UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE ELECTRICA
CARACAS
TRABAJO ESPECIAL DE GRADO

Mejoramiento y actualización de las redes inalámbricas WLAN de YPERGAS

Tutor Académico: Prof. Bruzual Zeldivar
Asesor Empresarial: Ing. Alberto Fernández

Presentado ante la Ilustre
Universidad Central de Venezuela para
Optar al Título de Especialista en
Comunicaciones y Redes de Comunicación de datos
Por la Lic. Rosellys Márquez Golindano

Caracas, Mayo 2009

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE ELECTRICA
CARACAS

Mejoramiento y actualización de las redes inalámbricas WLAN de YPERGAS

Trabajo Especial de Grado presentado por: Rosellys Márquez Golindano

Realizado con la asesoría de: Prof. Zeldivar Bruzual, Ing. Alberto Fernández

RESUMEN

El siguiente trabajo muestra en una etapa de evaluación preliminar, el estado en el que se encontraba la WLAN, sus riesgos y vulnerabilidades, además de identificar los equipos y su configuración, la topología lógica y física de la red inalámbrica, se determinó el uso que tenia la WLAN dentro de la empresa. En la etapa de análisis y documentación, se describieron las diversas recomendaciones, estándares y normas de seguridad en el área de redes inalámbricas, documentando las soluciones diseñadas según el fabricante Cisco, tecnología implantada en la empresa, además de señalar las mejores prácticas de la industria, se identificaron y analizaron los riesgos y vulnerabilidades existentes y las posibles actualizaciones de software en los equipos inalámbricos. En la etapa de implementación, se evalúo la situación de la WLAN y se diseñó un esquema basado en la etapa de análisis y documentación y en los objetivos planteados para este trabajo, se seleccionaron las mejores prácticas que se adaptaban a la solución señalada del fabricante, se documentaron los cambios que se realizaron a nivel físico y lógico en la WLAN, y la configuración que se realizó en los equipos, además se elaboraron guías rápidas de configuración para los usuarios visitantes y para personal técnico con el fin de facilitar el buen uso de la red.

PALABRAS CLAVES

seguridad, redes inalámbricas, wep, wpa, wpa2, wlan

DEDICATORIA

A mi mami, por apoyarme en todo momento y darme una carrera para mi futuro. Siempre amiga, compañera y excelente madre.

A mi hija Rosangel por ser el motivo de mi vida. Te amo mucho!

A mi hermano Luis Rafael, mi abuela Rosa y mi tío Pedro, a pesar de que no estén conmigo, sé que sus almas siempre me acompañan en todo momento. Siempre los recordaré!.

A mi esposo Luis Antonio, gracias por existir y ser parte de mi vida. Gracias por tu apoyo. Te amo mucho!

A mi tío Abigail, por ser mi guía y ejemplo a seguir.

AGRADECIMIENTOS

Gracias a Dios, por permitirme llegar a este momento tan importante de mi vida y lograr otra meta más en mi carrera.

Al Ing. Alberto Fernández, gracias por brindarme el apoyo incondicional en todo momento, sin ti no lo hubiese logrado.

Al Prof. Zeldivar Bruzual por brindarme su orientación y apoyo durante el desarrollo de este trabajo.

A mis excelentes y queridos compañeros de trabajo Luis, José Gregorio, Francisco y Emira por su apoyo incondicional durante la realización de este proyecto. Al fin lo logre!.

A todas aquellas personas que dentro y fuera de YPERGAS, quizás sin saberlo, me ayudaron en este proyecto y me permitieron aprender.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

LISTA DE SIMBOLOS Y ABREVIATURAS

PA	Punto de Acceso
WLAN	*Wireless Local Area Network*
UMTS	*Universal Mobile Telecommunications System*
LMDS	*Local Multipoint Distribution Service*
PYMES	Pequeñas y Medianas empresas
SSID	*Service Set Identifier*
SNMP	*Simple Network Management Protocol*
WEP	*Wired Equivalent Privacy*
WAP	*Wi-Fi Protected Access*
NIC	*Network Information Center*
VPN	*Virtual Private Network*
RADIUS	*Remote Access Dial-In User Server*
AAA	*Authentication, Autorización, Accounting*
PCMCIA	*Personal Computer Memory Card International Association*
ACK	*Acknowledgement*

INTRODUCCION

Las redes inalámbricas de área local, tienen un papel cada vez más importante en las comunicaciones de hoy en día. Debido a su facilidad de instalación y sus costos más asequibles se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red cableada. En muchas ocasiones son instaladas como complemento de redes cableadas para brindar mayor flexibilidad a los usuarios.

