

- Opcionalmente se puede incluir la clave privada del certificado que suele venir en formato PEM, si se muestra en texto claro. La clave privada sólo está incluida en el certificado que se entregará al propietario y en algunos formatos.

En la tabla 3.2 se observa los campos básicos que se encuentran en un certificado X.509.

Campo	**Significado**
Versión	Cuál versión del X.509.
Número de serie	Este número junto con el nombre de la CA identifican de manera única el certificado.
Algoritmo de firma	El algoritmo que se utilizó para firmar el certificado.
Emisor	El nombre X.500 de la CA.
Validez	Las fechas de inicio y final del periodo de validez.
Nombre del sujeto	La entidad cuya clave se está certificando.
Clave Pública	La clave pública del sujeto y el ID del algoritmo usado para generarla.
ID del emisor	Un ID opcional que identifica de manera única al emisor del certificado.
ID del sujeto	Un ID opcional que identifica de manera única al sujeto del certificado.
Extensiones	Se han definido muchas extensiones.
Firma	La firma del certificado (firmada por la clave privada de la CA)

Tabla 3.2 Campos básicos de un certificado X.509.
Fuente: Hansen, Fernandez Yago, 2008

Los formatos de codificación más frecuentes son:

- **BER** (Basic Encoding Rules). Es un conjunto de reglas para la codificación de los datos ADN.1 en formato binario para su transporte. Utiliza una codificación tipo TLV (tag-length-value) que define una cadena de datos mediante campos codificados de esta forma. Esta definido en el estándar X.690.

- **CER** (Canonical Encoding Rules). Es un subtipo de BER similar a DER para mensajes largos. No se utiliza tanto como DER. Está definido en el estándar X.690.

- **PER** (Packing Encoding Rules). Otro formato de reglas de codificación de ASN.1 en formato muy compacto. Evita campos vacíos y etiquetas de tamaño innecesarios.

- **XER** (XML Encoding Rules). Es un formato de codificación de ASN.1 en formato XML. Se define en el estándar X.693.

- **CXER** (Canonical XML Encoding Rules). Definido en el estándar X.693. Muy similar al XER pero codificado en un stream largo que no permite espacios en blanco entre los datos.

- **DER** (distinguished Encoding Rules). Es un subtipo de BER que mejora la seguridad de codificación-decodificación. El formato DER no es visible mediante editores de texto ya que es un formato completamente binario. No lleva cabeceras ASCII. Puede almacenar certificados con claves públicas y privadas. Los archivos codificados en este formato suelen llevar extensión ".der". Es el formato por defecto utilizado por la mayoría de los navegadores de Internet. Está definido en el estándar X.690.
- **PEM** (Privacy-enhanced Electronic Mail). El formato PEM es un formato ASCII (convertido a binario en base-64) del formato DER al que se le añade una cabecera (BEGIN) y un pie (END) para verlo en formato imprimible. Una de las ventajas de este formato es que puede incluir comentarios u otro tipo de texto y que al no ser un formato binario, puede ser manejado por programas de correo o similares, para los que el envío de binarios se hace complejo.

También permite copiar y pegar los certificados de un programa a otro. Los archivos codificados en este formato utilizan extensiones ".pem" o a veces ".cer".

- **PKCS#12** (Public Key Criptography Standards number 12 de los laboratorios norteamericanos RSA) depende del software utilizado para su manipulación la elección de una u otra codificación. El formato PKCS12 conocido por la extensión ".p12" de archivo es uno de los más comunes y se le conoce también como PFX. Se codifican también en formato binario no imprimible y pueden contener certificados con sus claves públicas y privadas. Lo suelen utilizar también los navegadores de Internet. Permite proteger las claves mediante cifrado por clave simétrica y la exportación de la clave privada.

- **PKCS#7. (**Public Key Criptography Standars number 7 de los laboratorios norteamericanos RSA), usualmente archivo con extensión ".p7c" o ".p7b", que se utiliza para el transporte de certificados, además de permitir incluir contenidos y la firma digital. Su contenido es de tipo binario. Este es un formato similar al S/MIME para el empaquetamiento seguro de archivos.

Existen herramientas para convertir un mismo certificado entre cualquiera de estos formatos. Ambos formatos (DER-PEM) se pueden utilizar, además de para almacenar las claves públicas, para archivar las claves privadas RSA o DSA.

Existen varias clases, que definen la clasificación del certificado:

- **Certificados de clase 1**. Se emiten a personas y no muestran su identidad, aunque sí que relacionan su nombre distinguido, único en la CA, con un nombre real. Esta clase representa el menor nivel de confianza y son válidos para firma digital de correo, transacciones comerciales de nivel bajo, o cualquier otra donde la identidad del poseedor no deba ser comprobada.

- **Certificados de clase 2 reconocidos**. Sirven para identificar inequívocamente al poseedor de ellos (sujeto) e incluyen además datos personales (dirección, teléfono, etc). Son validos para la firma digital y han sido comprobados por una entidad de registro. Proporcionan un nivel de seguridad medio.

- **Certificados de clase 2 no reconocidos**. Identifican al usuario, pero no incorporan todas las garantías de identificación para operaciones de riesgo. Pueden ser utilizados para la firma digital, encriptación de documentos, transacciones comerciales, control de acceso, etc.

- **Certificados de clase 3**. Ofrecen el mayor nivel de confianza. Sirven para identificar a personas u organizaciones de forma inequívoca. En el caso de personas, éstas han sido previamente verificadas mediante autoridades de registro. Su uso supone un mayor nivel de seguridad, y sus funciones son las mismas que las clase 2, además de poder utilizarse para la identificación de la persona u organización que mantiene la total confianza de la CA emisora.

- **Certificados Clase 4**. A todas las comprobaciones anteriores se suma la verificación del cargo o la posición de una persona dentro de una organización

Desde el punto de vista de la finalidad, los certificados digitales se dividen en:

a) **Certificados SSL para cliente**. Usados para identificar y autenticar a clientes ante servidores en las transacciones mediante el protocolo Secure Socket Layer (SSL), y se expiden normalmente a una persona física, bien un particular, bien un empleado de una empresa.

b) **Certificados SSL para servidor**. Usados para identificar a un servidor ante un cliente en comunicaciones mediante SSL, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer,

vinculando también el dominio por el que se debe acceder al servidor. La presencia de este certificado es condición imprescindible para establecer comunicaciones seguras SSL.

c) **Certificados S/MIME**. Usados para servicios de correo electrónico firmado y cifrado, que se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona autenticación, integridad y no-repudio. También se puede cifrar el mensaje con la clave pública del destinatario, lo que proporciona confidencialidad al envío.

d) **Certificados de firma de objetos**. Usados para identificar al autor de software o porciones de código en algún lenguaje de programación (Java, JavaScript, CGI, etc.).

e) **Certificados para CA**. Identifican a las propias Autoridades de Certificación, y es usado por el software cliente para determinar si puede confiar en un dado certificado, accediendo al certificado de la CA y comprobando que ésta es de confianza.

CAPITULO IV

4 PRUEBAS Y RESULTADOS.

4.1 Selección de las herramientas basadas en Linux (Zeroshell y VirtualBox)

Para realizar el diseño y configuración del laboratorio de un sistema de control de acceso a WLAN mediante EAP y RADIUS, se escogieron dos herramientas basadas

en software libre como lo son Zeroshell y VirtualBox, estas permiten elaborar la arquitectura propuesta y plasmar las ventajas de estas, teniendo en consideración aspectos como la seguridad en redes inalámbricas. Además se escogieron por ser versátiles, permiten su configuración de una manera más viable, ya que existe documentación en los foros de comunidades código abierto, son herramientas que pueden ser soportados en varios tipos de plataformas o sistemas operativos.

4.2 Virtual Box

VirtualBox es un software de virtualización para arquitecturas x86, creado originalmente por la empresa alemana innotek GmbH. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización.

Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como sistemas invitados, dentro de otro sistema operativo anfitrión, cada uno con su propio ambiente virtual. Entre los sistemas operativos soportados (en modo anfitrión) se encuentran GNU/Linux, Mac OS X, OS/2 Warp, Microsoft Windows, y Solaris/OpenSolaris, y dentro de ellos es posible virtualizar los sistemas operativos FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris, MS-DOS y muchos otros.

4.3 Zeroshell

Zeroshell es una distribución Linux para servidores y dispositivos embebidos, que provee de servicios de red. Dispone de un interfaz Web para su configuración, pero también puede ser administrado desde un terminal remoto (ssh) Esta basado en Debian. Se pueden descargar los diferentes paquetes que lo forman, para adaptarlo a nuestro hardware.

4.4 Topología de Red.

En la Fig. 4.1 se muestra la topología de red inalámbrica que permite visualizar como sería el funcionamiento o la gestión del control de acceso a los usuarios mediante un servidor RADIUS a una red, mediante el uso de la herramienta opensource Zeroshell. La primera imagen muestra un diagrama general de su funcionamiento, donde se indica, los clientes que van a acceder a la red, mediante un punto de acceso inalámbrico.

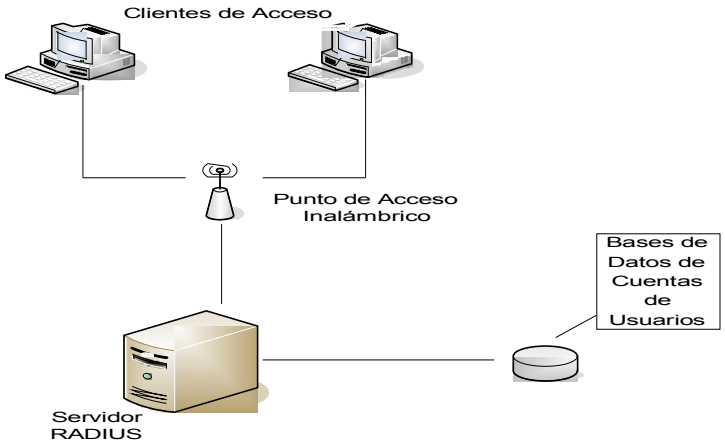

Figura 4.1 Topología de Red Inalámbrica para controlar el acceso a los usuarios mediante un servidor RADIUS.
Fuente: Elaboración propia.

En la Fig.4.2 podemos observar una topología de red, más específica, donde se visualiza nuestro escenario. Podemos observar a los clientes intentando acceder a la red mediante el punto de acceso cuya IP es la 192.168.0.1, para entrar debe validar sus credenciales ante el servidor RADIUS, que esta configurado en la herramienta opensource ZeroShell, cuya IP es la 192.168.0.75, la cual esta soportado en una maquina virtual en VirtualBox, una vez que se haya validado el certificado de acceso, conjuntamente con el usuario configurado en el servidor RADIUS, se le da el acceso a la misma.

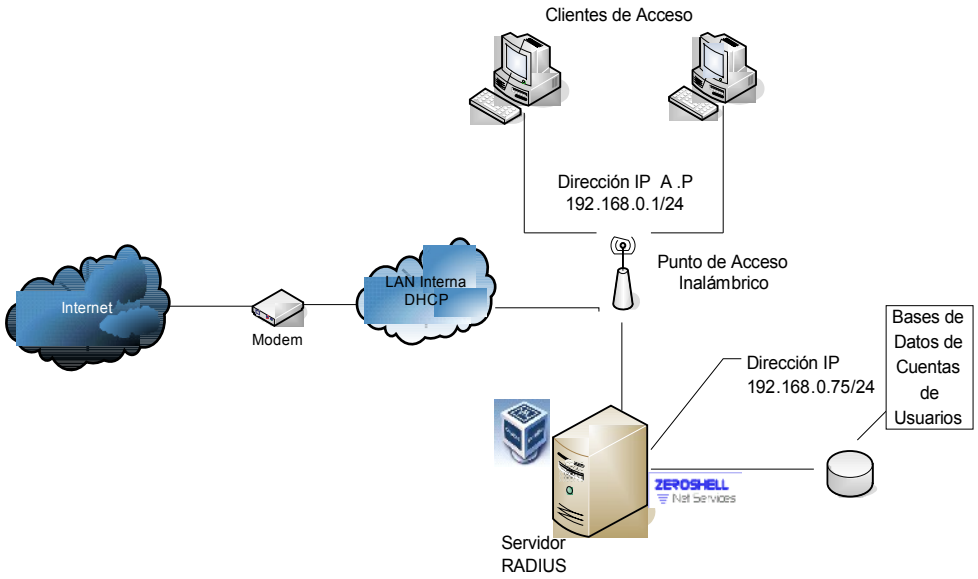

Figura 4.2 Escenario de prueba utilizando la herramienta ZeroShell
Fuente: Elaboración propia.

4.5 Escenario y Pruebas Realizadas.

Como primer paso para el diseño y configuración del laboratorio para el estudio del sistema de control de acceso a WLAN mediante EAP y RADIUS, se descarga e instala el software VirtualBox, el cual contendrá así mismo a las herramientas open source Zeroshell.

Como primer paso se instala la herramienta, para ello se utilizó la ultima versión **VirtualBox 4.0.6 para Windows hosts** x86/amd64, como puede observarse en la Fig.4.3

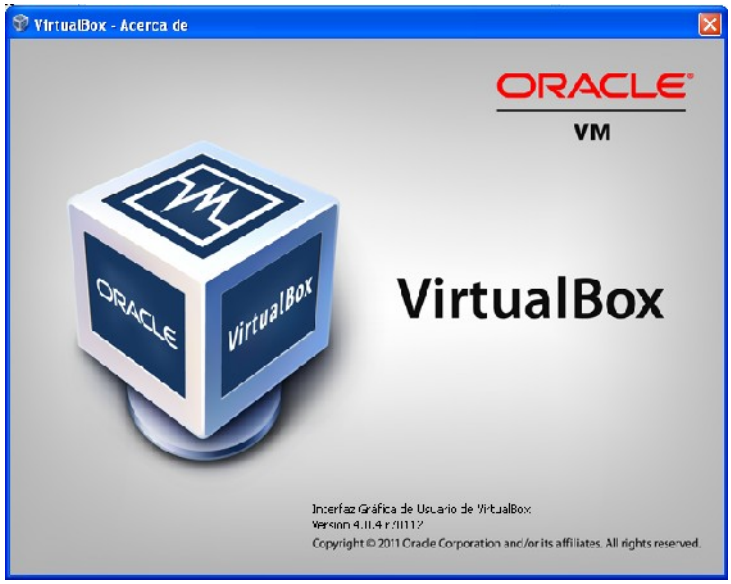

Figura 4.3 Herramienta de Virtualización (VirtualBox).
Fuente: Elaboración propia.

Se crea la maquina virtual que contendrá a la herramienta Zeroshell, pero para que esta pueda correr, necesita así misma una configuración propia de elementos de software y hardware, entre las cuales nombraremos:

General

Nombre: ZR14
Tipo SO: Linux 2.6

Sistema:

Memoria base: 256 MB
Orden de arranque: Disquete, CD/DVD-ROM, Disco duro
Pantalla:

Memoria de vídeo: 7 MB
Servidor de escritorio remoto: Inhabilitado

Almacenamiento:

Controlador IDE

IDE primario maestro (CD/DVD): ZeroShell-1.0.beta14.iso
Controlador SATA

Puerto SATA 0: ZR14.vdi (Normal, 8,00 GB)

Audio:

Controlador de anfitrión: Windows DirectSound
Controlador: ICH AC97

Red:

Adaptador 1:

Intel PRO/1000 MT Desktop (Adaptador puente, NIC Fast Ethernet PCI Familia RTL8139 de Realtek)

Adaptador 2:

Intel PRO/1000 MT Desktop (Adaptador puente, NIC Fast Ethernet PCI Familia RTL8139 de Realtek)

USB:

Filtros de dispositivos: 0 (0 activo)

Carpetas Compartidas:

No aplica

En la siguiente figura puede observarse la configuración que anteriormente se explicó:

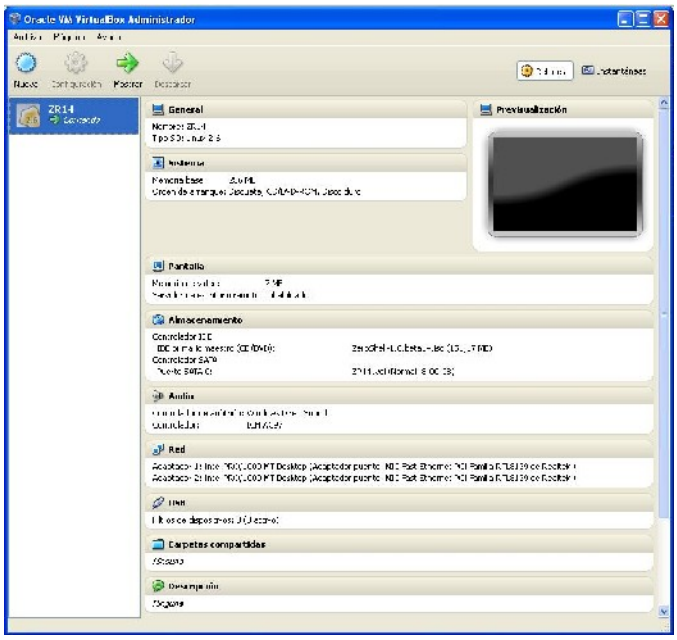

Figura 4.4 Configuración de requerimientos (Sistema, Almacenamiento y Red) de la máquina virtual a utilizar (VirtualBox).
Fuente: Elaboración propia.

Finalizado la configuración de la maquina virtual que contendrá la herramienta Zeroshell, se procede a la instalación de dicha herramienta.

Se instala la versión ZeroShell-1.0.beta14 para montar un servidor Radius, entre otras cosas, porque me permite disponer rápidamente de un servidor Radius sin tener que montar toda la infraestructura software que ello requiere y evitando la complejidad que supone.

ZeroShell se encuentra disponible en dos formatos:

• Como LiveCD.
• Como imagen Compact Flash.

Una de las ventajas que existe es la posibilidad de configurar ZeroShell desde un terminal o vía ssh, para usuarios avanzados. No obstante, también podemos administrarlo de forma remota desde nuestro navegador gracias a que dispone de una interfaz web.
Pero la principal ventaja, es que no requiere ser instalado en disco duro. Funciona directamente en modo live desde un CD o incluso en un dispositivo USB, lo que nos da juego para tener un servidor altamente disponible.

Los datos y ajustes se almacenan en una base de datos que puede ser almacenada en discos ATA, SATA, SCSI y USB. Cuando lo configuramos, creamos un perfil. Ese perfil podemos copiarlo a otro equipo y, en caso de avería de la máquina, tener funcionando de nuevo nuestro servidor en pocos minutos. Además, si tenemos guardado un perfil en nuestro equipo, al arrancar ZeroShell lo detectará y directamente lo cargará.
La base de datos se puede almacenar en un equipo que ya tenga un sistema operativo instalado sin destruir nada. El sistema de archivos donde se almacena puede ser ext2, ext3, reiserfs o fat32.

Otra opción para tener un servidor altamente disponible es montarlo en una máquina virtual y, en lugar de guardar tan sólo la BD de ZeroShell, guardar la máquina virtual completa.

Ya introducido el ISO en nuestro caso en el equipo lo iniciamos para que arranque.
Veremos una pantalla de inicio como en la Fig.4.5:

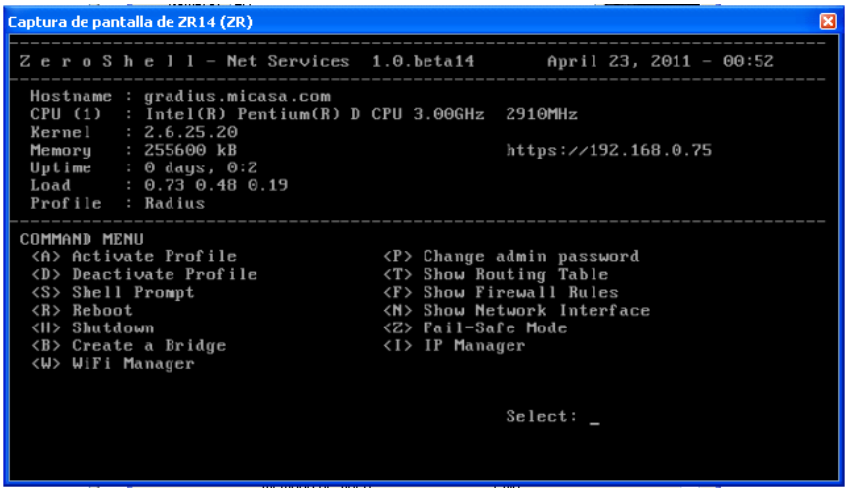

Figura 4.5 Menú de inicio de la herramienta ZeroShell.
Fuente: Elaboración propia.

