UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE REDES INALAMBRICAS CORPORATIVAS DE CONTROL CENTRALIZADO

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

CARLOS MANUEL NEIRA GONZALES

PROMOCIÓN
1999 - I

LIMA – PERU
2009

IMPLEMENTACION DE REDES INALAMBRICAS CORPORATIVAS DE CONTROL CENTRALIZADO

Dedicatoria:

A mis padres, por su esfuerzo
y apoyo en hacerme un buen
hombre, mejor padre.
A mi esposa por soportar
mi natural y desordenado
ritmo de vida.

SUMARIO

El presente trabajo analiza, evalúa y propone la implementación de una infraestructura para redes wireless LAN de altas prestaciones para una empresa del sector Corporativo (Grandes Empresas), basado en equipamiento Wireless de Control Centralizado, integrando un esquema de alta seguridad basado en 802.1X y EAP/TLS.

El proyecto considera que las Grandes Empresas, al manejar altos volúmenes de información, apuestan mucho por el uso de las tecnologías, y al ser esta información de naturaleza sensible y estratégica, estas Empresas resultan ser muy exigentes en cuanto a la funcionalidad y seguridad de los sistemas.

El trabajo se basa en mi experiencia como Bachiller, en la formulación de proyectos de plataformas wireless LAN para el sector de Grandes Empresas.

ÍNDICE

INTRODUCCIÓN

El presente trabajo analiza, evalúa y propone la implementación de una infraestructura de redes wireless de altas prestaciones, para una empresa del sector Corporativo (Grandes Empresas), basado en equipamiento Wireless de Control Centralizado, integrando un esquema de alta seguridad basado en 802.1X y EAP/TLS.

El presente trabajo propone una metodología de trabajo para el diseño y explica el proceso de implementación a tener en cuenta, así como el análisis de los recursos y componentes de infraestructura necesarios.

En el primer Capítulo se analiza el panorama de las redes inalámbricas y específicamente, la problemática vinculada a la implementación de redes 802.11.

En el capítulo Segundo, se desarrolla un marco teórico general resumido de la tecnología 802.11, su arquitectura, tipos de topología, los niveles físico y de acceso al medio, su arquitectura y especialmente, los conceptos de seguridad relacionados a 802.1x, EAP y en la parte final, conceptos de Autoridad Certificadoras y Certificados Digitales.

En el Tercer Capítulo se expone el caso práctico de una Corporación Peruana, se describen los componentes de la solución propuesta, el rol de cada uno de ellos, el proceso de implementación con el producto de marca Cisco Systems, la plataforma de seguridad EAP/TLS bajo ambiente Windows, así como el análisis en tiempo y presupuesto necesarios.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA DE INGENIERIA

Actualmente, en Comunicaciones de Datos se manejan varios conceptos y tecnologías, las cuales se fueron introduciendo como parte del rápido desarrollo tecnológico. Algunos conceptos que escuchamos hoy en día, son redes LAN (Local Area Network), redes WAN (Wide Area Network), seguridad de las redes, gestión de redes, redes multiservicio, redes de banda ancha, fibra óptica, WDM y DWDM, ATM, redes de datos inalámbricas y otros más; cada plataforma y tecnología se está desarrollando constantemente, dando lugar a nuevos productos, con el fin de tener cada vez redes más rápidas, de fácil crecimiento, de fácil gestión, fácil implementación, que tengan gran nivel de seguridad y además, que la relación costo beneficio sea la más adecuada.

En este contexto, las redes Wireless LAN o estándar 802.11, han pasado de ser una "curiosidad tecnológica" a un verdadero boom que hace posible que para estar hoy conectado a la gran red (www), ya no es necesario ni siquiera un "click", basta que nuestra portátil tenga una interfase "WIFI" en modo automático y nos ubiquemos en cualquier café o restaurante con cobertura wireless gratuita, para conectarnos de manera automática. Las empresas de todo tipo no escapan a las bondades que esta tecnología ofrece.

1.1 Descripción del Problema

Las redes inalámbricas de área local (WLAN) juegan en la actualidad un papel muy importante en el desarrollo y productividad de las empresas y compañías de hoy en día.

Este tipo de redes facilita la interconexión de equipos y dispositivos, proporcionando un acceso móvil a los servicios y aplicaciones de la red desde cualquier parte. Los muchos beneficios y ventajas que ofrecen las WLAN deben ser diseñadas y planificadas de tal forma, que únicamente los usuarios legítimos aprovechen al máximo la flexibilidad y movilidad, y puedan igualmente, sentirse tranquilos de la seguridad en sus comunicaciones. Esta es quizás la mayor duda de las grandes empresas, al apostar por una tecnología de este tipo como parte de su plataforma de soporte al Negocio, saber si

es lo suficientemente confiable y operativamente práctica. La mayoría de las redes inalámbricas instaladas no cuentan con todas las características de seguridad, calidad de servicio (QoS) para soporte de aplicaciones de voz y video, roaming, planificación y selección de los canales de operación, administración y monitoreo de la red, planes de contienda y procesos a seguir cuando existan inconvenientes, etc. Por estas razones, este tipo de redes, cuando se implementan sin tener en cuenta aspectos, tales como la seguridad, calidad de servicio o performance, se convierten en un problema en vez de una solución.

1.2 Objetivos Del Trabajo

Retomando los argumentos vertidos en el numeral anterior, lo que buscamos con este trabajo en primer lugar, es proponer una plataforma de red wireless para el sector de Grandes Empresas, que ofrezca movilidad con altos niveles de performance, calidad de servicio, seguridad y administración.

1.3 Límites del Trabajo

El trabajo se ha realizado en base a una experiencia con el producto, si bien se hace un análisis de la ingeniería del proyecto con algunas herramientas de software libre para medición, somos conscientes que en el mercado existen herramientas bastante potentes que pemiten hacer un trabajo mucho más completo a nivel de campo (Site Survey); por el alto costo de estas herramientas es que no se ha incluido este nivel de análisis como hubiera sido deseable. Aun con estas limitaciones, consideramos que la metodología si cumple con su objetivo y permite tener una visión general del proceso de site Survey necesario.

1.4 Síntesis del Trabajo

El presente trabajo incluirá

- En el capítulo II , Una base teórica general sobre la tecnología wireless LAN IEEE 802.11
- En el capítulo III, se realiza la exposición de la arquitectura propuesta a nivel de equipamiento e implementación, también se incluye un resumen de la inversión del proyecto, así como los plazos de ejecución del mismo.
- En las conclusiones finales y tomando como punto de partida el Proyecto SAN ANDRES, se resaltan los considerandos a tener presente en proyectos de este tipo.

CAPÍTULO II

MARCO TEORICO CONCEPTUAL

En tan solo unos pocos años, las WLAN han pasado de tener un alto precio y de ser una tecnología curiosa para algunos expertos, a ser una tecnología predominante. La tecnología inalámbrica más exitosa es sin duda el conjunto de estándares 802.11, conocido comercialmente como Wi-Fi (Wireless Fidelity, Fidelidad Inalámbrica), convirtiéndose así en el estándar defacto para las WLAN, debido a la implementación en múltiples productos comerciales. Hoy en día, el término WIFI es quizás uno de los más empleados en cuanto a términos tecnológicos se refiere.

2.1 Desarrollo Teórico del Estándar IEEE 802.11

2.1.1 El Estándar IEEE 802

Las especificaciones del IEEE 802 se centran en las dos capas inferiores del modelo OSI: La capa física y la capa de enlace de datos. Como se muestra en la Fig. 2.1 todas las redes 802 tienen un componente MAC, también llamado Capa de Acceso Al medio y un componente físico PHY, también llamado Capa Física.

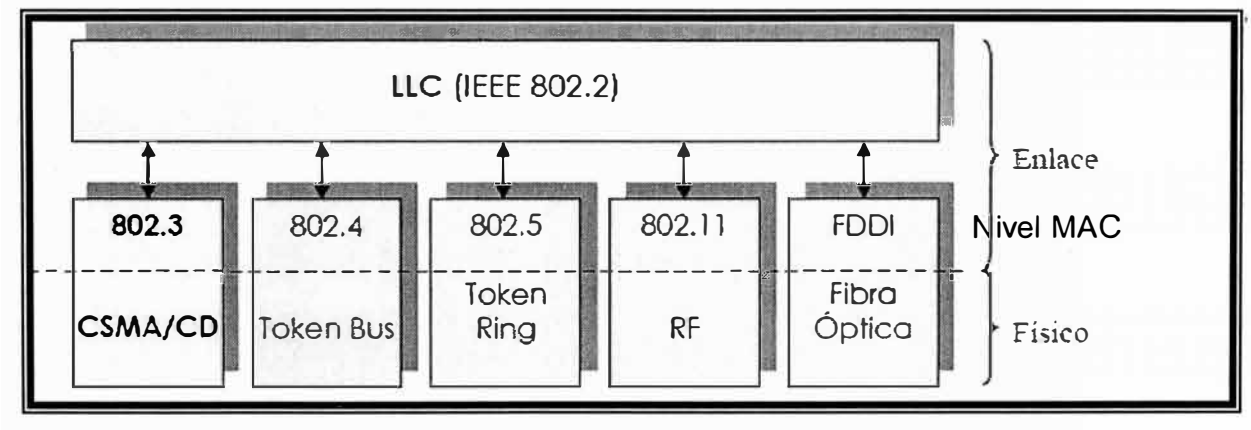


Fig. 2.1 Capa Física y Capa MAC del 802.11

2.1.2 El Estándar IEEE 802.11

En junio de 1997, el IEEE ratificó el estándar para redes inalámbricas IEEE 802.11, que llegaban a velocidades de 1 y 2 Mbps, con una modulación de señal de espectro expandido por secuencia directa DSSS (Direct Sequence Spread Spectrum), y

por salto de frecuencia FHSS (Frequency Hopping Spread Spectrum); sin embargo, a finales de 1999 se publican 2 suplementos al estándar original que son el IEEE 802.11b y el IEEE 802.11a.

2.1.3 El Estándar IEEE 802.11b

IEEE 802.11b fue la segunda extensión del estándar original y fue la base para la mayoría de las redes de área local inalámbricas que existen en la actualidad.

Este estándar opera en la banda de 2.4 GHz y utiliza como técnica de modulación HR/DSSS (High-Rate Direct Sequence Spread Spectrum) conjuntamente con la modulación CCK (Complementary Code Keying).

El IEEE 802.11b tiene 11 canales de 22 MHz, de los cuales, tres canales son no solapados, de esta forma se disponen de 3 Puntos de Acceso para diferentes canales en la misma área sin interferencia.

Los rangos de velocidad de datos que soporta 802.11b son 1, 2, 5.5 y 11 Mbps, y su alcance máximo es de 100 metros en condiciones ideales.

2.1.4 El Estándar IEEE 802.11a

IEEE 802.11a fue la primera extensión del estándar original, opera en la banda de 5 GHz denominada U-NII (Infraestructura de Información Nacional sin Licencia) menos congestionada y con menos interferencias.

802.11a utiliza la modulación por Multiplexación por División de Frecuencias Ortogonales OFDM (Orthogonal Frequency Division Multiplexing), la cual divide una señal de datos a través de 52 subportadoras (48 subportadoras de datos y 4 subportadoras para sincronización) con canales de 20 MHz para proveer transmisiones en velocidades de datos de 6, 9, 12,18, 24, 36, 48 ó 54 Mbps y con velocidades reales máximas de 25 Mbps.

IEEE 802.11a tiene 12 canales no solapados (8 para red inalámbrica y 4 para conexiones punto a punto), de esta forma, se disponen de 8 Puntos de Acceso para diferentes canales sin interferencia dentro de la misma área de cobertura.

2.1.5 El Estándar IEEE 802.11g

La tercera extensión del estándar original es 802.11g. De forma similar a 802.11b, 802.11g opera en la banda de 2.4 GHz y las señales transmitidas utilizan 11 canales de 22 MHz cada uno, lo que es aproximadamente un tercio de la banda total. Esto limita el número de puntos de acceso no solapados a tres, de igual manera que 802.11b. La técnica de modulación utilizada es OFDM en banda angosta, que funciona en los 2.4

GHz. El estándar 802.11g provee transmisiones teóricas de hasta 54 Mbps y es capaz de alcanzar una velocidad real de hasta 24 Mbps. Además, es compatible con 802.11b.

2.1.6 El Estándar IEEE 802.11n

El IEEE 802.11n es una tecnología en desarrollo, en marzo de 2007 se aprobó el Draft 2.0 (Draft-N) de 802.11n por parte del IEEE y desde junio de 2007, la Wi-Fi Alliance está revisando los productos 802.11n del mercado, para certificar que cumplan con el borrador 2.0 de esta tecnología.

Se espera que la tecnología final no tenga mayores cambios frente al Draft 2.0, y que los equipos 802.11n actuales puedan se actualizados por software. Según el IEEE, el estándar 802.11n podría ratificarse a finales de 2009.

2.1.7 Comparación de las Tecnologías

La Tabla 2.1 muestra un resumen comparativo de las tecnologías referidas.

2.1.8 Arquitectura del Estándar IEEE 802.11

La arquitectura 802.11 es muy similar a un sistema celular. En la Fig. 2.2 se puede ver sus componentes

ME : Movil Equipment , dispositivo móvil que accede a los servicios .

AP : Base Equipment, punto de acceso a los servicios, comunmente llamado punto de acceso o access point.

BSS: Base Service Set (celda) , área de control del AP.

DS: Distribution System(Inter. BSS) infraestructura que interconecta los AP

ESS: Extended Service Set (InterBSS) AP pertenecientes al mismo dominio.

2.1.9 Topologías para el Estándar IEEE 802.11

Dependiendo de las necesidades y requerimientos de interconectividad de alguna red, las redes WLAN ofrecen diferentes grados de complejidad.

Los dispositivos 802.11 son muy fáciles de adquirir en el mercado, sin embargo la configuración y protección óptima de redes inalámbricas resulta compleja; es necesario tener en cuenta ciertas prácticas y recomendaciones al implementarlas. Uno de los aspectos a considerar, es el tipo de topología a implementar.

Las redes inalámbricas tradicionalmente se configuran utilizando dos topologías básicas :

- Las redes independientes o Ad-Hoc y
- Redes dependientes o de infraestructura .

Tabla 2.1 Comparación de los Estándares 802.11

Parâmetro	**802.11a**	**802.11b**	**802.11g**	**802.11n**
Frecuencia	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz hasta 40 GHz
Ancho de Banda	300 MHz	83.5 MHz	83.5 MHz	>1 GHz
Modulación	OFDM	HR/DSSS y CCK	OFDM	OFDM y MIMO
Ancho de Banda por Cana	20 MHz	22 MHz	22 MHz	20 MHz y 40 MHz
Canales no solapados	12	3	3	Depende del Fabricante
Tasa de Transmisión Teórica	De 6 a 54 Mbps	De 1 a 11 Mbps	De 1 a 54 Mbps	De 124 a 600 Mbps
Tasa de Transmisión Real Máxima	25 Mbps	5 Mbps	24 Mbps	300 Mbps
Rango de cobertura en interiores	10 - 40 metros	Más de 50 metros	30 - 50 metros	40 - 70 metros
Usuarios Simultáneos	64	32	50	Depende del Fabricante
Compatibilidad con otros Estándares WLAN	Incompatible con 802.11b/g	802.11g	802.11b	802.11 a/b/g

a) Redes Independientes (Ad hod)

La configuración más básica para redes inalámbricas es la Ad-Hoc (de igual a igual). En este tipo de topología no se requiere de ningún Punto de Acceso para la comunicación entre las estaciones, sino que los propios dispositivos inalámbricos se

comunican entre sí, siempre que se encuentren dentro del alcance directo de la comunicación. Ver Fig. 2.3(a)

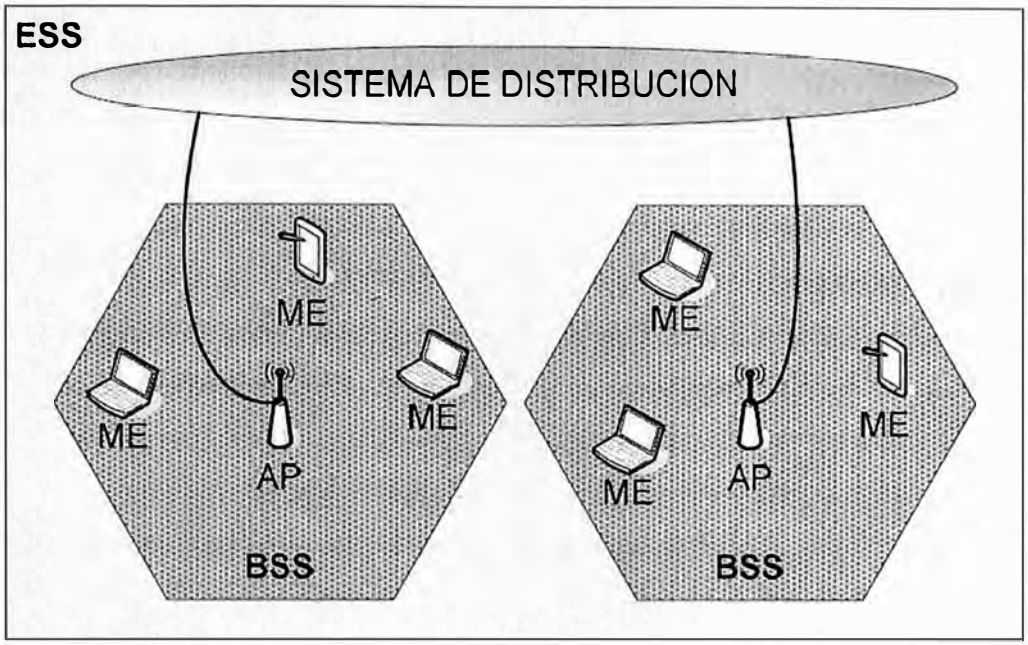


Fig. 2.2 Arquitectura del Estándar 802.11a

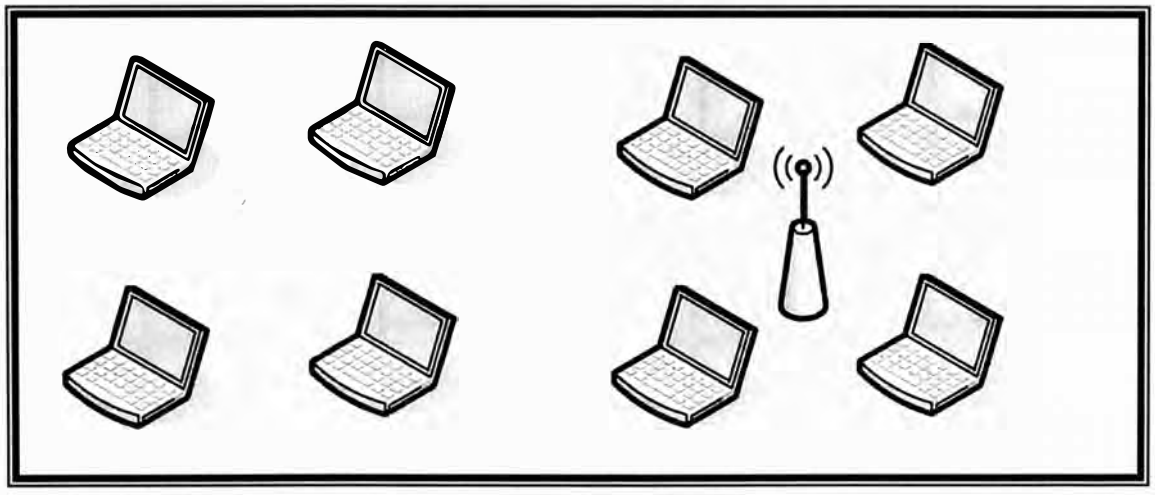


Fig. 2.3 (a) : Red Ad hoc (b) : Red Infraestructura.

b) Redes de Infraestructura

Las redes de infraestructura se distinguen porque utilizan un Punto de Acceso formando un BSS (Basic Service Set) de Infraestructura, de esta forma, las estaciones móviles tienen que asociarse con un Punto de Acceso para obtener los servicios de red; siempre las estaciones móviles inician el proceso de asociación y los Puntos de Acceso, pueden conceder o denegar el acceso basándose en el contenido de una petición de asociación. Ver Fig. 2.3(b)

2.1.10 La Capa Física de 802.11

La Capa Física (PHY) se divide lógicamente en tres subcapas correspondientes a dos funciones de protocolos:

- PLCP (Physical Layer Converge Procedure o Procedimiento de Convergencia de Capa Física).
- PMD (Physical Medium Dependent o Dependiente del Medio Físico)
- PLME (Physical Layer Management Entity o Subcapa de Administración a Nivel Físico).

La subcapa PLCP se encarga de evaluar la detección de portadora y de transformar la PDU MAC (unidades de datos MAC) a un formato adecuado para su transmisión y recepción a través de un sistema físico dependiente del medio.

La subcapa PMD especifica las técnicas de modulación y codificación a ser utilizadas y define las características del medio de transmisión inalámbrico.

Finalmente, la subcapa de administración a nivel físico (PHY Management o PLME) determina ajustes de diferentes opciones de cada capa física.

a) Tecnologías de la Capa Física

Diferentes tecnologías de capa física se definen para transmitir información por el medio inalámbrico. En la revisión inicial del 802.11 publicada en 1997 se estandarizaron tres capas físicas

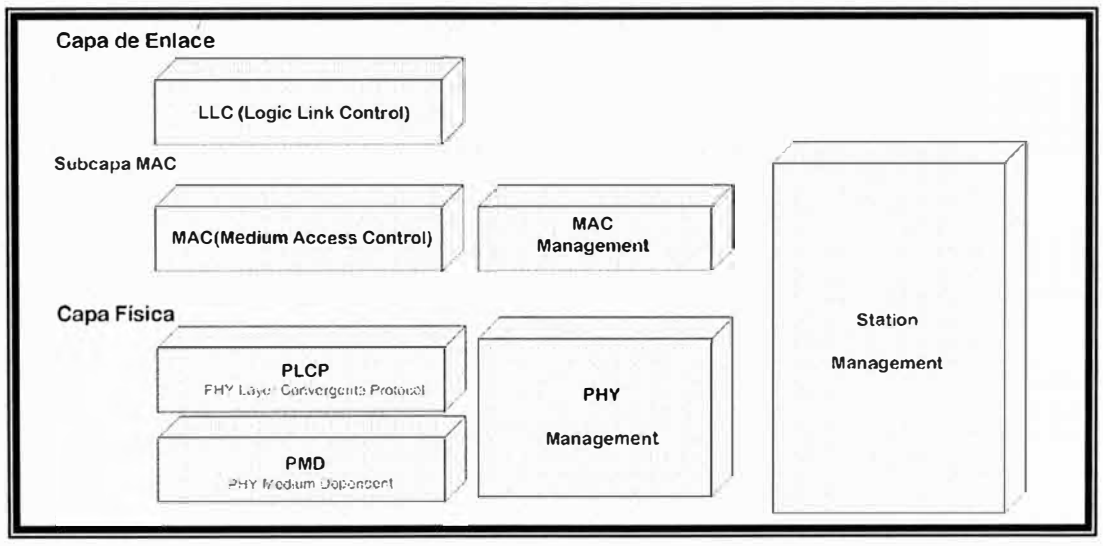


Fig. 2.4 La Capa Física 802.11.

- Capa Física de Radio de Espectro Disperso de Salto de Frecuencia (FHSS, Frequency-Hopping Spread Spectrum).

- Capa Física de Radio de Espectro Disperso de Secuencia Directa (DSSS, Direct-Sequence Spread Spectrum).
- Capa Física de Luz Infrarroja (IR, Infrared Light).

Posteriormente, en 1999 se desarrollaron tres capas físicas más, basadas en la tecnología de radio y una que está en perfeccionamiento (802.11n) :

- 802.11a: Capa Física de Multiplexado de División de Frecuencia Ortogonal (OFDM, Orthogonal Frequency Division Multiplexing).
- 802.11b: Capa Física de Secuencia Directa de Alta Tasa (HR/DS o HR/DSSS, High-Rate Direct Sequence).
- 802.11g: Capa Física de Velocidad Extendida (ERP, Extended Rate PHY).
- Futuro 802.11n: Capa Física MIMO PHY o PHY de Alto Rendimiento.

b) La Técnica de Espectro Disperso de Salto de Frecuencia (FHSS)

La técnica FHSS, consiste en modular la señal a transmitir, con una portadora que salta de frecuencia en frecuencia dentro de una secuencia específica, en función del tiempo. Este cambio periódico de frecuencia de la portadora, reduce la interferencia producida por otra señal originada por un sistema de banda estrecha.

Como se muestra en la Fig. 2.5, un patrón de saltos determina las frecuencias de la portadora en cada momento.

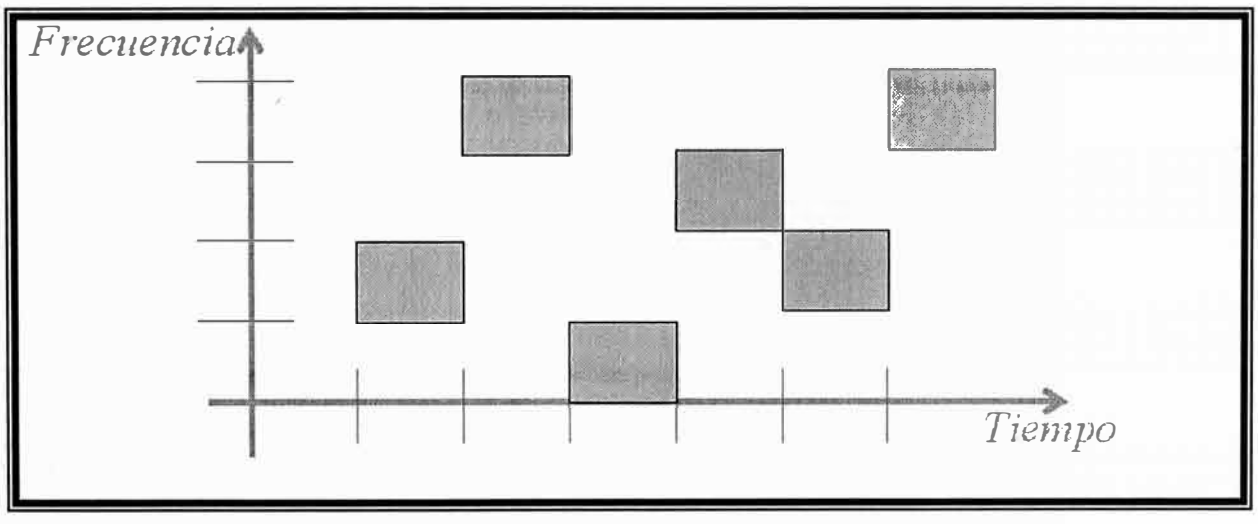


Fig. 2.5 Modulación por Salto de Frecuencia

c) La Técnica de Espectro Disperso de Secuencia Directa (DSSS)

La modulación de secuencia directa funciona aplicando una secuencia de chips para el flujo de datos. Un chip es un dígito binario utilizado por el proceso de propagación.

Los bits son datos de nivel superior mientras que los chips son números binarios utilizados en el proceso de codificación.

Cada bit se codifica utilizando toda la palabra de Barker como una secuencia de 11 chips, 802.11 utiliza la secuencia Barker {+1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1}, en donde los +1 se convierten en 1 y los -1 en 0, por lo que la secuencia de Barker se convierte en 10110111000, lo que se aplica a cada bit en el flujo de datos a través de un sumador módulo dos.

Cuando se codifica un bit cuyo valor es 1, todos los bits en el código de propagación cambian, para un bit 0 el código de propagación permanece de la misma forma. La Fig. 2.6 muestra el esquema de codificación explicado.

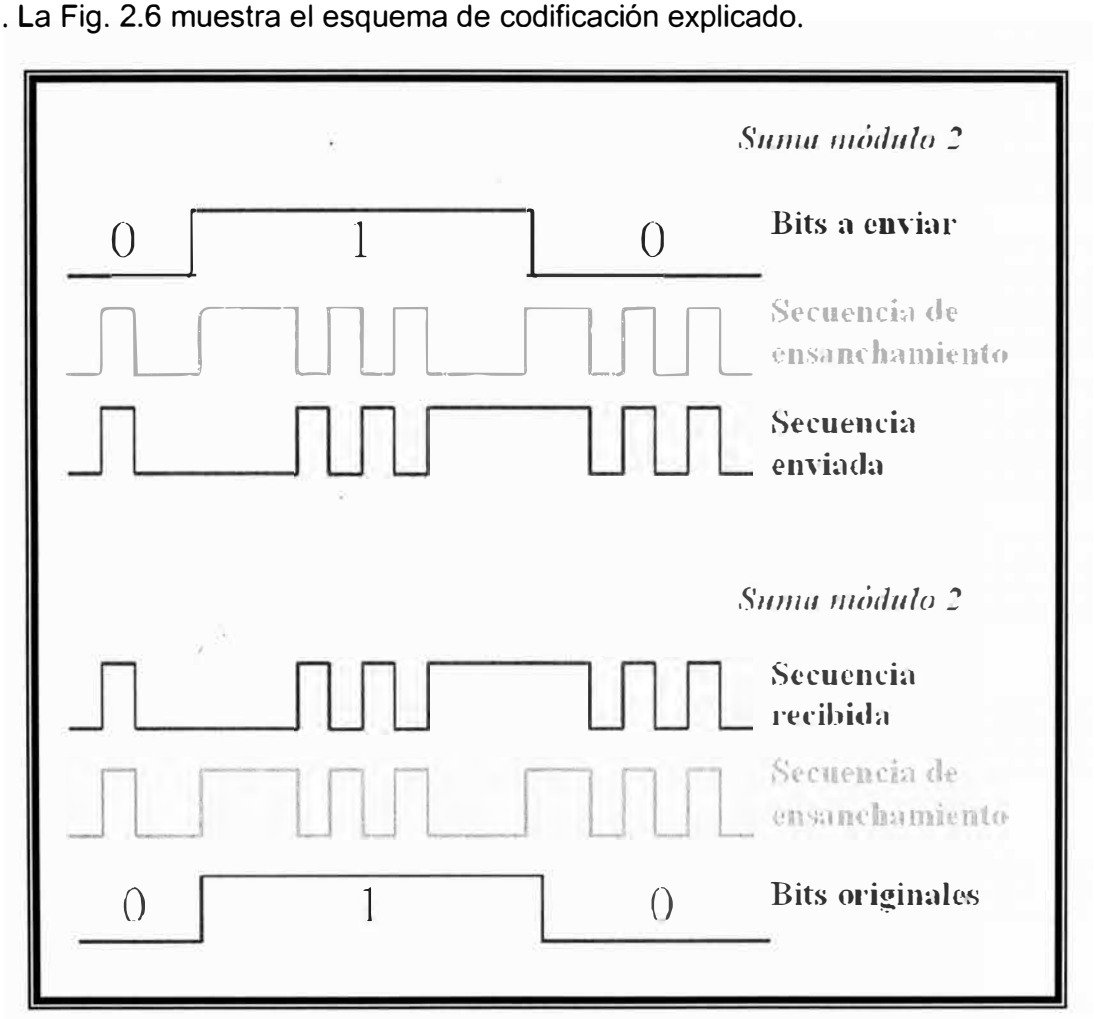


Fig. 2.6 Modulación por Espectro Disperso de Secuencia Directa (DSSS).

d) La Técnica de Multiplexado de División de Frecuencia Ortogonal (OFDM)

La técnica OFDM es un método que divide el ancho de banda disponible en sectores o canales denominados subportadoras y hace que éstas transmitan datos al mismo tiempo en paralelo; además OFDM realiza un multiplexado de datos sobre el conjunto de todas las subportadoras, incrementando el rendimiento de transmisión.

802.11a utiliza una técnica de Modulación de Amplitud de Cuadratura QAM (Quadrature Amplitude Modulation) en cada una de las subportadoras para transmitir datos a velocidades superiores (24 a 54 Mbps); las velocidades de transmisión más bajas (6 a 18 Mbps) utilizan la modulación BPSK (Binary Phase Shift Keyed) y QPSK (Quadrature Phase Shift Keying).

e) La Técnica de Secuencia Directa de Alta Tasa (HR/DSSS)

De igual forma que la Capa Física DSSS, la Capa Física HR/DSSS para 802.11b utiliza 14 canales, cada canal tiene un ancho de banda de 22 MHz, separado del siguiente canal por 5 Mhz.