La movilidad que proporcionan las redes inalámbricas ha generado el auge de las mismas, ya que es una manera de realizar conectividad de datos sin necesidad de cableado estructurado. El acceso sin necesidad de cable, es la razón que hace popular estas redes y es a la vez el problema más grande en cuanto a seguridad se refiere.

Las redes inalámbricas envían los datos a través del aire, en forma de ondas de radio, y pueden ser accesibles desde fuera de los límites físicos de una empresa. Son susceptibles a múltiples tipos de ataques como intercepción de datos, inserción de usuarios y equipos de red no autorizados, interrupción del servicio, aumento de cobertura de forma no autorizada, entre otras. Todos estos ataques aprovechan las vulnerabilidades inherentes a la propia tecnología y exponen la debilidad en la configuración de seguridad de muchas redes inalámbricas.

Las amenazas más comunes son: revelación de información a personas no autorizadas, inexactitud de los datos almacenados, tratados o transmitidos, inaccesibilidad de la información cuando se necesita. Generalmente las redes inalámbricas seguras deben proveer mecanismos de autenticación, integridad de datos, confidencialidad de la información y disponibilidad del servicio.

Este trabajo consta de siete 6 capítulos.

1.1 - Proyecto Yucal Placer

El 29 de Junio del 2001, el Ministerio de Energía y Minas de Venezuela concluye el proceso de selección para el otorgamiento de las primeras licencias de gas al Grupo Trío Yucal Placer de la licencia para el desarrollo de los bloques de gas Yucal Placer Sur y Norte.

Estas licencias son de tipo concesión con una duración de 35 años. La regalía es de 20% sobre la producción a la cual se añade la contraprestación. Los bloques de Yucal-Placer están ubicados al noreste del estado Guárico cerca de la localidad de Altagracia de Orituco, 150 Km, al sureste de Caracas.

El desarrollo de los bloques Yucal-Placer se concibe por etapas para una mejor evaluación del campo y de sus potencialidades durante la primera fase. Esta modalidad permite la introducción progresiva de gas natural en el mercado, sin necesidad de saturarlo, pero satisfaciendo adecuadamente el incremento de la demanda. Este incremento se espera aumente en un 85% en los próximos veinte (20) años. En las etapas de desarrollo del campo se llevarán campañas de sísmica, perforación de nuevos pozos y la construcción de estaciones de recolección, de unidades de procesamiento del gas y de líneas de flujo. Las fases están programadas como se indica a continuación:

- Una primera fase consiste en una producción inicial de 2,83 millones de metros cúbicos estándar por día, en la cual se deshidratará el gas y se despachará a través de una tubería a la estación de comprensión al norte de los bloques. Con esta fase se podrá adquirir la mayor cantidad posible de información de los yacimientos que no han sido hasta ahora evaluados. A esta primera fase se la ha llamado Fase EPS o esquema de Producción Temprana (*Early Production Sheme*-EPS).

- Una segunda fase, a comenzar después, consiste en elevar la producción a 8,4 millones de metros cúbicos estándar por día. En esta fase se deshidratará y se separará el CO2 a través de un tratamiento de endulzamiento. Con esta fase se logrará un nivel de producción adecuado para la rentabilidad del proyecto y el abastecimiento del mercado. A esta segunda fase se le ha llamado: Fase 300.

El proyecto plantea grandes retos técnicos, dada la difícil productividad de los pozos, la alta concentración de CO2, las altas temperaturas de los yacimientos y la rápida planificación que se ha previsto para el mismo.