Podemos observar cuando arranca, como se inician todos sus servicios:

boot

Una vez instalado y configurado la herramienta de ZeroShell, procedemos a realizar los siguientes pasos.

Después de arrancar VirtualBox con la herramienta ZeroShell, se configura la tarjeta de red local a una dirección IP en la red 192.168.0.X, como 192.168.0.24 y se coloca la siguiente dirección http://192.168.0.75 en nuestro navegador.

Como se observa en la pantalla de inicio, se muestran los datos necesarios para configurar el servidor por primera vez:

IP de ZeroShell: 192.168.0.75
Username: admin
Password: admin

Configurado el servidor ZeroShell con una IP de nuestra red, ya se accede a su configuración mediante la interfaz Web qué este nos ofrece. Así que, cogemos

nuestro equipo, abrimos el navegador y, en la barra de direcciones, ponemos la IP que le hemos asignado. Por ejemplo, si le hemos asignado la IP 192.168.0.75

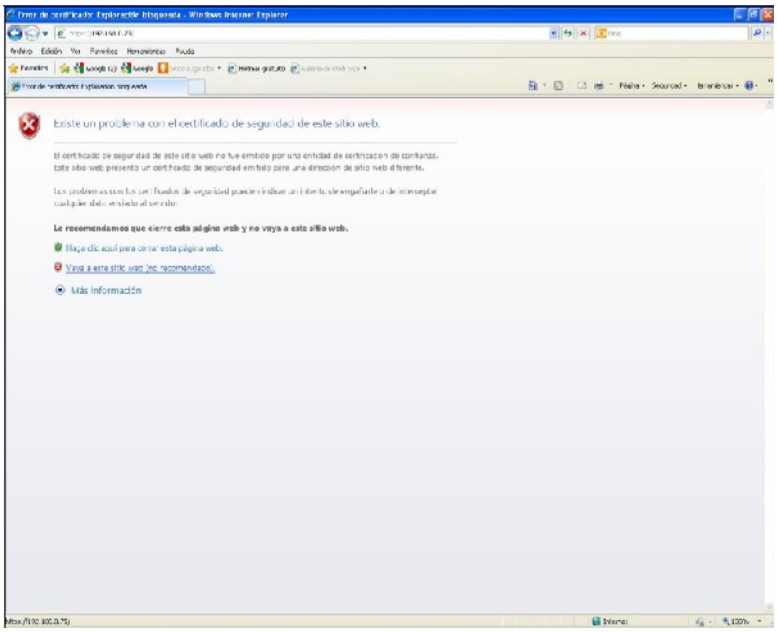

Figura 4.6 Certificado de seguridad para inicio de la herramienta ZeroShell. Fuente: Elaboración propia.

La Fig.4.6 indica que el servidor usa un certificado de seguridad no válido, algo que es cierto porque aún no lo hemos configurado. Se hace clic sobre la opción de añadir una excepción y nos aparecerá una ventana donde podremos confirmar la excepción de seguridad. Tenemos que confirmar la excepción de seguridad porque el servidor aún no tiene creados sus certificados.

Una vez hecho esto, se observa la pantalla de acceso de zeroshell. Para iniciar la interfaz gráfica de usuario, se debe introducir los datos para acceder como administrador:

admin - zeroshell

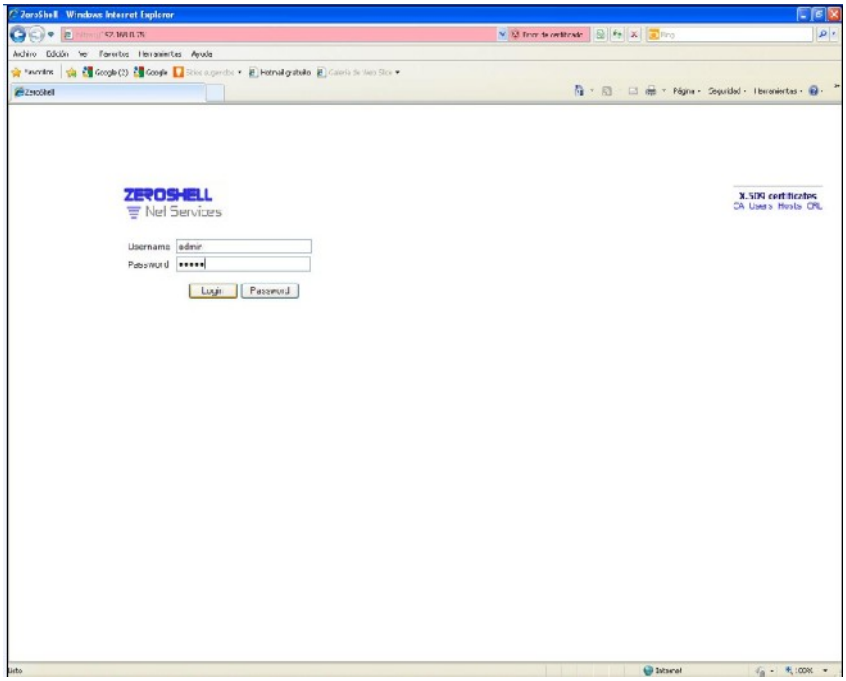

Figura 4.7 Interfaz Gráfica de Usuario de la herramienta ZeroShell.
Fuente: Elaboración propia.

Una vez autenticados por la interfaz gráfica, se observar una imagen como la Fig.4.8, donde se observa la página de inicio de administración de la herramienta.

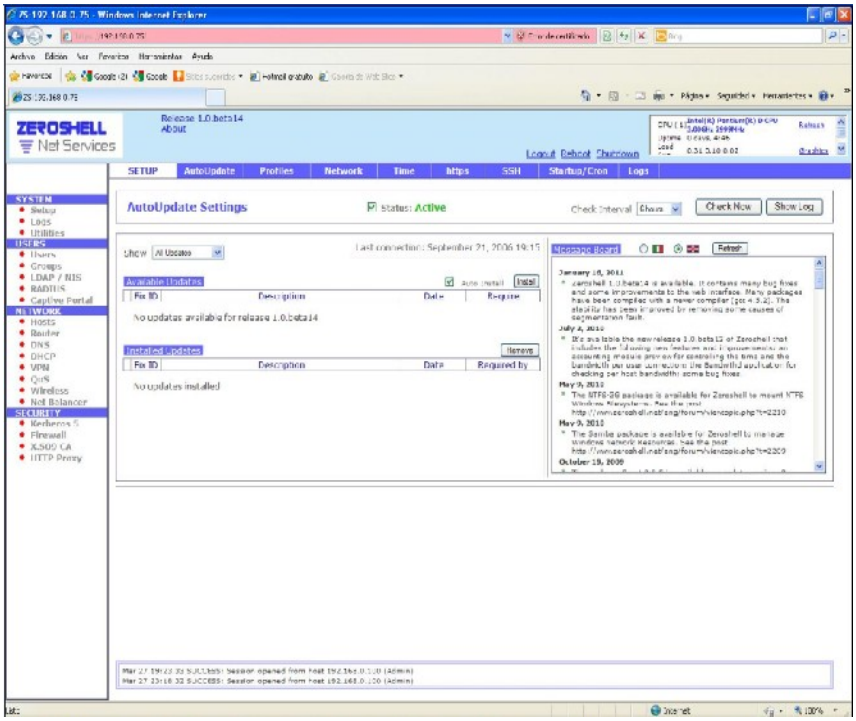

Figura 4.8 Administración a nivel de GUI de la herramienta ZeroShell. Fuente: Elaboración propia.

Instalación de la base de datos ZeroShell

El primer paso es crear un perfil para guardar nuestra configuración. Un perfil es la base de datos donde se van a guardar los ajustes. Mientras no se cree un perfil, cada vez que se arranque Zeroshell se iniciará con la configuración por defecto. Para ello, hacemos clic en **Profiles** y seleccionamos el disco duro en el que vamos a guardar el perfil. Una vez seleccionado, aparecerá el botón que permiten trabajar con perfiles:

Se crea una partición, para ello, en la siguiente pantalla, hago clic en el botón "**New partition**".

Se escribe un nombre para el disco virtual en **Label** y se hace clic en "Create Partition". Una vez creada la partición, aparecerá una ventana en la que seleccionaré el disco sda1, para guardar allí el perfil:

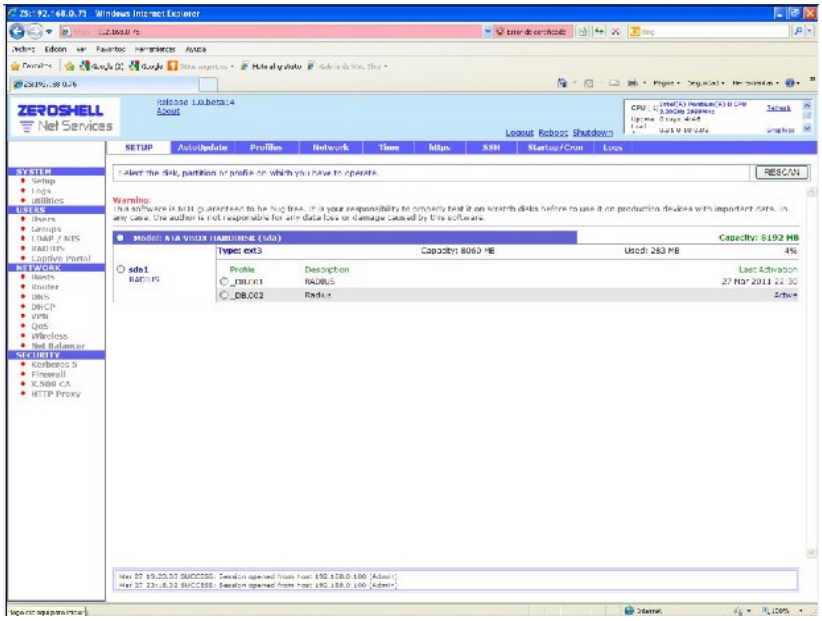

Figura 4.9 Configuración de una partición para la creación de un Perfil. Fuente: Elaboración propia.

En la Fig.4.9, hacemos clic en el botón "**Create Profile**" y se abrirá una ventana como la siguiente, en la que se especifica una serie de datos de nuestro nuevo servidor:

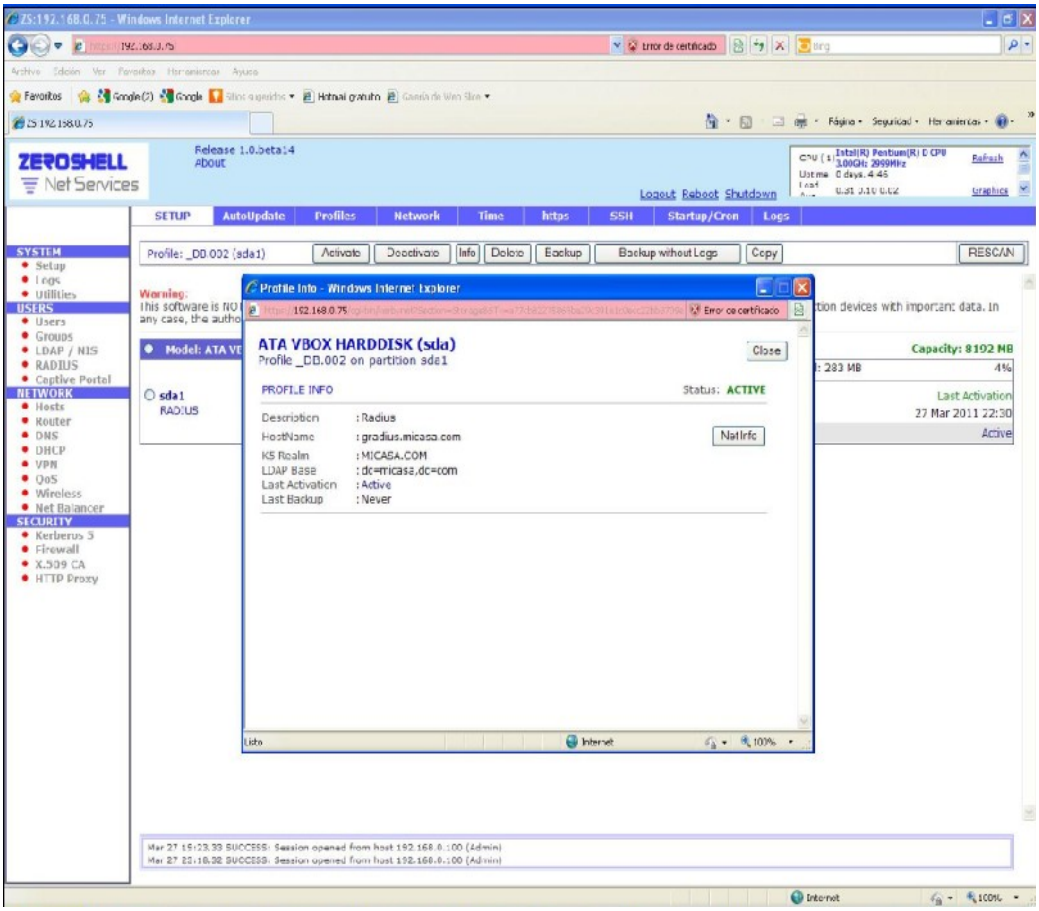

Figura 4.10 Formulario para la creación de un Perfil.
Fuente: Elaboración propia.

Se coloca la descripción, Hostname, Realm, LDAP Base, nuestra contraseña de administrador y la IP del gateway por defecto. Una vez especificados los datos, se pulsa el botón **Create** y se creará nuestro perfil.

Ahora que se tiene un perfil creado, se debe activar. Para ello, se selecciona el perfil (**_DB002**) y se hace clic en el botón **Activate**.

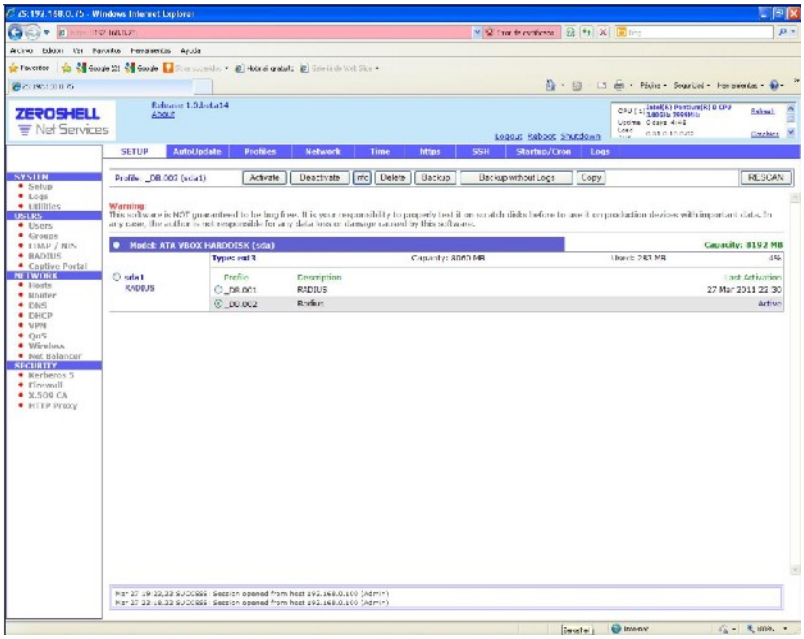

Figura 4.11 Vista de las particiones creadas.
Fuente: Elaboración propia.

Se observará los datos del perfil, como en la siguiente Fig. 4.12:

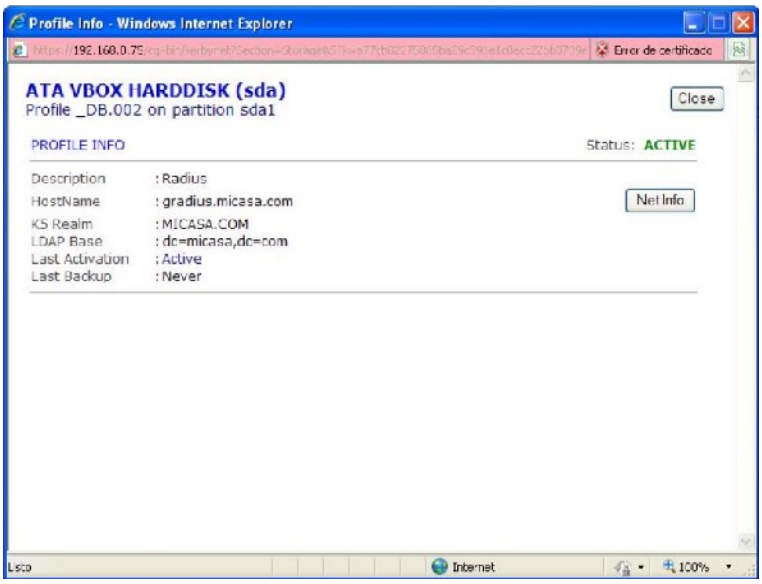

Figura 4.12 Vista del perfil creado.
Fuente: Elaboración propia

Si son correctos, se pulsa el botón "**Activate**". Se reiniciará el servidor para establecer los ajustes que hemos realizado y, por tanto se cerrará la sesión. Se espera a que el servidor vuelva a iniciarse para seguir configurándolo.

Al volver a iniciarse la máquina, se intenta acceder al interfaz Web desde el navegador, se observa que vuelve a aparecer la información de que la conexión con el servidor no ha sido verificada. Se vuelve a añadir la excepción de seguridad, después de eliminar la caché del navegador.

Ahora que ya hemos iniciado la sesión con nuestro perfil, se crea una autoridad de certificación. Para ello, hacemos clic en el botón **X.509 CA** del apartado **SECURITY** que hay en la parte izquierda de la pantalla principal Fig.4.13

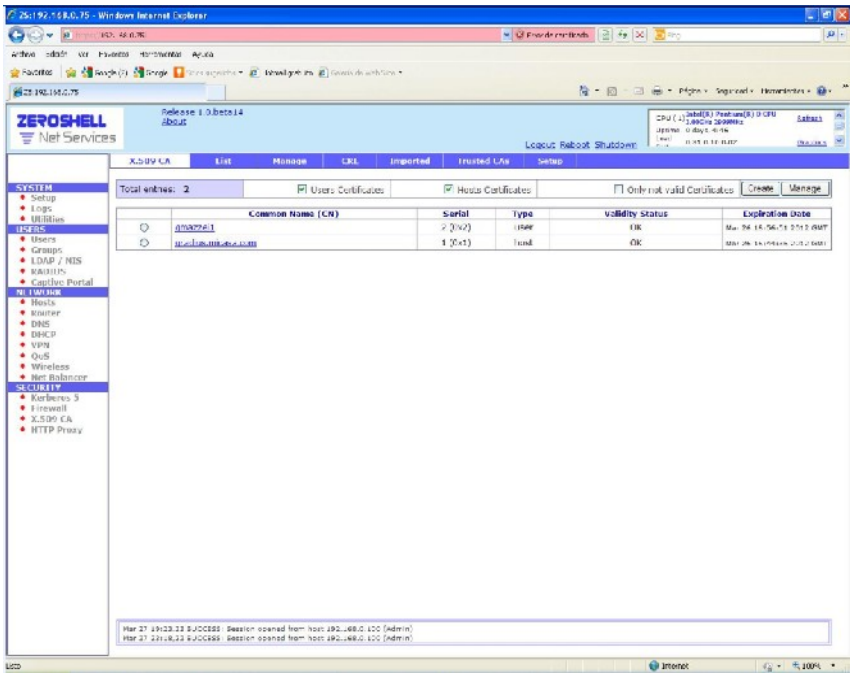

Figura 4.13 Creación del Certificado de Seguridad X.509.
Fuente: Elaboración propia.