De los 14 canales disponibles, las especificaciones del FCC determinan el uso de 11 canales, de los cuales solo tres son no solapados (non-overlapping): los canales 1, 6 y 11; de esta forma, tres sistemas (Puntos de Acceso) pueden ser localizados en la misma área sin interferencias. (ver Fig. 2.7)

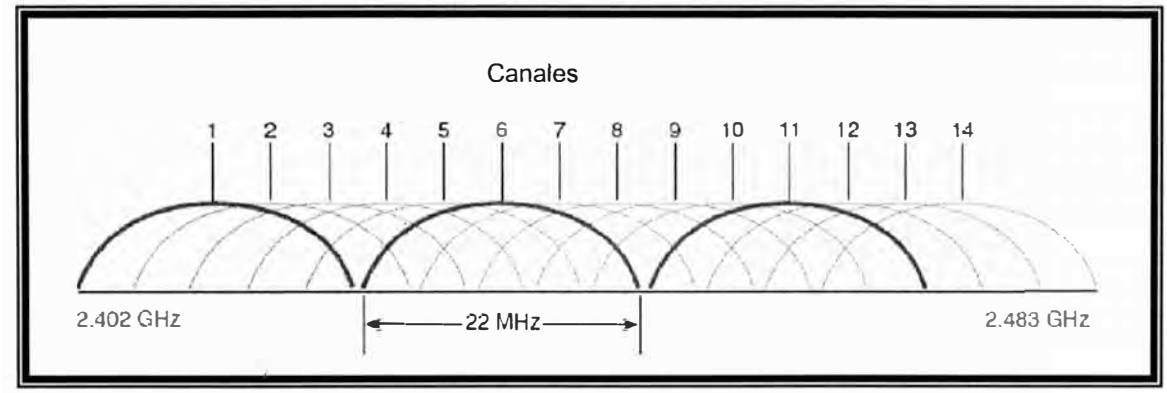


Fig. 2.7 Localización de Canales DSSS

La Capa Física HR/DSSS puede transmitir y recibir datos a 1 y 2 Mbps, para asegurar la compatibilidad con DSSS.

Para transmisiones a 5,5 y 11 Mbps, HR/DSSS utiliza técnicas de modulación de fase basadas en DQPSK y una codificación CCK (Complementary Code Keying).

f) La Técnica de Velocidad Extendida (ERP 802.11g)

802.11g está compuesto por diversas especificaciones, se añade una normativa que comprende a varios tipos de ERP (Capa Física de Velocidad Extendida, Extended Rate PHY):

- **ERP-DSSS y ERP-CCK**

Estos módulos son compatibles hacia atrás con las especificaciones de secuencia directa DSSS original de 1 y 2 Mbps, así como las mejoras de 802.11b a 5,5 y 11 Mbps.

- **ERP-OFDM**

Éste es el módulo principal de 802.11g, ejecuta la misma funcionalidad de 802.11a en la banda de frecuencia ISM de 2,4 GHz. Admite las mismas velocidades que 802.11a de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps, siendo las velocidades de 6,12 y 24 obligatorias.

- **ERP-PBCC y DSSS-OFDM**

Estos módulos permiten una compatibilidad hacia atrás con la tecnología 802.11b, son módulos opcionales y la mayoría de los dispositivos 802.11g no la utilizan ampliamente. Al igual que 802.11a, 802.11g utiliza diferentes técnicas de modulación dependiendo de la velocidad de transmisión de datos.

Dado que 802.11g adopta el plan de frecuencias de 802.11b, se dispone también de tres canales no solapados

g) Capa Física de Alto Rendimiento (MIMO 802.11n)

El objetivo del Grupo de Trabajo llamado TGn, es conseguir un rendimiento neto para el 802.11 de 100 Mbps, mediante la mejora de la eficiencia de la Capa MAC o incrementando la velocidad de datos máxima de más de 100 Mbps (o ambos) .

Se han presentado seis propuestas completas para estandarizar a 802.11n, que es la denominación acordada, siendo las dos principales la de los grupos de trabajo TGnSync y WWiSE (World-Wide Spectrum Efficiency).

Ambas propuestas TGnSync y WWiSE utilizan la tecnología MIMO e incluyen un esquema de modulación OFDM similar a 802.11g.

MIMO usa múltiples antenas transmisoras y receptoras para mejorar el desempeño del sistema. MIMO es una tecnología que usa múltiples antenas para manejar más información (cuidando la coherencia) que utilizando una sola antena. Dos beneficios importantes que provee a 802.11n, son la diversidad de antenas y el multiplexado espacial. En la Fig. 2.8 se muestra un esquema de arreglo MIMO para multiplexar señales usando M antenas de transmisión y N antenas de recepción.

2.1.11 La Capa de Acceso al Medio de 802.11

La capa de acceso al medio en 802.11, se encarga de proporcionar un servicio de datos fiable a los protocolos de capas superiores y al mismo tiempo, permitir un acceso ordenado y equitativo al medio inalámbrico compartido.

Para proporcionar un acceso fiable, el estándar 802.11 define un protocolo para el intercambio de tramas de información. La secuencia mínima en este intercambio consiste en el envío de una trama de información del origen al destino y un asentimiento o Acuse

de Recibo ACK (Acknowledgment) enviado por el destino, en el caso que la primera trama haya sido recibida correctamente. Este es el principio básico en realidad.

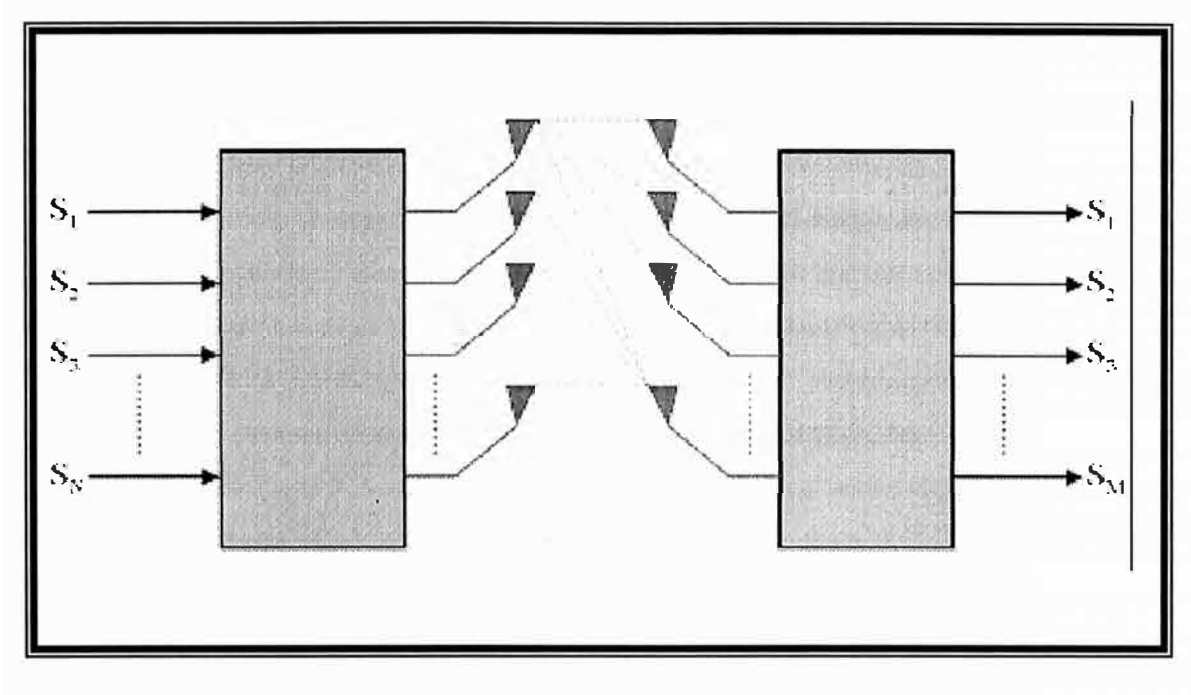


Fig. 2.8 Configuración de antenas MIMO

2.1.12 Servicios de Red para 802.11

Se definen nueve servicios de Red para el estándar 802.11, sólo se utilizan tres de los servicios para transportar datos, los seis servicios restantes son operaciones de administración que permiten a la red registrar las estaciones móviles. Se los puede agrupar en servicios del sistema de distribución, servicios de estación y servicios de administración de espectro. Este último, es un subgrupo especial de los servicios de estación. Definiremos los dos primeros que son los más conocidos.

2.1.13 Servicios del Sistema de Distribución

Los servicios de distribución, conectan los Puntos de Acceso al Sistema de Distribución, permiten que los Puntos de Acceso extiendan los servicios de la red cableada a la red inalámbrica. Adicionalmente, estos servicios se encargan de administrar la asociación de estaciones móviles.

Se tienen cinco servicios pertenecientes a este grupo, que son

- Distribución
- Integración
- Asociación
- Reasociación

- Desasociación

2.1.14 Servicios de Estación

Forman parte de cualquier estación 802.11. Los servicios de estación permiten que una estación móvil se autentique para formar una asociación y pueda trasmitir tramas de forma confidencial, para proteger los mensajes a medida que recorren el enlace inalámbrico vulnerable.

Se tienen cuatro servicios pertenecientes a este grupo, que son:

- Autenticación
- Desautenticación
- Confidencialidad
- Entrega de MSDU

La Tabla 2.2 ofrece una descripción de cada servicio mencionado.

2.2 Seguridad en Redes Wireless LAN

Cuando las WLAN fueron introducidas al mercado, se pensó que se difundirían rápidamente, sin embargo, sus limitaciones contuvieron a su éxito. Una de las principales causas por la que administradores y usuarios prefieren aún las redes cableadas a las WLANs, es la inseguridad inherente a su medio de transmisión.

Al utilizar como medio de transmisión el aire, las redes inalámbricas son más susceptibles a vulnerabilidades relacionadas con la integridad y la confidencialidad de los mensajes, en comparación con las redes cableadas.

Así, cuando nació el estándar 802.11 se incluyó un mecanismo de encriptación y autenticación el WEP (Wired Equivalent Privacy), que con la misma llave se podía encriptar y autenticar al usuario.

Con el desarrollo de la computación y los programas de Internet, quedó ampliamente en evidencia la fragilidad de WEP. Hoy en día se puede encontrar gran cantidad de material público y manuales enteros que muestran como romper un sistema basado en WEP en un promedio de 8 minutos.

Consciente de esto, se formó un grupo de trabajo llamado el Task Group i (IEEE), que tenía por objetivo encontrar un mecanismo seguro para la encriptación y autenticación de las comunicaciones inalámbricas 802.11.

Este grupo, finalmente, en el 2004 tomó la opción más conveniente: llevar la filosofía de otro estándar ya existente para redes ethernet cableadas, el 802.1x, adecuándolo al entorno wireless y enmarcando este desarrollo en la norma 802.11i. Previo a esto, la industria en el 2003 ya había presionado para que la WIFI Alliance

Tabla 2.2 Servicios de Red para 802.11

Servicio	Grupo	Descripción
Distribución	Distribución	Servicio utilizado en la entrega de tramas para determinar la dirección de destino en redes de infraestructura.
Integración	Distribución	Entrega de tramas a una LAN IEEE 802 fuera de una red inalámbrica
Asociación	Distribución	Utilizado para establecer conexión entre la estación móvil y el AP.
Reasociación	Distribución	Utilizado para cambiar de AP conectado, el AP sirve como pasarela a una estación móvil determinada
Desasociación	Distribución	Elimina la comunicación de la estación con la red y la conexión con el AP.
Autenticación	Estación	Establece la identidad de la Estación (dirección MAC) antes de establecer la asociación.
Desautenticación	Estación	Utilizado para terminar la autenticación y por ende, la asociación.
Confidencialidad	Estación	Proporciona protección frente a escuchas secretas.
Entrega MSDU	Estación	Entrega de Datos al Destinatario.
Control de Potencia de Transmisión	Estación/Administración de Espectro	Reduce la interferencia minimizando la potencia de transmisión de la estación.
Selección Dinámica de Frecuencia (DFS)	Estación/Administración de Espectro	Evita la interferencia con la operación de sistemas de radar en la banda de 5 GHZ.

aprobase y certificase un estándar basado en alguno de los borradores previos del 802.11i; este estándar de la industria se llamó el WPA. Cuando se publica el 802.11i que era mucho más exigente que el WPA, la industria a través de la WIFI ALLIANCE tiene

que alinearse y genera su sello de certificación propio: El WPA2, que es la implementación comercial de la norma. Esto ocurre también en el 2004. A continuación entraremos en una revisión más a detalle de cada uno de estos estándares :

2.2.1 WEP (Wired Equivalent Privacy)

El algoritmo WEP forma parte de la especificación 802.11 y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica. WEP opera a nivel 2 del modelo OSI y es soportado por todos los fabricantes de soluciones inalámbricas.

Por sus características, WEP es una solución para WLANs pequeñas, en las que no se requiere niveles elevados de seguridad. Su implementación resulta fácil y no requiere de inversiones adicionales; por ser parte de 802.11, soporta interoperabilidad con clientes basados en distintas plataformas

El funcionamiento del cifrado WEP establece una clave secreta en el Punto de Acceso que es compartida con los diferentes dispositivos móviles Wi-Fi. Con esta clave que puede ser de 40 ó 104 bits, con el algoritmo de encriptación RC4 y con el Vector de Inicialización (IV), se realiza el cifrado de los datos transmitidos por Radio Frecuencia.

Las principales debilidades del protocolo WEP son tres

- El Vector de Inicialización es demasiado corto (24 bits), ocasionando problemas de transmisión en redes inalámbricas con mucho tráfico.
- Las claves WEP que se utilizan son estáticas y se deben cambiar manualmente.
- No se tiene un sistema de control de secuencia de paquetes.

Para garantizar la autenticación, la clave estática debe ser conocida solo por los usuarios lícitos de la red, pero como se puede ver el nivel de seguridad proporcionado por WEP es limitado, si la clave se ve comprometida, las comunicaciones de todos los usuarios pueden ser descifradas.

Por otra parte, WEP no provee mecanismos que protejan a la red de ataques internos.

Tipos de Autenticación : WEP especifica dos tipos de autenticación:

Open System Authentication.- En este tipo no se requiere que los usuarios conozcan la clave estática. Si un usuario conoce el SSID de la red, puede ingresar a ésta. En este tipo de autenticación se permite que cualquier dispositivo inalámbrico se asocie a la red.

Shared Key Authentication.- Dentro de este tipo de autenticación, el cliente envía una petición hacia el AP, luego, el AP envía un desafío (en texto plano) al cliente, el cliente cifra el desafío con la clave WEP y lo devuelve. El AP comprueba que el desafío se haya cifrado con la clave apropiada; de ser así, envía una respuesta al cliente indicándole que ha sido autenticado.

2.2.2 WPA (Wi-Fi Protected Access)

Los mecanismos de encriptación WPA y WPA2 se desarrollaron para solucionar las debilidades detectadas en el algoritmo de encriptación WEP. El nombre de WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi) es el nombre comercial que promueve la Wi-Fi Alliance. Las especificaciones y consideraciones técnicas se encuentran definidas en el estándar IEEE 802.11i.

El estándar 802.11i especifica dos nuevos protocolos de seguridad TKIP (Temporary Key Integrity Protocol o Protocolo de Integridad de Claves Temporales) y CCMP (Counter Mode CBC-MAC o Protocolo de Modo Contador con CBC-MAC)

TKIP se diseñó para ser compatible hacia atrás con el hardware 802.11b existente, mientras que CCMP se diseñó desde cero.

Para solucionar los inconvenientes de WEP, la Wi-Fi Alliance decidió implementar dos soluciones de seguridad:

Una solución rápida y temporal para todos los dispositivos inalámbricos ya instalados hasta el momento, especificando al estándar comercial intermedio WPA y una solución más definitiva y estable para aplicar a nuevos dispositivos inalámbricos, especificando al estándar comercial WPA2.

2.2.3 WPA versión 1 (WPA)

WPA se fundamenta en el protocolo de cifrado TKIP. Este protocolo se basa en el tercer borrador de 802.11i a mediados del 2003.

TKIP se encarga de cambiar la clave compartida entre el Punto de Acceso y el cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave.

Las mejoras a la seguridad introducidas en WPA son

- Se incrementó el Vector de Inicialización (IV) de 24 a 48 bits.
- Se añadió la función MIC (Message Integrity Check, Chequeo de Integridad de Mensajes) para controlar y detectar manipulaciones de los paquetes de información.
- Se reforzó el mecanismo de generación de claves de sesión.

2.2.4 WPA versión 2 (WPA2)

WPA2 es el nombre comercial de la Wi-Fi Alliance a la segunda fase del estándar IEEE 802.11i, dando una solución de seguridad de forma definitiva. WPA2 se diferencia de WPA1, fundamentalmente en el tipo de cifrado; utiliza el algoritmo de encriptación AES (Advanced Encryption Standard), que es un estándar de encriptación mucho más potente que sus predecesores, pudiendo soportar muchas longitudes de claves.

WPA2 se fundamenta en el protocolo de seguridad de la capa de enlace basado en AES denominado CCMP.

2.2.5 Estándar 802.1X

El estándar 802.1x fue aprobado en junio del año 2001 por el IEEE. Su nombre original es "Port-Based Network Access Control"; este estándar contiene normas para el control de acceso y la autenticación dentro de redes LAN y MAN.

802.1X utiliza las características de acceso físico de los estándares IEEE 802, para proporcionar un mecanismo que permita autenticar y autorizar a dispositivos relacionados con un puerto, con características de conexión punto a punto; en caso de que los procesos de autenticación y autorización fallen, se aplican mecanismos que evitan el ingreso a la red.

Dentro del estándar, un puerto es un punto que liga a un dispositivo a la infraestructura LAN; se puede utilizar para la autenticación puertos de puentes MAC, servidores, routers y las asociaciones entre estaciones y APs en WLANs 802.11.

a) Definiciones

Para el entendimiento de 802.1x es necesario conocer las siguientes definiciones:

EAP.- El protocolo EAP fue desarrollado por el IETF y se encuentra registrado en el RFC 3748. EAP define una técnica de encapsulación con un formato de trama que permite el intercambio de credenciales. El EAP soporta diferentes protocolos de capa enlace, por este motivo, se seleccionó para trabajar conjuntamente con 802.1x para realizar la autenticación en diferentes ambientes (LAN, MAN y WAN; cableados o inalámbricos).

Autenticador.- Es la entidad ubicada en un segmento LAN, que facilita la autenticación de otra entidad en un enlace punto a punto. Solo sirve como un punto intermedio a través del cual el servidor de autenticación y el suplicante intercambian credenciales.

Servidor de Autenticación.- Es una entidad que provee el servicio de autenticación a un autenticador. Este servicio determina si las credenciales presentadas por un suplicante son válidas para completar el proceso de autenticación. El servidor de autenticación presta los servicios de AAA dentro de redes WLANs; el más utilizado es el servidor RADIUS.

Puerto de acceso a la Red.- Es el punto de conexión entre un sistema y una LAN. Puede ser un puerto físico; por ejemplo, un puerto MAC conectado físicamente a un segmento. También puede ser lógico; por ejemplo, una asociación entre una estación y un AP.

PAE (Port Access Entity).- Es la entidad de protocolo asociada con el puerto, ésta soporta funcionalidades del protocolo asociadas con el autenticador, el suplicante o los dos.

Suplicante.- Es la entidad ubicada en un segmento LAN que solicita una autenticación a un autenticador en un enlace punto a punto.

Sistema.- Dispositivo que se conecta a una LAN por uno o más puertos; por ejemplo, estaciones, servidores, puentes, routers, etc.

EAPOL (EAP over LANs).- Protocolo que define la técnica de encapsulación para intercambio de paquetes EAP entre PAEs suplicantes y PAEs autenticadoras dentro de ambientes LAN.

b) Funcionamiento de 802.1X

El estándar 802.1x define mecanismos que permiten realizar el intercambio de credenciales y la validación o negación de acceso entre el cliente y el servidor de autenticación. En la Fig. 2.9 se muestra un esquema con los elementos necesarios para la operación del estándar 802.1x.

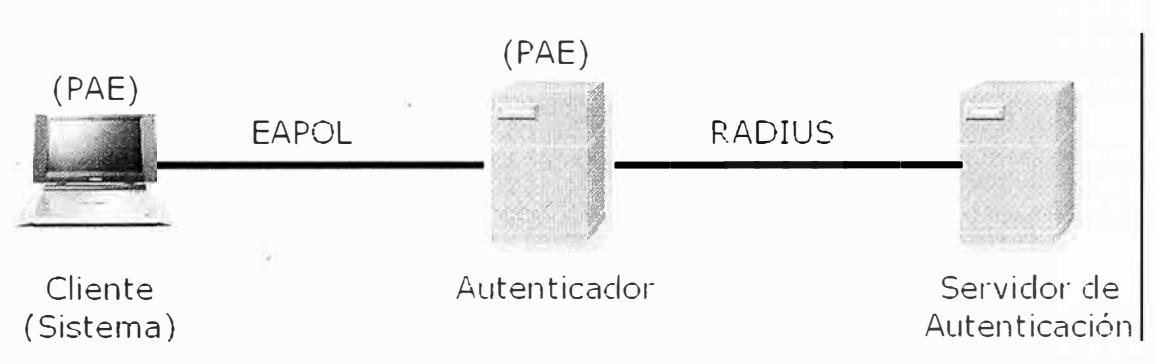


Fig. 2.9 Esquema 802.1x

El autenticador sirve como un puente entre el cliente y el servidor de autenticación durante el proceso de autenticación. El protocolo EAPOL es utilizado para el intercambio de paquetes entre el autenticador y el cliente mediante un puerto no controlado. Para la comunicación entre el autenticador y el servidor se utiliza el protocolo RADIUS.

Como se muestra en la Fig. 2.10, cuando el proceso de validación de credenciales ha sido exitoso, el servidor activa un puerto controlado, a través del cual el cliente tiene acceso a la red.

El proceso de autenticación es definido enteramente en el servidor; por este motivo, si se llega a cambiar la técnica de autenticación, las modificaciones en los clientes son mínimas.

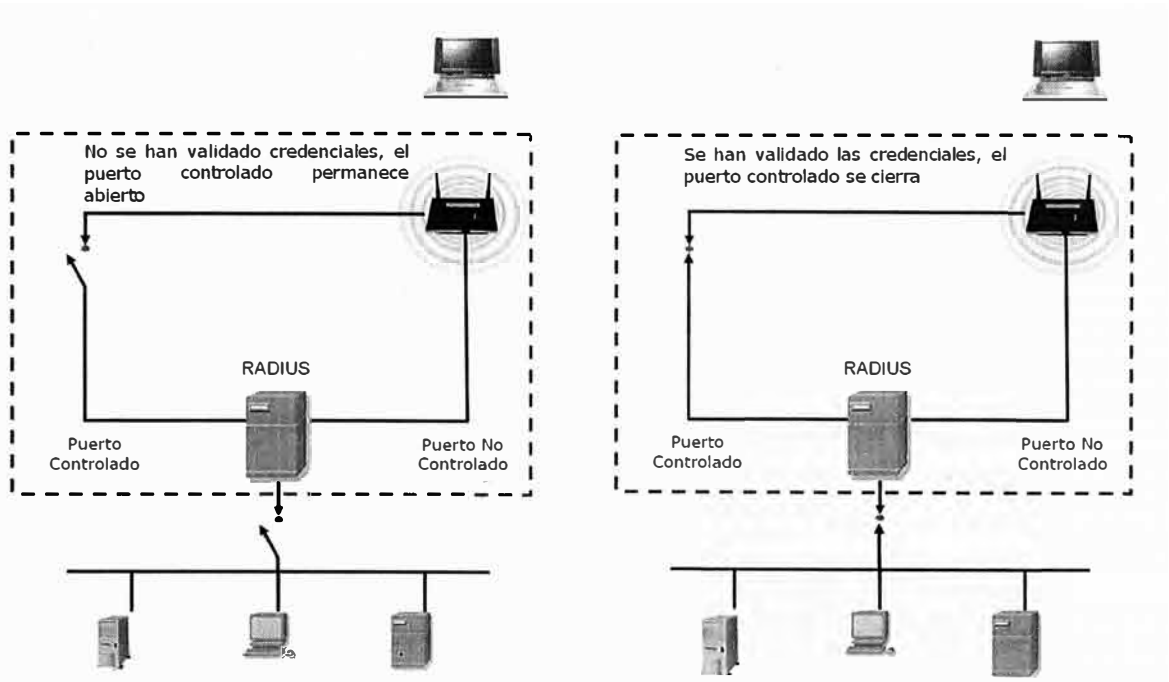


Fig. 2.10 Puertos en 802.1x

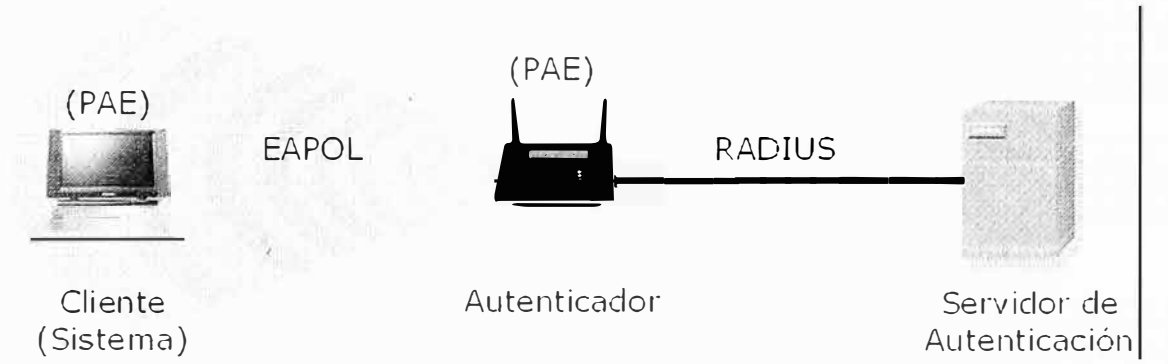


Fig. 2.11 Esquema de funcionamiento de 802.1x para WLANs

En ambientes inalámbricos, el AP cumple la función de autenticador y se utiliza un servidor RADIUS para autenticar las credenciales del cliente, como se muestra en la Fig. 2.11. La conexión entre el cliente y el autenticador se realiza también a través de un puerto lógico no controlado; a través de este canal se intercambian credenciales y respuestas de acceso.

Durante el intercambio de credenciales, el cliente recibe una clave que le permite cifrar sus mensajes durante una sesión, el AP identifica al cliente al reconocer su clave. Si el cliente no posee una clave válida, el AP descarta sus paquetes. Cuando la

validación se ha completado, el cliente tiene acceso a la red a través del puerto lógico controlado.

2.2.6 Radius

El estándar RADIUS define un esquema de cliente/servidor que brinda los servicios AAA. Las especificaciones de autenticación y autorización se encuentran registradas en el RFC 2865; las especificaciones que se refieren a Accounting están registradas en el RFC 2866.

Operación RADIUS

Cuando una estación ingresa al área de cobertura de una WLAN que realiza autenticación mediante 802.1x y un servidor RADIUS, se establece el siguiente procedimiento:

- El Punto de Acceso (AP) envía un desafío a la estación.
- La estación recibe el desafío y responde con su identidad.
- El AP reenvía la identidad de la estación al servidor.
- El servidor verifica la identidad del cliente y solicita un tipo de credencial de acuerdo al perfil de la estación.
- La estación envía su credencial al servidor.
- El servidor valida la credencial de la estación, si ésta es legítima transmite una clave WEP de sesión al AP.
- El punto de acceso (AP) envía al cliente la clave.
- Cuando el servidor autentica al cliente, el proceso se repite en reversa y el cliente autentica al servidor.
- Si se desea aumentar el nivel de seguridad, se puede realizar el proceso de autenticación periódicamente.
- La comunicación con un servidor RADIUS y los servicios AAA, por defecto se encuentran deshabilitados en un punto de acceso (AP) ; para evitar problemas de seguridad, sólo se deben configurar estos servicios si son necesarios para la autenticación en la red.
- Para configurar autenticación en una WLAN utilizando un servidor RADIUS, se debe configurar en el AP la dirección IP del servidor y definir una lista de métodos para la autenticación.

La lista de métodos define procedimientos y secuencias necesarias para el proceso de autenticación y autorización, o para el registro de accounting. Se puede

utilizar listas de métodos para designar uno o más protocolos de seguridad, de este modo se tienen alternativas en caso que el método inicial falle.

2.2.7 EAP

EAP es un protocolo diseñado para optimizar los procesos de autenticación mediante la transmisión de credenciales; no es un método de autenticación en sí, sino más bien, un mecanismo que soporta la transmisión de distintos tipos de credenciales de acuerdo a la técnica que se utilice para la autenticación. Sus especificaciones se encuentran registradas en el RFC 3748.

802.1X utiliza EAP para la negociación de la técnica de autenticación y sus parámetros entre el cliente y el autenticador; se requiere que un servidor valide las credenciales.

2.2.8 Infraestructura EAP

Para mantener el control en el proceso de comunicación entre el cliente y el autenticador, la trama EAP incluye los campos identificador y código; el campo identificador relaciona a una petición con una respuesta. Este campo se marca con el mismo valor para una pareja petición/respuesta.

El campo código permite determinar si se trata de una petición o de una respuesta; también puede indicar si se ha tenido éxito o fracaso durante el proceso de entrega de las credenciales.

Existen distintos esquemas de autenticación usando el protocolo EAP. El protocolo EAP está formado por un conjunto de módulos que proporcionan compatibilidad de arquitectura con cualquiera de sus distintos esquemas. Para que el proceso de autenticación pueda realizarse, el cliente y el autenticador deben tener instalado el mismo módulo de autenticación EAP.

2.2.9 Módulos EAP

Existen diferentes tipos de autenticación EAP. Cada tipo permite transmitir credenciales específicas. La trama EAP incluye el campo tipo; éste permite identificar el tipo de EAP que se utiliza en el proceso de autenticación. Dentro de redes WLAN se encuentra difundido el uso de los siguientes tipos de EAP: Desafío **MD5, TTLS, PEAP, FAST, LEAP y EAP-TLS**.

Desafío MD5.- MD5 utiliza para la autenticación un desafío que se envía al cliente. El cliente debe cifrar el desafío con una clave compartida y enviar el resultado al

autenticador; el autenticador compara el valor recibido con su propio resultado. Si el valor coincide, el cliente queda autenticado.

EAP-TTLS.- Fue creado por Funk Software y Certicom, provee autenticación segura mediante el establecimiento de un túnel con el protocolo TLS; las claves necesarias para cifrar los datos se generan por cada sesión. Después de establecer el túnel TLS, se produce la autenticación del servidor mediante certificados digitales; los clientes se autentican utilizando contraseñas. Las contraseñas son validadas en el servidor utilizando CHAP1, PAP2, MSCHAP, que son esquemas seguros de validar por usuario y password.

EAP-TLS.- Este protocolo fue creado por Microsoft y se encuentra registrado en el RFC 2716, provee autenticación mutua con un alto nivel de seguridad; durante el proceso de autenticación, tanto el cliente como el servidor requieren certificados digitales

PEAP.- Es un protocolo propietario de Microsoft, provee niveles similares de seguridad que EAP-TTLS. Este tipo de autenticación permite transmitir otros tipos de EAP, sin necesidad de establecer un túnel TLS. El usuario debe enviar su contraseña hacia el servidor RADIUS, la identidad del usuario es protegida mediante el uso de MSCHAPv2. El servidor RADIUS se autentica utilizando un certificado digital.

EAP-FAST.- Éste es un protocolo propietario de Cisco. Para la autenticación se utiliza PAC (Protected Access Credential) en lugar de usar un certificado digital. La PAC puede manejarse dinámicamente por el servidor de autenticación y ser distribuida a los clientes a través de un dispositivo de almacenamiento o mediante sesiones seguras.