1.2 - La Empresa: YPERGAS

Ypergas, surge de la alianza estratégica de la empresa francesa Total (58,3%), la Hispano Argentina Repsol-YPF (11,5%), las venezolanas Inepetrol (0,1%) y Otepi (0,1%) para la búsqueda y explotación de gas libre en el campo Yucal Placer.

Dentro del grupo, se ha incluido una operadora cuya mayoría accionaria de 51% pertenece a socios venezolanos, el 49% restante controlado por Total y Repsol YPF. La Figura 0-1 representa la organización jurídica y legal de YPergas, tal como se mencionó anteriormente.

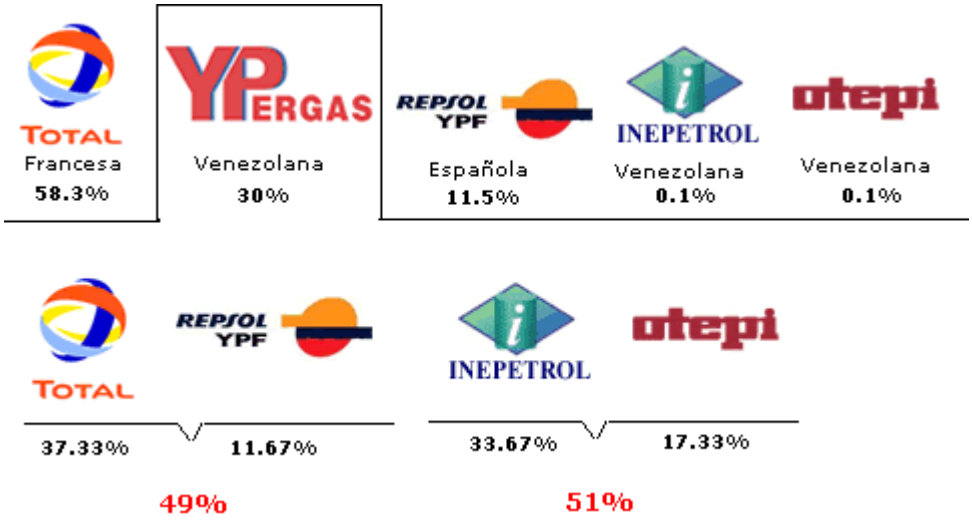


Figura 0-1 Organización jurídica y legal de Ypergas

1.3 - Planteamiento del problema

Ypergas, cuenta con una red local, *Ethernet*, a la cual se encuentran conectados aproximadamente 170 usuarios. Además, tiene una red inalámbrica de área local (WLAN) provista de puntos de accesos y tarjetas inalámbricas Cisco, la cual será nuestro caso de estudio.

La red inalámbrica de la empresa actualmente está provista de una configuración muy débil, tiene los mecanismos básicos de seguridad, no está totalmente protegida, con lo cual se está poniendo en riesgo la confidencialidad e integridad de la información.

La seguridad de la red inalámbrica en la empresa es una necesidad, dadas las características de la información que por ellas se transmite y porque en algunos casos esta red se utiliza como una opción alternativa a la red cableada.

De lo mencionado se derivan las siguientes preguntas de investigación:

¿Qué cambios son necesarios en los equipos inalámbricos, tomando en cuenta la reutilización de equipos, mejoramiento de seguridad, facilidad de uso y administración para proveer servicios que garanticen a los usuarios de la red la preservación de la confidencialidad, integridad y disponibilidad de los datos y recursos computacionales?

1.4 - Objetivos

- Describir el uso actual de las redes inalámbricas en la empresa YPergas.
- Precisar y determinar los potenciales riesgos de seguridad que presentan actualmente las redes inalámbricas en la empresa YPergas.
- Evaluar e implementar cambios necesarios en los equipos inalámbricos, tomando en cuenta la reutilización de equipos, mejoramiento de seguridad, facilidad de uso y administración y cobertura en las áreas de interés.
- Configurar conexiones de equipos corporativos y equipos no corporativos dentro de la misma infraestructura inalámbrica.
- Elaborar documentos para usuarios y personal técnico, con el fin de facilitar el uso y administración de las redes inalámbricas.
- Especificar el desarrollo general del proyecto.

