Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación

Implementación de una arquitectura de red WLAN basada en el estándar IEEE 802.11 y en el esquema de seguridad WPA2-Enterprise

Trabajo Especial de Grado
presentado ante la ilustre
Universidad Central de Venezuela
por el bachiller
Ramón Alberto Forsyth Figueroa
para optar al título de
Licenciado en Computación

Tutora académica: Prof. Ana Morales (M.Sc.)
Tutor industrial: Lic. Marco Brando

Caracas, octubre de 2009

Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación

ACTA DEL VEREDICTO

Quienes suscriben, miembros del Jurado designado por el Consejo de la Escuela de Computación para examinar el Trabajo Especial de Grado presentado por el bachiller **Ramón Alberto Forsyth Figueroa**, cédula de identidad número **V-13.533.584**, bajo el título ***"Implementación de una arquitectura de red WLAN basada en el estándar IEEE 802.11 y en el esquema de seguridad WPA2-Enterprise"***, a los fines de cumplir con el requisito legal para optar al título de Licenciado en Computación, dejan constancia de lo siguiente:

Leído el trabajo por cada uno de los miembros del Jurado, se fijó el día 27 de octubre de 2009, a las 11:00 am, para que su autor lo defendiera en forma pública, en el aula PA-III de la Escuela de Computación, lo cual éste realizó mediante una exposición oral de su contenido, y luego respondió satisfactoriamente a las preguntas que le fueron formuladas por el Jurado, todo ello conforme a lo dispuesto en la Ley de Universidades y demás normativas vigentes de la Universidad Central de Venezuela. Finalizada la defensa pública del Trabajo Especial de Grado, el jurado decidió aprobarlo.

En fe de lo cual se levanta la presente acta, en Caracas a los veintisiete días del mes de octubre del año 2009, dejándose también constancia de que, conforme a lo dispuesto en la normativa jurídica vigente, actuó como Coordinadora del Jurado la Tutora Académica, Profesora Ana Morales.

_____

Prof. Ana Morales
Tutora Académica

_____ _____

Prof. María Elena Villapol
Jurado Principal

Prof. Robinson Rivas
Jurado Principal

Resumen

Título:
"Implementación de una arquitectura de red WLAN basada en el estándar IEEE 802.11 y en el esquema de seguridad WPA2-Enterprise"

Autor: *Br. Ramón A. Forsyth F.*
Tutora Académica: *Prof. Ana Morales (M.Sc.)*
Tutor Industrial: *Lic. Marco Brando*

Resumen:
La empresa C.G.S.I., C.A. (Consultoría Global en Seguridad Informática) requería implementar una red inalámbrica con fuerte énfasis en la seguridad, para remplazar su antigua WLAN basada en un dispositivo orientado a redes hogareñas y con bajos niveles de protección.

En este Trabajo Especial de Grado se presenta el proceso de diseño, implementación y pruebas de una nueva red inalámbrica para C.G.S.I, C.A., acorde con las mejores prácticas de la industria. Esta red consta de una arquitectura de conectividad que da soporte al acceso de los clientes inalámbricos, conforme al estándar IEEE 802.11. Los componentes de esta arquitectura están basados en dispositivos del fabricante de equipamiento para WLAN Aruba Networks. Por otra parte, existe también una arquitectura de seguridad donde se establece la infraestructura de autenticación y control de acceso a la red inalámbrica. La arquitectura de seguridad, construida sobre los componentes de la plataforma Microsoft Active Directory de la compañía, implementa el esquema WPA2-Enterprise (*WI-Fi Protected Access 2*), que provee autenticación IEEE 802.1X y cifrado de datos CCMP-AES. El resultado final es una solución WLAN completamente funcional que cumple con la especificación de red de seguridad robusta (RSN) definida en el estándar IEEE 802.11-2007.

Palabras clave:
Redes inalámbricas, WLAN, IEEE 802.11, Wi-Fi, seguridad, WPA2, IEEE 802.1X, CCMP, AES.

Dedicatoria

Por traerme a la vida,
por tu amor y tus constantes sacrificios,
por las alegrías y por las lágrimas,
porque me has inculcado valores y principios,
porque has procurado hacer de mí persona de bien,
porque más que nadie has anhelado
que alcanzara este momento;
hoy el fruto de mi esfuerzo
está dedicado enteramente a ti,
amada Madre…

Agradecimientos

A Dios, en primer lugar, por bendecir mi vida de tantas maneras.

A mi amada madre, por todo el amor y los sacrificios. Te agradezco por tu incansable empeño en hacer de mí un hombre íntegro y un ser de bien. Sé que esta meta alcanzada es un logro también para ti.

A mi padre. A ti papá, porque tus lecciones más valiosas las estoy entendiendo y asimilando hoy en día.

A mis hermanos, Patricia y Javier, porque de ustedes aprendo cada día el valor de poder contar siempre con alguien.

A mi adorada abuela María, por ser ejemplo del amor más puro, incondicional y, por qué no, también del amor más consentidor y alcahueta…

A mis tías y tíos: Nieves, Isabel, María, Ramón, José, Víctor y Rafael. Siempre han sabido estar cuando han sido más necesarios. Cada uno a su manera ha sido ejemplo de vida, guía y mentor, y cuando les ha tocado, también padre y madre para mí y mis hermanos.

A la magna e ilustre Universidad Central de Venezuela, por brindarme una educación de excelencia, tanto en lo académico como en lo humano. A la Facultad de Ciencias, a la Escuela de Computación, y a todos y cada uno de los profesores y preparadores que contribuyeron en mayor o menor medida en mi formación. A mi querida tutora, Ana Morales, por su infinita paciencia y disposición para que pudiera culminar este proyecto y poder graduarme este mismo año. También quiero manifestar mi gratitud a mi tutor original, Jesús Castillo.

Muchas personas tocaron mi vida para bien durante mi paso por la Facultad. A todos aquellos con quienes compartí momentos de estudio, pero también de “sano ocio”, gracias por su tiempo y su disposición. No alcanzaría el espacio para nombrarlos a todos, pero igual cada uno tiene su lugar en mis recuerdos. Vaya para ustedes mi reconocimiento. Especial

cariño y agradecimiento a Mercedes, Isaura y Mario, con quienes compartí tantos gratos momentos durante la carrera.

A C.G.S.I., C.A. por darme la valiosa oportunidad de desarrollar este Trabajo Especial de Grado en sus instalaciones y con sus recursos tecnológicos. Gracias también por permitirme el tiempo necesario para llevar a feliz término la realización de este proyecto. Allí también he tenido la oportunidad de crecer como profesional y como persona. A Marco por su amistad, su guía y buenos consejos. Al resto del *team*, también muchas gracias, en especial a Marisela, Marta, Mario y Gustavo, quienes se han convertido en estos años, más que en simples compañeros de trabajo, en verdaderos amigos. Gracias por sus consejos y su preocupación porque yo sacara este proyecto adelante.

A *my dear friend*, Mª Emilia, por estar presente en cada ocasión que necesité ánimo y una palabra de aliento. También a Raiza y Gabriel, grandes amigos, por ayudarme a encontrar el camino de vuelta al *aquí* y al *ahora*.

¡Infinitas gracias a todos!

—Ramón Forsyth

Tabla de contenidos

Lista de figuras

Lista de tablas

Introducción

En los últimos años las redes inalámbricas de área local (WLAN) han pasado a ocupar un lugar considerablemente importante en el universo de las comunicaciones de ámbito local. Cada vez más, las organizaciones se han dado cuenta de que las WLAN son un complemento indispensable a las redes cableadas tradicionales, a fin de satisfacer necesidades de movilidad, traslado, redes ad hoc y cobertura de lugares difíciles de cablear. Sin embargo, hasta hace relativamente poco tiempo, las redes WLAN eran poco usadas debido al alto precio, baja velocidad de transmisión, y necesidades de licencia.

A medida que fueron apareciendo en el mercado productos WLAN comerciales basados en estándares, estos obstáculos se fueron derrumbando poco a poco. Pese a ello, la penetración de las redes inalámbricas en el segmento empresarial seguía siendo muy baja; esto debido, primordialmente, a la facilidad para comprometer su seguridad, y con ello el bien más valioso de las organizaciones modernas: la información. Con la aparición de esquemas como WPA y WPA2, que combinan distintos mecanismos de protección para brindar altos niveles de seguridad, ha repuntado el interés de las empresas en las WLAN, dadas sus ventajas inherentes.

C.G.S.I., C.A. (Consultoría Global en Seguridad Informática) es una empresa venezolana cuya operación se circunscribe, como describe su nombre, al área de seguridad de la información. Como empresa consultora que presta servicios al mercado corporativo, la información que allí se maneja, perteneciente a la propia organización, así como a sus clientes y proveedores, está clasificada en su mayoría como de tipo sensible y confidencial. El eventual compromiso de esta información podría acarrear consecuencias negativas a nivel económico, legal y de imagen para la organización. Es por ello que cualquier elemento de generación, almacenamiento, gestión y distribución de información utilizado por la empresa, y aquí se incluye la red WLAN, debe implementar un alto nivel de seguridad.

Existía en C.G.S.I., C.A. una implementación de red WLAN basada en un dispositivo orientado a redes hogareñas, con características de protección bastante pobres, en comparación con los estándares actuales.

Por ello, se planteó como objetivo principal de este Trabajo Especial de Grado el diseño y la implementación de una nueva red de área local inalámbrica, completamente funcional, basada en el estándar IEEE 802.11 y en el esquema de seguridad WPA2-Enterprise. Esto permite ofrecer un nivel de protección que maximiza el cumplimiento con los tres pilares de la seguridad de la información: integridad, confidencialidad y disponibilidad.

Para el diseño de la red WLAN se tomaron en cuenta las mejores prácticas de la industria, así como diseños de referencia de los fabricantes de los componentes utilizados. Además, la empresa estableció una serie de requerimientos que debían tomarse como premisas para la especificación de la red. Este diseño contempló, por una parte el equipamiento que permite la conectividad de los clientes inalámbricos a la WLAN, en base a las especificaciones establecidas en el estándar IEEE 802.11. Por otro lado, se definió la infraestructura de seguridad, tratando de aprovechar al máximo la plataforma tecnológica preexistente en la empresa.

En cuanto a la implementación de la arquitectura de conectividad, se utilizaron equipos del fabricante Aruba Networks. Esta compañía desarrolla exclusivamente dispositivos de infraestructura WLAN orientados al mercado empresarial, cumpliendo con todos los estándares y certificaciones propias de este tipo de redes. Esto brinda robustez y escalabilidad a la red inalámbrica de C.G.S.I., C.A.

Por otro lado, buscando el ahorro de costos y una fácil integración, para la arquitectura de seguridad de la red se utilizaron componentes opcionales disponibles con el sistema operativo Microsoft Windows Server 2003, como es el caso de la entidad emisora de certificados digitales, *Certificate Services*, y el servicio RADIUS, IAS (*Internet Authentication Service*). Ambos elementos se integraron de manera transparente con la plataforma Active Directory de la empresa, facilitando la gestión de los usuarios y dispositivos autorizados a hacer uso de la red WLAN.

Este documento de Trabajo Especial de Grado está estructurado de la siguiente manera:

- El Capítulo 1 describe el problema planteado y establece un conjunto de objetivos a cumplir. Se incluye además la justificación de la pertinencia como Trabajo Especial de Grado del tema seleccionado, y se presentan algunos antecedentes de investigación. Termina el capítulo con un esbozo de la metodología a utilizar para la consecución de los objetivos trazados, y el alcance que delimita el trabajo de investigación.

- Seguidamente, el Capítulo 2 introduce las redes inalámbricas de área local (WLAN), sus aplicaciones, requisitos de operación y tecnologías asociadas. Luego, se expone el estándar IEEE 802.11, que constituye la representación predominante de este tipo de redes. Se introduce brevemente el tema de la seguridad informática y se describe la evolución de los esquemas de protección utilizados hasta el momento en redes WLAN, con énfasis en los mecanismos utilizados por el esquema WPA2-Enterprise, seleccionado para ser implementado en la red WLAN de C.G.S.I., C.A.

- Tras establecer un conjunto de requisitos y criterios de diseño a cumplir, el Capítulo 3 se centra en definir la arquitectura sobre la que se construye la red inalámbrica de C.G.S.I., C.A. Esta arquitectura se subdivide en una arquitectura de conectividad centralizada, que hace uso de equipamiento de infraestructura del fabricante Aruba Networks, y una arquitectura de seguridad, basada en la plataforma Microsoft Active Directory ya existente en la empresa,

- Luego, el Capítulo 4 presenta una síntesis general de las actividades de implementación. Se inicia con la adecuación del ambiente tecnológico de la empresa, continuando con la instalación y configuración de la infraestructura de clave pública, del servicio de autenticación RADIUS y de los elementos de la infraestructura de conectividad. Por último, los clientes inalámbricos son configurados para el acceso a la WLAN.

- El Capítulo 5 reseña diferentes escenarios de prueba que fueron ejecutados sobre los componentes de la red inalámbrica desplegada, buscando certificar su correcta operación y apego al diseño establecido. Para cada escenario se describe el motivo de su selección, el proceso de ejecución, los resultados derivados de la prueba y su correspondiente análisis.

- Finalmente, se ofrecen conclusiones sobre este Trabajo Especial de Grado, evaluando el cumplimiento de los objetivos trazados. Se establecen, además, las limitaciones encontradas, sugerencias para trabajos de investigación futuros relacionados con el mismo tema, así como algunas recomendaciones finales.

Capítulo 1

Planteamiento del problema

Como punto de inicio del Trabajo Especial de Grado, en este capítulo se describe y delimita el problema que se abordará. Partiendo de allí, se plantean objetivos claros y se establecen los elementos que permiten justificar su pertinencia como tema de investigación. Se presentan también algunos antecedentes de investigación previos a este trabajo. Finalmente, se delinean el alcance y la metodología que se seguirá para la consecución de los objetivos propuestos.

1.1. Contexto del problema

El uso de redes inalámbricas de área local (WLAN, *Wireless Local Area Network*) en el ámbito empresarial ha venido aumentando progresivamente en los últimos años [10]. El concepto de movilidad, implícito en este modelo de comunicaciones, se ha venido transformando en una ventaja competitiva para muchas organizaciones, al proveer acceso instantáneo y en cualquier lugar de la empresa a la información requerida. Se eliminan además las barreras impuestas por la necesidad de estar conectado a un cable para mantener la comunicación, haciendo que las conexiones permanezcan activas en todo momento, mientras los usuarios, y con ellos los dispositivos de cómputo, se desplazan. Esto trae como ventaja el incremento de los niveles de productividad de los empleados y la reducción en los costos de implementación, al eliminar la necesidad de tender nuevo cableado y desplegar dispositivos de infraestructura de red [37].

Por otra parte, también en los últimos años, el campo de la seguridad informática ha crecido y evolucionado considerablemente. Como área de estudio y aplicación de la computación, la seguridad informática busca prevenir la divulgación de información a personas o sistemas no autorizados (confidencialidad), mantener los datos libres de modificaciones no permitidas (integridad) y a disposición de quienes deben acceder a ella (disponibilidad) [25].

C.G.S.I., C.A. (Consultoría Global en Seguridad Informática) es una empresa venezolana, creada en el año 2002, dedicada a ofrecer soluciones orientadas hacia el mercado corporativo para la seguridad de las tecnologías de información. Sus principales áreas de acción comprenden la comercialización de dispositivos y software, la gestión tercerizada, los servicios profesionales de consultoría y el adiestramiento, todo circunscrito al ámbito de la seguridad de la información.

Actualmente, la empresa cuenta con una implementación de red WLAN basada en un dispositivo orientado a redes hogareñas. Como esquema de seguridad se implementa WEP (*Wired Equivalent Privacy*) con clave compartida para la autenticación y el cifrado. Adicionalmente, se utiliza autenticación mediante una lista de control de acceso (ACL, *Access Control List*) de las direcciones MAC de los dispositivos cliente.

La decisión de incorporar una red WLAN en C.G.S.I., C.A. surgió inicialmente de la necesidad de ofrecer conectividad en las salas de reuniones de la empresa, donde no se cuenta con suficientes puertos de acceso a la red cableada, y donde introducir nuevos elementos de infraestructura de red como *switches* tiene implicaciones de costos y de estética, además de que cada usuario requeriría desplazarse no sólo con su computador, sino con un cable para conectarse a la red. Hoy en día, la red WLAN no sólo se usa en los espacios de reuniones de la organización, sino también en el ambiente de laboratorio, además de ser el esquema de conexión preferente de algunos usuarios, que debido a la flexibilidad que otorga, permanecen conectados a la red inalámbrica mientras se encuentran en sus puestos de trabajo, donde cuentan con un puerto de conexión a la red cableada.

1.2. Planteamiento del problema

A pesar de los beneficios tecnológicos y de productividad que ofrecen, muchas organizaciones aún permanecen reacias a la implementación de redes WLAN, debido a que en su concepción original éstas contemplaban esquemas de seguridad que demostraron prontamente ser vulnerables [42].

La seguridad de la información de una empresa comienza siempre por el establecimiento de políticas claras que rijan el uso de sus activos de información, entendidos éstos como datos de diferente índole con los que una organización desarrolla su actividad y que suelen ser vitales dentro de su modelo de negocios [25]. No obstante, ninguna política, por muy rigurosa o claramente expresada, es efectiva si no se establecen los mecanismos adecuados que permitan llevarla a la práctica.

Paradójicamente, la misma ubicuidad y flexibilidad que hacen a las redes WLAN útiles, las hace igualmente inseguras. El uso de un medio de transmisión abierto, representado por las ondas de radio que viajan por el aire, permite que, a falta de mecanismos apropiados, cualquiera pueda tener acceso a la red. Una red WLAN sin ningún esquema de seguridad es inmediatamente vulnerable a ataques de denegación de servicio, intercepción no autorizada del tráfico, inyección de paquetes, usurpación de identidad, entre otros [42].

La información que se maneja dentro C.G.S.I., C.A., perteneciente a la propia organización, así como a sus clientes y proveedores, está clasificada en su mayoría como de tipo sensible y confidencial. El eventual compromiso de esta información podría acarrear consecuencias negativas a nivel económico, legal y de imagen para la empresa. Es por ello que cualquier elemento de generación, almacenamiento, gestión y distribución de información utilizado por la empresa, y aquí se incluye la red WLAN, debe implementar un alto nivel de seguridad.

El problema fundamental del esquema de red WLAN existente en C.G.S.I, C.A. es que no discrimina entre los clientes inalámbricos. El mero hecho de conocer la clave compartida y pertenecer al listado de direcciones MAC permitidas, brinda un acceso irrestricto a la red WLAN de la organización, y de allí al resto de la red corporativa. Las direcciones MAC son fácilmente suplantables, permitiendo a un usuario con intenciones maliciosas usurpar la dirección física de otro cliente, haciéndose pasar por éste último. De igual forma, a medida que crece el universo de usuarios de la WLAN, la gestión del listado de direcciones MAC autorizadas se vuelve inmanejable. Por otra parte, el esquema de clave compartida es vulnerable no sólo por la debilidad inherente del protocolo WEP, sino porque además, es relativamente sencillo obtener la clave valiéndose inclusive de métodos como la ingeniería social.

Además, el dispositivo utilizado como punto de acceso de la red WLAN no soporta esquemas de seguridad más recientes como WPA o WPA2, ni la integración con esquemas de autenticación más robustos como IEEE 802.1X. La red WLAN tampoco ofrece cobertura a todo el espacio físico de las instalaciones de la empresa y no se contemplan esquemas de escalabilidad ni redundancia, pudiendo esto afectar la disponibilidad de la red.

La implementación de una nueva WLAN, conformada por la combinación apropiada de hardware y software, capaz de soportar los esquemas de seguridad actuales para redes WLAN, podría permitir a C.G.S.I., C.A. tener una red inalámbrica óptima a nivel de seguridad, de acuerdo a los estándares y mejores prácticas vigentes.

De lo anteriormente expuesto surge la siguiente interrogante:

¿Es factible diseñar e implementar una red de área local inalámbrica (WLAN) completamente funcional en C.G.S.I., C.A. (Consultoría Global en Seguridad Informática), basada en el estándar IEEE 802.11 y en el esquema de seguridad WPA2-Enterprise?

1.3. Objetivos

1.3.1. Objetivo general

Para este Trabajo Especial de Grado se estableció el siguiente objetivo general:

- Diseñar e implementar una arquitectura de red inalámbrica de área local (WLAN) para la compañía C.G.S.I., C.A. (Consultoría Global en Seguridad Informática), basada en el estándar IEEE 802.11 y el esquema de seguridad WPA2-Enterprise.

1.3.2. Objetivos específicos

Como objetivos específicos se fijaron los siguientes:

- Establecer los requerimientos específicos de una red WLAN para C.G.S.I., C.A., basada en las necesidades y justificación de negocio actuales de la organización.

- Investigar los diferentes esquemas de seguridad existentes para la protección de redes WLAN IEEE 802.11.

- Diseñar una red WLAN de tipo empresarial, con una arquitectura robusta de seguridad.

- Implementar los diferentes elementos de infraestructura para proveer conectividad en la red WLAN.

- Implementar la arquitectura de seguridad diseñada para la red WLAN.

- Realizar pruebas que permitan validar la correcta implementación de la red WLAN, tanto a nivel de conectividad como a nivel de seguridad.

1.4. Justificación

La seguridad informática, es vista hoy en día como una necesidad vital para las organizaciones, dado el valor subyacente de sus activos de información, que muchas veces superan en gran medida el valor de sus activos físicos. Por otra parte, el concepto de movilidad en las comunicaciones, dentro del cual las redes inalámbricas de área local (WLAN) juegan un papel preponderante, ha permitido elevar los niveles productividad al introducir la ubicuidad en el acceso a la información.

C.G.S.I., C.A. es una empresa en la que prevalece un alto grado de uso de la tecnología en la gestión de sus procesos, y en la que además se maneja una cantidad significativa de información clasificada como sensible de sus clientes, proveedores y de la propia empresa. En virtud de esto, en cada componente tecnológico incorporado a la organización deben implementarse mecanismos de seguridad que permitan preservar y garantizar en una amplia medida la integridad, confidencialidad y disponibilidad de dicha información.

Es imperioso para C.G.S.I., C.A. migrar desde la implementación actual red WLAN con niveles bastante pobres de seguridad, hacia una red inalámbrica de tipo empresarial que ofrezca un grado de seguridad robusto. De esta manera es posible seguir dando soporte a los requerimientos de acceso móvil a los datos, que se han ido incrementando a medida que se ha hecho palpable en la organización los beneficios de las redes inalámbricas, pero sin comprometer la información que se maneja en la empresa.

A efectos académicos, la consecución de este Trabajo Especial de Grado, permite llevar al terreno práctico los conocimientos adquiridos en las diferentes materias cursadas en la Escuela de Computación dentro del área de redes, específicamente redes móviles e inalámbricas, así como en el área de seguridad informática.

Finalmente, el diseño e implementación de una red WLAN de grado empresarial con esquemas de seguridad robustos que se presenta en este trabajo, puede servir como marco de referencia y objeto de estudio para próximos proyectos de investigación que se desarrollen en el Laboratorio Ícaro de la Escuela de Computación.

1.5. Antecedentes

Se describen a continuación, de manera breve, algunas investigaciones realizadas en la Facultad de Ciencias de la Universidad Central de Venezuela, y algunas otras universidades del exterior, previas a la elaboración de este Trabajo Especial de Grado. Las referencias consultadas están relacionadas con el tema de estudio desarrollado en este documento.

- ***Estudio de seguridad de la red inalámbrica de la Facultad de Ciencias de la UCV*** [12]***:*** con el objetivo de realizar una auditoría de seguridad a las diferentes tecnologías inalámbricas existentes dentro del área de la Facultad de Ciencias de la UCV, este Trabajo Especial de Grado busca identificar debilidades de seguridad y establecer recomendaciones para elevar los niveles de protección. Para ello, se utiliza una metodología abierta denominada OSSTM (*Open Source Security Testing Methodology*).

- ***Evaluación de mecanismos y protocolos de seguridad desarrollados para redes inalámbricas 802.11b*** [39]***:*** en este Trabajo Especial de Grado se desarrollan una serie de pruebas a los esquemas de seguridad disponibles en su momento para redes basadas en la revisión 802.11b y se establece un conjunto de recomendaciones en base a los resultados obtenidos.

- ***Implementación de una solución de seguridad para la red inalámbrica de la Facultad de Ciencias*** [26]***:*** este Trabajo Especial de Grado propone la implementación de un servidor RADIUS que se encargue de la autenticación de los usuarios y clientes inalámbricos que conforman la red WLAN de la Facultad de Ciencias de la UCV. Adicionalmente, en este trabajo se desarrolla una aplicación Web

para facilitar la administración del servidor de autenticación, así como el registro y control de usuarios.

- ***Seguridad en redes inalámbricas IEEE 802.11 (WLAN) con WEP mejorado*** [11]***:*** se presentó esta tesis de pregrado en la Universidad de las Américas, Campus de Puebla, en México. Inicia este trabajo de investigación con una discusión de la seguridad para redes 802.11 y las vulnerabilidades encontradas en el algoritmo WEP. Posteriormente se analiza y simula el funcionamiento de WEP mejorado con un enfoque denominado *Fake Character Insertion and Compression Technique* (FCICT), concluyendo que provee un nivel mayor de seguridad al del algoritmo original.

- ***Wi-Fi security: how to break and exploit*** [14]***:*** esta tesis de maestría desarrollada en la Universidad de Bergen, Noruega, explora las vulnerabilidades de seguridad de las redes Wi-Fi. Se proveen descripciones detalladas de algunos agujeros de seguridad críticos y ejemplos prácticos de ataques. La tesis brinda suficientes detalles como para permitir la duplicación del trabajo práctico propuesto.

1.6. Metodología

La metodología de trabajo a seguir para la consecución de los objetivos planteados en este Trabajo Especial de Grado surge de la combinación de las mejores prácticas recomendadas por Microsoft [28] [30], Aruba Networks [7] [8] y la Wi-Fi Alliance [41]. La metodología, a grandes rasgos, está conformada por las siguientes actividades:

- Determinación de requisitos específicos para la red WLAN.

- Diseño de la arquitectura lógica y de seguridad.

- Implementación de los elementos de infraestructura de la red.

- Implementación de la arquitectura de seguridad.

- Pruebas sobre la implementación y análisis de resultados.

1.7. Alcance

El alcance de este Trabajo Especial de Grado está delimitado de acuerdo a los siguientes aspectos:

- Se implementará una red inalámbrica de área local (WLAN) basada en el estándar IEEE 802.11 en la empresa Consultoría Global en Seguridad Informática (C.G.S.I., C.A.).

- Previo al inicio de este proyecto, la empresa había seleccionado y adquirido el equipamiento de infraestructura WLAN, del fabricante Aruba Networks, por lo que el diseño y la implementación de la arquitectura de conectividad estarán supeditados al modelo de operación provisto por este fabricante.

- La red WLAN a implementar sólo brindará conectividad a computadoras portátiles (*laptops*) bajo plataforma Microsoft Windows.

Capítulo 2

Marco teórico

En este capítulo se describen las aplicaciones, requerimientos y tecnologías de transmisión de las WLAN, así como la especificación más prominente de este tipo de redes: el estándar IEEE 802.11. Por otra parte, se abordan temas relacionados con la seguridad en redes WLAN, exponiendo brevemente la evolución de los mecanismos utilizados hasta ahora para protegerlas. Finalmente se ofrece una explicación de los diferentes elementos involucrados en la operación de una WLAN con seguridad WPA2-Enterprise.

2.1. Redes de área local inalámbricas (WLAN)

Una red Inalámbrica de área local (WLAN) es, como su nombre sugiere, una red de alcance local que hace uso de un medio de transmisión inalámbrico [37]. Proporciona un sistema flexible de comunicación que puede implementarse como una extensión o como una alternativa a las redes cableadas.

2.2. Aplicaciones de las WLAN

Las cuatro principales áreas de aplicación para las redes WLAN son: ampliación de redes LAN, interconexión de edificios, acceso nómada y redes ad hoc [36]. A continuación se analizan todas ellas.

2.2.1. Ampliación de redes LAN

Los primeros productos WLAN, aparecidos a finales de los 80, eran ofrecidos como sustitutos de las LAN cableadas tradicionales. Una red WLAN evita el costo asociado a la instalación del cableado y facilita la tarea de traslado y otras modificaciones en la estructura de la red. Sin embargo, debido al aumento en la necesidad de redes LAN, muchas edificaciones nuevas o preexistentes fueron provistas de cableado para datos. Además con los avances en la tecnología de transmisión de datos, se incrementó la confiabilidad en el par trenzado para redes LAN. De manera que aún hoy en día resulta escaso el uso de LAN inalámbricas frente a LAN cableadas.

Sin embargo, el papel de una WLAN como alternativa a las LAN cableadas es importante en un gran número de entornos. Algunos ejemplos incluyen edificios de gran superficie, como fábricas, establecimientos comerciales y almacenes; edificios históricos donde está prohibido modificar la planta física para introducir nuevo cableado; y pequeñas oficinas donde la instalación y el mantenimiento de una LAN cableada no resultan económicos. En todas estas situaciones, una WLAN ofrece una alternativa más efectiva y atractiva. En la mayor parte de los casos, se dispondrá también de una LAN cableada con servidores y algunas estaciones de trabajo fijas. Por tanto, una WLAN está conectada en muchas ocasiones con una LAN cableada en el mismo recinto, denominándose este campo de aplicación ampliación o extensión de redes LAN.

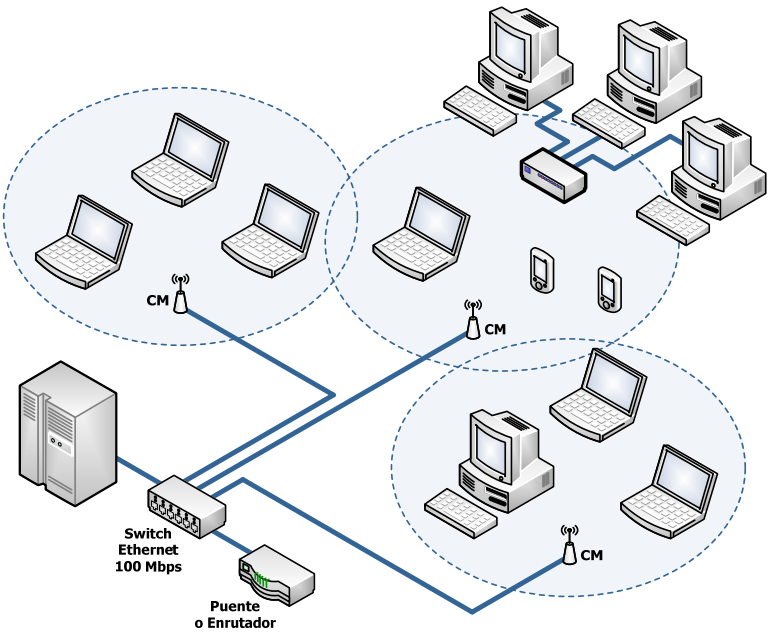

Figura 2-1. Ejemplo de una configuración típica de WLAN

En la Figura 2-1 se muestra una configuración sencilla de una WLAN típica en muchos entornos. Existe una LAN troncal (*backbone*) cableada, como una red Ethernet, que conecta varios servidores, estaciones de trabajo y uno o más puentes (*bridges*) o enrutadores (*routers*) para comunicarse con otras redes. Adicionalmente, existen módulos de control (CM, *Control Modules*) que funcionan como interfaz con la WLAN. Los módulos de control incluyen funciones de puentes o enrutadores para conectar la WLAN con la LAN troncal. Además, contienen algún tipo de lógica para regular el acceso de los sistemas finales. Algunos de los sistemas finales, denominados módulos de usuario (UM, *User Modules*), son dispositivos independientes, como estaciones de trabajo y servidores. Los concentradores (*hubs*), conmutadores (*switches*) u otros elementos que controlan varias estaciones de una LAN cableada también pueden formar parte de la WLAN.

2.2.2. Interconexión de edificios

Otro uso de las WLAN es la conexión de redes LAN situadas en edificios vecinos, sean LAN cableadas o inalámbricas. En este caso se usa un enlace no guiado entre dos edificios. Los dispositivos así conectados son generalmente puentes o enrutadores. Este enlace punto a punto no es en sí mismo una LAN, pero es usual la inclusión de esta aplicación en el contexto de redes WLAN.

2.2.3. Acceso nómada

El acceso nómada permite un enlace no guiado entre un dispositivo de interconexión LAN y un terminal de datos móvil, como un computador portátil. Un ejemplo de la utilidad de este tipo de conexiones es posibilitar a un empleado que vuelve de viaje la transferencia de datos desde un computador portátil a un servidor en la oficina. El acceso nómada resulta útil también en un entorno amplio como un campus o un centro financiero situado lejos de un grupo de edificios. En ambos casos los usuarios se pueden desplazar con sus computadores portátiles y pueden, desde distintos lugares, desear conectarse con los servidores a través de una WLAN.

2.2.4. Redes ad hoc

Una red ad hoc es una red igual a igual establecida temporalmente para satisfacer alguna necesidad inmediata. Por ejemplo, un grupo de empleados, cada uno con su computador,

puede congregarse para una reunión de negocios o para una conferencia, conectando sus computadores a una red temporal que existe sólo durante el transcurso de la reunión.

La WLAN de la Figura 2-1 presentaba una infraestructura estática consistente en una o más celdas con un módulo de control para cada una; pudiendo existir dentro de cada celda varios sistemas finales estacionarios. Las estaciones nómadas se pueden desplazar de una celda a otra. Por el contrario, en una WLAN ad hoc como la de la Figura 2-2 no existe infraestructura; más aún, un conjunto de estaciones localizadas en el mismo dominio se puede auto-configurar dinámicamente para formar una red temporal.

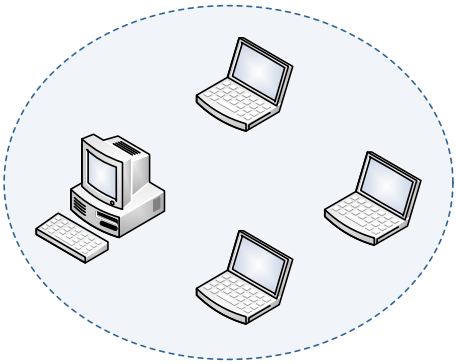

Figura 2-2. Ejemplo de una WLAN ad hoc

2.3. Requisitos de las WLAN

Una WLAN debe cumplir los mismos requisitos típicos de cualquier otra red LAN [13], incluyendo alta capacidad, cobertura de pequeñas distancias, conectividad total de las estaciones y capacidad de difusión. Además, existe un conjunto de necesidades específicas para entornos WLAN, de las cuales las más importantes son listadas en la Tabla 2-1.

Tabla 2-1. Requisitos de las redes WLAN. *Fuente:* **[13]**

Requisito	Descripción
Rendimiento	El protocolo de control de acceso al medio (MAC) debe hacer un uso del medio inalámbrico tan eficiente como sea posible para maximizar la capacidad de transmisión
Número de nodos	Las WLAN pueden necesitar dar soporte a cientos de nodos mediante el uso de varias celdas

Requisito	Descripción
Conexión a la LAN troncal	En la mayoría de los casos es necesaria la interconexión con estaciones situadas en una LAN troncal cableada. En el caso de redes WLAN con infraestructura, esto se consigue fácilmente a través del uso de módulos de control que se conectan con ambos tipos de LAN. Puede ser también necesario dar soporte a usuarios móviles y redes inalámbricas ad hoc
Área de servicio	Una superficie de cobertura para una red WLAN tiene un diámetro típico de entre 100 y 300 metros
Consumo de batería	Los usuarios móviles utilizan estaciones de trabajo con batería que necesitan maximizar la eficiencia del consumo de energía cuando se usan con adaptadores de red inalámbricos. Esto sugiere que resulta inapropiado un protocolo MAC que necesita que los nodos móviles supervisen constantemente los módulos de control
Robustez en la transmisión y seguridad	A menos que exista un diseño apropiado, una WLAN puede ser propensa a sufrir interferencias y escuchas no deseadas. El diseño de una WLAN debe permitir transmisiones fiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas
Funcionamiento ordenado de la red	A medida que las WLAN se están haciendo más populares, es probable que dos o más de estas redes operen en alguna zona en la que sea posible la interferencia entre ellas. Estas interferencias pueden frustrar el normal funcionamiento de la red y pueden permitir accesos no autorizados a una LAN particular
Funcionamiento sin licencia	Los usuarios podrían preferir adquirir y trabajar sobre una WLAN que no precisa de una licencia para la banda de frecuencia usada por la red
Re-asociación	El protocolo MAC usado en la WLAN debería permitir a las estaciones móviles desplazarse de una celda a otra sin pérdida de conectividad
Configuración dinámica	Los aspectos de direccionamiento y gestión de red de la WLAN deberían permitir la inserción, eliminación y traslado dinámico de sistemas finales sin afectar a otros usuarios

2.4. Tecnologías WLAN

Las WLAN se clasifican generalmente de acuerdo con la técnica de transmisión usada. Todas las WLAN actuales se encuentran dentro de una de las siguientes categorías [36]:

- ***LAN de infrarrojos.*** Una celda individual en este tipo de LAN está limitada a una sola habitación dado que la luz infrarroja no es capaz de atravesar muros opacos.

- ***LAN de espectro expandido.*** Este tipo de LAN hace uso de tecnologías de transmisión de espectro expandido. En la mayoría de los casos estas LAN operan en las bandas ISM (*Industrial, Scientific and Medical*, Industrial, Científica y Médica), de modo que no se necesita licencia para su utilización.

- ***Microondas de banda estrecha.*** Estas LAN operan en el rango de las microondas pero no hacen uso de espectro expandido. Algunos de estos productos operan a frecuencias para las que es necesario licencia, mientras que otras lo hacen en alguna de las bandas ISM.

2.5. Estándar IEEE 802.11

El IEEE (*Institute of Electrical and Electronics Engineers*, Instituto de Ingenieros Eléctricos y Electrónicos) [23], es una asociación técnica/profesional sin fines de lucro creada en 1884. Cuenta con más de 360.000 miembros alrededor de 175 países. Su propósito es realizar investigaciones, ofrecer servicios educativos y publicar literatura, especificaciones y estandarizaciones en áreas como ingeniería de computación, telecomunicaciones, tecnología biomédica, energía eléctrica, tecnología aeroespacial, dispositivos electrónicos de consumo masivo, etc.

El Comité de Estándares LAN/MAN 802 fue creado en febrero de 1980 y desde entonces ha desarrollado una serie de especificaciones y estandarizaciones relacionadas con las capas bajas del Modelo de Referencia OSI. El comité está dividido en varios grupos de trabajo dedicados a diversas áreas como Control de Enlace Lógico (802.2), Ethernet (802.3), Token-bus (802.4), Token-ring (802.5), entre otros.

El trabajo en el comité IEEE 802 concerniente a redes WLAN comenzó en 1987 dentro del grupo IEEE 802.4. El interés inicial era desarrollar una especificación de red inalámbrica en el espectro ISM utilizando el equivalente a un protocolo MAC *token-passing bus*. En algún momento durante la investigación se decidió que *token bus* no era apropiado porque generaba un uso ineficiente del espectro de radiofrecuencia. IEEE 802 decidió entonces, en 1990, formar un nuevo grupo de trabajo, el IEEE 802.11 [15], dedicado específicamente al propósito de desarrollar un protocolo MAC y una especificación de medio físico para las WLAN. Desde entonces han generado un conjunto de normalizaciones para redes WLAN. En 1997 se publicó el estándar ANSI/IEEE 802.11 [19] que fue revisado posteriormente en 1999 [4]. La versión más reciente, denominada IEEE 802.11-2007 [20], contiene todas las extensiones y correcciones completadas hasta la fecha de su publicación.

La terminología y algunas de las características específicas de 802.11 son exclusivas de este estándar y no se reflejan en todos los productos comerciales. Sin embargo, es útil

familiarizarse con el estándar dado que sus características son representativas de las capacidades necesarias en cualquier WLAN.

2.6. Arquitectura de IEEE 802.11

El bloque de construcción más elemental de una WLAN es el conjunto de servicios básicos (BSS, *Basic Service Set*), consistente de dos o más estaciones (STAs, abreviatura proveniente de *stations*) ejecutando el mismo protocolo MAC y compitiendo para acceder al mismo medio compartido. Un BSS puede estar aislado o puede conectarse con un sistema de distribución (DS, *Distribution System*) troncal a través de un punto de acceso (AP, *Access Point*), que funciona como puente. El protocolo MAC puede ser completamente distribuido o controlado por una función de coordinación centralizada localizada en el punto de acceso. El conjunto de servicios básicos corresponde generalmente con lo que se conoce en la bibliografía como una celda. El sistema de distribución puede ser un conmutador, una red cableada o una red inalámbrica.