LEAP.- Este método también es propietario de Cisco, permite conexiones seguras dentro de una WLAN, entre clientes y APs Cisco Aironet Series. La técnica que se usa para la autenticación está basada en contraseñas y nombres de usuarios almacenados en la base de datos de un servidor RADIUS. Las contraseñas no se envían por la red directamente. Para el proceso de autenticación, el cliente envía al servidor su nombre de usuario junto con un desafío generado a partir de su contraseña; utilizando el desafío del cliente, el servidor genera su propio desafío y se lo envía al cliente. Cuando se ha realizado la validación correspondiente, el cliente queda autenticado.

Los módulos EAP que utilizan contraseñas para la autenticación de usuarios y no implementan un túnel seguro para transmitirlas son vulnerables a ataques de diccionario

2.2.10 Autenticación con EAP-TLS

EAP-TLS necesita de una infraestructura que permita mantener una administración adecuada de los certificados. Su implementación demanda de una inversión superior a la requerida por otros módulos EAP; por esto, es recomendable para

redes corporativas con un gran número de usuarios o en redes donde se requiera un alto nivel de seguridad.

EAP-TLS Trabaja sobre PPP (Point to Point Protocol) en enlaces punto a punto. Soporta el uso de tarjetas inteligentes, proporcionando un método de generación de claves dinámicas y autenticación más eficaz.

EAP-TLS sólo se admite en servidores RADIUS que sean miembros de un dominio. Los servidores de acceso remoto que se ejecutan como servidores independientes o miembros de un grupo de trabajo, no admiten EAP-TLS.

2.2.11 Establecimiento de una Conexión con EAP-TLS

Cuando un cliente ingresa en el área de cobertura de un AP (autenticador), éste envía al AP una trama EAPOL start, para indicarle que desea establecer una conexión.

A continuación el AP solicita la identidad del cliente mediante una trama EAP de tipo EAP-Request/Identity, la identidad del cliente se envía en texto plano en una trama EAP-Response/Identity; luego, el AP encapsula la trama y se la envía al servidor en una trama RADIUS Access Request, que contiene el identificador del cliente.

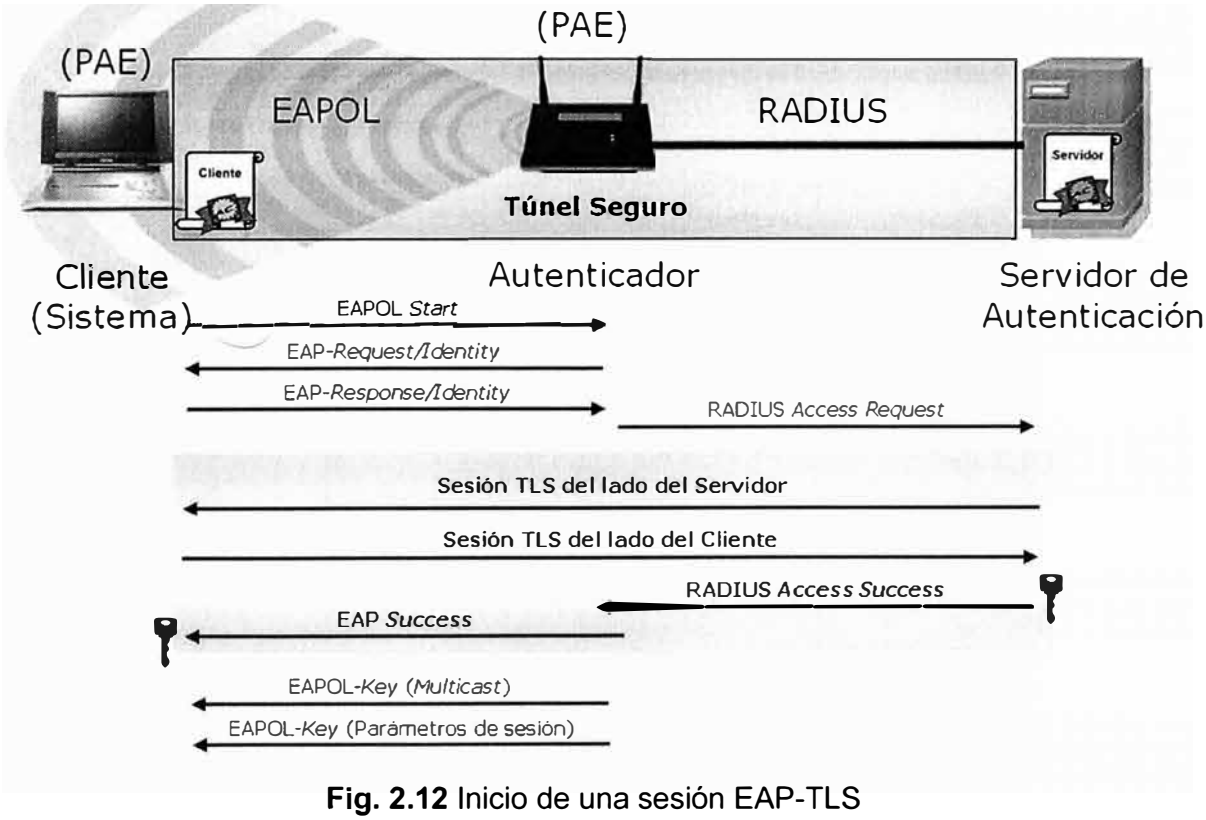


Fig. 2.12 Inicio de una sesión EAP-TLS

El cliente y el servidor poseen una clave maestra, con esta clave establecen un túnel; si el servidor comprueba que el cliente posee la clave maestra, envía un mensaje

RADIUS Access Success hacia el AP; este mensaje contiene una clave de sesión que es enviada luego desde el AP hacia el cliente dentro de un mensaje EAP Success; entonces, el cliente obtiene su clave de sesión. El AP envía además dos tramas EAPOL-Key cifradas con la clave de sesión; la primera trama contiene una clave para mensajes Multicast, la segunda trama contiene los parámetros que se utilizarán durante la sesión. Este proceso se encuentra graficado en la Fig. 2.12.

Con la clave de sesión se inicia una comunicación cifrada entre el cliente y el servidor; ésta se inicia con un paquete EAP-TLS/Start enviado por el servidor. Este paquete indica que el tipo de autenticación será EAP-TLS (EAP-Type=EAP-TLS); la trama tiene marcado el bit de inicio y no incluye datos.

Como respuesta el cliente envía una trama EAP-Response, la cual contiene información TLS client_hello con los parámetros TLS soportados por el cliente; por ejemplo: versión TLS, identificador de sesión, un número generado aleatoriamente y características de encriptación.

El servidor responde con una trama EAP-Request marcada con EAP-Type=EAP-TLS. El campo de datos de este paquete encapsula información TLS server_hello con los parámetros soportados por el servidor. Este paquete incluye además, el certificado digital del servidor y su clave pública.

Entonces, el cliente envía una trama EAP-Response marcada con EAP-Type=EAP-TLS que contiene información sobre los parámetros seleccionados después de la negociación; incluye también su certificado digital y su clave pública; indica que la negociación ha terminado.

El servidor acepta los parámetros enviados por el cliente con una trama EAP-Request marcada con EAP-Type=EAP-TLS; esta trama indica también que la negociación ha terminado.

El cliente contesta con una trama EAP-Response, informando que recibió la trama; finalmente, el servidor envía una trama EAP-Success indicando que la autenticación fue exitosa. Este proceso se encuentra graficado en la Fig. 2.13 autenticación EAP.

2.2.12 Comparación de los Diferentes Módulos EAP

El incremento en el nivel de seguridad dentro de una red siempre involucra inversión y un aumento en los procesos de administración. Cuando una red es más segura, los procesos se vuelven más complejos y por lo tanto se elevan los costos; además, se requieren equipos con mayores capacidades y sistemas operativos que manejen mayores funcionalidades.

Existen técnicas que logran que una WLAN sea extremadamente segura, esto es muy deseable, pero, debido a que involucran una inversión, siempre es necesario realizar un análisis previo, que permita descubrir cuál es el nivel de seguridad que una red necesita, incluso si se cuenta con recursos ilimitados.

Para este análisis, se debe tener en cuenta que soluciones como WEP y WPA, ofrecen niveles básicos de seguridad, teniendo como ventaja sus bajos costos. Otra ventaja es que no requieren de software especializado en el cliente. Estas soluciones son ideales para hogares y pequeñas empresas, en donde no se maneje información que involucre propiedad intelectual.

Por otra parte, las soluciones 802.1x/EAP requieren de la implementación de un servidor RADIUS, lo que implica costos, requerimientos de administración y de ser posible, una política de seguridad; sin embargo, si se demanda limitar la inversión, soluciones como Desafío MD5, LEAP y FAST brindan un nivel aceptable de seguridad.

Las soluciones Desafío MD5, LEAP y FAST son recomendables para redes de medianas empresas, en donde la información tiene importancia, pero no es la base fundamental para la operación de la empresa. También hay que considerar que soluciones como LEAP y FAST son propietarias y por lo tanto, requieren equipos Cisco para ser implementadas.

Cuando se requiere compatibilidad e interoperabilidad, lo mejor que se puede escoger son las soluciones basadas en estándares, Desafío MD5 y EAP-TLS, ya que son ideales. EAP-FAST y EAP-TTLS se encuentran en desarrollo, aunque el draft de EAP-TTLS se encuentra caducado.

Para empresas con redes corporativas o para empresas en donde la información es crítica, lo más recomendable es la implementación con soluciones que involucren certificados digitales como EAP- TLS, PEAP y EAP – TTLS, pues brindan mayores niveles de seguridad.

Para PEAP y EAP-TTLS se requiere la creación de una autoridad certificadora, pues solo se necesita expedir certificados para los servidores y por lo tanto, no se requiere de una infraestructura que consuma mayores recursos.

En cambio, EAP-TLS requiere de la implementación de una PKI, lo que implica una inversión de tiempo y dinero e incremento en los procesos de administración; en este caso, es obligatoria una política de seguridad. Esta solución garantiza un alto nivel de seguridad debido a que establece un túnel seguro y la autenticación mutua se lleva a cabo con el uso de certificados digitales.

Por otra parte, debido a que EAP-TLS involucra expedición de certificados para los clientes de una WLAN, también provee herramientas para asegurar el servicio de

aceptación, por lo que es ideal para empresas en donde se realiza transacciones entre los usuarios.

La implementación de EAP-TLS en muchos casos puede aumentar la complejidad de la administración de una red; pero en redes con usuarios distribuidos en distintas zonas geográficas, facilita los procesos de administración que tienen que ver con el control de usuarios, pues se puede establecer una AC subordinada por cada zona mediante una jerarquía. Así se establece la identidad de un usuario y se lo ubica en una zona determinada y de ser necesario en un departamento de la empresa.

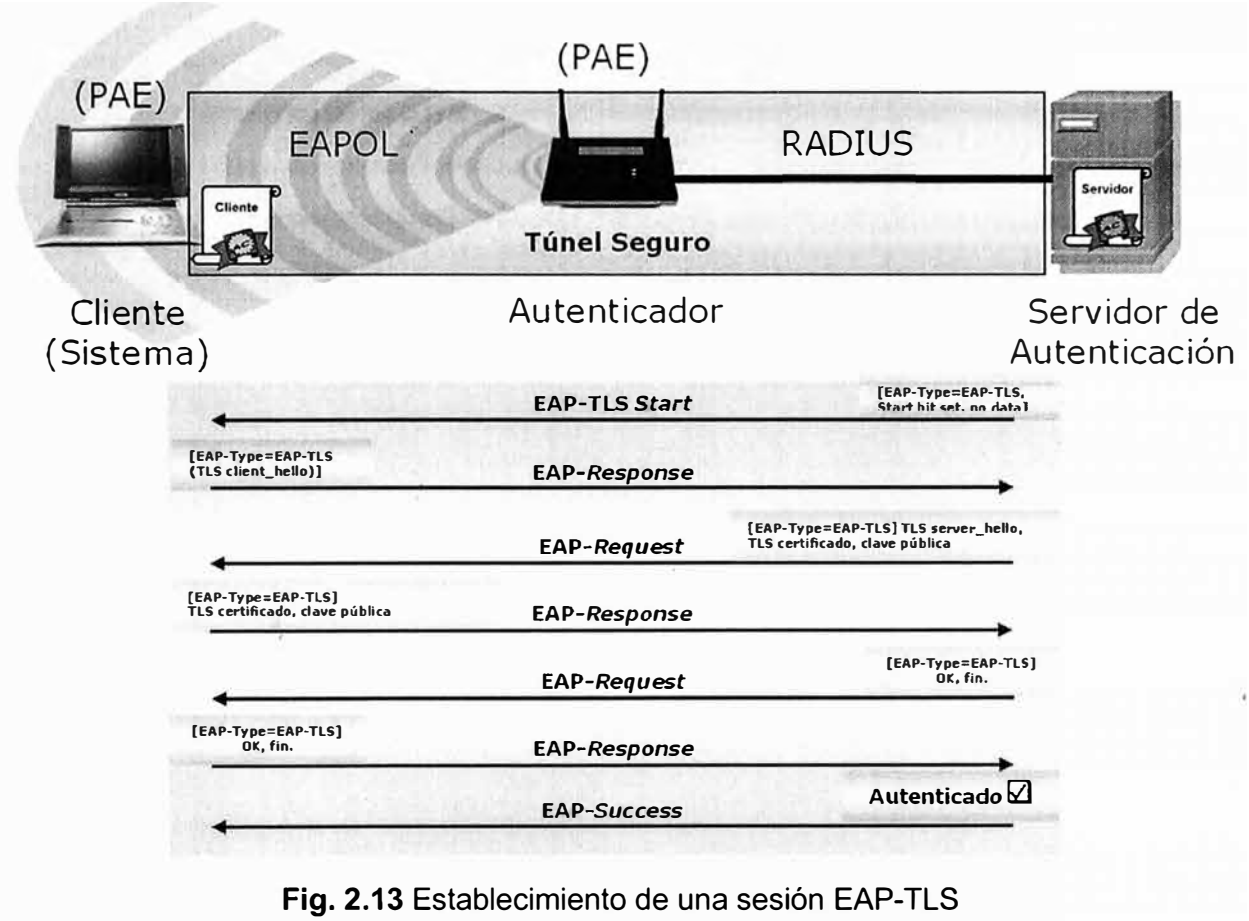


Fig. 2.13 Establecimiento de una sesión EAP-TLS

2.2.13 Ventajas y Desventajas de EAP-TLS

Entre las principales ventajas de EAP-TLS, con respecto otras técnicas utilizadas para brindar seguridad dentro de redes WLAN, se pueden mencionar:

- Utiliza certificados digitales como credenciales de clientes y servidores.
- Establece una autenticación con un alto nivel de seguridad.
- Facilita el establecimiento del servicio de aceptación.
- Establece facilidades para la administración de acuerdo a la ubicación geográfica de un usuario e incluso, al área en que se desempeña.

- Permite un mayor control de los usuarios.
- Brinda confidencialidad de la información al establecer un túnel seguro.
- Es la solución que brinda el mayor nivel de seguridad para WLANs.
- Es un estándar lo que garantiza compatibilidad e interoperabilidad con varias plataformas.

Entre las principales desventajas de EAP-TLS, con respecto otras técnicas utilizadas para brindar seguridad dentro de redes WLAN, se pueden mencionar:

- Requiere de la implementación de una PKI en redes pequeñas. Esto incrementa innecesariamente los costos y los procesos de administración.
- El establecimiento de un túnel seguro requiere que los equipos tengan mayores capacidades, para que esto resulte transparente para los usuarios.
- Se encuentra poco difundida debido a que requiere de una infraestructura compleja.

2.3 Definiciones de Infraestructura para Certificados Digitales

Hemos mencionado la importancia del esquema EAP/TLS como unos de los esquemas de seguridad más seguros para implementaciones de redes wireless (en opinión de algunos el más seguro). También hemos visto que EAP/TLS usa certificados digitales para autenticar, tanto al usuario como al servidor.

A continuación vamos a revisar algunos de los más importantes conceptos referidos a los certificados digitales, que nos permitirán entender mejor el capítulo III del presente trabajo.

2.3.1 Encriptación Asimétrica: Clave Pública y Clave Privada

La encriptación asimétrica se basa en algoritmos que manejan matemáticas más complejas que las utilizadas en algoritmos simétricos. Los algoritmos asimétricos demandan la generación de dos claves relacionadas matemáticamente, una clave es conocida como clave privada y la otra como clave pública.

El principio básico de la encriptación asimétrica, es que sí se cifra un mensaje con una clave privada, éste solo puede descifrarse con su respectiva clave pública; y sí se cifra con una clave pública, solo se consigue descifrarlo con su clave privada.

Es importante aclarar que una de las dos claves, no puede por sí sola cifrar y descifrar un mensaje; además, no se puede obtener una clave a partir de la otra. Esto permite que la clave pública pueda estar disponible para todos los usuarios.

En cambio, la clave privada debe estar disponible solo para el dueño de la pareja de claves. Si se cumple con esta condición, se puede intercambiar información entre

usuarios sin la necesidad de establecer comunicaciones en las que se intercambie información con anterioridad; adicionalmente, se elimina el problema de la interceptación de claves.

2.3.2 Administración de Claves Públicas y Privadas

La administración de claves es un tema trascendental. Las claves públicas pueden estar disponibles, teóricamente, para todos los usuarios; sin embargo, es una práctica recomendable restringir el acceso, de modo que solo los interesados accedan a las claves. Debe existir una zona en la que los usuarios puedan obtener las claves públicas de los otros usuarios y publicar su propia clave

La administración de las claves privadas es más crítica, de acuerdo al propósito para el que se generaron las claves. Sí una clave privada fue generada con el propósito de cifrar datos y realizar firmas digitales, se requiere que estrictamente esté solo al alcance de quien generó la clave.

2.3.3 Función HASH

Una función hash es aquella que toma como entrada un mensaje y entrega como resultado un resumen conocido como valor hash; estas funciones tienen gran importancia en criptografía. Se puede verificar la integridad de un mensaje enviando el mensaje y su valor hash al receptor; en el destino, el receptor puede aplicar la misma función hash al mensaje y luego comparar su resultado con el valor recibido. Para evitar que un atacante cambie el mensaje y el valor hash introduciendo valores falsos, el valor hash debe enviarse cifrado con la clave privada del emisor.

2.3.4 Firma Digital

Las firmas digitales son producto de la combinación de funciones hash y encriptación asimétrica. En general, se dice que un usuario firma un mensaje de datos cuando lo cifra con su clave privada. Debido a que cifrar datos con encriptación asimétrica consume demasiados recursos, el concepto de firma digital se enfoca en cifrar el valor hash de un mensaje (por ser más pequeño); de esta manera, se garantiza autenticación e integridad.

2.3.5 Certificados Digitales

Un certificado digital, provee un mecanismo que permite obtener un mejor nivel de resistencia a la suplantación de claves públicas

Los certificados son credenciales digitales; en su forma más simple, un certificado contendrá una clave pública y el nombre de su propietario. De esta manera, el nombre del usuario queda unido a su clave; así se genera confianza en la legitimidad de una clave pública, protegiéndola de suplantación o alteración.

Por otra parte, se brinda un ambiente más amigable para los usuarios, debido a que ya no se tiene que buscar en un directorio la clave pública de un usuario en particular; ahora se podrá descargar su certificado digital.

Este certificado Digital es emitido y firmado digitalmente por una entidad tercera, en la que las partes confían plenamente. Esta entidad recibe el nombre de Autoridad Certificadora.

El certificado puede tener la forma de un archivo electrónico cuya estructura se muestra por ejemplo en la Fig. 2.14 en la siguiente página

2.3.6 Infraestructura de Claves Públicas

La encriptación asimétrica y el uso de certificados digitales proporciona herramientas apropiadas para la implementación de servicios de seguridad, como es el caso de: autenticación, confidencialidad, integridad y aceptación. Sin embargo, requiere de una infraestructura que brinde un sistema adecuado de administración de certificados digitales y parejas de claves.

Esta infraestructura es conocida como PKI (Infraestructura de Claves Públicas). Aunque la complejidad de una arquitectura PKI depende de los servicios a los que estará destinada, en general cuenta con elementos que le permiten mantener un nivel razonable de confianza.

2.3.7 Autoridad Certificadora

En general, se conoce al tercero de confianza como AC (Autoridad Certificadora), debido a que se encarga de verificar la identidad de cada usuario y la autenticidad de sus claves pública/privada, luego de lo cual vincula el nombre del usuario y su clave pública a un certificado digital.

Para evitar que los certificados generados por una determinada AC sean alterados posteriormente, ésta firma digitalmente cada certificado, de esta manera los certificados se vuelven una estructura auto-protegida.

Para que el usuario A pueda confiar en la identidad registrada en el certificado del usuario B, y a su vez, el usuario B en la identidad registrada en el certificado del usuario A sin la necesidad de conocerse previamente, pueden acudir a una AC que goce de la confianza de los dos, y que certifique la legitimidad de sus identidades y la

correspondencia entre las parejas de claves por medio de la expedición de un certificado digital.

2.3.8 EAP –TLS en Wireless LAN y la PKI

Un PKI ofrece el ambiente ideal para cualquier aplicación que requiera proveer de los servicios de autenticación, confidencialidad, integridad y aceptación con niveles razonables de confianza y seguridad; por lo mismo, existen muchas aplicaciones que utilizan certificados digitales.

Como se vió dentro del numeral 2.3, EAL-TLS se encuentra registrado en el RFC 2716 y provee autenticación con el más alto nivel de seguridad por medio de certificados digitales dentro de WLANs. Durante el proceso de autenticación, todos los miembros de la WLAN utilizan certificados digitales para autenticarse mutuamente (clientes y servidor); por lo tanto, el número de certificados a expedirse es elevado. Por este motivo EAP-TLS necesita de una infraestructura que permita mantener una administración adecuada de éstos. Además, a pesar de que la implementación de una PKI puede resultar compleja, introduce herramientas que permiten gestionar las credenciales de los usuarios dentro de la WLAN, manteniendo niveles adecuados de seguridad y escalabilidad. EAP-TLS es necesario dentro redes corporativas con un gran número de usuarios móviles, distribuidos en distintas áreas geográficas u organizacionales; también es necesario para empresas que transmiten a través de medios inalámbricos información que consideren estratégica.

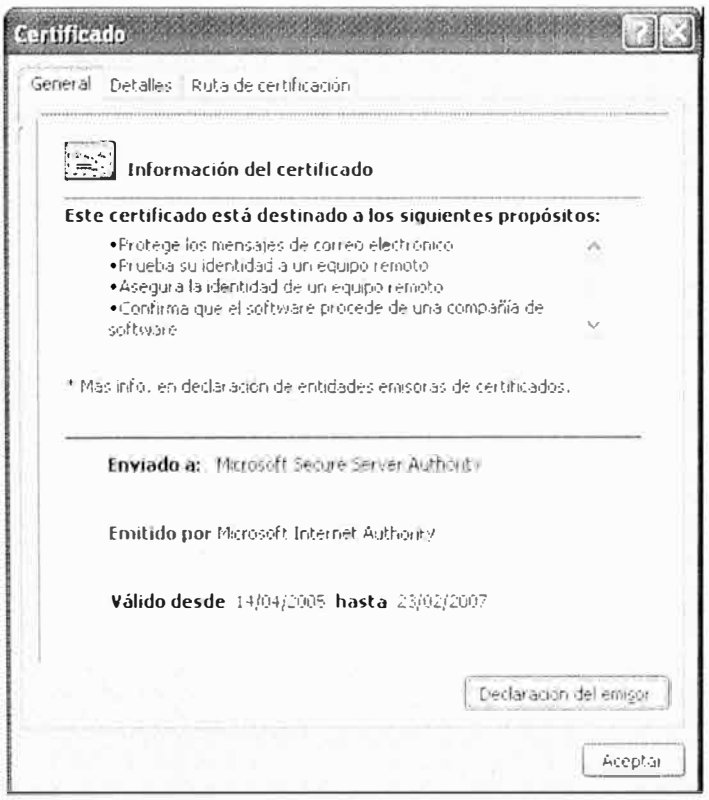


Fig. 2.14 Certificado Digital Real

CAPÍTULO III

EXPOSICION DE LA IMPLEMENTACION PROPUESTA

3.1 Introducción

En cuanto a su infraestructura física, las Oficinas de nuestro caso, CORPORACION SAN ANDRES, se ubican en un edificio de 10 pisos. El edificio consta de dos alas. En el ala izquierda del edificio se ubican generalmente, las Gerencias y secretarias, aquí las divisiones son básicamente de material dry-wall. En el ala derecha están ubicadas las oficinas del personal, salas de reuniones, auditorio, etc y las divisiones aquí son de paredes de ladrillo, aunque no tan gruesas.

El objetivo del proyecto es cubrir los 10 pisos con un nivel de señal óptimo que se ha definido en un valor límite de -60 dbm, en el peor caso. Se ha propuesto atender dos tipos de usuarios: usuarios corporativos (internos) y visitantes (externos), cada uno con capacidades y características funcionales específicas. Se ha realizado el site Surrey respectivo y a continuación se mostrarán los resultados del mismo piso por piso.

En cuanto a infraestructura de TI, la CORPORACION SAN ANDRES tiene una red de acceso del tipo Fast Ethernet con equipos Cisco serie 2960. El backbone que es controlado por un equipo de marca Cisco modelo Catalyst 4510R como equipo de Core, es del tipo Gigabit Ethernet. Los Sistemas operativos son Windows y se cuenta con un Directorio Activo Basado en Windows 2003 Server, cuyo dominio es sanandres.

3.2 Estudio de Site Survey Propuesto

3.2.1 Herramientas Utilizadas

Para el estudio de campo se ha usado una laptop COMPAQ modelo Presario C760LA, con procesador Intel T5450 Core 2 Duo y una tarjeta wireless marca INTEL modelo INTEL PRO 3945ABG.

El equipo Access Point utilizado, es un equipo AIRONET modelo Cisco 1231AG en su versión de equipo autónomo. Este equipo puede trabajar en entornos Indoor y acepta antenas externas de 2.4 GHz y 5.8 GHz.El tipo de antena utilizada es la antena de 2.4 Ghz, modelo AIR-ANT5959 de la marca Cisco, es una antena omnidireccional de 2.2 dbi. Se ha escogido este tipo de antenas siguiendo las recomendaciones del fabricante Cisco, para plataformas multiservicio de voz y datos (20).

El software de análisis es la herramienta Wireless Mon que permite evaluar el nivel de la señal de manera bastante precisa.(Ver Fig. 3.1 con el Logo del Producto).

Fig. 3.1 Programa Wireless Mon usado para el Site Survey.

3.2.2 Consideraciones Previas al Site Survey

El estudio por piso ha considerado dos aspectos importantes: cobertura y capacidad. Para la cobertura ya se indicó que se utilizaría un mínimo de señal de -60 dbm. La capacidad se analizará en términos de la demanda media estimada.

Revisando la demanda de usuarios de uno u otro tipo se ha elaborado la Tabla 3.1 por piso, donde podremos evaluar cuantitativamente el número de Access Point mínimo requeridos. En la Tabla 3.1, la columna I y V representan la cantidad de usuarios por piso según sea corporativo o visitante respectivamente.

La columna Total (T) calcula la demanda total en Mbps considerando un consumo máximo de 5 Mbps para el usuario tipo I y de 2 Mbps como máximo para el usuario tipo V. En ambos casos las demandas parciales se multiplican por un factor de simultaneidad que atenúa cada producto considerando que no todos los usuarios accederán de manera simultánea. (se considera 0.3 para los usuarios tipo I y de 0.5 para los usuarios tipo V)

Finalmente la última columna divide el valor de T, entre la capacidad efectiva de un access point 802.11g. Un valor razonable es 24Mbps. Este resultado nos dará una

idea de cuantos access point por piso como mínimo son necesarios para atender la demanda. Obviamente este factor no toma en cuenta la distribución física de los usuarios pero nos pone una línea base inferior para trabajar.

Tabla 3.1 : Cantidad de Access Points según Demanda

Piso	Usuario Corporativo (I)	Usuario Visitantes (V)	Total[(Mbps) = (Ix5x0.3)+(Vx2x0.5)] (T)	Mínimo Número de APs por Piso = (T/24)
1	4	4	10	0.4
2	10	4	19	0.8
3	10	4	19	0.8
4	12	10	28	1.2
5	10	30	45	1.9
6	10	4	19	0.8
7	12	4	22	0.9
8	10	4	19	0.8
9	10	4	19	0.8
10	5	4	11.5	0.5

Seguidamente mostraremos el análisis de Site Survey desarrollado para encontrar el número de access point necesarios para la cobertura solicitada.

3.2.3 Resultado del Site Survey

A continuación, se muestra el resultado del análisis piso por piso, así como comentarios y observaciones del mismo.

a. Primer Piso : Recepción.

En la Fig. 3.2 se tiene el resultado del estudio de cobertura para el primer piso. Son 3 access point los considerados. En el ala izquierda se considera un único access point para brindar una señal óptima a los visitantes. En el ala derecha, Auditorio, se han considerado dos access point. Si bien el Auditorio se podría cubrir con un único access point, se han colocado dos para soportar mayor simultaneidad de usuarios. Con esta configuración podría soportarse hasta 40 usuarios del tipo invitado en el Auditorio

trabajando en simultáneo. En el estudio, como se muestra en la Fig. 3.3 el nivel de señal en los ambientes es óptimo manejándose niveles entre -40dBm y -50 dBm.