Ahora bien, entre todos lo botones que hay para trabajar con la autoridad de certificación, se hace clic en el botón "**Setup**" y se ve una pantalla como en la Fig.4.14:

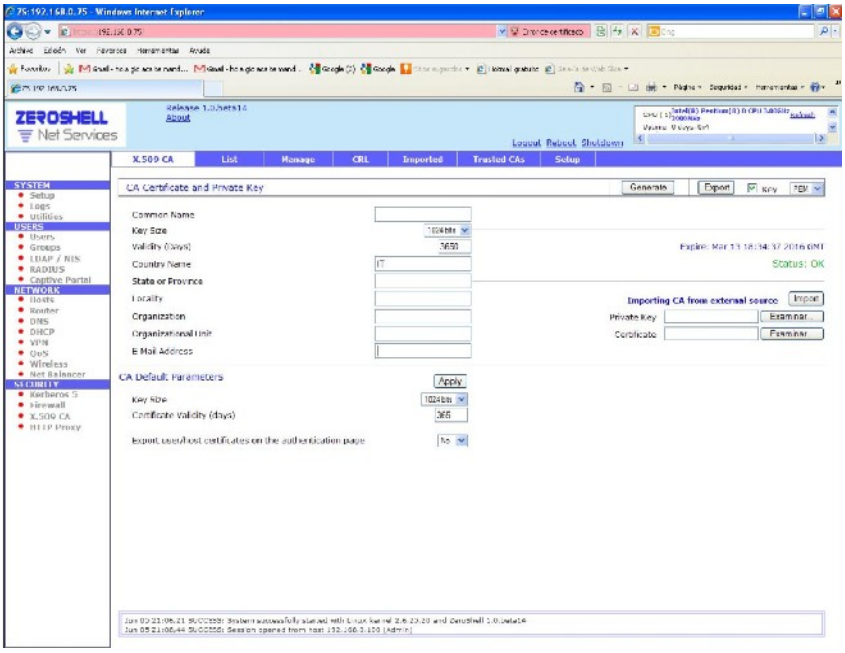

Figura 4.14 Formulario para la Creación del Certificado de Seguridad X.509. Fuente: Elaboración propia.

Una vez introducidos nuestros datos, se pulsa el botón "**Generate**". Esta muestra un mensaje en el que se pregunta si se está seguro. Se oprime "**OK**" y listo. En la Fig.4.14.1 se observa el certificado generado.

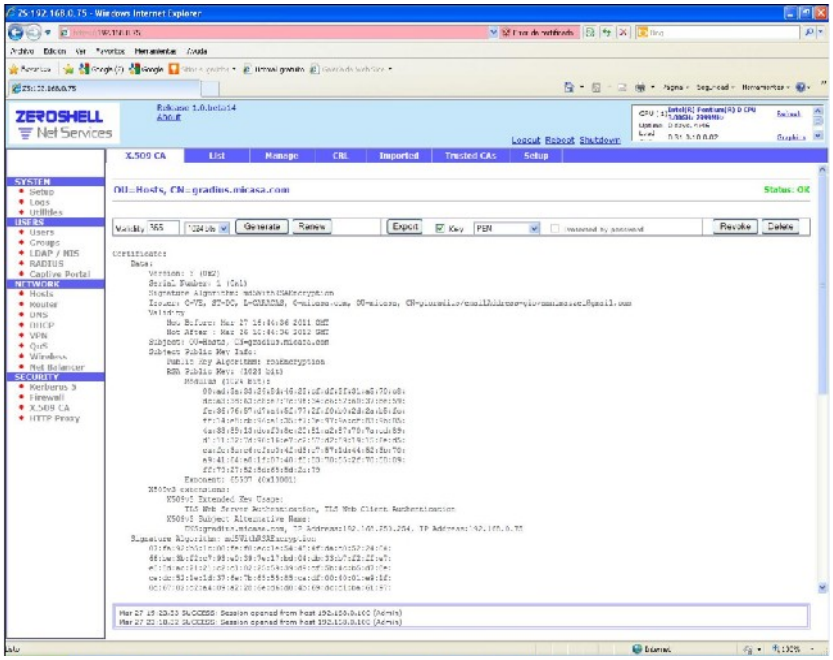

Figura 4.14.1 Certificado de Seguridad X.509.
Fuente: Elaboración propia

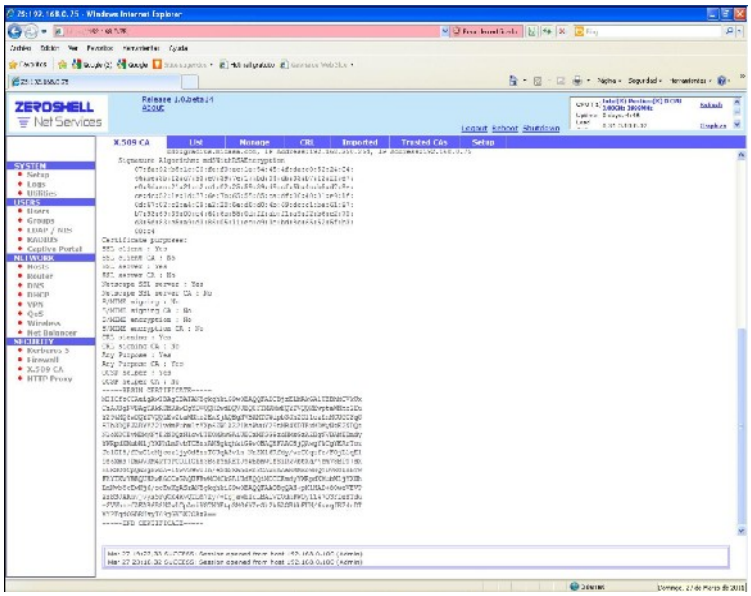

Figura 4.14.2 Certificado de Seguridad X.509
Fuente: Elaboración propia.

Certificado Digital:

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=VE, ST=DC, L=CARACAS, O=micasa.com, OU=micasa, CN=gioradius/emailAddress=giovannimazzei@gmail.com
Validity
Not Before: Mar 27 16:44:36 2011 GMT
Not After : Mar 26 16:44:36 2012 GMT
Subject: OU=Hosts, CN=gradius.micasa.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:ad:3a:33:26:8d:46:23:cf:df:3f:31:a5:70:c8:
dc:a3:3d:63:c8:e7:7c:9f:34:c6:52:a0:37:be:59:
fe:36:76:57:d7:a4:5f:77:2f:f0:b0:2d:2a:b5:fc:
ff:14:e8:cb:96:a1:35:f7:3e:97:9a:cf:83:9b:05:
4a:33:89:13:dc:f0:8e:20:81:a2:87:70:7a:cd:89:
d1:11:32:7d:90:16:e7:c2:57:d2:89:19:15:6e:d5:
ea:fe:3a:e6:ef:c0:4f:d3:e7:57:1d:44:52:3b:70:
a9:41:64:a0:1f:07:40:f8:83:70:55:2f:70:50:89:
ff:79:27:52:5d:68:5d:2a:79
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication

X509v3 Subject Alternative Name:

DNS:gradius.micasa.com, IP Address:192.168.250.254, IP Address:192.168.0.75

Signature Algorithm: md5WithRSAEncryption

07:fa:92:b5:1c:00:fe:f0:ec:1e:54:45:4f:da:c0:52:24:04:
66:be:3b:f2:c7:93:e0:39:7e:17:bd:04:db:33:b7:f2:ff:e7:
e0:8d:ac:21:21:c2:c1:02:25:59:39:d9:cf:5b:4c:b5:d7:8e:
ce:dc:52:1e:1d:37:6e:7b:65:55:85:ca:df:00:40:01:e9:1f:
0d:67:02:c2:a4:09:a2:28:6e:d6:d0:4b:69:dc:c1:ba:61:97:
b7:93:69:39:00:e4:64:6c:55:0d:ff:ab:f1:a9:f2:b6:e2:70:
d3:5d:83:c5:a9:d3:86:05:11:ec:c9:3e:bd:8c:65:52:5f:b3:
80:c4

Certificate purposes:

SSL client : Yes

SSL client CA : No

SSL server : Yes

SSL server CA : No

Netscape SSL server : Yes

Netscape SSL server CA : No

S/MIME signing : No

S/MIME signing CA : No

S/MIME encryption : No

S/MIME encryption CA : No

CRL signing : Yes

CRL signing CA : No

Any Purpose : Yes

Any Purpose CA : Yes

OCSP helper : Yes

OCSP helper CA : No

-----BEGIN CERTIFICATE-----

MIICfzCCAeigAwIBAgIBATANBgkqhkiG9w0BAQQFADCBjzELMAkGA1U
EBhMCVkUx
CzAJBgNVBAgTAkRDMRAwDgYDVQQHEwdDQVJBQ0FTMRMwEQYDV
QQKEwptaWNhc2Eu
Y29tMQ8wDQYDVQQLEwZtaWNhc2ExEjAQBgNVBAMTCWdpb3JhZGl1cz
EnMCUGCSqG
SIb3DQEJARYYZ2lvdmFubmltYXp6ZWlAZ21haWwuY29tMB4XDTExMDM
yNzE2NDQz
NloXDTEyMDMyNjE2NDQzNlowLTEOMAwGA1UECxMFSG9zdHMxGzAZ
BgNVBAMTEmdy
YWRpdXMubWljYXNhLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwg
YkCgYEArToz
Jo1GI8/fPzGlcMjcoz1jyOd8nzTGUqA3vln+NnZX16Rfdy/wsC0qtfz/FOjLlqE1
9z6Xms+DmwVKM4kT3PCOIIGih3B6zYnRETJ9kBbnwlfSiRkVbtXq/jrm78B
P0+dX
HURSO3CpQWSgHwdA+INwVS9wUIn/eSdSXWhdKnkCAwEAAaNMMEow
HQYDVR0lBBYw
FAYIKwYBBQUHAwEGCCsGAQUFBwMCMCkGA1UdEQQiMCCCEmdyY
WRpdXMubWljYXNh
LmNvbYcEwKj6/ocEwKgASzANBgkqhkiG9w0BAQQFAAOBgQAH+pK1HA
D+8OweVEVP
2sBSJARmvjvyx5PgOX4XvQTbM7fy/
+fgjawhIcLBAiVZOdnPW0y1147O3FIeHTdu
e2VVhcrfAEAB6R8NZwLCpAmiKG7W0Etp3MG6YZe3k2k5AORkbFUN/6vx
qfK24nDT
XYPFqdOGBRHsyT69jGVSX7OAxA==
-----END CERTIFICATE-----

Figura 4.14.3 Certificado de Seguridad X.509
Fuente: Elaboración propia.

Para crear usuarios locales se hace clic en la opción "**Users**" del apartado "**USERS**" del menú de la izquierda de la pantalla:

Como se puede ver, tan sólo aparece el usuario "**admin**". Para crear uno nuevo, se oprime en el botón "Add" del menú superior y aparecerá un formulario donde se añaden los datos:

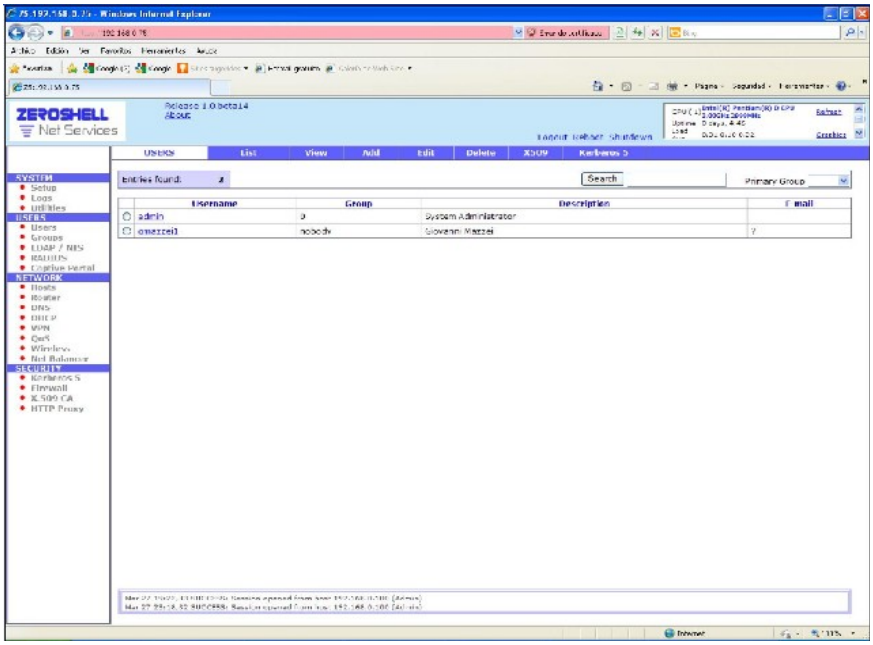

Figura 4.15 Creación de Usuarios.
Fuente: Elaboración propia.

A continuación se procede a agregar un nuevo usuario, como se observa en la Fig.4.16, se debe llenar los campos con información referente a nuestro usuario, el cual es el que se va a autenticar en el sistema de control de acceso contra el RADIUS.

Como mínimo, se coloca el nombre de usuario, el password, el nombre y apellido. Si no introducimos el home de usuario, le pondrá /home/nombredelusuario.

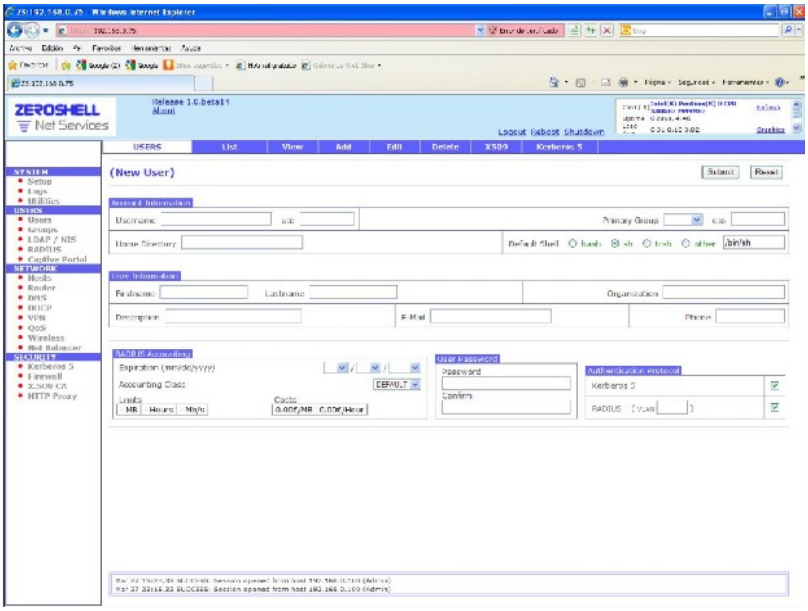

Figura 4.16 Formulario para la Creación de Usuarios.
Fuente: Elaboración propia.

Configurando RADIUS

El siguiente paso a seguir es configurar **RADIUS**. Para ellose hace clic en la opción "**RADIUS**" del menú "**USERS**" que se encuentra a la izquierda de la pantalla, como se observa en la Fig.4.17:

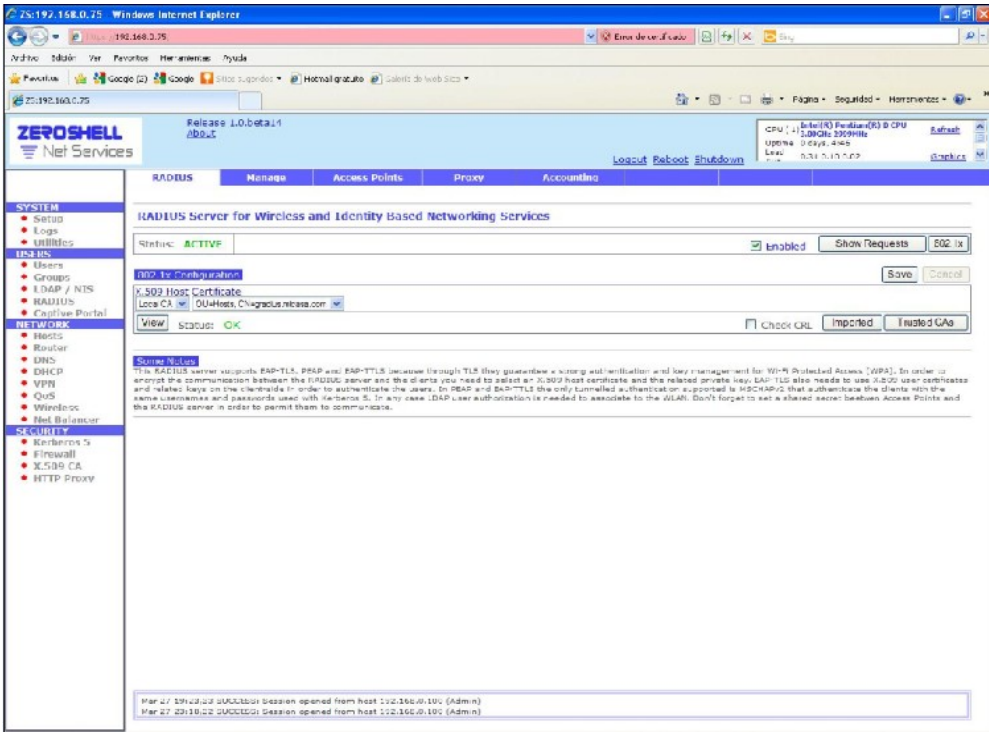

Figura 4.17 Configuración del Servidor RADIUS.
Fuente: Elaboración propia.

Como se observa el servicio RADIUS aún no está activo. Antes de activarlo, se registran los puntos de acceso que van a poder contactar con el servidor RADIUS:

De los tres botones que hay para configurar el servidor RADIUS, se hace clic en el botón "**Access Points**". Como se observa en la Fig.4.18

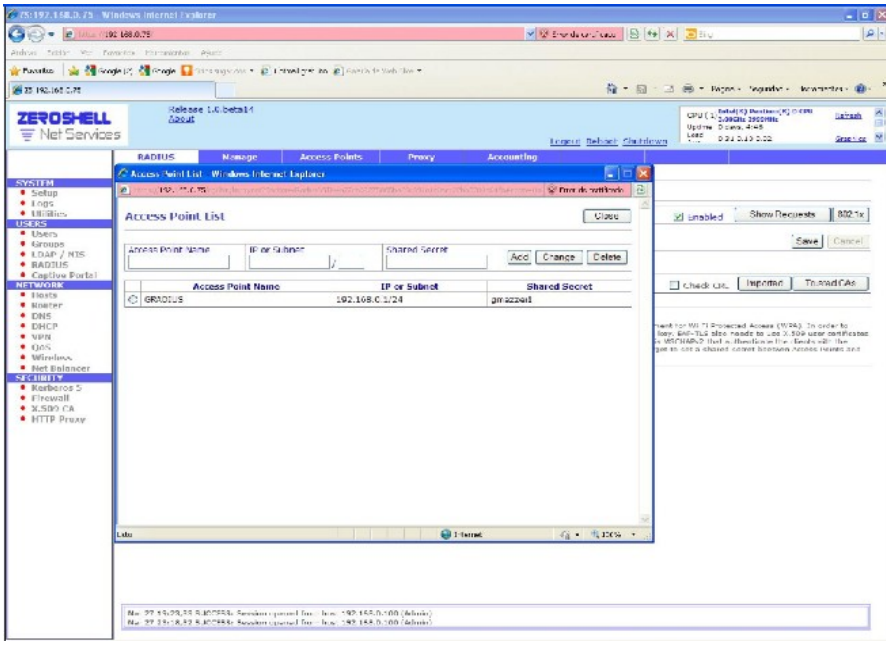

Figura 4.18 Lista de los Puntos de Acceso (Access Point) a ser utilizados. Fuente: Elaboración propia.

Para cada punto de acceso que vaya a comunicarse con el servidor RADIUS se específica un **nombre** que servirá para identificarlo, su **IP**, la **máscara de red** y una **contraseña** compartida entre el servidor RADIUS y el punto de acceso. La contraseña debería ser una combinación de caracteres numéricos y alfanuméricos mayúscula y minúscula. No puede ser de más de 32 caracteres.

Como se observa en la Fig.4.19, se agregó el access point **GRADIUS**, con la ip 192.168.0.1/24 con el shared secret **gmazzei1**

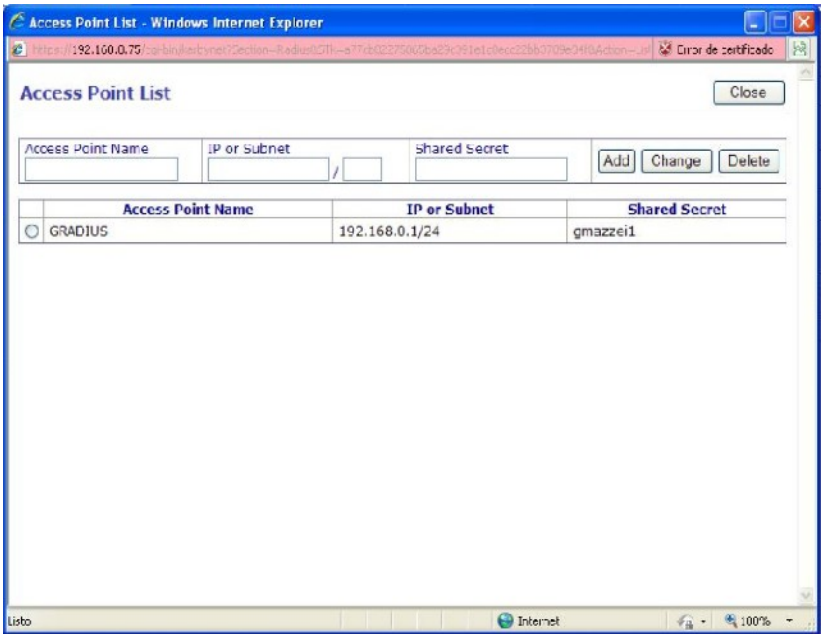

Figura 4.19 Introducción de los datos del Punto de Acceso (Access Point) a ser utilizado.
Fuente: Elaboración propia.