La Figura 2-3 ilustra la configuración más simple del modelo desarrollado por el grupo de trabajo 802.11, en el que cada estación pertenece a un único BSS, es decir, cada estación está sólo dentro del rango inalámbrico de las otras estaciones pertenecientes al mismo BSS. También es posible que dos o más BSS se superpongan geográficamente, permitiendo que una estación participe en más de un BSS. Más aún, la asociación entre una estación y un BSS es dinámica. Las estaciones pueden salirse o entrar en el rango de cobertura, o, simplemente, ser apagadas.

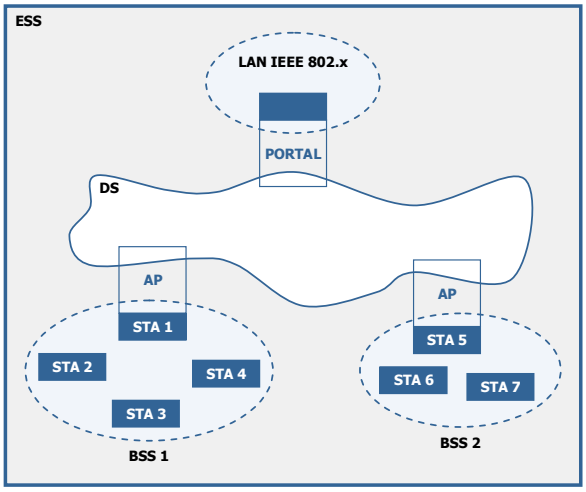

Figura 2-3. Arquitectura funcional de IEEE 802.11. *Fuente:* **[20]**

Un conjunto de servicios extendido (ESS, *Extended Service Set*) consta de dos o más servicios básicos interconectados por un sistema de distribución. Generalmente, el sistema de distribución es una LAN troncal cableada. El ESS aparece a nivel de la capa LLC como una única LAN lógica.

Un punto de acceso es implementado como parte de una estación. El punto de acceso es la lógica dentro de una estación que provee acceso al DS prestando los servicios propios del DS además de actuar como una estación. Para integrar la arquitectura IEEE con una LAN cableada tradicional, se utiliza un portal. La lógica del portal es implementada en un dispositivo como un puente o un enrutador que es parte de la red cableada y que está conectado al DS.

Adicionalmente, en cuanto al establecimiento de redes ad hoc, el estándar IEEE 802.11 define el conjunto de servicios básicos independiente (IBSS, *Independent Basic Service Set*). Las estaciones en un IBSS se comunican directamente, y por tanto deben estar en el rango de cobertura, unas con otras. La red 802.11 más pequeña que es posible establecer es un IBSS entre dos estaciones. Generalmente, los IBSS se constituyen con un propósito específico y por períodos cortos de tiempo; y suelen están compuestos por un número reducido de estaciones.

2.7. Servicios IEEE 802.11

IEEE 802.11-2007 define trece servicios que deben ser ofrecidos por la WLAN para proveer la funcionalidad equivalente a aquella que es inherente a las redes LAN cableadas [20].

El proveedor del servicio puede ser tanto la estación (STA) como el sistema de distribución (DS). Los servicios de estación deben ser implementados en cada estación 802.11, incluyendo los puntos de acceso (AP). Los servicios del sistema de distribución son provistos para dar soporte a la comunicación entre los BSS. Estos servicios pueden ser implementados en el punto de acceso o en otro dispositivo de propósito especial conectado al DS.

Tres de los servicios son usados para controlar el acceso y confidencialidad en la LAN IEEE 802.11. Otros seis servicios son usados para soportar la entrega de MSDU (*MAC Service Data Unit*, Unidad de Datos de Servicio MAC) entre estaciones. Un MSDU es un bloque de datos que pasa el usuario MAC a la capa MAC, típicamente un PDU LLC. Si el MSDU es demasiado grande para ser transmitido en una sola trama MAC, puede ser fragmentado y transmitido

en una serie de tramas MAC. Dos servicios más proveen administración del espectro de radiofrecuencia y finalmente dos servicios dan soporte a esquemas de calidad de servicio (QoS, *Quality of Service*).

En la Tabla 2-2 se listan los servicios ofrecidos por las redes IEEE 802.11, diferenciados según son implementados por el sistema de distribución o por las estaciones.

Tabla 2-2. Servicios ofrecidos por las redes WLAN IEEE 802.11. *Fuente:* **[20]**

Tipo de servicio	Servicio	Descripción
Servicios del Sistema de Distribución (DSS, *Distribution System Services*)	Distribución	Es el servicio principal utilizado por las estaciones para el intercambio de tramas MAC que deben atravesar el DS para llegar de una estación en un BSS a una estación en otro BSS. La forma como el mensaje es transportado a través del DS está más allá del alcance del estándar IEEE 802.11. Si la fuente y el destino de se encuentran dentro del mismo BSS, entonces el servicio de distribución se realiza a través del AP de dicho BSS
	Integración	Habilita la transferencia de datos entre una estación en una LAN IEEE 802.11 y una estación en una LAN IEEE 802.x integrada. El término "integrada" se refiere a una red no-IEEE 802.11 que está físicamente conectada al DS.
	Asociación	Establece una asociación inicial entre una estación y un punto de acceso. Antes de que una estación pueda transmitir o recibir tramas en una WLAN, su identidad y dirección deben ser conocidas. Tras establecer la asociación, el AP puede comunicar esta información a otros AP dentro del ESS para facilitar el enrutamiento y la entrega de tramas hacia la estación asociada
	Re-asociación	Permite que una asociación establecida pueda ser transferida de un AP a otro, permitiendo a una estación móvil trasladarse de un BSS a otro
	Des-asociación	No es más que una notificación, bien sea de la estación o del AP, indicando la terminación de una asociación existente. Una estación puede emitir esta notificación antes de abandonar el ESS o apagarse. Sin embargo, la lógica de administración MAC se protege a sí misma contra estaciones que desaparecen sin notificación
Servicios de Estación (SS, *Station Services*)	Entrega de MSDU	Transmisión de paquetes de capas superiores entre estaciones.
	Autenticación	Utilizada para que las estaciones puedan establecer su identidad unas con otras. En una red cableada, generalmente se asume que el acceso a una conexión física otorga autoridad para tener acceso a la LAN. Pero éste no es un argumento válido en una WLAN, en la que la conectividad es obtenida simplemente porque un dispositivo inalámbrico se encuentra dentro del rango de cobertura de la WLAN. IEEE 802.11 soporta varios esquemas de autenticación y permite la expansión de la funcionalidad de estos esquemas, aunque no obliga al uso de algún esquema específico. Sin embargo, IEEE 802.11 requiere que la autenticación sea mutuamente aceptada antes de que una estación pueda establecer una asociación con un AP

Tipo de servicio	Servicio	Descripción
	Des-autenticación	Este servicio es invocado cuando debe terminarse una autenticación existente
	Privacidad	Utilizado para prevenir que el contenido de los mensajes sea leído por otros elementos diferentes al receptor deseado. El estándar provee el uso opcional de esquemas de cifrado para asegurar la privacidad
	Planificación de calidad de servicio	Gestiona la entrega de MSDU de acuerdo al nivel de prioridad asignado según el tipo de tráfico. Sólo se utiliza en las WLAN que implementan los esquemas de QoS proporcionados por el estándar
	Sincronización de tiempo para capas superiores	Algunas aplicaciones altamente sensibles al tiempo, como la transmisión de flujos (*streams*) de audio y video requieren la sincronización de temporizadores, con un nivel importante de granularidad, entre diferentes STA. Igualmente, este servicio se utiliza sólo en las WLAN que implementan los esquemas de QoS proporcionados por el estándar
	Selección dinámica de frecuencia (DFS, *Dynamic Frecuency Selection*)	El marco regulatorio del espectro radioeléctrico de algunos países requiere que las WLAN que operan en la banda de 5 GHz aseguren dinámicamente la utilización uniforme de todos los canales de frecuencia y que eviten la co-utilización de canales con sistemas de radar
	Control de la potencia de transmisión (TPC, *Transmit Power Control*)	El marco regulatorio del espectro radioeléctrico de algunos países, requiere que las WLAN que operan en la banda de 5 GHz controlen dinámicamente la potencia máxima de transmisión para evitar la interferencia con sistemas satelitales

2.8. Subcapa MAC

La subcapa MAC IEEE 802.11 cubre tres áreas funcionales: entrega de datos confiable, control de acceso y seguridad [20]. A continuación se describen las dos primeras, mientras que la seguridad de redes 802.11 será abordada más adelante en este mismo capítulo.

2.8.1. Entrega de datos confiable

En general, cualquier WLAN está sujeta a una considerable falta de fiabilidad. El ruido, la interferencia y los efectos de propagación resultan en la pérdida de una cantidad significativa de tramas. Incluso con códigos de corrección de errores, muchas tramas MAC no serán recibidas exitosamente. Esta situación puede ser enfrentada con mecanismos de confiabilidad implementados en capas superiores, como por ejemplo TCP. Sin embargo, los tiempos de retransmisión en las capas superiores están típicamente por el orden de los segundos. Es por lo tanto más eficiente enfrentar los errores de transmisión a nivel de la

capa MAC. Con este propósito, IEEE 802.11 incluye protocolos propios para el intercambio de tramas. Cuando una estación recibe una trama de datos desde otra estación, devuelve una trama de confirmación (ACK, *acknowledgment*) a la estación fuente. Este intercambio es tratado como una unidad atómica, que no debe ser interrumpida por la transmisión de cualquier otra estación. Si la estación fuente no recibe un ACK en un corto período de tiempo, bien sea porque la trama de datos estaba dañada o porque el mismo ACK se dañó, entonces se retransmite la trama de datos. De este modo, el mecanismo básico de transferencia de datos en IEEE 802.11 involucra el intercambio de dos tramas.

Para mejorar aún más la confiabilidad, puede usarse un mecanismo de intercambio de cuatro tramas. En este esquema, la fuente transmite una trama de solicitud de envío (RTS, *Request To Send*) al destino. El destino responde entonces con una trama de libre para enviar (CTS, *Clear To Send*). Luego de recibir el CTS, la fuente transmite la trama de datos, y el destino responde con un ACK. El RTS alerta a todas las estaciones que están dentro del rango de recepción de la fuente que un intercambio está en marcha. Estas estaciones se abstienen de transmitir con el fin de evitar una colisión entre dos tramas transmitidas al mismo tiempo. De manera similar, el CTS alerta a las estaciones que están dentro del rango de recepción del destino que un intercambio está en marcha. La porción RTS/CTS del intercambio es una función requerida de la capa MAC IEEE 802.11, pero puede ser deshabilitada.

2.8.2. Control de acceso

El grupo de trabajo 802.11 consideró dos tipos de propuestas para el algoritmo MAC: protocolos de acceso distribuido, que como Ethernet, distribuyen la decisión de transmitir sobre todos los nodos usando un mecanismo de detección de portadora; y un protocolo de acceso centralizado. Un protocolo de acceso distribuido tiene sentido en redes ad hoc, aunque también puede ser atractivo en configuraciones de WLAN que consisten básicamente de tráfico a ráfagas. Un protocolo de acceso centralizado es de uso natural en configuraciones en las que una cantidad de estaciones inalámbricas están interconectadas entre sí y con algún tipo de estación base que se conecta a la red troncal (*backbone*) cableada. Este tipo de protocolos es especialmente útil si parte del tráfico es sensible al tiempo o de alta prioridad [37].

El resultado final para 802.11 es un algoritmo MAC llamado MAC inalámbrico base distribuido (DFWMAC, *Distributed Foundation Wireless MAC*) que provee un mecanismo de control de acceso distribuido con un mecanismo de control centralizado opcional construido sobre él.

La Figura 2-4 ilustra esta arquitectura de protocolos. La mitad inferior de la subcapa MAC es la Función de Coordinación Distribuida (DCF, *Distributed Cooordination Function*). DCF utiliza un algoritmo de contención o competición para proveer acceso a todo el tráfico. El tráfico asíncrono ordinario utiliza DCF directamente. La Función de Coordinación Puntual (PCF, *Point Cooordination Function*) es un algoritmo MAC centralizado usado para proveer un servicio sin competición. PCF se implementa sobre DCF y explota las características de DCF para asegurar el acceso a sus usuarios. A continuación se consideran en detalle estas dos subcapas.

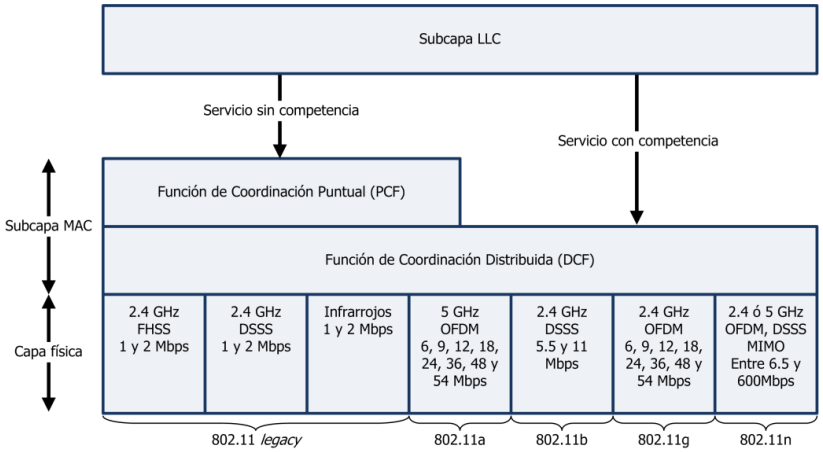

Figura 2-4. Arquitectura de protocolos IEEE 802.11. *Fuente:* [28]

2.8.3. Función de Coordinación Distribuida (DCF)

La subcapa DCF hace uso de un sencillo algoritmo CSMA (*Carrier Sense Multiple Access*, Acceso Múltiple con Escucha de la Portadora). Si una estación desea transmitir una trama MAC, sondea el medio. Si el medio está libre, la estación puede transmitir, si no debe esperar hasta que se haya completado la transmisión en curso antes de poder transmitir. DCF no incluye una función de detección de colisiones (es decir, CSMA/CD) puesto que la detección de colisión no resulta práctica en redes inalámbricas. El rango dinámico de las señales en el medio es muy elevado, de manera que una estación que transmita no puede distinguir de forma efectiva entre las señales débiles de ruido de entrada y los efectos de su propia transmisión.

Para asegurar el correcto funcionamiento de este algoritmo, DCF incluye un conjunto de retardos que equivale a un esquema de prioridades. Considérese un único retardo conocido como Espacio Intertrama (IFS, *Inter-Frame Space*). En la práctica existen tres valores

diferentes de IFS, pero el algoritmo se comprende mejor ignorando inicialmente este detalle. Haciendo uso de un IFS, las reglas de acceso CSMA son:

1. Una estación con una trama a transmitir sondea el medio. Si éste se encuentra libre, la estación espera ver si el medio permanece libre durante un tiempo igual a IFS. Si es así, la estación puede transmitir inmediatamente.

2. Si el medio está ocupado (bien porque la estación lo encuentra inicialmente así o porque se ocupa durante el tiempo libre IFS), la estación aplaza la transmisión y continúa supervisando el medio hasta que finalice la transmisión en curso.

3. Una vez concluida la transmisión actual, la estación espera otro IFS. Si el medio permanece libre durante este periodo, la estación espera según un esquema de retroceso exponencial binario y sondea de nuevo el medio. Si éste se encuentra libre aún, la estación puede transmitir. Durante el tiempo de retroceso exponencial, si el medio es ocupado, el temporizador de retroceso es detenido y es reiniciado cuando el medio es liberado.

Como en Ethernet, la técnica de retroceso exponencial binario proporciona un método para gestionar una carga alta. Si una estación intenta transmitir y encuentra ocupado el medio, espera un cierto tiempo y lo intenta de nuevo. Sucesivos intentos de transmisión fallidos provocan tiempos de retroceso cada vez mayores. Sin el uso de esta técnica podría presentarse la siguiente situación: dos o más estaciones tratan de transmitir al mismo tiempo, causando una colisión. Estas estaciones intentan retransmitir inmediatamente, causando una nueva colisión.

El esquema anterior se ha mejorado para que DCF proporcione un método básico de acceso simplemente mediante el uso de tres valores de prioridad de IFS:

- **SIFS (*Short IFS*, IFS Corto):** es el IFS más breve, y se usa para todas las acciones de respuesta inmediata como se explica más adelante.

- **PIFS (*Point Cooordination Function IFS*, IFS de Función de Coordinación Puntual):** IFS intermedio, empleado por el controlador centralizado en el esquema PCF cuando realiza sondeos.

- **DIFS (*Distributed Cooordination Function IFS*, IFS de Función de Coordinación Distribuida):** es el IFS mayor y se utiliza como retardo mínimo para tramas asíncronas que compiten para conseguir el acceso.

En la Figura 2-5 se ilustra el uso de estos valores temporales. Considérese primero el SIFS. Cualquier estación que use SIFS para determinar la oportunidad de transmitir tiene, de hecho, la prioridad superior, ya que siempre conseguirá el acceso en preferencia a una estación que espera una cantidad de tiempo igual a PIFS o DIFS. SIFS se utiliza en las siguientes circunstancias:

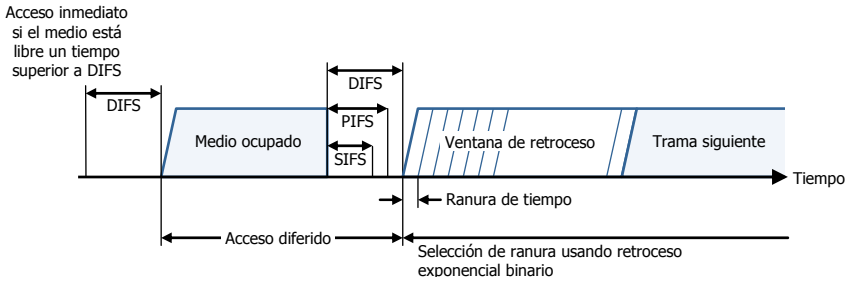

Figura 2-5. Método de acceso básico. Fuente: **[20]**

- ***Confirmación (ACK):*** cuando una estación recibe una trama dirigida sólo a ella (no multi-destino ni de difusión), responde con una trama ACK después de esperar un tiempo SIFS. Esto presenta dos efectos deseables. En primer lugar, dado que no se usa la detección de colisión, la probabilidad de colisiones es mayor que en CSMA/CD, permitiendo la trama ACK de nivel MAC la recuperación eficiente de éstas. En segundo lugar, SIFS se puede emplear para proporcionar un envío eficiente de una unidad de datos de protocolo LLC que necesite varias tramas MAC. En este caso se produce la siguiente situación: una estación con una PDU LLC multi-trama a transmitir envía las tramas MAC de una en una. Tras un SIFS, el receptor confirma cada una de las tramas. Cuando el origen recibe una trama ACK, inmediatamente (tras un SIFS) envía la siguiente trama de la secuencia. El resultado es que una vez que una estación ha luchado por conseguir el canal, mantendrá el control de éste hasta que haya enviado todos los fragmentos de una PDU LLC.

- ***Permiso para enviar (CTS):*** una estación puede asegurar que su trama de datos se enviará emitiendo primero una pequeña trama de petición de envío (RTS, *Request To Send*). La estación a la que va dirigida esta trama debería responder inmediatamente con una trama CTS (*Clear To Send*) si está lista para recibir. El resto de estaciones reciben el RTS y aplazan el uso del medio hasta que detectan un CTS correspondiente o hasta que expire un contador de tiempo.

- ***Respuesta ante sondeo:*** ésta se explica en la discusión sobre PCF más adelante.

El siguiente intervalo IFS más largo es el PIFS, usado por el controlador centralizado para llevar a cabo el envío de sondeos, y tiene precedencia sobre tráfico de contención normal. Sin embargo, las tramas transmitidas usando SIFS tienen prioridad sobre un sondeo PCF. Por último, el intervalo DIFS se usa para todo tráfico asíncrono ordinario.

2.8.4. Función de Coordinación Puntual (PCF)

La función de coordinación puntual (PCF, *Point Coordination Function*) es un método de acceso alternativo implementado en un nivel superior a DCF. El procedimiento consiste en la realización de un sondeo por parte del gestor de sondeo centralizado (coordinador puntual). El coordinador puntual hace uso de PIFS cuando realiza sondeos. Dado que PIFS es menor que DIFS, el coordinador puntual puede tomar el medio y bloquear todo el tráfico asíncrono mientras realiza sondeos y recibe respuestas.

Ahora, considérese la siguiente situación extrema: una WLAN se configura de modo que varias estaciones con tráfico sensible al tiempo son controladas por el coordinador puntual, mientras que el resto del tráfico compite haciendo uso de CSMA para conseguir el acceso. El coordinador puntual podría realizar sondeos en forma de rotación circular a todas las estaciones configuradas para sondeo. Cuando se realiza un sondeo, la estación sondeada puede responder usando SIFS. Si el coordinador puntual recibe una respuesta, envía otro sondeo usando PIFS. Si no se recibe respuesta durante el tiempo esperado de exploración circular de todas las estaciones, el coordinador envía un sondeo.

Si se implementase el esquema del párrafo anterior, el coordinador puntual paralizaría todo el tráfico asíncrono mediante el envío repetido de sondeos. Para evitar esto se define un intervalo conocido como supertrama. Durante la primera parte de este intervalo, el coordinador puntual envía sondeos en forma de rotación circular a todas las estaciones configuradas para sondeo. El coordinador puntual está ocioso durante el resto de la supertrama, permitiendo un periodo de competencia para acceso asíncrono.

En la Figura 2-6 se ilustra el uso de la supertrama. Al comienzo de ésta, el coordinador puntual puede tomar opcionalmente el control y enviar sondeos durante un periodo de tiempo dado. Este intervalo cambia debido al tamaño variable de la trama enviada por las estaciones correspondientes. El resto de la supertrama se encuentra disponible para un acceso basado en competición. Al final del intervalo de supertrama, el coordinador puntual

compite para conseguir el medio usando PIFS. Si el medio se encuentra libre, el coordinador puntual obtiene inmediatamente el acceso y sigue un periodo de trama completo. Sin embargo, el medio puede estar ocupado al final de una supertrama, en cuyo caso el coordinador puntual debe esperar hasta que el medio se encuentre libre para conseguir el acceso; esto da lugar a un periodo de supertrama menor para el siguiente ciclo.

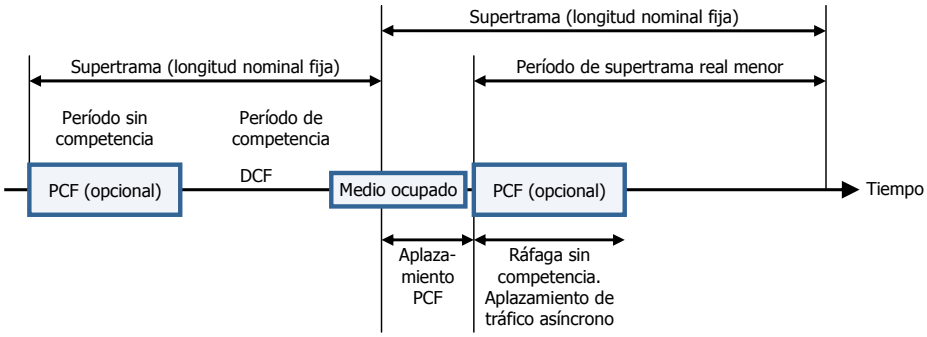

Figura 2-6. Construcción de supertramas PCF. Fuente:**[20]**

2.8.5. Trama MAC IEEE 802.11

La Figura 2-7 muestra el formato de trama MAC 802.11. Este formato general es usado para todas las tramas de datos, administración y control, pero no todos los campos son usados en todos los contextos. La Tabla 2-3 describe los campos de la trama MAC 802.11.

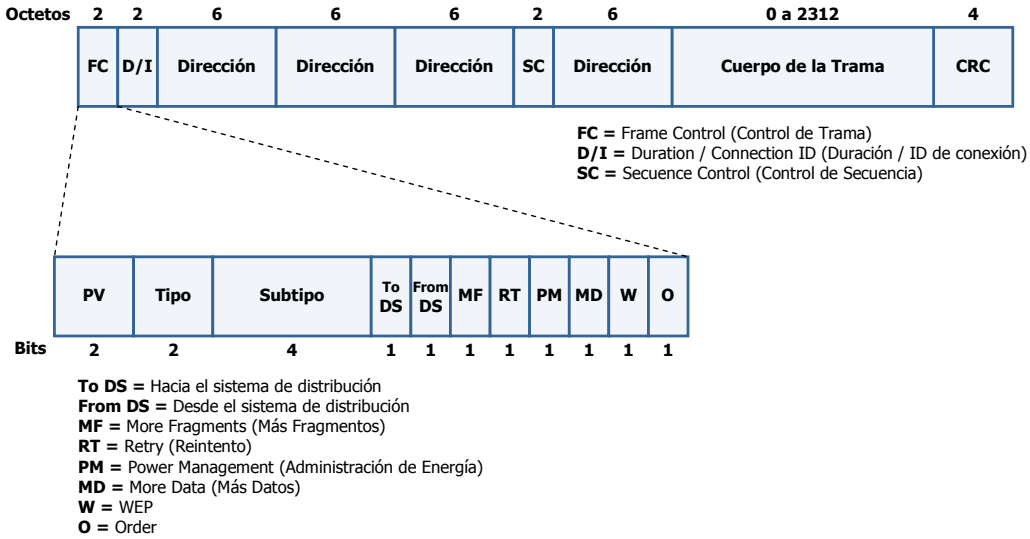

Figura 2-7. Formato de trama MAC IEEE 802.11. Fuente: **[37]**

Tabla 2-3. Campos de la trama MAC IEEE 802.11. Fuente: **[20]**

Campo	Descripción
Control de trama	Indica el tipo de trama y provee información de control. Está compuesto por los siguientes subcampos: ▪ **Versión del protocolo (*Protocol Version*):** indica la versión del protocolo 802.11 usada. Actualmente el valor de versión es cero ▪ **Tipo (*Type*):** identifica la trama como de control, administración o datos. ▪ **Subtipo (*Subtype*):** indica la función específica de la trama ▪ **Hacia DS (*To DS*):** un valor 1 indica que la trama está destinada al sistema de distribución ▪ **Desde DS (*From DS*):** un valor 1 indica que la trama está dejando el sistema de distribución. ▪ **Más fragmentos (*More Fragments*):** un valor 1 indica que más fragmentos prosiguen al actual ▪ **Reintento (*Retry*):** un valor 1 indica que ésta es una retransmisión de una trama previa ▪ **Administración de energía (*Power Management*):** un valor 1 indica que la estación está en modo de ahorro de energía ▪ **Más datos (*More Data*):** un valor 1 indica que una estación tiene más datos para enviar. Cada bloque de datos puede ser enviado como una sola trama o como un grupo de fragmentos en múltiples tramas ▪ **WEP:** un valor 1 indica el uso de WEP ▪ **Orden (*Order*):** un valor 1 indica que los datos están usando el servicio de orden estricto, el cual dice a la entidad receptora que las tramas deben ser procesadas en orden
Duración / ID de conexión (*Duration / Connection ID*)	Si es usado como campo de Duración, indica el tiempo (en microsegundos) que el canal estará asignado para la transmisión exitosa de una trama MAC. En algunas tramas de control, este campo contiene un identificador de asociación o conexión
Direcciones	El número y significado de los campos de direcciones dependen del contexto. Los tipos de dirección incluyen fuente, destino, estación transmisora y estación receptora
Control de secuencia	Contiene un subcampo de número de fragmento de 4 bits, usado para fragmentación y reensamblaje; y un subcampo de número de secuencia de 12 bits usado para enumerar las tramas enviadas entre un transmisor y un receptor dados
Cuerpo de la trama	Contiene un MSDU o un fragmento de un MSDU
Secuencia de chequeo de trama	Contiene un chequeo de redundancia cíclica de 32 bits

2.9. Capa física (PHY)

Las especificaciones de capa física para IEEE 802.11 han sido promulgadas en varias etapas. Estas especificaciones se detallan a continuación.

2.9.1. Capa física del estándar IEEE 802.11 original

El estándar IEEE 802.11 original, conocido actualmente como 802.11 *legacy*, fue publicado en 1997 y revisado en 1999. En él se definen tres medios físicos para redes inalámbricas [4]:

- ***Espectro Expandido por Secuencia Directa:*** Los sistemas WLAN DSSS (*Direct Sequence Spread Spectrum*, Espectro Expandido por Secuencia Directa) operan en la banda ISM de 2.4 GHz con tasas de datos de 1 y 2 Mbps. El número de canales disponibles para la transmisión depende del ancho de banda asignado por las diversas agencias reguladoras nacionales. Esto varía desde 13 canales disponibles en la mayoría de los países europeos hasta un solo canal disponible en Japón. Cada canal tiene un ancho de banda de 5 Mhz. El esquema de codificación utilizado es DBPSK (*Differential Binary Phase-Shift Keying*, Codificación por Desplazamiento de Fase Binario Diferencial) para la velocidad de 1 Mbps y DQPSK (*Differential Quadrature Phase-Shift Keying*, Codificación por Desplazamiento de Fase en Cuadratura Diferencial) para la velocidad de 2 Mbps.

  DSSS hace uso de un *chipping code*, o secuencia de pseudo-ruido, para expandir la tasa de datos y por tanto el ancho de banda de la señal. En el caso específico de IEEE 802.11 se utiliza una secuencia conocida como secuencia de Barker de 11 chips. Las secuencias de Barker añaden robustez contra la interferencia y no son susceptibles ante la propagación multi-camino. Al momento de la transmisión, cada cero y uno binario son mapeados a sus respectivas secuencias.

- ***Espectro Expandido por Salto de Frecuencia:*** Los sistemas WLAN FHSS (*Frequency-Hopping Spread Spectrum*, Espectro Expandido por Salto de Frecuencia), también operan en la banda ISM de 2.4 GHz con tasas de datos de 1 y 2 Mbps. Se utilizan múltiples canales, con la señal transmitida saltando de un canal a otro basado en una secuencia de pseudo-ruido. En el caso del esquema 802.11, se utilizan canales de 1 MHz. El número de canales usado varía desde 23 en Japón hasta 70 en los Estados Unidos. Los detalles del esquema de salto son ajustables. Por ejemplo, la mínima tasa de saltos en los Estados Unidos es de 2.5 por segundo. La distancia mínima de salto es de 6 MHz en la mayor parte de América y Europa y de 5 MHz en Japón.

  Para la modulación, el esquema FHSS utiliza GFSK (*Gaussian Frequency Phase-Shift Keying*, Codificación por Desplazamiento de Frecuencia Gaussiano) de dos niveles para los sistemas de 1 Mbps. Los bits 0 y 1 son codificados como desviaciones de la frecuencia portadora utilizada en el momento. Para los sistemas de 2 Mbps se utiliza

GFSK de cuatro niveles, en los que cuatro diferentes desviaciones de la frecuencia central definen las cuatro combinaciones de dos bits que se usan en la transmisión.

- ***Infrarrojos:*** IEEE 802.11 define un esquema de infrarrojos omnidireccional. Es posible obtener un rango de transmisión de hasta 20 metros. El esquema de modulación para la velocidad de 1 Mbps es conocido como 16-PPM (*Pulse Position Modulation*, Modulación por Posición de Pulso). Cada grupo de 4 bits de datos es mapeado a una cadena de 16 bits consistente de quince ceros y un uno binario. Para la velocidad de 2 Mbps, cada grupo de 2 bits de datos es mapeado a una cadena de 4 bits consistente de tres ceros y un uno binario. La transmisión real consiste de un esquema de modulación de intensidad, en el que la presencia de señal representa un uno binario y la ausencia de señal representa un cero binario.

2.9.2. Capa física del estándar IEEE 802.11-2007

Luego de la publicación del estándar original, el grupo de trabajo 802.11 desarrolló tres especificaciones adicionales de capa física. Originalmente denominadas 802.11a, 802.11b y 802.11g, por estar ahora completamente incorporadas en la versión del estándar del año 2007, ya no son formalmente conocidas por esos nombres. Sin embargo, comercialmente se sigue usando la denominación original de las especificaciones a efectos de identificar fácilmente de qué tipo de capa física se está hablando.

- ***IEEE 802.11a:*** esta extensión fue publicada en 1999 y hace uso de la banda de frecuencia de 5 GHz. A diferencia de las especificaciones de 2.4 GHz, no se hace uso de técnicas de espectro expandido, sino que se utiliza OFDM (*Orthogonal Frequency Division Multiplexing, Multiplexación* por División de Frecuencia Ortogonal). OFDM utiliza múltiples señales portadoras a diferentes frecuencias, enviando conjuntos de bits por cada canal. Esto es similar al FDM tradicional, aunque en OFDM todos los subcanales están dedicados a una única fuente de datos. Las velocidades transmisión de 802.11a van desde 6 hasta 54 Mbps. El sistema usa hasta 52 subportadoras que son moduladas usando BPSK, QPSK, 16-QAM, o 64-QAM, dependiendo de la velocidad requerida. El espaciado entre frecuencias subportadoras es de 0.3125 MHz. Se provee corrección de errores hacia adelante mediante el uso de códigos de convolución a una tasa de 1/2, 2/3 ó 3/4. Esta especificación de capa física no tuvo mayor éxito comercial debido que por operar en una banda de frecuencia distinta a 802.11b, no eran mutuamente compatibles.

- ***IEEE 802.11b:*** publicado también en 1999, es una extensión del esquema DSSS del 802.11 original que provee velocidades de 5.5 y 11 Mbps. La tasa de *chipping* es de 11 MHz, igual que en el esquema DSSS original. Esto significa que se ocupa el mismo ancho de banda. Para alcanzar velocidades más altas se utiliza un esquema de modulación conocido como CCK (*Complementary Code Keying*, Codificación por Clave Complementaria). Los datos son manejados en bloques de 8 bits a una tasa de 1.375 MHz (8 bits / Símbolo • 1.375 MHz = 11 Mbps). Seis de estos bits son mapeados en una de 64 secuencias de códigos basados en el uso de la matriz de Walsh. La salida del mapeado más los dos bits adicionales forman la entrada para un modulador QPSK.

- ***IEEE 802.11g:*** Este estándar fue publicado en 2003. Provee una extensión a los esquemas DSSS tanto del 802.11 original como 802.11b, brindando compatibilidad hacia atrás con este último. Proporciona velocidades de transmisión similares a la de la especificación 802.11a y se utiliza el mismo esquema de modulación OFDM, pero trabajando en la banda de frecuencias ISM de 2.4 GHz. La compatibilidad es alcanzada en un modo de operación que combina características de DSSS y OFDM. Vale destacar que la mayoría de las implementaciones actuales de WLAN están basadas en las especificaciones del b y g estándar IEEE 802.11.

2.9.3. IEEE 802.11n

En enero de 2004 el IEEE anunció la formación de un grupo de trabajo (TGn) encargado de desarrollar una nueva revisión del estándar 802.11. El proceso de aprobación del estándar se produjo en septiembre de 2009, y se espera su publicación definitiva en octubre de este mismo año [16] [17]. Con esta revisión se espera proveer una tasa de datos teórica de 540 Mbps, lo que requeriría un desempeño incluso mayor en la capa física. En consecuencia, una red 802.11n podría llegar a ser hasta 10 veces más rápida que una red 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. Otra de las mejoras esperadas es una mayor distancia operativa que la de las redes inalámbricas actuales.

Los esquemas de modulación utilizados son OFDM y QAM, lo que facilita la compatibilidad con los estándares previos. Adicionalmente se utiliza una tecnología conocida como MIMO (*Multiple-Input/Multiple-Output*, Entradas-Mútliples/Salidas-Múltiples) en la que mediante el uso de una combinación de antenas para la transmisión y recepción de flujos de datos simultáneos, se obtiene un mayor rendimiento.

El proceso de estandarización comenzó con un conjunto de propuestas competidoras, de las cuales TGn Sync y WWiSE (*World Wide Spectrum Efficiency*) obtuvieron mayor aceptación. Finalmente se decidió utilizar la propuesta TGn, pero incorporando las mejores características de WWiSE, con el objetivo de obtener un equilibrio entre velocidad de transmisión, distancia efectiva de operación y eficiencia en el uso del espectro electromagnético.

Actualmente, están comercialmente disponibles dispositivos, denominados "pre-n", que se han adelantado al protocolo y ofrecen de forma no oficial éste estándar, con la promesa de actualizaciones que cumplan con la versión definitiva cuando ésta sea definitivamente publicada.

2.10. Otras extensiones de IEEE 802.11

Desde su creación, el grupo de trabajo IEEE 802.11 ha establecido una serie de grupos de tarea (*task groups*) destinados a elaborar diversas extensiones al estándar. En la Tabla 2-4 se describe el propósito de algunos de los grupos de tarea más relevantes.

Tabla 2-4. Grupos de tarea relevantes de IEEE 802.11. *Fuente:* **[18]**

Grupo de tarea	Propósito
TGc	Especifica el uso de puentes (*bridges*) en redes WLAN 802.11. *Estatus:* el trabajo de este grupo se considera completado y es parte de los estándares 802.1D y 802.11-2007
TGd	Trata asuntos relacionados con la adopción del estándar IEEE 802.11 en países con marcos regulatorios distintos a los usados en Estados Unidos, Europa y Japón. *Estatus:* el trabajo de este grupo se considera completado y es parte del estándar 802.11-2007
TGe	Relacionado con la implementación de esquemas de calidad de servicio (QoS) en redes 802.11. *Estatus:* el trabajo de este grupo se considera completado y es parte del estándar 802.11-2007
TGF	Especifica protocolos de intercomunicación entre puntos de acceso (IAPP, *Inter Access Point Protocol*). No es un estándar, sino un conjunto de prácticas recomendadas. *Estatus:* el trabajo de este grupo se considera completado. Fue publicado como 802.11F-2003, aunque fue retirado en 2006
TGh	Requerimientos especiales para el espectro de 5 GHz en redes WLAN usadas en Europa. *Estatus:* el trabajo de este grupo se considera completado y es parte del estándar 802.11-2007
TGi	Mejoras en los mecanismos de seguridad y autenticación para redes 802.11. *Estatus:* el trabajo de este grupo se considera completado y es parte del estándar 802.11-2007

Grupo de tarea	Propósito
TGj	Extensiones específicas para Japón. *Estatus:* el trabajo de este grupo se considera completado y es parte del estándar 802.11-2007
TGk	Mejoras en la medición de los recursos de radio, para proveer información a las capas superiores. *Estatus:* el trabajo de este grupo se considera completado y es parte del estándar 802.11k-2008
TGm	Encargado del mantenimiento de las correcciones técnicas y editoriales sobre la versión actual del estándar IEEE 802.11. *Estatus:* activo
TGp	WAVE (*Wireless Access for the Vehicular Environment*, Acceso Inalámbrico para el Ambiente Vehicular). Especificaciones especiales para el uso de tecnología 802.11 en vehículos como ambulancias, autobuses, etc. *Estatus:* activo
TGr	*Fast roaming* entre distintos BSS. *Estatus: e*l trabajo de este grupo se considera completado y es parte del estándar 802.11r-2008
TGs	Desarrollar un *Extended Service Set* (ESS) con topología de malla usando un sistema de distribución inalámbrico (WDS, *Wireless Distribution System*). *Estatus:* activo
TGT	Métodos de prueba y métricas de desempeño de la red. No es un estándar, sino un conjunto de prácticas recomendadas. *Estatus:* activo
TGu	*Internetworking* con redes no-802. *Estatus:* activo
TGv	Administración a nivel de capa de enlace, centralizada o distribuida, de las estaciones en una red WLAN. Esto incluye monitoreo, configuración y actualización. *Estatus:* activo
TGw	Mejoras en la seguridad de algunas tramas de administración y control del estándar 802.11. Define mejoras a nivel de integridad de datos, autenticación del origen, protección contra *replay* de tramas y confidencialidad. *Estatus:* activo
TGy	Mecanismos para permitir la operación de 802.11 en la banda de frecuencias de 3650-3700 MHz (sólo en Estados Unidos). *Estatus:* esta extensión ha sido aprobada, pero se encuentra pendiente por publicación
TGz	Soporte para *Direct Link Setup* (DLS). *Estatus:* activo
TGaa	Transmisión robusta de flujos de audio y video a través de redes 802.11. *Estatus:* activo
TGad	Mejoras significativas en las velocidades de transmisión de datos para redes WLAN 802.1. *Estatus:* activo
WNG SG *Wireless Next Generation*	No es propiamente un grupo de tarea, sino un grupo de estudio encargado de establecer la próxima generación de características y mejoras al estándar IEEE 802.11. Agrupa todas las investigaciones e innovaciones que puedan considerarse como alternativas futuras para la mejora del rendimiento y la confiabilidad de las redes WLAN. *Estatus:* activo

2.11. Seguridad de la información

La seguridad de la información puede definirse como el conjunto de procesos y tecnologías relacionadas con la protección contra el acceso, uso, divulgación, modificación o destrucción no autorizados de la información y de los sistemas computacionales utilizados para gestionarla [25].