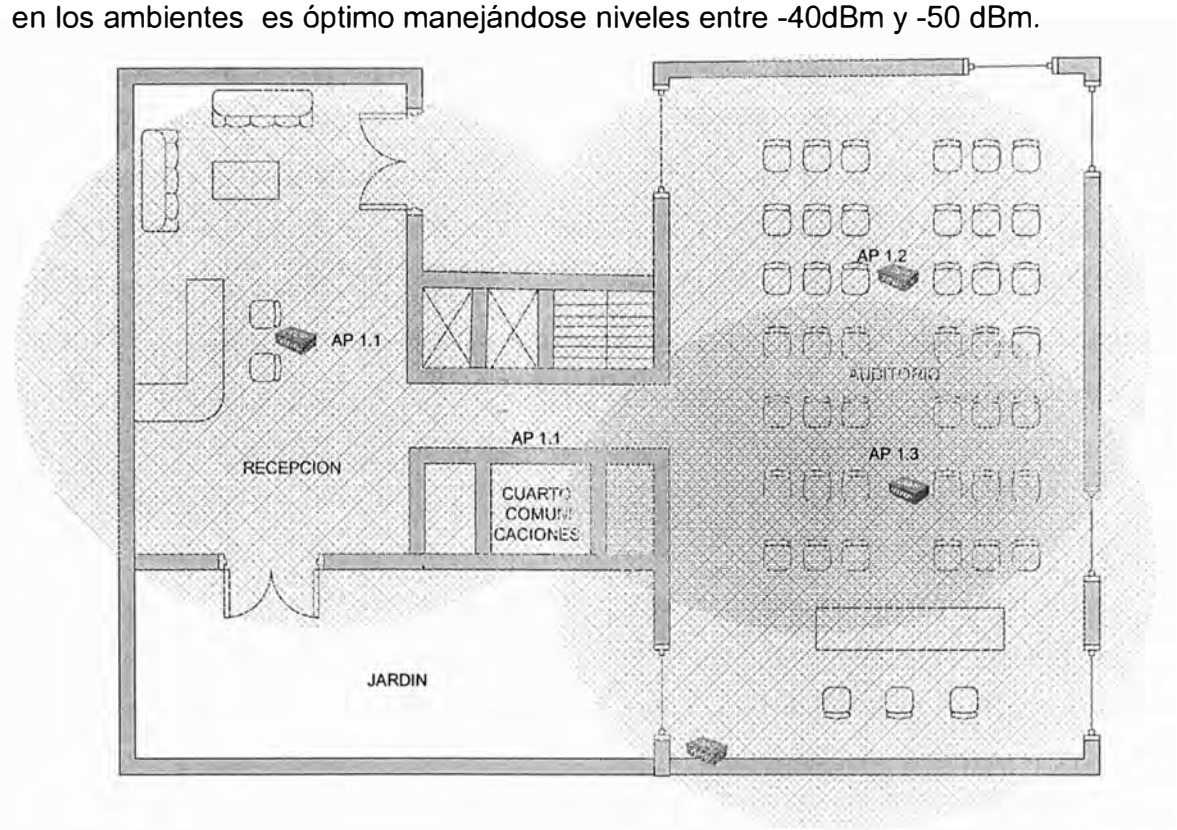


Fig. 3.2 Cobertura Wireless Planta Primer Piso

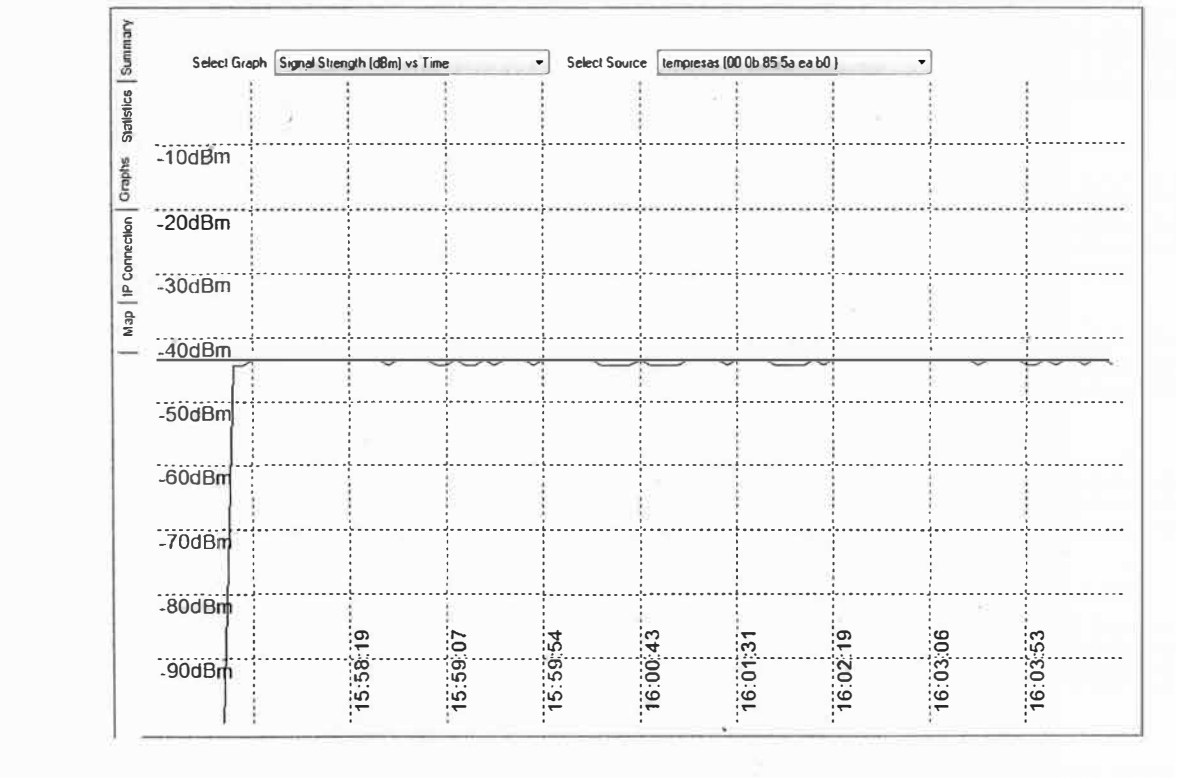


Fig. 3.3 Medición de Señal en promedio en los ambientes Plata Primer Piso.

b. Segundo Piso : Administración

El nivel de señal en los ambientes de la izquierda se encuentra, en promedio, en -45 dbm, como se puede ver en el reporte del software (Fig. 3.5), con un único access point, lo cual es suficiente.

El nivel de señal en los ambientes extremos de la derecha (Contador 1, Atención de Pedidos, Servicios Generales), considerando un único access point al centro se muestra en la Fig. 3.6. El nivel de cobertura con dos access points mejora notablemente en estos ambientes, como se puede ver en la Fig. 3.7.

Comparando ambos resultados, se resuelve considerar dos access points como indica la Fig. 3.4. El nivel de cobertura, si bien podría parecer excesivo, es el conveniente para preparar la red para futuras implementaciones de tráfico de VoIP o algún otro que requiera un óptimo nivel de señal.

El AP 2.1 será ubicado tras la pared de DryWall de la sala de reuniones del ala derecha, esto es conveniente por la baja atenuación. El AP2.2 y el AP2.3 se instalarán dentro del falso techo del piso, quedando visibles únicamente las antenas, evitando posibles atenuaciones y pérdidas por la estructura metálica del techo.

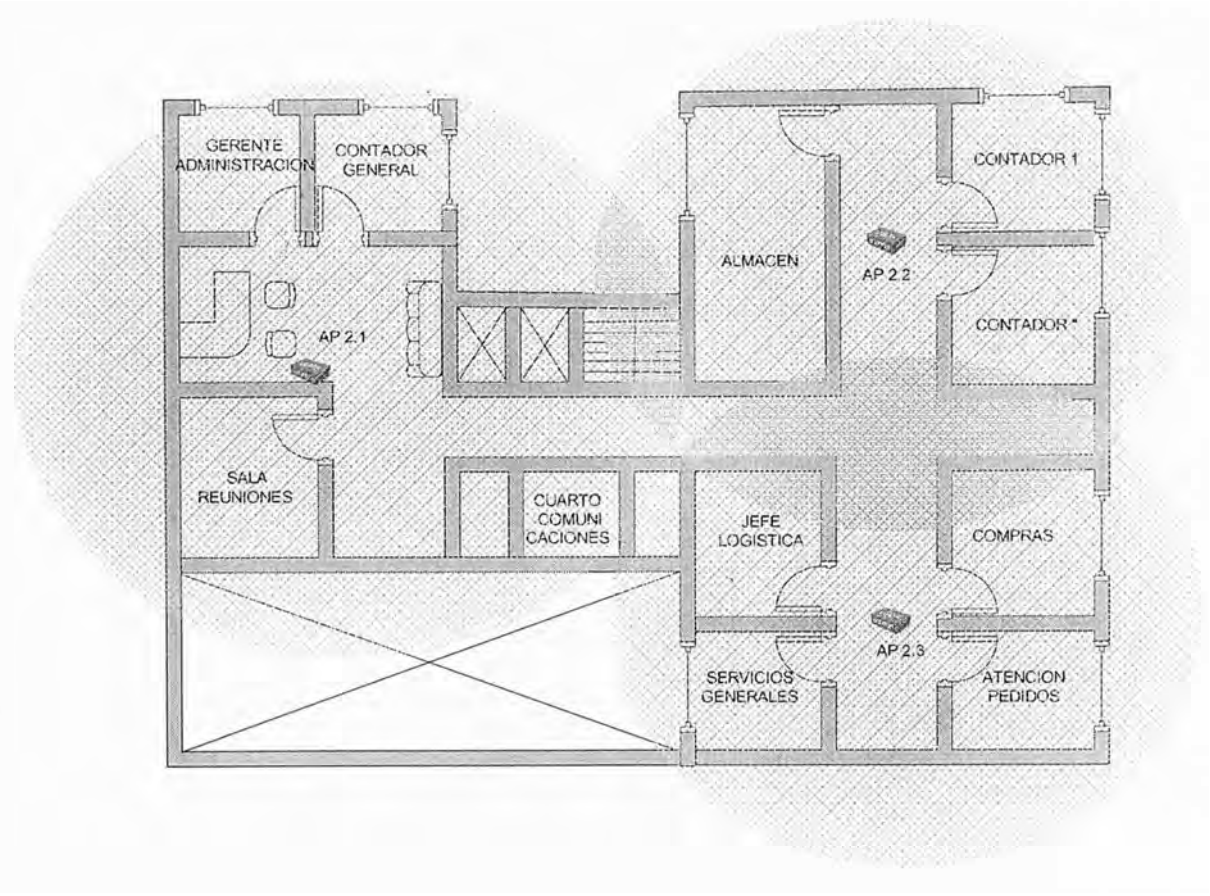


Fig. 3.4 Cobertura Wireless Planta Segundo Piso

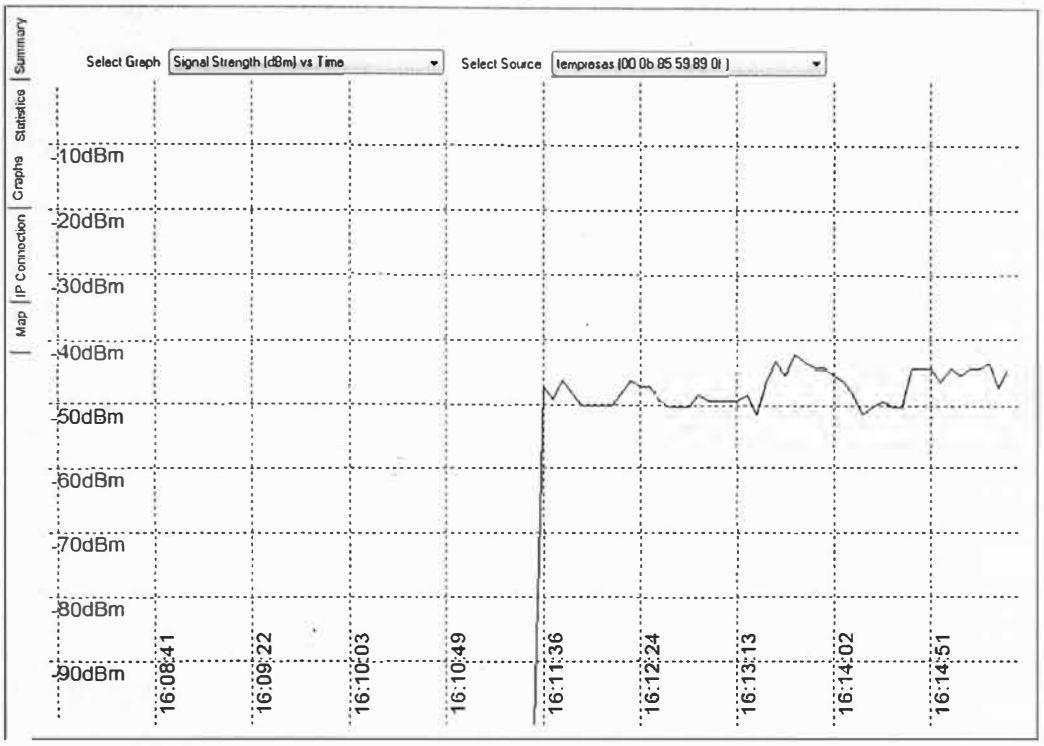


Fig. 3.5 Medición de Señal en el ala izquierda Planta Segundo Piso

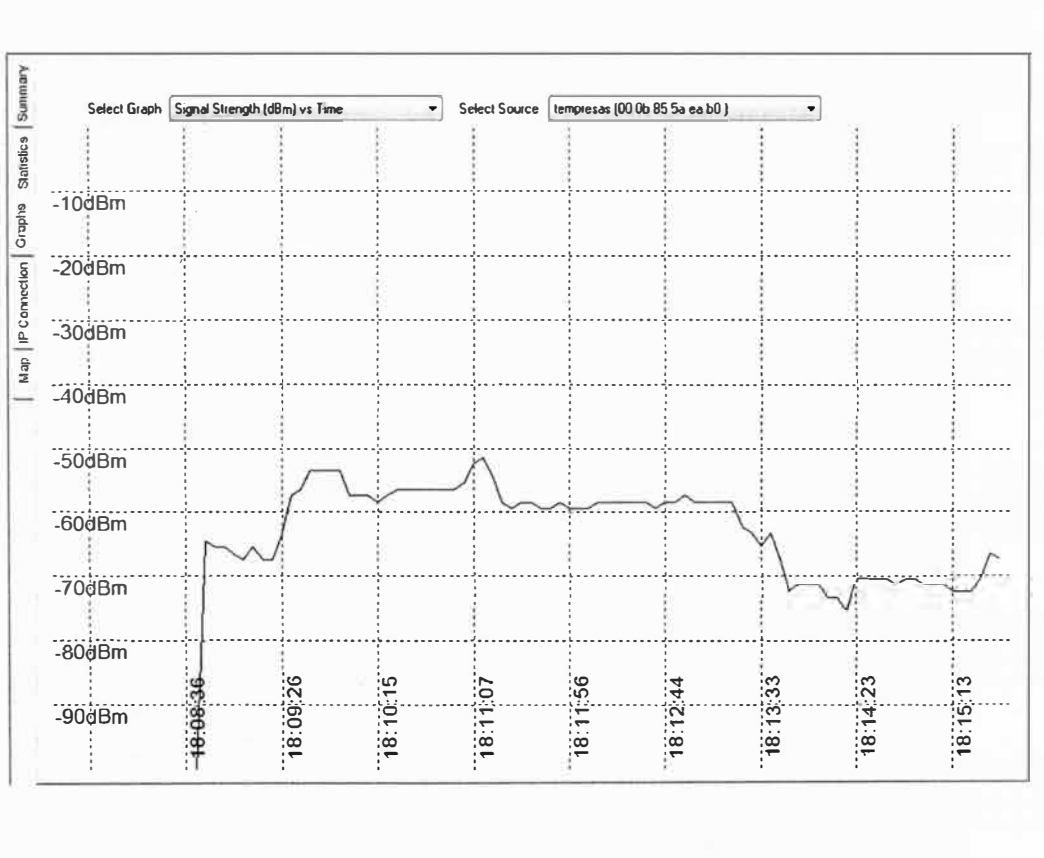


Fig. 3.6 Medición de Señal Ala Derecha Segundo Piso con un Access Point.

Comparando Fig. 3.6 y Fig. 3.7 es notoria la diferencia de señales en ambos casos.

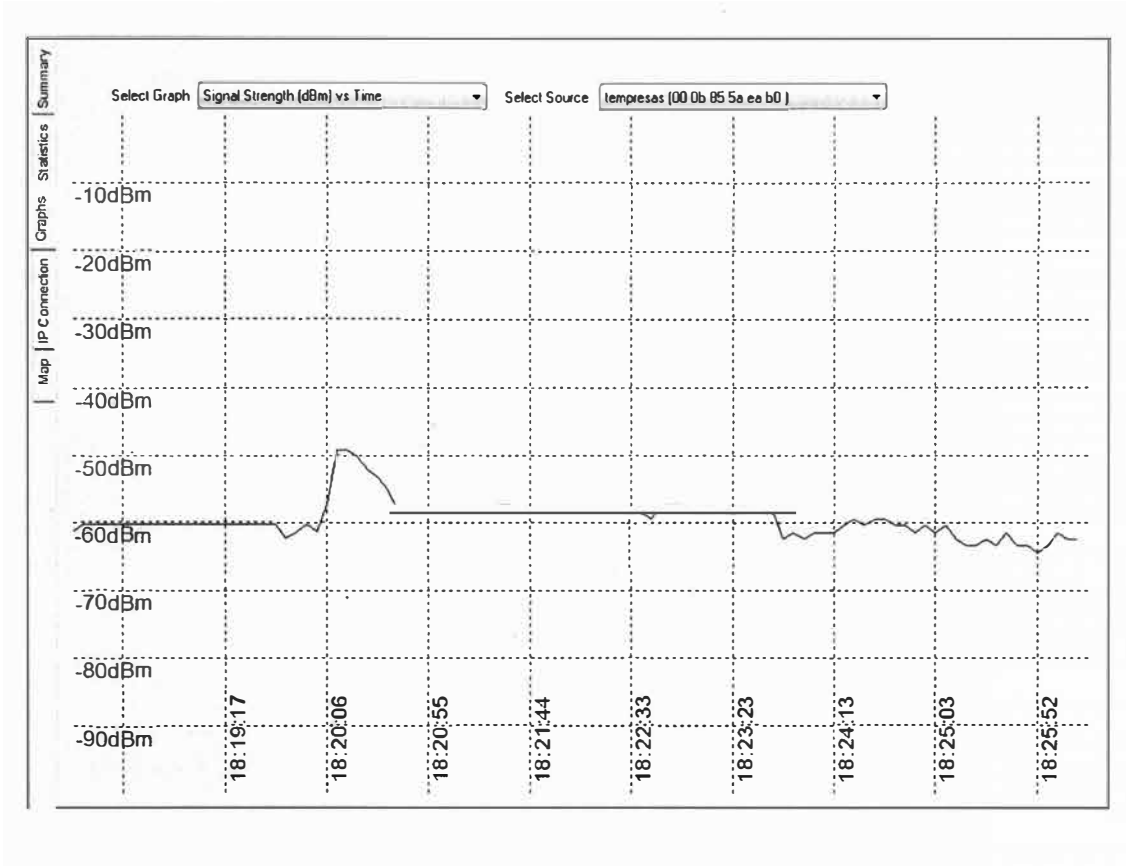


Fig. 3.7 Medición de Señal Ala Derecha Segundo Piso con dos Access Point

c. Tercer Piso : Finanzas

La distribución es similar a la segunda planta.

Se consideran tres access points, como indica la Fig. 3.8

d. Cuarto Piso : Proyectos

La distribución es similar a la segunda planta.

Se consideran tres access points, como indica la Fig. 3.9

e. Quinto Piso : Recursos Humanos

La distribución es un poco distinta al resto de pisos, como puede apreciarse en la Fig. 3.10.

El ala izquierda es similar al resto de pisos y por ende, y se considera un único access point.

En el ala derecha se tienen dos ambientes de capacitación. Según nos indican, con capacidad de hasta 20 alumnos cada uno. Por el criterio de simultaneidad, se considera un AP por ambiente. El nivel de señal para estas dos salas se muestras en la Fig. 3.11 y es en promedio, de -40dbm.

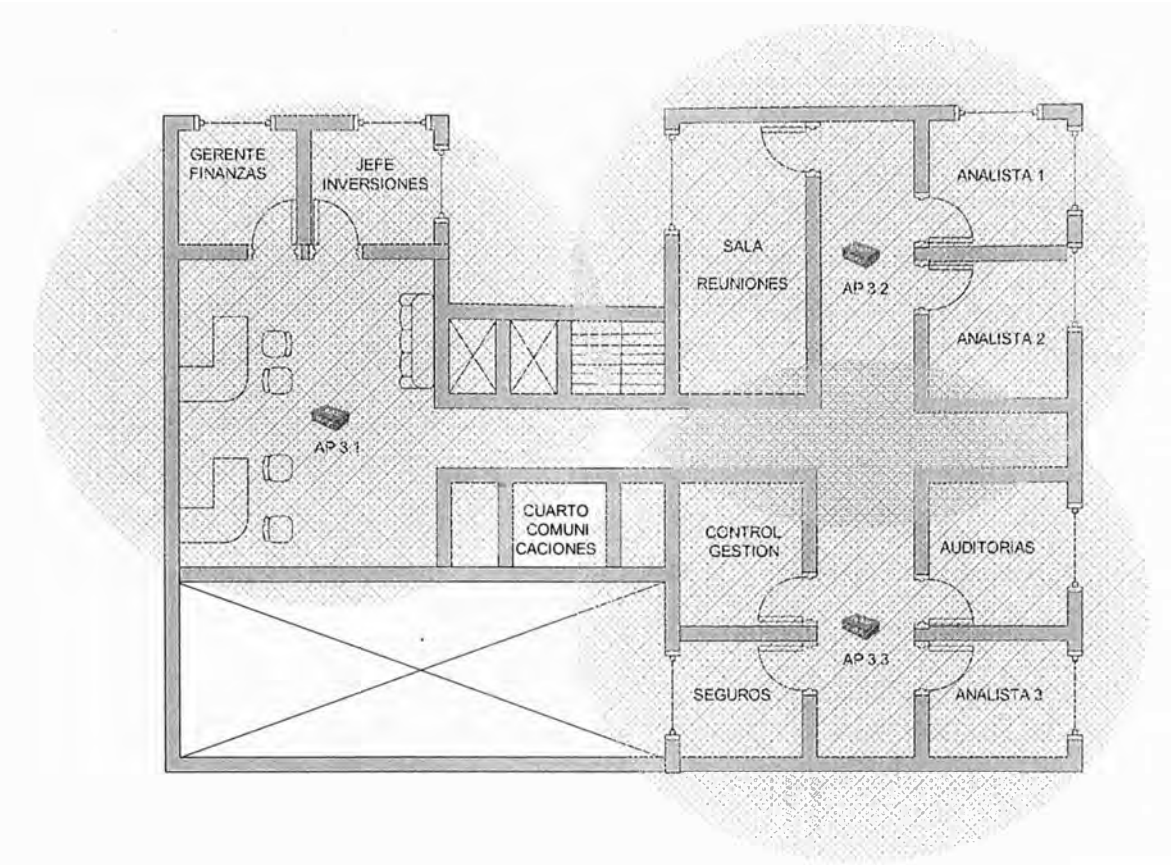


Fig. 3.8 Cobertura Wireless Planta Tercer Piso

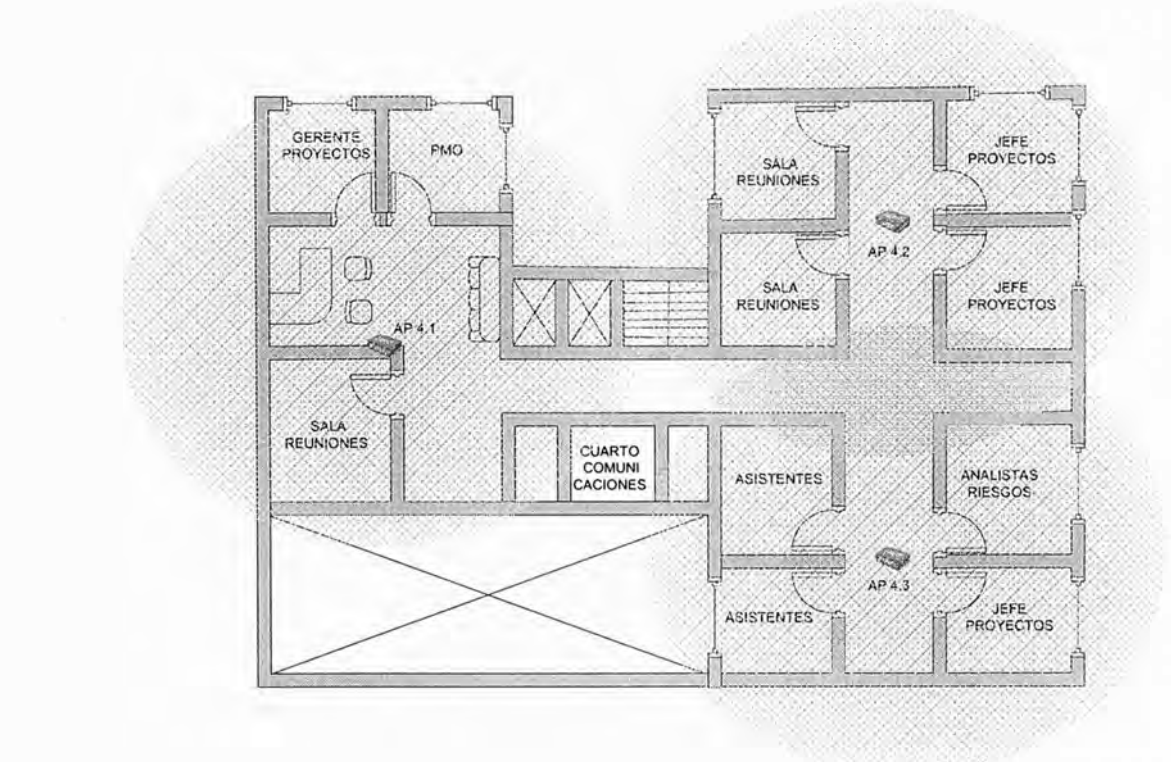


Fig. 3.9 Cobertura Wireless Planta Cuarto Piso

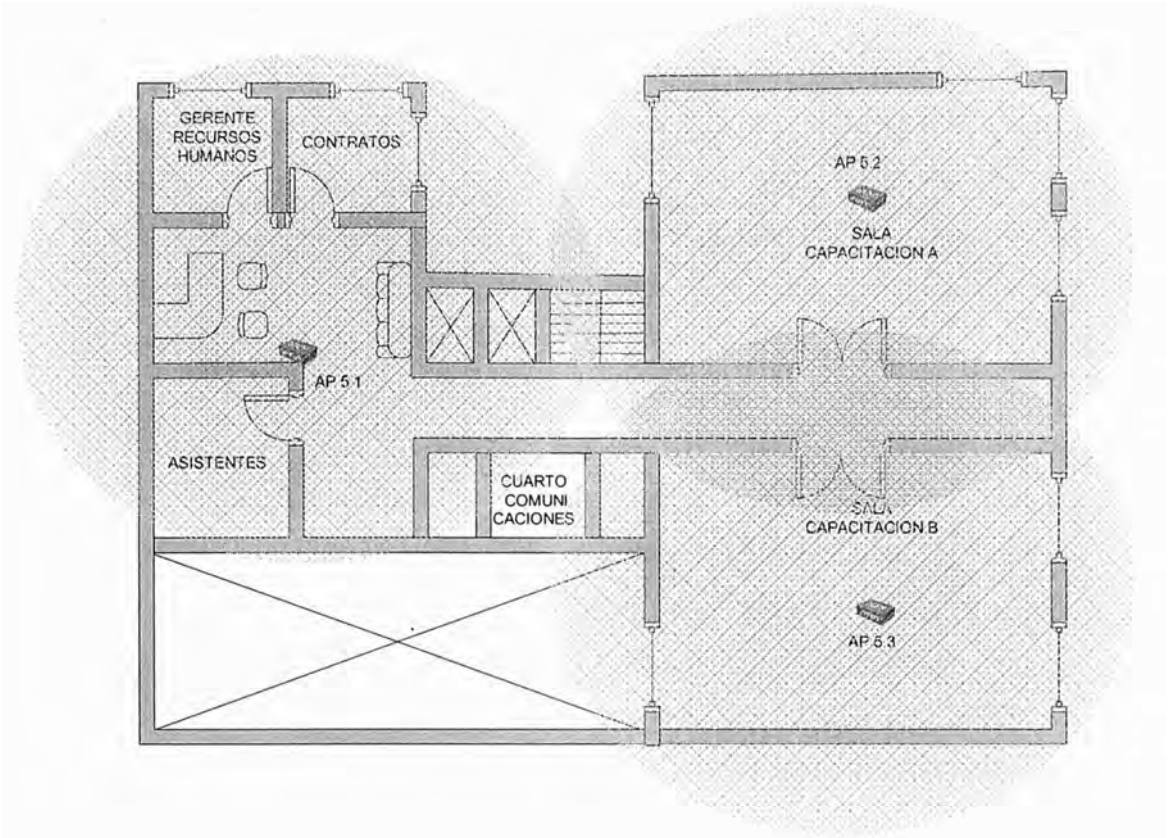


Fig. 3.10 Cobertura Wireless Planta Quinto Piso

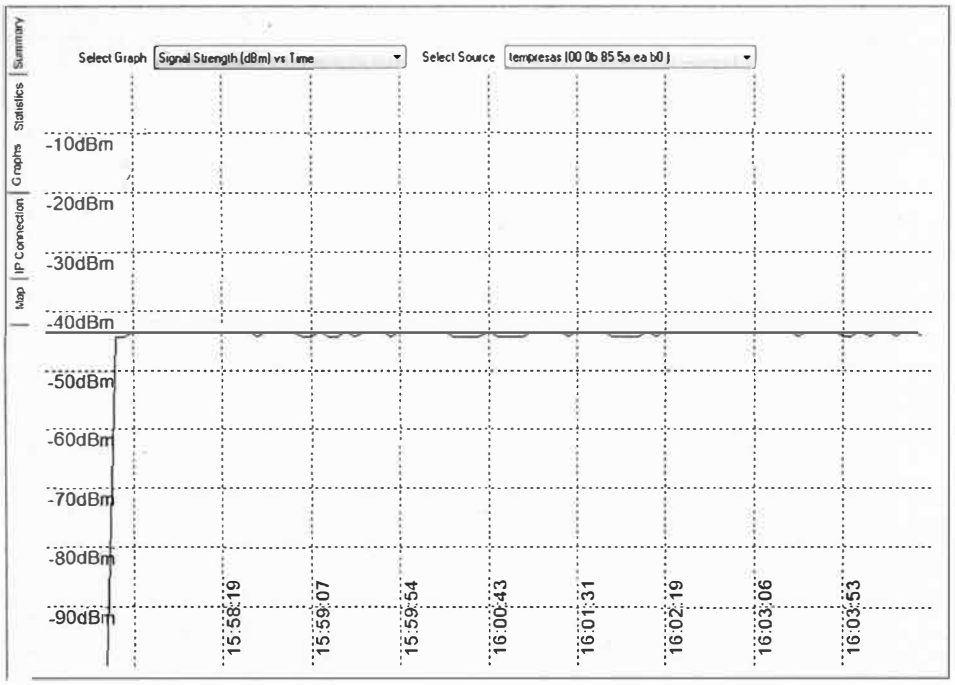


Fig. 3.11 Medición de Señal elas salas de Capacitación.

f. Sexto Piso : Legal

La distribución es similar a la segunda planta, como se ve en la Fig. 3.12

Se consideran tres access points, como indica la Fig. 3.12

g. Sétimo Piso : Sistemas

La distribución de ambientes en este piso, es similar al de la segunda planta.

Replicando el mismo modelo de cobertura que el segundo piso se van a considerar tres access points como indica la Fig. 3.13.

Bajo este criterio, los niveles deben ser los mismos que la segunda planta, los mismos que se indican en la Fig. 3.7.

h. Octavo Piso : Marketing

La distribución de ambientes de este piso difiere un tanto del resto. En el ala derecha se tienen menos ambientes que cubrir.

Como se indica en la Fig. 3.14, se coloca un único access point en la parte central del ala derecha y otro access point en el ala izquierda, como el resto de pisos.

El resultado del nivel de señal en el ala izquierda con un único access point, se muestra en la Fig. 3.15.

El nivel de señal está alrededor de -60 dbm, que resulta en un valor adecuado.

i. Noveno Piso : Ventas

La distribución de ambientes de este piso es similar al octavo piso, como se en la Fig. 3.16, con una menor cantidad de oficinas que cubrir en el ala derecha.

Se consideran dos access points similar al piso ocho, como indica la Fig. 3.16

j. Decimo Piso : Vicepresidencia y Gerencia General.

La distribución de ambientes es similar a la segunda planta, salvo por el ambiente de sala de directorio.

Para este ambiente, se considera la instalación de un access point en su interior, con esto se logra un óptimo nivel de señal, que la señal mejore notablemente brindando simultaneidad y capacidad suficiente para la capacidad de la sala directorio, que se asume entre 5 a 6 usuarios como máximo.

Finalmente, se considerarán tres access points, como indica la Fig. 3.17.

3.2.4 Resumen del Estudio de Cobertura

En la Tabla 3.2 se resumen las cantidades de equipamiento necesarios. Como nos podemos dar cuenta, el número final de la Tabla 3.2 cubre las necesidades de capacidad requeridas por la Tabla 3.1.

En conclusión el Proyecto considerará la instalación de 28 equipos access point, con los cuales se espera lograr un excelente nivel de cobertura.