Una vez introducidos los datos de cada punto de acceso se pulsa el botón "**Add**" y se añadirá a la lista. Cuando se finaliza el añadir los puntos de acceso, se oprime el botón "**Close**". Ahora que ya se tiene registros de los puntos de acceso se activa el servidor marcando la casilla "**Enabled**", como en la Fig.4.20.

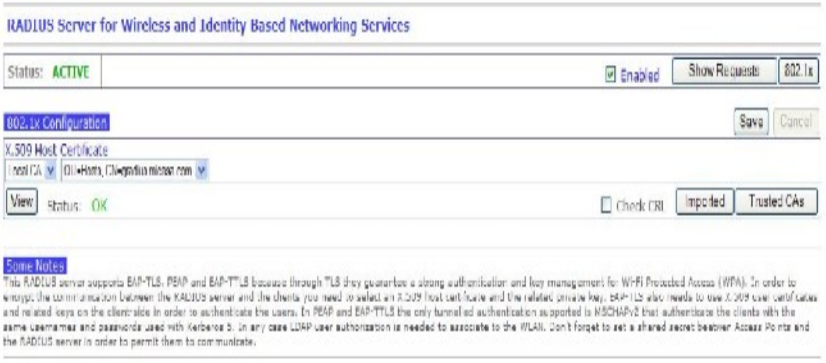

Figura 4.20 Activación del Servidor RADIUS.
Fuente: Elaboración propia.

En la Fig.4.21 se puede visualizar en los logs la autenticación satisfactoria

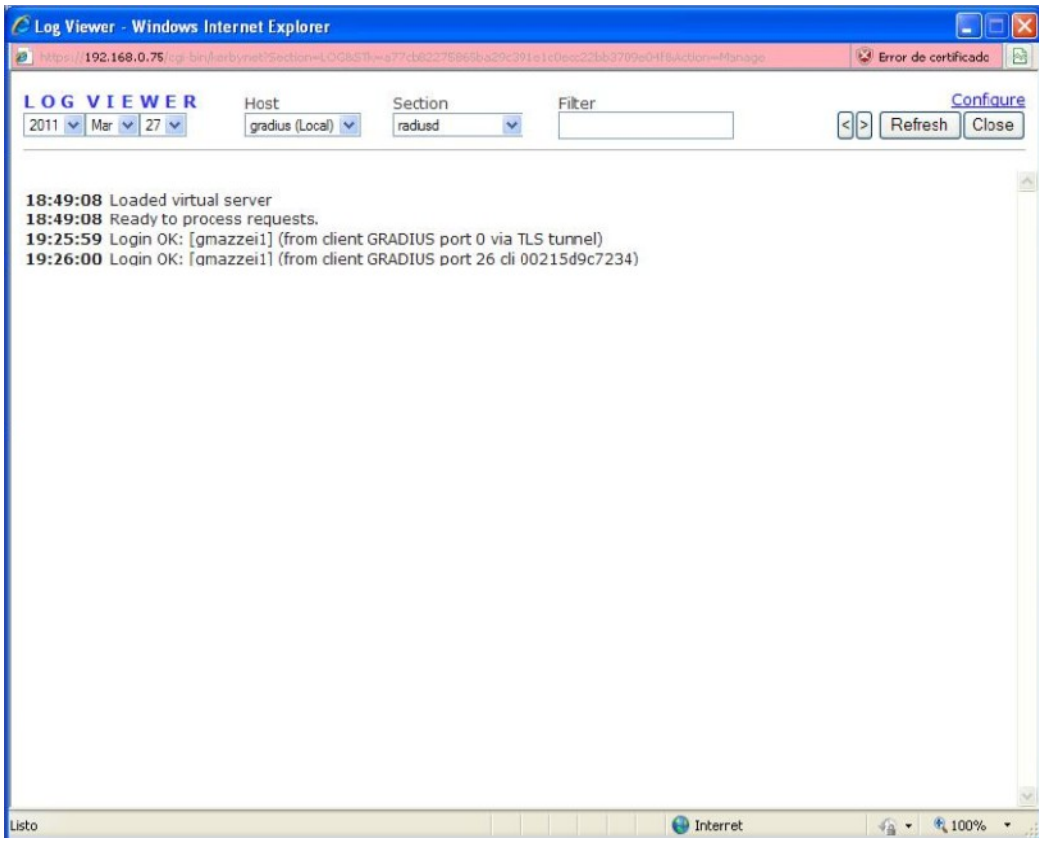

Figura 4.21 Visualización de la autenticación, mediante logs, facilitada por la herramienta.
Fuente: Elaboración propia.

A continuación, en otra muestra de Logs, puede observarse la autenticación satisfactoria, al punto de acceso, cuya IP, es la 192.168.0.1/24, específicamente en la sección o estándar 802.1X, que garantiza como lo hemos comentado, la seguridad a partir de la capa 2 del modelo OSI. Podemos visualizar también en el proceso o secuencia de autenticación, el protocolo PEAP (Protected Extensible Authentication Protocol), la cual proporciona una autenticación basada en el password.

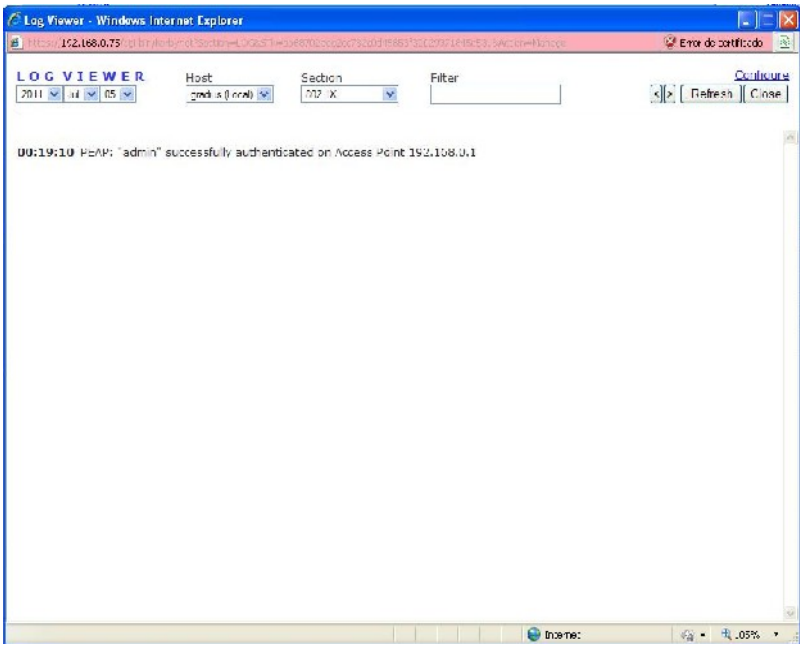

Figura 4.21.1 Visualización de la autenticación, mediante logs, sección 802.1X. Fuente: Elaboración propia.

Configurando Punto de Acceso (Access Point).

El siguiente paso será configurar nuestro punto de acceso. Se accede a él mediante la interfaz web y se busca la opción que permita configurarlo. Como punto de acceso he utilizado un router Linksys WRT54GS.

Los datos para su configuración básica son los siguientes:

Router Name	GRADIUS
Host Name	GRADIUS
Domain Name	micasa.com
MTU	Auto
Local IP Address	192.168.0.1/24
DHCP	Enable

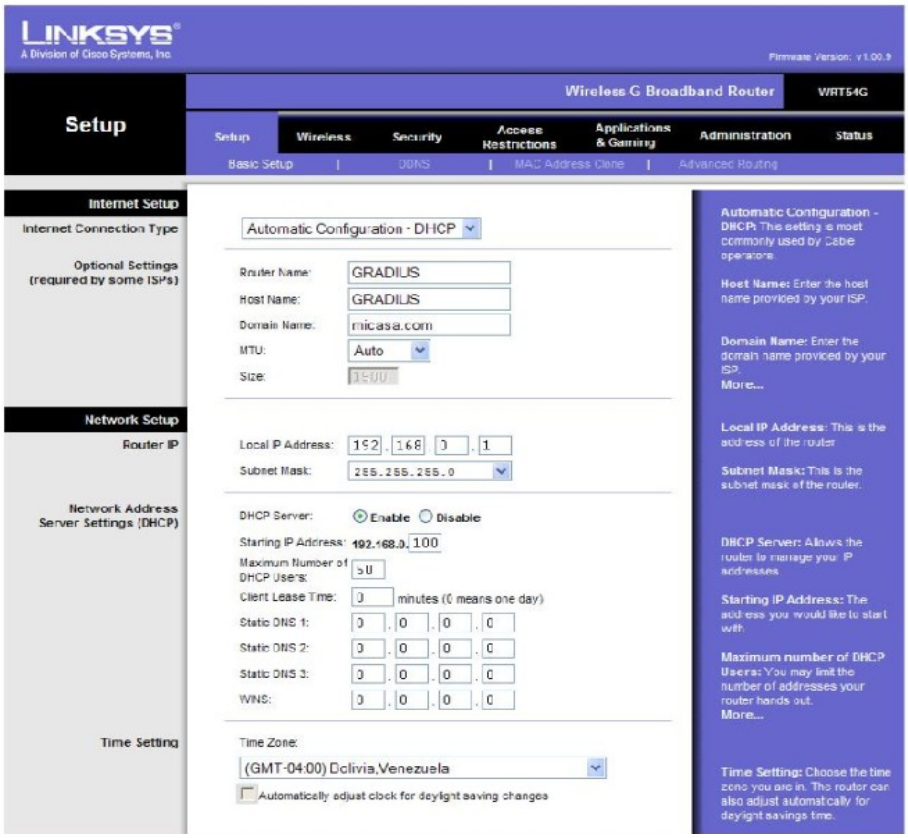

Figura 4.22 Interfaz Gráfica de Usuario para la administración del Access Point. Fuente: Elaboración propia.

Ubicamos en la sección Wireless, la pestaña Basic Wireless Setings:

Wireless Network Mode	**Mixed**
Wireless Network Name (SSD)	**Linksys**
Wireless Channel	**6-2 437GHz**
Wireless SSID Broadcast	**Enable**

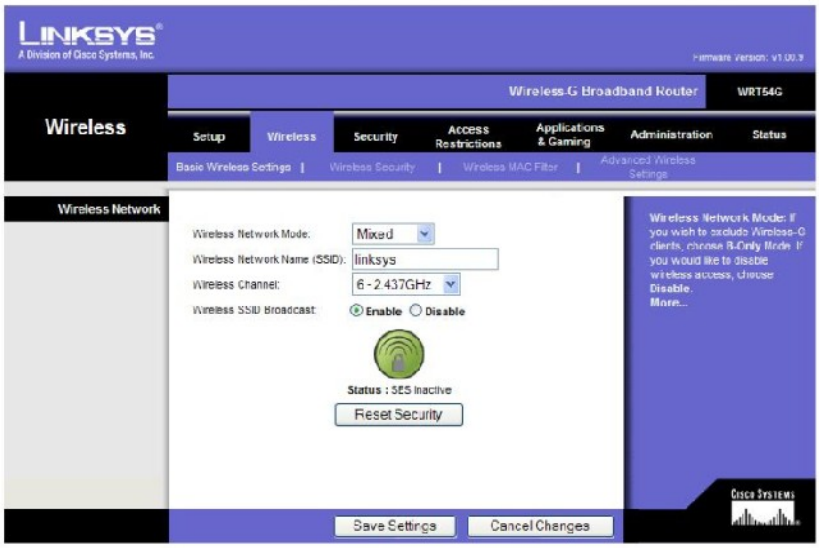

Figura 4.23 GUI Wireless Security.
Fuente: Elaboración propia.

En la sección Wireless, específicamente en la pestaña Wireless Security tenemos la siguiente configuración:

Security Mode	**WPA2**
WPA Algorithms	**AES**
Radius Server Address	**192.168.0.75**
Radius Port	**1812**
Shared Key	**gmazzei1**
Key Renewal Timeout	**3600**

En cuanto a la clave que se debe colocar en el apartado "**Radius Auth Shared Secret**" es la que se crea en la casilla "**Shared secret**" cuando se configuró el punto de acceso en ZeroShell.

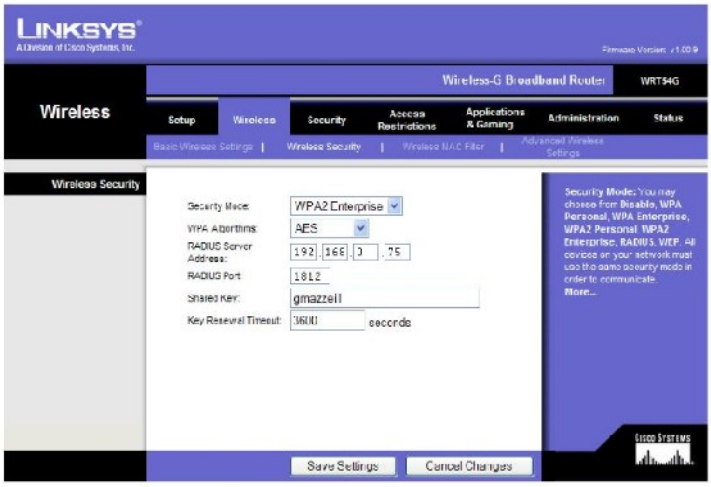

Figura 4.24 Configuración del Shared Key.
Fuente: Elaboración propia.

Configurando un cliente en Windows XP:

Primero exporta tu CA de ZeroShell. Para ello, ve la pantalla de radius en ZeroShell y pulsa el boton "trusted CA". Esto generara un pop-up:

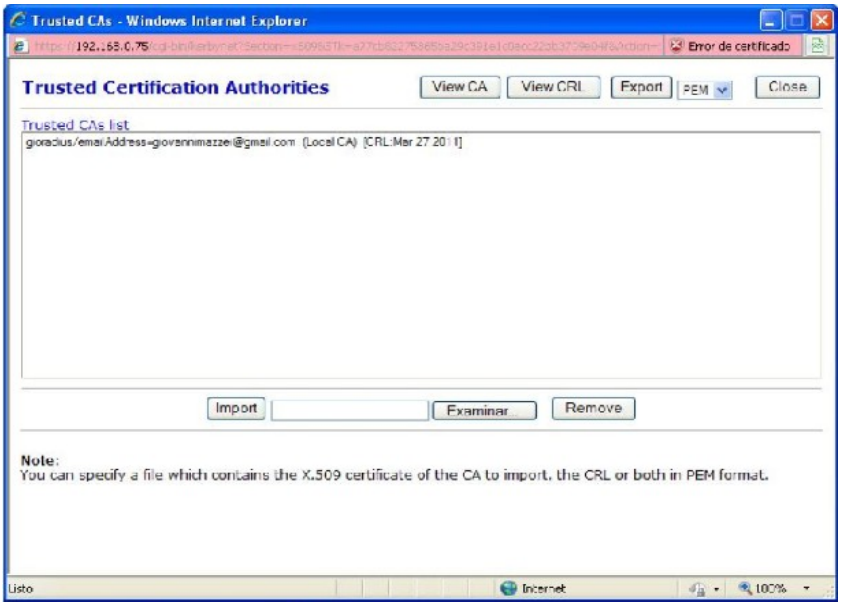

Figura 4.25 Exportación del Certificado de Autenticación (CA).
Fuente: Elaboración propia.

A continuación, seleccione el CA y pulsa el botón Exportar. El navegador se descargara un archivo llamado "TrustedCA.pem". Ahora, en Windows, seleccionamos Inicio, Ejecutar, y escribimos MMC y pulsamos aceptar, en la nueva ventana pulsamos archivo, y agregar o quitar complemento, después hacemos click en Agregar y seleccionamos Certificados. En la siguiente pantalla, seleccione "administracion de equipos" y "Equipo local". A continuación pulsamos Aceptar.

Se debes tener las pantallas similares a estas:

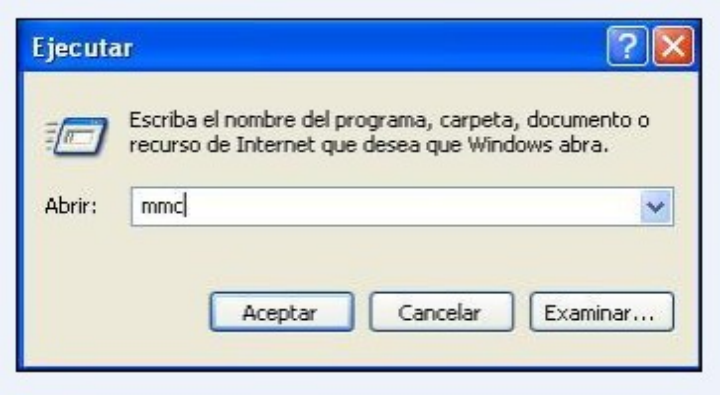

Figura 4.26 Ejecución del comando MMC en Windows.
Fuente: Elaboración propia.

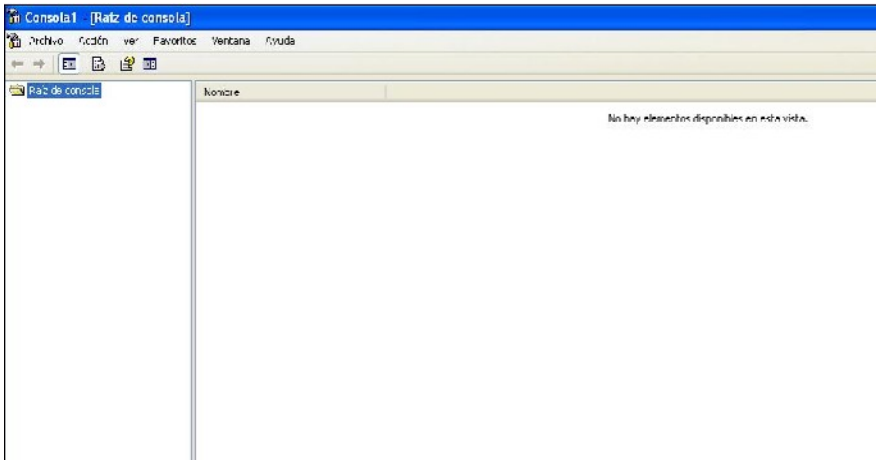

Figura 4.27 Ubicación del la Raíz de Consola
Fuente: Elaboración propia.

Se selecciona la pestaña **Archivo** y se escoge **"Agregar o quitar complementos**"

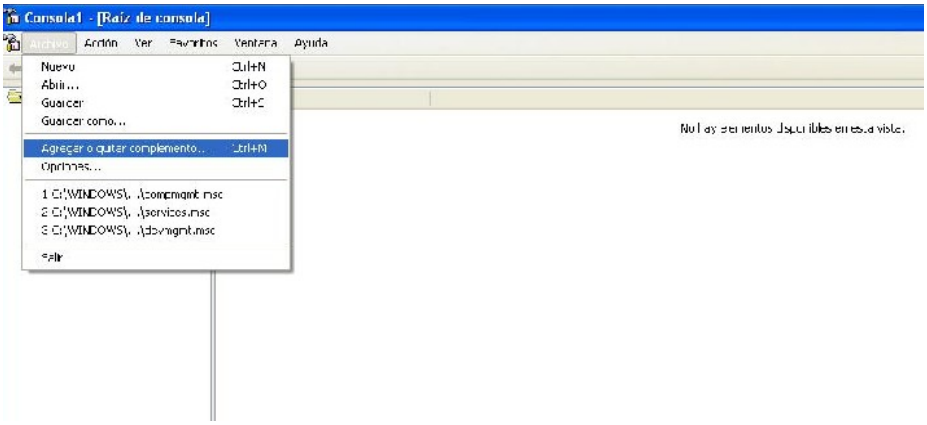

Figura 4.28 Vista para Agregar o Quitar Complementos.
Fuente: Elaboración propia.