En el mundo globalizado actual, la organización o el individuo que dispone de la información apropiada en el momento oportuno incrementa significativamente su eficacia y productividad, lo que al final se traduce en valor estratégico y, la mayoría de las veces, también económico [27]. Hoy en día se habla de que el valor de mercado de muchas empresas, grandes y pequeñas, no viene dado mayormente sus activos físicos, sino por el valor de la información que en éstas se maneja. De allí nace precisamente la necesidad de proteger la información.

Con el crecimiento exponencial de la adopción de las tecnologías de información y comunicación en las empresas, entes gubernamentales y usuarios finales, también ha venido asociado un incremento de las amenazas que afectan a la información que éstos manejan. Como consecuencia, el campo de la seguridad de la información ha evolucionado significativamente en los últimos años.

2.11.1. Principios básicos de la seguridad de la información

Como concepto, la seguridad de la información está construida sobre tres pilares: confidencialidad, integridad y disponibilidad, conocidos también como la tríada CIA (*Confidentiality, Integrity, Availability*) [25]. Éstos constituyen los principios básicos que permiten definir si un sistema o pieza de información cuenta con un nivel apropiado de seguridad.

- ***Confidencialidad:*** es la propiedad de prevenir la divulgación de la información a individuos o sistemas no autorizados.

- ***Integridad:*** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

- ***Disponibilidad:*** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

La Tabla 2-5 muestra otros conceptos asociados a la seguridad de la información que complementan o ayudan a preservar los tres pilares fundamentales.

Tabla 2-5. Otros conceptos asociados a la seguridad de la información. *Fuente:* [35]

Concepto	Definición
Amenaza	Cualquier acción o evento que puede ocasionar consecuencias adversas
Ataque	Tipo y naturaleza de inestabilidad en la seguridad
Auditabilidad	Permitir la reconstrucción, revisión y análisis de la secuencia de eventos
Autenticación	Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, que se tiene o una combinación de todas éstas
Autorización	Aquello que se permite una vez que se ha otorgado acceso
Contra medida	Cualquier acción o proceso que reduce la vulnerabilidad
Control	Cualquier acción o proceso que se utiliza para mitigar el riesgo
Control de acceso	Limitar el acceso autorizado sólo a entidades autenticadas
Criticidad	La importancia o valor que tiene un recurso de información para una organización
Impacto	Resultados y consecuencias de que se materialice un riesgo
No repudio	Evitar que se puede negar un evento o una transacción
Norma	Establece los límites permisibles de acciones y procesos para dar cumplimiento a las políticas
Política de seguridad de la información	Declaración de alto nivel sobre la intención y la dirección de la organización en cuanto a la seguridad de su información
Riesgo	Es el producto del nivel de la amenaza por el nivel de vulnerabilidad. Establece la probabilidad de éxito de un ataque
Vulnerabilidad	Deficiencia o debilidad que puede ser explotadas por una amenaza

2.11.2. Estándares sobre la seguridad de la información

Organismos como el Instituto Nacional de Estándares y Tecnología (NIST, *National Institute of Standards and Technology*) de los Estados Unidos, y la Organización Internacional para la Estandarización (ISO, *International Organization for Standardization*) han establecido estándares que se usan actualmente como referencia sobre el tema de seguridad de información.

El NIST ha desarrollado un conjunto de publicaciones conocidas como el Estándar Federal de Procesamiento de Información (FIPS, *Federal Information Processing Standard*) [32]. Por otra parte, la ISO ha establecido una serie de estándares bajo la serie ISO/IEC 27000, que hasta la fecha abarca seis documentos publicados, dedicados a diversos aspectos de la seguridad de la información como gestión, metodología y elementos técnicos [24].

2.12. Amenazas a la seguridad de la redes WLAN

A pesar de todos los beneficios que ofrecen, existen debilidades de seguridad en las redes WLAN, que hasta cierto punto han limitado su adopción; particularmente en el sector corporativo y de gobierno, que son los que frecuentemente tienen mayores requerimientos de protección de datos. Sin embargo, aunque los riesgos de la transmisión de datos en plano en una red desprotegida deberían ser evidentes; sorpresivamente, un número importante de redes WLAN son desplegadas sin ningún tipo de medidas de seguridad [42]. Por otra parte, la mayoría de las organizaciones que han implementado algún tipo de seguridad inalámbrica, lo han hecho de forma básica, primordialmente con esquemas de primera generación, que ofrecen una protección inadecuada, de acuerdo a los estándares actuales [28].

Cuando se desarrollaba el estándar IEEE 802.11 original, la seguridad de la información no era un tema de preocupación de la magnitud que lo es hoy en día. Además, el nivel de sofisticación de las amenazas era mucho menor y la adopción de las tecnologías inalámbricas apenas estaba iniciando.

En el diseño de WEP se subestimaron las medidas necesarias para hacer a la seguridad del medio inalámbrico "equivalente" a la del par trenzado. En contraste, los mecanismos de seguridad más recientes han sido diseñados para operar en ambientes hostiles donde no existen límites físicos claramente definidos.

Las debilidades de seguridad concernientes al esquema WEP estático traen como consecuencia que las WLAN protegidas por éste son vulnerables a varios tipos de amenazas. Existen herramientas de auditoría de WLAN, disponibles libremente, que permiten irrumpir de manera trivial en redes protegidas por WEP.

Antes de estudiar los esquemas de seguridad existentes para redes WLAN, es importante comprender las principales amenazas que éstas confrontan, resumidas en la Tabla 2-6.

Tabla 2-6. Principales amenazas a la seguridad de las WLAN. *Fuente:* [13]

Amenaza	Descripción
Escucha no autorizada (fuga de información)	Un atacante se conecta a la WLAN con el objetivo de obtener acceso a datos confidenciales o capturar credenciales de usuarios válidos. El intruso también puede recolectar información sobre la plataforma tecnológica de la organización, como fase de preparación para un ataque de mayor envergadura

Amenaza	Descripción
Intercepción y modificación de los datos transmitidos	Si el atacante puede ganar acceso a la red, puede insertar un equipo furtivo para interceptar o modificar la data transmitida entre dos entes legítimos
Suplantación (*Spoofing*)	El fácil acceso a la red interna permite que un intruso pueda forjar datos aparentemente legítimos, de manera que no sería posible fuera de la red (por ejemplo, un mensaje falso de correo electrónico). En general, las personas, incluyendo a los administradores de sistemas, tienden a confiar mucho más en la información que se origina internamente que en algo que se procede del exterior de la red corporativa
Denegación de Servicio (DoS, *Denial of Service*)	Es fácil disparar diversos tipos ataques de denegación de servicio contra una WLAN, que afecten en mayor o menor medida su disponibilidad. Por ejemplo, se puede interferir la señal de radio con elementos que operan en la misma banda de frecuencia que la red; y aquí es factible utilizar elementos tan simples como un horno de microondas. Algunos ataques más sofisticados tienen como objetivo los protocolos inalámbricos de bajo nivel, mientras que otros más simples buscan inundar la red con cantidades descomunales de tráfico aleatorio para saturar el medio
Uso no autorizado de recursos(*free-loading*)	Un intruso pudiera querer utilizar la WLAN de la organización como un punto de acceso gratuito (*hotspot*) hacia Internet. Aunque en sí misma no es un tipo de amenaza tan peligrosa como el resto, eventualmente disminuirá los niveles de servicio de la red y puede convertirse en un punto de entrada de código malicioso (como virus, troyanos y gusanos)
Amenazas accidentales	Algunas características de las WLAN convierten a algunos incidentes no intencionales en amenazas reales. Por ejemplo, un visitante legítimo puede iniciar su computador portátil sin intenciones de ingresar a la red de la organización, pero es conectado automáticamente a la WLAN. Ahora ese computador puede convertirse en una potencial amenaza para la red
Redes WLAN furtivas (*rogue WLAN*)	Aunque la organización no haya desplegado "oficialmente" una WLAN, se puede estar bajo amenaza debido a puntos de acceso inalámbricos conectados furtivamente a la red corporativa. La conjunción de hardware de bajo costo y empleados "entusiastas" puede vulnerar gravemente la red de la organización

2.13. Esquemas de seguridad para redes IEEE 802.11

La protección de redes WLAN implica tres elementos principales [14]:

- Autenticar a la persona (o dispositivo) que se está conectando a la WLAN, de manera que se pueda tener un alto grado de certeza sobre quién o qué intenta ingresar a la red.

- Autorizar el uso de la red, para poder controlar quién tiene acceso a ésta.

- Proteger la data transmitida en la red, de manera de asegurarla contra escuchas o modificaciones no autorizadas.

Adicionalmente se pueden requerir funcionalidades de auditoría, como medida para validar y reforzar los elementos anteriores.

El estándar IEEE 802.11-2007 establece el concepto de asociación a la red con seguridad robusta (RSNA, *Robust Security Network Association*) [20], que define funciones para la protección de las tramas de datos. Se hace uso del estándar IEEE 802.1X para proveer autenticación y gestión de claves de cifrado. Todas las estaciones en una RSNA tienen una entidad correspondiente que maneja estos servicios.

De acuerdo a lo definido en el estándar, se establecen dos tipos de mecanismos de seguridad para redes WLAN: algoritmos pre-RSNA y algoritmos RSNA [20].

Los métodos de seguridad pre-RSNA incluyen:

- Privacidad equivalente a la del cable (WEP, *Wireless Equivalent Privacy*).
- Autenticación abierta de sistemas (OSA, *Open System Authentication*).
- Autenticación por clave compartida (SKA, *Shared Key Authentication*).
- Filtrado de direcciones MAC

A excepción de OSA, todos los mecanismos de seguridad pre-RSNA han sido descontinuados, porque no cumplen con las metas de seguridad del estándar. Las nuevas implementaciones de redes IEEE 802.11 sólo deben soportar métodos pre-RSNA para ayudar a la migración hacia métodos RSNA.

Los métodos de seguridad RSNA incluyen:

- TKIP (*Temporal Key Integrity Protocol*).
- CCMP (*Counter Mode with CBC-MAC Protocol*).
- Autenticación IEEE 802.1X para el establecimiento y terminación de RSNAs
- Procedimientos de manejo de claves.

El resto de este capítulo se ocupa de describir los métodos de seguridad presentes en el estándar IEEE 802.11-2007.

2.14. WEP

En las WLAN, la escucha no autorizada de la transmisión es una de las preocupaciones principales, debido a la facilidad con la que puede ser capturada la información. IEEE 802.11 original incorporaba WEP para proveer un nivel modesto de seguridad. Para brindar privacidad, así como integridad de los datos, WEP utiliza el algoritmo de cifrado RC4 PRNG (*Pseudo-Random Number Generator*, generador de números pseudo-aleatorios) de la empresa RSA Data Security [13].

La Figura 2-8 muestra el proceso de cifrado. El algoritmo de integridad es simplemente un CRC de 32 bits que se agrega al final de la trama MAC. Para el proceso de cifrado, una clave secreta de 40 o 104 bits es compartida por los dos participantes en la comunicación. Un vector de inicialización (IV, *Initialization Vector*) es concatenado a la clave secreta. El bloque resultante forma la semilla que es la entrada del algoritmo PRNG definido en RC4. A partir de allí se genera un secuencia de bits de la misma longitud de la trama MAC más el CRC. Un XOR a nivel de bits entre la trama MAC y la secuencia PRNG forma el texto cifrado. El IV es concatenado al texto cifrado y el bloque resultante es transmitido. El IV es cambiado periódicamente (tan frecuentemente como con cada transmisión). Cada vez que el IV es cambiado, la secuencia PRNG también cambia, lo que complica la tarea de la escucha de la información por parte de intrusos.

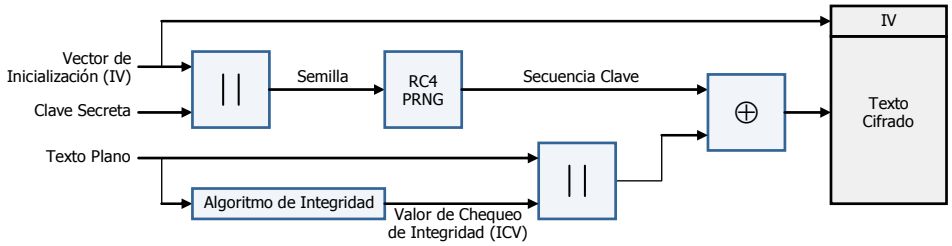

Figura 2-8. Proceso de cifrado WEP. Fuente [37]

En el extremo receptor (Figura 2-9), se recupera el IV del bloque de datos recibido y se concatena con la clave compartida para generar la misma secuencia usada por el emisor. Se realiza un XOR entre esta secuencia y el bloque entrante de datos para recuperar el texto plano. Esta técnica hace uso de la siguiente propiedad del XOR:

$$A \oplus B \oplus B = A$$

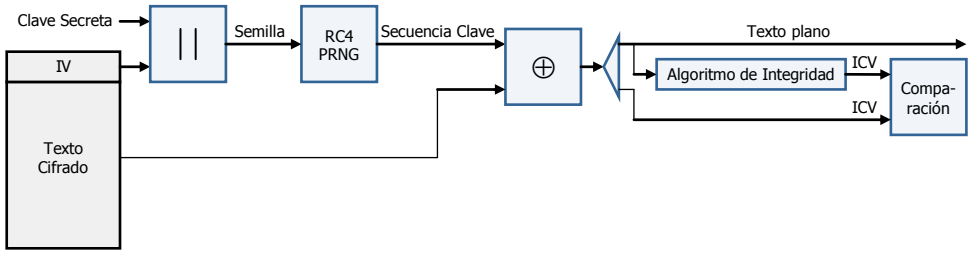

Figura 2-9. Proceso de descifrado WEP. Fuente [37]

Por tanto, si se toma el texto plano, se realiza un XOR entre éste y la secuencia clave, y de nuevo se realiza un XOR con la misma secuencia clave, se obtiene el texto plano. Finalmente, el receptor compara el CRC del bloque entrante con el CRC calculado por él mismo para validar la integridad de los datos.

Cuando empezó a crecer el despliegue de redes WLAN a nivel residencial y empresarial se incrementó el escrutinio de los investigadores sobre WEP, y sus limitaciones como esquema válido de seguridad fueron prontamente identificadas [9]. Como solución de primera generación, WEP es vulnerable debido a limitaciones en el tamaño de las claves de cifrado (inicialmente 40 bits, y posteriormente incrementadas a 104 bits) y su falta de detección de ataques de repetición (*replay attacks*) [38].

Por otra parte, la principal vulnerabilidad de WEP radica en que no implementa adecuadamente el vector de inicialización del algoritmo RC4, ya que utiliza un enfoque predecible para incrementar el vector de un paquete a otro [9]. Además existe un problema con el tamaño del propio vector (24 bits): a pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación. Conociendo los IV utilizados repetidamente y aplicando técnicas relativamente simples de descifrado puede finalmente vulnerarse la seguridad de la WLAN [38]. Aumentar los tamaños de las claves de cifrado aumenta el tiempo necesario para romperlo, pero no hace imposible el descifrado.

Esto hizo que los usuarios tuvieran que complementar el uso de WEP con esquemas de seguridad a niveles superiores, como VPNs (*Virtual Private Networks*, redes privadas virtuales), IEEE 802.1X y soluciones propietarias. Como consecuencia, el uso de WEP para confidencialidad, autenticación y control de acceso ha sido descontinuado en IEEE 802.11-2007, bajo el argumento de que WEP ya no apto es para los propósitos del estándar.

2.15. Métodos de autenticación pre-RSNA

El estándar IEEE 802.11 original [19] proveía dos tipos de autenticación: de sistema abierto y de clave compartida.

La autenticación de sistema abierto (*Open System Authentication*) simplemente provee una forma para que dos partes acuerden el intercambio de datos y no provee beneficios en cuanto a seguridad. En la autenticación de sistema abierto, una parte envía una trama MAC de control, conocida como trama de autenticación a la otra parte. La trama indica que el tipo de autenticación es de sistema abierto. La otra parte responde con su propia trama de autenticación y el proceso es completado. Entonces, este tipo de autenticación consiste simplemente del intercambio de identidades entre las partes.

La autenticación por clave compartida (*Shared Key Authentication*) requiere que las dos partes compartan una clave secreta. Esta clave es usada para asegurar que ambos lados son autenticados entre sí. El procedimiento para la autenticación entre dos partes A y B, se realiza de la siguiente manera:

1. A envía una trama de autenticación con el tipo de algoritmo de autenticación configurado como de clave compartida además de enviar su identificador.

2. B responde con una trama de autenticación que incluye un texto de desafío de 128 octetos. El texto de desafío es generado utilizando el algoritmo PRNG RC4. La clave y el IV utilizados en la generación del desafío carecen de importancia, debido a que no juegan un rol fundamental en el resto del procedimiento.

3. A transmite un trama de autenticación que incluye el texto de desafío que acaba de recibir de B. La trama entera es cifrada usando WEP.

4. B recibe la trama cifrada y la descifra usando WEP y la clave que comparte con A. Si el descifrado es exitoso (coinciden las sumas de comprobación), entonces B compara el texto de desafío entrante con el texto de desafío que envió en el segundo mensaje. B envía entonces un mensaje de autenticación a A con un código de estatus que indica el éxito o la falla del procedimiento.

2.16. Autenticación IEEE 802.1X

El estándar IEEE 802.1X [22] establece el concepto de autenticación de puerto de red *(network port authentication*) para redes IEEE 802, incluyendo Ethernet, Token Ring y redes inalámbricas 802.11. IEEE 802.1X sólo define un *framework* de autenticación, dejando los detalles de los métodos de autenticación a otros documentos como el RFC 2716, *"PPP EAP TLS Authentication Protocol"* [3].

Originalmente, 802.1X fue desarrollado para su uso en redes cableadas IEEE 802, y en su especificación no describe como adaptarlo para su uso en redes IEEE 802.11. Los detalles de esta adaptación son descritos en la especificación de seguridad mejorada del estándar IEEE 802.11-2007. Por ejemplo, 802.1X no define si la autenticación se lleva a cabo antes o después del servicio de asociación, ni como son utilizadas las claves derivadas en las suites de cifrado especificadas (TKIP y CCMP). Tampoco describe cómo lidiar con las vulnerabilidades encontradas en el protocolo WEP.

2.16.1. Protocolo de autenticación extensible (EAP)

Extensible Authentication Protocol (EAP, protocolo de autenticación extensible) [1] es un *framework* de autenticación usado habitualmente como parte del estándar IEEE 802.1X. En sí, es una estructura de soporte, no un mecanismo específico de autenticación. Provee algunas funciones comunes y negociaciones para el o los mecanismos de autenticación escogidos. Estos mecanismos son llamados métodos EAP, de los cuales se conocen actualmente unos cuarenta distintos.

2.16.2. Métodos EAP para redes IEEE 802.11

Los métodos EAP modernos capaces de operar en ambientes inalámbricos incluyen EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP y EAP-TTLS [2]. Los requerimientos para métodos EAP usados en LAN inalámbricas son descritos en el RFC 4017. Cuando EAP es invocado por un dispositivo NAS (*Network Access Server*) capacitado para 802.1X, como por ejemplo un punto de acceso 802.11, los métodos EAP proveen un mecanismo seguro de autenticación y negocian un PMK (*Pair-wise Master Key*) entre el dispositivo cliente y el NAS. En esas circunstancias, la PMK puede ser usada para establecer una sesión inalámbrica cifrada basada en TKIP o AES.

2.16.3. Arquitectura de IEEE 802.1X

El estándar IEEE 802.1X define tres componentes que hacen parte del proceso de autenticación, y que se ilustran en la Figura 2-10 (a). El solicitante (*suplicant*) representa al dispositivo de usuario final que requiere acceso a la red. El acceso a la red es controlado por el autenticador *(authenticator)***.** Éste ejerce el mismo rol que un servidor de acceso en una red de discado (*dial-up network*). Tanto el solicitante como el autenticador son referidos como entidades de autenticación de puerto (PAE, *Port Authentication Entities*) en la especificación del estándar. El autenticador sólo se encarga de la terminación del intercambio de autenticación a nivel de capa de enlace, y no mantiene ningún tipo de información sobre el usuario. Cualquier petición del dispositivo es pasada al servidor de autenticación, basado en el protocolo RADIUS (*Remote Authentication Dial-In User Server*) [34], para su procesamiento.

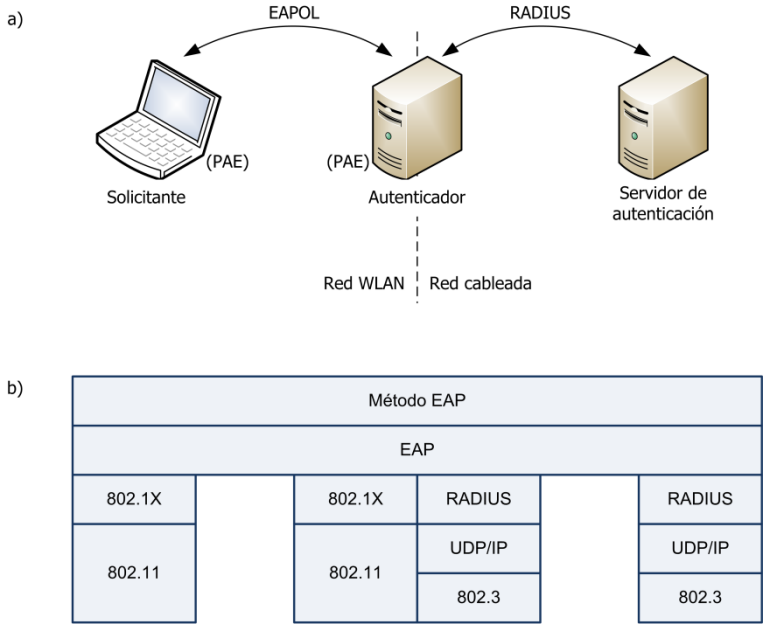

Figura 2-10. Arquitectura IEEE 802.1X. *Fuente:* [13]

Los puertos en un dispositivo con capacidades 802.1X se pueden encontrar en un estado autorizado, en el que el puerto se encuentra habilitado, o en un estado no-autorizado, en el que el puerto se encuentra deshabilitado. Incluso en el estado no-autorizado la especificación permite el tráfico de inicialización, como DHCP.

El intercambio para la autenticación se lleva a cabo de manera lógica entre el solicitante y el servidor de autenticación, mientras que el autenticador sólo actúa como un puente. La

Figura 2-10 (b) muestra la arquitectura lógica de protocolos. Entre el solicitante y el autenticador (lo que se denomina como *"front-end"*) el tráfico viaja mediante el protocolo EAPOL (*EAP Over LAN*, EAP sobre LAN), que está definido por el estándar IEEE 802.1X. Mientras que en el *"back-end"*, el método EAP seleccionado viaja a través del protocolo RADIUS. Como resultado, se establece un intercambio EAP entre el solicitante y el servidor de autenticación, aunque el puerto se mantenga en estado no-autorizado y el solicitante ni siquiera tenga una dirección IP.

Una de las ventajas de utilizar RADIUS es que éste ofrece soporte para una gran cantidad de bases de datos de usuarios. Además de bases de datos locales, un servidor RADIUS puede utilizarse como puerta de enlace (*gateway*) hacia directorios LDAP, esquemas de autenticación de sistemas operativos UNIX, cuantas de usuario de Microsoft Active Directory, o incluso otros servidores RADIUS.

2.16.4. IEEE 802.1X en redes WLAN

IEEE 802.1X provee un *framework* de autenticación de usuarios sobre cualquier tipo de redes LAN, incluyendo redes 802.11. Un puerto 802.1X en una red WLAN puede definirse como una asociación entre una estación y un punto de acceso. Una vez que una estación se ha asociado exitosamente a un punto de acceso. Puede empezar el intercambio 802.1X para intentar ser autorizada a ingresar a la red. el estado del intercambio de autenticación puede ser reportado al usuario a medida que se "levanta" la interfaz inalámbrica.

La Figura 2-11 muestra un ejemplo de autenticación 802.1X, que consta de los siguientes pasos:

1. El solicitante se asocia con el punto de acceso WLAN, mediante el procedimiento definido en el estándar IEEE 802.11.

2. El solicitante inicia el intercambio 802.1X con un mensaje de inicio EAPOL.

3. El autenticador (punto de acceso) emite un mensaje EAP Solicitud/Identidad. Este mensaje puede ser enviado sin que exista previamente un mensaje de inicio por parte de la estación.

4. El solicitante responde con un mensaje EAP Respuesta/Identidad, que pasado al servidor de autenticación como un mensaje de petición de acceso RADIUS.

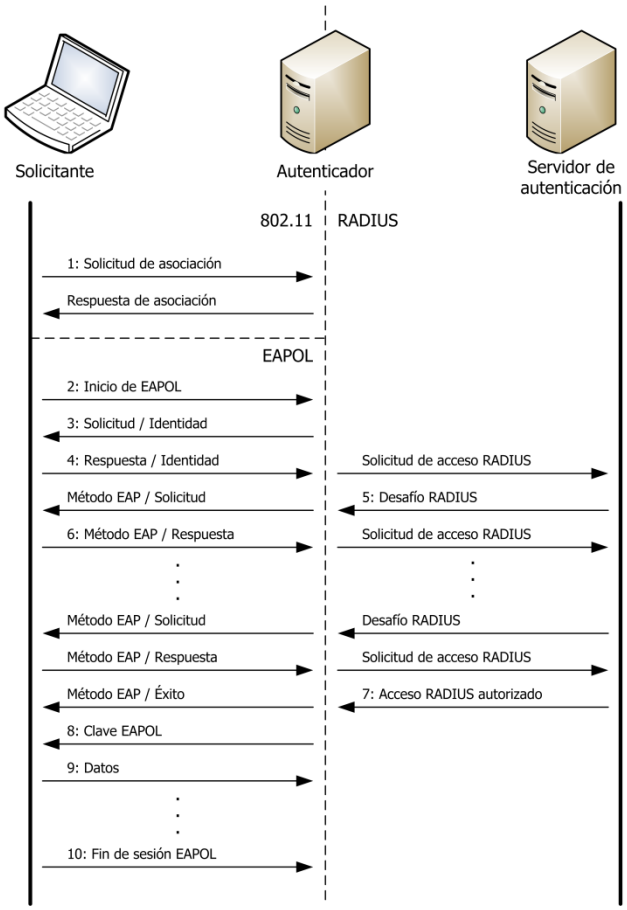

Figura 2-11. Ejemplo de intercambio 802.1X en una WLAN 802.11. *Fuente:* [13]

5. El servidor RADIUS determina el tipo de autenticación requerida, y envía un mensaje de solicitud EAP según el método seleccionado. La solicitud EAP es encapsulada en un mensaje de desafío RADIUS. Cuando esta solicitud alcanza el punto de acceso, este des-encapsula el mensaje y lo envía al solicitante.

6. El solicitante envía una respuesta a la solicitud EAP. Esta respuesta es traducida por el autenticadoren un mensaje de petición de acceso RADIUS, con la correspondiente respuesta al desafío.

Los pasos 5 y 6 se repiten tantas veces como sea necesario para completar el proceso de autenticación. Algunos métodos EAP requieren entre 10 y 20 rondas de intercambio de solicitudes y respuestas para completar el proceso de autenticación.

7. El servidor RADIUS comunica la autorización de acceso con un mensaje de aceptación de acceso de RADIUS. El autenticador envía por su parte un mensaje de éxito del protocolo EAP.

8. Inmediatamente a la recepción del mensaje de autenticación, el punto de acceso distribuye las claves al solicitante mediante mensajes apropiados del protocolo EAPOL.

9. Una vez que las claves se encuentran en el solicitante, se puede iniciar el intercambio de tráfico de datos. Es probable que este punto se realice una solicitud DHCP para que la estación pueda obtener una dirección IP.

10. Cuando el solicitante ya no requiere acceso a la red, puede enviar un mensaje de fin de sesión, para colocar el puerto 802.1X nuevamente en un estado no-autorizado.

Un intercambio como el del ejemplo anterior puede darse en cualquier momento. No es necesario que la estación inicie el intercambio. En cualquier punto, el autenticador puede comenzar un intercambio EAPOL emitiendo un mensaje de Solicitud/Identidad para refrescar los datos de autenticación. De hecho, es común que el servidor RADIUS dispare procesos de re-autenticación como respuesta al vencimiento de un temporizador de sesión, con el objeto de refrescar las claves maestras de cifrado.

2.17. Redes de seguridad robusta

Una red de seguridad robusta (RSN, *Robust Security Netowork*) define un conjunto de características de seguridad adicionales a WEP y la autenticación IEEE 802.11 original. Estas características incluyen:

- Mecanismos mejorados de autenticación para las estaciones.

- Algoritmos de administración de claves.

- Establecimiento de claves criptográficas.

- Un mecanismo de encapsulación criptográfica de datos, denominado Modo de Conteo con Protocolo CBC-MAC (CCMP, *Counter mode with Cipher-Block Chaining Message Authentication Code Protocol*), y, opcionalmente el Protocolo de Integridad de Clave Temporal (TKIP, *Temporal Key Integrity Protocol*).

Los servicios de seguridad en el estándar IEEE 802.11 son provistos por el servicio de autenticación y por los mecanismos TKIP y CCMP [20]. El alcance de los servicios de seguridad está limitado al intercambio de datos de estación a estación. El servicio de confidencialidad de datos ofrecido por TKIP y CCMP en una implementación de IEEE 802.11 es la protección del MSDU. Para propósitos del estándar, TKIP y CCMP son vistos como servicios lógicos que se localizan dentro de la subcapa MAC. Las implementaciones de los servicios TKIP y CCMP es transparente para la subcapa LLC y otras capas superiores.

Un RSN se basa en varios componentes externos a la arquitectura de IEEE 802.11. El primer componente es una Entidad de Acceso de Puerto (PAE, *Port Access Entity*) de IEEE 802.1X. PAE está presente en todas las estaciones de una RSNA, y controla el envío de datos desde y hacia la subcapa MAC. Un punto de acceso siempre implementa los roles de PAE autenticador (*Authenticator PAE*) y autenticador EAP (*EAP Authenticator*). Una estación que no sea punto de acceso siempre implementa los roles de PAE suplicante (*Suplicant PAE*) y par EAP (*EAP peer*). En un IBSS (red ad hoc) una estación siempre implementa los cuatro roles anteriores.

Un segundo componente es el servidor de autenticación (AS, *Authentication Server*). El AS puede autenticar a los elementos de la RSNA, es decir, las estaciones. El punto de acceso puede proveer el material que se requiere para que los elementos de la RSNA se autentiquen entre ellos. El AS se comunica con el suplicante 802.1X en cada estación a través del autenticador 802.1X. Esto permite que la estación pueda autenticarse con el AS y viceversa. Una RSNA depende del uso de un método EAP que soporte autenticación mutua del AS y de la estación, como aquellos que cumplen los requerimientos del RFC 4017. En ciertas aplicaciones, el AS puede estar integrado dentro del mismo dispositivo físico que el punto de acceso.

2.18. Certificaciones WPA y WPA2

Los primeros productos que implementaban tecnologías WLAN experimentaban problemas de compatibilidad. Tras la aprobación de la primera iteración del estándar IEEE 802.11, en

1997, no existía ningún ente que se encargara de validar la adhesión de estos productos con el estándar.

En 1999, un grupo de empresas entre las que se encontraban 3Com, Aironet (ahora parte de Cisco), Harris Semiconductor, Lucent Technologies, Nokia y Symbol Technologies (ahora parte de Motorola) establecieron la *Wireless Ethernet Compatibility Alliance* (WECA, Alianza para la Compatibilidad de Ethernet Inalámbrico). En 2003 la organización pasó a denominarse Wi-Fi Alliance [40], y actualmente está conformada por cerca de 300 empresas involucradas con el desarrollo de productos relacionados con redes inalámbricas.

Como organización independiente, Wi-Fi Alliance tiene el propósito de probar y certificar la interoperabilidad de productos, establecer regulaciones y promover la adopción de la tecnología Wi-Fi, que es la denominación comercial de redes WLAN que cumplen con el estándar IEEE 802.11.

Wi-Fi Alliance es dueña de varias marcas comerciales entre las que se incluyen "Wi-Fi", "Wi-Fi Alliance", "Wi-Fi CERTIFIED", "Wi-Fi Protected Access (WPA)", el logotipo de Wi-Fi y el logotipo de la certificación Wi-Fi. Esto permite a la organización garantizar, inclusive a nivel legal, que cualquier producto certificado, y por lo tanto autorizado a hacer uso de estas marcas, ha cumplido con las pruebas realizadas por la organización, y por lo tanto es capaz de interoperar correctamente con dispositivos de otros fabricantes.

En 2003, la Wi-Fi Alliance introdujo WPA (*Wi-Fi Protected Access*, acceso Wi-Fi protegido), que incluía un subconjunto de características de la, para entonces en desarrollo, revisión IEEE 802.11i [21], que luego fue completamente incorporada en el estándar IEEE 802.11-2007. WPA utiliza TKIP para el cifrado de los datos, mientras que la autenticación es implementada con IEEE 802.1X y EAP para usuarios empresariales, y una clave pre-compartida (PSK, *pre-shared key*) para uso doméstico.

Concurrentemente con la ratificación de IEEE 802.11i en 2004, la Wi-Fi Alliance introdujo WPA2, que inicialmente era una certificación opcional, pero en 2006 se volvió obligatoria. Construido sobre los fundamentos de WPA, WPA2 incluye cifrado más fuerte con la adopción del protocolo CCMP y el algoritmo de cifrado de bloques AES.

Con WPA2, la tecnología de redes WLAN ha alcanzado un nivel de madurez que permite llevar hasta los usuarios el estado del arte de la seguridad para este tipo de esquemas de comunicación, mediante el uso de cualquier dispositivo de cualquier fabricante, que cumpla con las pruebas y certificaciones de la Wi-Fi Alliance [42].

El soporte a múltiples tipos de protocolo EAP permite que se pueda seleccionar la tecnología de autenticación más apropiada para el ambiente en el que operará la WLAN. A nivel de la red, debe habilitarse soporte para uno o más tipos de EAP en el punto de acceso y el servidor AAA (*Authentication, Authorization and Accounting*, Autenticación, Autorización y Contabilización). Tanto el dispositivo cliente como la red (punto de acceso y servidor AAA) deben soportar el mismo método EAP para poder completar el proceso de autenticación. La selección del método EAP depende del tipo de dispositivos cliente a soportar, de las aplicaciones hospedadas en la red, de los sistemas operativos de la plataforma y de requerimientos específicos de seguridad (como el uso de contraseñas, *tokens*, certificados digitales, claves pre-compartidas o cualquier combinación de éstos).

IEEE 802.11i y WPA2 obligan al uso de CCMP, un protocolo de cifrado en el que las mismas claves son utilizadas tanto para el cifrado de la data como para la comprobación de su integridad. CCMP usa internamente AES, que es un algoritmo de cifrado de bloque que opera con múltiples longitudes de clave y tamaños de bloques. En el caso de IEEE 802.11i y WPA2 se utilizan tanto claves de cifrado como bloques de 128 bits. Las claves de cifrado AES son derivadas del PTK (*Pairwise Transient Key*) usando el *handshake* de 4 vías definido en el protocolo de manejo de claves de IEEE 802.11i.

La inclusión de AES dentro de WPA2, ofrece a las redes WLAN uno de los estándares de cifrado más ampliamente probado y usado en la actualidad. Hoy en día, AES es utilizado dentro de múltiples tecnologías de transporte de datos y ha sido sometido a rigurosos escrutinios por parte de especialistas en criptografía [42].

En resumen, como ventajas de utilizar el esquema de seguridad WPA2 para la protección de redes WLAN IEEE 802.11 se tienen:

- ***Autenticación mutua.*** WPA2 utiliza IEEE 802.1X (esquema *Enterprise*) y PSK (esquema *Personal*) para proveer autenticación mutua. Esto requiere que el cliente verifique las credenciales del dispositivo contra el que se está autenticando, antes de enviar sus propias credenciales de autenticación y establecer conectividad completa. La idea detrás de esto es prevenir que el usuario se conecte a puntos de acceso no autorizados.

- ***Cifrado fuerte.*** AES está definido como un estándar del gobierno federal de los Estados Unidos. El soporte a AES es requerido por muchos protocolos y aplicaciones de uso común en redes empresariales. Hasta la fecha, AES ha probado ser extremadamente resistente a un gran número de ataques. La data que viaja a través

de una WLAN con WPA2 habilitado está cifrada con el algoritmo CCMP que internamente hace uso de AES.

- ***Interoperatividad.*** WPA2 es una solución basada netamente en estándares. WPA2 puede ser habilitado para proteger el tráfico de datos entre clientes y puntos de acceso, independiente de la marca de los dispositivos. Esto expande en gran medida la disponibilidad de WPA2 y ofrece confianza a los usuarios de que la data que fluye en la WLAN está protegida.

Capítulo 3

Diseño de la red WLAN

En este capítulo se presentan los requerimientos para la red WLAN de C.G.S.I., C.A.; tanto los establecidos explícitamente por la empresa, como aquellos que son inherentes a una red que implementa el esquema de seguridad WPA2-Enterprise. A partir de allí se especifica el diseño de la WLAN a nivel de arquitecturas de conectividad y seguridad, detallando los diferentes componentes necesarios para su implementación.

3.1. Requerimientos para la WLAN

Antes de iniciar el diseño de la red WLAN, deben conocerse todos los requerimientos con los que ésta debe cumplir. Algunos de ellos han sido especificados de manera explícita por la empresa, mientras que otros nacen de las mejores prácticas usadas para la implementación de redes WLAN seguras.

3.1.1. Perfil tecnológico de la organización

La plataforma de tecnologías de información C.G.S.I., C.A. está compuesta por servidores de producción y laboratorio, una red LAN basada en *switches*, y enlaces de acceso a Internet. Todos los equipos pertenecen a una única subred IP, con direccionamiento 192.168.100.0/24 (clase C).

Previo al desarrollo de este Trabajo Especial de Grado, se contaba además con una implementación de red inalámbrica basada en un único dispositivo de punto de acceso orientado a redes hogareñas. Esta red inalámbrica implementaba WEP como esquema de cifrado, mientras que para la autenticación y control de acceso se utilizaba una clave pre-compartida (PSK) y filtrado por dirección MAC.

La Figura 3-1 muestra un diagrama lógico de la red corporativa antes de la implementación de la nueva red WLAN basada en el esquema de seguridad WPA2-Enterprise.

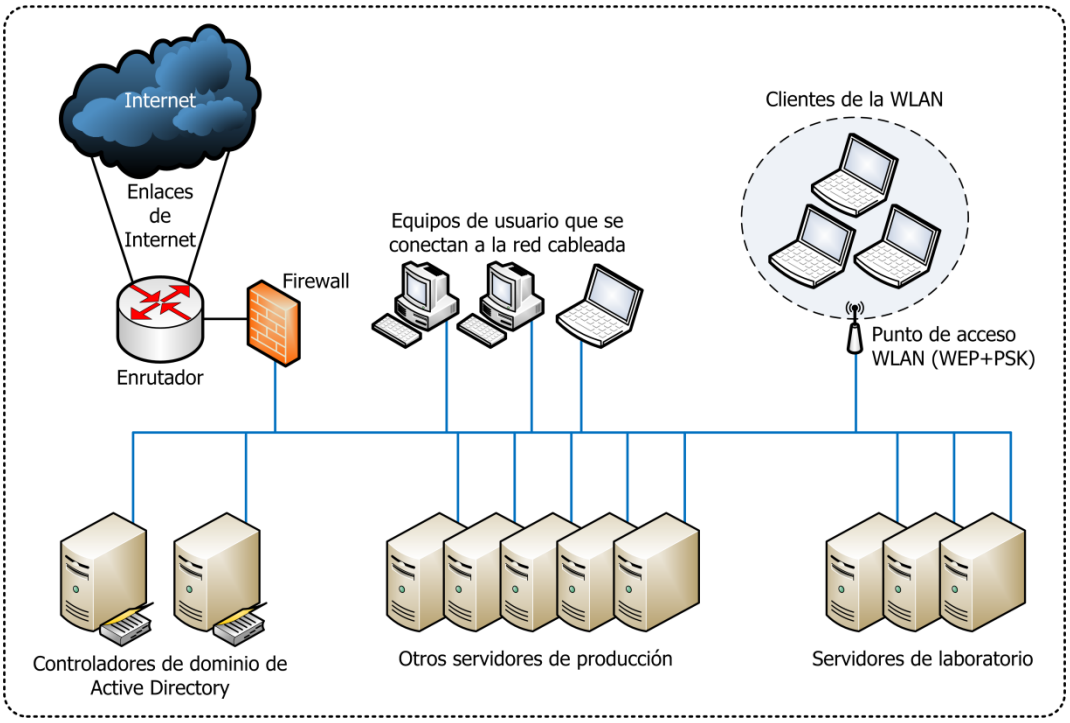

Figura 3-1. Diagrama lógico de la red de C.G.S.I., C.A. previo a la implementación de la nueva WLAN

Existe en la red corporativa una implementación del servicio Microsoft Active Directory consistente de un único dominio, denominado *cgsi.corp*, con dos controladores de dominio, *apolo.cgsi.corp* y *poseidon.cgsi.corp*, ejecutando Microsoft Windows Server 2003 Standard Edition. Esta implementación provee servicios de directorio, acceso a recursos compartidos en la red y autenticación a aplicaciones como el servidor de correo electrónico corporativo Microsoft Exchange 2003. En los controladores de dominio se ejecutan adicionalmente otros servicios como DNS (*Domain Name System*) y DHCP (*Dynamic Host Configuration Protocol*).