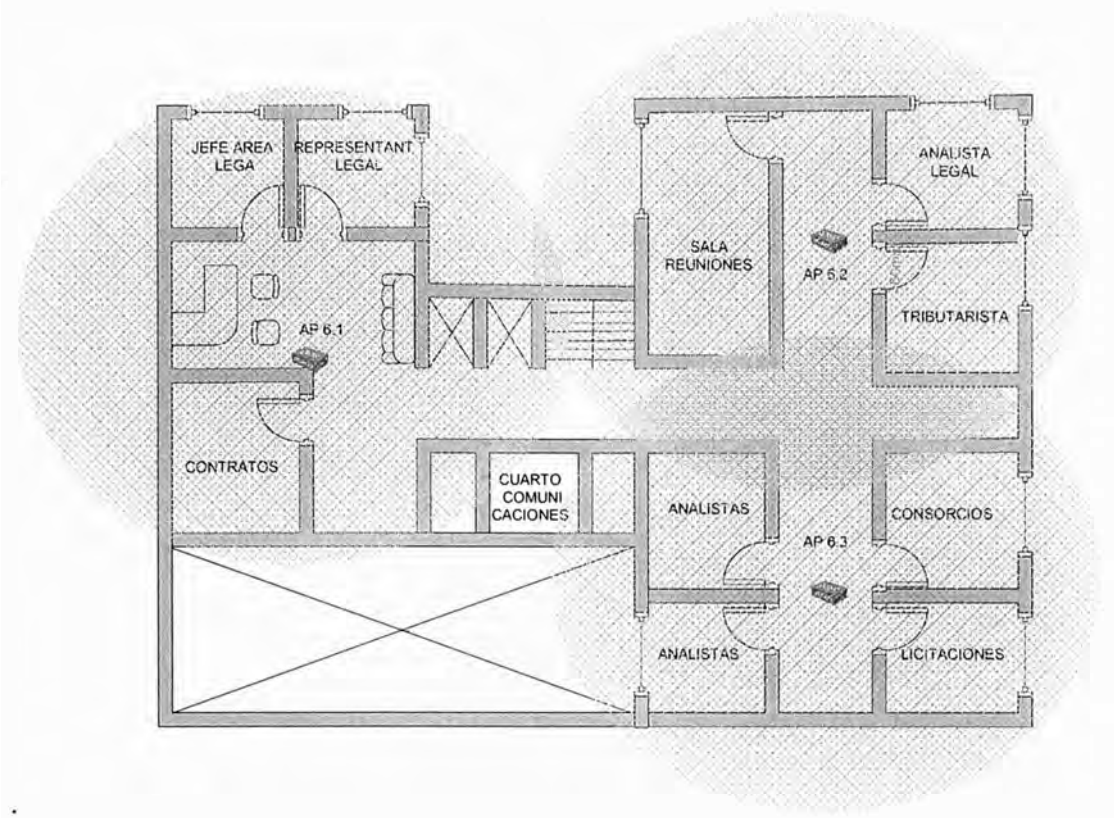


Fig. 3.12 Cobertura Wireless Planta Sexto Piso

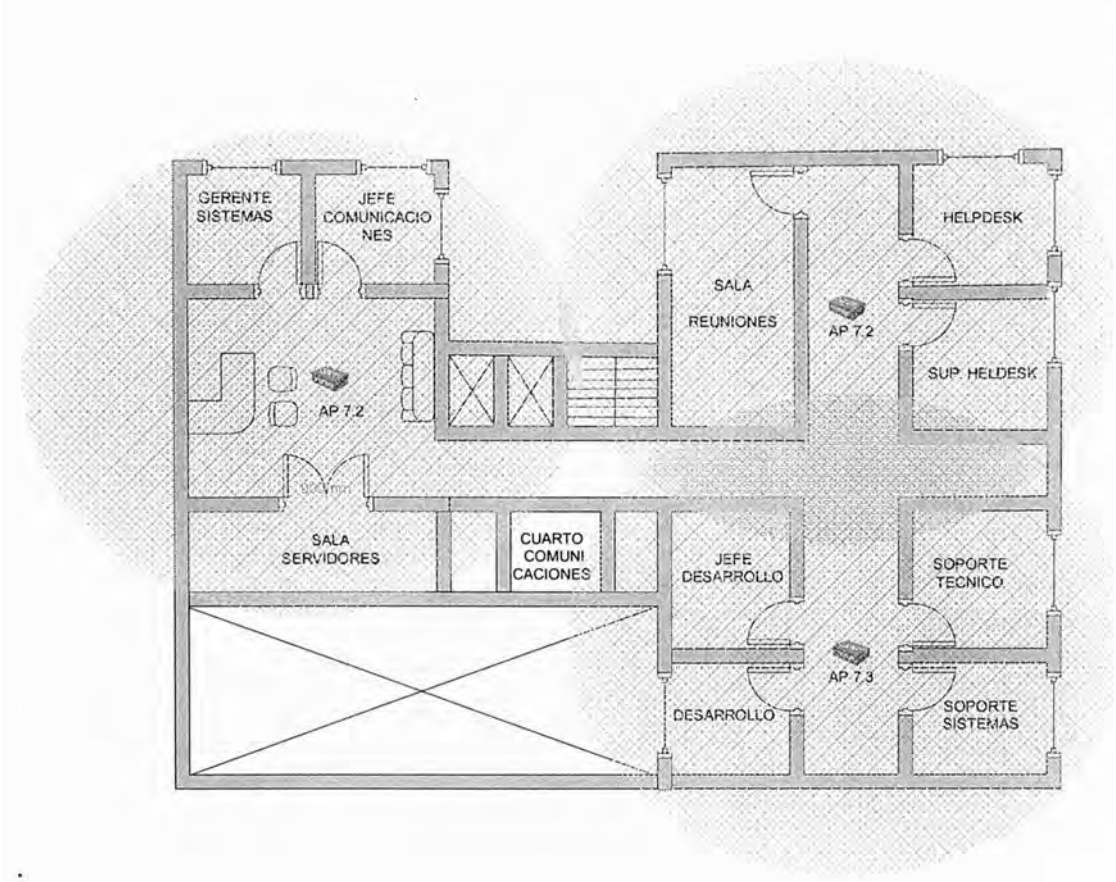


Fig. 3.13 Cobertura Wireless Planta Sétimo Piso

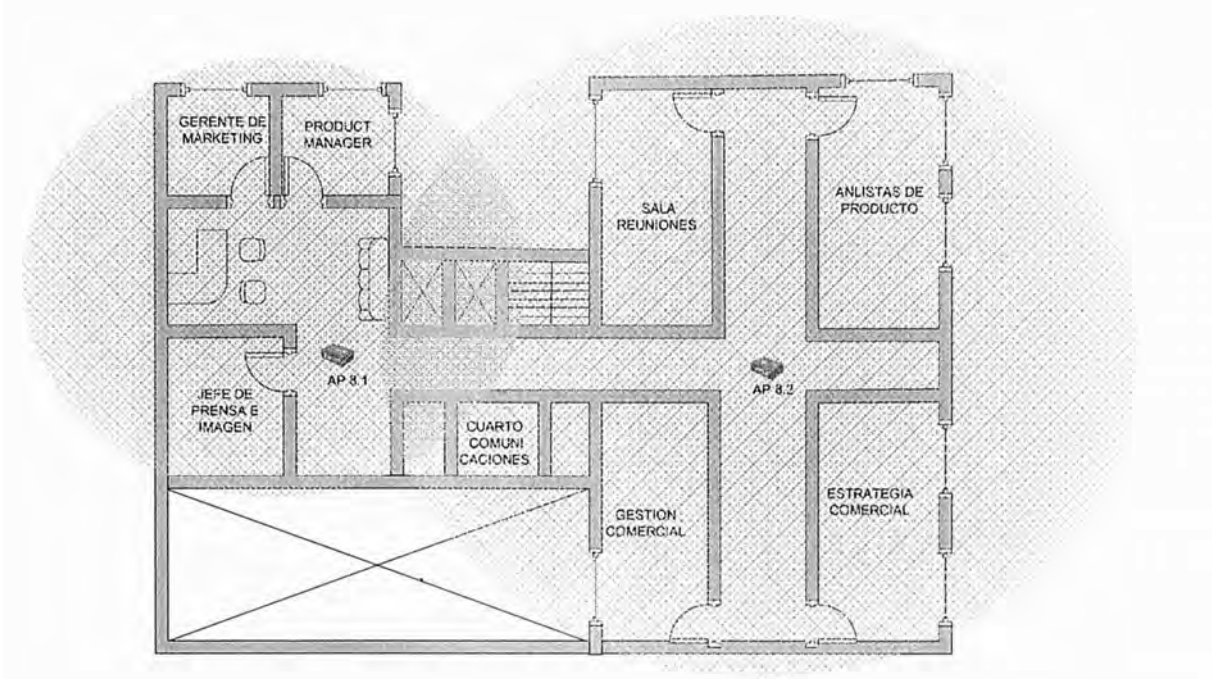


Fig. 3.14 Cobertura Wireless Planta Octavo Piso

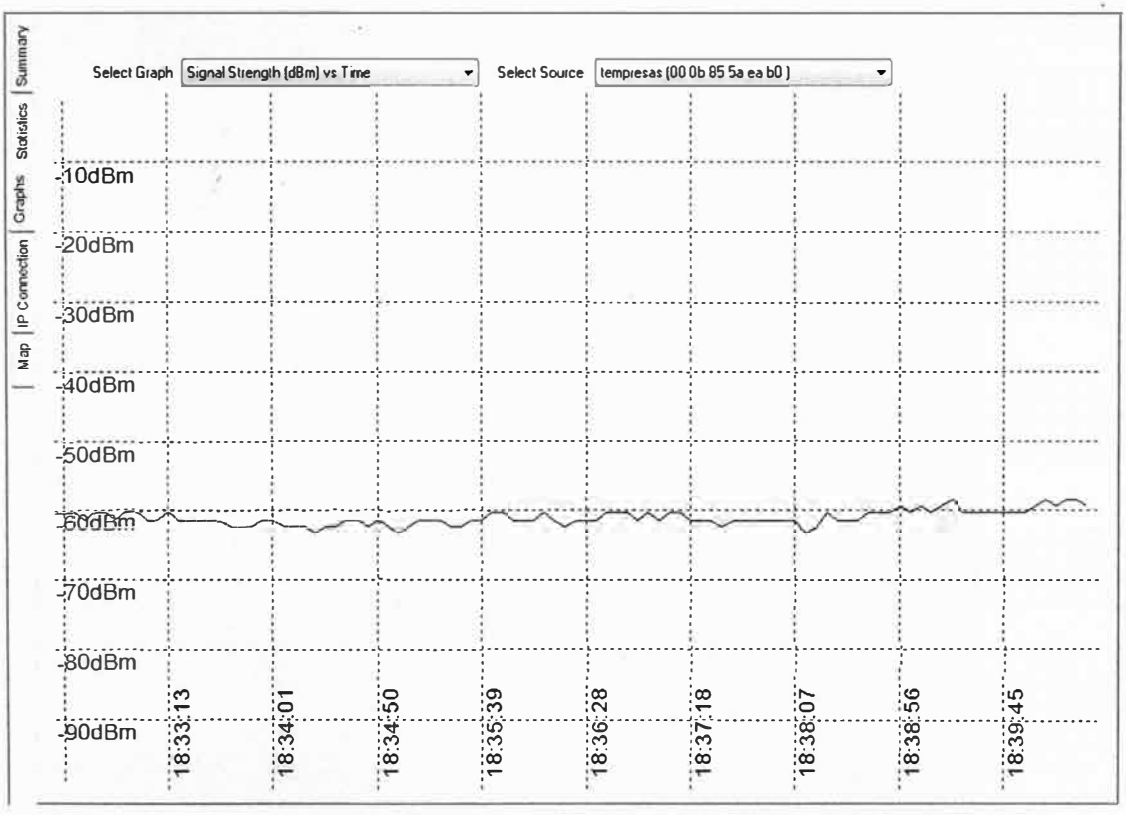


Fig. 3.15 Medición de Señal en el ala derecha Planta Octavo Piso.

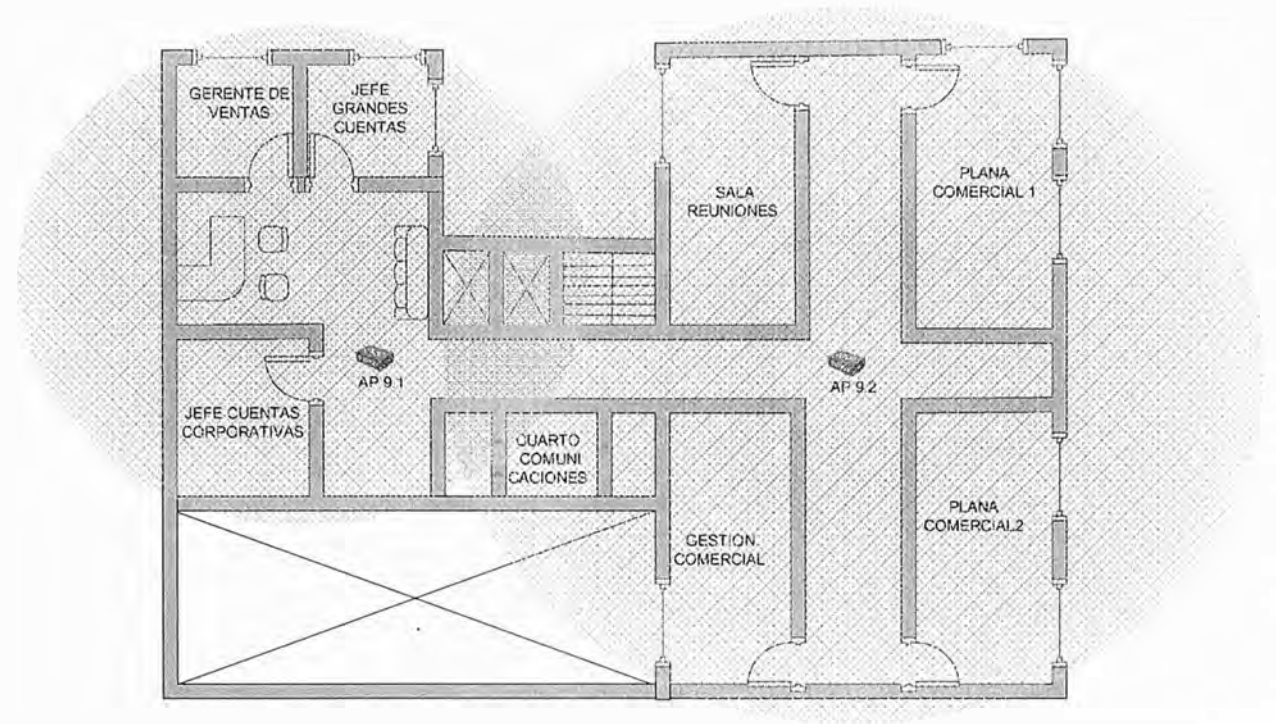


Fig. 3.16 Cobertura Wireless Planta Noveno Piso

a) Componente 2 :

Este incluye el hardware y software necesario para implementar el esquema de autenticación elegido EAP/TLS. Como lo comentamos en el capítulo II, es necesario para este objetivo la implementación de una PKI. Para ello se considera :

- 01 Licencia de Windows 2003 Server Enterprise, para la creación de la Autoridad Certificadora.
- 01 Servidor para la instalación del Windows 2003 Server Enterprise.
- 100 Licencias de Software Cliente 802.1x Odisey para Windows XP.
- 01 Licencia de Cisco Secure ACS 4.2 para Windows (Servidor Radius)
- 01 Licencia de Windows 2003 Server para la instalación del Cisco Secure ACS 4.2 para Windows.
- 01 Servidor para la instalación del Windows 2003 Server y el Cisco Secure ACS 4.2 para Windows.

b) Adicionales :

- 01 Switch Cisco Catalyst 2960 24TT-L para interconectar los equipos.
- 01 Rack de 45 UR en el Centro de Cómputo para la correcta instalación de los equipos nuevos.
- Materiales para el cableado estructurado.

- 10 Bandejas para los Racks de los cuartos de comunicaciones en cada piso.

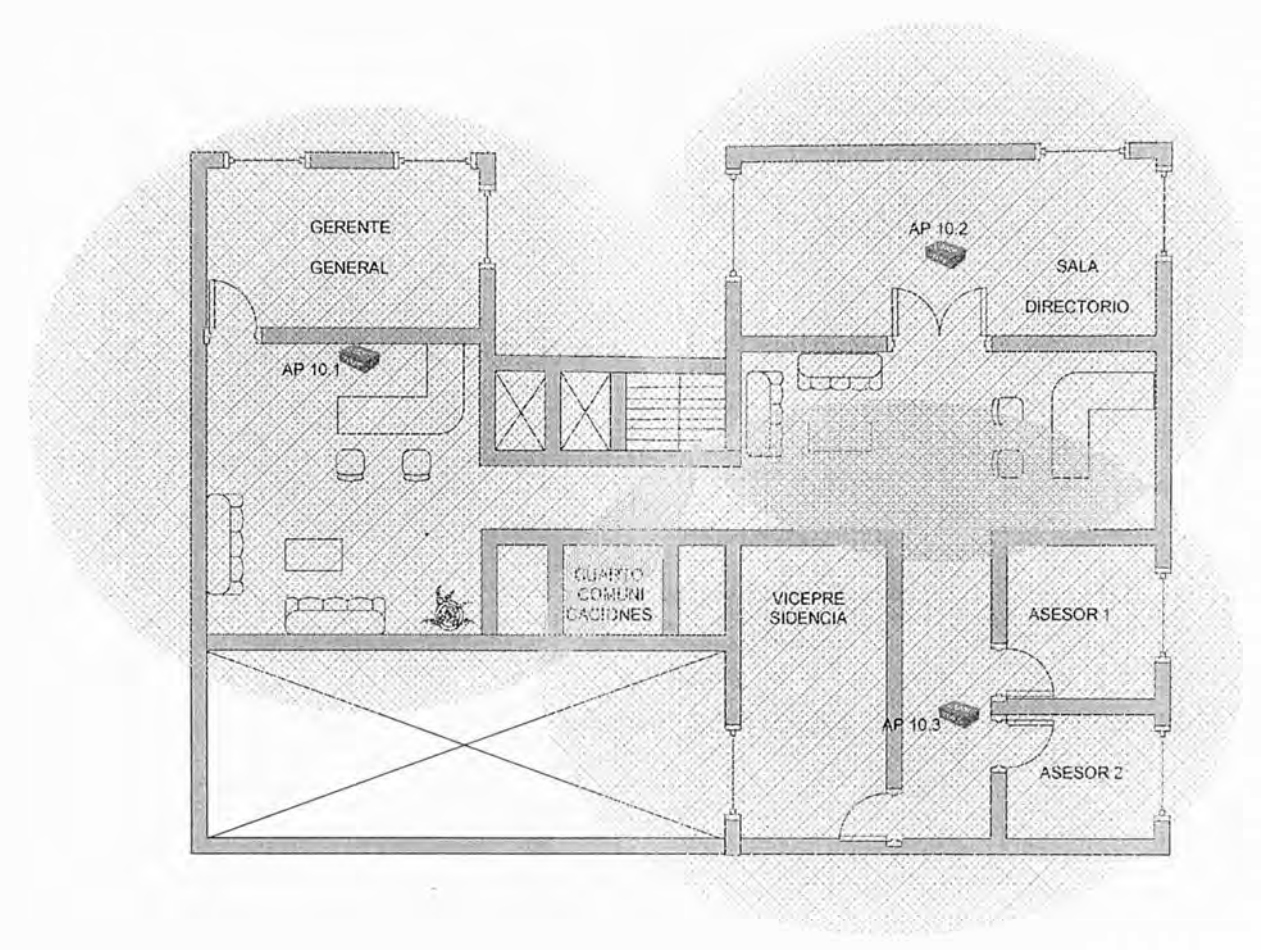


Fig. 3.17 **Cobertura Wireless Planta Décimo Piso**

3.4 Equipo de Proyecto

El Proyecto considera el siguiente personal y organigrama de trabajo

a) Jefe de Proyecto (cantidad 01 persona)

Responsable de la correcta ejecución del proyecto, administrará el presupuesto y controlará el cumplimiento de los plazos establecidos. Es el responsable del producto final hasta el pase a producción del servicio.

b) **Ing. de Comunicaciones (cantidad 01 persona)**

Responsable del planeamiento o provisión de recursos de comunicaciones necesarios para la implementación (cables, puertos de equipos, energía eléctrica, espacio físico, entro otros). Responsable además de la correcta configuración e integración de los equipos del proyecto (access points, Wireless LAN Controller y el Cisco Secure ACS 4.2) con los equipos de comunicaciones existentes.

c) **Administrador de Sistemas (cantidad 01 persona)**

El administrador de sistemas será responsable de la puesta en operación de cada uno de los servidores con sus respectivos sistemas operativos. Será responsable de la implementación de la PKI y la configuración de los Clientes móviles. En conjunto con el Ing. de Comunicaciones implementarán el software RADIUS en el Servidor Cisco Secure ACS 4.2.

d) **Personal Técnico de Apoyo (cantidad 04 personas)**

Personal encargado de realizar los trabajos de cableado estructurado para los access points, así como de realizar la instalación física de los mismos y en general, se ocuparán de la instalación física de todo el equipamiento considerado.

3.5 Esquema Funcional Propuesto

Es importante entender que los componentes que hemos enumerado para la solución de red wireless corporativa para San Andrés, cumplen cada uno con una función específica. En la Tabla 3.3 se explicar el rol de cada uno, dentro de la plataforma propuesta.

3.5.1 Sobre la Infraestructura de la Solución Propuesta

El diseño de la Red Inalámbrica Unificada para SAN ANDRES, se encuentra estructurada a diferentes niveles, lo que permite que la arquitectura sea escalable, con un alto rendimiento y redundancia que se traduce en disponibilidad del servicio.

Partiendo del Core de la red, actualmente, un equipo Cisco Catalyst 4510R, éste se encarga de dirigir el tráfico de datos lo más rápidamente posible hacia cada uno de los servicios de red. A este equipo se tiene conectados los switches para los servidores y Servicios del DataCenter. Aquí estarán conectados los componente de la Red Inalámbrica Unificada mediante los dispositivos WLC y WCS; además, este nivel contempla la seguridad de la red inalámbrica, mediante los servidores: 1)Active Directory 2) RADIUS Cisco ACS y 3) Servidor de Certificados, en una arquitectura 802.1X /EAP-TLS.

El WLC como se observa en la Fig. 3.18 es en realidad un arreglo de dos WLC configurados de manera redundantes. Esto es importante para mantener la alta disponibilidad. Este arreglo administra los recursos de radio frecuencia de todos los

Puntos de Acceso conectados y permite la conexión de cada una de las VLANs inalámbricas a los servicios y aplicaciones definidas.

Tabla 3.2 Cantidad de Access Points según Demanda

Piso	Cantidad de Access Point por Piso
1	3
2	3
3	3
4	3
5	3
6	3
7	3
8	2
9	2
10	3
TOTAL	28

El WCS permite el monitoreo y gestión de la red inalámbrica mediante reportes detallados de uso de espectro, niveles de potencia, usuarios inalámbricos conectados, rendimiento de cada Punto de Acceso, etc., que simplifican la administración y permiten una mejor respuesta del administrador de la red, ante problemas e inconvenientes. Este componente no tiene redundancia. Por su grado de criticidad no es necesario.

La capa de acceso utiliza equipos de conmutación a nivel de capa 2 del modelo OSI; el cliente dispone, en su mayoría, de switches Cisco Catalyst serie 2960. Aquí se conectorizarán los Puntos de Acceso inalámbricos con soporte de LWAPP.

Los Puntos de Acceso forman celdas, las cuales proporcionan áreas de cobertura definidas y permiten acceder a servicios y aplicaciones soportados por la red inalámbrica Wi-Fi. En la parte inferior de la Fig. 3.18, se muestran los dispositivos Wi-Fi, medio por el cual cada usuario accede a las aplicaciones y servicios proporcionados por la red inalámbrica.

Es importante señalar que estos dispositivos, para poder trabajar con la solución de red wireless propuesta, deben soportar 802.1x EAP/TLS.

3.5.2 Esquema Funcional de Autenticación

El esquema propuesto es el 802.1X EAP/ TLS y aprovecha el servicio de Active Directory existente en la organización.

La Fig. 3.19 muestra en detalle, el proceso de autenticación y autorización de un usuario inalámbrico para acceder a la red Wireless. El procedimiento será el siguiente :

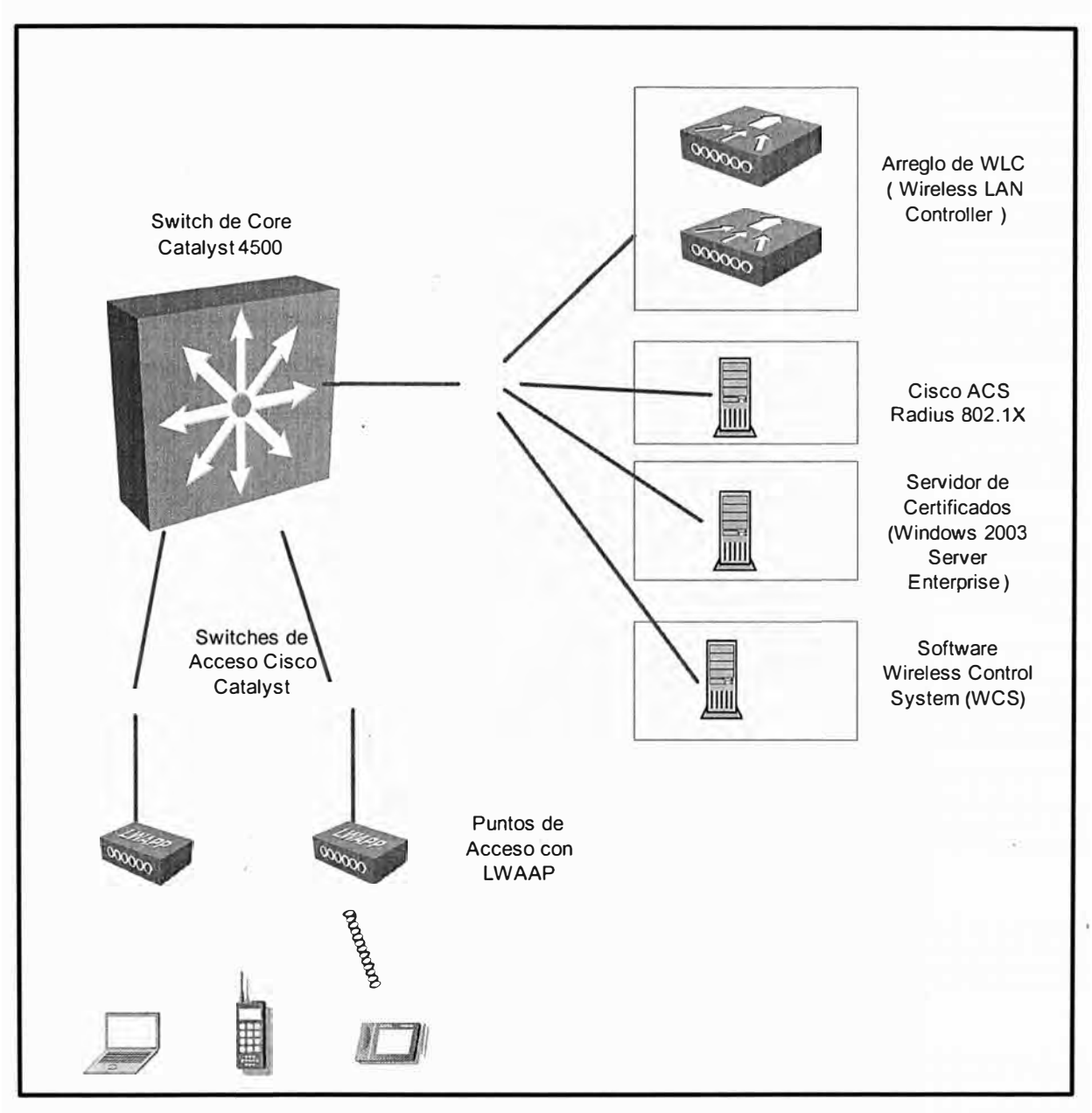


Fig. 3.18 Componentes de la Solución

1,2 El dispositivo inalámbrico detecta el SSID "Corporativo" en un determinado Access Point. El software Odyssey del cliente inalámbrico (suplicante) solicita al Wireless LAN Controller permiso para establecer una conexión.

3,4 El Wireless LAN Controller, responde solicitando al usuario se identifique.

5,6 El usuario envía su usuario y password para identificarse.

7, El Access Point está configurado para enviar la solicitud de conexión al Controlador de Puntos de Acceso (Wireless LAN Controller, WLC), permitiendo de esta forma un control total en el establecimiento de la conexión. El WLC va a determinar a qué VLAN el usuario quiere conectarse (corporativo o visitante) y le va a aplicar la política de seguridad que

corresponda. En el WLC tiene configurado que el esquema de autenticación es 802.1x EAP/TLS e inicia el proceso con el usuario y el Radius 802.1X como se ha visto en el capítulo II.

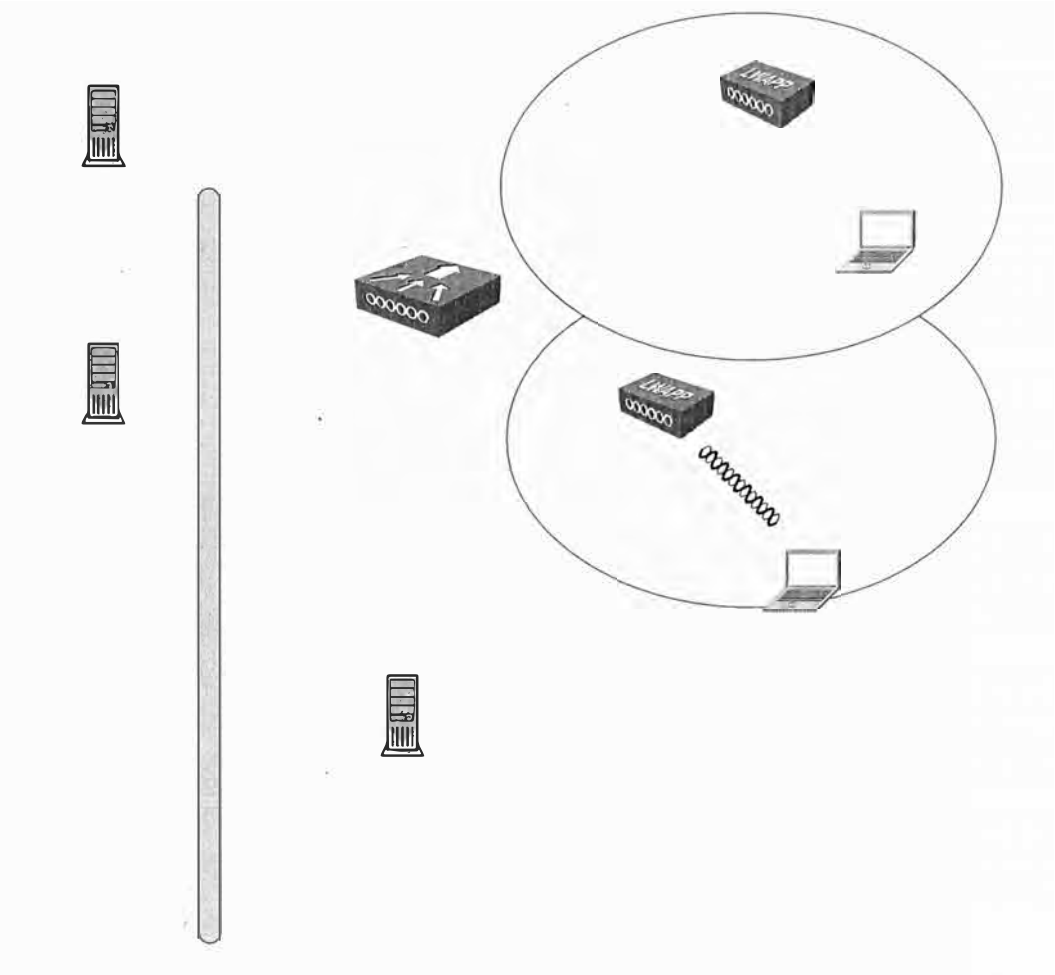


Fig. 3.19 Funcionamiento del esquema de Seguridad considerado

8, El servidor RADIUS consulta al Active Directory, para comprobar la contraseña de dominio del usuario y su validez. Además se consulta las políticas de acceso establecidas al usuario (horarios de conexión, requisitos de cifrado y autenticación, pertenencia del usuario a algún grupos, etc.)