1.5 - Alcance del proyecto

El proyecto es realizado en las instalaciones de la empresa YPergas, y se tiene previsto desarrollar las siguientes actividades:

- Evaluación del estado actual de la red inalámbrica. En esta actividad se tiene contemplado: identificar los componentes de la red inalámbrica, verificar las

bondades de los equipos, determinar las necesidades de actualización y los mecanismos de seguridad con que cuenta, investigar los ítems que se van a configurar en el equipamiento.

- Actualización de *software* en los equipos. En el análisis de la red inalámbrica se determina el *software* que tienen los equipos y en esta actividad se realizará una actualización de los mismos.

- Adaptar los mecanismos de seguridad necesarios. En esta actividad se configurarán los mecanismos de seguridad, que se adapten a las necesidades de la red inalámbrica.

- Determinar los cambios físicos y lógicos que se aplicarán a la infraestructura de redes a fin de permitir las conexiones inalámbricas de usuarios corporativos así como usuarios no corporativos en todas las áreas de interés.

- Configurar los equipos inalámbricos existentes tomando en consideración los requisitos físicos, lógicos.

- Elaboración de guías de referencia rápida para usuarios así como documentos de administración para el personal técnico de la empresa.

Es de resaltar que este proyecto no tiene contemplado el estudio de cobertura de la red inalámbrica ni la incorporación de VPN.

CAPÍTULO 1 - MARCO TEORICO

1.1 - Seguridad

Los 3 pilares fundamentales en los que se basa la seguridad son:

- Confidencialidad

  Asegura que sólo las personas autorizadas tengan acceso a la información. La confidencialidad protege contra la revelación de la información.

  Impide que el contenido de un mensaje o un documento puedan ser entendidos por entes no autorizados.

- Integridad

  Comprueba que los datos recibidos sean exactamente igual a los datos transmitidos. Es decir que los datos no hayan sido dañados por errores causados por interferencia y ruido radioeléctrico y que no haya sido alterada intencionalmente en su contenido o en su secuencia (ej. párrafos o trozos cambiados de posición).

- Disponibilidad

  Asegura que:

  El servicio no sea negado a los usuarios autorizados.

  Los sistemas informáticos trabajen con un buen desempeño y con un retardo mínimo.

  Se pueda restablecer prontamente el servicio en caso de fallas (ej. daño de un disco duro), accidentes menores (ej. infección de virus) y desastres naturales (ej. terremoto).

Los servicios de seguridad se implantan por medio de mecanismos, controles y funciones de seguridad.

Los mecanismos de seguridad utilizados se basan en los siguientes métodos o técnicas:

- Cifrado, permite garantizar la privacidad e integridad.
- Autenticación, permite identificar a cada usuario y equipo como medio para controlar el acceso a recursos y servicios.
- Autorización, controlar el acceso a recursos y servicios.
- Auditoría, registro de los accesos.

1.2 - Redes WLAN

El término WLAN, es una acepción inglesa cuyas siglas se corresponde con *Wireless Local Area Net*, o lo que es lo mismo en castellano Redes de Área Local Inalámbricas. Este tipo de redes nos proporcionan un sistema de comunicación muy flexible al eliminar por completo la utilización de cables, a diferencia de las otras LAN, si bien las WLAN no intentan sustituir por completo al resto de LAN´s sino que se suelen utilizar como complemento a estas.

Una red de área local inalámbrica (WLAN), es un sistema de comunicación de datos flexible que puede reemplazar o extender una red de área local cableada (LAN) para ofrecer funcionalidad adicional. Una red de área local cableada tradicional (LAN) envía paquetes de datos desde un equipo a otro a través de cables. Una red de área local inalámbrica (WLAN), por el contrario, depende de ondas de radio para transferir datos (Ver Figura 1-1). Estos datos son sobrepuestos en una onda de radio por medio de un proceso denominado modulación, y esta onda portadora, actúa entonces como el medio de transmisión, ocupando el lugar del cable.