Los equipos de usuario están compuestos por computadoras de escritorio, en el caso del personal administrativo, y computadoras portátiles (*laptops*) en caso del personal técnico, de ventas, gerencial y directivo. Estos equipos ejecutan en su mayoría Windows XP Professional como sistema operativo, salvo algunos nuevos equipos que ejecutan Windows Vista Business. De las 45 personas que hacen uso de la red corporativa, unas 20 acceden a la misma, de forma eventual o exclusiva, a través de la red WLAN.

El espacio físico que aloja a la empresa ocupa tres oficinas ubicadas en el mismo piso de un edificio de oficinas. En conjunto, estas tres oficinas ocupan un área aproximada de 525 metros cuadrados. No existen sucursales u oficinas regionales a las que se deba prestar servicio a través de la red corporativa.

3.1.2. Requerimientos establecidos por C.G.S.I., C.A.

En reuniones previas, establecidas con personal tanto gerencial como de administración de la plataforma informática de C.G.S.I., C.A., surgieron una serie de requerimientos que son de obligatorio cumplimento para la red inalámbrica a implementar. A saber:

- Como esquema de seguridad de la red WLAN deberá implementarse WPA2-Enterprise. Este requerimiento se justifica en el hecho de que WPA2-Enterprise es el esquema de seguridad, basado en las especificaciones de red de seguridad robusta (RSN) del estándar IEEE 802.11-2007, que al día de hoy provee mayores niveles de protección.

- Se deberán utilizar, en tanto sea posible, los elementos existentes en la plataforma informática de la empresa. Esto incluye la plataforma Microsoft Active Directory desplegada, así como la infraestructura de red cableada, según sea necesaria. Este requerimiento busca aprovechar la capacidad instalada de hardware y software de los servidores y dispositivos de red previamente implementados en la empresa. Esto trae como consecuencia, además, el ahorro de costos en la adquisición de nuevos elementos para la plataforma.

- Sólo se brindará conectividad a equipos *laptop* bajo plataforma Microsoft Windows. Se excluyen PDA, teléfonos celulares con capacidades Wi-Fi, y cualquier otro tipo de dispositivos y plataformas. Hasta el momento, el universo de dispositivos cliente de la red inalámbrica está basado únicamente en computadoras portátiles que ejecutan en su mayoría el sistema operativo Windows XP Professional, y en el caso de algunos

equipos nuevos, Windows Vista Business. Para la nueva implementación de red WLAN se espera mantener el mismo tipo de dispositivo cliente.

- El acceso a la red inalámbrica estará supeditado a un conjunto de usuarios específicos. No todos los usuarios de la red corporativa de C.G.S.I, C.A. requieren acceso a la WLAN. El diseño de la red inalámbrica debe contemplar la necesidad de restringir el acceso a usuarios determinados.

- Los elementos de infraestructura de la red WLAN que se usarán serán del fabricante Aruba Networks, y están conformados por un Aruba Controller MC-800, tres puntos de acceso AP-61 y un punto de acceso AP-70. Las características de estos dispositivos son descritas más adelante en este capítulo. La decisión de utilizar dispositivos específicamente de Aruba Networks viene dada, en principio, por el hecho de que C.G.S.I, C.A. es aliado comercial (*partner*) para la distribución en Venezuela de los productos de este fabricante. Sin embargo, es importante destacar que Aruba Networks es una empresa especializada en la producción de equipamiento para redes WLAN de grado industrial, con énfasis en la seguridad.

- Las especificaciones de capa física soportadas en la WLAN serán las definidas en las revisiones 802.11b y 802.11g. Todos los dispositivos cliente que harán uso de la red inalámbrica soportan estos dos tipos de capa física. Aún no se cuenta en la empresa con dispositivos que cumplan con la recientemente ratificada revisión 802.11n y los modelos de punto de acceso que se desplegarán, tampoco ofrecen soporte para esta especificación.

- La solución a implementar debe ser robusta y proveer un alto nivel de rendimiento. Se espera que la red WLAN sea "resistente" a la interferencia de otras redes WLAN cercanas. Se espera también que el acceso a la red corporativa para la mayoría de las tareas habituales de los usuarios, como navegación Web, acceso al correo electrónico corporativo, acceso a aplicaciones y archivos en la red, etc., se mantenga con un nivel de rendimiento bastante similar al que se obtiene al conectarse mediante la red cableada.

- La red debe ser escalable en cuanto al número de clientes inalámbricos soportados, expansión de la cobertura, fácil adaptabilidad a nuevas especificaciones de capa física, entre otros elementos.

3.1.3. Criterios de diseño

Partiendo de los requerimientos dispuestos por la empresa, que establecen el uso de la plataforma de servidores Microsoft Windows Server ya desplegada, así como la implementación de infraestructura de conectividad inalámbrica de Aruba Netowrks, se consultó documentación de ambos fabricantes sobre mejores prácticas y modelos de referencia para el diseño e implementación de redes WLAN basadas en sus respectivas tecnologías [5] [6] [29] [30].

La Tabla 3.1 resume algunos de los criterios de diseño que se utilizaron para la solución WLAN implementada en C.G.S.I., C.A. El resto de este capítulo describe los diferentes componentes utilizados para dar cumplimiento a estos criterios y las razones para su escogencia.

Tabla 3-1. Criterios de diseño para la red WLAN

Requerimiento	Criterio de diseño
Requerimientos de seguridad	▪ Autenticación y autorización robusta de los clientes inalámbricos ▪ Control de acceso robusto que permita el acceso a la red únicamente a usuarios y dispositivos autorizados y niegue cualquier intento de acceso no autorizado ▪ Esquema de cifrado fuerte del tráfico inalámbrico ▪ Manejo seguro de las claves de cifrado
Escalabilidad (número máximo de usuarios soportados)	La solución a implementar debe ser escalable desde una decena hasta unos miles usuarios inalámbricos. En todo caso se requiere agregar redundancia de los distintos componentes para dar soporte a una mayor cantidad de usuarios
Escalabilidad (número de localidades soportadas)	En principio, la solución está diseñada para dar soporte a una única localidad, pero puede ser fácilmente adaptada para dar soporte a una gran empresa con múltiples localidades
Requerimientos de disponibilidad	El uso de múltiples puntos de acceso, servidores RADIUS y controladores de dominio brinda un nivel importante de tolerancia a fallos
Soporte de la plataforma	La plataforma de sistemas operativos de los servidores (Windows Server 2003) para la instalación del servicio RADIUS y la autoridad certificadora; así como la plataforma de sistemas operativos de los dispositivos cliente (Windows XP Professional y Windows Vista Business) soportan plenamente las tecnologías que conforman la implementación de la WLAN segura
Extensibilidad (reutilización de los componentes para otras aplicaciones)	Otras aplicaciones de acceso a la red como VPN (*Virtual Private Network*s, Redes Privadas Virtuales) para acceso remoto, acceso 802.1X a la red cableada y autenticación de firewalls, pueden aprovechar los mismos componentes de autenticación de la red WLAN
Requerimientos de la organización	Por una parte, la organización ha establecido una serie de requerimientos propios que deben observarse en el diseño de la red WLAN. Luego, la implementación y posterior gestión y mantenimiento de los distintos componentes de la red WLAN requieren personal con capacitación en las tecnologías utilizadas

Requerimiento	Criterio de diseño
Requerimientos de gestión	La implementación debe requerir un nivel de gestión mínimo para mantener la operatividad. La solución está configurada para la generación de alertas a través del registro de eventos de auditoría (*EventLog*) de los servidores
Cumplimiento con los estándares	La solución diseñada cumple con los siguientes estándares: ▪ IEEE 802.11 (b y g). ▪ IEEE 802.1X para la autenticación, usando PEAP y MS-CHAP v2. ▪ Cifrado de la data con claves dinámicas, utilizando CCMP (AES) como algoritmo de cifrado. ▪ RADIUS (soporte de los RFC 2865 y 2866).

3.2. Arquitectura de conectividad de la WLAN

La infraestructura de conectividad de la red WLAN de C.G.S.I., C.A. está basada en un modelo centralizado conformado por un controlador y algunos puntos de acceso. En esta sección se describen los componentes de esta arquitectura y se establecen algunos lineamientos de diseño que debe seguir la implementación.

3.2.1. Modelo de red WLAN centralizada de Aruba Networks

Las primeras implementaciones de redes WLAN utilizaban puntos de acceso inalámbricos que funcionaban de manera autónoma, como cualquier otro *switch* o enrutador en la red. Estos puntos de acceso eran gestionados y mantenidos de forma independiente. Sin embargo, a medida que las redes WLAN empresariales fueron incrementando su tamaño, pronto se hicieron palpables las limitaciones e inconvenientes de manejar cada punto de acceso de manera separada. Tener que mantener configuraciones consistentes para decenas o cientos de puntos de acceso independientes era una tarea propensa a errores y que consumía mucho tiempo, limitando en gran medida la escalabilidad de la red [13].

En años recientes, diferentes fabricantes de equipamiento WLAN han adoptado una arquitectura de red basada en controladores centralizados que gestionan las funcionalidades de los puntos de acceso. Esto permite ofrecer redes inalámbricas basadas en un modelo estructurado que da soporte a la movilidad de los usuarios, sin sacrificar la seguridad, administración o escalabilidad de la red.

En terminología del fabricante Aruba Networks, este modelo es denominado *user-centric network* (red centrada en el usuario) y consiste básicamente en dos componentes: los

denominados Aruba Controllers y los puntos de acceso delgados (*thin access points*) que trabajan de manera conjunta y coordinada sobre una plataforma de red LAN preexistente [6].

La Figura 3-2 muestra esta arquitectura de operación. Un dispositivo centralizado (el controlador) gestiona, de forma segura y confiable, cientos o miles de radios (puntos de acceso delgados) conectados a la red LAN cableada. En este modelo, la inteligencia que una vez residía en los puntos de acceso autónomos está ahora integrada en el controlador centralizado, diseñado para proveer alto rendimiento en el procesamiento de paquetes 802.11, y gestión de la movilidad y la seguridad. Por lo general, estos controladores son desplegados físicamente en los centros de datos o cuartos de cableado de las organizaciones.

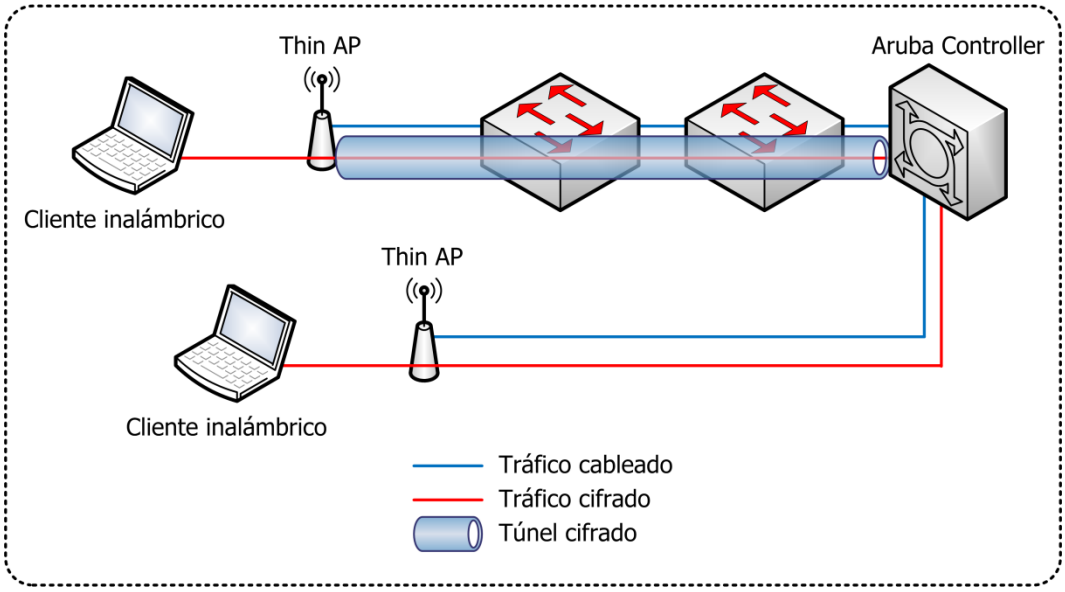

Figura 3-2. Modelo centralizado de WLAN. *Fuente:* [6]

Al trasladar la mayor parte de la inteligencia hacia el controlador, la función de los puntos de acceso se simplifica, y se convierten simplemente en interfaces de radio conectadas a la red cableada que realizan sólo funciones de conectividad de capa física y monitoreo del espectro. De allí el termino punto de acceso delgado (*thin AP*). Estos puntos de acceso se conectan al controlador, bien sea directamente, o mediante túneles cifrados sobre una red capa 3 (red lógica), convirtiéndose de esta manera en puertos de acceso extendidos que dirigen el tráfico inalámbrico hacia el controlador para su procesamiento, a la vez que proveen visibilidad y control sobre el espectro de radiofrecuencias.

Un aspecto importante a considerar es que el controlador se convierte en un punto único de falla que puede comprometer la disponibilidad de la red. Para solventar esta situación, lo ideal es implementar esquemas de alta disponibilidad (HA, *High Availability*) mediante redundancia a nivel de los controladores de la WLAN, de manera que en caso de falla de uno de estos dispositivos, automáticamente el tráfico inalámbrico pueda conmutarse hacia un controlador secundario.

Una de las ventajas que ofrece esta arquitectura centralizada es la posibilidad de establecer múltiples SSID (*Service Set Identifiers*, Identificadores del Conjunto de Servicio) simultáneamente sobre los mismos puntos de acceso. Cada SSID puede manejar sus propios esquemas de autenticación y cifrado, basado en las capacidades de los clientes inalámbricos y en los servicios que cada uno de éstos requiere.

3.2.2. Aruba Controller

El Aruba Controller es el centro de una red WLAN implementada con dispositivos Aruba Networks. Un controlador es un *appliance* que provee la capacidad de gestionar toda la red inalámbrica. Un Aruba Controller ejecuta el software propietario ArubaOS. Éste funge tanto como sistema operativo y como entorno de aplicación de los controladores. Entre sus principales características se incluyen:

- Soporte para múltiples esquemas de autenticación y cifrado.
- Soporte para puntos de acceso virtuales, permitiendo el manejo de múltiples SSID en la red WLAN.
- Protección contra puntos de acceso furtivos (*rogue APs*).
- Re-asociación rápida de los clientes inalámbricos entre distintos puntos de acceso.
- Herramientas de análisis y gestión automatizada del espectro de radiofrecuencia.
- Configuración centralizada de los puntos de acceso.
- Seguimiento de la localización física de puntos de acceso y clientes inalámbricos.
- Sistema inalámbrico de detección y prevención de intrusos (WIDPS, *Wireless Intrussion Detection and Prevention System*).
- *Firewall* para reforzamiento de políticas de seguridad.

- Gestión de voz sobre WLAN (VoWLAN, *Voice over WLAN*) para dispositivos inalámbricos de voz sobre IP (VoIP).

Los controladores proveen capacidades avanzadas para el manejo del espectro de radiofrecuencias en la WLAN de una organización. Estos dispositivos implementan una tecnología denominada *Adaptative Radio Management* (ARM, administración adaptativa del radio) que monitorea constantemente el espectro y ajusta dinámicamente el poder de transmisión y parámetros de los canales de frecuencias. Por otra parte, el tener un dispositivo que maneja de manera centralizada funcionalidades como la asociación y autenticación facilita en gran medida la movilidad, permitiendo que los usuarios se trasladen dentro del ámbito de la organización, haciendo *roaming* de un punto de acceso a otro sin perder conectividad o cambiar de dirección IP.

Estando orientados estos dispositivos hacia el ambiente empresarial, ofrecen un alto nivel de seguridad para la red WLAN. Además de cumplir con las certificaciones WPA y WPA2 de la Wi-Fi Alliance, se ofrecen características como el escaneo continuo del espectro en busca de amenazas para la seguridad de la red, como puntos de acceso furtivos y atacantes potenciales. El *firewall* integrado en el dispositivo permite discriminar a los clientes inalámbricos en diferentes perfiles y establecer políticas sobre el tráfico permitido hacia la red cableada.

En el caso del equipamiento para la nueva red WLAN de C.G.S.I., C.A., se cuenta con un Aruba Controller modelo MC-800. La Figura 3-3 muestra una foto referencial de este dispositivo.

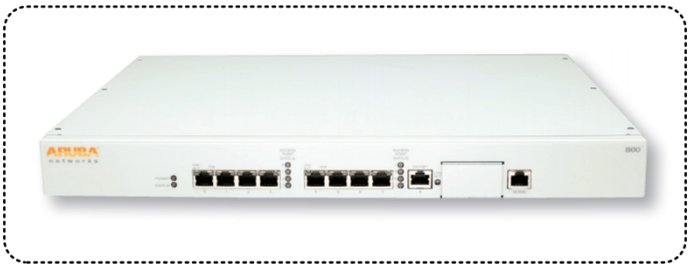

Figura 3-3. Aruba Controller MC-800

Este modelo específico soporta las siguientes funciones:

- 8 puertos Fast Ethernet (10/100 Mbps) con *Power-over-Ethernet* (PoE, Energía sobre Ethernet) y 1 puerto Gigabit Ethernet (10/100/1000 Mbps).

- Gestión de hasta 16 puntos de acceso delgados de Aruba Networks.
- Manejo de hasta 256 clientes inalámbricos conectados concurrentemente a la red.
- Rendimiento concurrente de hasta 200 Mbps cuando está activado el cifrado CCMP-AES.

3.2.3. Puntos de acceso delgados

Los puntos de acceso delgados de Aruba Networks pueden tener múltiples funciones, de acuerdo a su rol en el modelo de red WLAN centralizada. Estos roles incluyen:

- ***Punto de acceso:*** este es, obviamente, el escenario más común. En este rol el punto de acceso es utilizado para brindar conectividad a los clientes de la red inalámbrica. El punto de acceso actúa como la interfaz de radio, mientras que muchas funcionalidades tienen lugar en el Aruba Controller. El tráfico no se procesa directamente en el punto de acceso, sino que es entregado por éste, mediante un túnel cifrado, al controlador, quien se encarga del manejo del tráfico y de funcionalidades como la autenticación y el cifrado de la data.

- ***Air Monitor:*** en la terminología de Aruba Networks, un *Air Monitor* (AM, Monitor del Aire) es un punto de acceso que actúa como un *sniffer* de la red inalámbrica. El Air Monitor se encarga de escanear la red en busca de redes ad hoc no autorizadas, puntos de acceso furtivos (*rogue APs*) y los puntos de acceso de otras organizaciones que puedan causar interferencia. Si se implementa la funcionalidad de sistema inalámbrico de detección/prevención de intrusos (WIDPS), el Air Monitor funciona como sensor del sistema.

- ***Híbrido:*** bajo este rol, un punto de acceso permite la conectividad de los clientes inalámbricos a la vez que actúa como Air Monitor.

Los diferentes modelos de puntos de acceso de este fabricante pueden estar orientados para ambientes de exteriores e interiores, con antenas fijas o externas, con una o dos interfaces de radios y con soporte para las especificaciones de capa física 802.11 a/b/g/n.

Para la nueva WLAN de C.G.S.I., C.A., se cuenta con 3 puntos de acceso delgados de Aruba Networks modelo AP-61 y 1 punto de acceso modelo AP-70. Ambos modelos de puntos de acceso han sido certificados por la Wi-Fi Alliance operando en conjunto con el Aruba

Controller MC-800 (certificaciones N° WFA5261 y WFA5259, respectivamente). La Tabla 3-2 muestra las características más resaltantes de estos dispositivos.

Tabla 3-2. Características de los puntos de acceso Aruba AP-61 y AP-70

Característica	**AP-61**	**AP-70**
Foto referencial		
Aplicaciones	Diseñado para uso en interiores, con capacidad para ser montado en paredes y techos, o ser apoyado en una superficie plana (*desktop mount*)	Diseñado para uso en interiores, con capacidad para ser montado en paredes y techos
Interfaces de radio	1 interfaz de radio con soporte para las especificaciones de capa física a/b/g, en las bandas de frecuencias de 2,4 GHz y 5GHz (sólo puede ser configurado para operar en una banda a la vez)	2 interfaces de radio con soporte para las especificaciones de capa física a/b/g, en las bandas de frecuencias de 2,4 GHz y 5GHz
Interfaces de red cableada	1 interfaz Fast Ethernet (10/100 Mbps) para conexión a la red cableada o directamente al Aruba Controller, con soporte para Power-over-Ethernet (PoE)	2 interfaces Fast Ethernet (10/100 Mbps) para conexión a la red cableada o directamente al Aruba Controller, con soporte para Power-over-Ethernet (PoE)
Antena	Omnidireccional integrada con ganancia de 2,8 dBi en la banda de 2,4 GHz y 4,0 dBi en la banda de 5 GHz	Omnidireccional integrada con ganancia de 4,5 dBi en la banda de 2,4 GHz y 7,2 dBi en la banda de 5 GHz. Cuenta además con 4 interfaces RP-SMA para la conexión de antenas externas (2 por cada interfaz de radio)
Poder máximo de Transmisión (TX)	+20 dBm	+20 dBm
Sensibilidad máxima de recepción (RX)	-95 dBm	-92 dBm

3.2.4. Planificación de la ubicación física de los puntos de acceso

La Figura 3-4 muestra el plano de la planta física de las instalaciones de C.G.S.I., C.A. Actualmente, la empresa ocupa tres oficinas ubicadas en un mismo piso de un edificio comercial. En conjunto estas tres oficinas ocupan un área aproximada de 525 metros

cuadrados. Dos de las oficinas se encuentran contiguas, y tras trabajos de remodelación, quedaron unidas. Un pasillo común del edificio comunica estas dos oficinas con la oficina restante. A efectos de evitar cortes de comunicación si un usuario se desplaza entre las oficinas, también se desea ofrecer cobertura a este pasillo. En esta misma figura se delimitan, además, las zonas en las que no se requiere el despliegue de la red WLAN, bien sea porque pertenecen a la oficina de otra empresa o porque en estas áreas se encuentran los ascensores y escaleras emergencia del edificio.

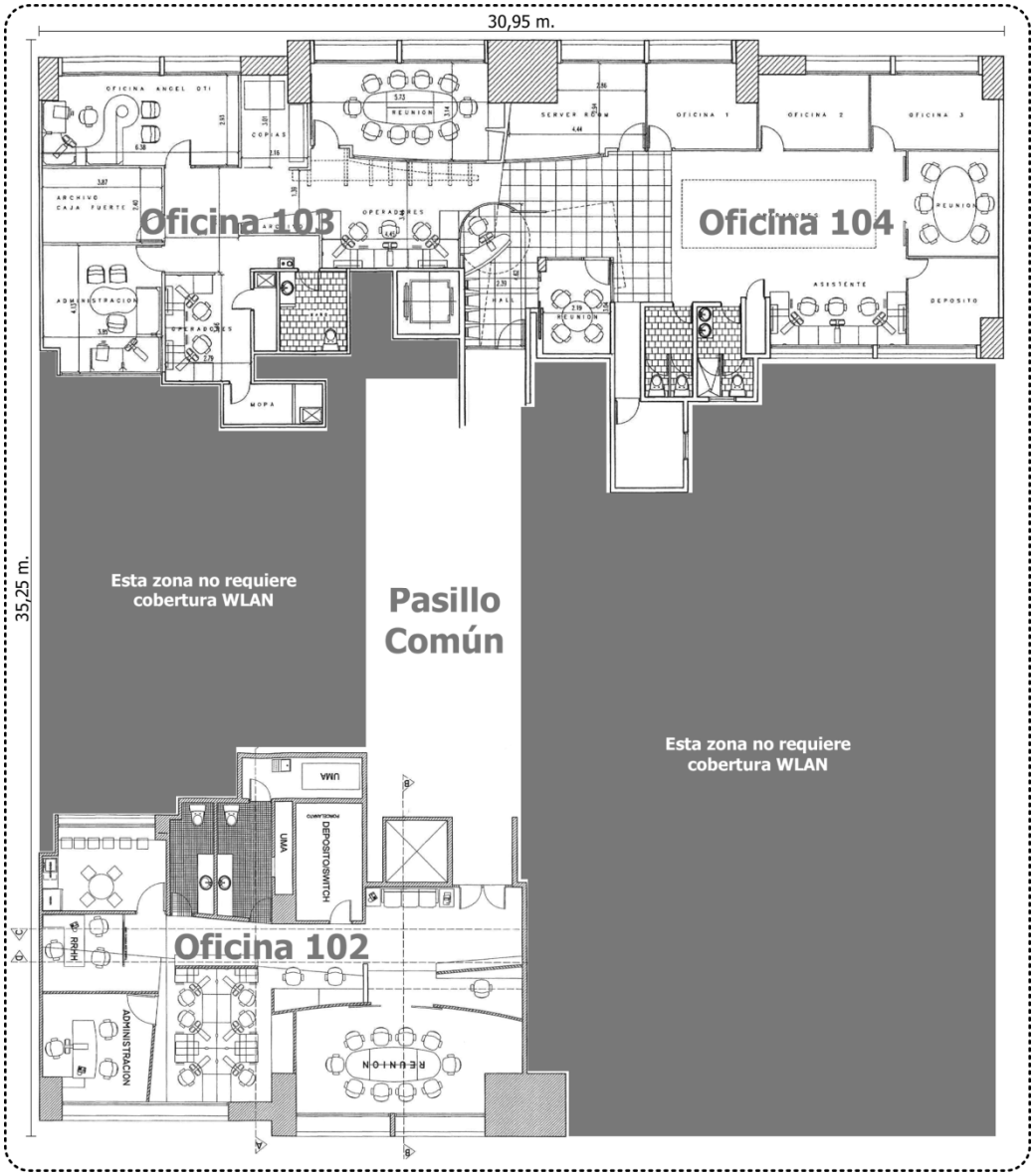

Figura 3-4. Plano de las instalaciones físicas de C.G.S.I., C.A.

Aruba Networks produce una aplicación denominada RF Plan, que facilita la planificación de la colocación de los puntos de acceso en el espacio físico de una organización. La aplicación permite cargar planos de los sitios que requieren despliegue de puntos de acceso. A partir de allí es posible dejar que la aplicación sugiera el número y modelos de puntos de acceso recomendados, tras seleccionar si se requiere ofrecer el mejor rendimiento posible o la mayor cobertura posible por cada punto de acceso.

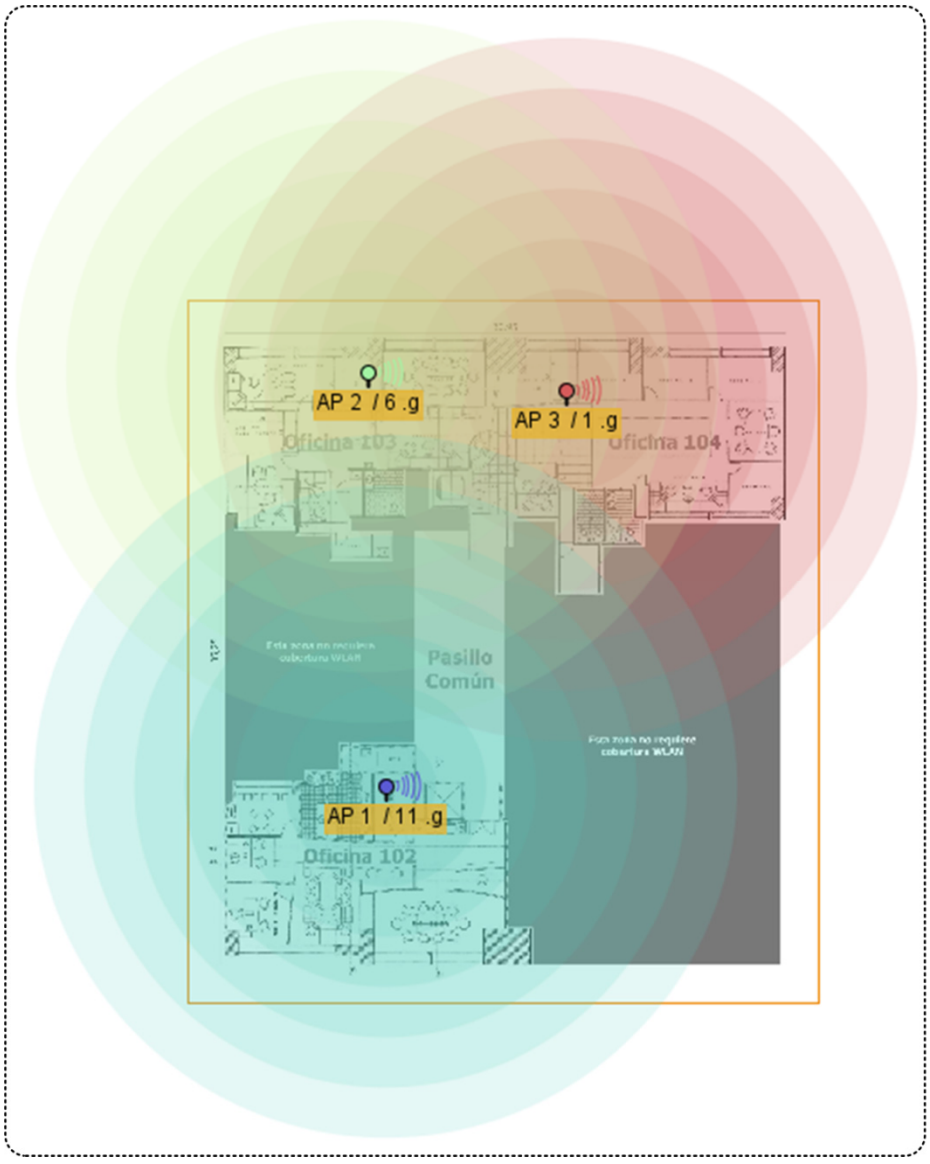

Figura 3-5. Cobertura teórica del diseño de la red WLAN

Otra posibilidad es introducir manualmente la cantidad y modelos de punto de acceso con los que se cuenta, así como las zonas donde no se requiere cobertura de la red, y permitir que la aplicación sugiera la ubicación de los puntos de acceso. Éste último fue el método seguido para la WLAN de C.G.S.I., C.A., porque ya se tenían de antemano los puntos de acceso que se iban a desplegar. La aplicación sugiere también el canal de frecuencias y el nivel de potencia de transmisión en los que debería operar cada punto de acceso. Finalmente es posible mover en la aplicación la ubicación de los puntos de acceso hacia aquellos lugares que por sus características faciliten su instalación física. La Figura 3-5 muestra la salida final de la aplicación RF Plan, que resulta en la cobertura teórica de la red WLAN.

3.2.5. Lineamientos de diseño establecidos para la arquitectura de conectividad de la WLAN

- Aunque la infraestructura de red de Aruba Networks soporta la implementación de múltiples SSIDs, en el caso de la red WLAN de C.G.S.I., C.A. se desplegará un único SSID denominado *CORP_WLAN*.

- El Aruba Controller MC-800 funcionará como ente centralizador de la red WLAN. El controlador provee los servicios definidos para el sistema de distribución en la capa MAC IEEE 802.11. Este dispositivo ejecuta, además, el rol de Autenticador para el esquema 802.1X y proporciona el cifrado CCMP-AES para la infraestructura de la WLAN. El controlador será instalado físicamente en el cuarto de servidores de la empresa.

- Los tres puntos de acceso AP-61 serán utilizados para la conectividad de los clientes inalámbricos a la WLAN. Se utilizará uno de estos dispositivos para dar cobertura a cada una de las tres oficinas ocupadas por C.G.S.I., C.A. La operación de las interfaces de radio se configurará para dar soporte a las especificaciones de capa física 802.11 b y g.

- Los puntos de acceso serán instalados físicamente en posiciones tan cercanas como sea posible a las sugeridas por la herramienta RF Plan. Estos dispositivos serán fijados al techo de las oficinas, por encima del cielo raso, de manera que no estarán a la vista de los usuarios.

- El manejo de canales de frecuencias, poder de transmisión y otros elementos de administración del espectro radioeléctrico de la red WLAN serán gestionados de manera dinámica y automatizada por la funcionalidad ARM (*Adaptative Radio Management*) implementada en el Aruba Controller.

- Aruba Networks recomienda el uso de Air Monitors dedicados como una mejor práctica de seguridad, dado que proveen una mejor vigilancia del espectro de radio frecuencias. En este caso se dedicará a la labor de Air Monitor el punto de acceso AP-70, que es el que provee mayor rango de cobertura, de manera que con este solo punto de acceso se puede abarcar el espacio físico completo de C.G.S.I., C.A. Adicionalmente, se hará uso de la funcionalidad de sistema inalámbrico de detección/prevención de intrusos (WIDPS)

- Los clientes inalámbricos, una vez asociados y autenticados exitosamente en la WLAN, pertenecerán a la misma subred IP que el resto de la red corporativa: 192.168.100.0/24.

3.3. Arquitectura de seguridad de la WLAN

La implementación de una red WLAN basada en WPA2-Enterprise requiere el despliegue de algunos componentes adicionales a los de la infraestructura de conectividad. Los elementos de la arquitectura de seguridad se implementan, básicamente, para dar soporte al esquema de autenticación 802.1X.

El componente central de la arquitectura de seguridad es el servidor de autenticación, que según lo establecido en el estándar IEEE 802.1X, debe ser un servidor RADIUS. Este servidor se apoya en tres componentes adicionales: una autoridad certificadora que genera el certificado digital con el que el propio servidor RADIUS demuestra su identidad ante los clientes que desean autenticarse, un método EAP que transporta el tráfico de autenticación, y una base de datos de autenticación usada como criterio para decidir si se autoriza, o no, el acceso a la red WLAN.

Dado que uno de los requisitos establecidos por la empresa dictamina que deben utilizarse en lo posible los elementos preexistentes en su plataforma de red, y en vista de que esta plataforma está compuesta por servidores con sistema operativo Microsoft Windows Server, se ha elegido implementar aquellos componentes que forman parte del esquema de

autenticación, y que Microsoft distribuye como parte del sistema operativo. Esto permite, entre otras cosas, aprovechar los recursos disponibles, se garantiza la completa compatibilidad de los componentes por ser productos del mismo fabricante y se ahorra en costos de adquisición de nuevo software, y quizás hardware, para la ejecución de estos componentes.

Los componentes de autenticación específicos que se utilizarán para la red WLAN de C.G.S.I., C.A., son desplegados como servicios del sistema operativo Windows Server, y en este caso incluyen:

- ***Internet Authentication Services (IAS):*** es la implementación de Microsoft de un servidor RADIUS. Por una parte cumple con el protocolo estándar definido en los RFC 2865 [34] y 2866 [33], a la vez que se integra de manera, prácticamente, transparente con el resto de la plataforma de servicios del mismo fabricante.

- ***Certificate Services:*** el sistema operativo Windows Server incluye este componente como servicio de autoridad emisora de certificados digitales. Como ventaja de su plena integración con la plataforma Active Directory, está el hecho de que los certificados digitales pueden ser emitidos y distribuidos de manera automatizada a los equipos del dominio que los requieran.

- ***Active Directory:*** como implementación de servicio de directorio, Active Directory contiene una base de datos jerárquica de usuarios, dispositivos y grupos, que permite establecer roles y permisología en una red bajo plataforma Microsoft. Esta misma base de datos puede ser utilizada por el servicio IAS para permitir o denegar el acceso a la red inalámbrica.

3.3.1. Internet Authentication Services (IAS):

Existe un conjunto de criterios que deben considerarse para la implementación del servicio IAS. Estos criterios permiten ofrecer un servicio de autenticación eficiente, robusto, y resistente a fallos, en la medida de lo posible.

- ***Co-ubicación del servicio IAS con los controladores de dominio:*** en esta solución, el servicio IAS se instala en los controladores de dominio existentes, *apolo.cgsi.corp* y *poseidon.cgsi.corp*. De esta forma, los costos de implementación se mantienen bajos y, como efecto secundario, se consigue una ligera mejora del rendimiento debido a

que el servicio IAS puede comunicarse con Active Directory en el mismo equipo, sin que tenga lugar retraso alguno en la red.

- ***Asignación de clientes RADIUS a los servidores IAS:*** en el caso de la red WLAN de C.G.S.I., C.A., el único cliente del servicio IAS planificado hasta el momento es el Aruba Controller MC-800. Dado que el servicio IAS se está instalando en ambos controladores de dominio, se configurará en el controlador el servidor *apolo.cgsi.corp* como servidor RADIUS primario, y *poseion.cgsi.corp* como servidor secundario, en caso de que no pueda ponerse en contacto con el primario o éste no funcione. Esto es fundamental para ofrecer robustez y resistencia a fallos en el servicio de autenticación.

- ***Configuración del servidor IAS:*** para la comunicación en la red, el servidor IAS escucha por los puertos estándar asignados a RADIUS, que son UDP 1812 y 1813 para la autenticación y la contabilidad respectivamente.

- ***Directiva de acceso remoto:*** las directivas de servidor IAS controlan la autenticación y la autorización de las cuentas en la red. Este tipo de directiva contiene un grupo de condiciones de filtro que determinan si la directiva es apropiada para una solicitud de conexión concreta. Algunos ejemplos de condiciones de filtro son: especificación del grupo de seguridad de Windows al que un cliente debe pertenecer; especificación del tipo de conexión (inalámbrica, VPN, etc.) del cliente que realiza la solicitud, y especificación del momento del día en que el cliente intenta conectarse. Cada directiva de acceso remoto posee una acción de directiva, que se establece en permitir o denegar una solicitud de conexión. Las solicitudes de conexión que coincidan con el filtro de condición de la directiva de acceso remoto obtendrán permiso de acceso o no en función de la configuración de esta acción de directiva.

  Asimismo, una directiva de acceso remoto contiene una serie de parámetros que se aplican a una conexión permitida, conocidos como perfil de directiva de acceso remoto. Estos parámetros incluyen los métodos de autenticación que se consideran aceptables para esta conexión, el modo en que una dirección IP se asigna al cliente y la cantidad de tiempo durante la que el cliente puede permanecer conectado antes de que la re-autenticación sea necesaria. Pueden existir muchas directivas de acceso remoto en un servidor IAS. Así, cada solicitud de conexión se evalúa en relación con éstas (por orden de prioridad), hasta que una directiva coincidente permita o deniegue la solicitud. La directiva de acceso remoto para la red WLAN se configurará tal y como se muestra en la Tabla 3-3.

Tabla 3-3. Parámetros de configuración de la directiva de acceso remoto

Parámetro	Configuración
Nombre de la directiva	Permitir acceso a la red WLAN corporativa
Tipo de directiva	Permitir (*allow*)
Condiciones de la directiva de acceso remoto	
Coincidencias de tipo de puerto NAS	IEEE 802.11 inalámbrico Otros dispositivos inalámbricos
Coincidencias del grupo de Windows	Acceso WLAN
Perfil de la directiva de acceso remoto	
Restricciones de marcado: tiempo de espera del cliente	60 minutos
Asignación de dirección IP	La configuración del servidor determina la asignación de la dirección IP
Filtrado IP	Ninguno
Autenticación	Todo deshabilitado aparte de EAP
Autenticación: tipo de EAP empleado	EAP protegido (PEAP)
Autenticación: tipo de PEAP empleado	EAP MS-CHAP v2
Autenticación: reconexión rápida	Habilitado
Atributos RADIUS	Ignorar propiedades de acceso telefónico del usuario = "True" Acción de terminación = "RADIUS-Request"

- ***Registro de eventos RADIUS:*** se configurarán los servidores IAS para registrar sucesos de autenticación aceptados y rechazados. Los sucesos de autenticación generados a partir de dispositivos y usuarios de la WLAN se pueden escribir en el registro de sucesos del sistema del servidor donde se encuentra instalado IAS. La información que el registro de sucesos de autenticación contiene es útil con fines de alerta y auditoría de seguridad, así como para la solución de problemas de autenticación.