9, Recibida la confirmación del Active Directory, de permitir el acceso, tanto el Servidor Radius como el cliente proceden a intercambiar sus credenciales para validarse uno ante el otro (certificados digitales), tal como se explicó en la sección 2.2.11 del capítulo II. Al finalizar el proceso satisfactoriamente, el Servidor Radius envía un mensaje al equipo Wireless LAN Controller de aperturar una sesión segura con el usuario.

10, El Wireless LAN Controller inicia un intercambio de claves para establecer un cifrado de sesión con el cliente y permitirle finalmente el acceso al usuario.

3.6 Desarrollo de la Implementación

Dejando de lado las actividades de adquisición de los bienes y servicios necesarios, el desarrollo del proyecto contempla las siguientes actividades

3.6.1 Implementación del Componente 1:

Para el componente 1 se tiene que desarrollar las siguientes actividades :

a) Implementar el Cableado Estructurado

Tabla 3.3 Rol de cada componente

Elemento	Funciones de Acceso y Seguridad
Usuario Móvil Corporativo / Equipo Móvil	Este usuario móvil, es aquél que tiene acceso vía la Red Wireless, a los sistema críticos de la Corporación, por lo tanto, su mecanismo de autenticación EAP/TLS exige que como tal, deber estar registrado dentro del dominio Windows, como perteneciente al grupo de usuarios con derecho a conectarse. Igual condición tiene el equipo sobre el que intenta realizar tal conexión. Según la arquitectura EAP/TLS, este usuario dispone de un certificado digital emitido por la Autoridad Certificadora (AC) SAN ANDRES, para el proceso de autenticación.
Usuario Móvil Visitante	Este usuario es aquél que accede a la red wireless únicamente para el servicio de internet. Su esquema de autenticación es más sencillo, lo hace a través de un sistema de portal cautivo que dispone el Wireless LAN Controller directamente.
Punto de Acceso **Cisco Aironet LWAPP**	• Bajo la arquitectura inalámbrica de Cisco Unified Wireless Network, es quien maneja la parte de radio frecuencia. • También realiza la encriptación y desencriptación de tramas
Controlador de Puntos de Acceso.	• Bajo la arquitectura inalámbrica de Cisco Unified Wireless Network, es quien realiza la configuración y gestión de los puntos de acceso (AP) LWAPP.

Wireless LAN Controller(WLC)	• Dentro del Esquema 802.1X, este equipo hace las veces del Autenticador entre el usuario Móvil Corporativo y el Servidor de Autenticación.
Servidor 802.1X. **Cisco Secure ACS**	Dentro del esquema 802.1X este es el Servidor de Autenticación, por ende, según la arquitectura EAP/TLS este servidor debe disponer de un certificado digital emitido por la Autoridad Certificadora (AC) SAN ANDRES, para intercambiar credenciales al momento de la conexión de algún usuario corporativo. La información sobre los usuarios los recoge del Servidor de Validación de usuarios (Active Directory).
Servidor de validación de usuario. **Active Directory**	Esta Base de Datos del Dominio Windows SAN_ANDRES, se encarga de la gestión sobre el tipo de acceso de usuarios a los recursos de red, definido en las políticas de acceso. El Servidor 802.1X consulta esta base de datos externa para saber por ejemplo, si un usuario o está autorizado a conectarse a la red wireless o no.
Servidor Autoridad Certificadora. **Windows 2003 Server**	Este servicio del Windows 2003, permite la implementación de la PKI SAN ANDRES. La Autoridad Certificadora se encarga de la Emisión, administración, actualización y revocatoria de los certificados digitales que usarán los usuarios autorizados de la Corporación.
Software de Administración y Gestión de la WLAN. **Wireless Control System** **WCS**	• Gestión y monitorización de los Puntos de Acceso (mediante SNMP y/o syslog) • Estudio de la localización de los Puntos de Acceso para controlar el tráfico inalámbrico y monitorear conexión a la red desde zonas no deseadas y conexiones hotspot de la organización. Monitorización y auditoría de los registros de acceso del servicio RADIUS.

A partir del estudio del Site Survey realizado, se necesitan 28 puntos de cableado estructurado categoría 6 en los pisos del edificio.

Los equipos se instalarán en el falso techo, quedando visibles únicamente la ANTENAS.

Para la canalización del cableado se usarán las bandejas metálicas existentes, terminándose el punto en una caja rectangular 4x2 adosada en el mismo techo.

En cada piso existe, como se puede ver en los planos, un cuarto de comunicaciones que es donde se concentra el cableado horizontal de cada piso. Desde cada piso, existen enlaces de cobre en categoría 6 que interconectan los pisos con la sala de datos que se ubicar en el piso 7, como se observa en la Fig. 3.13.

En cada cuarto de comunicaciones actualmente existe un rack de comunicaciones de 42 Unidades de Rack de altura. Cada rack contiene internamente un equipo UPS de 1 KVA, un switch Cisco de 48 puertos 10/100 modelo 2960 24 TTL, un panel de cobre categoría 6 marca Systimax y un ordenador de cables UTP. Para la instalación tomaremos dos o tres posiciones del patch panel que están libres en cada piso. De esta forma, únicamente necesitaremos adquirir el cable UTP, caja de montaje, face plate, jacks RJ.45 y dos patch cord por cada punto que necesitemos implementar. En Resumen, para el cableado estructurado se va a necesitar lo indicado en la Tabla 3.4 :

Tabla 3.4 Materiales de Cableado Estructurado Necesarios

Piso	Access Point por piso	Jack RJ45+Caja de Montaje+Face Plate	Patch Cord de 3 pies+patch cord de 5 pies	Rollos de Cable de 305 m.
1	3	3	6	0.3
2	3	3	6	0.3
3	3	3	6	0.3
4	3	3	6	0.3
5	3	3	6	0.3
6	3	3	6	0.3
7	3	3	6	0.3
8	2	2	4	0.2
9	2	2	4	0.2
10	3	3	6	0.3
Total	28	28	56	2.8

b) Instalación y Conectorización de los Access Points

En la Fig. 3.20 se muestra la topología de red existente. Se va a utilizar tres o dos puertos de cada switch existente en cada cuarto de comunicaciones. Para la alimentación de los access point se usará un dispositivo conocido como “Power Injector”, que permite

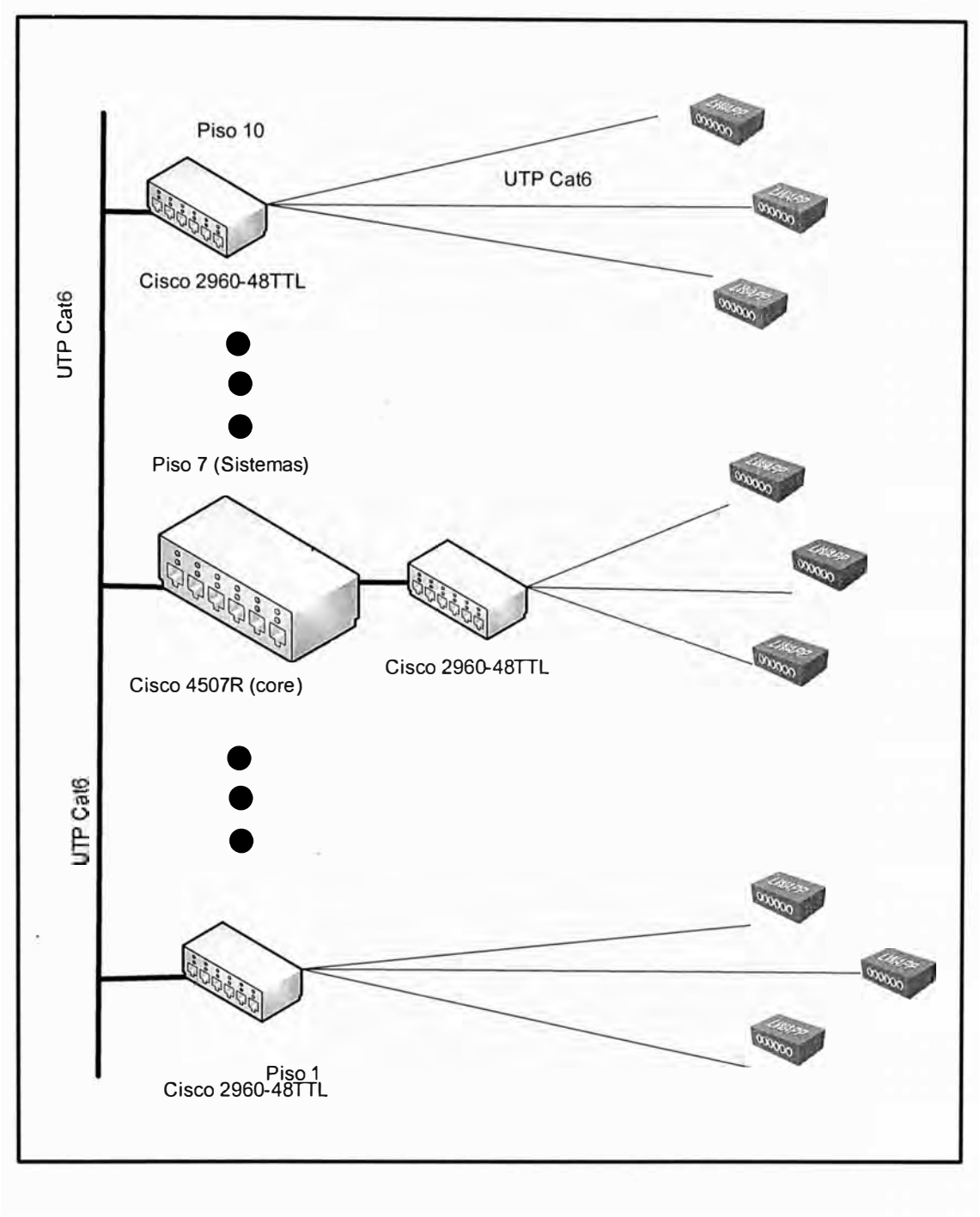


Fig. 3.20 Backbone de Red LAN Existente

alimentar de energía eléctrica a un dispositivo por el puerto de red Ethernet. En la Fig. 3.21 se muestra el detalle de conexión. Se incluirá en la compra una bandeja de 2UR en cada rack de comunicaciones para la instalación de los power injector. Los power injector se conectarán a la red eléctrica de 220 voltios, a través de las regletas eléctricas de 8 tomas que tiene cada rack de comunicaciones y de las que sólo usa una o dos actualmente. Cada Power Injector demandará un consumo de 15 a 20 watts. Si sumamos a esto el consumo de cada switch de 50 a 60 watts, el consumo totaliza unos 80 watts, a lo más.

Como el UPS tiene una capacidad de 1KVAx0.9 = 900 watts, no necesitamos mayor capacidad de alimentación que la ya existente

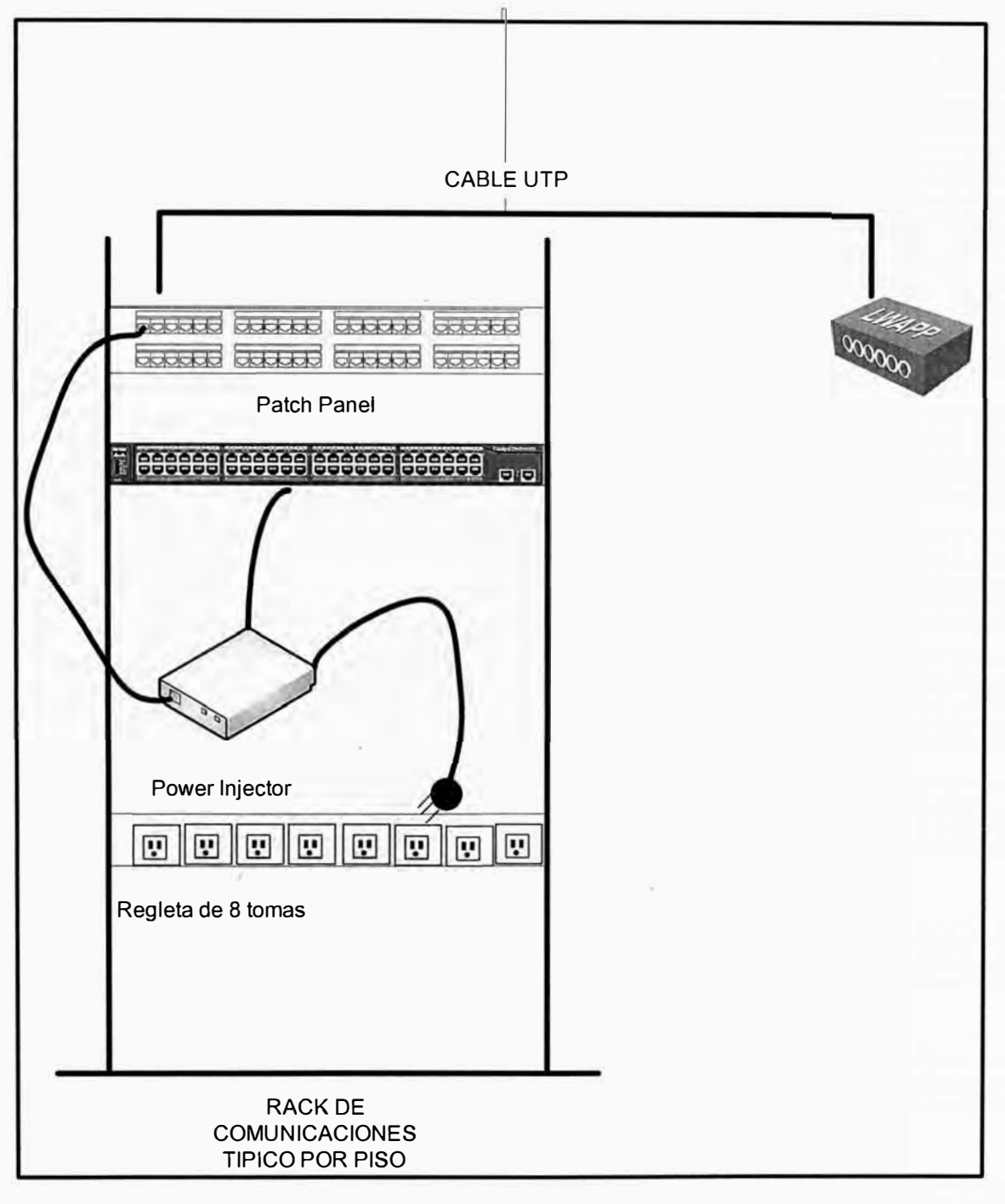


Fig. 3.21 Conectorización del los access point

c) Instalación y Configuración del Wireless LAN Contoller y el Cisco Wireless Contro System (WCS)

En la Fig. 3.22 se muestra el layout de instalación de los equipos y en la Fig. 3.23 se muestra el detalle de la lógica de red y los parámetros IP a considerar. En el esquema propuesto vemos que el equipo core 4510R está en la parte central de arquitectura. Los

wireless LAN controller identificados en la topología como A y B respectivamente. Estos controladores se conectan mediante trunks 802.1Q al switch.

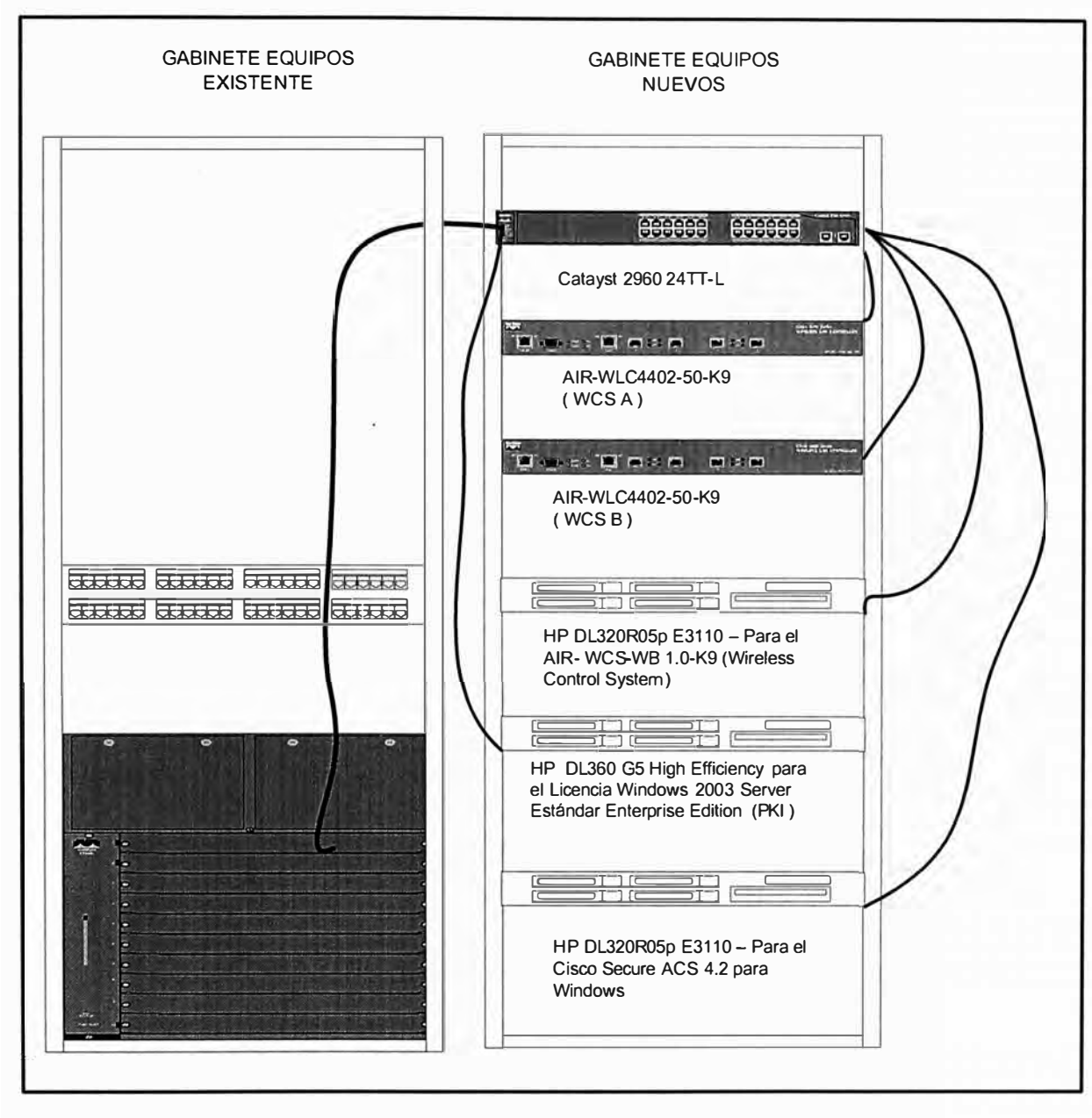


Fig. 3.22 Layout del Equipamiento Nuevo

La implementación debe considerar la definición de las VLANs y segmentos asociados en el 4510R, según se muestra en la Tabla 3.5

La VLAN 10 servirá para comunicar los puntos de acceso con los dos equipos Wireless Lan Controllers, a fin de que se levanten los túneles LWAPP entre ambos (Ver ANEXO A para este detalle). Encapsulados en esos túneles, viajará la información de los SSIDs que serán publicados.

En el esquema propuesto, vemos que el equipo core 4510R está en la parte central de arquitectura. Los wireless LAN controller, identificados en la topología como A y B, respectivamente. Estos controladores se conectan mediante trunks 802.1Q al switch.

La implementación debe considerar la definición de las VLANs y segmentos asociados en el 4510R, según se muestra en la Tabla 3.5.

La VLAN 10 servirá para comunicar los puntos de acceso con los dos equipos Wireless Lan Controllers, a fin de que se levanten los túneles LWAPP entre ambos (Ver ANEXO A para este detalle).

Encapsulados en esos túneles, viajará la información de los SSIDs que serán publicados.

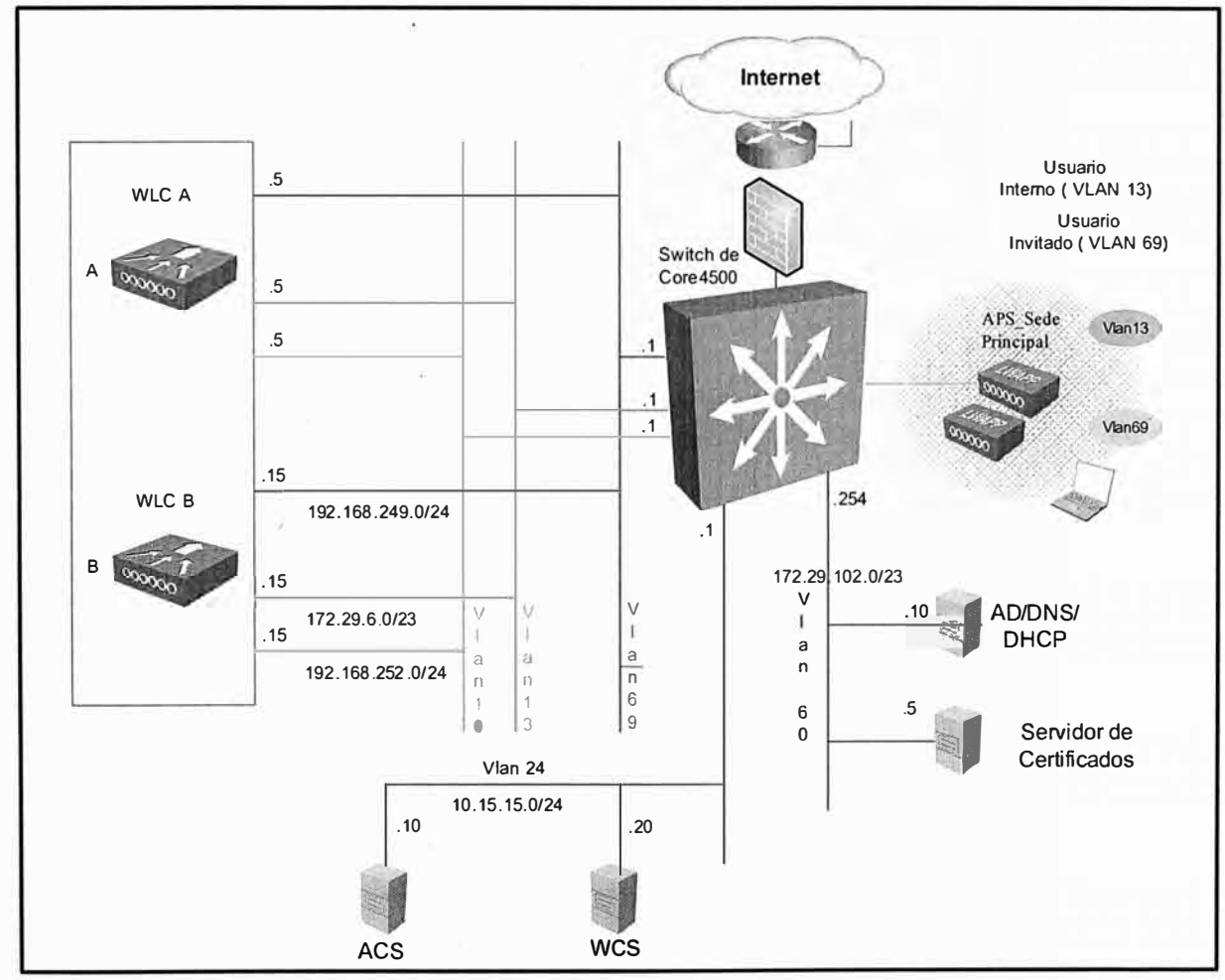


Fig. 3.23 Esquema de Red Propuesta

En la VLAN 24 se tendrán ubicados el servidor ACS, para la autenticación de usuarios corporativos y el WCS, que permite el monitoreo y gestión, tanto de los equipos Wireless LAN Controller (WLC) como de los puntos de acceso.

En la VLAN 60 se encuentra el servidor de dominio de Windows (Directorio activo), que también brindará el servicio DNS en este escenario, así como el Servidor de Certificados Digitales (AC).

Las demás VLANs serán asociadas a redes inalámbricas o identificadores de servicio (SSID), que serán publicados.

En el caso del SSID VLAN13 (Corporativos) mapeado a la VLANs 13, la política de seguridad utilizada, como se ha presentado es 802.1x/EAP TLS, los usuarios deberán estar definidos en el Directorio Activo de Windows.

En el caso de la VLAN 69, para el acceso de visitantes, la autenticación es abierta, teniéndose una política de seguridad en capa 3, para que el acceso sea autenticado mediante un portal cautivo. Los visitantes únicamente podrán accesar a Internet.

Tabla 3.5 VLANs y Redes a Implementarse en el Proyecto SAN ANDRES

Vlan	Segmento	Gateway	Aplicación
10	192.168.252.0/24	192.168.252.1	Gestión de access point
13	172.29.6.0/23	172.29.6.1	Usuarios Corporativos
24	10.15.15.0/24	10.15.15.1	Servidores ACS y WCS
60	172.29.102.0/23	172.29.102.1	Segmento red AD/DNS
69	192,168.249.0/24	192.168.249.1	Usuarios Visitantes

La interface de configuraciónde los Wireless Lan Controller Cisco (WCS) es web, totalmente gráfica como se puede apreciar en la Fig. 3.24.

Para la configuraciónde los Controladores debe tenerse en cuenta lo siguiente :

a) Definir los parámetros de administración, user y pasword, así como las direcciones IP para a interfase de administración.

   En el proyecto son las siguientes :

   Wireless Lan Controller (WLC) A : 192.168.252.5

   Wireless Lan Controller (WLC) B : 192.168.252.15.

b) Definir los parámetros IP en cada equipo Wireless Lan Controller, para las VLANs que se crearán. En este caso, serán dos, ya que tenemos dos tipos de usuarios definidos. Lo correcto es asignar una VLAN a cada tipo de usuario. Los parámetros IP se visualizan en la topología de la Fig.3.23 y son los siguientes:

Controller A :

VLAN Identificador	IP Adrress	Interface Name
13	172.29.6.5	Corporativo
69	192.168.249.5	Visitante

Controller B :

VLAN Identificador	IP Adrress	Interface Name
13	172.29.6.15	Corporativo
69	192.168.249.15	Visitante

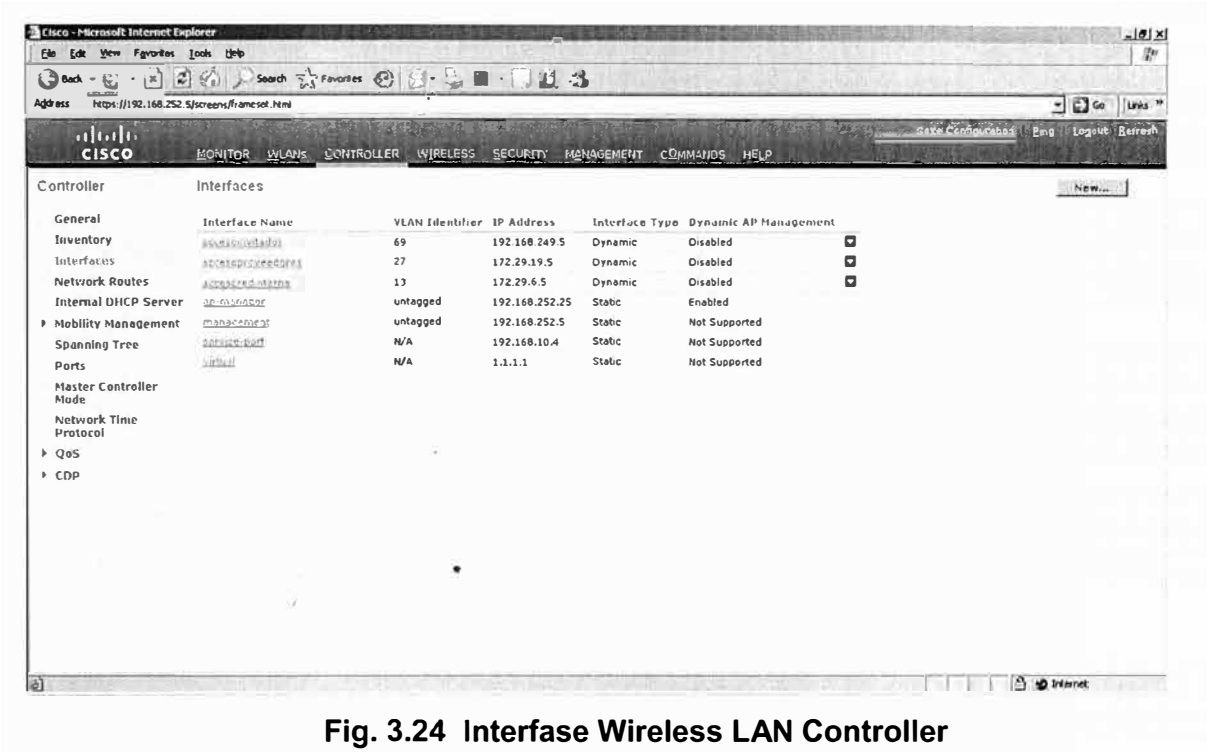


Fig. 3.24 Interfase Wireless LAN Controller

c) Para cada interface se debe precisar el DHCP Server. En nuestro caso su IP es 192.168.249.1.

d) Definir las WLANs o SSID . El equipo puede soportar hasta 16 SSID. Para nuestro caso son dos

Profile Name	WLAN ID	WLAN SSID
Corporativo	1	Vlan13
Visitante	2	Vlan69

e) La configuración del tipo de autenticación es bastante sencillo. Basta con seleccionar el SSID para el que requerimos implementar 802.1X. En nuestro caso tenemos que

seleccionar el SSID Vlan13 y escogemos dentro de las opciones de seguridad, la opción de 802.1x y encriptación DES, como se muestra en la Fig. 3.25

Finalmente, queda por Configurar el RADIUS o servidor de autenticación. La pantalla es como la que se muestra a continuación en la Fig. 3.25

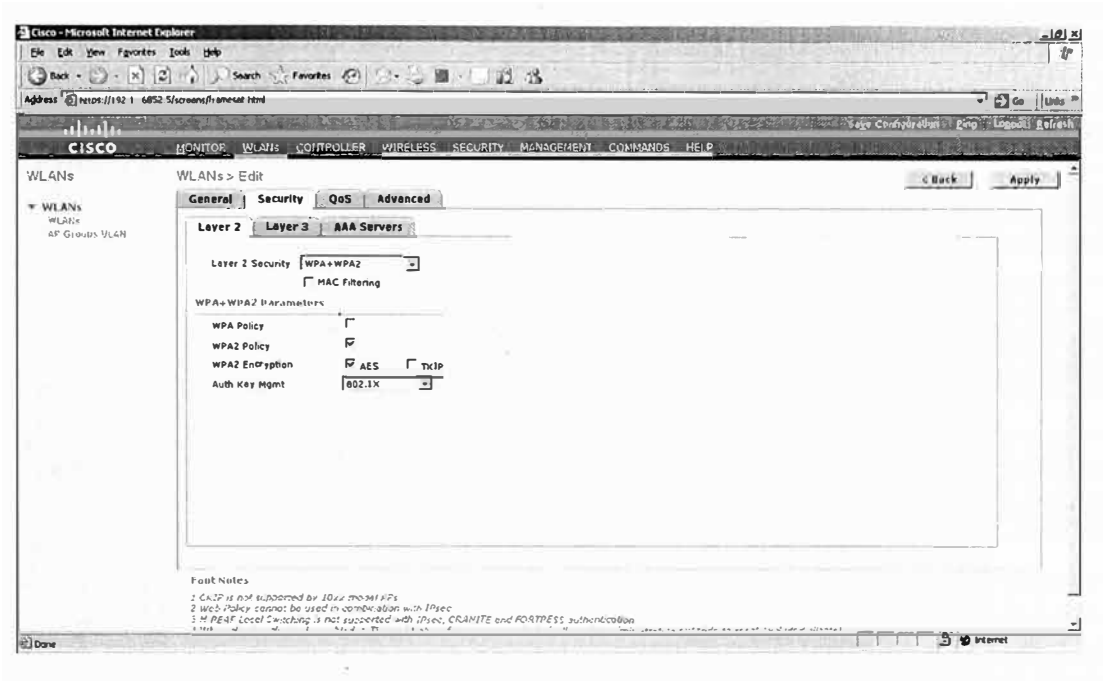


Fig. 3.25 Interfase Wireless LAN Controller - Seguridad

Como se puede observar, el Wireless LAN Controller de Cisco soporta hasta 3 Servidores Radius redundantes. En nuestro caso, colocamos la dirección IP del Equipo Cisco Secure ACS que es 10.15.15.10/24., como se muestra en la Fig. 3.26.