La importancia de la red de área local inalámbrica, sin embargo, va mucho más lejos de ausencia de cables. La llegada de la WLAN da inicio a una completa nueva definición de la infraestructura de red. Una infraestructura ya no necesita ser sólida y fija, difícil de movilizar y costosa de cambiar. Por el contrario, puede moverse con el usuario y cambiar tan rápido como la organización lo haga. Por ejemplo, la gente de negocios puede permanecer conectada mientras se moviliza a través del campo corporativo, explotando fácilmente los recursos de la red cableada.

Entre los componentes que permiten configurar una WLAN podemos mencionar los siguientes:

- **Terminales de Usuarios (Clientes)**

Tarjeta Interfaz de Red (NIC) o cliente, también conocida como Tarjeta Inalámbrica, es una tarjeta generalmente de tipo PCMCIA, que se instala en la computadora portátil (o en cualquier otro terminal de red que se desee conectar). Incluye un transceptor de radio y la antena; puntos de acceso (PA), que permiten enviar la información de la red cableada (Por ejemplo: *Ethernet*) hacia los NIC/clientes.

- **Punto de Acceso (PA)**

El punto de acceso o PA (típicamente dotado de una antena omnii-direccional) es el *"hub"* que permite reenviar la información de la red cableada (Por ej. *Ethernet*) hacia los NIC/Clientes. En algunas ocasiones una WLAN puede exigir el empleo de varios PA para garantizar la cobertura radio de todos los usuarios de la zona considerada. (Ver Figura 1-1) Algunas redes WLAN de topología sencilla y que trabajan de forma autónoma no necesitan utilizar PA, como las redes *ad-hoc*.

Por medio de la instalación de un PA, es posible duplicar la distancia a la cual los dispositivos pueden comunicarse, ya que éstos actúan como repetidores de la señal. Desde que el PA se conecta a la red, cualquier cliente tiene acceso a los recursos del servidor y, además, este dispositivo gestiona el tráfico de la red entre las terminales más próximas. Cada PA puede servir a varias máquinas, según el tipo y el número de transmisiones que se realicen.

Los PA tienen un alcance finito, que generalmente es del orden de los 150 metros en lugares cerrados y de 300 metros en áreas abiertas. Además, puede existir un rango de 15 a 50 dispositivos cliente con un solo PA.

En zonas grandes, como por ejemplo un *campus* universitario o un edificio, es probable que se necesite la instalación de más de uno de éstos (repitiendo la señal). El objetivo es cubrir el área con células que solapen sus áreas así los clientes puedan moverse sin cortes entre los grupos de PA. Esto es llamado *roaming* o itinerancia.

Siempre que la red inalámbrica disponga de más de una celda es posible para los clientes inalámbricos desplazarse entre las áreas de cobertura de cada uno de ellos sin perder la conexión.

Para hacer posible el *roaming* las áreas de cobertura definidas por las celdas deben solaparse ligeramente. Si no hay solapamiento, al desplazarnos de un área a otra perderemos la conexión, aunque la recuperaremos de nuevo automáticamente al entrar en el área de cobertura de otro PA. Para que el *roaming* sea posible, todas las estaciones base deben utilizar el mismo nombre de red SSID y las mismas claves de encriptación WEP. La legislación Europea permite la utilización de los Canales 1-13 de los definidos en el Estándar IEEE 802.11b. Para evitar la interferencia entre canales adyacentes, las estaciones bases contiguas deben utilizar frecuencias separadas al menos 5 canales.

- **Controlador de PA**

Necesario para despliegues que requieren varios PA por razones de cobertura y/o tráfico. Suele incorporar funcionalidad de PA, de clientes VPN, de cliente RADIUS para labores de autenticar y autorizar con un servidor AAA apropiado, *de routing*, y de *firewalls*.

Las redes de área local inalámbricas (WLANs), constituyen en la actualidad una solución tecnológica de gran interés en el sector de las comunicaciones inalámbricas de banda ancha. Estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado y le permite competir con otro tipo de tecnologías de acceso inalámbrico de última generación como UMTS y LMDS, pues éstas requieren de un importante desembolso económico previo por parte de los operadores del servicio. Ahora bien, ello también obliga al desarrollo de un marco regulatorio adecuado que permita un uso eficiente y compartido del espectro radioeléctrico de dominio público disponible.