- ***Seguridad del servicio IAS:*** las precauciones de seguridad para el servicio IAS deben ser las mismas que se usan para los servidores controladores de dominio. Un control seguro de la red depende de la seguridad de la infraestructura de IAS. Para mejorar la seguridad del servicio IAS, deben implementarse una serie de medidas:

  - Utilizar contraseñas seguras para los clientes RADIUS (Aruba Controller).

- Habilitar el autenticador de mensajes de RADIUS en todos los clientes RADIUS a fin de evitar la suplantación de direcciones IP.

- Aplicar las actualizaciones y parches de seguridad más recientes en el servidor y, asimismo, que se obtienen revisiones actualizadas de forma periódica.

- Usar configuraciones seguras para las cuentas de usuarios dominio con las que se inicia sesión en el servidor IAS. En concreto, se deben utilizan contraseñas seguras y cambiarlas con regularidad.

3.3.2. Selección del método EAP (PEAP + MS-CHAPv2)

Diversa bibliografía consultada, tanto de Microsoft [31] como independiente [13], coincide en que para implementaciones de autenticación 802.1X con componentes de servidor y también clientes bajo ambiente Microsoft Windows, donde la autenticación está basada en un nombre de inicio de sesión (*login*) y una contraseña, el método EAP que provee mayor flexibilidad y seguridad es MS-CHAPv2 (*Microsoft Challenge Handshake Authentication Protocol version 2*), viajando dentro de PEAP (*Protected Extended Authentication Protocol*).

PEAP crea un canal cifrado SSL/TLS (*Secure Socket Layer / Transport Layer Security*, capa de sockets seguros / seguridad para la capa de transporte) entre el cliente y el servidor IAS. Este canal es luego usado para el transporte del tráfico de autenticación. Para crear este canal seguro, el cliente inalámbrico primero autentica al servidor mediante un certificado digital. Cuando se ha establecido la conexión segura se puede seleccionar un método EAP estándar para completar la autenticación. En este caso, el método seleccionado es MS-CHAP v2, dado que combina seguridad, interoperabilidad, flexibilidad y facilidad de implementación en un esquema de autenticación basado en nombre de usuario y contraseña,.

Una ventaja adicional de la selección de este esquema es el hecho de que los clientes Windows XP y Windows Vista permiten activar una opción que envía automáticamente las credenciales de autenticación del usuario hacia el servidor de autenticación. Una vez que el usuario ha iniciado sesión en su equipo con sus credenciales de dominio, no debe volver a introducir esas mismas credenciales para ingresar a la red WLAN.

3.3.3. Autoridad emisora de certificados

Los servidores IAS requieren tener certificados para autenticarse ante los clientes WLAN. Los certificados de servidor son necesarios para crear el túnel TLS entre el servidor IAS y los clientes que se desean autenticar. TLS sirve para proteger el intercambio de tramas de autenticación entre el servidor IAS y los clientes.

Para obtener estos certificados, puede optarse por instalar una entidad emisora de certificados, o bien adquirir los certificados de un proveedor comercial. Ambas posibilidades son válidas, y decantarse por una u otra no supone una diferencia técnica real para la implementación de la red inalámbrica. Sin embargo, en el sentido de seguir dándole uso a los recursos existentes y abaratar costos, se implementará el Microsoft Certificate Services, en uno de los servidores controladores de dominio: *apolo.cgsi.corp*.

Un beneficio importante de utilizar este servicio, es que al estar integrado con uno de los servidores de Active Directory, los certificados son expedidos y distribuidos automáticamente, tanto en el propio servidor *apolo.cgsi.corp*, como en el servidor *poseidon.cgsi.corp*., donde se encuentra el servicio IAS secundario.

3.3.4. Clientes WLAN

La arquitectura de seguridad diseñada es plenamente compatible con Windows XP Professional y Windows Vista Business. Todos los clientes Windows XP se deben actualizar al Service Pack 3. Asimismo, los equipos deben ser miembros del dominio *cgsi.corp*. La pertenencia al dominio es necesaria para que los equipos se autentiquen en la WLAN correctamente.

Windows XP y Vista permiten autenticar tanto al usuario como al equipo de manera independiente. Cuando un equipo se inicia, utiliza una cuenta de dominio y una contraseña para autenticarse en la WLAN. Aun cuando ningún usuario haya iniciado sesión, el equipo se podrá administrar si se conecta a la WLAN a través de sus propias credenciales. Por ejemplo, se podrá aplicar una configuración de directiva de grupo (GPO) en el equipo, así como distribuir software y parches.

Cuando un usuario inicia sesión en el equipo, este proceso de autenticación y autorización se repite, pero, en este caso, con el nombre de usuario y la contraseña del usuario. La sesión de un usuario sustituye la sesión de WLAN del equipo, de modo que no hay dos sesiones

activas al mismo tiempo. Además, esto evita que un usuario no autorizado utilice un equipo autorizado para obtener acceso a la WLAN.

3.3.5. Base de datos para la autenticación

El acceso a la WLAN en esta solución se controla por medio de grupos de seguridad de dominio de Active Directory. Como se describió previamente, la directiva de acceso remoto del servicio IAS utiliza una condición de filtro que concede acceso a WLAN a todos los miembros del grupo *Acceso WLAN*.

3.3.6. Proceso completo de autenticación de la WLAN

La Figura 3-6 muestra el proceso completo de autenticación con todos los componentes de la red WLAN diseñada para C.G.S.I., CA.

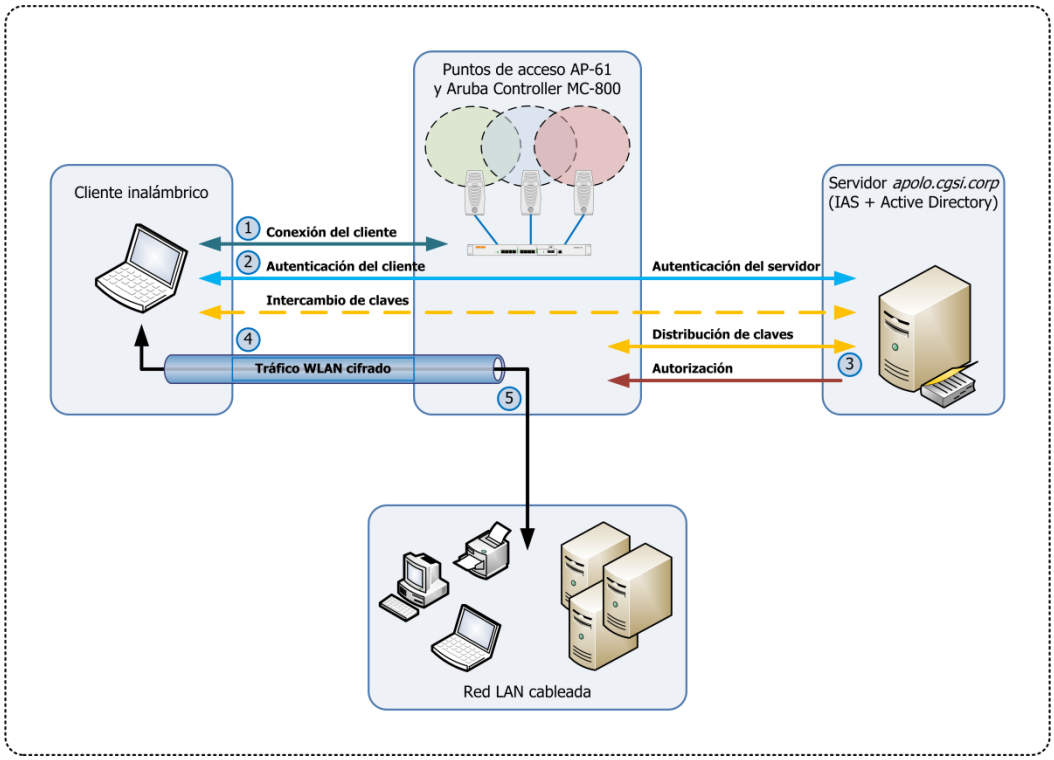

Figura 3-6. Proceso de autenticación en la WLAN

Los siguientes pasos describen cómo un cliente inalámbrico realiza una petición de autenticación y se le autoriza el acceso a la WLAN, y en consecuencia, a la red corporativa:

1. Cuando el cliente inalámbrico se encuentra dentro del rango de cobertura de uno de los puntos de acceso, intenta conectarse a la red WLAN, identificada por su SSID, *CORP_WLAN*. El SSID es usado por el cliente para determinar los parámetros y credenciales a utilizar durante la conexión.

2. El Aruba Controller está configurado para permitir sólo conexiones seguras (autenticadas mediante 802.1X) a la red inalámbrica. Cuando el cliente trata de conectarse a la WLAN, el controlador envía un desafío (*challenge*) al cliente. Luego el controlador establece un canal restringido (puerto no-controlado 802.1X) que permite al cliente comunicarse únicamente con el servidor IAS (*apolo.cgsi.corp* como servidor primario), bloqueando el acceso al resto de la red. El servidor IAS sólo acepta peticiones de autenticación provenientes de un NAS (*Network Access Server*) confiable, es decir, de aquel que ha sido configurado como cliente del servidor IAS y conoce el secreto compartido.

   El cliente trata de autenticarse contra el servidor IAS sobre el canal restringido, usando 802.1X. Como parte de la negociación PEAP, el cliente establece una sesión TLS (*Transport Layer Security*) con el servidor IAS. El establecimiento de una sesión TLS como parte de PEAP permite:

   - Que el cliente autentique al servidor IAS, es decir, que el cliente sólo establecerá la sesión con el servidor que tenga el certificado digital en el que confía el cliente.

   - Protege el protocolo de autenticación MS-CHAP v2 contra espionaje de paquetes.

   - La negociación de la sesión TLS genera una clave que será utilizada por el cliente y el servidor IAS para establecer claves maestras (*master keys*) comunes, de las que se derivan las claves usadas para el cifrado del tráfico WLAN.

   Una vez establecido el canal seguro, el cliente envía las credenciales de autenticación al servidor IAS usando el protocolo EAP MS-CHAP v2. Durante este intercambio, el tráfico dentro del túnel TLS sólo es visible para el cliente y el servidor IAS, y nunca es expuesto al punto de acceso.

3. El servidor IAS valida las credenciales, del equipo o del usuario, contra el servicio de directorio de Active Directory. Si el cliente es autenticado exitosamente, el servidor IAS ensambla la información necesaria que le permite decidir si debe autorizar al cliente para utilizar la WLAN. Para ello, se utiliza información del directorio (en este caso la membrecía al grupo *Acceso WLAN*) junto con las restricciones establecidas en la política de acceso a la red para permitir o negar el acceso al cliente. El servidor IAS envía su decisión al punto de acceso.

   Si se le permite el acceso al cliente, el servidor IAS transmite la clave maestra al punto de acceso. El cliente y el punto de acceso ahora comparten una clave común que, por el uso de WPA2, será usada para derivar las claves de cifrado y descifrado del tráfico de datos en la WLAN. Estas claves de cifrado son únicas para cada paquete transmitido.

4. El Aruba Controller puede ahora puentear la conexión inalámbrica del cliente hacia la red interna, permitiendo al cliente interactuar libremente con los sistemas en esta red. El tráfico enviado entre el cliente y el controlador está cifrado, mientras que el tráfico enviado entre el controlador y la red interna no lo está.

5. Si el cliente requiere la asignación de una dirección IP, ahora puede realizar una petición hacia algún servidor DHCP en la LAN, que puede ser *apolo.cgsi.corp* o *poseidon.cgsi.corp*. Una vez que se ha asignado la dirección IP, el cliente puede comunicarse normalmente con cualquier equipo en el resto de la red.

3.4. Diagrama lógico actualizado de la red de C.G.S.I., C.A.

A efectos de comparación con la Figura 3-1, la Figura 3-7 muestra lo que sería el diagrama lógico de la red de C.G.S.I., C.A. tras la implementación de la nueva red WLAN.

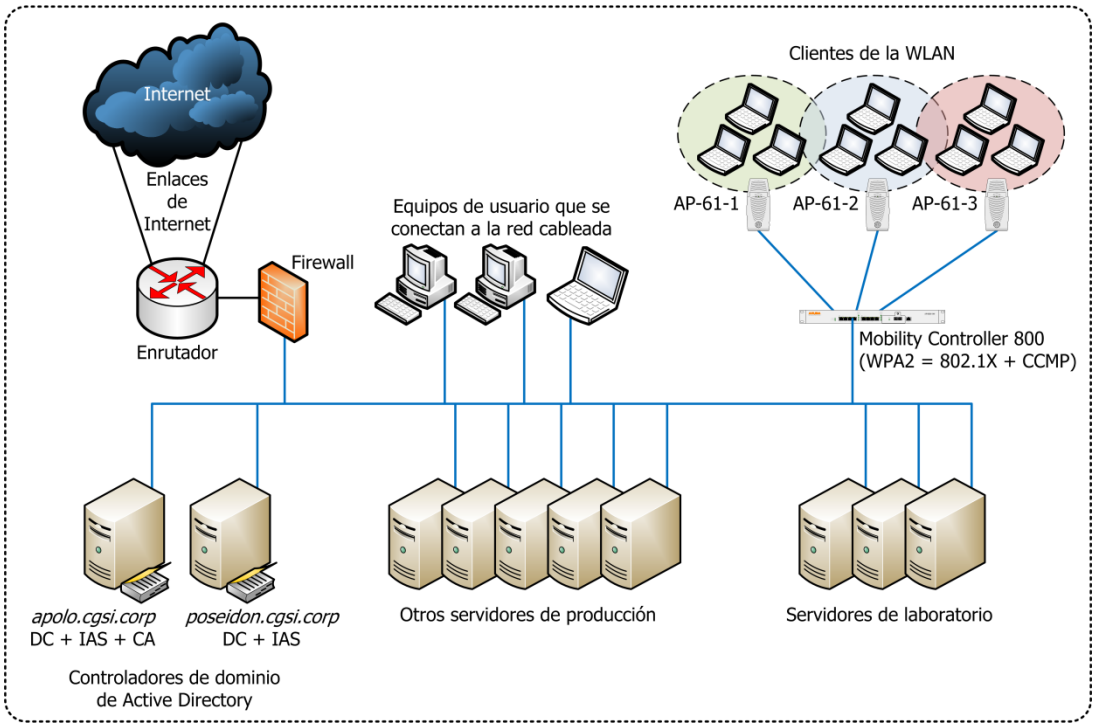

Figura 3-7. Diagrama lógico de la red de C.G.S.I., C.A. incluyendo la nueva WLAN

Capítulo 4

Implementación de la red WLAN

Partiendo del diseño especificado previamente, en este capítulo se detalla el proceso de implementación de los diferentes componentes de la red WLAN de C.G.S.I., C.A. El despliegue de esta red inalámbrica implica diferentes etapas que van desde la adecuación de la plataforma de tecnologías de información de la empresa, pasando por la implementación de la arquitectura de seguridad y de los elementos de conectividad inalámbrica, hasta la integración final de todos los componentes.

4.1. Preparación del ambiente para la implementación

El objetivo de esta fase es asegurar que todo el ambiente tecnológico necesario para la implementación de la red WLAN se encuentre listo antes de comenzar el despliegue. Las actividades ejecutadas en esta fase no se describen con detalle porque no forman parte directa de la implementación. Sin embargo, contribuyen a una mejor operación de la red y a elevar los niveles de seguridad generales de la solución propuesta.

4.1.1. Preparación del ambiente de servidores

Esta implementación parte de la existencia previa en la plataforma tecnológica de C.G.S.I., C.A. de los siguientes elementos:

- ***Requerimientos de infraestructura:*** se requieren dos o más servidores ejecutando Windows 2003 Server Standard Edition, que funcionan como controladores de dominio de la plataforma Active Directory. Estos servidores cuentan con los suficientes recursos y capacidad para la ejecución de IAS y Certificate Services. El servidor de autenticación, IAS, será instalado en ambos servidores de dominio, mientras que la autoridad emisora de certificados digitales se instalará en uno solo de los servidores de dominio.

- ***Requerimientos de hardware:*** para asegurar que la carga de solicitudes de autenticación no degrade el desempeño de las funciones propias de los servidores de dominio, éstos deben proveerse suficiente capacidad de recursos de hardware. En la Tabla 4-1 se comparan los requisitos mínimos de hardware para la ejecución del servidor IAS, contra la capacidad instalada de los servidores reales donde se está instalando la solución.

Tabla 4-1. Requerimientos mínimos versus capacidad instalada en los controladores de dominio

Característica	Requerimiento mínimo	Instalado en el servidor
Procesador	Procesador de un solo núcleo de 1 GHz	Procesador de un solo núcleo Intel Xeon de 2.8 GHz
Memoria RAM	512 MB	2 GB
Almacenamiento de disco	30 GB	150 GB
Interfaces de red	1 adaptador de red de 10/100 Mbps	2 adaptadores de red de 10/100/1000 Mbps

- ***Permisología requerida:*** para llevar a cabo las actividades de configuración necesarias a nivel de controladores de dominio, es necesario contar con credenciales de inicio de sesión de un usuario que pertenezca al grupo de administradores del dominio de Windows.

- ***Direccionamiento dinámico y resolución de nombres:*** las direcciones IP y el resto de los parámetros de red son asignadas a los clientes por el servicio DHCP que se ejecuta en uno de los servidores de dominio de la empresa. Por otra parte, la resolución de nombres para todos los clientes, cableados e inalámbricos es llevada a cabo por el servicio DNS que se ejecuta en ambos controladores de dominio.

- ***Política de contraseñas:*** esta solución utiliza activamente los nombres de inicio de sesión y las contraseñas de usuarios del dominio Active Directory para la autenticación de los usuarios en la red inalámbrica. Es por tanto de extrema

importancia no permitir el uso de contraseñas débiles o en blanco. El uso de contraseñas fácilmente predecibles facilita a un atacante irrumpir en la red WLAN. Adicionalmente, como las mismas contraseñas se usan para el inicio de sesión en el dominio, esto permitiría al atacante acceder al resto de recursos de la red. Se puede forzar el uso de contraseñas fuertes y con expiración periódica mediante el establecimiento de políticas de grupo (GPO) en el dominio.

- ***Actualizaciones de seguridad:*** antes de comenzar con la implementación de la red inalámbrica se verificó que los servidores Windows Server 2003 tuvieran instalado el Service Pack 2 y los parches de seguridad más reciente, con el objetivo de erradicar la mayor cantidad posible de vulnerabilidades de estos dispositivos antes de proceder al despliegue de la red.

4.1.2. Preparación de los clientes inalámbricos

Para soportar el esquema WPA2, los clientes inalámbricos que ejecutan el sistema operativo Windows XP Professional requieren tener instalado el Service Pack 2, más la actualización definida en el artículo KB893357 de la base de conocimientos de Microsoft. Dado que esta actualización está incluida en el Service Pack 3 para Windows XP, se verificó que los clientes tuvieran instalada esta versión, además de las actualizaciones de seguridad más recientes liberadas por Microsoft. En aquellos casos que no contaban con las actualizaciones necesarias, se procedió a su instalación.

En el caso de clientes Windows Vista Business no es requerida ninguna actualización. Sin embargo, a efectos de incrementar los niveles de seguridad de estos dispositivos, fueron actualizados al Service Pack 2, aplicando también las actualizaciones de seguridad más recientes.

4.1.3. Preparación de la infraestructura de conectividad

Como actividad previa a la implementación de la arquitectura de conectividad de la red inalámbrica, se procedió a actualizar el software del Aruba Controller, ArubaOS, desde la versión con la que venía el equipo de fábrica (v3.1.0.0), hasta la versión más reciente disponible para el momento de esta implementación (v3.4.1.0). Es de suma importancia poder contar con un controlador actualizado a nivel de software, ya que entre una versión y la otra, el fabricante ha liberado numerosas mejoras a nivel de interfaz gráfica de gestión,

soporte para nuevas funcionalidades y dispositivos, así como la corrección de errores y vulnerabilidades descubiertas.

El firmware de los cuatro puntos de acceso delgados es actualizado automáticamente por el Aruba Controller, una vez que existe conectividad en la red cableada entre estos dispositivos.

4.2. Implementación de la infraestructura de clave pública de la red

Esta fase consiste en la instalación y configuración del componente *Certificate Services* de Microsoft. Éste es un componente opcional de Windows Server 2003, y no se instala por defecto con el sistema operativo.

Una instalación de *Certificate Services* se conoce como una entidad emisora de certificados. Esta entidad emisora se utilizará para emitir sólo un tipo de certificado: certificados de servidor para los servidores IAS.

Sólo se necesita una entidad emisora de certificados para esta implementación que, de acuerdo al diseño, se instalará en el controlador de dominio *apolo.cgsi.corp*.

4.2.1. Instalación del componente Certificate Services

La instalación del componente Microsoft Certificate Services consistió en los siguientes pasos:

1. En el servidor *apolo.cgsi.corp* se abrió el *Panel de control*, *Agregar o quitar programas* y luego *Agregar o quitar componentes de Windows*.

2. En el *Asistente para componentes de Windows*, se seleccionó *Servicios de Certificate Server*, y se hizo clic en *Siguiente*, como se muestra en la Figura 4-1.

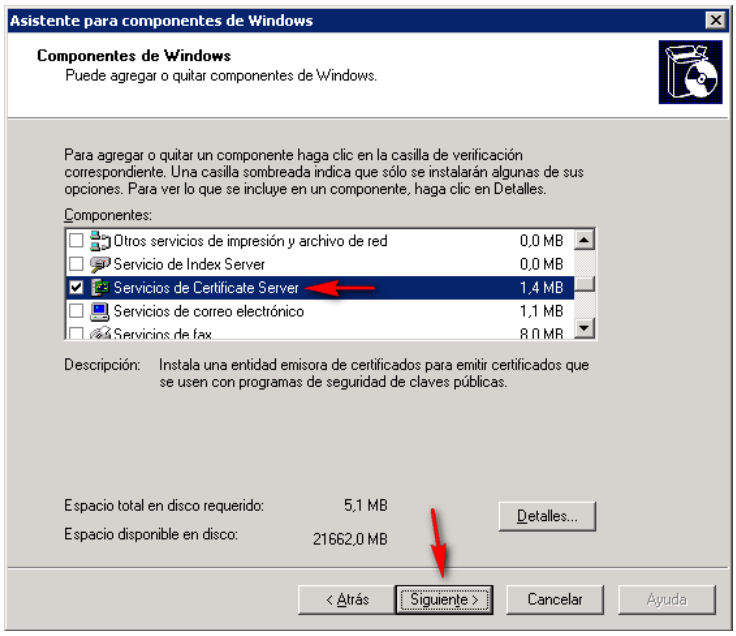

Figura 4-1. Agregar componente Servicios de Certificate Server

3. En la página *Tipo de entidad emisora de certificados*, se seleccionó *Entidad emisora raíz de la empresa*. También se seleccionó *Usar la configuración personalizada para generar el par de claves y el certificado de entidad emisora*, y se hizo clic en *Siguiente*, como se muestra en la Figura 4-2.

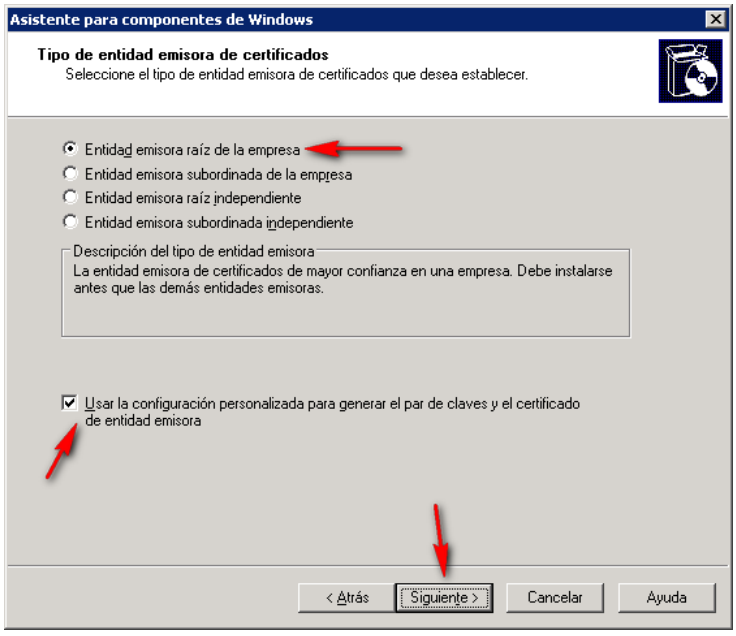

Figura 4-2. Tipo de entidad emisora de certificados

4. En la página *Pareja de claves públicas y privadas*, se seleccionó *Microsoft Strong Cryptographic Provider* como proveedor de servicios de cifrado. Luego, se seleccionó SHA-1 como algoritmo *hash* y 4096 bits como longitud de la clave de cifrado, como se muestra en la Figura 4-3. Se hizo clic en *Siguiente*.

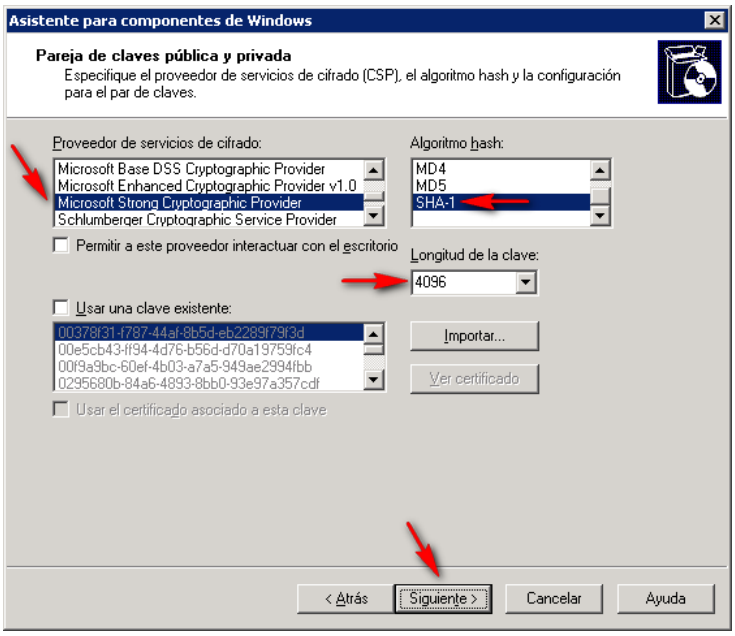

Figura 4-3. Pareja de claves públicas y privadas

5. En la página *Identificación de la entidad emisora de certificados*, se escribió el nombre común para la entidad implementada, *CGSI_Cert_Authority*. Se estableció el período de validez del certificado raíz en 25 años, y se hizo clic en *Siguiente*, como se muestra en la Figura 4-4.

6. En la página *Configuración de la base de datos de certificados*, se aceptaron los parámetros por defecto, y se hizo clic en *Siguiente*, como se muestra en la Figura 4-5.

7. El sistema operativo continuó la instalación del componente Certificate Server, copiando algunos archivos del CD de instalación de Windows Server 2003. Al finalizar instalación se solicitó reiniciar el servidor. De esta manera queda concluida la instalación de la entidad emisora de certificados.

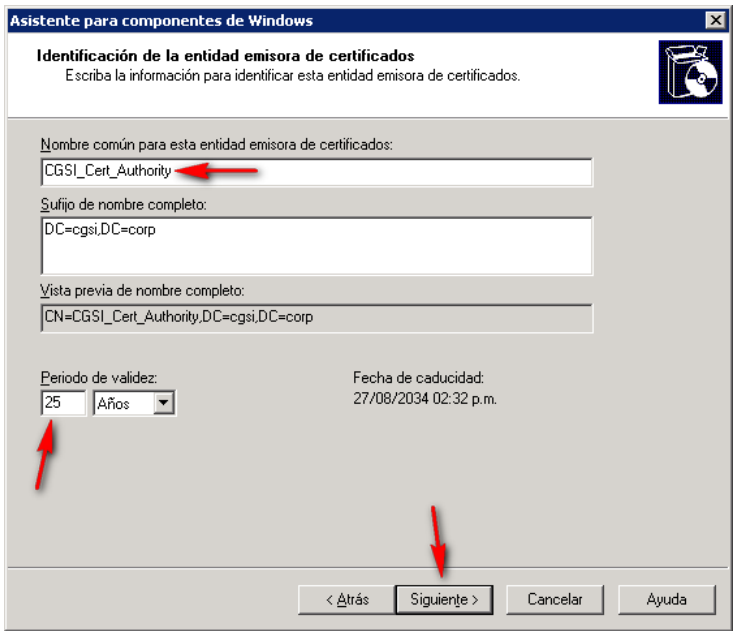

Figura 4-4. Identificación de entidad emisora de certificados

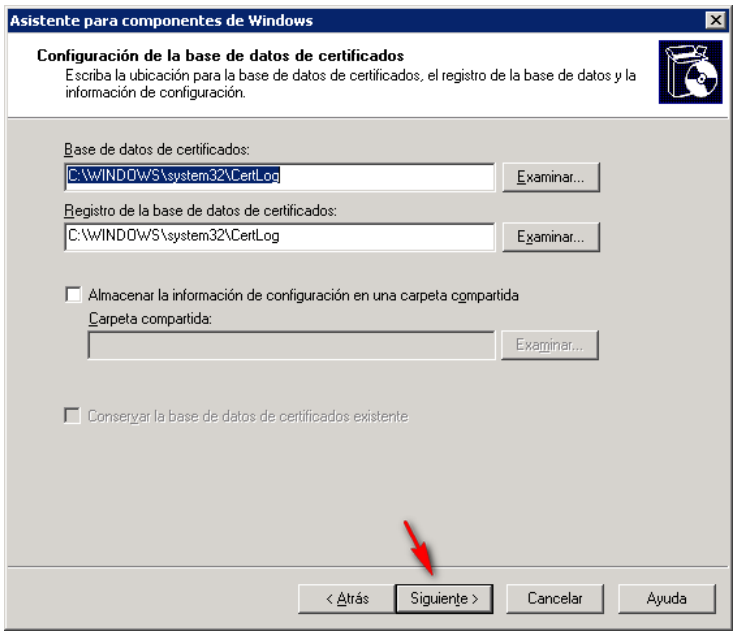

Figura 4-5. Configuración de la base de datos de certificados

4.2.2. Configuración del componente Certificate Services

El componente *Certificate Services* fue configurado para emitir certificados automáticamente a los equipos solicitantes. Los pasos para realizar esta configuración fueron:

1. En el servidor *apolo.cgsi.corp* se abrió la consola de administración *Entidad emisora de certificados* y se hizo clic con el botón secundario sobre el nombre de la entidad, *CGSI_Cert_Authority*. Se seleccionó *Propiedades*, como se muestra en la Figura 4-6.

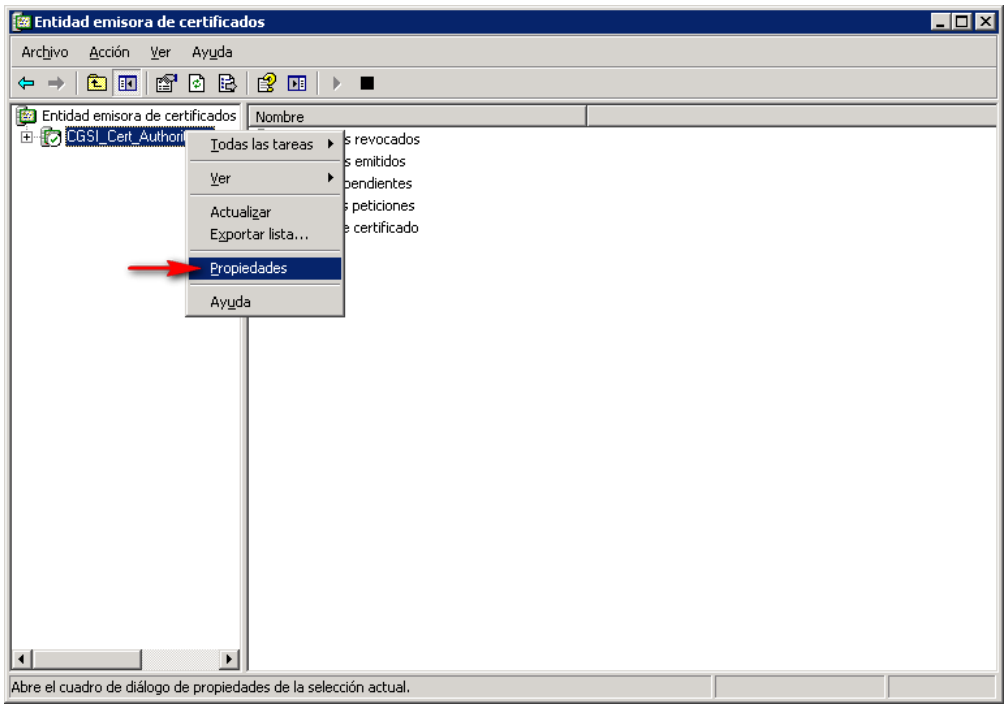

Figura 4-6. Consola de administración de la entidad emisora de certificados

2. En el cuadro de diálogo *Propiedades de CGSI_Cert_Authority*, se hizo clic en el botón *Propiedades*, como se muestra en la Figura 4-7.

3. En la pestaña *Tratamiento de la petición*, se seleccionó la opción *Seguir la configuración de la plantilla de certificados si es aplicable. De otra manera emitir el certificado automáticamente*, como se muestra en la Figura 4-8.

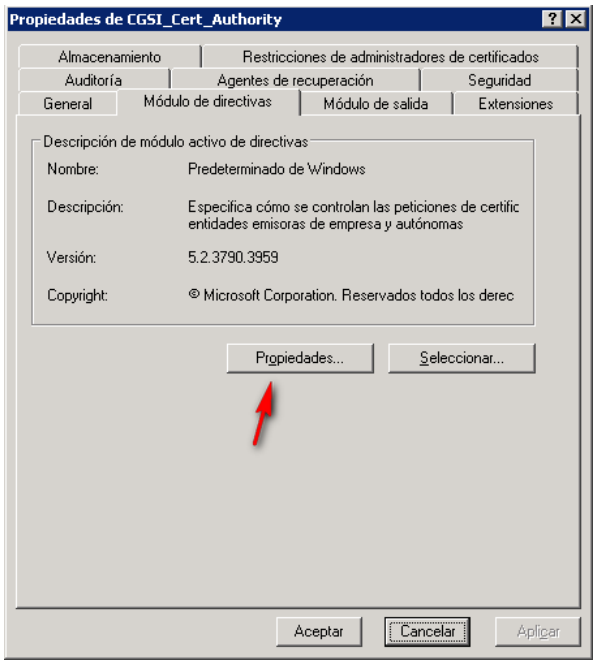

Figura 4-7. Propiedades de CGSI_Cert_Authority

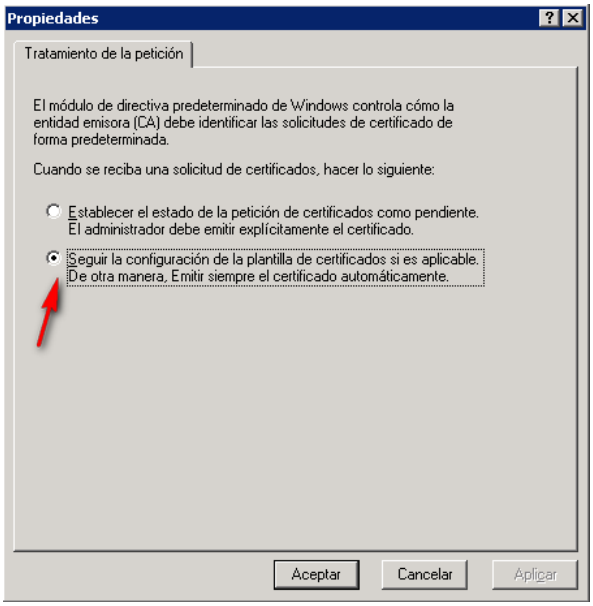

Figura 4-8. Tratamiento de la petición

4. Se cerraron los cuadros de diálogo abiertos, así como la consola de administración *Entidad emisora de certificados*.

4.3. Implementación del servicio de autenticación RADIUS

En esta fase se instaló y configuró el componente IAS (*Internet Authentication Service*). IAS es la implementación de Microsoft de un servidor RADIUS, y por tanto es el centro del esquema de autenticación IEEE 802.1X planteado. Por otra parte, se configuraron los grupos en el servicio Active Directory que contienen los usuarios y equipos que tienen permitida la conexión a la red WLAN de C.G.S.I, C.A.

4.3.1. Instalación del componente Microsoft IAS

La instalación del componente Microsoft IAS estuvo basada en los siguientes pasos:

1. En el servidor *apolo.cgsi.corp* se abrió el *Panel de control*, *Agregar o quitar programas* y luego *Agregar o quitar componentes de Windows*.

2. En el *Asistente para componentes de Windows*, se seleccionó *Servicios de red*, y se hizo clic en *Detalles*, como se muestra en la Figura 4-9.

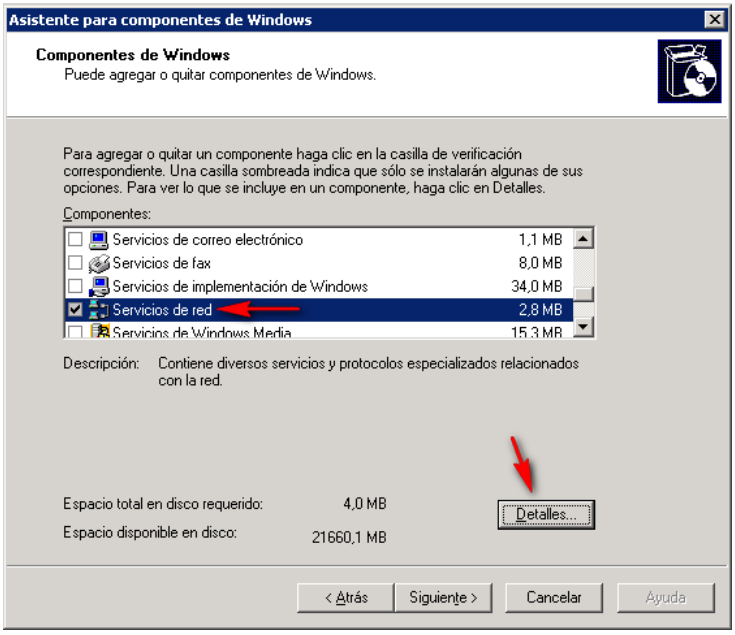

Figura 4-9. Agregar componente de Servicios de red

3. En se seleccionó Servicio de autenticación de Internet, y se hizo clic en Aceptar, como se muestra en la . Luego se hizo clic en *Siguiente*.

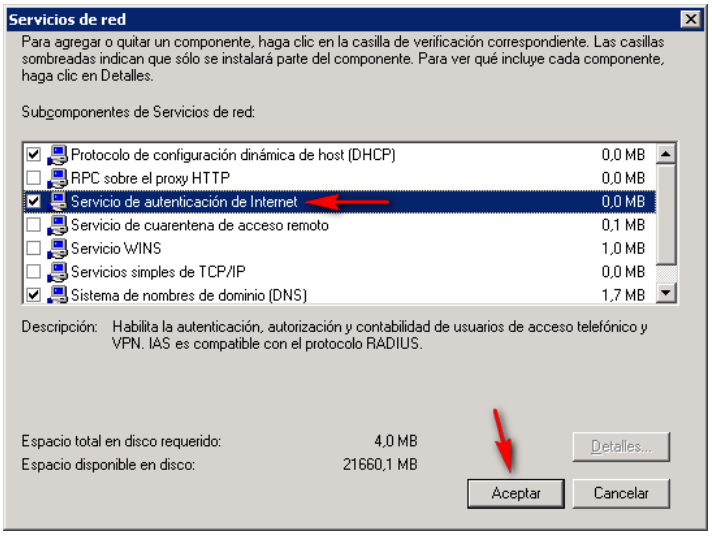

Figura 4-10. Agregar Servicio de autenticación de Internet

4. El sistema operativo continuó la instalación del componente IAS, copiando algunos archivos del CD de instalación de Windows Server 2003. De esta manera queda concluida la instalación del servidor de autenticación.

El mismo proceso de instalación se llevó a cabo en el controlador de dominio *poseidon.cgsi.corp*.

4.3.2. Configuración de grupos de seguridad en el servicio Active Directory

El componente IAS utiliza como base de datos para la autenticación el servicio de directorio de Microsoft, Active Directory. El criterio para permitir la conexión a la red WLAN es la pertenecía a un grupo de seguridad del directorio: *Acceso WLAN*. Este grupo está compuesto a su vez por otros dos grupos de seguridad, Usuarios WLAN y *Computadores WLAN*, que contienen respectivamente a los usuarios y computadores del dominio *cgsi.corp* con autorizados a ingresar a la red inalámbrica.

Estos grupos sólo se crearon en el servidor *apolo.cgsi.corp*, ya que estos son copiados automáticamente hacia el servidor *poseidon.cgsi.corp*, a través de los mecanismos de replicación de Active Directory.