Queda por comentar referente a la configuración del Wireless Control System o software de Monitoreo. En realidad, es bastante sencilla, además de colocar los parámetros IP 10.15.15.20 /24, basta con registrar las direcciones IP de los dos Wireless Lan Controller para que inmediatamente comience a descubrir los Access points registrados en cada Wireless Lan Controller.

A partir de este momento, se pueden ya generar reportes de utilización de access point, reporte de patrones de ataques detectados (IPS básico). Una muestra de estos se pueden visualizar en la Fig. 3.27 y la Fig. 3.28.

La herramienta permite subir planos formato jpg, tiff, entre otros, y de esta forma, se puede aprovechar una interesante interface, que además de ubicar cada punto de acceso con su nombre sobre el plano, nos ayuda a darnos una idea de su radio de cobertura.

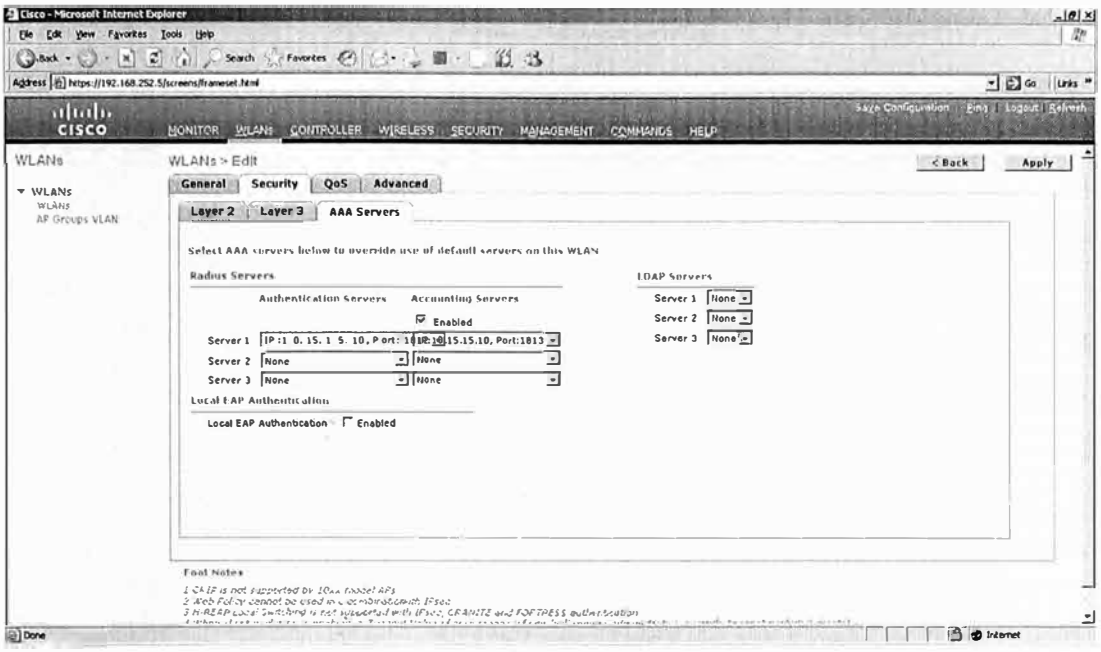


Fig. 3.26 Interfase Wireless LAN Controller – RADIUS Server

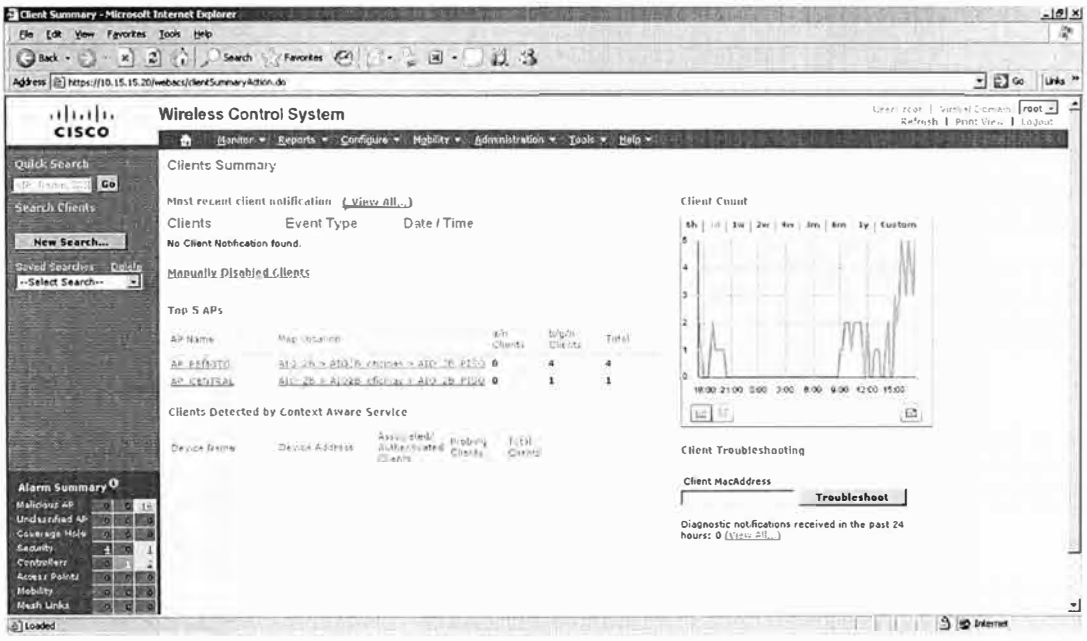


Fig. 3.27 Interfase Wireless Control System

3.6.2 Implementación del Componente 2:

En realidad la implementación de la infraestructura de autenticación es mucho más compleja. Las tareas que tienen que realizarse son las siguientes :

a) Instalación del Windows 20003 Server Enterprise, creación o inclusión en el dominio y Activación del Internet Information Server (IIS). Para nuestro caso el dominio es sanandres.local.

b) La creación de la PKI. Para ello vamos a instalar en el Servidor el servicio de Certificate Server. Para ello se debe ir a la consola de Componentes de Windows y activar el servicio, escogiendo de las dos opciones de CA (Autoridad Certificadora), la opción Enterprise Root CA, como muestra la Fig. 3.29.

c) Seguidamente, debe de crearse un grupo en el Directorio Activo del Dominio que agrupe a los usuarios del servicio wireless. A este grupo se deben agregar, tanto las máquinas como los usuarios que tendrán acceso. Para nuestro caso, este grupo lo vamos a llamar " wirelessgroup".

d) En el Servidor de Certificados debe de crearse una plantilla de certificado digital para el servidor ACS. El Servidor almacena una gran cantidad de plantillas tipo, dependiendo quien sea el que lo requiera. Este método de platillas es un procedimiento particular de Windows 2003 Server.

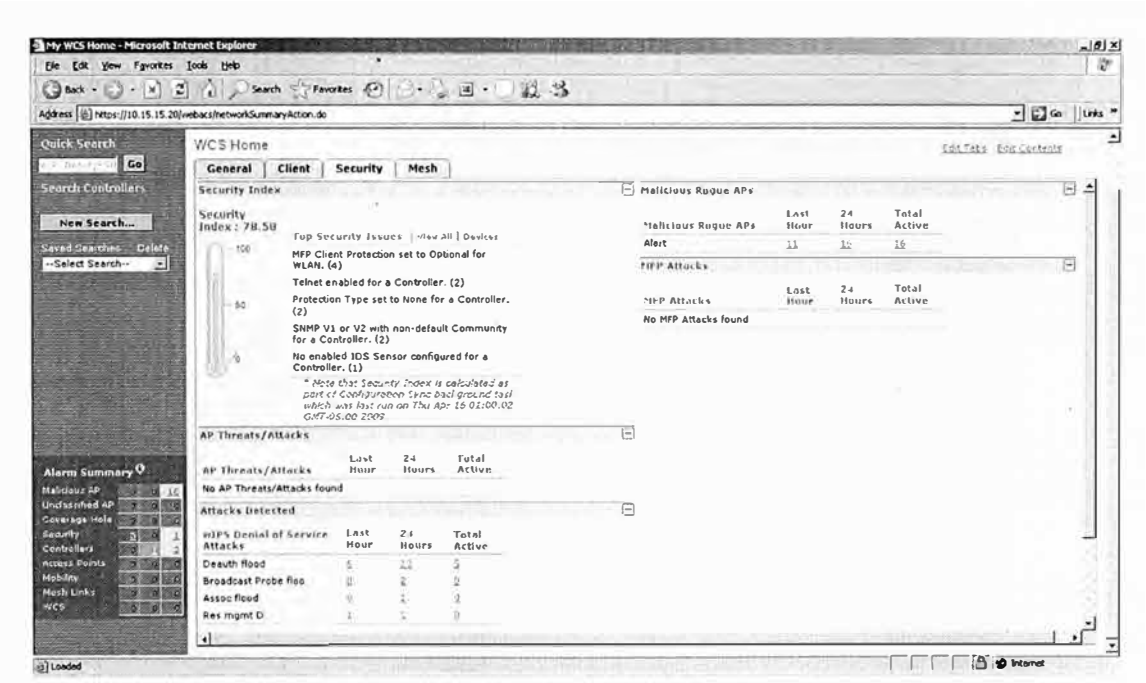


Fig. 3.28 Interface Wireless Control System

e) Paso seguido debemos de instalar y configurar el Cisco Secure AC 4.0 sobre el segundo equipo servidor requerido. Un detalle importante a tener en cuenta en la configuración es pemitir enlazar el Cisco Secure ACS 4.0 con servicios de directorio externos, como la del Active Directory. Una vez instalado el software Cisco Secure AC 4.0 (ACS) debe de obtenerse un certificado del servidor de Certificados (CA) para poder autenticar un cliente WAP-TLS. Para ello, es necesario que desde el mismo

servidor ACS se acceda al servidor de certificados. La interfaces es similar a la mostrada en la Fig. 3.30

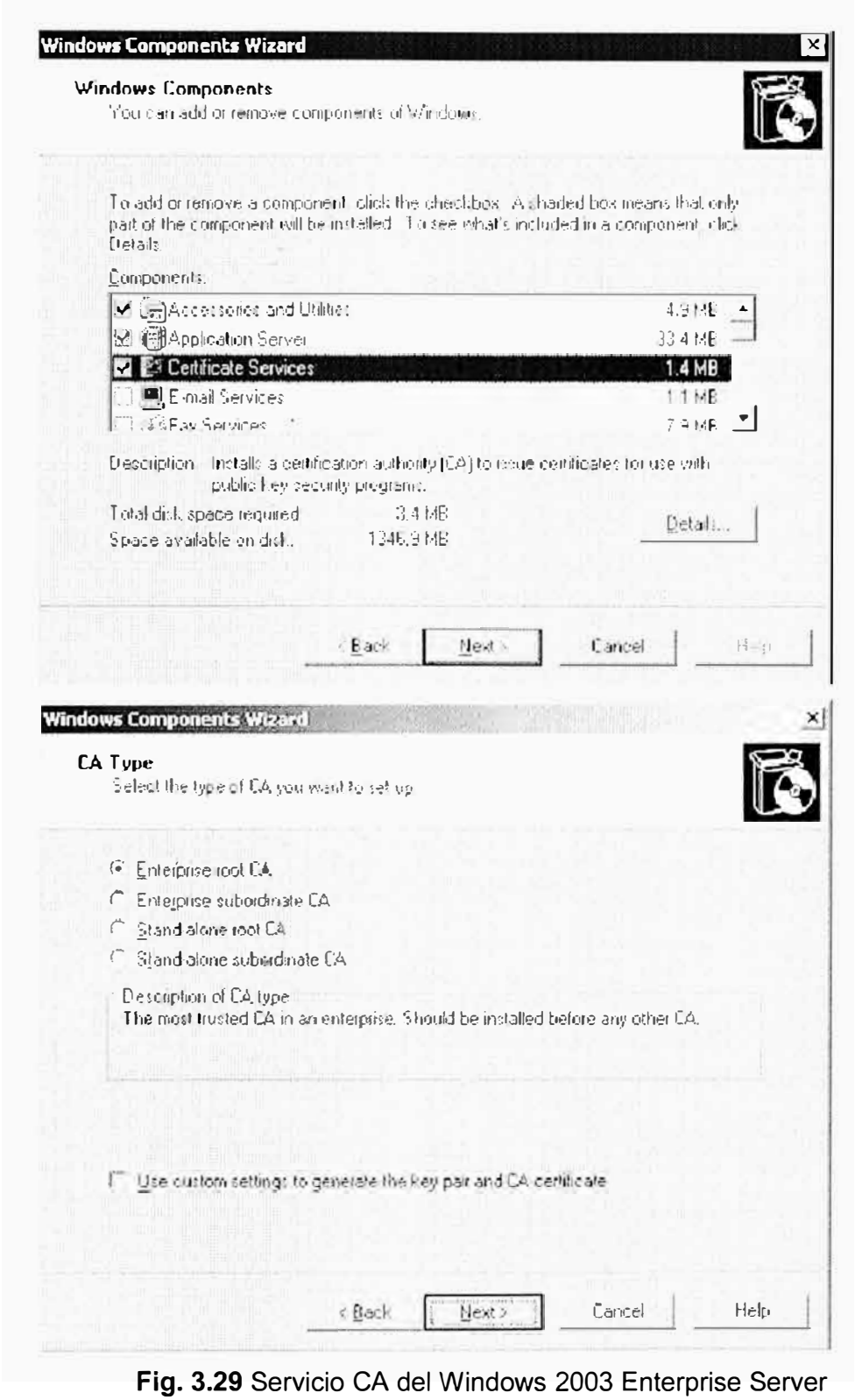


Fig. 3.29 Servicio CA del Windows 2003 Enterprise Server

f) Una vez descargado e instalado el certificado, el Servidor ACS estará listo para comenzar a autenticar. Pero antes debe de hacerse lo mismo en cada cliente de la

red wireless. Cada cliente, antes de accesar de manera inalámbrica debe conectarse al Servidor de Certificados y descargar su certificado usando la red cableada.

Fig. 3.30 Web Service para Descarga de Certificados.

3.6.3 Verificación de la Conexión :

Para verificar la conexión, finalmente se debe probar con un cliente que esté debidamente registrado en el grupo de usuarios autorizados y que haya descargado su certificado.

Vamos a mostrar como verificar un usuario al que ya le hemos instalado el software cliente suplicante.

La solución considera el uso del Cliente Odyssey en los usuarios móviles. La configuración del Cliente (Fig. 3.31) requiere básicamente lo siguiente :

a) Crear un nuevo perfil.
b) Indicar el certificado digital que usar (el generado por el Servidor de Certificados)
c) Indicar que el mecanismo de autenticación será EAP/TLS
d) Indicar el SSID de la red Wireless (Vlan13 – usuarios corporativos)
e) Indicar el tipo de encriptación : (AES)

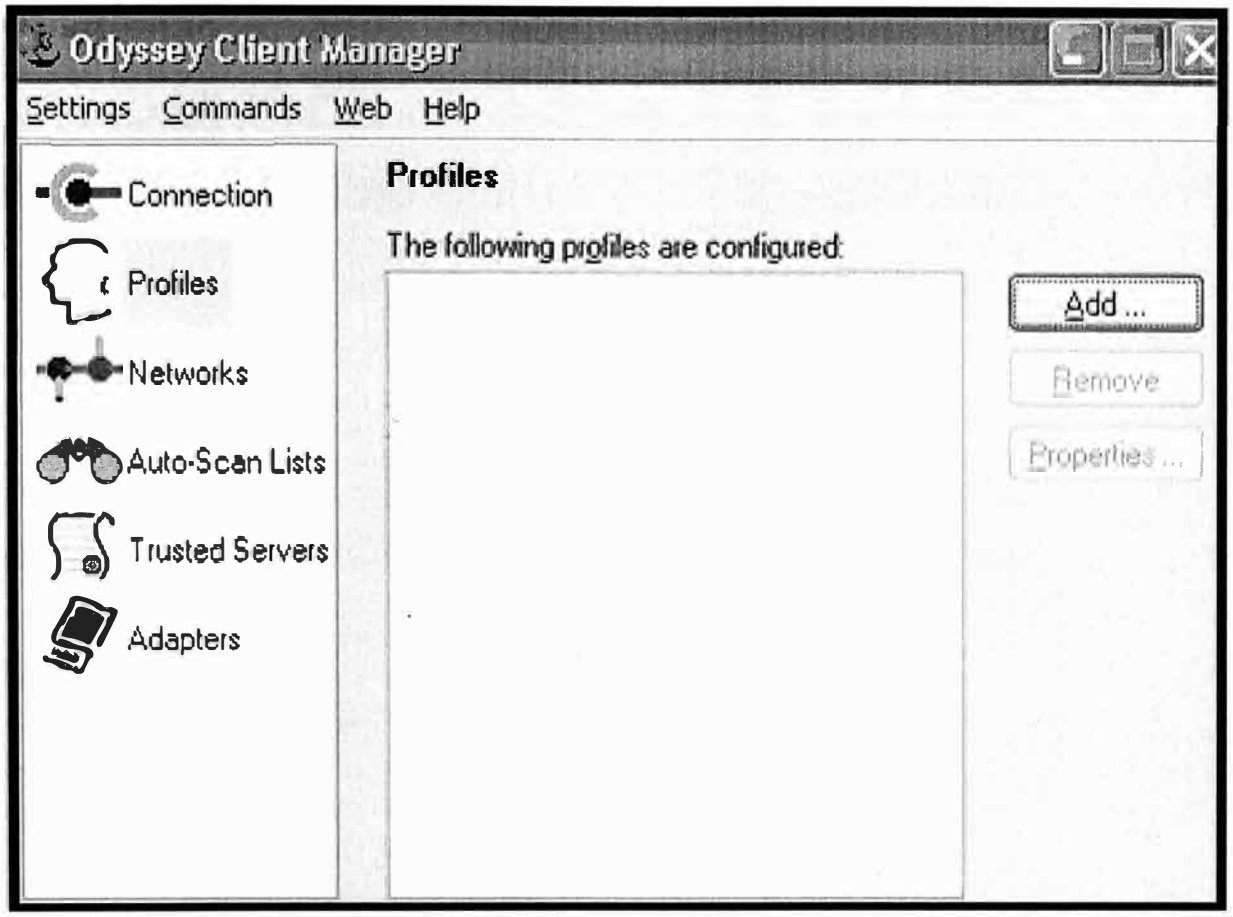
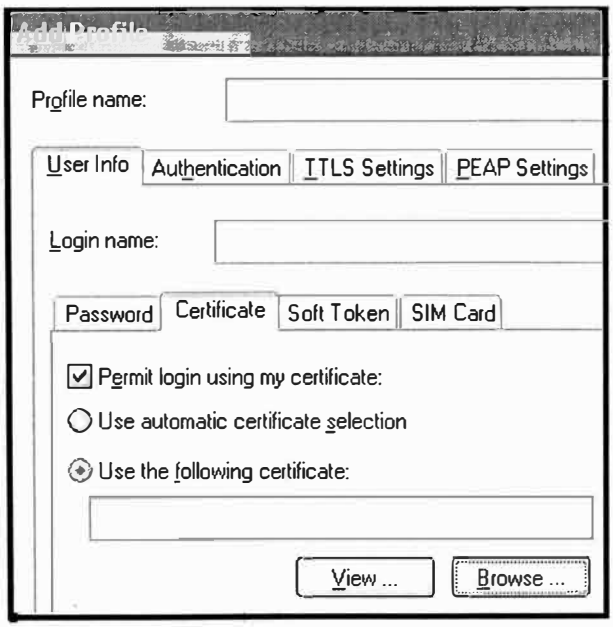


Fig. 3.31 Cliente Odyssey



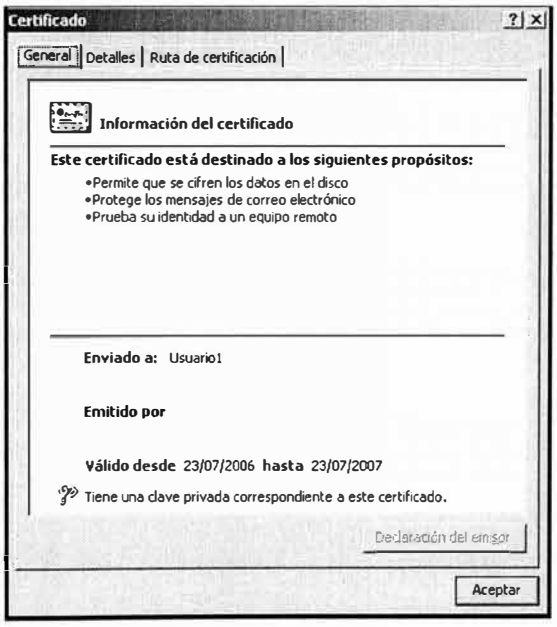


Fig. 3.32 Configuración del Perfil de Autenticación Odyssey

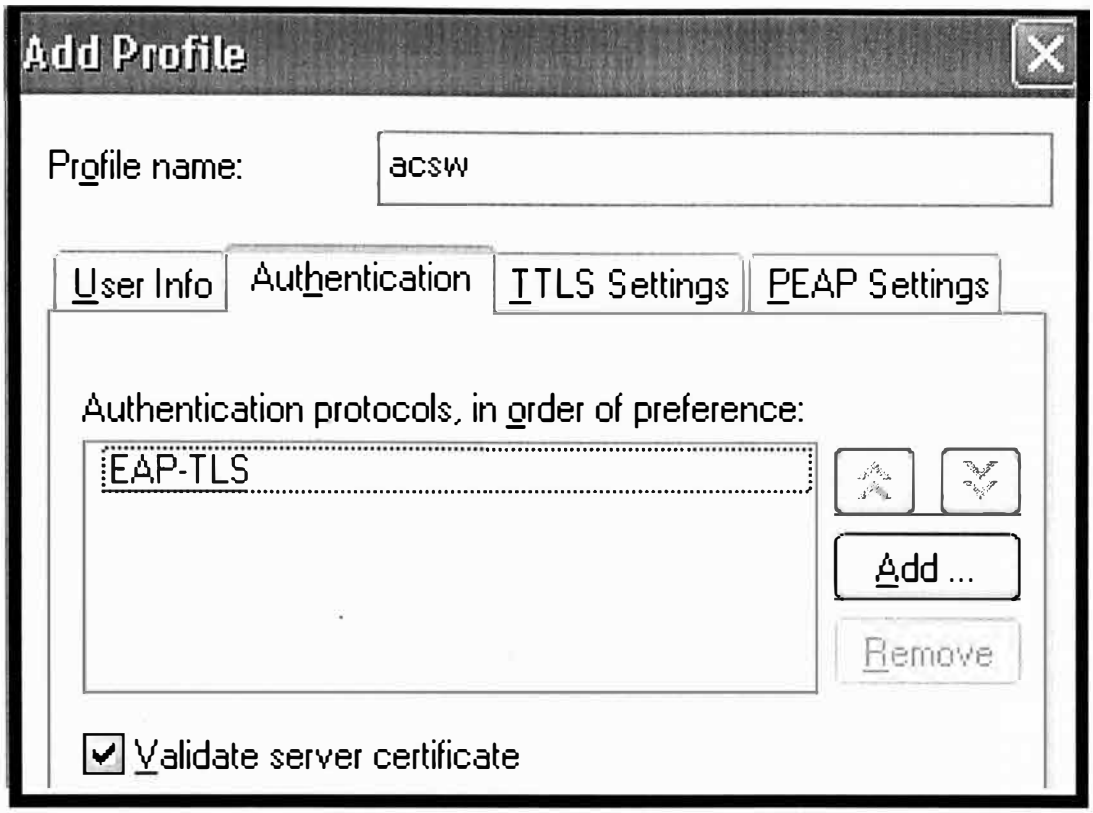


Fig. 3.33 Configuración del Perfil EAP-TLS

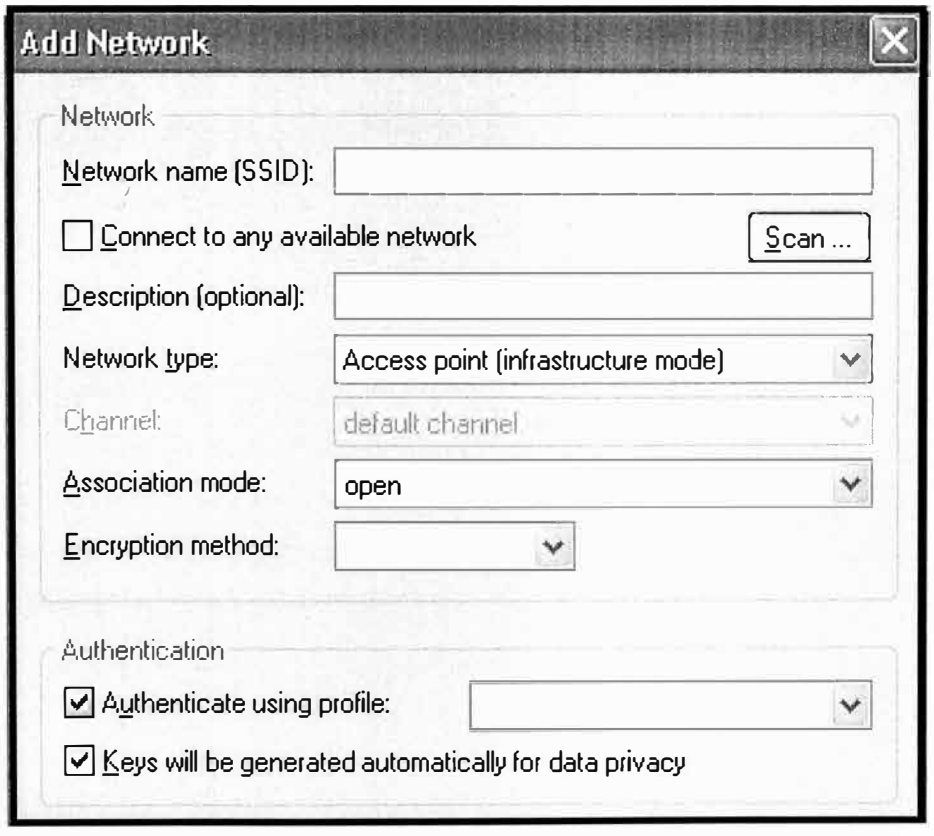


Fig. 3.34 Configuración de los Parámetros de red

Cuando un usuario WLAN enciende su equipo, el proceso de autenticación inicia después de que éste ingresa su nombre de cuenta y contraseña; entonces el software cliente intenta acceder a la clave privada y la aplicación de protección de claves solicita la contraseña que protege la clave, tal cual se ve en la Fig. 3.35

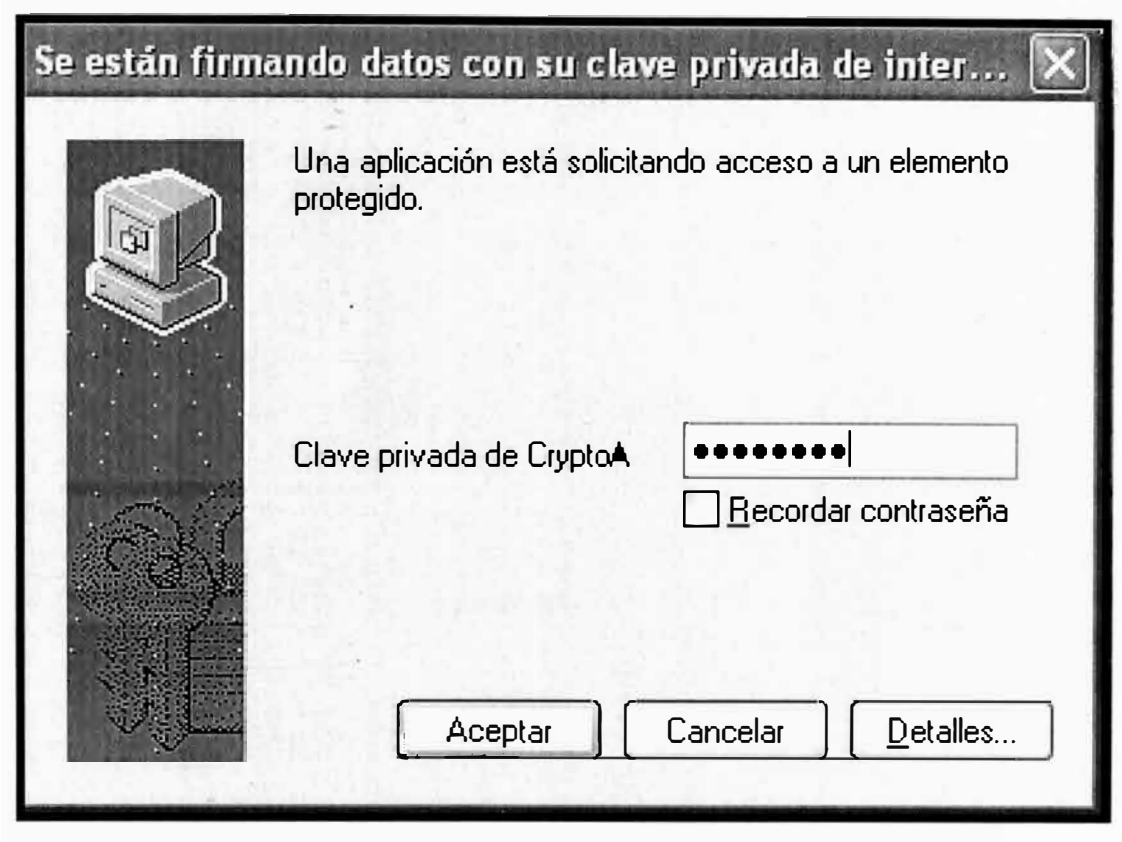


Fig. 3.35 Configuración de los Parámetros de red

Después de ingresar la contraseña y permitir el acceso a la clave privada, se inicia el intercambio de credenciales y parámetros TLS.

Durante el proceso de negociación para la autenticación se genera una clave dinámica para cifrar la comunicación.

El servidor DHCP sólo asigna una dirección después que las credenciales del usuario han sido validadas exitosamente.

En la barra de tareas de Windows se puede verificar el estado de la comunicación.

En la Fig. 3.36(a) se muestra al cliente OAC en estado open and authenticated y en la Fig. 3.36(b) se muestra el estado final de la conexión WLAN.

En la Fig. 3.37 se puede verificar el estado de la comunicación a través de la aplicación Odyssey Client Manager.

En la parte inferior derecha de la aplicación se muestra el estado de la comunicación de acuerdo a las siguientes especificaciones.