Al realizar esta operación, aparece una nueva ventana, para agregar o quitar el complemento. Se selecciona la carpeta que esta a la derecha y se despliega una lista como se observa en la Fig.4.29.

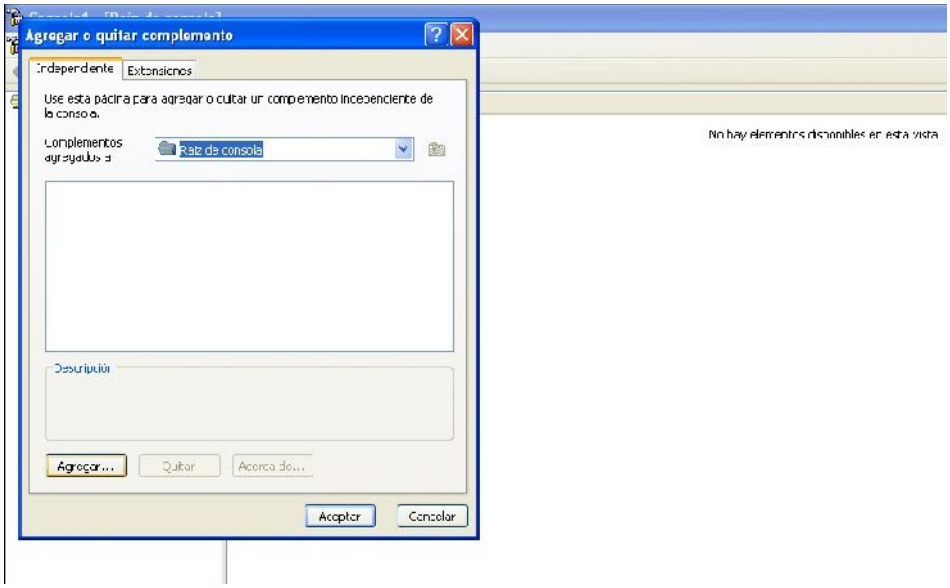

Figura 4.29 Ubicación de la Raíz de Consola para exportar Certificados.
Fuente: Elaboración propia.

Se selecciona "**Certificados**", se abre una ventana, donde se debe tildar la opción "**Cuenta de equipo"**

Figura 4.30 Ubicación de Certificados de Autenticidad.
Fuente: Elaboración propia.

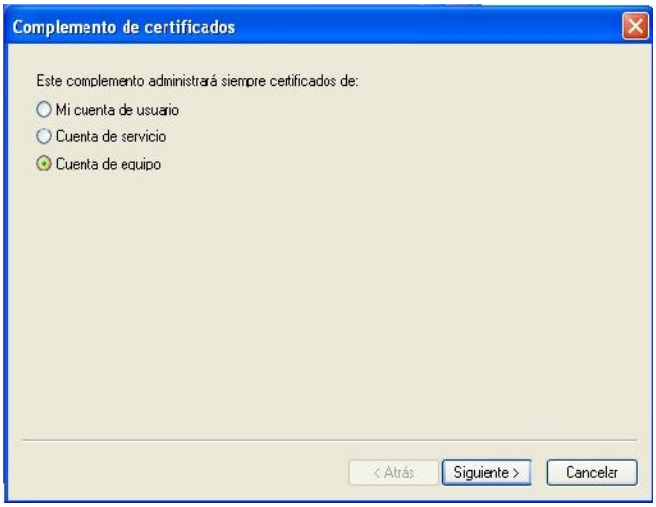

Figura 4.31 Selección de la opción "Cuenta de equipo".
Fuente: Elaboración propia.

A su vez se establece la siguiente ventana, la cual debemos tildar la opción "**Equipo local"**

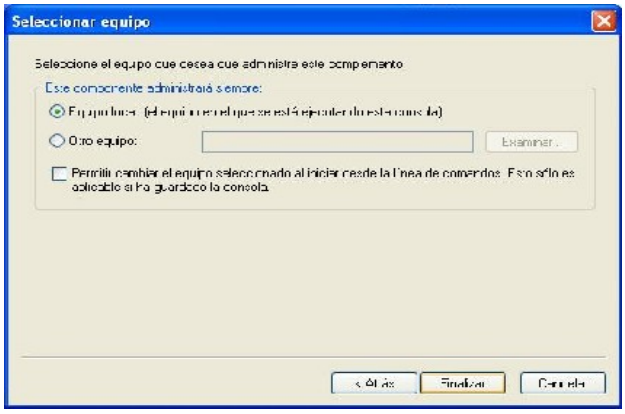

Figura 4.32 Selección de la opción "Equipo local".
Fuente: Elaboración propia.

Una vez hecho esto, aparecerá la lista que a continuación visualizamos en la Fig.4.33, donde se localiza el certificado, llamado **gradius.**

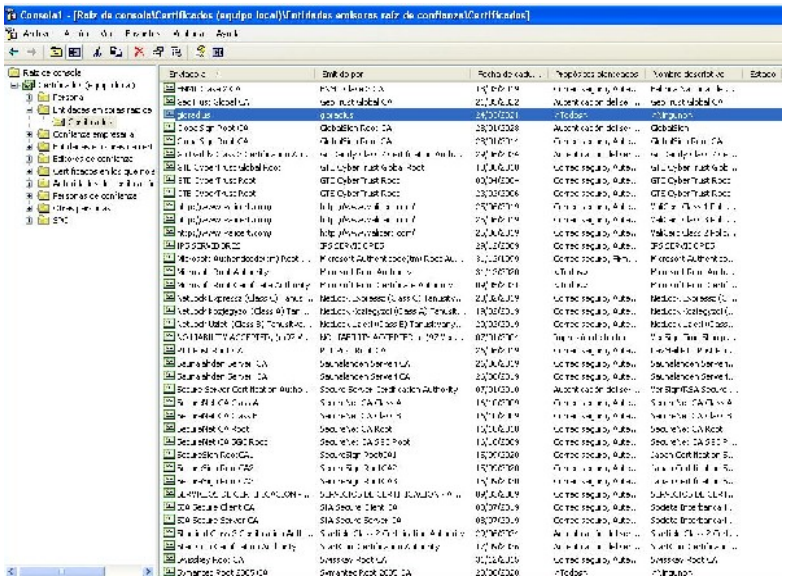

Figura 4.33 Ubicación del Certificado de Autenticidad "gradius".

Fuente: Elaboración propia.

A continuación se despliega la raíz "trusted root certification, y se hace clic en Certificados, Ahora, se importa el archivo de certificado que exportaste desde ZeroShell

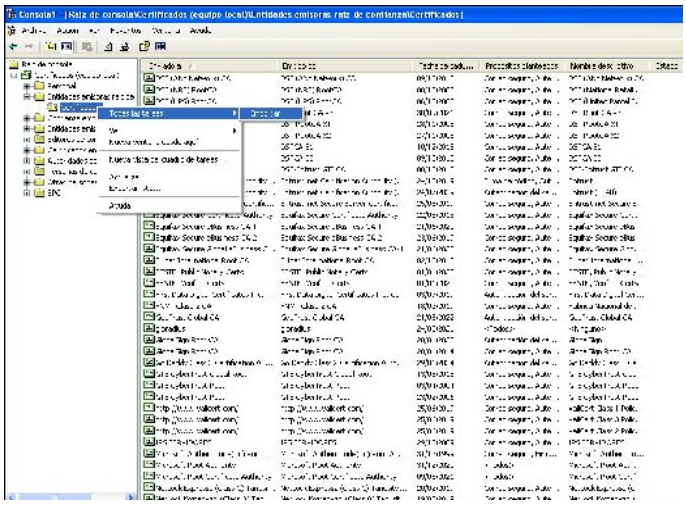

Figura 4.34 Exportación del Certificado de Autenticación "gradius".

Fuente: Elaboración propia.

Se despliega un asistente para poder importar el Certificado

Figura 4.35 Asistente para la Exportación del Certificados.
Fuente: Elaboración propia.

Al oprimir el botón **Siguiente**, se observa un campo vacío y la opción de "Examinar", al hacer click a dicha opción, se trae la ruta donde se descarga el Certificado que se importó de la herramienta de Zeroshell.

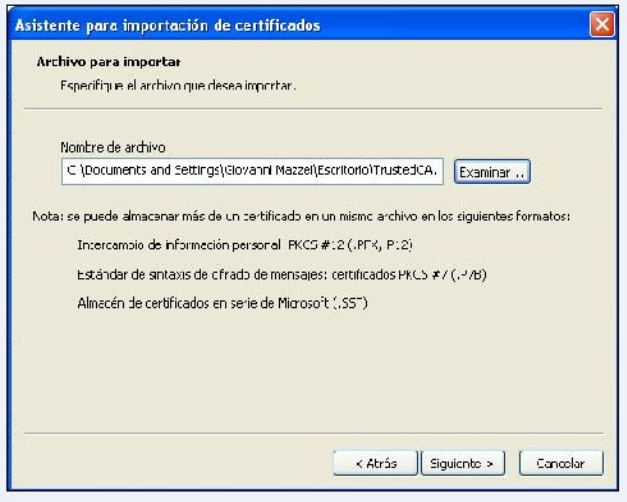

Figura 4.36 Ruta de ubicación del Certificado de Autenticación.
Fuente: Elaboración propia.

A continuación, se ubica la pestaña de Redes inalámbricas en las propiedades de la tarjeta inalámbrica, como se observa en la Fig.4.37:

Figura 4.37 Selección de la Red Inalámbrica (linksys).
Fuente: Elaboración propia.

Se hace click en el botón Propiedades de la red en cuestión. Para autentificación de red, se selecciona WPA2, y para cifrado de datos seleccione, AES:

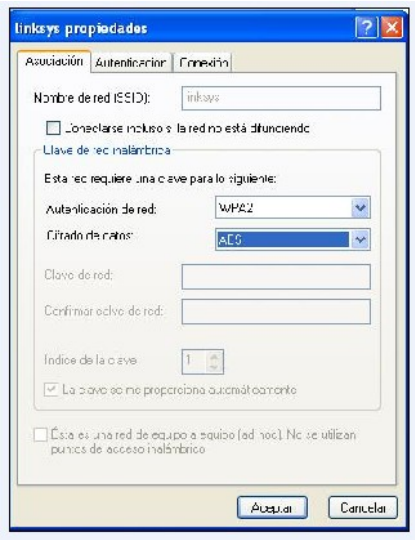

Figura 4.38 Selección de la Autenticación de Red y Cifrado de Datos.
Fuente: Elaboración propia.

Se pulsa la pestaña Autentificación, marcamos la casilla "Enable IEEE 802.1x ", y seleccionamos PEAP para su tipo de EAP. Nos aseguramos que de las otras dos casillas de verificación están sin marcar:

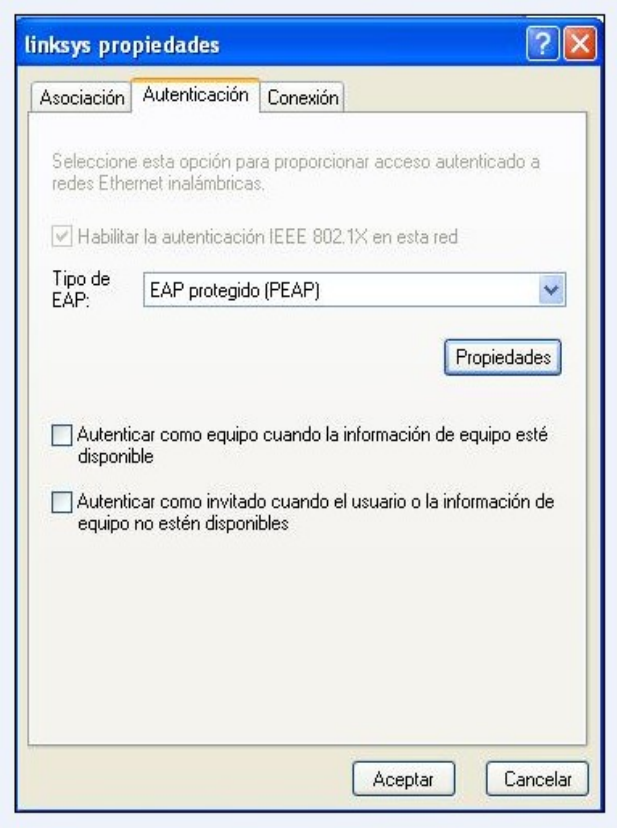

Figura 4.39 Selección del tipo de EAP.
Fuente: Elaboración propia.

Se selecciona la opción **Propiedades**. A su vez la casilla de verificación para su CA raíz. La cuál es **gradius CA**. Asimismo, se define el método de autenticación de MSCHAP.

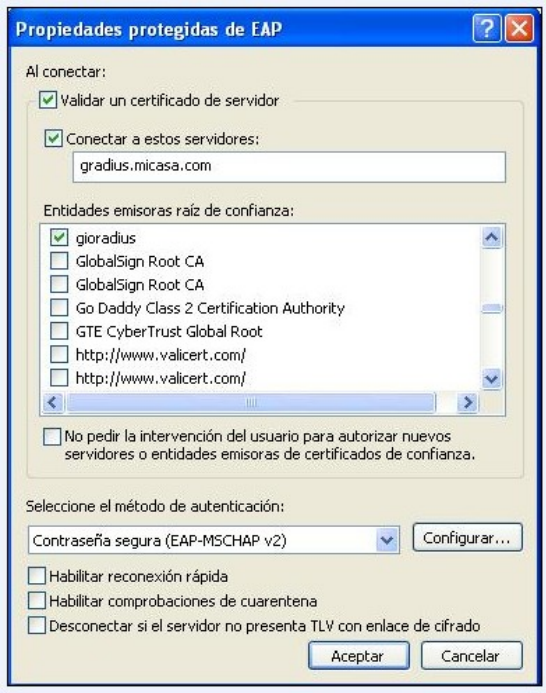

Figura 4.40 Selección del Método de Autenticación y Servidor.
Fuente: Elaboración propia.

Se pulsa el botón Configurar para MSCHAP y se valida que la casilla "Usar automáticamente mi nombre de inicio de sesión y contraseña de Windows" esté sin marcar.

Puede observarse, el icono de nuestra red, llamado linksys, con seguridad habilitada con WPA2, como en la Fig.4.41

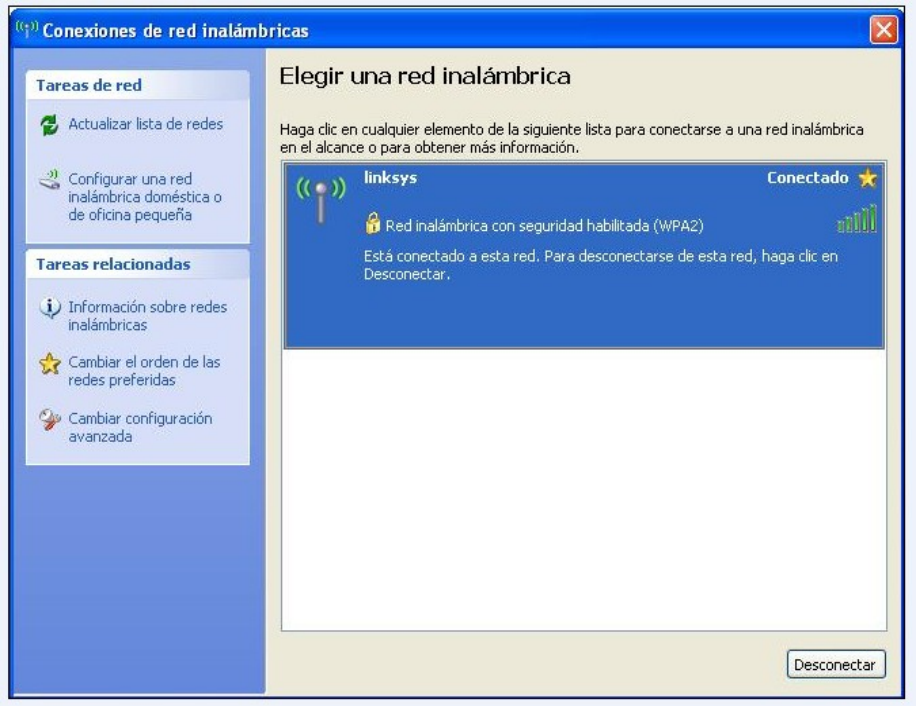

Figura 4.41 Visualización de la Red Inalámbrica con Seguridad Habilitada (WAP2).
Fuente: Elaboración propia.

Para finalizar la sesión con ZeroShell, lo que se debe escoger del menú, es la opción **<H>,** una vez seleccionada dicha opción aparece este aviso, como se observa en la figura. Para apagarla se escogería **(y)** si no, escogemos **(n).**

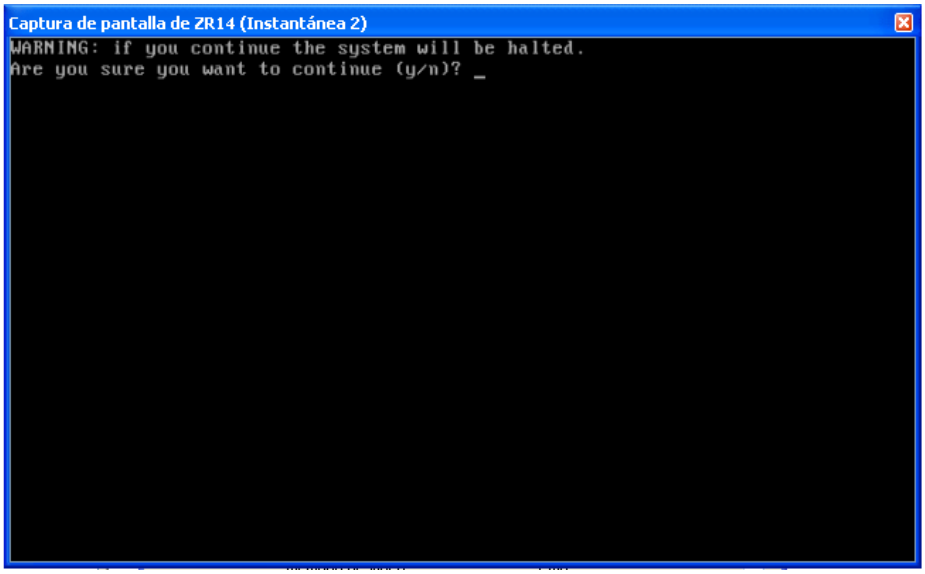

Figura 4.42 Pantalla de finalización de ZeroShell.
Fuente: Elaboración propia.

Escogido la opción **(y),** afirmando para apagarla, se observa como los servicios se detienen y finalizan.

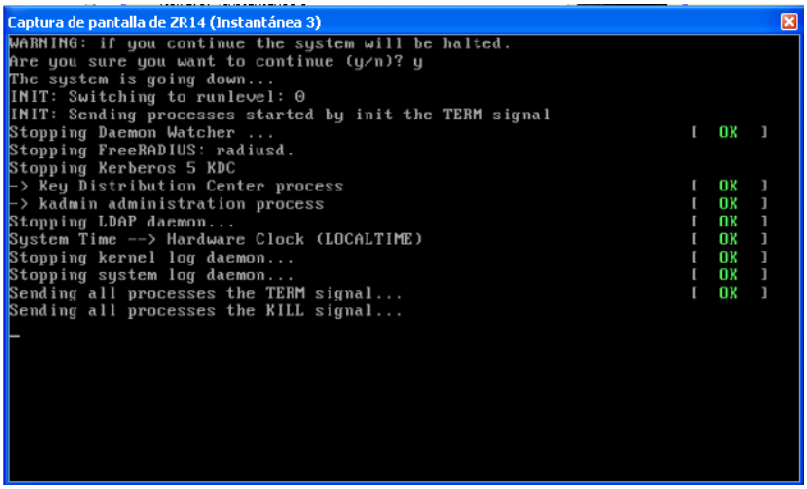

Figura 4.43 Finalización de los servicios de ZeroShell.
Fuente: Elaboración propia.

4.6 Auditoría a redes WLAN – ZeroShell.

Una vez concluido el laboratorio, y recreado el ambiente de red, se realiza una revisión del trafico que ingresa o egresa de la rede inalámbrica estudiada. Para tal fin se habilitó el sniffer Wireshark para la tarjeta inalámbrica Wi-Fi, para observar el tráfico entre las dos máquinas, tal como se muestra en la figura 4.44.