Los pasos para la creación y configuración de estos grupos fueron:

1. En el servidor *apolo.cgsi.corp* se abrió la consola de administración *Usuarios y equipos de Active Directory* y se hizo clic con el botón secundario sobre el contenedor *Builtin*, que alberga los grupos por defecto de Active Directory. Se seleccionó *Nuevo* y luego *Grupo*, como se muestra en la Figura 4-11.

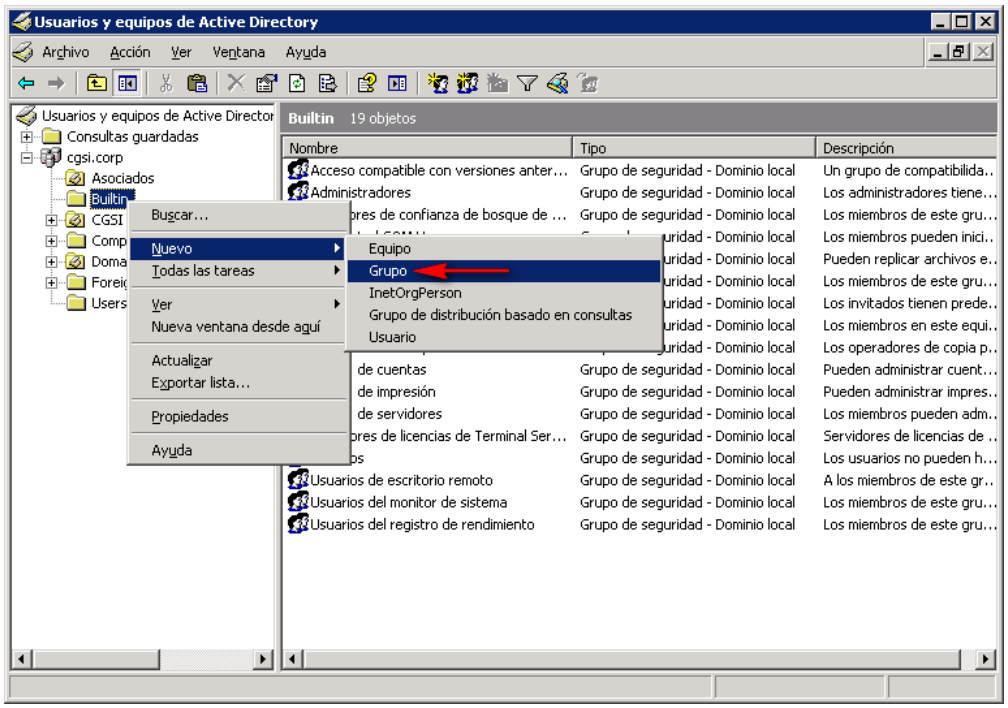

Figura 4-11. Usuarios y equipos de Active Directory

2. En el cuadro de diálogo *Nuevo objeto - Grupo* se escribió *Acceso WLAN* como nombre de grupo, y se seleccionó *Dominio local* como ámbito del grupo, como se muestra en la Figura 4-12. De forma similar se crearon los grupos *Usuarios WLAN* y *Computadoras WLAN*, como se muestra en la Figura 4-13.

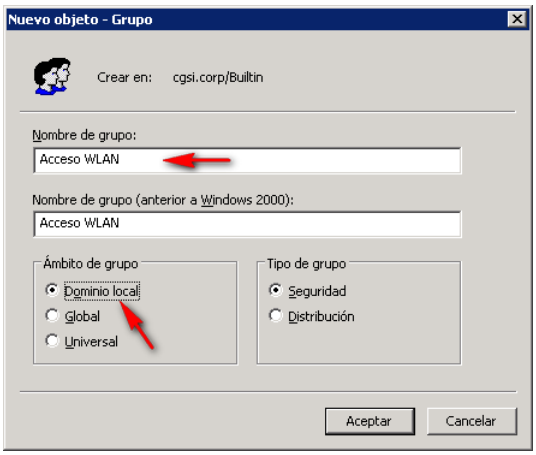

Figura 4-12. Nuevo grupo de seguridad: Acceso WLAN

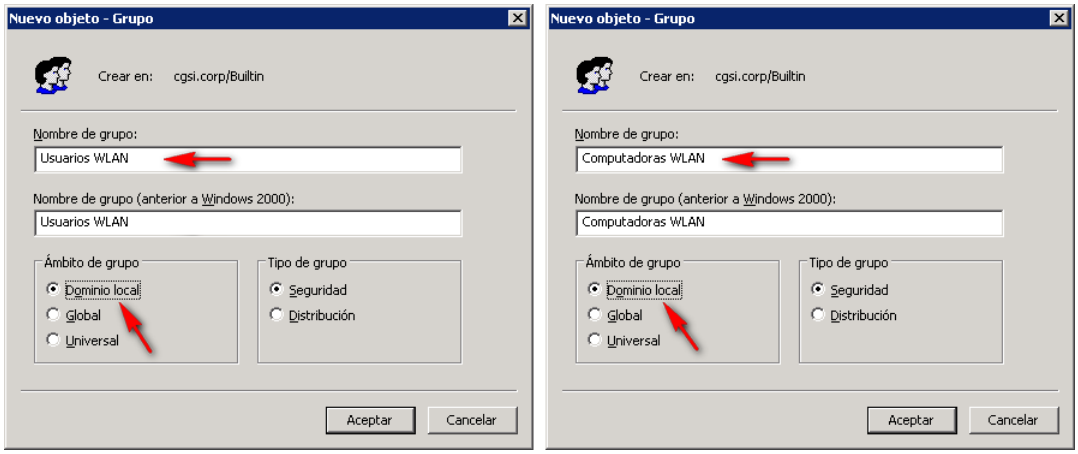

Figura 4-13. Nuevos grupos de seguridad: Usuarios WLAN y Computadoras WLAN

3. Se hizo clic con el botón secundario sobre el grupo *Acceso WLAN*, y se seleccionó *Propiedades*. En la pestaña *Miembros* del cuadro de diálogo *Propiedades de Acceso WLAN*, se hizo clic en el botón *Agregar*, como se muestra en la Figura 4-14.

4. En el cuadro de diálogo *Usuarios, Contactos, Equipos o Grupos*, se escribieron los nombres de los grupos *Usuarios WLAN* y *Computadoras WLAN*. Luego, se hizo clic en el botón *Aceptar*, como se muestra en la Figura 4-15.

5. En la pestaña *Miembros* del cuadro de diálogo *Propiedades de Acceso WLAN*, se verificó que hubieran agregado los grupos deseados, como se muestra en la Figura 4-16. Luego, se hizo clic en el botón *Aceptar*.

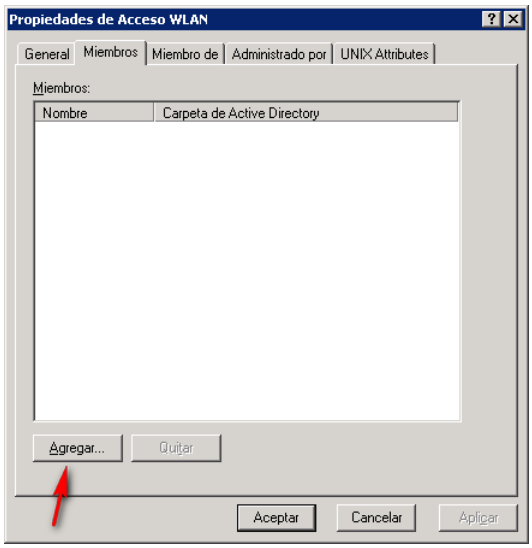

Figura 4-14. Propiedades del grupo Acceso WLAN

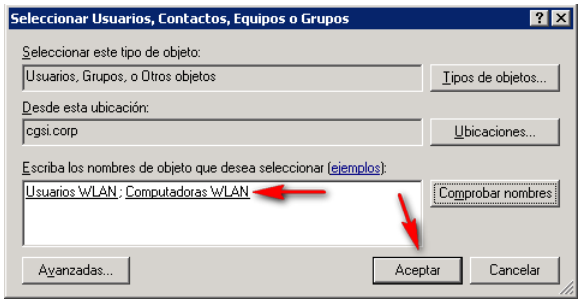

Figura 4-15. Seleccionar miembros del grupo Acceso WLAN

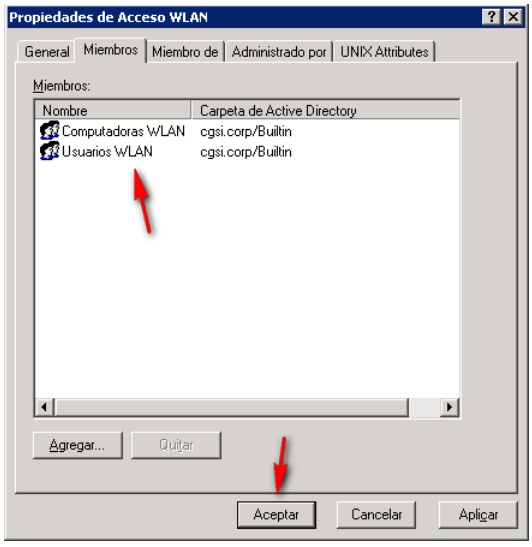

Figura 4-16. Miembros del grupo Acceso WLAN

6. De manera similar, se agregaron los usuarios y equipos autorizados a acceder a la WLAN en los grupos Usuarios WLAN y Computadoras WLAN, respectivamente, como se muestra en las Figura 4-17 y Figura 4-18.

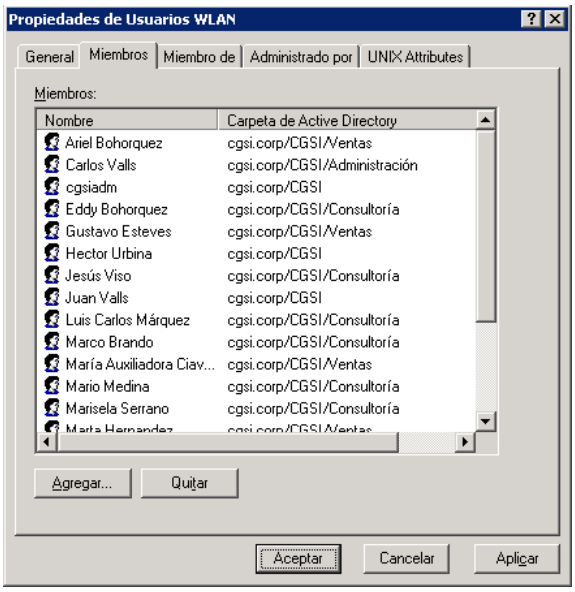

Figura 4-17. Miembros del grupo Usuarios WLAN

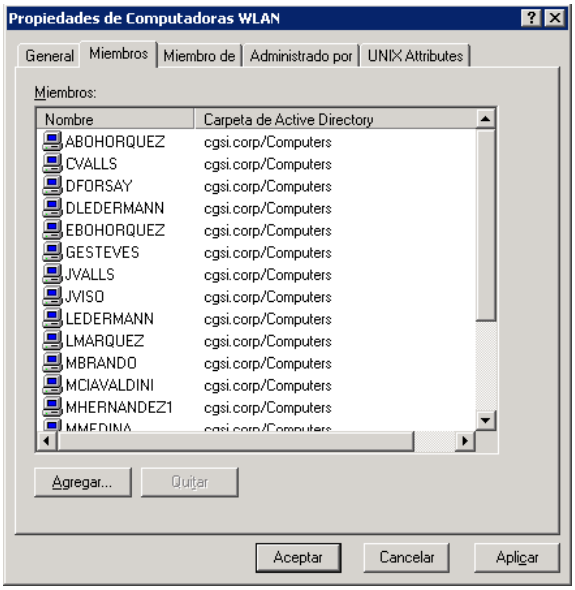

Figura 4-18. Miembros del grupo Computadoras WLAN

7. Se cerraron los cuadros de diálogo abiertos, así como la consola de administración *Usuarios y equipos de Active Directory*.

4.3.3. Configuración del componente Microsoft IAS

En esta sección se describe el proceso de configuración del servicio IAS de Microsoft. Esta actividad incluye la definición de un cliente RADIUS, el Aruba Controller, y la creación de la directiva de acceso remoto (RAP, *Remote Access Policy*) para la red WLAN de C.G.S.I., C.A.

La configuración del componente Microsoft IAS requirió los pasos siguientes:

1. En el servidor *apolo.cgsi.corp* se abrió la consola de administración *Servicio de autenticación de Internet* y se hizo clic con el botón secundario sobre *Clientes RADIUS*. Se seleccionó *Nuevo cliente RADIUS*, como se muestra en la Figura 4-19.

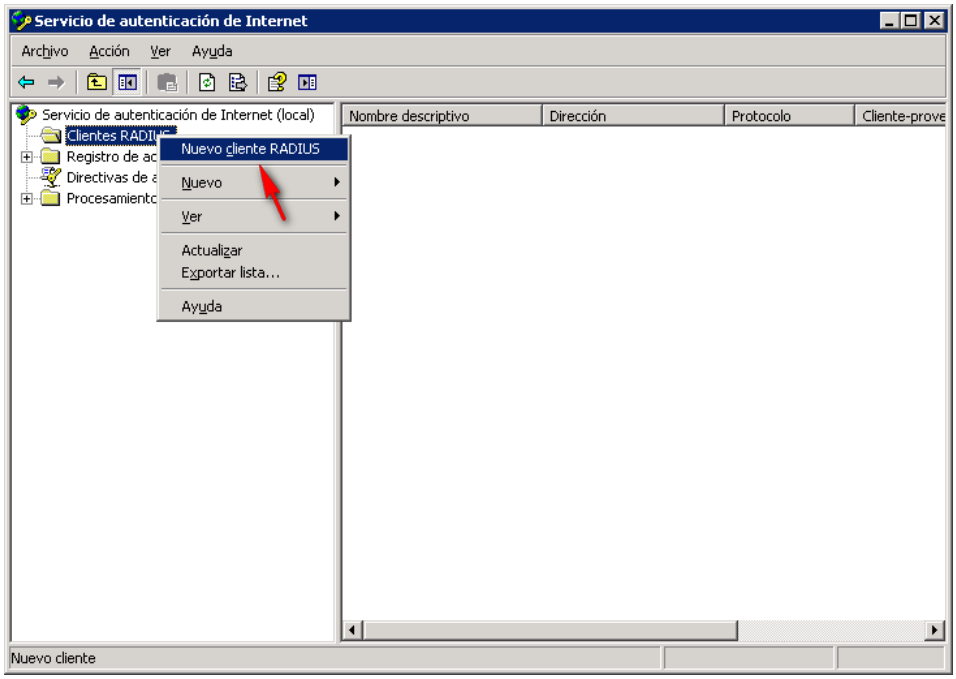

Figura 4-19. Consola de administración del Servicio de autenticación de Internet

2. En la página *Nombre y dirección* del asistente *Nuevo cliente RADIUS*, se escribió el nombre descriptivo del cliente, *Aruba MC-800 (CGSI)* y la dirección IP del cliente, *192.168.254.42*, como se muestra en la Figura 4-20. Luego, se hizo clic en el botón *Siguiente*.

3. En la página *Información adicional* del asistente *Nuevo cliente RADIUS*, se escribió el secreto compartido (no se muestra por razones de seguridad), como se muestra en la Figura 4-21. Luego, se hizo clic en el botón *Finalizar*.

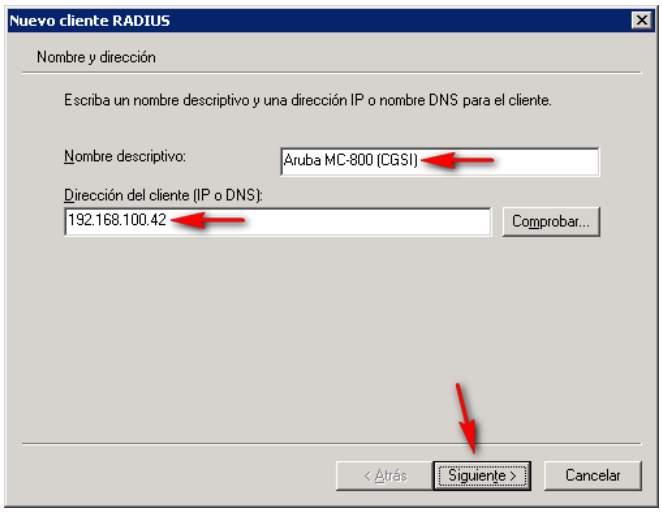

Figura 4-20. Nuevo cliente RADIUS - Nombre y dirección

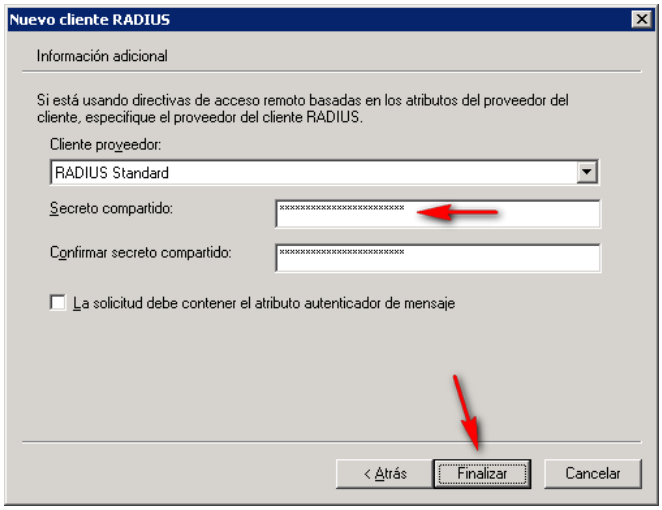

Figura 4-21. Nuevo cliente RADIUS - Información adicional

4. En la consola de administración *Servicio de autenticación de Internet* aparece creado el cliente RADIUS *Aruba MC-800 (CGSI)*, como se muestra en la Figura 4-22.

5. Se hizo clic con el botón secundario sobre *Directiva de acceso remoto*, y se seleccionó *Nueva directiva de acceso remoto*, como se muestra en la Figura 4-23.

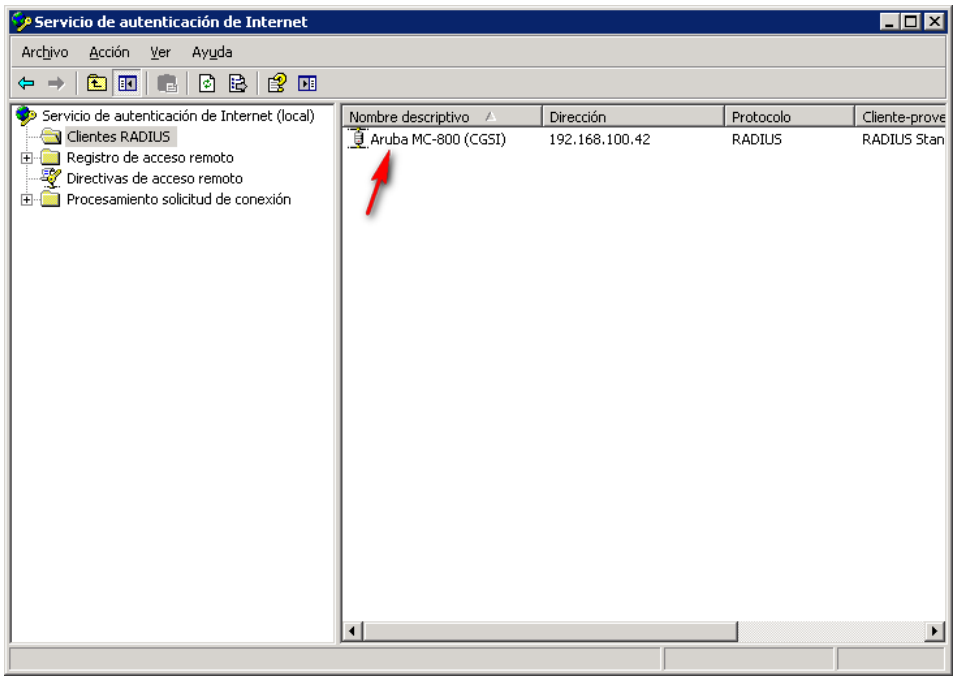

Figura 4-22. Cliente RADIUS Aruba MC-800 (CGSI)

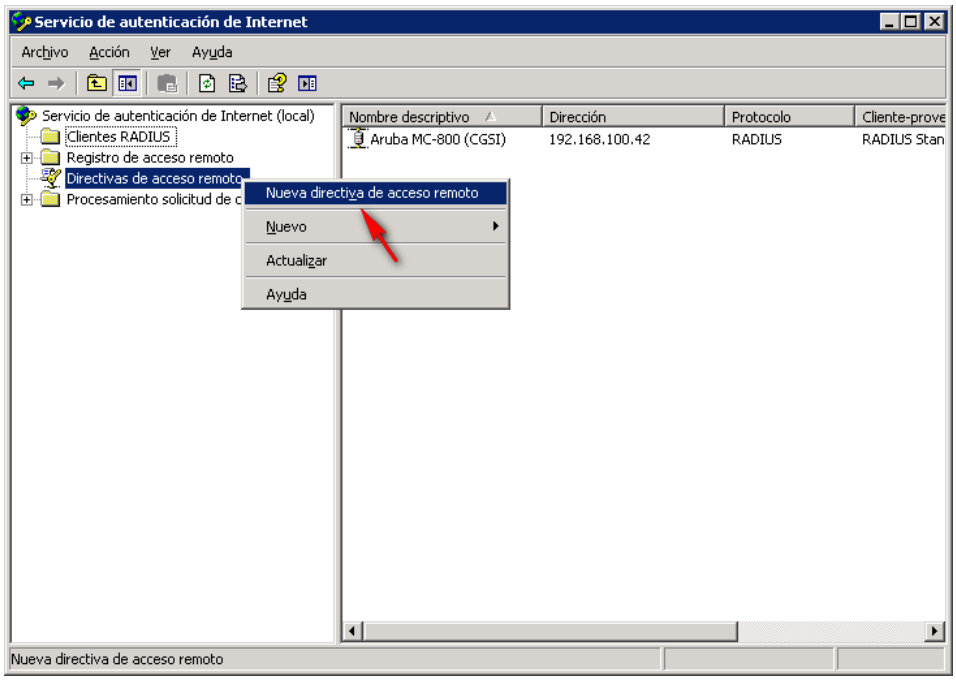

Figura 4-23. Nueva directiva de acceso remoto

6. En la página inicial del *Asistente para nueva directiva de acceso remoto* se hizo clic en *Siguiente*, como se muestra en la Figura 4-24.

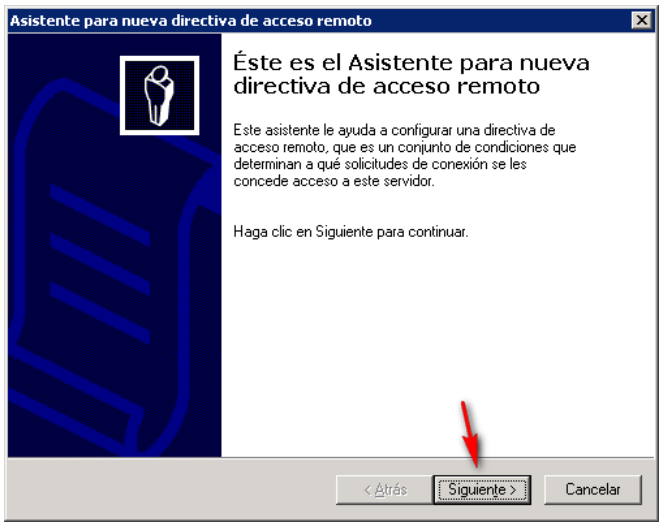

Figura 4-24. Asistente para nueva directiva de acceso remoto

7. En la página *Método de configuración de directiva* del asistente, se seleccionó la opción *Configurar una directiva personalizada*. También se escribió el nombre de directiva *Permitir acceso a la red WLAN corporativa*, como se muestra en la Figura 4-25. Luego, se hizo clic en *Siguiente*.

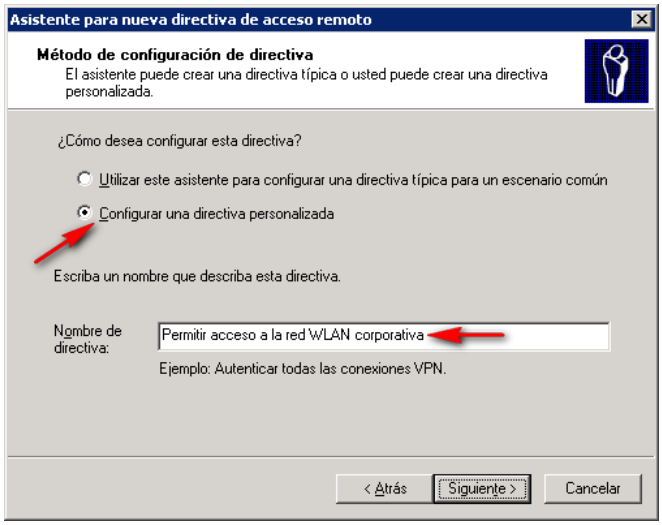

Figura 4-25. Método de configuración de directiva

8. En la página *Condiciones de directiva* del asistente, se hizo clic en el botón *Agregar* para adicionar tres condiciones a la directiva de acceso remoto: Tipo de autenticación "MS CHAP v2", tipo de puerto "Inalámbrica IEEE 802.11 u otra", y

grupo coincide con “CGSI\Acceso WLAN”, como se muestra en la Figura 4-26. Luego, se hizo clic en *Siguiente*.

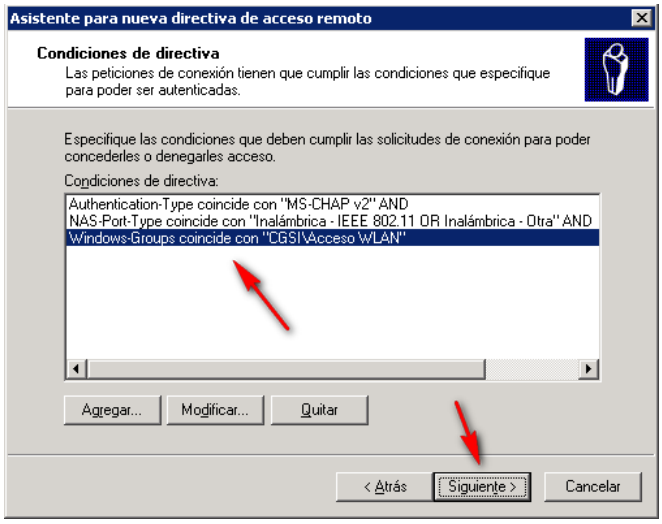

Figura 4-26. Condiciones de directiva

9. En la página *Permisos del asistente*, se seleccionó la opción *Conceder permiso de acceso remoto*, como se muestra en la Figura 4-27. Luego, se hizo clic en *Siguiente*.

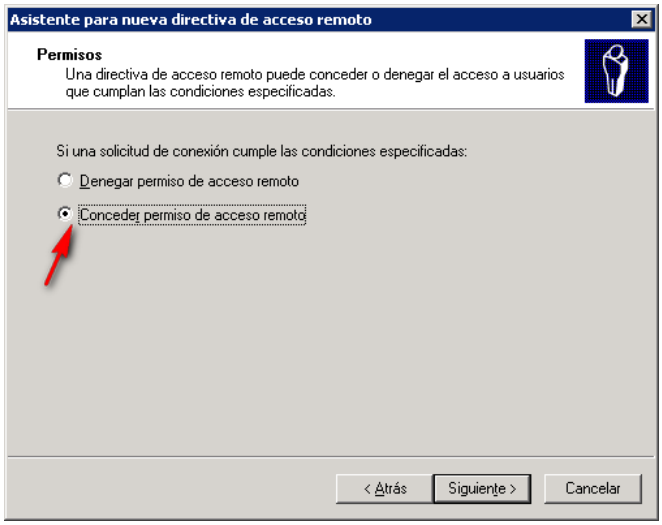

Figura 4-27. Permisos de la directiva

10. En la página *Perfil* del asistente, se hizo clic en el botón *Editar perfil*. En la pestaña *Autenticación* sólo se dejó seleccionada la opción *Autenticación cifrada de Microsoft*

versión 2 (MS-CHAP v2), y se hizo clic en el botón *Métodos EAP*, como se muestra en la Figura 4-28.

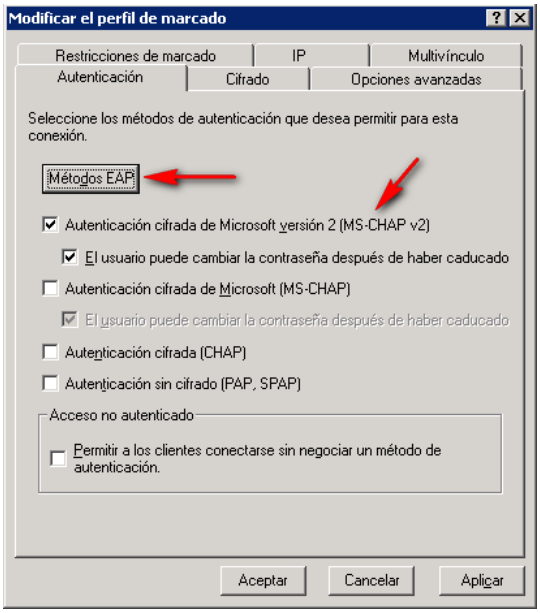

Figura 4-28. Perfil de autenticación

11. En el cuadro de diálogo *Agregar EAP* se seleccionó *EAP protegido (PEAP)*, y se hizo clic en el botón *Aceptar*, como se muestra en la Figura 4-29.

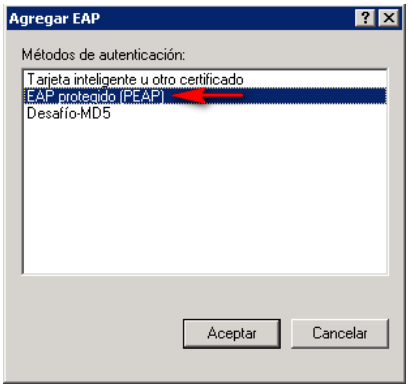

Figura 4-29. Agregar método EAP

12. En el cuadro de diálogo *Propiedades de EAP protegido*, se seleccionó la opción *Habilitar reconexión rápida*, como se muestra en la Figura 4-30. Luego, se hizo clic en el botón *Aceptar*.

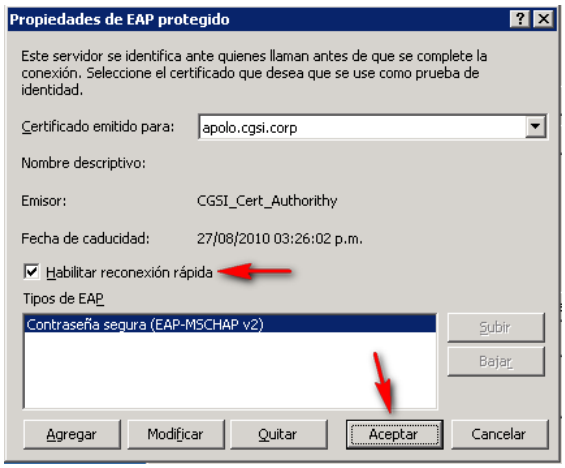

Figura 4-30. Propiedades de EAP protegido

13. Se hizo clic en el botón *Finalizar* para terminar el *Asistente para nueva directiva de acceso remoto*. Ahora en la consola de administración *Servicio de autenticación de Internet* aparece creado la directiva de acceso remoto *Permitir acceso a la red WLAN corporativa*, como se muestra en la Figura 4-31.

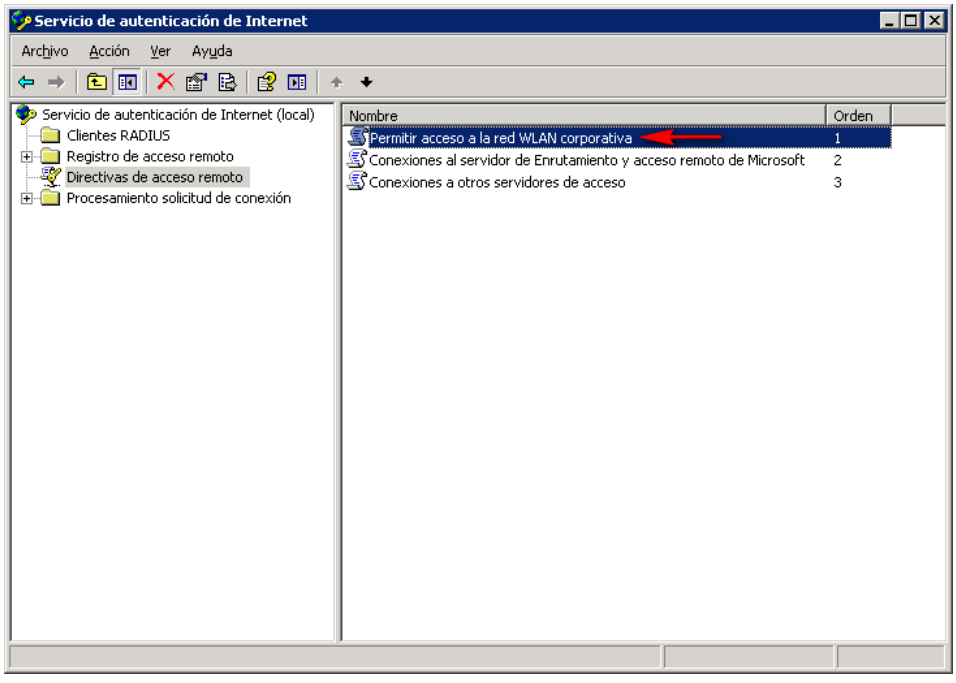

Figura 4-31. Directiva *Permitir acceso a la red WLAN corporativa*

14. Se cerró la consola de administración *Servicio de autenticación de Internet*, dando por terminada la configuración del componente IAS en el servidor *apolo.cgsi.corp*.

El mismo proceso de configuración se llevó a cabo en el servidor de dominio *poseidon.cgsi.corp*, de manera de contar con un servidor IAS secundario en caso de que falle el servidor primario.

4.4. Implementación de la arquitectura de conectividad de la red WLAN

Esta fase consiste en la implementación de los diferentes componentes que conforman la infraestructura de conectividad de la red WLAN de C.G.S.I., C.A. De acuerdo al diseño planteado, la arquitectura de conectividad de esta red es de tipo centralizado, y fue implementada utilizando equipamiento del fabricante Aruba Networks.

4.4.1. Configuración del Aruba Controller vía interfaz de línea de comandos

La configuración general del Aruba Controller se realizó mediante la interfaz de línea de comandos (CLI, *Command Line Interface*). Dado que hasta el momento este dispositivo carecía de configuración de red, la conexión a la línea de comandos se realizó mediante un cable serial de consola, que conectaba directamente este equipo y la computadora utilizada para la configuración, así como el software emulador de terminal HyperTerminal de Microsoft.

Contando el controlador con los parámetros básicos de red (dirección IP y máscara de subred), esta misma configuración puede realizarse por la interfaz Web de gestión del dispositivo. Sin embargo, por sencillez y flexibilidad, se prefirió realizar la configuración por la interfaz de línea de comandos.

Gran parte de la configuración del controlador, específicamente aquella no relacionada directamente con esta implementación, permaneció por defecto como viene de fábrica. sólo se agregaron o modificaron fragmentos de la configuración relevantes para la red WLAN de C.G.S.I., C.A.

Dado que en el Aruba Controller se instaló una nueva versión del software ArubaOS, al iniciar el equipo se ejecuta un asistente para la configuración básica del dispositivo. En este asistente se establecen parámetros básicos como nombre del equipo, dirección IP y

máscara de subred, puerta de enlace predeterminada, código de país, zona horaria y contraseñas de administración.