Existen dos prácticas bien conocidas para localizar redes inalámbricas:

- **El *warchalking***, que consiste en caminar por la calle con un computador portátil dotado de una de una tarjeta WLAN, buscando la señal de puntos de acceso.

Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red.

- **El *wardriving*,** propio para localizar puntos de acceso inalámbricos desde un automóvil. Se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada, un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas, que se encuentra libremente en Internet.

Originalmente las redes WLAN fueron diseñadas para el ámbito empresarial. Sin embargo, en la actualidad se ha encontrado una gran variedad de escenarios de aplicación, tanto públicos como privados: entorno residencial y del hogar, grandes redes corporativas, PYMES, zonas industriales, campus universitarios, entornos hospitalarios, ciber-cafés, hoteles, aeropuertos, medios públicos de transporte, entornos rurales, etc. Incluso son ya varias las ciudades en donde se han instalado redes inalámbricas libres para acceso a Internet.

En la Figura 1-1, se puede observar una red WLAN que permite reemplazar por conexiones inalámbricas los cables que conectan a la red los PCs, portátiles u otro tipo de dispositivos, dotando a los usuarios de movilidad en las zonas de cobertura alrededor de cada uno de los puntos de acceso, los cuales se encuentran interconectados entre sí y con otros dispositivos o servidores de la red cableada. Entre los componentes que permiten configurar una WLAN se pueden mencionar los siguientes: terminales de usuario o clientes (dotados de una tarjeta interfaz de red que integra un transceptor de radiofrecuencia y una antena), puntos de acceso y controladores de puntos de acceso, que incorporan funciones de seguridad, como autorización y autenticación de usuarios, *firewall*, etc.

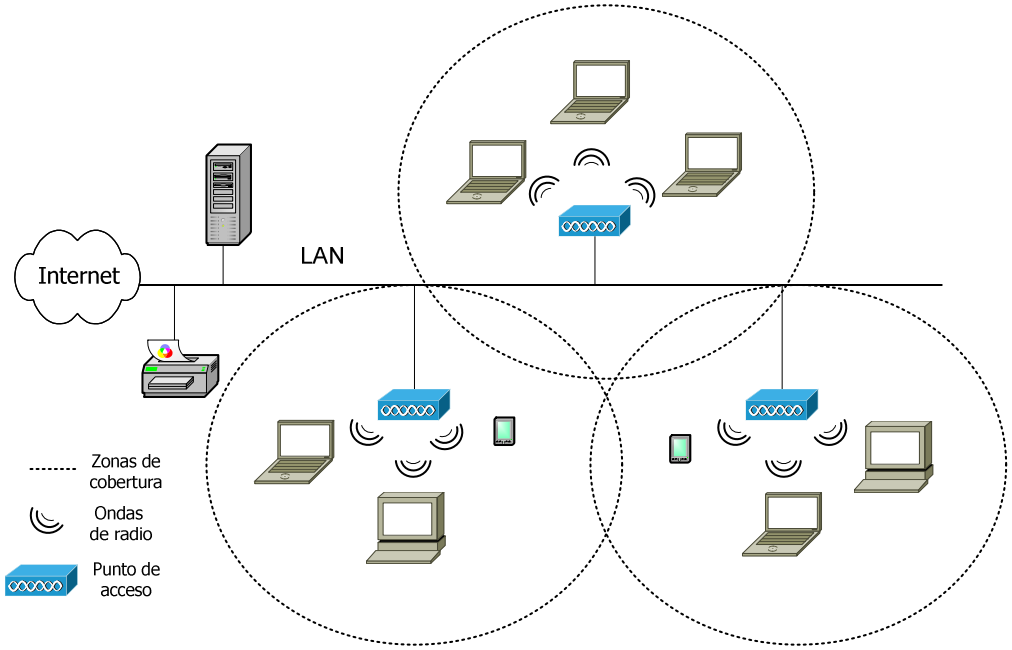


Figura 1-1 Redes WLAN en ambiente corporativo

Utilizando una WLAN se puede acceder a información compartida sin necesidad de buscar un lugar para conectar el computador, y los administradores de la red pueden aumentar la red sin instalar o mover cables.