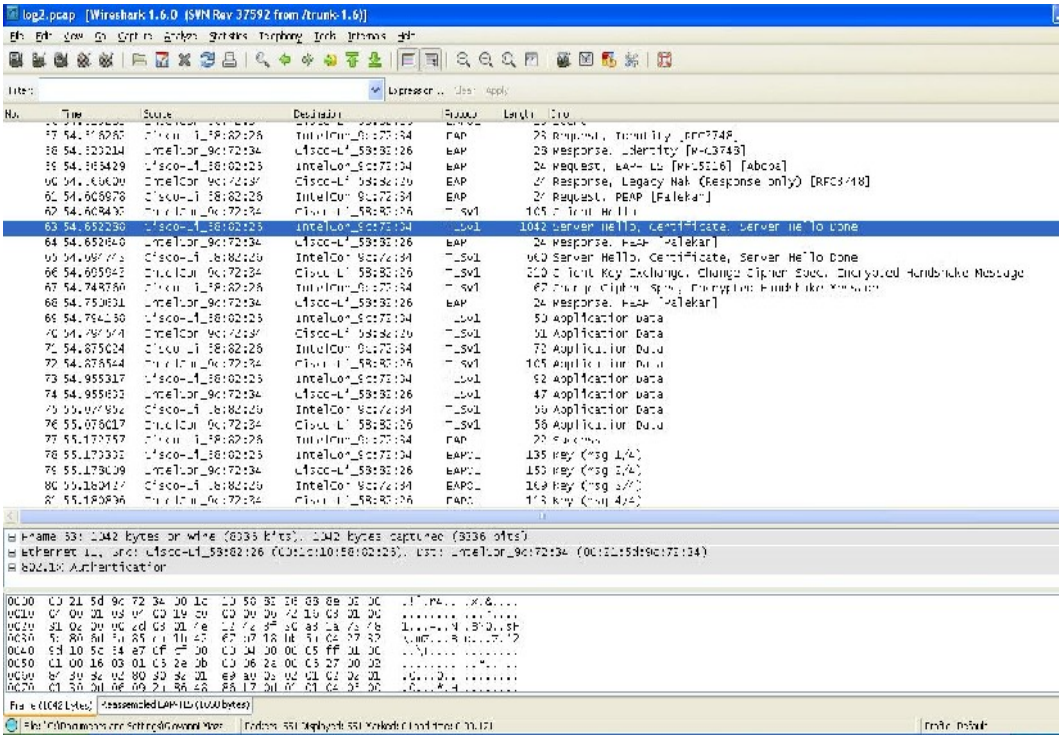

Figura 4.44 Visualización de tráfico por la red inalámbrica.
Fuente: Elaboración propia.

Al realizar el análisis del tráfico de los paquetes, se puede observar en la fig.4.45, como se realiza la autenticación mediante el protocolo EAP (Extensible Authentication Protocol), que en conjunto se observó también en los logs tomados de la herramienta ZeroShell.

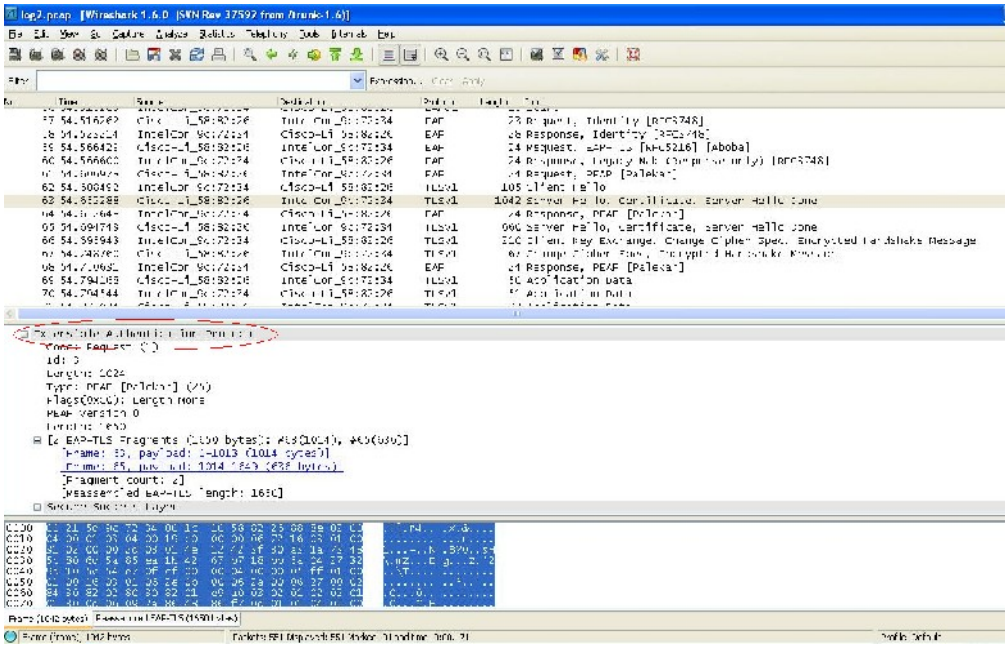

Figura 4.45 Visualización del protocolo EAP (Extensible Authentication Protocol).
Fuente: Elaboración propia.

Luego de analizar los paquetes capturados, se pudo notar que la información visible intercambiada entre ambos era la del certificado digital. Esta información no está visible de manera directa para un usuario que escuche la interfaz inalámbrica, ya que se encuentra cifrada.

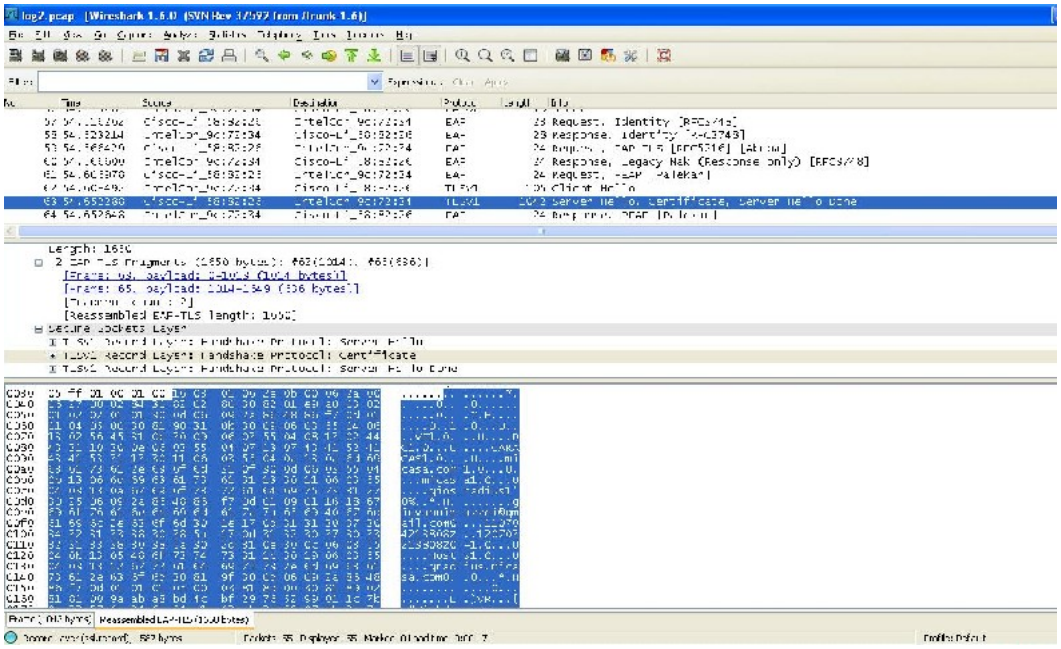

Figura 4.46 Visualización del Certificado Digital, a través del sniffer Wireshark.
Fuente: Elaboración propia.

4.7 Selección de la herramienta (FreeRADIUS).

Para realizar el diseño y configuración del siguiente sistema de control de acceso a WLAN mediante EAP y RADIUS, se escogió la herramienta basada en software libre FreeRADIUS, que correrá bajo el sistema operativo Ubuntu, el cual se instalará en una maquina virtual (VMware), esto permitirá elaborar la arquitectura propuesta y plasmar las ventajas de las mismas. A continuación veremos las propiedades de cada una de ella.

4.7.1 GNU/Linux.

La principal razón para la elección de la plataforma GNU/Linux sobre el sistema operativo Windows no está asociada a una reducción de costos. Elegir código libre no es fomentar código gratis. Es así como lo expresa Richard Stallman, con su lema; "Free as is freedom" versus "Free as in free beer". El código abierto tiene la característica de mantenerse libre, que no es lo mismo que ser gratis. Para mantener esta libertad, los Proyectos de Open Source se mantienen con una filosofía de crear un entorno con estándares abiertos. Esto asegura una plataforma de desarrollo abierto para todos los que tengan interés.

GNU/Linux es un proyecto que comprueba la validez de una filosofía abierta. Ha crecido desde ser calificado como un sistema operativo "amateur", hasta lograr ser uno de los competidores más fuertes que ha tenido el mercado de servidores; y desde hace mucho tiempo con soporte empresarial. El gran valor que puede ofrecer este sistema operativo debe ser la capacidad de integrar las diversas tecnologías desarrolladas en esta plataforma con fabricantes terceros.

Dependiendo del tamaño de instalación, es impensable el uso de una implementación Windows debido a su alto coste de licenciamiento. Por otro lado muchas instalaciones del tipo embebido simplemente utilizan GNU/Linux como sistema operativo en la propia máquina debido a su ligereza, por ejemplo, Suse comienza a desarrollar una nueva plataforma embebed con soporte, con lo que se puede crear fácilmente un equipo de bajo o medio coste con Linux embebida y aprovecharlo para su uso como servidor RADIUS.

4.7.2 FreeRADIUS

El principal motivo para elegir FreeRADIUS como servidor de autenticación es su relación coste-calidad, que a coste cero ofrece un rendimiento y una potencia muy elevada. Es cierto que lo que se conoce como TCO (Total Ownership Cost o coste

total de propiedad) no es igual a cero, ya que la valoración del coste del hardware, el coste de mano de obra de implementación, formación y mantenimiento siempre es importante. Pero igualmente la inversión en costes de licenciamiento es muy alta en productos propietarios de fabricantes como Cisco, Juniper Networks, etc.

FreeRADIUS cumple y colabora con los estándares dedicados a RADIUS, por lo que es un servidor RADIUS estándar que puede ser implementado para dar soporte a cualquier plataforma que soporte múltiples módulos que incluye. Como servidor de RADIUS, es uno de los más versatiles del mercado, incluyendo los de pago o los libres.

Estas son las caracteristicas de FreeRADIUS:

- FreeRADIUS se puede instalar como daemon en cualquier sistema operativo UNIX, Linux o Solaris, tanto en plataformas x86, x64 o cualquier otra soportada por estos sitemas.

- FreeRADIUS es compatible con casi cualquier plataforma o sistema operativo (Windows, Linux, MacOs, WindowsCE, PocketPC, sistemas móviles, etc.)

- FreeRADIUS soporta una gran variedad de Bases de Datos y servidores de directorio, como Oracle, MS SQL Server, MySQL, Active Directory, LDAP, Unix, etc.

- Soporte para gran cantidad de módulos de autenticación como PAP, CHAP, MS-CHAPv1 y v2, SIP y la mayor parte de los tipos de EAP.

- Soporte para la mayor parte de lenguajes de programación como Perl, Python, Java y PHP.
- Soporte para la asignación de IP basado en IP pools.

- Compatible con una infraestructura basada en certificados PKI.

- FreeRADIUS soporta más de cien diccionarios actualizados de VSA.

- Al ser un servidor OpenSource, permite la participación en la comunidad para su desarrollo, y en listas de correo para las consultas de soporte.

4.7.3 Topología de Red.

En la Fig.4.47, se observa la topología de red propuesta para la realización del laboratorio.

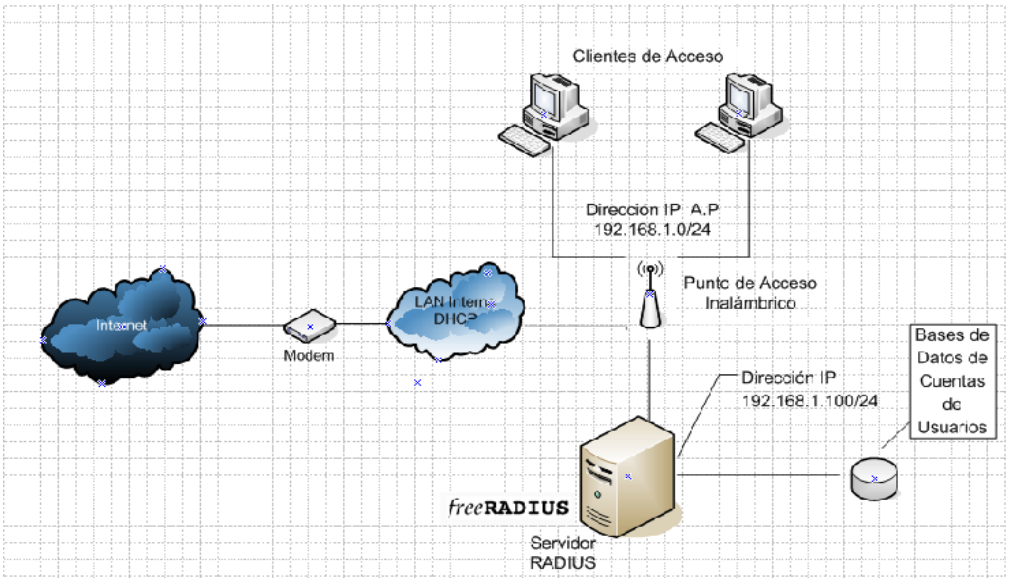

Figura 4.47 Escenario de prueba utilizando FreeRADIUS.
Fuente: Elaboración propia.

4.7.4 Escenario y Pruebas Realizadas

Para la puesta en marcha del laboratorio, se configuró un servidor con el archivo o paquete *freeradius,* se realizó a su vez la configuración de cuatro archivos principales, como lo son: radiusd.conf, eap.conf, clients.conf, users. Todos los

archivos de configuración de Freeradius se encuentran, en la estructura de directorios de Linux, en el directorio */etc/freeradius*. Anteriormente, y todavía en algunos servidores RADIUS se utiliza ***/etc/raddb/***

Cabe destacar los siguientes archivos de configuración:

radiusd.conf - Archivo general de configuración de FreeRADIUS y del daemon.

eap.conf – Archivo de configuración de las directivas EAP a utilizar. Es un include de radiusd.conf

clients.conf – Descripción y credenciales de los diferentes dispositivos que consultan al RADIUS (Aps, NAS, etc).

users – Archivo donde se especifican las credenciales de los usuarios de la red. Se usa este archivo si no existe otro backend para el almacenamiento de los usuarios.

4.7.5 Auditoría a WLAN – FreeRADIUS.

La Fig.4.48 corresponde a la captura mediante el sniffer Wireshark, de dos paquetes o mensajes de autenticación RADIUS contra el servidor FreeRADIUS. El siguiente paquete consiste en un mensaje Access-Request realizado desde un PC contra el servidor FreeRADIUS con la dirección IP 192.168.1.100. El equipo contra el sniffer está en el segmento de red, entre el NAS y el servidor RADIUS:

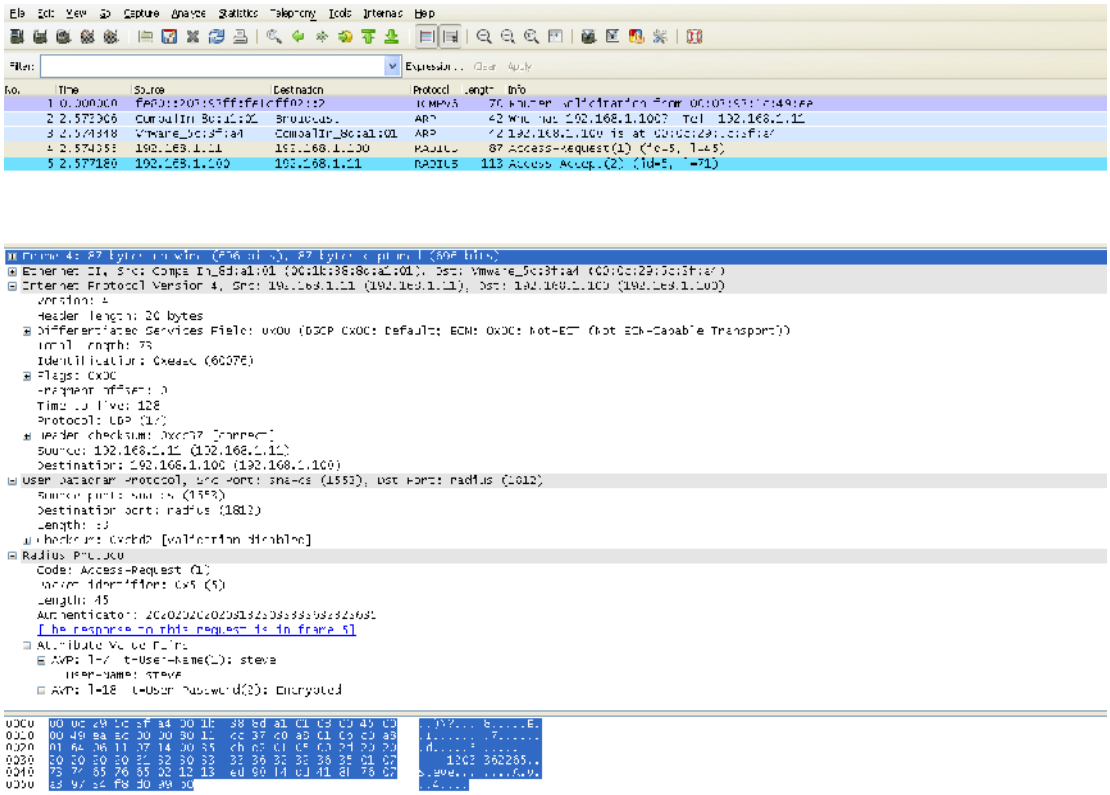

Figura 4.48 Captura mediante sniffer Wireshark de paquetes RADIUS. Fuente: Elaboración propia.

Este paquete es la respuesta recibida del servidor FreeRADIUS aceptando la solicitud de autenticación de cliente en forma de Access-Accept. Puede observarse los atributos de respuesta en el mensaje:

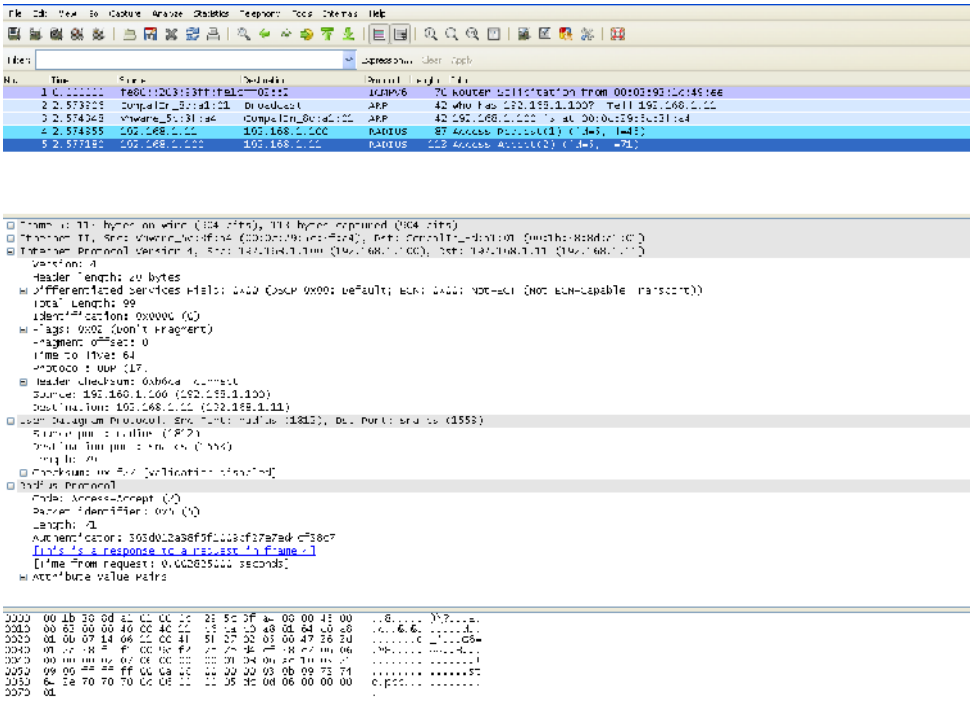

Figura 4.49 Captura mediante sniffer Wireshark de paquetes RADIUS (Access-Accept).
Fuente: Elaboración propia.