Se muestra a continuación la traza de la ejecución de este asistente de configuración básica:

```
Enter System name [Aruba800]: ArubaMC800
Enter VLAN 1 interface IP address [172.16.0.254]: 192.168.100.42
Enter VLAN 1 interface subnet mask [255.255.255.0]: 255.255.255.0
Enter IP Default gateway [none]: 192.168.100.1
Enter Switch Role, (master|local) [master]: master
Enter Country code (ISO-3166), <ctrl-I> for supported list: VE
You have chosen Country code VE for Venezuela (yes|no)?: yes
Enter Time Zone [PST-8:0]: VET-4:30
Enter Time in GMT [20:27:05]: 20:27:05
Enter Date (MM/DD/YYYY) [08/26/2009]: 08/26/2009
Enter Password for admin login (up to 32 chars): *************
Re-type Password for admin login: *************
Enter Password for enable mode (up to 15 chars): *************
Re-type Password for enable mode: *************
Do you wish to shutdown all the ports (yes|no)? [no]: no
Current choices are:
System name: ArubaMC800
VLAN 1 interface IP address: 192.168.100.42
VLAN 1 interface subnet mask: 255.255.255.0
IP Default gateway: 192.168.100.4
Switch Role: master
Time Zone: VET-4:30
Ports shutdown: no
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no) yes
Creating configuration... Done.
System will now restart!
```

Tras el reinicio del Aruba Controller se procedió a la configuración propia de la conectividad de la red WLAN, así como la integración con la infraestructura de autenticación. Para el resto de la configuración del Aruba Controller se siguieron los siguientes pasos:

1. Se inició sesión en el equipo, se cambió al modo de operación *enable*, y luego se pasó al modo de configuración.

```
(ArubaMC800)
User: admin
Password: *************
(ArubaMC800) >enable
Password: *********
(ArubaMC800) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
```

2. Se configuró un servidor NTP (*Network Time Protocol*) para que el equipo sincronice la hora automáticamente.

```
(ArubaMC800) (config) #ntp server 169.229.70.201
```

3. El Aruba Controller contiene un firewall integrado que permite establecer políticas de acceso, una vez se está conectado a la red WLAN. Estas políticas están asociadas a un perfil de usuario que se asigna a los clientes (usuarios o equipos) una vez autenticados.

```
(ArubaMC800) (config) #ip access-list session CGSI_Policy
(ArubaMC800) (config-sess-CGSI_Policy)#any any any permit queue high
(ArubaMC800) (config-sess-CGSI_Policy)#exit
(ArubaMC800) (config) #user-role CGSI_User_Role
(ArubaMC800) (config-role) #session-acl CGSI_Policy
(ArubaMC800) (config-role) #exit
```

4. Se definió un perfil con los parámetros de autenticación IEEE 802.1X que usarán los clientes inalámbricos cuando completan su asociación inicial con el Aruba Controller.

```
(ArubaMC800) (config) #aaa authentication dot1x CGSI_dot1x_Profile
(ArubaMC800) (802.1X Authentication Profile "CGSI_dot1x_Profile") #machine-
authentication machine-default-role CGSI_User_Role
(ArubaMC800) (802.1X Authentication Profile "CGSI_dot1x_Profile") #machine-
authentication user-default-role CGSI_User_Role
(ArubaMC800) (802.1X Authentication Profile "CGSI_dot1x_Profile") #reauthentication
(ArubaMC800) (802.1X Authentication Profile "CGSI_dot1x_Profile") #tls-guest-role
CGSI_User_Role
(ArubaMC800) (802.1X Authentication Profile "CGSI_dot1x_Profile") #exit
```

5. Se definieron los servidores RADIUS que utilizará el Aruba Controller para la autenticación de los usuarios. Estos servidores son utilizados en el orden en que fueron definidos. En caso de que fallase el servidor principal, *apolo.cgsi.corp*, se empezaría a usar el servidor secundario, *poseidon.cgsi.corp*. Luego se definió un grupo que concentra a los dos servidores para poder utilizarlos posteriormente en los perfiles de autenticación.

```
(ArubaMC800) (config) #aaa authentication-server radius Apolo
(ArubaMC800) (RADIUS Server "Apolo") #host 192.168.100.3
(ArubaMC800) (RADIUS Server "Apolo") #key ************ (no se muestra por seguridad)
(ArubaMC800) (RADIUS Server "Apolo") #nas-identifier "Aruba MC-800 (CGSI)"
```

```
(ArubaMC800) (RADIUS Server "Apolo") #nas-ip 192.168.100.42
(ArubaMC800) (RADIUS Server "Apolo") #exit
(ArubaMC800) (config) #aaa authentication-server radius Poseidon
(ArubaMC800) (RADIUS Server "Poseidon") #host 192.168.100.4
(ArubaMC800) (RADIUS Server "Apolo") #key ************* (no se muestra por seguridad)
(ArubaMC800) (RADIUS Server "Poseidon") #nas-identifier "Aruba MC-800 (CGSI)"
(ArubaMC800) (RADIUS Server "Poseidon") #nas-ip 192.168.100.42
(ArubaMC800) (RADIUS Server "Poseidon") #exit
(ArubaMC800) (config) #aaa server-group CGSI_RADIUS_Servers
(ArubaMC800) (Server Group "CGSI_RADIUS_Servers") #auth-server Apolo
(ArubaMC800) (Server Group "CGSI_RADIUS_Servers") #auth-server Poseidon
(ArubaMC800) (Server Group "CGSI_RADIUS_Servers") #exit
```

6. Se definió un perfil AAA que asocia el grupo de servidores de autenticación, el perfil 802.1X, y el rol de los usuarios.

```
(ArubaMC800) (config) #aaa profile CGSI_AAA_Profile
(ArubaMC800) (AAA Profile "CGSI_AAA_Profile") #authentication-dot1x
CGSI_dot1x_Profile
(ArubaMC800) (AAA Profile "CGSI_AAA_Profile") #dot1x-default-role CGSI_User_Role
(ArubaMC800) (AAA Profile "CGSI_AAA_Profile") #dot1x-server-group CGSI_RADIUS_Servers
(ArubaMC800) (AAA Profile "CGSI_AAA_Profile") #radius-accounting CGSI_RADIUS_Servers
(ArubaMC800) (AAA Profile "CGSI_AAA_Profile") #exit
```

7. Se definió el perfil de SSID de la red WLAN. En este paso se asignan el nombre del SSID, *CORP_WLAN*, y el modo de operación de la red, *WPA2-AES*.

```
(ArubaMC800) (config) #wlan ssid-profile CGSI_SSID_Profile
(ArubaMC800) (SSID Profile "CGSI_SSID_Profile") #essid CORP_WLAN
(ArubaMC800) (SSID Profile "CGSI_SSID_Profile") #opmode wpa2-aes
(ArubaMC800) (SSID Profile "CGSI_SSID_Profile") #exit
```

8. Se definieron un Virtual AP (punto de acceso virtual) un grupo de puntos de acceso a los que pertenecerán los puntos de acceso delgados (*thin APs*) que dan acceso a la red WLAN.

```
(ArubaMC800) (config) #wlan virtual-ap CGSI_Virtual_AP
(ArubaMC800) (Virtual AP profile "CGSI_Virtual_AP") #aaa-profile CGSI_AAA_Profile
(ArubaMC800) (Virtual AP profile "CGSI_Virtual_AP") #exit
(ArubaMC800) (config) #ap-group CGSI_AP_Group
(ArubaMC800) (AP group "CGSI_AP_Group") #virtual-ap CGSI_Virtual_AP
(ArubaMC800) (AP group "CGSI_AP_Group") #exit
```

9. Se definió un perfil regulatorio, que utiliza la información de manejo del espectro de radio frecuencias disponible para Venezuela. Además se definió un perfil que deshabilita la configuración automática del perfil de radio de los puntos de acceso.

```
(ArubaMC800) (config) #ap regulatory-domain-profile "CGSI_Regulatory_Domain_Profile"
(ArubaMC800) (Regulatory Domain) "CGSI_Regulatory_Domain_Profile") #country-code VE
(ArubaMC800) (Regulatory Domain) "CGSI_Regulatory_Domain_Profile") #exit
(ArubaMC800) (config) #rf arm-profile "CGSI_ARM_Off_Profile"
(ArubaMC800) (ARM Profile "CGSI_ARM_Off_Profile") #assignment disable
(ArubaMC800) (ARM Profile "CGSI_ARM_Off_Profile") #exit
```

10. Se configuraron perfiles de radio con información sobre el canal de frecuencias y la potencia de transmisión, para posteriormente asignárselos a los puntos de acceso.

```
(ArubaMC800) (config) #rf dot11g-radio-profile "CGSI_RF_Ch1-g_Profile"
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch1-g_Profile") #channel 1
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch1-g_Profile") #tx-power 30
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch1-g_Profile") #arm-profile
"CGSI_ARM_Off_Profile"
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch1-g_Profile") #exit
(ArubaMC800) (config) #rf dot11g-radio-profile "CGSI_RF_Ch6-g_Profile"
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch6-g_Profile") #channel 6
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch6-g_Profile") #tx-power 30
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch6-g_Profile") #arm-profile
"CGSI_ARM_Off_Profile"
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch6-g_Profile") #exit
(ArubaMC800) (config) #rf dot11g-radio-profile "CGSI_RF_Ch11-g_Profile"
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch11-g_Profile") #channel 11
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch11-g_Profile") #tx-power 30
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch11-g_Profile") #arm-profile
"CGSI_ARM_Off_Profile"
(ArubaMC800) (802.11g Radio Profile "CGSI_RF_Ch11-g_Profile") #exit
```

11. Se procedió a configurar los puntos de acceso, asignándoles un nombre, una dirección IP, un perfil de radio y un perfil regulatorio. El controlador descubre los puntos de acceso una vez que son conectados a la red, y les asigna su configuración según el número de serial.

```
(ArubaMC800) (config) #ap-serial "A30094075"
(ArubaMC800) (AP Serial "A30094075") #ap-name "AP_OFC102"
(ArubaMC800) (AP Serial "A30094075") #ip address 192.168.100.46 255.255.255.0
(ArubaMC800) (AP Serial "A30094075") #dot11g-radio-profile "CGSI_RF_Ch1-g_Profile"
(ArubaMC800) (AP Serial "A30094075") #regulatory-domain-profile
"CGSI_Regulatory_Domain_Profile"
(ArubaMC800) (AP Serial "A30094075") #exit
(ArubaMC800) (config) #ap-serial "A30094075"
(ArubaMC800) (AP Serial "A30093959") #ap-name "AP_OFC103"
(ArubaMC800) (AP Serial "A30093959") #ip address 192.168.100.47 255.255.255.0
(ArubaMC800) (AP Serial "A30093959") #dot11g-radio-profile "CGSI_RF_Ch6-g_Profile"
```

```
(ArubaMC800) (AP Serial "A30093959") #regulatory-domain-profile
"CGSI_Regulatory_Domain_Profile"
(ArubaMC800) (AP Serial "A30093959") #exit
(ArubaMC800) (config) #ap-serial "A30094075"
(ArubaMC800) (AP Serial "A30094082") #ap-name "AP_OFC104"
(ArubaMC800) (AP Serial "A30094082") #ip address 192.168.100.48 255.255.255.0
(ArubaMC800) (AP Serial "A30094082") #dot11g-radio-profile "CGSI_RF_Ch11-g_Profile"
(ArubaMC800) (AP Serial "A30094082") #regulatory-domain-profile
"CGSI_Regulatory_Domain_Profile"
(ArubaMC800) (AP Serial "A30094082") #exit
```

12. Terminada la configuración del equipo se procede a guardarla en la memora flash del Aruba Controller y se reinicia el equipo.

```
(ArubaMC800) (config) #write memory
Saving Configuration...

Configuration Saved.

(ArubaMC800) (config) #reload
Do you really want to reset the system(y/n): y
System will now restart!
```

4.5. Configuración de los clientes inalámbricos

Como fase final de la implementación, teniendo ya disponible toda la infraestructura de conectividad y seguridad de la red inalámbrica, se procede a la configuración de los clientes inalámbricos.

En esta sección se muestra el proceso de configuración de los clientes utilizando la funcionalidad de políticas de grupo (*Group Policies*) de Active Directory. Adicionalmente se describe el proceso alternativo de configuración manual de un cliente inalámbrico individual.

La Tabla 4-2 contiene los parámetros de configuración utilizados en los clientes inalámbricos.

Tabla 4-2. Parámetros de configuración para los clientes inalámbricos

Parámetro	Configuración
Grupo para permitir el acceso a la WLAN	Acceso WLAN
Grupo para permitir el acceso a la WLAN de los usuarios	Usuarios WLAN
Grupo para permitir el acceso a la WLAN de los equipos	Computadoras WLAN
Nombre de objeto de directiva de grupo de WLAN	Configuración de clientes WLAN (GPO)
Grupo de seguridad de filtrado de objetos de directiva de grupo	Configuración de clientes WLAN (filtro)
Nombre de directiva de red inalámbrica	Configuración de clientes WLAN (PEAP-WPA2)
Nombre de red de WLAN (SSID)	CORP_WLAN
Tipo de Protocolo de autenticación extensible (EAP)	PEAP
Método de autenticación de PEAP	Contraseña protegida (EAP-MSCHAP v2)
Reconexión rápida de PEAP	Habilitado

4.5.1. Configuración de los clientes inalámbricos mediante una directiva de grupo de Active Directory

Para automatizar la entrega de la configuración del cliente WLAN, se utilizó la directiva de grupo de Active Directory. El editor de directivas de grupo en Windows Server 2003 incluye un grupo de configuraciones denominado *Directiva de red inalámbrica*, que permite establecer configuraciones específicas para clientes de la WLAN que sean parte del dominio de Windows.

Para la creación de la directiva de grupo se siguieron los siguientes pasos:

1. En el servidor *apolo.cgsi.corp* se abrió la consola de administración *Usuarios y equipos de Active Directory* y se seleccionó el grupo de seguridad *Acceso WLAN*. Se hizo clic con el botón secundario en el objeto *Acceso WLAN* y se seleccionó *Propiedades*, como se muestra en la Figura 4-32.

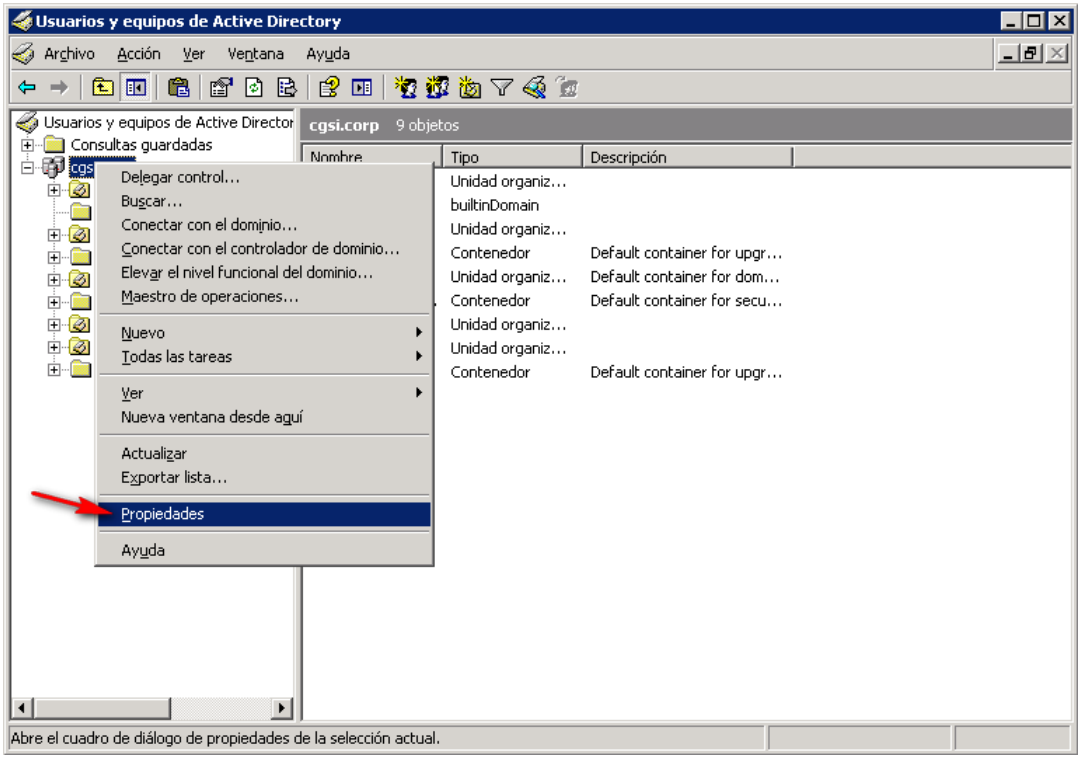

Figura 4-32. Selección de la opción *Propiedades* en la consola *Usuarios y equipos de Active Directory*

2. Se hizo clic en la ficha *Directiva de grupo* y, a continuación, en el botón *Nueva*. Se escribió *Configuración de clientes WLAN (GPO)* como nombre de objeto de directiva de grupo, como se muestra en la Figura 4-33.

3. Se hizo clic en el botón *Propiedades* y, a continuación, en la ficha *Seguridad*. Luego, se seleccionó *Usuarios autentificados* en la lista *Nombres de grupos o usuarios* y se hizo clic en el botón *Quitar*, como se muestra en la Figura 4-34.

4. Se hizo clic en *Agregar* y se buscó la opción *Configuración del equipo de LAN inalámbrica*. Luego se hizo clic en Aceptar. Luego, con el nombre del grupo *Configuración del equipo de LAN inalámbrica* resaltado en la lista *Nombres de grupos o usuarios*, se hizo clic en los permisos de *Lectura* y *Aplicar directiva de grupo* en la columna *Permitir* de la lista *Permisos*, como se muestra en la Figura 4-35.

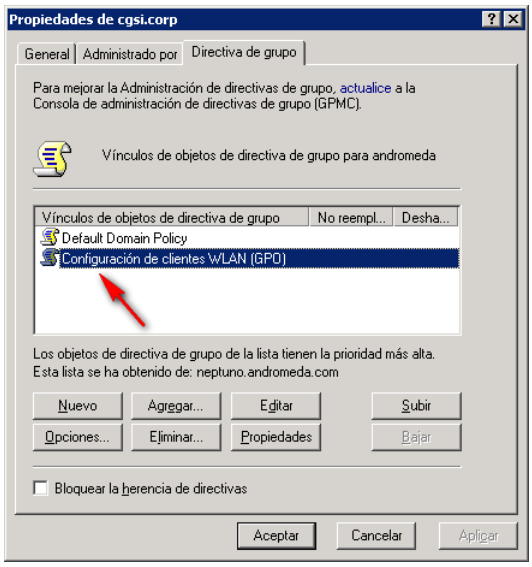

Figura 4-33. Creación de directiva de grupo

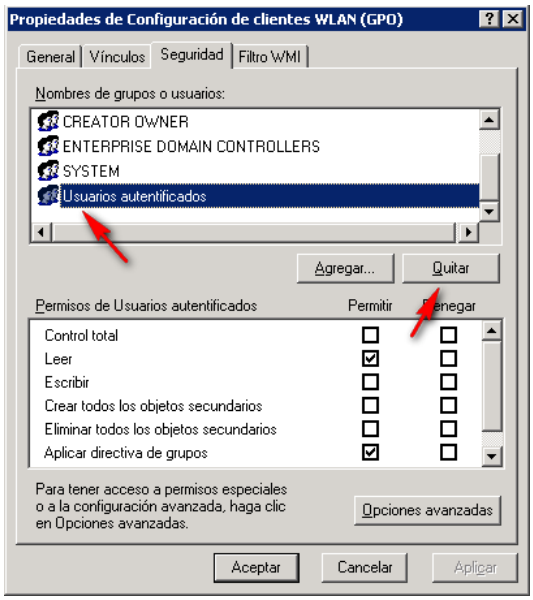

Figura 4-34. Propiedades de seguridad de la directiva de grupo

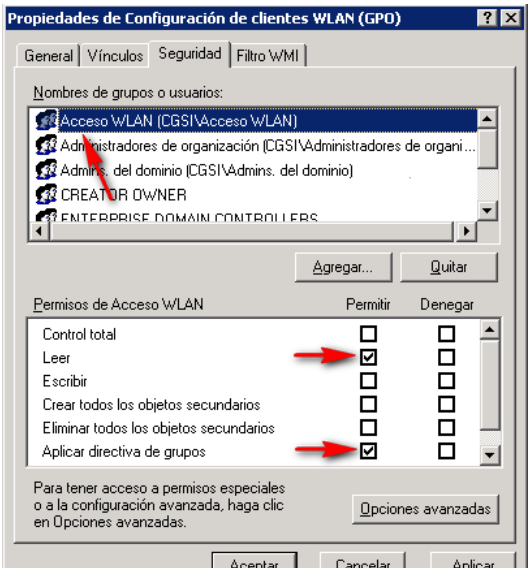

Figura 4-35. Agregar permisos en la directiva de grupo a Acceso WLAN

5. Se hizo clic en la ficha *General* y en *Deshabilitar los parámetros de configuración de usuario*, como se muestra en la Figura 4-36. Luego, se hizo clic en *Aceptar* para aplicar los cambios y cerrar la ventana de propiedades del objeto de directiva de grupo.

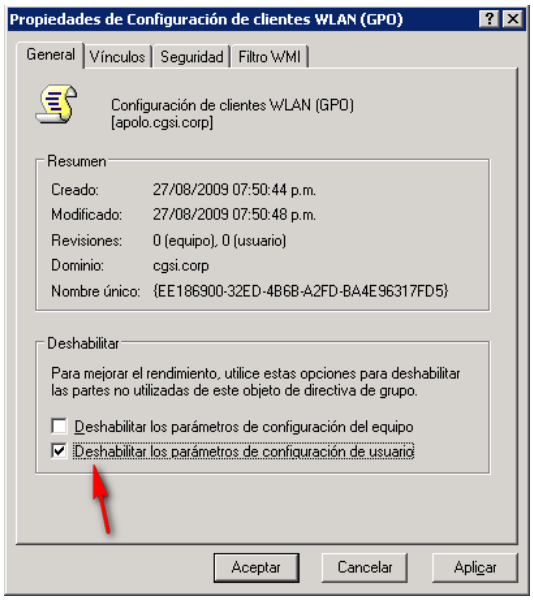

Figura 4-36. Deshabilitar parámetros de configuración de usuario

6. Se hizo clic en el botón *Editar* para modificar la directiva y se desplazó hasta *\Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas de red inalámbrica (IEEE 802.11)*. Luego, se seleccionó el objeto *Directivas de red inalámbrica (IEEE 802.11)* en el panel de exploración y, a continuación, se seleccionó *Crear directiva de red inalámbrica* en el menú *Acción*, como se muestra en la Figura 4-37.

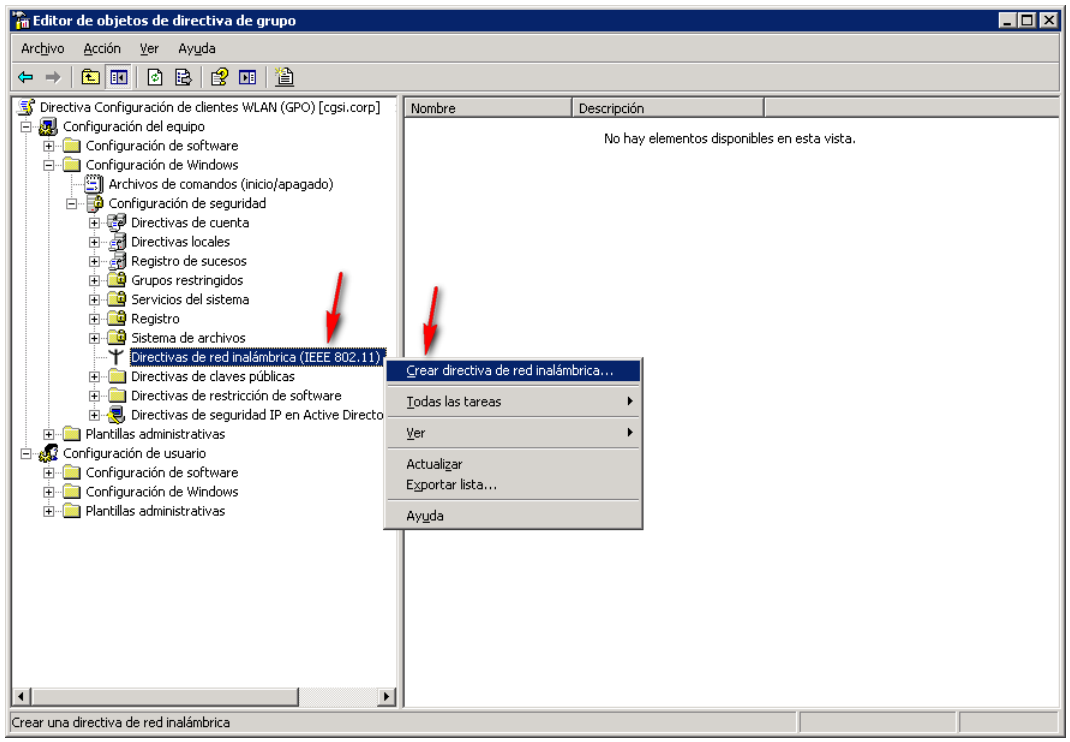

Figura 4-37. Crear directiva de red inalámbrica

7. Se utilizó el asistente para llamar a la directiva *Configuración de clientes WLAN (PEAP-WPA2)*. Se dejó seleccionada la casilla de verificación *Modificar propiedades* y, a continuación, se hizo clic en *Finalizar* para cerrar el asistente.

8. Se hizo clic en la ficha *Redes preferidas* y, a continuación, se hizo clic en *Agregar* para agregar una nueva red preferida. Como se muestra en la Figura 4-38, en el campo *Nombre de red (SSID)*, se escribió el nombre de la red inalámbrica, *CORP_WLAN y* en el campo *Descripción*, se escribió una descripción de la red: *Red WLAN de C.G.S.I., C.A.* Luego, en el campo *Autenticación de red* se seleccionó *WPA2* y en *Cifrado de datos* se seleccionó *AES*.

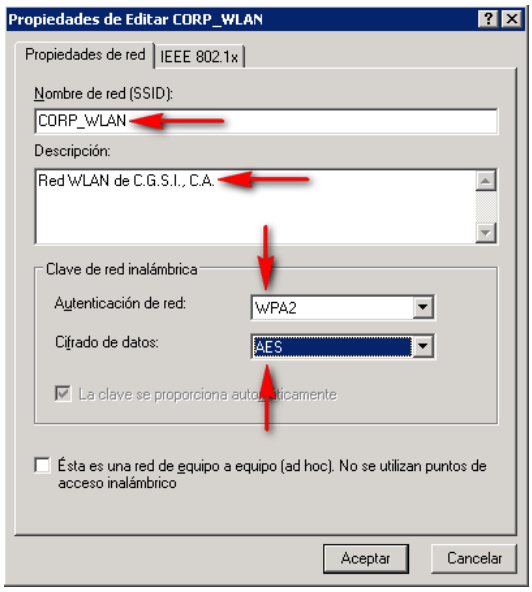

Figura 4-38. Propiedades de red para CORP_WLAN en la directiva de grupo

9. Se hizo clic en la ficha *IEEE 802.1X* y se seleccionó *EAP protegido (PEAP)* en la lista desplegable *Tipo de EAP*, como se muestra en la Figura 4-39.

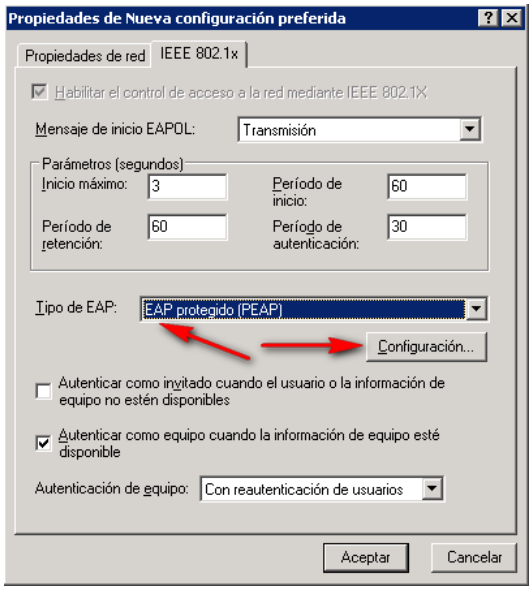

Figura 4-39. Propiedades de IEEE 802.1X en la directiva de grupo

10. Se hizo clic en el botón *Configuración* para modificar la configuración PEAP. En la lista *Entidades emisoras raíz confiables*, se seleccionó el certificado de entidad emisora raíz de la entidad emisora que se instaló previamente, *CGSI_Cert_Authority*.

Luego, Se seleccionó *Contraseña segura (EAP-MSCHAP v2)* en *Seleccione el método de autenticación* y se seleccionó la opción *Habilitar reconexión rápida*, como se muestra en la Figura 4-40.

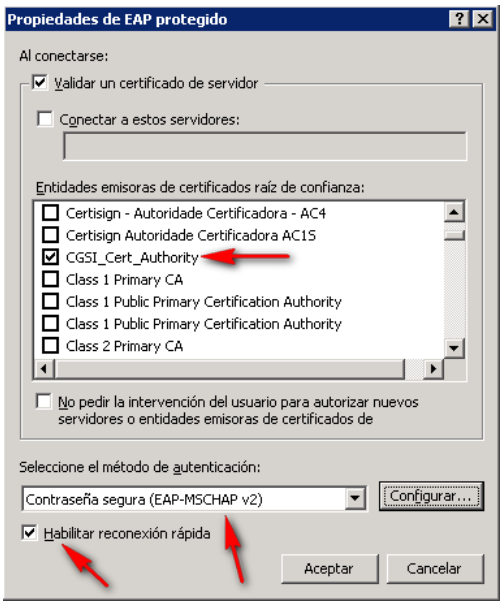

Figura 4-40. Propiedades de EAP protegido en la directiva de grupo

11. Se hizo clic en el botón *Configurar* y se seleccionó *Usar automáticamente el nombre de inicio de sesión y la contraseña de Windows (y dominio, si existe alguno)*, como se muestra en la Figura 4-41.

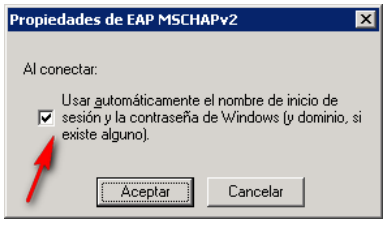

Figura 4-41. Propiedades de EAP MSCHAPv2 en la directiva de grupo

12. Se cerró cada una de las ventanas de propiedades haciendo clic en *Aceptar*, así como el editor del objeto de directiva de grupo y la consola *Usuarios y equipos de Active Directory*.

4.5.2. Configuración manual de los clientes inalámbricos

En aquellos casos donde sea necesario la configuración manual de los clientes inalámbricos, existe un procedimiento alternativo que puede ejecutarse directamente en estos dispositivos.

Se procedió a configurar uno de los clientes inalámbricos usando este procedimiento, que estuvo basado en los siguientes pasos:

1. En uno de los clientes inalámbricos Windows XP, *rforsyth.cgsi.corp*, se abrió el cuadro de diálogo *Propiedades de Conexiones de red inalámbrica* y se seleccionó la pestaña *Redes inalámbricas*, como se muestra en la Figura 4-42. Luego, se hizo clic en el botón *Agregar*.

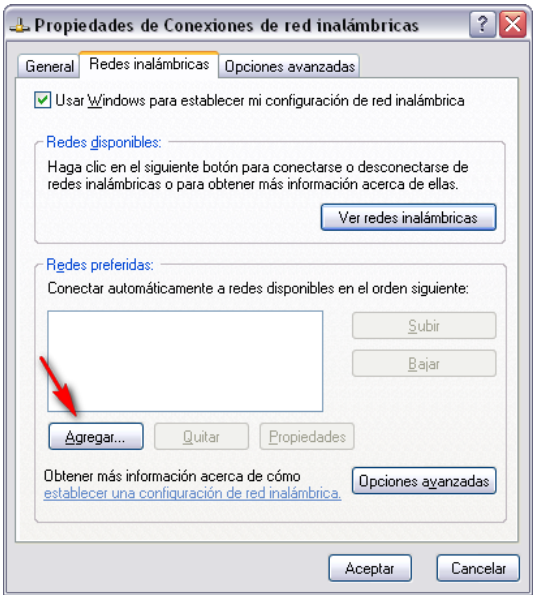

Figura 4-42. Propiedades de redes inalámbricas en un cliente Windows XP

2. En la pestaña *Asociación* del cuadro de diálogo *Propiedades de red inalámbrica*, se escribió el nombre de la red inalámbrica, *CORP_WLAN*, en el campo *Nombre de red (SSID)*, Luego, en el campo *Autenticación de red* se seleccionó *WPA2* y en *Cifrado de datos* se seleccionó *AES*, como se muestra en la Figura 4-43.

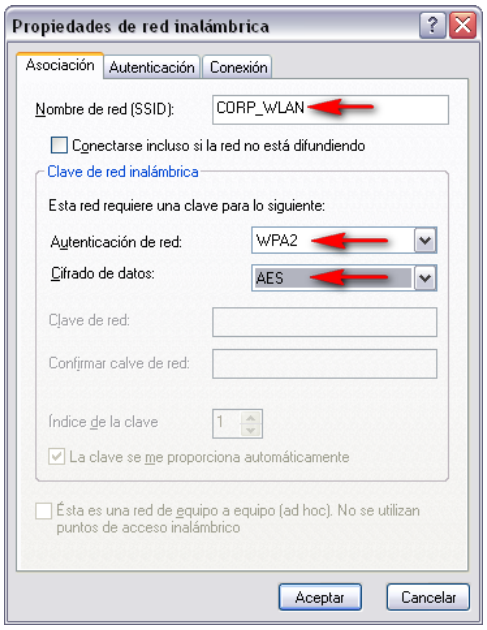

Figura 4-43. Propiedades de asociación en un cliente Windows XP

3. En la pestaña *Autenticación*, se seleccionó *EAP protegido (PEAP)* en *Tipo de EAP*, como se muestra en la Figura 4-44.

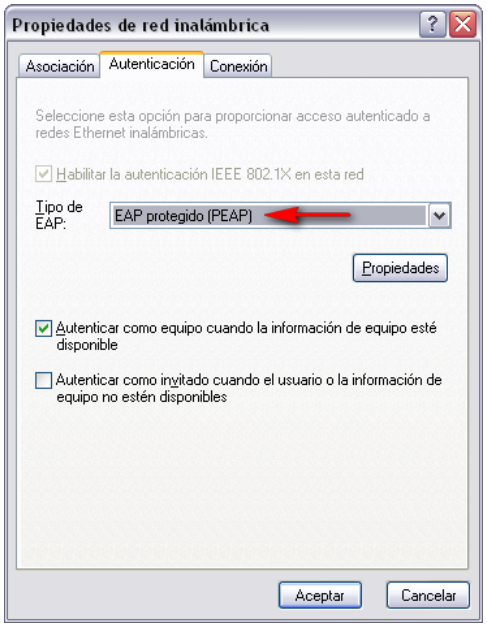

Figura 4-44. Propiedades de autenticación en un cliente Windows XP

4. Se hizo clic en el botón *Propiedades*, y en el cuadro de diálogo *Propiedades protegidas de EAP* se seleccionó el certificado de entidad emisora raíz de la entidad emisora que se instaló previamente, *CGSI_Cert_Authority, de* la lista *Entidades emisoras raíz confiables*. Luego, se seleccionó *Contraseña segura (EAP-MSCHAP v2)* en *Seleccione el método de autenticación* y se seleccionó la opción *Habilitar reconexión rápida*, como se muestra en la Figura 4-45.

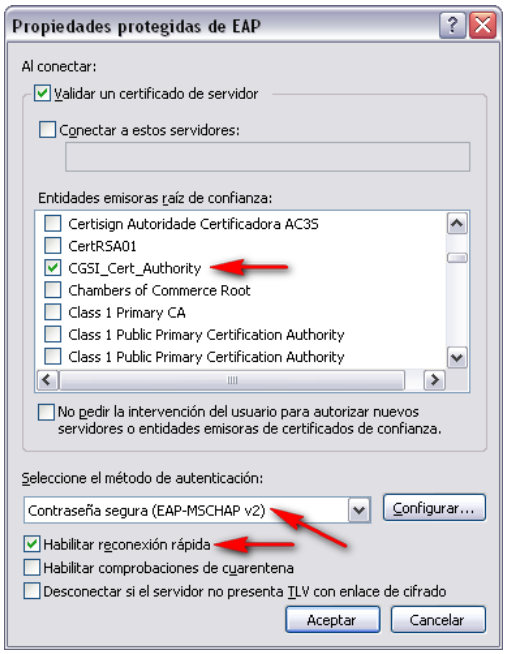

Figura 4-45. Propiedades protegidas de EAP en un cliente Windows XP

5. Se hizo clic en el botón *Configurar* y se seleccionó *Usar automáticamente el nombre de inicio de sesión y la contraseña de Windows (y dominio, si existe alguno)*, como se muestra en la Figura 4-46.

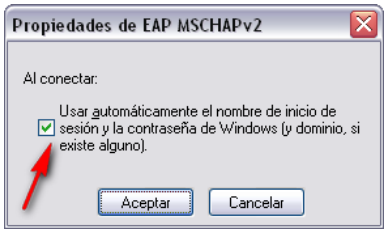

Figura 4-46. Propiedades de EAP MSCHAPv2 en un cliente Windows XP

6. Finalmente, se cerró cada una de las ventanas de propiedades haciendo clic en *Aceptar*.

Capítulo 5

Pruebas y análisis de resultados

Este capítulo plantea diversos escenarios de pruebas que validan el apego al diseño especificado en este Trabajo Especial de Grado y la correcta operación de la red WLAN implementada en C.G.S.I., C.A. Cada escenario busca verificar el funcionamiento de los diferentes componentes, tanto a nivel de arquitectura de seguridad, como a nivel de arquitectura funcional, presentando un breve análisis sobre los resultados obtenidos.

5.1. Escenario de prueba 1: Comprobación de la implementación de certificados de servidor IAS

- ***Descripción del escenario:*** en este escenario se comprueba que una vez instalado y configurado el servicio IAS en ambos servidores de dominio, éstos reciben el certificado de autenticación de servidor con inscripción automática de la entidad emisora de certificados digitales.

- ***Ejecución de la prueba:*** esta prueba está basada en la ejecución de los siguientes pasos:

1. En el servidor de dominio *apolo.cgsi.corp*, se abrió una línea de comandos de Windows, y se ejecutó el comando *ComputerCerts.msc* para abrir la consola de administración de *Certificates Services*.

2. Se comprobó que al navegar por el árbol de la consola, hacia *Certificados (equipo local)* → *Personal* → *Certificados*, aparecen certificados con el nombre de los servidores donde se encuentra instalado IAS en la columna *Emitido para* y el nombre de la entidad emisora en la columna *Emitido por*. Al desplazarse por la lista mostrada, se debe comprobar que el valor de la *Plantilla de certificado* sea *Equipo* para este certificado.

3. Si el certificado necesario no aparece en la consola de administración de certificados, es necesario seleccionar *Certificados (equipo local)* en el árbol de la consola del panel de la izquierda, hacer clic en *Todas las tareas* en el menú *Acción* y, a continuación, hacer clic en *Inscribir certificados automáticamente*. A continuación, debe actualizarse la vista de la consola de certificados.

- ***Resultados obtenidos:*** la Figura 5-1 y la Figura 5-2 muestran los certificados digitales emitidos para los servidores de domino, *apolo.cgsi.corp* y *poseidon.cgsi.corp*, donde se encuentra instalado el servicio de autenticación IAS. Los certificados tienen como fecha de vencimiento el 27 de agosto de 2010. Según la configuración establecida, un mes antes de su vencimiento, la autoridad certificadora debería emitir automáticamente un nuevo certificado digital para estos servidores.

- ***Análisis de los resultados:*** al contarse con certificados digitales válidos para los servidores de donde se ejecuta el servicio IAS, se está dotando al componente de autenticación de un mecanismo a través del cual demostrar su identidad contra los clientes inalámbricos, habilitando de esta manera la autenticación mutua. Con esto queda validado el funcionamiento correcto de la infraestructura de clave pública (PKI) implementada en C.G.S.I., C.A. como parte de la arquitectura de seguridad de la red inalámbrica.

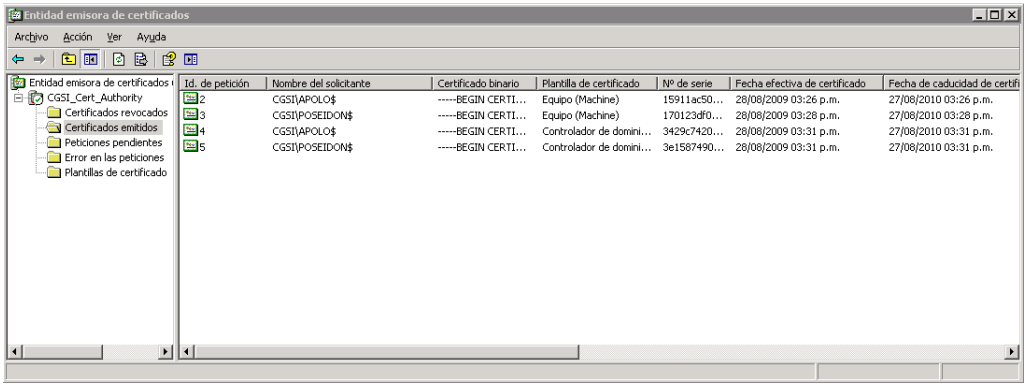

Figura 5-1. Consola de gestión de la entidad emisora de certificados

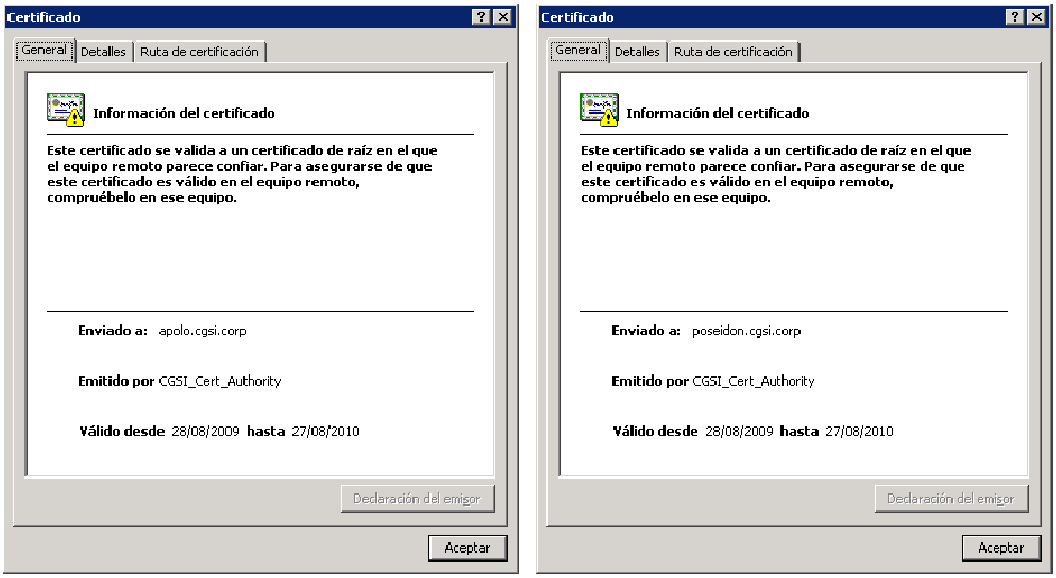

Figura 5-2. Certificados emitidos a los servidores de dominio

5.2. Escenario de prueba 2: Comprobación del certificado de entidad emisora raíz en los clientes inalámbricos Windows XP

- ***Descripción del escenario:*** en este escenario se comprueba que un cliente inalámbrico Windows XP válido recibe el certificado raíz de la entidad emisora de red en el almacén de entidades emisoras raíz de confianza. Este certificado se descarga y se agrega al almacén cuando se actualiza la directiva de grupo.

- ***Ejecución de la prueba:*** esta prueba está basada en la ejecución de los siguientes pasos:

    1. En uno de los clientes Windows XP, se abrió una consola de línea de comandos de Windows, y se ejecutó el comando *MMC.exe* para abrir la consola de administración de Microsoft (MMC).

    2. Desde el menú *Archivo* de MMC, se seleccionó *Agregar o quitar complemento*.

    3. En la ventana *Agregar o quitar complemento*, se hizo clic en el botón *Agregar*. Se seleccionó el elemento *Certificados* en la lista de complementos disponibles.

Luego se seleccionó *Cuenta de equipo*, se hizo clic en *Siguiente* y, a continuación, en *Finalizar*.

4. Se cerraron las ventanas *Agregar un complemento independiente* y *Agregar o quitar complemento*.

5. En el panel izquierdo, se desplazó hasta *Certificados (equipo local)\Entidades emisoras raíz confiables\Certificados*.

6. Se buscó el certificado de la entidad emisora, que aparecía con el nombre que se le proporcionó durante la instalación.

7. Si el certificado no aparece en la lista, se debe ejecutar el comando *Gpupdate /force* en un símbolo del sistema para forzar la actualización. Luego, debe volverse a la MMC de Certificados y hacer clic con el botón secundario en el nodo *Certificados (equipo local)*, seleccionar *Actualizar* y volver a comprobar si aparece el certificado de la entidad emisora.

- ***Resultados obtenidos:*** la Figura 5-3 y la Figura 5-4 muestran que el certificado de la entidad emisora raíz *CGSI_Cert_Authority* se encuentra presente en el cliente inalámbrico Windows XP. Esta prueba se repitió en otros tres clientes Windows XP y en un cliente Windows Vista con resultado exitoso.