Fig. 3.36 Conexión Cliente(a)

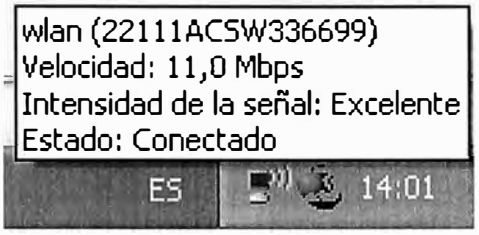


Fig. 3.36 Conexión Cliente (b)

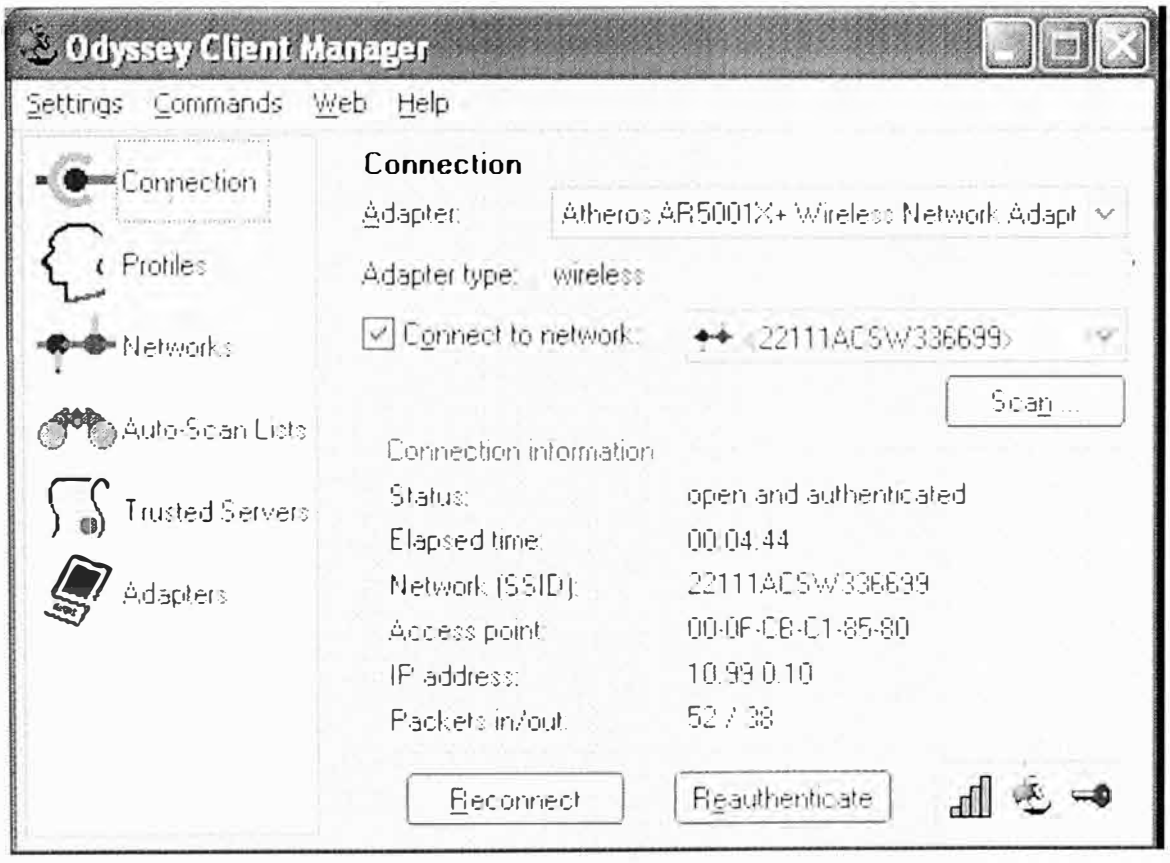


Fig. 3.37 **Conexión Cliente**

3.7 Análisis Económico

En la Tabla 3.6 siguientes se muestra un resumen con la inversión necesaria para la implementación del proyecto.

Tabla 3.6 Estructura de Costos Proyecto

ITEM	TIPO	DESCRIPCION	CANTIDAD	COSTO UNITARIO US $	COSTO TOTAL US $
COMPONENTE 1					
1.1	Hardware	Cisco AIR-WLC4402-50-K9 (Wireless LAN Controller)	2	15 350.00	30700.00
1.2	Hardware	AIR – AP1231G-A-K9 (Access Points)	28	670.00	18760.00
1.3	Hardware	AIR-ANT5959 (Antenas)	28	210.00	5880.00
1.4	Hardware	WS- C2960-24TTL (switch)	1	1200.00	1200.00
1.5	Software	AIR- WCS-WB 1.0-K9 (Wireless Control System)	1	2980.00	2980.00
1.6	Hardware	HP DL320R05p E3110 Procesador : Dual-Core Intel® Xeon® processor E3110 RAM : 4 GB. HD : 146 GB SAS, 15 rpm	1	2899.00	2899.00
1.7	Software	Licencia Windows 2003 Server Estándar	1	1299.00	1299.00
1.8	Servicios	Instalación Cisco AIR-WLC4402-50-K9	2	350.00	700.00
1.9	Servicios	Instalación AIR – AP1231G-A-K9 (Access Points)	28	30.00	840.00
1.10	Servicios	Instalación S.O. del Servidor HP DL320R05p	1	320.00	320.00
1.11	Servicios	Instalación del software AIR-WCS-WB 1.0-K9	1	550.00	550.00

ITEM	TIPO	DESCRIPCION	CANTIDAD	COSTO UNITARIO US $	COSTO TOTAL US $
1.12	Servicios	Soporte correctivo 7x24 anual	1	1580.00	1580.00
1.13	Materiales Cableado	28 Face Plate Systimax 28 jacks cat6 Systimax 28 Cajas de Montaje 56 Patch Cord 3 pies Systimax Cable UTP Cat6 Systimax. Canaleta, base de la canaleta, curvas, terminaciones. Gabinete de Comunicaciones de 45 UR. 10 Bandejas metálicas de 2 UR	1	3920.00	3920.00
1.14	Servicios	Instalación de los puntos de cableado estructurado	1	1100.00	1100.00
1.15	Servicios	Curso Cisco WCS Nivel Básico	3	1500.00	4500.00
1.16	Servicios	Curso Cisco WCS Nivel Avanzado	3	1800.00	5400.00
COMPONENTE 2					
2.1	Hardware	HP DL360 G5 High Efficiency Procesador : (1) Quad-Core Intel® Xeon® Processor L5420 (2.50GHz) RAM : 6 GB. HD : 146 GB SAS, 15 rpm	1	4399.00	4399.00

ITEM	TIPO	DESCRIPCION	CANTIDAD	COSTO UNITARIO US $	COSTO TOTAL US $
2.2	Hardware	HP DL320R05p E3110 Procesador : Dual-Core Intel® Xeon® processor E3110 RAM : 4 GB. HD : 146 GB SAS, 15 rpm	1	2899.00	2899.00
2.3	Software	Licencia Windows 2003 Server Estándar Enterprise Edition	1	3250.00	3250.00
2.4	Software	Licencia Windows 2003 Server Estándar	1	1299.00	1299.00
2.5	Software	Cisco Secure ACS 4.2 para Windows	1	6750.00	6750.00
2.6	Software	Paquete con 100 licencias Odyssey Access Client v4.51; compatibles con Windows 98/98SE/2000/Me/XP.	1	3200.00	3200.00
2.7	Servicios	Instalación S.O. del Servidor HP	2	320.00	640.00
2.8	Servicios	Instalación/Configuración del Servicio PKI Windows	1	350.00	350.00
TOTAL INVERSION PARA EL PROYECTO : US $ 105 415.00 + IGV					

3.8 Estructura de Tiempos

En la Tabla siguiente se muestra el diagrama en tiempos del proyecto; los plazos están considerados en días calendario. Se ha estimado un total de 13 semanas para el proyecto :

Tabla 3.7 Estructura de Tiempos del Proyecto

Nº	ACTIVIDADES	DURACION EN SEMANAS												
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S 10	S 11	S 12	S 15
1	**FASE ADQUISICIONES**													
1.1	Preparar y enviar RFP	X												
1.2	Recibir Propuestas		X											
1.3	Evaluar y elegir proveedor			X										
1.4	Recepción de pedido materiales cableado				X	X								
1.5	Recepción de pedido equipos				X	X	X	X	X	X				
2	**FASE EJECUCION**													
2.1	**COMPONENTE1 INFRAESTRUCTURA WIRERELESS**													
2.1.1	**CABLEDO ESTRUCTURADO**													
2.1.1.1	Canalización						X							
2.1.1.2	Tendido							X						
2.1.1.3	Conectorización								X					
2.1.1.4	Certificación								X					
2.1.2	**EQUIPAMIENTO CISCO**													
2.1.2.1	Protocolo de Operatividad Física de los Equipos									X				
2.1.2.2	Instalación y Despliegue de los Access Point									X	X			
2.1.2.3	Instalación y configuración de los Controladores										X			
2.1.2.4	Instalación y configuración del software de monitoreo										X			

Nº	ACTIVIDADES	DURACION EN SEMANAS												
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S 10	S 11	S 12	S 15
2.2	**COMPONENTE2 INFRAESTRUCTURA DE SERVICIO**													
2.2.1	Instalación del Servidor de Certificados									X	X			
2.2.2	Implementación de la PKI									X	X			
2.2.3	Instalación/Configuración del Servidor Radius Cisco ACS									X	X			
2.2.4	Registro de Equipos y Clientes en el Directorio Windows.									X	X			
2.2.5	Instalación de Certificados en el Servidor Radius y los Clientes									X	X			
2.2.6	Desarrollo de Pruebas de Verificación										X			
3	**FASE PREOPERATIVA**													
3.1	Evaluación Conjunta con el área de Operaciones											X	X	
3.2	Capacitación y Entrenamiento al personal operativo											X		
3.3	Preparación de Documentación y Manuales de operación												X	X
3.4	Pase a Producción/Fín de Proyecto													X

CONCLUSIONES

1. La solución presentada tiene un muy alto nivel de calidad de señal. Además existe un solapamiento en la cobertura por antenas configuradas a diferentes canales no destructivos (1, 6 y 11), por ende, puede soportar un despliegue de Telefonía IP a futuro sin inconvenientes.
2. La plataforma propuesta, representa un considerable nivel de inversión y complejidad, se ha propuesto de esta forma, considerando atender un elevado nivel de seguridad en la comunicación, usando el esquema 802.1X y EAP con certificados digitales. Sin embargo, cada negocio debe evaluar la criticidad de la información que pondría al alcance de los usuarios inalámbricos, a fín de encontrar el esquema de seguridad que mejor costo/beneficio le represente. En algunos casos, un esquema más sencillo y de menor costo como EAP-LEAP y EAP-FAST puede resultar suficiente.
3. En la solución se optó por la solución Cisco, no obstante existir en el mercado de productos igualmente líderes, sin embargo, se buscó en este caso, homogenizar la plataforma. En general, es recomendable manejar implementaciones con productos que cubran todo el equipamiento necesario, si se opta por una infraestructura tecnológica de datos, tanto para la red WLAN y LAN de varios fabricantes, la probabilidad que existan problemas de compatibilidad, performance, administración de la red, "cuellos de botella", etc. es bastante alta. Además, se pueden generar inconvenientes en servicios como: roaming, calidad de servicio QoS, seguridad en VLANs, balanceo de carga, ACLs (Access Control List), VoIP, etc., debido a que cada fabricante especifica sus propios estándares y normas, para proporcionar los servicios adicionales que manejan las WLAN.
4. El método mediante WEP con clave estática es el mínimo nivel de protección que debería existir. En una red casera puede ser suficiente; en una red empresarial el

uso de WEP está formalmente desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico.

5. La solución wireless propuesta de control centralizado tiene enormes ventajas en comparación con la red tradicional de equipos autónomos. Además de las facilidades de administración e instalación, resulta ventajoso cuando se desarrolla soluciones de integración como el propuesto, con un gran número de ellos presente.

ANEXO A

Cisco Unified Wireless Network

Cisco propone la utilización de la arquitectura inalámbrica Cisco Unified Wireless Network (Plataforma de Red Inalámbrica Unificada de Cisco).Esta arquitectura de red tiene tres componentes

- Los Puntos de Acceso con soporte de LWAPP (Access Point LWAPP, AP LWAPP).
- El Controlador de Puntos de Acceso (Cisco Wireless LAN Controller, WLC).
- El software administrador de la red inalámbrica (Cisco Wireless Control. System, WCS).

a) Puntos de Acceso

Para tener una arquitectura de red inalámbrica centralizada, de tal forma que permita la administración y· configuración de los todos los puntos de acceso (AP) instalados en la empresa, es indispensable en el caso de la plataforma Cisco, que los Puntos de Acceso soporten el Protocolo LWAPP, que es un protocolo propietario de la marca.

Básicamente, este protocolo crea un túnel de comunicación entre el AP LWAPP y el Controlador de Puntos de Acceso WLC como indica la Fig. 3.7.

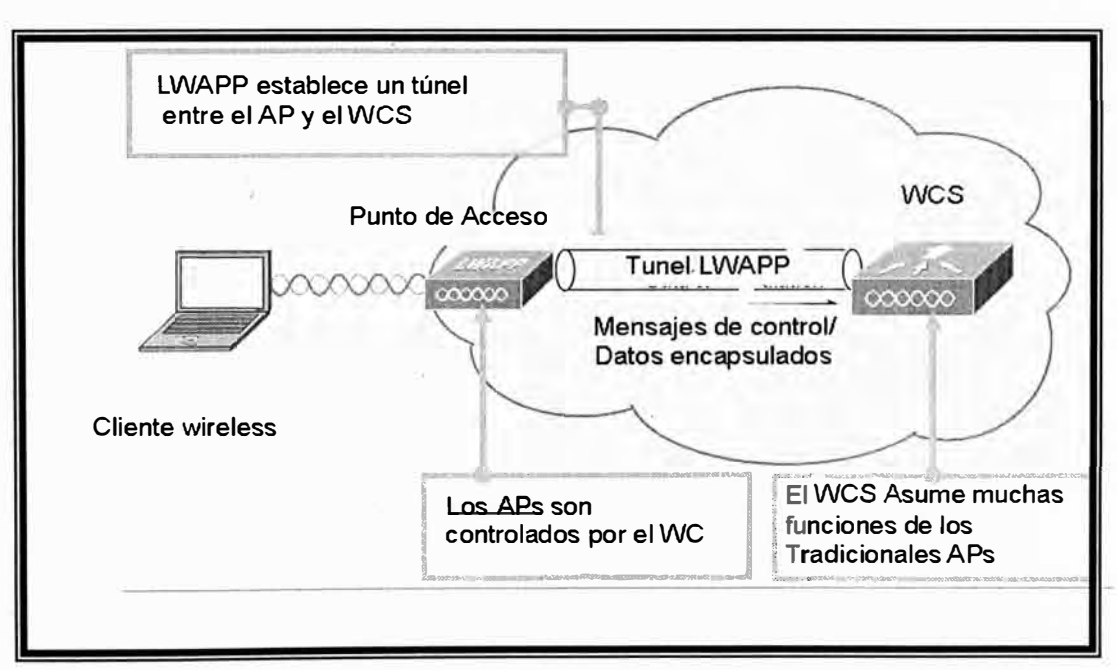


Fig. A.1 Túnel de comunicación entre los AP LWAPP y el WLC

La principal característica del protocolo LWAPP es el concepto del split MAC, donde parte del tráfico de datos del estándar 802.11 es manejada por el AP LWAPP y otra por el WLC a través de un túnel de comunicación. En la Tabla A.1 se descubre algo

muy importante : hay funciones que permanecen del lado del punto de acceso y sólo son algunas, las más importantes como autenticación, asociación y manejo de calidad de servicio, entre otras, que quedan del lado del equipo Controlador de Puntos de acceso.

Tabla A.1 División del Trabajo AP LWAPP y el WLC

DISPOSITIVO	TIPO DE TRÁFICO 802.11 MANIPULADO
AP LWAPP	Transmisión de tramas beacon. Transmisión de tramas del cliente en modo de ahorro de energía. Monitoreo de otros Puntos de Acceso. Encriptación y Desencriptación de tramas
WLC	Tramas de Autenticación. Tramas de Asociación y Desasociación. Procesos de seguridad con 802.1X/EAP Tramas de translación y enlace.

b) Equipo Controlador de Puntos de Acceso o Wireless Lan Controller (WLC)

Los Controladores de Puntos de Acceso son fundamentales en una arquitectura de red inalámbrica empresarial. Cisco promueve su serie de dispositivos Wireless LAN Controller (WLC) escalable y dimensionable para cada empresa.

La solución de Cisco WLC permite un control total en los recursos de radio frecuencia, en lo referente a: seguridad, cobertura, roaming, QoS, movilidad, etc.

Sin embargo, todos los Puntos de Acceso deben estar configurados con soporte de LWAPP (Lightweight APs, Puntos de Acceso Ligero) y no de manera independiente (Autónomos APs, Puntos de Acceso Autónomos).

El dispositivo WLC descubre a todos los AP LWAPP y toma control de las funciones anteriormente señaladas; como se mencionó, se crea un túnel de comunicaciones entre el AP LWAPP y el WLC.

Se puede tener varios WLC en dos arquitecturas principales: centralizada y distribuida. En una arquitectura centralizada se dispone de un solo WLC para todos los Puntos de Acceso instalados, incluyendo Puntos de Acceso en otros edificios.

En cambio, en una arquitectura distribuida se tienen varios WLC que balancean la carga de todos los Puntos de Acceso instalados. Esta arquitectura es recomendable cuando se tienen Puntos de Acceso en varios edificios. El dispositivo WLC permite un control de las redes virtuales (VLAN) creadas en la red inalámbrica; cabe mencionar que

los Puntos de Acceso AP LWAPP permiten definir diferentes SSID y asociarlos a una determinada VLAN.

c) Wireless Control System (WCS)

Éste es el tercer componente de la infraestructura Cisco Unified Wireless Network; el Wireless Control System (WCS) es una herramienta que permite la administración, monitoreo y gestión de redes inalámbricas empresariales. El WCS es básicamente, un software que permite visualizar el rendimiento de la red inalámbrica y permite al administrador de la red el monitoreo y gestión de todos los dispositivos inalámbricos instalados. Además, el sistema incluye un módulo de planeación, diseño y simulación de redes inalámbricas Wi-Fi, de tal forma que se tiene una buena aproximación al caso real.

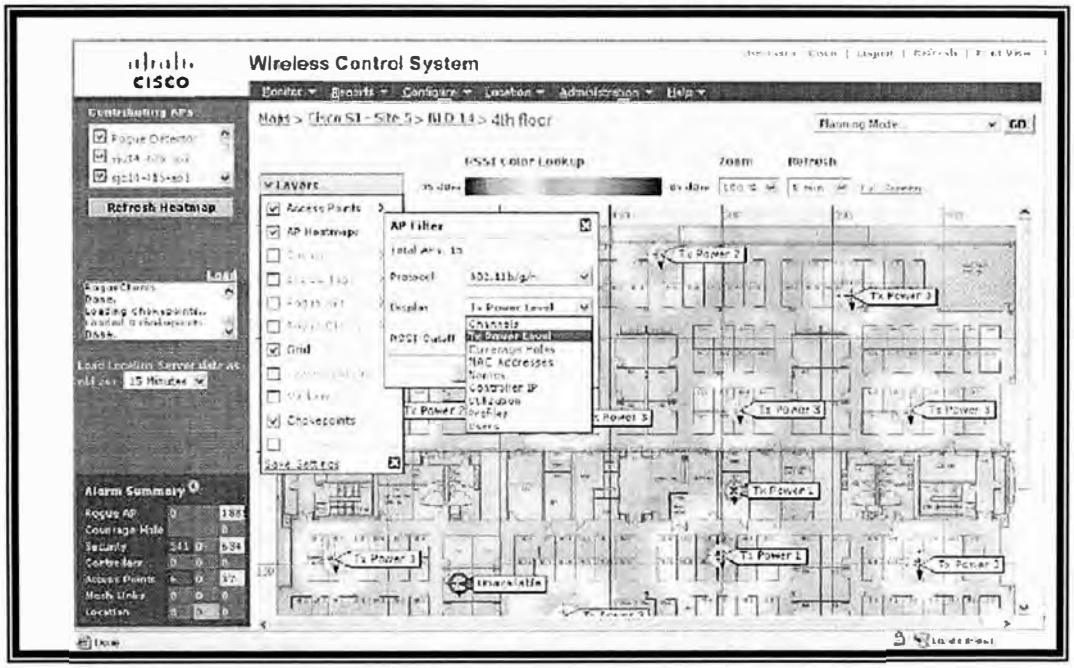


Fig. A.2 Interfase de Administración del WCS de Cisco

El software WCS puede ser implantado en servidores con sistema operativo Windows 2003 Server o Red Hat Enterprise 4 y es administrado mediante vía web-browser

Mediante el uso de los tres componentes de esta tecnología (AP LWAPP, WCL y WCS) es factible construir una solución de red inalámbrica a nivel empresarial.

En el caso de SAN ANDRES, el objetivo mediante la arquitectura Cisco Unified Wireless Network es disponer de una red inalámbrica capaz de soportar en tiempo real aplicaciones de video y voz, con soporte de aplicaciones de negocio empresarial con el mayor rendimiento, que provea seguridad y movilidad a usuarios, compatible con nuevos

estándares inalámbricos como el 802.11n, y sea administrable y gestionada de forma centralizada.

ANEXO B

Los Beneficios de las Wireless LAN Centralizadas

Tradicionalmente, las redes LAN inalámbricas han tenido una falta de perspectiva, porque cada punto de acceso funciona como un nodo independiente, autónomo configurado con canales y ajustes de potencia de RF de un plan (generalmente una predicción de RF). Si bien estos puntos de acceso autónomos pueden oír un punto de acceso operando en el mismo canal, el punto de acceso autónomo no tiene manera de determinar si el punto de acceso adyacente es parte de la misma red o de un vecino de red. En algunos casos, la aplicación de una WLAN utilizando puntos de acceso autónomo impone límites a la WLAN. Las ventajas de la solución centralizada de Cisco permiten optimizar los siguientes aspectos.

- Seguro Roaming a nivel de capa 2 y capa 3.
- Funcionalidades de IDS, habilidad para detectar ataques y accesos no autorizados por la red inalámbrica.
- Servicios de ubicación, de dispositivos WIFI usando a los parámetros de RSSI
- Manejo Dinámico del comportamiento RF, mediante la adaptación automática al entorno RF.
- Balanceo de Carga, entre puntos de acceso vecinos.
- Servicios para invitados, permite un rápido desarrollo de esquemas de acceso controlados con niveles de seguridad adecuados.
- Voz sobre WLAN, servicios de real time con QoS.
- Administración, Administración e implementación de la solución de manera rápida y sencilla.

Centralización de WLAN

Siguiendo el camino de las redes celulares, Cisco Systems ® WLAN es pionera en la centralización y entrega a la industria de la primera plataforma unificada de servicios avanzados de LAN inalámbrica. La clave de la arquitectura unificada de Cisco, denominado Red inalámbrica unificada de Cisco, es la entrega de datos desde un punto de acceso llamado lightweight access point, a través de la red a un equipo controlador de la LAN inalámbrica.

Cisco ofrece muchos controladores de LAN inalámbrica que permiten la centralización de las redes LAN inalámbricas, tales como la serie Cisco 4400 y los controladores de LAN inalámbrica de Cisco Serie 2300, así como los controladores de LAN inalámbrica integrados dentro de otros equipos de tipo modular, como el Módulo de servicios inalámbricos (WiSM) de la serie Cisco Catalyst 6500 y el módulo de controlador de LAN inalámbrica (WLCM) para Routers de Servicios Integrados.

Para desarrollar la comunicación entre el llamado lightweight access point y un controlador de LAN inalámbrica, un nuevo protocolo era necesario. Este protocolo fue necesario implementarlo para hacer frente a los siguientes requisitos:

Facilidad de despliegue, la configuración de los APs se hace más sencilla al manejar el controller una única interfase y plantilla de configuración para todos los puntos de acceso.

Despliegue de seguridad, el hecho de que un punto de acceso esté conectado a la red, no significa que éste deberá tener acceso total a los servicios de la red. El protocolo proporciona un camino para ofrecer una forma de autenticación de todos los puntos de acceso y usuarios conectados a la red.

Control en tiempo real del punto de acceso, una vez que el punto de acceso está desplegado, autenticado y conectado al controlador, el protocolo proporciona lo necesario para la gestión y despliegue de servicios en tiempo real.

Protocolo extensible, es decir permite trabajar a través de una multitud de plataformas, desde el chasis a base de módulos en los grandes switches Ethernet, a equipos routers y cualquier otro elementos de la red.

El protocolo ha de ser capaz de funcionar a baja velocidad a través de enlaces WAN e incluso, por el aire (para aplicaciones como redes inalámbricas de malla).

Cisco ha explorado muchas opciones para hacer frente a las necesidades de desarrollo del nuevo protocolo de comunicaciones. La Encapsulación de enrutamiento genérico (GRE) se consideró como una opción inicial, pero GRE no admite visibilidad en las variedades de paquetes de capa 2, que es una necesidad para la seguridad WLAN. SNMP también se consideró, ya que este protocolo proporciona el mando y el control del punto de acceso, pero su volumen de información hace que no sean las ideales.

Después de examinar otros protocolos, Cisco decidió elaborar un nuevo Protocolo, el Lightweight Acceso-Point Protocol (LWAPP), que permite operar, tanto al Nivel 2 y Nivel 3 de paquetes de información.

¿Qué es LWAPP?

LWAPP es un proyecto del Internet Engineering Task Force (IETF), realizado por Cisco Systems, que normaliza el protocolo de comunicaciones entre los puntos de acceso ligeros y los sistemas de WLAN, como controladores, switches y routers. Sus objetivos son:

- Reducir la cantidad de procesamiento en los puntos de acceso, liberando sus recursos informáticos, para centrarse exclusivamente, en el acceso inalámbrico en lugar de filtrado y la aplicación de la política de seguridad.

- Permitir el manejo centralizado del tráfico, autenticación, cifrado y la aplicación de la política de todo un sistema WLAN
- Proporcionar un encapsulado genérico y un mecanismo de transporte para la interoperatividad de access point multivendor, usando tanto una infraestructura de capa 2 o una red de ruteo IP.

El LWAPP logra estos objetivos con las siguientes funcionalidades:

Descubrimiento de dispositivos access point, intercambio de información y software de control para la encapsulación, fragmentación y formateo de paquetes; adicionalmente, facilitando la administración de la comunicación entre los access point y los controladores inalámbricos.

(Extracto Traducido del documento " The Benefits of Centralization in Wireless LANs via the Cisco Unified Wireless Network http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/prod_white_paper0900aecd8040f7b2_ps6108_Products_White_Paper.html)

ANEXO C

Glosario de Términos

A

AD (Active Directory), Directorio Activo

ACK (Acknowledgment), Acuse de Recibo

AES (Advanced Encryption Standard), Estándar de Encriptación Avanzado

AP (Access Point), Punto de Acceso

B

BSS (Basic Service Set), Conjunto de Servios Básicos

C

CCK (Complementary Code Keying), Clave de Código Complementaria

CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance), Acceso Múltiple con Detección de Portadora con Prevención de Colisiones

CTS (Clear To Send), Autorización de Envío

D

DHCP (Dynamic Host Configuration Protocol), Protocolo de Configuración de Hosts Dinâmicos

DNS (Domain Name Server), Servidor de Nombres de Dominio

DSSS (Direct Sequence Spread Spectrum), Espectro Disperso de Secuencia Directa

E

EAP (Extensible Authentication Protocol), Protocolo de Autenticación Extensible

ESS (Extended Service Set), Conjunto de Servicios Extendidos

EAP-TLS: EAP-Transport Layer Security

EAP-TTLS: EAP-Tunneled TLS

F

FHSS (Frequency Hopping Spread Spectrum), Espectro Disperso de Salto de Frecuencia

H

HR/DS o HR/DSSS (High-Rate Direct Sequence), Secuencia Directa de Alta Tasa

HTTP (Hypertext Transfer Protocol), Protocolo de Transferencia de páginas de Hipertexto

IP (Internet Protocol), Protocolo de Internet

IR (Infrared Light), Luz Infrarroja

L

LAN (Local Area Network), Red de Área Local

LWAPP (Lightweight Access Points Protocol), Protocolo de Ligero para Puntos de Acceso

M

MAC (Medium Access Control), Capa de Control de Acceso al Medio

MIMO (Multiple Inputs / Multiple Outputs), Múltiples Entradas / Múltiples Salidas

O

OFDM (Orthogonal Frequency Division Multiplexing), Multiplexación por División de Frecuencia Ortogonal

OSI (Open Systems Interconexión), Interconexión de Sistemas Abiertos

P

PHY (Physical Layer), Capa Física

PIFS (Point Coordination IFS), IFS de Función de Coordinación Centralizada

PSK (Pre-Shared Key), Pre-Clave Compartida

Q

QoS (Quality of Service), Calidad de Servicio

R

RADIUS(Remote Authentication Dial In User Services), Autenticación Remota para Servicios de Usuarios vía red Telefónica

RTS (Request To Send), Solicitud de Envío

S

SSID (Service Set Identify), Identificador de Conjunto de Servicios

T

TCP/ IP (Transport Control Protocol/Internet Protocol), Protocolo de Control deTransporte/Protocolo de Internet

TKIP (Temporary Key Integrity Protocol), Protocolo de Integridad de Claves Temporales

V

VLAN (Virtual LAN), Redes LAN Virtuales

VoIP (Voice over IP), Voz sobre IP

W

WAN

(Wide Area Network), Red de Área Extendida

WCS (Cisco Wireless Control System), Sistema de Control Inalámbrico

WDS (Wireless Distribution System), Sistema de Distribución Inalámbrico

WEP (Wired Equivalent Privacy), Privacidad Equivalente Cableada

Wi-Fi (Wireless Fidelity), Fidelidad Inalámbrica

WLAN (Wireless Local Area Network), Redes Inalámbricas de Área Local

WLC (Cisco Wireless LAN Controller), Controladores de Puntos de Acceso

WPA (Wi-Fi Protected Access), Acceso protegido Wi-Fi

WWW o WEB (World Wide Web), Red Extendida a nivel Mundial

BIBLIOGRAFIA

1. GAST MATTHEW S, “Redes Wireless 802.11”, 1ra Edición Español, ANAYA MULTIMEDIA S.A., España 2006.
2. STALLINGS WILLIAM,”Comunicación y Redes de Computadoras”, 7ma Edición, Pearson Educación S.A., Madrid 2004.
3. TANENBAUM ANDREW S., “Redes de Computadoras”, 4ta Edición, Pearson Educación, México 2003.
4. TABACMAN EDUARDO, “Redes Inalámbricas: Lo que saben los Hackers y UD. no”, VIRUSPROT.COM, 2007
5. GARCÍA CARLOS, “Propuesta de arquitectura de QoS en entorno inalámbrico 802.11e basado en Diffserv con ajuste dinámico de parámetros”, Tesis Doctoral, Departamento Ingeniería Telemática, Universidad Carlos III de Madrid, España 2006.

DIRECCIONES ELECTRÓNICAS:

6. Cisco Systems
   www.cisco.com
7. Cisco Unified Wireless Network
   http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html
8. Why Migrate to the Cisco Unified Wireless Network?
   http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_white_paper0900aecd804f19e3.shtml
9. Enterprise Mobility 4.0 Design Guide
   http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html)
10. Components, products, features and benefits of the Cisco Unified Wireless Network.
    http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a0080184925.html

11. Cisco Aironet Series products
http://www.cisco.com/en/US/products/hw/wireless/index.html
12. Cisco 4400 Series Wireless LAN Controllers
http://www.cisco.com/en/US/products/ps6366/index.html
13. Cisco Wireless Control System (WCS)
http://www.cisco.com/en/US/products/ps6305/index.html
14. Curso gratis de Redes Inalámbricas WIFI http://www.virusprot.com/cursos/Redes-Inalámbricas-Curso-gratis.htm
15. Microsoft TechNet Latinoamérica –Redes 802.11
http://www.intel.com/support/sp/wireless/wlan/sb/cs-008413.htm
16. Capítulo 6: Diseño de seguridad para LAN inalámbrica mediante 802.1X, Microsoft TechNet,
http://thesource.ofallevil.com/latam/technet/articulos/wireless/pgch06.mspx
17. Capítulo 13: Guía de prueba, Microsoft TechNet
http://thesource.ofallevil.com/latam/technet/articulos/wireless/tgch13.mspx
18. Site Survey Tips & Techniques
http://www.visiwave.com/index.php/ScrInfoTips.html
19. Wireless LAN (Wifi) Tutorial
http://www.tutorial-reports.com/wireless/wlanwifi/introduction_wifi.php
20. VoWLAN Design Recommendations
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html)
21. EAP−TLS under Unified Wireless Network with ACS 4.0 and Windows 2003
http://www.cisco.com/application/pdf/paws/71929/eap-tls-acs40-win2003.pdf
22. Seguridad en Redes WIFi
http://www.scribd.com/doc/3942243/seguridad-en-redes-WIFI