A continuación se desglosa el contenido del paquete:

```
No.     Time        Source                Destination
Protocol Info
      5 2.577180    192.168.1.100         192.168.1.11
RADIUS   Access-Accept(2) (id=5, l=71)

Frame 5 (113 bytes on wire, 113 bytes captured)
Ethernet II, Src: Vmware_5c:3f:a4 (00:0c:29:5c:3f:a4), Dst:
00:1b:38:8d:a1:01 (00:1b:38:8d:a1:01)
Internet Protocol, Src: 192.168.1.100 (192.168.1.100), Dst:
192.168.1.11 (192.168.1.11)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
    Total Length: 99
    Identification: 0x0000 (0)
    Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0xb6ca [correct]
    Source: 192.168.1.100 (192.168.1.100)
```

```
    Destination: 192.168.1.11 (192.168.1.11)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 1553
(1553)
    Source port: radius (1812)
    Destination port: 1553 (1553)
    Length: 79
    Checksum: 0x5f27 [correct]
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x5 (5)
    Length: 71
    Authenticator: 363D012A38F5F1009CF27E7ED4CF38C7
    Attribute Value Pairs
        AVP: l=6  t=Service-Type(6): Framed-User(2)
        AVP: l=6  t=Framed-Protocol(7): PPP(1)
        AVP: l=6  t=Framed-IP-Address(8): 172.16.3.33
        AVP: l=6  t=Framed-IP-Netmask(9): 255.255.255.0
        AVP: l=6  t=Framed-Routing(10): Broadcast-Listen(3)
        AVP: l=9  t=Filter-Id(11): std.ppp
        AVP: l=6  t=Framed-MTU(12): 1500
        AVP: l=6  t=Framed-Compression(13): Van-Jacobson-TCP-IP(1)

0000  00 1b 38 8d a1 01 00 0c 29 5c 3f a4 08 00 45 00
..8.....)\?...E.
0010  00 63 00 00 40 00 40 11 b6 ca c0 a8 01 64 c0 a8
.c..@.@......d..
0020  01 0b 07 14 06 11 00 4f 5f 27 02 05 00 47 36 3d
.......O_'...G6=
0030  01 2a 38 f5 f1 00 9c f2 7e 7e d4 cf 38 c7 06 06
.*8.....~~..8...
0040  00 00 00 02 07 06 00 00 00 01 08 06 ac 10 03 21
...............!
0050  09 06 ff ff ff 00 0a 06 00 00 00 03 0b 09 73 74
..............st
0060  64 2e 70 70 70 0c 06 00 00 05 dc 0d 06 00 00 00
d.ppp...........
0070  01                                              .
```

En esta sección se muestra una secuencia completa de autenticación de un suplicante inalámbrico, autenticándose contra un NAS. Para este caso un Linksys WRT-54GL, basado en el firmware DD-WRTv24, que hace de punto de acceso. Se colocó un sniffer Wireshark en la parte alámbrica y otra en la parte inalámbrica.

A continuación se observa como funciona el método completo EAP, capturando paquetes desde el lado inalámbrico para ver todos los paquetes EAPoW. En el lado alámbrico de la red se encuentra los paquetes EAP en formato UDP encapsulados dentro de paquetes RADIUS.

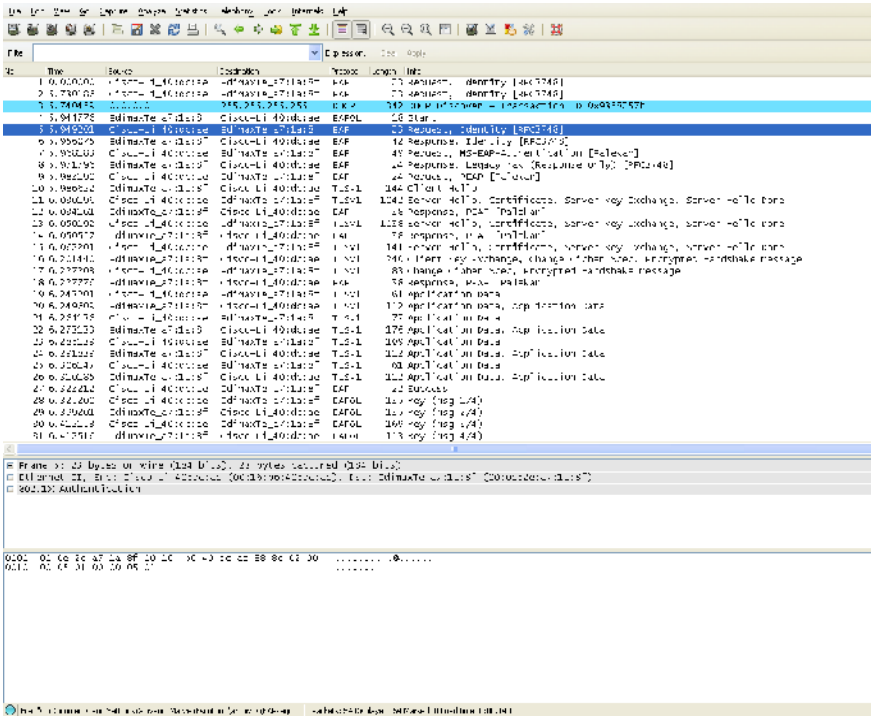

Figura 4.50 Captura mediante sniffer Wireshark de paquete EAP.

Desglose de la secuencia de paquetes:

No. Time Source Destination Protocol Info
1 0.000000 Cisco-Li_40:dc:ae EdimaxTe_a7:1a:8f EAP Request, Identity [RFC3748]

```
Frame 1 (23 bytes on wire, 23 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 5
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 0
        Length: 5
        Type: Identity [RFC3748] (1)
```

No. Time Source Destination Protocol Info
2 5.730186 Cisco-Li_40:dc:ae EdimaxTe_a7:1a:8f EAP Request, Identity [RFC3748]

```
Frame 2 (23 bytes on wire, 23 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 5
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 0
        Length: 5
        Type: Identity [RFC3748] (1)

No.     Time        Source                Destination
Protocol Info
      3 5.740459    0.0.0.0               255.255.255.255       DHCP
DHCP Discover - Transaction ID 0x9358257b

Frame 3 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255
(255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
---------------------------------------------------------------------
No.     Time        Source                Destination
Protocol Info
      4 5.944776    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae
EAPOL    Start

Frame 4 (18 bytes on wire, 18 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 1
    Type: Start (1)
    Length: 0
---------------------------------------------------------------------
----
No.     Time        Source                Destination
Protocol Info
      5 5.949201    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f     EAP
Request, Identity [RFC3748]

Frame 5 (23 bytes on wire, 23 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 5
    Extensible Authentication Protocol
        Code: Request (1)
```

```
        Id: 0
        Length: 5
        Type: Identity [RFC3748] (1)

No.     Time        Source                Destination
Protocol Info
      6 5.956075    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae     EAP
Response, Identity [RFC3748]

Frame 6 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 10
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 0
        Length: 10
        Type: Identity [RFC3748] (1)

-----------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
      7 5.968183    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f     EAP
Request, MS-EAP-Authentication [Palekar]

Frame 7 (49 bytes on wire, 49 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 31
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 1
        Length: 31
        Type: MS-EAP-Authentication [Palekar] (26)
        OpCode: 1 (Challenge)
        MS-CHAPv2-ID: 1
        MS-Length: 26
        Value-Size: 16
        Challenge: 43EA1023F51C82A6F977AA82941063B3

-----------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
      8 5.971796    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae     EAP
Response, Nak (Response only) [RFC3748]
```

```
Frame 8 (24 bytes on wire, 24 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 6
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 1
        Length: 6
        Type: Nak (Response only) [RFC3748] (3)
        Desired Auth Type: PEAP [Palekar] (25)
-------------------------------------------------------------------
---
No.     Time        Source                Destination
Protocol Info
      9 5.983190    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f     EAP
Request, PEAP [Palekar]

Frame 9 (24 bytes on wire, 24 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 6
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 2
        Length: 6
        Type: PEAP [Palekar] (25)
        Flags(0x20): Start
        PEAP version 0
-------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     10 5.986622    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae
TLSv1    Client Hello

Frame 10 (144 bytes on wire, 144 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 112
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 2
        Length: 112
        Type: PEAP [Palekar] (25)
        Flags(0x80): Length
```

```
        PEAP version 0
        Length: 102
        Secure Socket Layer
-------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     11 6.030196    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f
TLSv1    Server Hello, Certificate, Server Key Exchange, Server
Hello Done

Frame 11 (1042 bytes on wire, 1042 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 1024
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 3
        Length: 1024
        Type: PEAP [Palekar] (25)
        Flags(0xC0): Length More
        PEAP version 0
        Length: 2145
        [EAP-TLS Fragments (2145 bytes): #11(1014), #13(1014),
#15(117)]
        Secure Socket Layer
-------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     12 6.034161    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae     EAP
Response, PEAP [Palekar]

Frame 12 (38 bytes on wire, 38 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 6
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 3
        Length: 6
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
-------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
```

13 6.050192 Cisco-Li_40:dc:ae EdimaxTe_a7:1a:8f TLSv1 Server Hello, Certificate, Server Key Exchange, Server Hello Done

```
Frame 13 (1038 bytes on wire, 1038 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 1020
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 4
        Length: 1020
        Type: PEAP [Palekar] (25)
        Flags(0x40): More
        PEAP version 0
        [EAP-TLS Fragments (2145 bytes): #11(1014), #13(1014),
#15(117)]
        Secure Socket Layer
```

No. Time Source Destination Protocol Info
14 6.050557 EdimaxTe_a7:1a:8f Cisco-Li_40:dc:ae EAP Response, PEAP [Palekar]

```
Frame 14 (38 bytes on wire, 38 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 6
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 4
        Length: 6
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
--------------------------------------------------------------------
-----
```

No. Time Source Destination Protocol Info
15 6.062201 Cisco-Li_40:dc:ae EdimaxTe_a7:1a:8f TLSv1 Server Hello, Certificate, Server Key Exchange, Server Hello Done

```
Frame 15 (141 bytes on wire, 141 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
```

```
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 123
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 5
        Length: 123
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        [EAP-TLS Fragments (2145 bytes): #11(1014), #13(1014),
#15(117)]
        Secure Socket Layer
-------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     16 6.201440    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae
TLSv1    Client Key Exchange, Change Cipher Spec, Encrypted
Handshake Message

Frame 16 (240 bytes on wire, 240 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 208
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 5
        Length: 208
        Type: PEAP [Palekar] (25)
        Flags(0x80): Length
        PEAP version 0
        Length: 198
        Secure Socket Layer
-------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     17 6.227203    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f
TLSv1    Change Cipher Spec, Encrypted Handshake Message

Frame 17 (83 bytes on wire, 83 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 65
    Extensible Authentication Protocol
        Code: Request (1)
```

```
        Id: 6
        Length: 65
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        Secure Socket Layer
-------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     18 6.227776    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae     EAP
Response, PEAP [Palekar]

Frame 18 (38 bytes on wire, 38 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 6
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 6
        Length: 6
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
-------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     19 6.243201    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f
TLSv1    Application Data

Frame 19 (61 bytes on wire, 61 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 43
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 7
        Length: 43
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        Secure Socket Layer
-------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
```

20 6.249609 EdimaxTe_a7:1a:8f Cisco-Li_40:dc:ae TLSv1 Application Data, Application Data

```
Frame 20 (112 bytes on wire, 112 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 80
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 7
        Length: 80
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        Secure Socket Layer
```

No. Time Source Destination Protocol Info

21 6.264136 Cisco-Li_40:dc:ae EdimaxTe_a7:1a:8f TLSv1 Application Data

```
Frame 21 (77 bytes on wire, 77 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 59
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 8
        Length: 59
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        Secure Socket Layer
```

No. Time Source Destination Protocol Info

22 6.273133 EdimaxTe_a7:1a:8f Cisco-Li_40:dc:ae TLSv1 Application Data, Application Data

```
Frame 22 (176 bytes on wire, 176 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
```

```
    Type: EAP Packet (0)
    Length: 144
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 8
        Length: 144
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        Secure Socket Layer
-------------------------------------------------------------------------
----
No.     Time        Source                Destination
Protocol Info
     23 6.285139    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f
TLSv1    Application Data

Frame 23 (109 bytes on wire, 109 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 91
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 9
        Length: 91
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        Secure Socket Layer
-------------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     24 6.291839    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae
TLSv1    Application Data, Application Data

Frame 24 (112 bytes on wire, 112 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 80
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 9
        Length: 80
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        Secure Socket Layer
```

```
------------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     25 6.306147    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f
TLSv1    Application Data

Frame 25 (61 bytes on wire, 61 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 43
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 10
        Length: 43
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        Secure Socket Layer
------------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     26 6.310185    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae
TLSv1    Application Data, Application Data

Frame 26 (112 bytes on wire, 112 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 80
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 10
        Length: 80
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        Secure Socket Layer
------------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     27 6.323212    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f     EAP
Success

Frame 27 (22 bytes on wire, 22 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
```

```
802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 4
    Extensible Authentication Protocol
        Code: Success (3)
        Id: 10
        Length: 4
```

Al final de la secuencia puede observarse como se produce el intercambio de claves (Key).

```
-------------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     28 6.325200    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f
EAPOL    Key

Frame 28 (135 bytes on wire, 135 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 117
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x008a
    Key Length: 16
    Replay Counter: 1
    Nonce: 60C7DDCBD7822B658F2A71BD33AAD375A904CB68838E0E69...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Length: 22
    WPA Key: DD14000FAC04AEFA7101B5723BC71A3F546B4F7F6BD5
-------------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     29 6.399201    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae
EAPOL    Key

Frame 29 (135 bytes on wire, 135 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 117
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x010a
    Key Length: 16
    Replay Counter: 1
```

```
    Nonce: 9059B0727E2E46FAD68B80D55B7D0E0965EE9FD8A4D45AC5...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 112BA104727F773CFD1EE7CB59269AC4
    WPA Key Length: 22
    WPA Key: 30140100000FAC040100000FAC040100000FAC010000

No.     Time        Source                Destination
Protocol Info
     30 6.412153    Cisco-Li_40:dc:ae     EdimaxTe_a7:1a:8f
EAPOL    Key

Frame 30 (169 bytes on wire, 169 bytes captured)
Ethernet II, Src: Cisco-Li_40:dc:ae (00:16:b6:40:dc:ae), Dst:
EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f)
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 151
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x13ca
    Key Length: 16
    Replay Counter: 2
    Nonce: 60C7DDCBD7822B658F2A71BD33AAD375A904CB68838E0E69...
    Key IV: A904CB68838E0E69B6868C2575987DC4
    WPA Key RSC: BA00000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 300043A5790F101F24F4FAA868762C68
    WPA Key Length: 56
    WPA Key: 0B422A48E84CEDF5F7D4AB0E059F08BF5D4C476C72349524...
-------------------------------------------------------------------
-----
No.     Time        Source                Destination
Protocol Info
     31 6.412516    EdimaxTe_a7:1a:8f     Cisco-Li_40:dc:ae
EAPOL    Key

Frame 31 (113 bytes on wire, 113 bytes captured)
Ethernet II, Src: EdimaxTe_a7:1a:8f (00:0e:2e:a7:1a:8f), Dst: Cisco-
Li_40:dc:ae (00:16:b6:40:dc:ae)
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 95
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x030a
    Key Length: 16
    Replay Counter: 2
    Nonce: 9059B0727E2E46FAD68B80D55B7D0E0965EE9FD8A4D45AC5...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 605FA1A4ED3E58CD761A5A395A764803
```

```
WPA Key Length: 0
```

Captura de un paquete EAP encapsulado en un paquete RADIUS

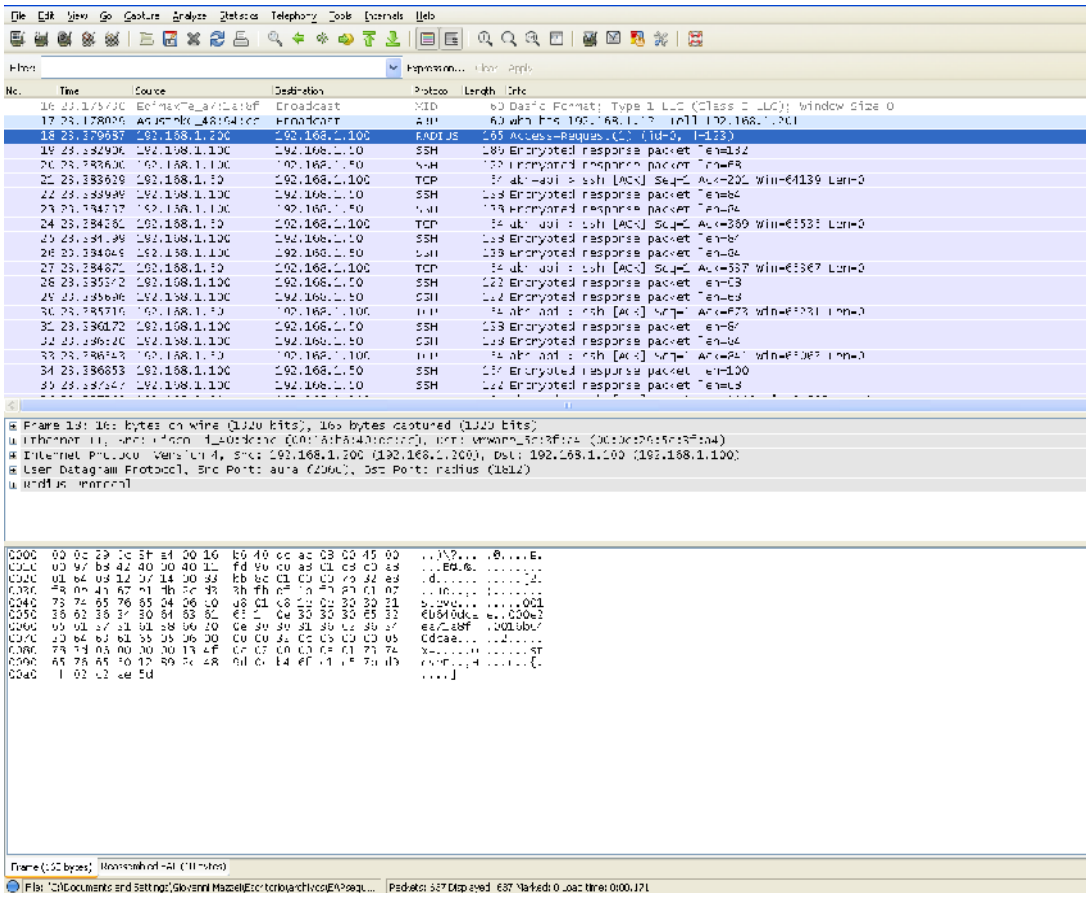

Figura 4.51 Captura de un paquete EAP encapsulado en un paquete RADIUS.

La Fig.4.51 muestra la captura de un paquete Access-Request con el contenido EAP, desde el lado del segmento de red del servidor RADIUS.