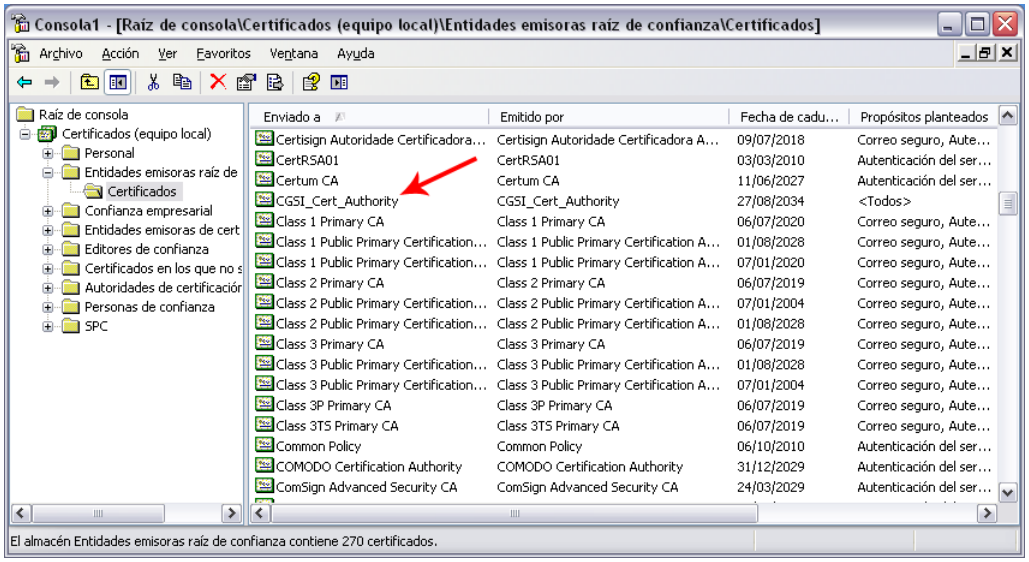

Figura 5-3. Certificados raíz de entidades emisoras en uno de los clientes Windows XP

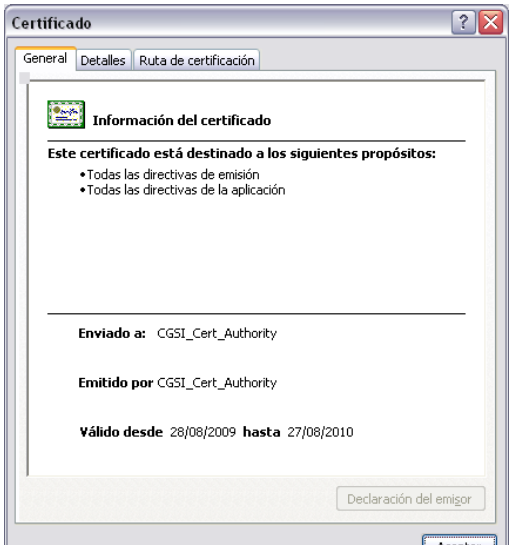

Figura 5-4. Certificado raíz de la entidad emisora CGSI_Cert_Authority

- ***Análisis de los resultados:*** al verificar que el certificado de la entidad emisora raíz se encuentra presente en los clientes inalámbricos, se está permitiendo que estos puedan comprobar la validez del certificado que presenta el servidor de autenticación IAS al cliente inalámbrico para realizar la autenticación mutua.

5.3. Escenario de prueba 3: Comprobación de la autenticación de usuarios en la red inalámbrica

- ***Descripción del escenario:*** en este escenario se comprueba que un usuario de la WLAN puede autenticarse y conectarse a la red después de instalar y configurar la solución. Éste puede considerarse el escenario de prueba más importante, ya que para que éste funcione deben estar operando correctamente todos los componentes de la red WLAN implementada.

- ***Ejecución de la prueba:*** esta prueba está basada en la ejecución de los siguientes pasos:

1. Un usuario del dominio, miembro del grupo *Usuarios WLAN*, en este caso el usuario *rforsyth*, inició sesión en un equipo cliente con una interfaz de red

inalámbrica instalada y sin que estuviera conectado a la red cableada. El usuario proporcionó sus credenciales del dominio durante el inicio de sesión.

2. Se abrió el panel *Conexiones de red* desde el *Panel de control* y se comprobó el estado de las *Conexiones de red inalámbricas*. Se mostraba el estado *Conectado* para la conexión inalámbrica.

3. Desde el símbolo del sistema, se utilizó el comando *ping* para comprobar la conexión a través de la red con un equipo interno, la puerta de enlace de la subred, y un equipo externo, un servidor DNS público.

4. En el servidor *apolo.cgsi.corp*, donde está instalado el servicio IAS primario, se abrió el *Visor de sucesos*. El registro de sucesos del Sistema contenía al menos un registro IAS de tipo de información con ID de suceso 1. Al examinar la descripción del registro, éste incluía los detalles de autenticación del usuario.

- ***Resultados obtenidos:*** la Figura 5-5, la Figura 5-6 y la Figura 5-7 constituyen evidencia que demuestra que un usuario autorizado puede autenticarse y conectarse exitosamente en la red WLAN implementada. En primer lugar se muestra el estado de la conexión inalámbrica para el equipo desde el que se conectó el usuario. Luego, estando ya conectado en la red es posible establecer comunicación, mediante el uso del comando *ping* tanto a un equipo de la red interna como a un equipo púbico de Internet. Finalmente, para validar la correcta autenticación del usuario en la WLAN se muestra el registro de suceso, que indica el estatus de acceso concedido a la red. Igualmente, esta prueba se repitió en otros tres clientes Windows XP y en un cliente Windows Vista con resultado exitoso.

- ***Análisis de los resultados:*** El hecho de que se pueda hacer *ping* desde un cliente inalámbrico hacia un dispositivo de la red interna, e incluso a un dispositivo en Internet, requiere que previamente se hayan completado los procesos de autenticación, intercambio de claves y conexión a la red WLAN. Los resultados muestran que estos procesos se están llevando a cabo de manera satisfactoria, de manera que todos los componentes de la arquitectura de red inalámbrica están operando correctamente.

Figura 5-5. Estado de la conexión en uno de los clientes inalámbricos Windows XP

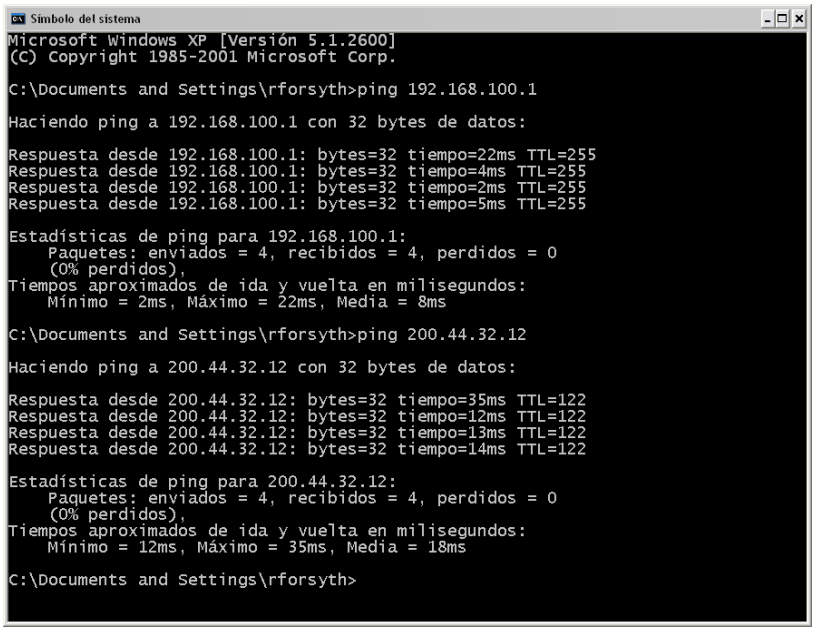

Figura 5-6. Resultados de ping desde uno de los clientes inalámbricos Windows XP

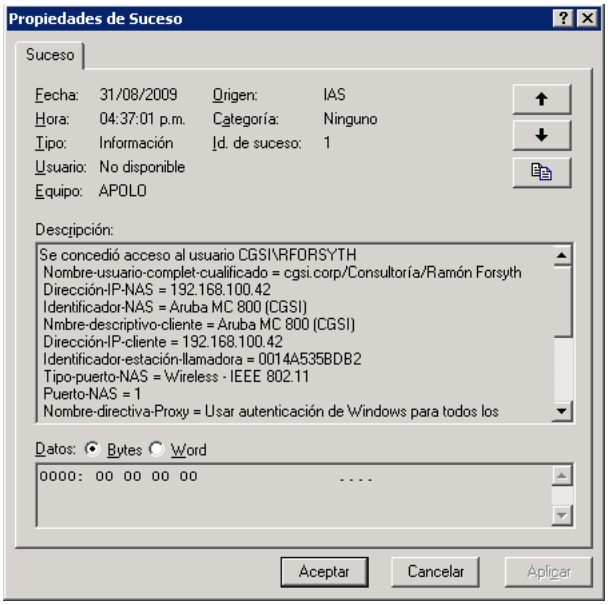

Figura 5-7. Registro de suceso del sistema para autenticación exitosa de un usuario en la WLAN

5.4. Escenario de prueba 4: Comprobación de la autenticación de equipos en la red inalámbrica

- ***Descripción del escenario:*** en este escenario se comprueba que se ha autenticado un equipo en la red WLAN cuando el usuario no ha iniciado una sesión.

- ***Ejecución de la prueba:*** esta prueba está basada en la ejecución de los siguientes pasos:

1. Se reinició un cliente inalámbrico, miembro del grupo *Equipos WLAN*; en este caso, el equipo *rforsyth.cgsi.corp*. Este equipo cuenta con una interfaz de red inalámbrica instalada y no estaba conectado a la red cableada.

2. Cuando apareció el mensaje de inicio de sesión, no se inició la sesión y se dejó el equipo inactivo durante unos minutos.

3. En el servidor *apolo.cgsi.corp*, donde está instalado el servicio IAS primario, se abrió el *Visor de sucesos*. El registro de sucesos del Sistema contenía al menos

un registro IAS de tipo de información con ID de suceso 1 para el nombre de host del equipo. Al examinar la descripción del registro, éste incluía los detalles de autenticación del equipo.

- ***Resultados obtenidos:*** la Figura 5-8 muestra el registro de suceso que se generó tras la autenticación del cliente inalámbrico, usando las credenciales del dominio para el equipo. Esta prueba se repitió en otro cliente Windows XP y en un cliente Windows Vista con resultado exitoso.

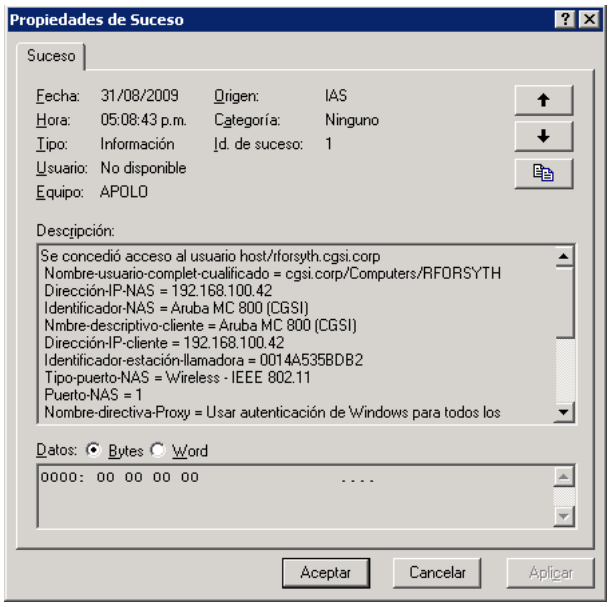

Figura 5-8. Registro de suceso del sistema para autenticación exitosa de un equipo en la WLAN

- ***Análisis de los resultados:*** para permitir que los clientes inalámbricos pudieran tener acceso a la red corporativa, de manera que puedan realizarse operaciones típicas de un ambiente Active Directory, era necesario permitir que pudieran autenticarse en la WLAN con las credenciales de equipo. Los resultados de esta prueba muestran que este proceso se lleva a cabo de manera satisfactoria.

5.5. Escenario de prueba 5: Re-autenticación del cliente inalámbrico porque se ha agotado el tiempo de espera de la sesión IAS

- ***Descripción del escenario:*** en este escenario se comprueba la rotación de claves dinámicas configuradas en la directiva de solicitud de conexión IAS. En esta prueba se verifica que los clientes se re-autentican periódicamente, después de cada hora de acuerdo a la configuración establecida, para que las claves de cifrado continúen cambiando.

- ***Ejecución de la prueba:*** esta prueba está basada en la ejecución de los siguientes pasos:

    1. Se Inició sesión en la red WLAN utilizando una cuenta de usuario de dominio con acceso autorizado, en este caso el usuario *rforsyth*. Luego se comprobó que la conexión de red se estableció correctamente.

    2. En el servidor *apolo.cgsi.corp*, donde está instalado el servicio IAS primario, se abrió el *Visor de sucesos*. El registro de sucesos del Sistema contenía al menos un registro IAS de tipo de información con ID de suceso 1. Al examinar la descripción del registro, éste incluía los detalles de autenticación del usuario.

    3. Se dejó al cliente conectado a la red un período de tiempo superior a una hora. Para comprobar que la conexión estuviera activa, se inició una solicitud ICMP continua hacia otro equipo de la red. En este caso se colocó un ping persistente hacia un equipo en la misma subred de la WLAN.

    4. Transcurrida la hora, se consultó nuevamente el registro de sucesos del Sistema en el servidor *apolo.cgsi.corp*. El registro de sucesos del Sistema contenía un nuevo registro IAS de tipo de información con ID de suceso 1. Al examinar la descripción del registro, éste incluía los detalles de re-autenticación del usuario.

- ***Resultados obtenidos:*** la Figura 5-9 muestra ambos registros de suceso para el mismo usuario, el de la autenticación original, y el de la re-autenticación una hora después. Esto demuestra que el proceso de re-autenticación automática, cada hora, se lleva a cabo de manera exitosa según lo configurado en el servicio IAS. Esta

prueba se repitió en otro cliente Windows XP y en un cliente Windows Vista con resultado exitoso.

- ***Análisis de los resultados:*** el proceso de re-autenticación automática es importante para garantizar la rotación de las claves maestras, de las cuales se derivan las claves AES que permiten el cifrado de cada trama de datos transmitida en la red WLAN. Esto incrementa el nivel de protección de la red inalámbrica, al evitar de manera contundente que se pueda llegar a repetir en algún momento alguna clave de cifrado.

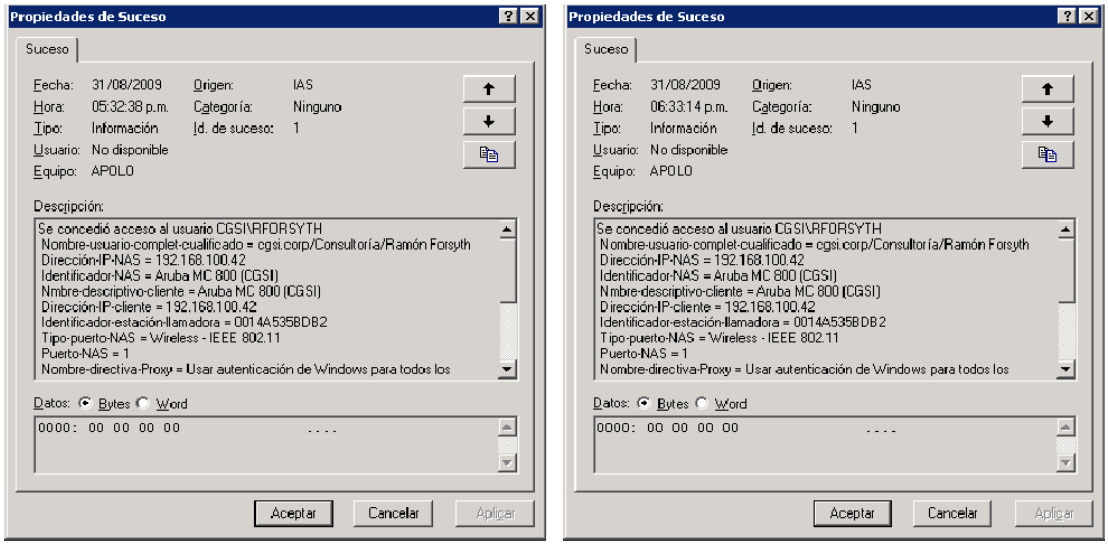

Figura 5-9. Registros de suceso para autenticación original de un usuario, y re-autenticación una hora después

5.6. Escenario de prueba 6: Acceso denegado si el usuario no es miembro del grupo de acceso a la WLAN

- ***Descripción del escenario:*** en este caso se comprueba que se deniega el acceso inalámbrico a la red a un usuario si no es miembro del grupo Usuarios WLAN. Este método es una alternativa al bloqueo del acceso inalámbrico del usuario a la red del escenario anterior.

- ***Ejecución de la prueba:*** esta prueba está basada en la ejecución de los siguientes pasos:

1. En uno de los servidores de dominio, *apolo.cgsi.corp*, se abrió la consola *Usuarios y equipos de Active Directory* en el panel *Herramientas administrativas*.

2. Se eliminó un usuario concreto del grupo Usuarios WLAN. En este caso se eliminó el usuario *rforsyth* del grupo.

3. El usuario inició sesión en un equipo cliente con una interfaz de red inalámbrica instalada y no estando conectado a la red cableada. El usuario introdujo las credenciales del dominio al iniciar sesión.

4. El usuario no pudo iniciar sesión en la red y apareció un mensaje de "error de autenticación".

5. En el servidor *apolo.cgsi.corp*, donde está instalado el servicio IAS primario, se abrió el *Visor de sucesos*. El registro de sucesos del Sistema contenía al menos un registro IAS de tipo de advertencia con ID de suceso 2. Al examinar la descripción del registro, éste incluía los detalles del error de autenticación del usuario.

- ***Resultados obtenidos:*** la Figura 5-10 muestra la ventana de estado de conexión a la red inalámbrica, donde se puede apreciar el mensaje de error de autenticación. Por otra parte, la Figura 5-11 muestra el registro de suceso generado por la denegación de acceso a la red WLAN.

Figura 5-10. Mensaje de error de autenticación

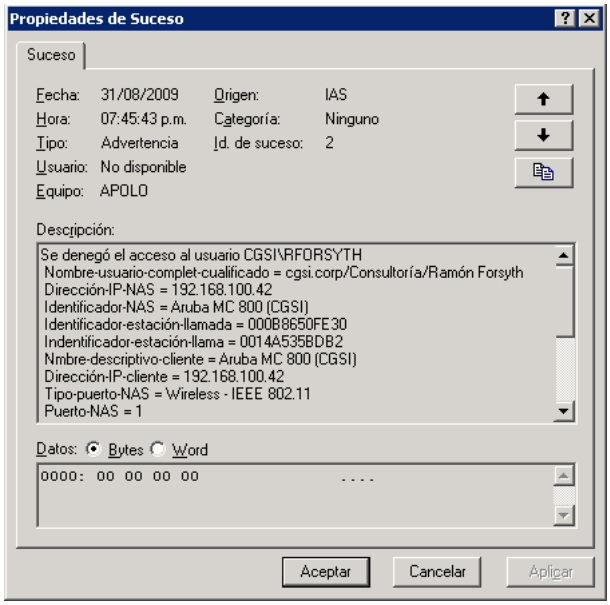

Figura 5-11. Registro de suceso del sistema para autenticación denegada de un usuario en la WLAN

- ***Análisis de los resultados:*** los resultados obtenidos demuestran el funcionamiento correcto del control de acceso a la red mediante la pertenecía a un grupo específico de usuarios. Esto permite garantizar que se puede controlar de manera efectiva cuáles de los usuarios del dominio de red de C.G.S.I., C.A. puede tener conectarse a la red WLAN.

5.7. Escenario de prueba 7: Comprobación de la redundancia del servicio IAS

- ***Descripción del escenario:*** en este escenario se comprueba la disponibilidad del servicio IAS en los clientes inalámbricos cuando uno de los servidores IAS no está disponible. Este tipo de errores no debería provocar la interrupción de la conexión con la red de los clientes inalámbricos. Éste es un escenario de prueba importante en el que se comprueba que el Mobility Controller de Aruba Networks cambia al servidor IAS secundario cuando el servidor IAS principal no está disponible.

- ***Ejecución de la prueba:*** esta prueba está basada en la ejecución de los siguientes pasos:

1. Se abrió la consola de administración del servicio IAS en el servidor de autenticación principal de la red, *apolo.cgsi.corp*, y se hizo clic en el nombre del servidor. A continuación, se detuvo el servicio IAS haciendo clic en el botón *Detener* de la barra de menús.

2. Se utilizó una cuenta de usuario de dominio con acceso autorizado a la WLAN, en este caso el usuario *rforsyth*, y se inició sesión en la red mediante una conexión inalámbrica.

3. El usuario pudo autenticarse en la red y conectarse correctamente a ella. Para comprobarlo, se abrió el panel *Conexiones de red* desde el *Panel de control* y se comprobó el estado de las conexiones de red inalámbricas. El estado mostraba la conexión satisfactoria a la red WLAN.

4. Desde el símbolo del sistema, se utilizó el comando *ping* para comprobar la conexión a través de la red con otro equipo de la misma.

5. En el servidor *poseidon.cgsi.corp*, donde está instalado el servicio IAS secundario, se abrió el *Visor de sucesos*. El registro de sucesos del Sistema contenía al menos un registro IAS de tipo de información con ID de suceso 1. Al examinar la descripción del registro, éste incluía los detalles de la autenticación del usuario.

- ***Resultados obtenidos:*** la Figura 5-12 muestra el registro de suceso de autenticación exitosa en el servidor IAS secundario.

- ***Análisis de los resultados:*** los resultados obtenidos demuestran que en caso de falla del servidor IAS primario, el proceso de autenticación pasa a ser ejecutado de manera transparente por el servidor IAS secundario. Con este esquema de redundancia se garantiza la robustez y la tolerancia a fallos del proceso de autenticación de la red WLAN implementada.

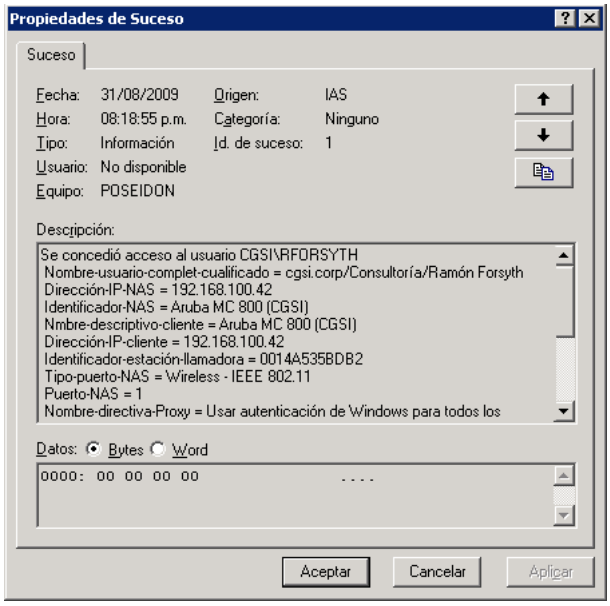

Figura 5-12. Registro de suceso del sistema para autenticación exitosa de un usuario usando el servidor IAS alterno

Conclusiones y recomendaciones

La movilidad, y con ella la tecnología de redes inalámbricas, tiene el potencial de exponer la red de cualquier organización a intrusos, fugas de información sensible o ataques de código malicioso. A medida que los dispositivos móviles se hacen más y más comunes dentro de los ambientes de red corporativos, también se incrementa la necesidad de brindar seguridad a la conectividad ofrecida a estos dispositivos.

Un diseño y planificación correctos pueden evitar, con un alto grado de certeza, estos inconvenientes. Claramente, el uso apropiado de esquemas de autenticación y cifrado, así como sistemas de detección y prevención de intrusos para redes inalámbricas, puede mitigar muchos de estos riesgos.

Mientras que una política de seguridad bien implementada puede hacer a una red inalámbrica incluso más segura que una red cableada, una mala implementación puede conducir a un completo desastre en términos de protección. Por ello, era imperioso para C.G.S.I., C.A. migrar desde su esquema anterior de red WLAN, con niveles bastante pobres de protección, hacia una red inalámbrica de tipo empresarial que ofreciera un grado de seguridad robusto.

Finalizadas las pruebas sobre la red WLAN diseñada e implementada para C.G.S.I., C.A. puede concluirse que se han cumplido exitosamente los objetivos y la metodología planteados para este Trabajo Especial de Grado.

Como producto del proceso de diseño e implementación, la empresa cuenta actualmente con una nueva red inalámbrica de área local completamente funcional, que está basada en el estándar IEEE 802.11 y en el esquema de seguridad WPA2-Enterprise, según establecía el objetivo general de este trabajo. Esta red inalámbrica ofrece un alto grado de confidencialidad, integridad y disponibilidad de los datos que por ella transitan, lo que se traduce en seguridad efectiva para la información sensible de la organización.

La empresa estableció inicialmente una serie de requerimientos específicos que delimitaban el alcance de este proyecto, y que fueron respetados durante el diseño de la red. Estos requerimientos nacieron internamente, producto del estudio de las necesidades y justificación de negocio de una nueva red WLAN para la empresa.

Es así que, cumplidas las actividades propuestas en la metodología, y en relación directa con los requerimientos de la organización, se puede afirmar que:

- Se implementó una red inalámbrica de área local (WLAN) basada en el estándar IEEE 802.11-2007, haciendo uso de dos de las especificaciones de capa física establecidas en éste, anteriormente conocidas como 802.11b y 802.11g. La conectividad mediante estas especificaciones de capa física está soportada en los clientes inalámbricos, así como en los puntos de acceso delgados que hacen parte de la infraestructura de la WLAN.

- Como esquema de seguridad para la red WLAN se implementó WPA2-Enterprise, consistente en autenticación basada en el estándar IEEE 802.1X, y en cifrado CCMP-AES. La arquitectura de seguridad, implementada con componentes de la plataforma Microsoft Windows Server preexistentes en la empresa, ofrece soporte para la autenticación 802.1X, incluyendo el servidor RADIUS y la autoridad certificadora que emitió el certificado digital para que éste pudiera validar su identidad contra los clientes inalámbricos. Una vez que se ha completado el proceso de autenticación y se ha autorizado el acceso a la red WLAN, se generan las llaves de cifrado que serán finalmente utilizadas por un determinado cliente inalámbrico y por el punto de acceso al cual éste se encuentre asociado, para establecer la confidencialidad de la comunicación.

- Para la implementación de la infraestructura de red inalámbrica se utilizaron dispositivos del fabricante Aruba Networks, consistentes de un equipo Mobility Controller MC-800, tres puntos de acceso AP-61 y un punto de acceso AP-70. Este equipamiento fue desplegado físicamente en las instalaciones de C.G.S.I., C.A., y configurado para permitir la comunicación de acuerdo a los esquemas de capa física seleccionados y a los requerimientos de seguridad de la red.

- Para la implementación de la arquitectura de seguridad de la red, se utilizaron elementos existentes en la plataforma informática de la empresa. El uso de estos componentes permitió el ahorro de costos en la adquisición de nuevo hardware y/o software.

- Se cuenta con una implementación de WLAN robusta que provee un alto nivel de rendimiento. La robustez de la red viene dada por la redundancia de elementos como los servidores IAS, así como el rango de cobertura solapada de los puntos de acceso inalámbricos. Por otro lado, la revisión de capa física 802.11g ofrece velocidades de conexión de hasta 54 Mbps, lo que se traduce en un nivel de rendimiento superior a las necesidades de los usuarios para sus labores habituales que implican acceso a la red corporativa.

- La red inalámbrica implementada es escalable en cuanto al número de clientes inalámbricos soportados, expansión de la cobertura, fácil adaptabilidad a nuevas especificaciones de capa física, entre otros elementos. Esta solución fue diseñada para admitir fácilmente nuevos clientes inalámbricos. La capacidad de los servidores IAS se encuentra bastante por debajo de los límites máximos recomendados, por lo que fácilmente pueden soportar una cantidad considerablemente mayor de clientes autenticándose contra ellos. Por otro lado, para dar soporte a una cantidad mayor de clientes inalámbricos o una cobertura de red mayor, es posible incorporar más puntos de acceso delgados al Aruba Controller MC-800. Este modelo de controlador soporta hasta 16 puntos de acceso. Tomando como referencia la recomendación del fabricante de tener un máximo de 25 clientes inalámbricos por cada punto de acceso, con este mismo controlador pudieran atenderse hasta unos 400 clientes inalámbricos. En cuanto a la cobertura sólo es necesario agregar físicamente nuevos puntos de acceso en aquellos lugares donde sea necesario proveer conectividad inalámbrica.

- La WLAN sólo brinda conectividad a computadoras portátiles (*laptops*) bajo plataforma Microsoft Windows. De acuerdo al requerimiento establecido se excluyeron del proceso de diseño el soporte a equipos como PDAs, teléfonos celulares con capacidad WLAN, y cualquier otro tipo de dispositivos y plataformas. Dado que el control de acceso a la red se lleva a cabo mediante grupos destinados para tal fin en el servicio Active Directory, es fácil controlar quién accede o no a la red inalámbrica de la empresa. Necesariamente se debe ser parte del dominio y pertenecer al grupo autorizado, bien sea el usuario o el dispositivo, para poder tener acceso a la red, con lo que es fácil dar cumplimiento a este requerimiento.

Limitaciones

Entre las limitaciones que se hallaron durante el desarrollo de este Trabajo Especial de grado se encuentran:

- Debido al hecho de que el equipamiento del fabricante Aruba Netowrks, utilizado para la implementación de la infraestructura de conectividad de la red WLAN, ya había sido seleccionado y adquirido previo al inicio de este proyecto, no se tuvo la oportunidad de evaluar las bondades de otro tipo de dispositivos y arquitecturas existentes en el mercado, desarrolladas por diferentes fabricantes.

- La red WLAN implementada ofrece redundancia a nivel del esquema de autenticación, debido a la instalación del servicio IAS en los dos controladores de dominio de la organización. Sin embargo, la existencia de un único dispositivo Aruba Controller, que funge como ente centralizador de toda la comunicación de los clientes inalámbricos, introduce un punto único de falla a nivel de la arquitectura de conectividad. En caso de error o malfuncionamiento del controlador, no existe un segundo dispositivo que pueda asumir la labor de procesamiento del tráfico de la WLAN.

- Dada la proliferación de dispositivos con capacidades Wi-Fi, incluyendo PDAs, teléfonos celulares, teléfonos VoIP, entre otros, el hecho de que no se brinde acceso a otro tipo de dispositivos más que *laptops* bajo plataforma Microsoft Windows, limita el aprovechamiento que se pudiera hacer de la infraestructura WLAN implementada.

Trabajos futuros

Algunas de las mejoras y funcionalidades adicionales que pudieran implementarse en la red WLAN de C.G.S.I, C.A. incluyen:

- En esta implementación de WLAN, los clientes inalámbricos, una vez autenticados, son colocados en el mismo segmento de red LAN que el resto de la red cableada y comparten la misma subred IP. Como recomendación para trabajos futuros, se podría separar la red inalámbrica en una VLAN (*Virtual LAN*) y subred IP dedicadas,

para segmentar física y lógicamente las conexiones cableadas de las conexiones inalámbricas.

- También podría implementarse acceso para invitados, incorporando un nuevo SSID a la red y redirigiendo a los usuarios que deseen acceder a dicha red hacia un portal captativo (*captive portal*) de autenticación, aprovechando las facilidades provistas por el equipamiento de Aruba Networks. Dentro del esquema de acceso para invitados podría contemplarse brindar conectividad a dispositivos PDA y teléfonos con capacidad Wi-Fi, actualmente no soportados por la red WLAN de la empresa.

- El modelo de red inalámbrica centralizada de Aruba Networks contempla la posibilidad de utilizar controladores redundantes, que se valen de protocolos estándares como VRRP (*Virtual Router Redundancy Protocol*, Protocolo de Redundancia de Enrutador Virtual) para conmutar todas la conexiones establecidas hacia el segundo controlador, en caso de falla del controlador primario. Corresponde a la empresa sopesar el costo de adquisición de un segundo Aruba Controller versus la posibilidad de contar con redundancia a nivel de este componente crítico de la arquitectura de conectividad.

Recomendaciones finales

El campo de la seguridad de la información es en extremo dinámico. Cada día surgen nuevos tipos de ataques que amenazan los esquemas de protección más recientes; aquellos que hoy se creen virtualmente invulnerables. Esto conduce a la creación de mecanismos de seguridad más robustos para los que eventualmente surgirán ataques que los dejarán obsoletos; y así sucesivamente. Este ciclo no pareciera tener un final a corto plazo.

Es por ello que se debe estar constantemente actualizado en cuanto a nuevos retos para la seguridad de redes inalámbricas y los nuevos esquemas de protección que vayan surgiendo, para irlos incorporando en tanto sea factible. Un ejemplo de ello es la recién aprobada extensión IEEE 802.11w que ofrece protección a las tramas de gestión de las redes 802.11.

De cualquier manera, al día de hoy, el esquema de seguridad WPA2-Enterprise ofrece un grado de protección a las redes inalámbricas que es sustancialmente superior, inclusive, al de las redes LAN cableadas. Una recomendación en este sentido es que las nuevas

implementaciones de redes WLAN hagan uso de este esquema, mientras que las implementaciones existentes deben buscar ser migradas, en la medida de lo posible, con el objeto de garantizar el mayor nivel de resguardo disponible.

Existen actualmente en el mercado dispositivos de conectividad de redes WLAN orientados a ambientes empresariales, como los utilizados en este Trabajo Especial de Grado, que ofrecen los niveles de seguridad, robustez, rendimiento y escalabilidad requeridos por cualquier organización que, como C.G.S.I., C.A., deba ofrecer un alto grado de confidencialidad, integridad y disponibilidad de su información. Estos dispositivos cuentan además con las certificaciones de cumplimiento con los estándares e interoperabilidad con otros dispositivos.

Por otra parte, los sistemas operativos modernos, basados en software libre o propietario, ofrecen soporte integrado a los esquemas de autenticación y cifrado requeridos en este tipo de redes empresariales, tales como IEEE 802.1X y AES. Además, se integran de manera sencilla con servicios de directorio comunes como LDAP o Active Directory, para facilitar la gestión de los clientes inalámbricos.

De manera que las condiciones, al menos a nivel tecnológico y de disponibilidad de mercado, están dadas para que puedan aprovecharse todas las ventajas asociadas a las redes WLAN, sin comprometer la seguridad de la información de las organizaciones que hacen uso de ellas.

Referencias bibliográficas

[1] Aboba, B., et al., *Extensible Authentication Protocol (EAP)*. RFC 3748, Junio de 2004.

[2] Aboba, B., Stanley, D., Walker, J., *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs*. RFC 4017, Marzo de 2005.

[3] Aboba, B., Simon, D., *PPP EAP TLS Authentication Protocol*. RFC 2716, Octubre de 1999.

[4] ANSI/IEEE, *Std 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999 edition*., 1999.

[5] Aruba Networks, *Best Practices Guides: WLAN Base Configuration*, Marzo de 2007.

[6] Aruba Networks, *Campus Wireless Networks Validated Reference Design Version 3.3.2*, 2009.

[7] Aruba Networks, *Network Design & Install Best Practices*, Junio de 2005.

[8] Aruba Networks, *Wireless Security Design Best Practices*, Mayo de 2005.

[9] Borisov, N., Goldberg, I., Wagner, D., *Intercepting Mobile Communications: The Insecurity of 802.11*. Proceedings of the 7th annual international conference on Mobile computing and networking, Julio de 2001.

[10] Davies, J., *Deploying Secure 802.11 Wireless Networks with Microsoft Windows*. 1ra. edición, Microsoft Press, 2004.

[11] De La Rosa, J., *Seguridad en redes inalámbricas IEEE 802.11 (WLAN) con WEP mejorado*. Tesis de pregrado, Universidad de las Américas, Campus de Puebla, México, Julio de 2006.

[12] Fioretti, R., *Estudio de seguridad de la red inalámbrica de la Facultad de Ciencias de la UCV*. Trabajo Especial de Grado, Facultad de Ciencias de la Universidad Central de Venezuela, Octubre de 2006.

[13] Gast, M., *802.11 Wireless Networks: The Definitive Guide*. 2da. edición, O'Reilly, Abril de 2005.

[14] Helleseth, H., *Wi-Fi security: how to break and exploit*. Tesis de maestría, Universidad de Bergen, Noruega, Marzo de 2006.

[15] IEEE 802.11 Wireless LAN Working Group. Sitio Web.
URL: *http://grouper.ieee.org/groups/802/11/*
Consultado: 25/08/2009.

[16] IEEE, *IEEE 802.11n-2009. Standard for Information technology— Telecommunications and information exchange between systems - Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) & Physical Layer specifications E*. Octubre 2009.

[17] IEEE. *IEEE Ratifies 802.11n, Wireless LAN Specification to Provide Significantly Improved Data Throughput and Range*. Artículo en línea.
URL: *http://standards.ieee.org/announcements/ieee802.11n_2009amendment_ratified.html*
Publicado: 11/09/2009.
Consultado: 14/09/2009.

[18] IEEE. *Quick Guide To IEEE 802.11 WG & Activities*. Sitio Web.
URL: *http://www.ieee802.org/11/QuickGuide_IEEE_802_WG_and_Activities.htm.*
Consultado: 25/08/2009.

[19] IEEE, *Std 802.11-1997: Information Technology- telecommunications and information exchange between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications*. Noviembre de 1997.

[20] IEEE, *Std 802.11-2007: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*., Junio de 2007.

[21] IEEE, *Std 802.11i-2004: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements*. Julio de 2004.

[22] IEEE, *Std 802.1X-2004: Port-Based Network Access Control*., Diciembre de 2004.

[23] Institute of Electrical and Electronics Engineers (IEEE). Sitio Web.
URL: *http://www.ieee.org/*
Consultado: 25/08/2009.

[24] ISO. *JTC 1/SC 27. Information Technologies - Security techniques Standards Commite*. Sitio Web.
URL: *http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306*
Consultado: 25/08/2009.

[25] Layton, T., *Information Security: Design, Implementation, Measurement, and Compliance*, 1ra. edición, Auerbach Publications, 2007.

[26] Maguiña, J., Ries, F., *Implementación de una solución de seguridad para la red inalámbrica de la Facultad de Ciencias*. Trabajo Especial de Grado, Facultad de Ciencias de la Universidad Central de Venezuela, Julio de 2007.

[27] Marín, J., *El valor de la información en la empresa moderna*. Revista Estrategia Financiera, N°259, pp. 51-53, Marzo de 2009.

[28] Microsoft Corporation, *IEEE 802.11 Wireless LAN Security with Microsoft Windows*. Enero de 2008.

[29] Microsoft Corporation, *Microsoft Solutions for Security: Choosing a Strategy for Wireless LAN Security*. Marzo de 2005.

[30] Microsoft Corporation, *Microsoft Solutions for Security: Securing Wireless LANs with PEAP and Passwords*. Marzo de 2005.

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

[32] NIST. *Federal Information Processing Standards Publications*. Sitio Web.
URL: *http://www.itl.nist.gov/fipspubs/*
Consultado: 25/08/2009.

[33] Rigney, C., *RADIUS Accounting*. RFC 2866, Junio de 2000.

[34] Rigney, C., et al, *Remote Authentication Dial In User Service (RADIUS)*. RFC 2865, Junio de 2000.

[35] SANS Institute. *Glossary of Terms Used in Security and Intrusion Detection*. Sitio Web.
URL: *http://www.sans.org/resources/glossary.php*
Consultado: 25/08/2009.

[36] Stallings, W., *Data and Computer Communications*, 8va. edición, Prentice Hall, Agosto de 2008.

[37] Stallings, W., *Wireless Communications & Networks*, 2da. edición, Prentice Hall, Noviembre de 2004.

[38] Stubblefield, A., et al, *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, NDSS Conference, 2002.

[39] Terrones E., Salcedo R., *Evaluación de mecanismos y protocolos de seguridad desarrollados para redes inalámbricas 802.11b*. Trabajo Especial de Grado, Facultad de Ciencias de la Universidad Central de Venezuela, Octubre de 2004.

[40] Wi-Fi Alliance. Sitio Web.
URL: *http://www.wi-fi.org/*
Consultado: 25/08/2009.

[41] Wi-Fi Alliance, *Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise*. Marzo de 2005.

[42] Wi-Fi Alliance, *The State of Wi-Fi Security*. Septiembre de 2009.