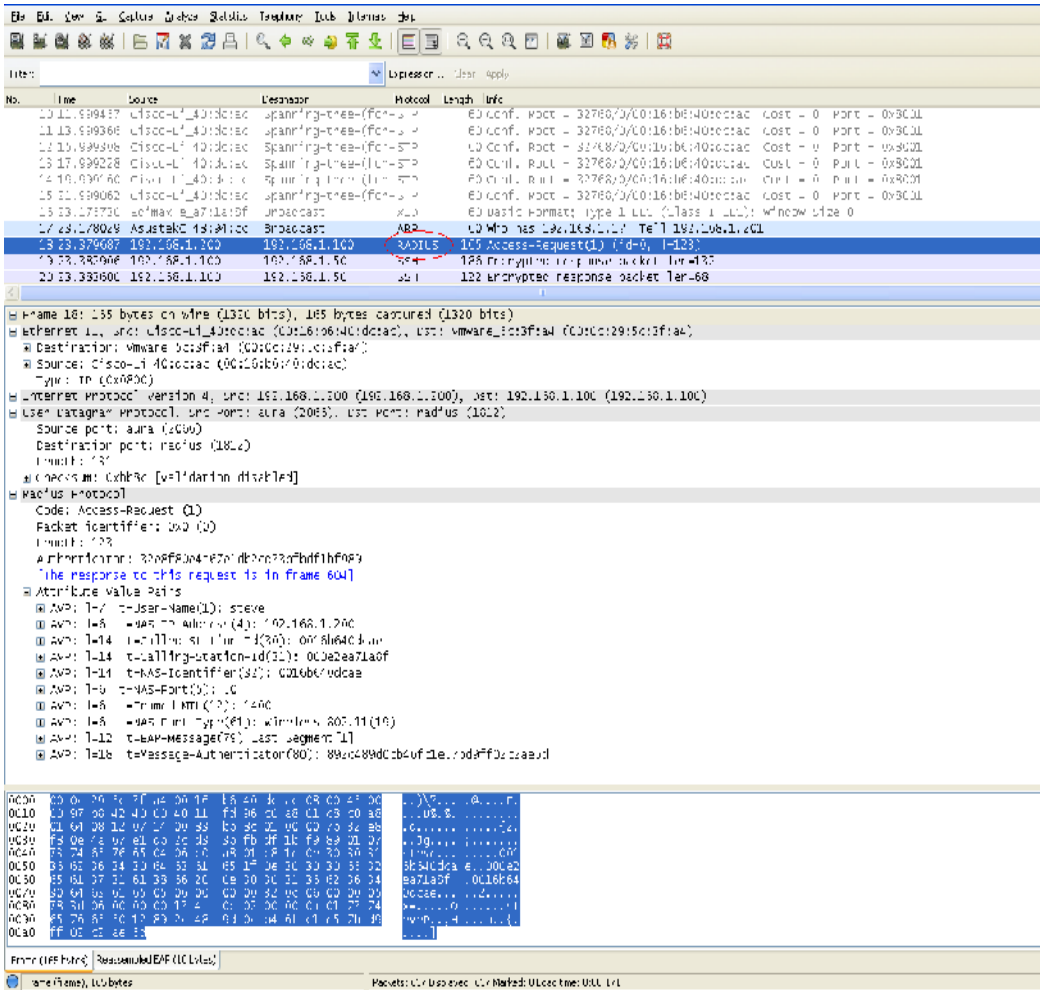

Figura 4.52 Captura de un paquete Access-Request con el contenido EAP.

4.8 Arquitectura de Red Recomendada.

Para concluir se va mostrar dos ejemplos estándar de cómo elaborar una infraestructura de red protegida y basada en autenticación AAA. Hay que tener en cuenta que cada entorno es diferente y cada organización tiene sus necesidades y capacidades en cuanto a funcionalidad, prestaciones, seguridad y redundancia, además de sus opiniones en cuanto al montaje de la infraestructura.

En la Fig.4.53, vemos una infraestructura sencilla, sin aporte de redundancia para una pequeña /mediana organización que desea implementar la seguridad basada en AAA en la capa de enlace mediante 802.1X. Cada uno de los equipos que se conectan a la infraestructura lo hace mediante una conexión basada en la autenticación 802.1Xcontra un servidor FreeRADIUS, que consulta un servidor de directorio con/sin utilización de certificado de cliente, aunque por supuesto utilizando autenticación mutua mediante certificado de servidor. En este caso de pequeña/mediana organización, el ipo de autenticación de sus empleados puede ser EAP-TTLS o EAP-PEAP, tanto para la zona inalámbrica como para la zona cableada de acceso. El punto de acceso utilizado es compatible 802.11i, así como los teléfonos IP o los PDA. Se podría incluir por seguridad un cortafuego en la conexión entre los conmutadores.

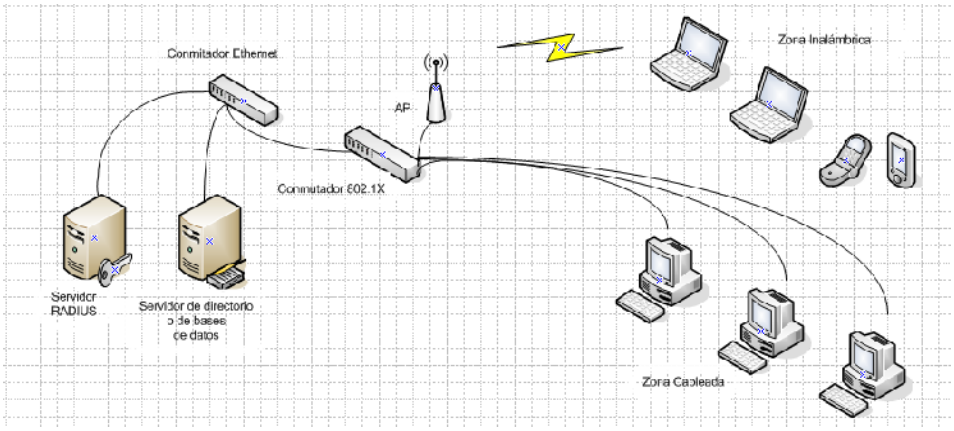

Figura 4.53 Arquitectura de red para pequeña/mediana empresa.

La Fig.4.54, muestra una organización de mayor tamaño, aunque no tanto como para tener redundancia en la zona segura (servidores RADIUS, Controladores de dominio y Certificate Server). Todas las conexiones entre los equipos de acceso (NAS) y los servidores utilizan cualquier tipo de túnel como VPN, IPSec, etc, para evitar interceptación de los datos delicados. Los equipos cableados de la empresa conectan mediante 802.1X y pueden estar adscritos a una VLAN de red interna.

Todas las conexiones que acceden a la red interna (cableada, inalámbrica, VPN, ect) utilizan acceso basado en la capa de enlace y autenticación a través de uno de los dos servidores Proxy RADIUS, que a su vez consultan a uno o más servidores RADIUS principales en una zona segura . Estos Proxy RADIUS disponen de dos conexiones NIC hacia dos conmutadores diferentes, uno hacia la zona DMZ y otro hacia la zona segura, aunque todas las conexiones son a través de un túnel.

La organización puede prestar servicio a Internet a través de servidores Web, de correo electrónico o webmail, FTP, etc.

En la zona desmilitarizada o DMZ el único tráfico que circula sin encriptación es el tráfico Web hacia los servidores de Internet. Todo el demás tráfico circula en un túnel, ya que es tráfico hacia los servidores de autenticación.

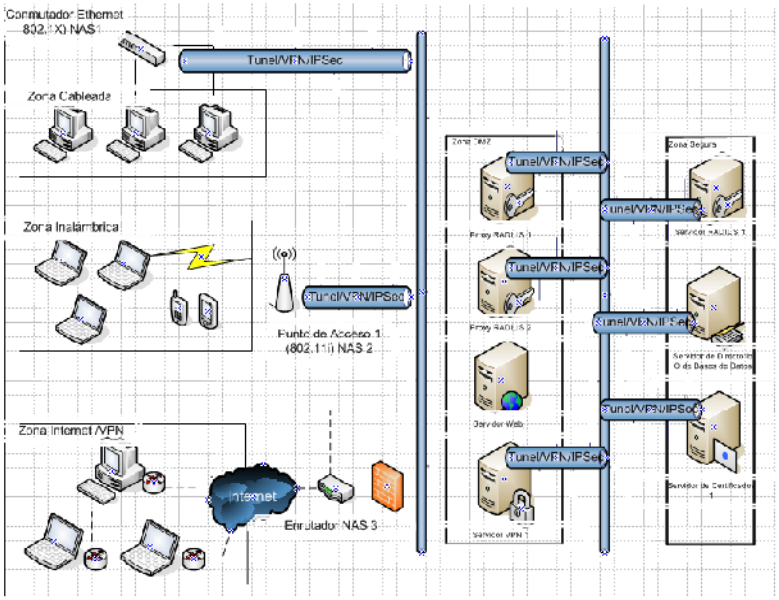

Figura 4.54 Arquitectura de red grandes organizaciones.

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES.

CONCLUSIONES

Con la tecnología inalámbrica se abre todo un mundo de posibilidades de conexión sin la utilización de un cableado clásico, proporcionando una flexibilidad y comodidad sin precedentes en la conectividad entre ordenadores. A lo largo de este Trabajo Especial de Grado, hemos hecho un análisis de todos los aspectos de seguridad que implica a la hora de acceder a una red, vía conexión inalámbrica, especialmente se ha hecho énfasis al protocolo de autenticación Remote Authentication Dial In User Service). Es un protocolo AAA (Autenticación, Autorización y Administración) para aplicaciones como acceso a redes o movilidad IP. Además es un protocolo de autentificación comúnmente utilizado por el estándar de seguridad del 802.1x (usado en redes inalámbricas), éste mejora el estándar de encriptación WEP, en conjunto con otros métodos de seguridad como EAP-PEAP, para la cual se utilizó para su configuración una herramienta basada en código abierto llamado ZeroShell, esta es una distribución Linux para servidores y dispositivos embebidos, que provee de servicios de red. Zeroshell dispone de un interfaz web para su configuración, pero además puede ser administrado desde un terminal remoto (ssh), basado en Debian, la cual nos permite descargar los diferentes paquetes que lo forman, para adaptarlo a nuestro hardware.

El estudio del diseño de una conexión segura en una red inalámbrica (EAP) mediante el protocolo de autenticación RADIUS, ha permitido cerrar un poco esa brecha que existe en las redes inalámbricas, y hacerlas más seguras, dando así confiabilidad e integridad a los usuarios que acceden a redes, ya sean

comerciales o domesticas, y que a la vez se garantice la integridad de la información y los datos que por allí circula. En la configuración de este laboratorio, donde además de configurar el servidor RADIUS, también se realizó la creación de un certificado de seguridad X.509.

X.509 es la pieza central de la PKI ya que enlaza la clave pública con los datos que permiten identificar al titular. Los certificados digitales X.509 son emitidos por Autoridades de Certificación privadas o públicas, tales como VeriSign, Thawte y British Telecom. Hay distintas clases de certificados, de acuerdo al uso que se le vaya a dar y al nivel de confianza. Debido a su propia naturaleza y al papel que desempeñan, no son documentos eternos, al igual que sucede con el resto de documentos de autenticación de otros tipos. Por esto existe la posibilidad de revocar o anular un certificado, y esta revocación puede llevarla a cabo el propietario del mismo o el administrador de sistemas.

Es de importancia recalcar que en la elaboración de esta investigación se realizó además un estudio de los diferentes tipos de ataques que puede sufrir una red inalámbrica, hemos nombrado y explicado cada una de ellas, su funcionamiento, como operan y que herramientas implementan las personas dedicadas a este tipo de delitos.

Una de las desventajas del uso de herramientas basadas en software libre, es la carencia de empresas que den soporte y servicio especializado a estas soluciones, teniendo en muchos casos que ser asumido por la empresa que los implante.

Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza

la calidad y confidencialidad de la información presente en los sistemas de la empresa.

RECOMENDACIONES

.

En base al estudio realizado, donde fue necesario generar un ambiente de laboratorio que permitiera recrear la funcionalidad de una conexión segura en una red inalámbrica (EAP) mediante el protocolo de autenticación RADIUS, se pueden dar las siguientes recomendaciones generales:

- ✓ Utilizar la distribución opensource ZeroShell y FreeRadius, basado en Linux estable, ya que esto va a simplificar la instalación y configuración de la herramienta, y evita inconvenientes propios de distribuciones en modo testing (prueba).

- ✓ Realizar la implementación de la solución de una conexión segura en una red inalámbrica (EAP) mediante el protocolo de autenticación RADIUS primeramente en un ambiente controlado considerado como prueba piloto, previa a su implantación en redes domesticas o corporativas. Esto se debe a que el ambiente de laboratorio se pueden simular algunos factores, pero la implantación en un ambiente real puede comprometer la integridad de la información y de los datos.

- ✓ Fortalecer los conocimientos a lo que refiere a la instalación, configuración y administración de herramientas como VirtualBox y VMware, para realizar virtualización de sistemas operativos invitados.

- ✓ Inhabilitar DHCP para la red inalámbrica. Las IP deben ser fijas.

- ✓ Actualizar el firmware de los puntos de acceso para cubrir los posibles aguajeros en las diferentes soluciones wireless.

- ✓ Proporcionar un entorno físicamente seguro a los puntos de acceso y desactivarlos cuando se pretenda un periodo de inactividad largo.

- ✓ Cambiar el SSID (Server Set ID) por defecto de los puntos de acceso, conocidos por todos. El SSID es un identificador configurable que permite la comunicación de los clientes con un determinado punto de acceso. Actúa como un password compartido entre la estación cliente y el punto de acceso.

- ✓ Inhabilitar la emisión de broadcast del SSID.

- ✓ Reducir la propagación de ondas de radio fuera del edificio.

- ✓ Establecer políticas de seguridad a la hora de emitir un certificado digital. Esta debe, tomando las mejores prácticas, tener un periodo de validez de un año. En caso de requerirlo, ya sea por que la clave este comprometida, la misma puede ser revocada por el administrador de sistemas o de la red.

GLOSARIO.

AAA: Corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización (Authentication, Authorization and

Accounting en inglés). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

Autenticación: La Autenticación es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, ordenador, etc) y la segunda un servidor (ordenador). La Autenticación se consigue mediante la presentación de una propuesta de identidad (un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla. Ejemplos posibles de estas credenciales son las contraseñas, los testigos de un sólo uso (one-time tokens), los Certificados Digitales, ó los números de teléfono en la identificación de llamadas.

Autorización: Autorización se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. La mayor parte de las veces el privilegio concedido consiste en el uso de un determinado tipo de servicio. Ejemplos de tipos de servicio son, pero sin estar limitado ha: filtrado de direcciones IP, asignación de direcciones, asignación de rutas, asignación de parámetros de Calidad de Servicio, asignación de Ancho de banda, y Cifrado.

Contabilización: La Contabilización se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación, u otros propósitos. La contabilización en tiempo real es aquella en la que los datos generados se entregan al mismo tiempo que se produce el consumo de los recursos. En contraposición la contabilización por lotes (en inglés "batch accounting") consiste en la grabación de los datos de consumo para su entrega en algún momento posterior. La información típica que un proceso de

contabilización registra es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó.

EAP: Definido en la RFC 2284, es un protocolo de autenticación para llevar a cabo tareas de AAA que fue diseñado originalmente como una extensión del protocolo PPP (Point-to-Point Protocol).EAP puede trabajar sobre cualquier capa de enlace y no asume una capa física segura.

LDAP: Lightweight Directory Access Protocol, protocolo de acceso a directorios más simple que X.500 para acceso a directorios.

RADIUS: (Remote Authentication Dial In User Service). Es un protocolo AAA (Autenticación, Autorización y Administración) para aplicaciones como acceso a redes o movilidad IP. RADIUS es un protocolo de autentificación comúnmente utilizado por el estándar de seguridad del 802.1x (usado en redes inalámbricas). RADIUS mejora el estándar de encriptación WEP, en conjunto con otros métodos de seguridad como EAP-PEAP.

WPA: WPA es la abreviatura de Wi-Fi Protect Access, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN (Transition Security Network).

WEP: (Wired Equivalent Privacy).Es un protocolo de cifrado a nivel de enlace contenido en la especificación original de estándar IEEE 802.11.WEP permite cifrar los datos que se transfieren a través de una red inalámbrica y autenticar los dispositivos móviles que se conectan a sus puntos de acceso.

BIBLIOGRAFÍA

Andréu, Fernando, Izaskun Pellejero, Amaia Lesta. (2006). Redes WLAN. Fundamentos y Aplicaciones de Seguridad. Ediciones Marcombo. Barcelona, España.

.

Casamor, Antonio Salavert. (2003).Los Protocolos en las redes de ordenadores. Ediciones Universidad Politécnica de Catalunya.

España Boquera, María Carmen. (2003). Servicio Avanzado de Telecomunicaciones. Ediciones Diaz de Santos S.A.Madrid, España. Págs. 222-229

Glenn, Walter. (2005). Linksys Networks. The Oficial Guide Mc-Grow Hill.

Habaken, Joe. (2006). Home Wireless Networking in a Snap. Sams Publisher. Indianápolis, Indiana USA.

Hansen, Yago Fernandez; Varón, Antonio Ramos; García-Morán, Jean Paul. RADIUS /AAA / 802.1X.Sistemas basados en la autenticación en Windows y GNU/Linux. Ediciones RA-MA. Madri, España.Págs.21-116, 505-522.

Mathon, Philippe. (2004). VPN Implementación en Windows Serve. Ediciones Eni. Barcelona, España. Págs. 160-175.

Mathon, Philippe. (2001). TCP IP/ entorno Windows 2000.Ediciones Eni. Barcelona, España.

Roger, Jean Marc. (2004). Seguridad en la Informática de la Empresa. Riesgos, amenazas, prevención y soluciones. Ediciones Eni .Barcelona, España.

Yang Xiao, Jie Li Yi Pan. (2005). Wireless Networks and Mobile Computing. Security and Rounting in Wireless Networks .Ediciones Nova.

Mendillo, V. Universidad Central de Venezuela. Seguridad en Informática y Comunicaciones. [DVD].

Protocolo EAP [en línea].
<http://books.google.co.ve/books?id=_9P9ImY3ITwC&pg=PA288&dq=radius+networking&hl=es&ei=z7_KTJ69H4GBlAf3yOimAQ&sa=X&oi=book_result&ct=result&resnum=10&ved=0CFMQ6AEwCQ#v=onepage&q=radius%20networking&f=false>[Consulta: 27-10-2010].

Protocolos de Seguridad [en línea].
<http://books.google.co.ve/books?id=dvzIJ3qobtQC&pg=PA559&dq=radius+networking&hl=es&ei=c8DKTPO8I8SBlAfb_53MAQ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCkQ6AEwADgK#v=onepage&q=radius%20networking&f=false>. [Consulta: 07-10-2010].

Tecnologías Móviles [en línea].
<http://books.google.co.ve/books?id=apvmc26aqkC&pg=PA917&dq=radius+networking&hl=es&ei=c8DKTPO8I8SBlAfb_53MAQ&sa=X&oi=book_result&ct=result&resnum=7&ve

d=0CE8Q6AEwBjgK#v=onepage&q=radius%20networking&f=false>.
[Consulta: 07-10-2010].

Home Wireless Networking in a Snap [en línea].
http://books.google.co.ve/books?id=JYboXJOCkDMC&pg=PA286&dq=WPA+network&hl=es&ei=RzW_TITUNsOAlAeXxfXlBw&sa=X&oi=book_result&ct=result&resnum=7&ved=0CEgQ6AEwBg#v=onepage&q=WPA%20network&f=false>
[Consulta: 02-10-2010].

. Security and routing in wireless networks [en linea]

<http://books.google.co.ve/books?id=xlKUrdpKAJgC&pg=PA48&dq=WPA+network+and+radius&hl=es&ei=hTW_TLuiAoKglAf-9NToBw&sa=X&oi=book_result&ct=result&resnum=4&ved=0CDcQ6AEwAw#v=onepage&q=WPA%20network%20and%20radius&f=false>

[Consulta: 23-10-2010].

. Linksys Networks [en línea]

<**http://books.google.co.ve/books?id=wfoAOenjdIIC&pg=PA137&dq=WPA+network+and+radius&hl=es&ei=EDa_TLKJBsaAlAfotf3gBw&sa=X&oi=book_result&ct=result&resnum=6&ved=0CEQQ6AEwBQ#v=onepage&q=WPA%20network%20and%20radius&f=false**> [Consulta: 07-10-2010].

. Wi-Fi Home Networking Just the Steps for Dummies [en línea]

http://books.google.co.ve/books?id=xceHcrSJ46kC&pg=PA59&dq=WPA+network+and+radius&hl=es&ei=mza_TLzAI4a0lQeN-5ziBw&sa=X&oi=book_result&ct=result&resnum=2&ved=0CC8Q6AEwATgK#v=onepage&q=WPA%20network%20and%20radius&f=false> [Consulta: 04-11-2010].

VirtualBox [Pagina Web en Línea]: Dipsonible http://www.virtualbox.org/. [Consulta:12-02-2011]

Fundamentos y aplicaciones de seguridad en redes WLAN [en línea]

http://books.google.co.ve/books?id=k3JuVG2D9lMC&pg=PA65&dq=protocolo+radius&hl=es&ei=QzO_TIbVGYXGlQfi0cjkBw&sa=X&oi=book_result&ct=result&resnum=5&ved=0CD8Q6AEwBA#v=onepage&q=protocolo%20radius&f=false > [Consulta: 01-11-2010].

ZeroShell [Pagina Web en Línea]: Disponible http://www.zeroshell.net/. [Consulta: 12-02-2011].

FreeRadius [Pagina Web en Línea]: Disponible http://freeradius.org/ [Consulta: 21-10-2011].