Frente a las redes tradicionales se tienen las siguientes ventajas en cuanto a productividad, comodidad y costos:

- Movilidad: Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.
- Facilidad de instalación: Evita obras para incorporar cable por muros y techos.
- Flexibilidad: Permite llegar donde el cable no puede.
- Reducción de costos: Cuando se dan cambios frecuentes o el entorno es muy dinámico el costo inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.
- Escalabilidad: El cambio de topología de red es sencillo y trata igual pequeñas y grandes redes.

1.3 - Topologías

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no administradas, alojadas y par a par, e infraestructura y "*ad hoc*". En este documento se utilizarán los términos "infraestructura" y "*ad hoc*". Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

1.3.1 - Modo *Ad-Hoc*

En una topología *ad hoc*, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas *ad hoc* serían un domicilio sin red.

Una red *ad-hoc* (entre iguales), es una red de área local independiente que no está conectada a una infraestructura con cables y en la que todos los puestos están directamente conectados entre sí (lo que se conoce como topología de malla). La configuración de una WLAN en modo *ad-hoc* se emplea para establecer una red cuando no exista una infraestructura inalámbrica o cuando no se requieran servicios. Ver Figura 1-2

En el modo *ad hoc* se puede decir que no tiene punto de acceso. En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controla el punto de acceso, como la señalización y la sincronización, son controladas por una estación. La red *ad hoc* no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

1.3.2 - Modo Infraestructura

Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica con la red LAN cableada y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la

transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

En una red de infraestructura, los clientes de la WLAN se conectan a la red corporativa a través de un punto de acceso inalámbrico, trabajando como lo haría un cliente con cable. La mayoría de las LAN inalámbricas corporativas funcionan en modo de infraestructura y acceden a la red de cable para conectar con impresoras y servidores de archivos. Ver Figura 1-2

La mayoría de las redes *wireless* que podemos encontrar en las empresas utilizan modo infraestructura con uno o más Puntos de Acceso. El PA actúa como un *hub* en una LAN, redistribuye los datos hacia todas las estaciones.

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones. Observe que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

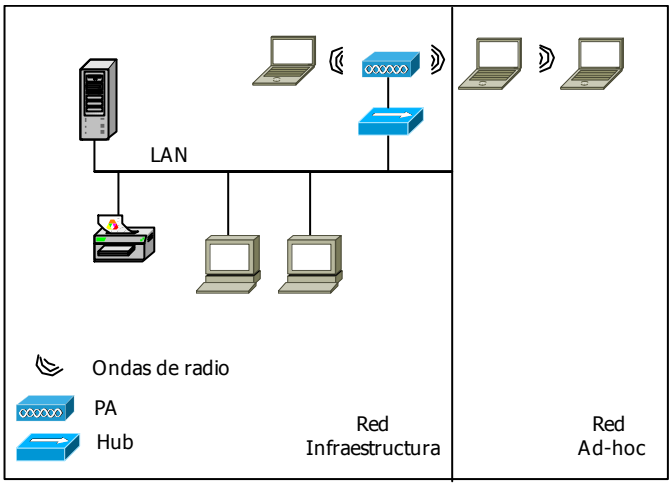


Figura 1-2 Red Infraestructura versus Red *Ad-hoc*

1.4 - Como trabaja una WLAN

Se utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio, son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. En una configuración típica de WLAN los puntos de acceso (*transceiver*) conectan la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos 30 metros y 100 metros.

El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: *Network Operating System*) y las ondas, vía una antena.

1.5 - Conexión a WLAN

La Figura 1-3, muestra los pasos que debe realizar un cliente para asociarse con un PA.

El proceso de asociación tiene dos pasos, envueltos en 3 estados:

1.- No autenticado y no asociado

2.- Autenticado y no asociado

3.- Autenticado y asociado

En la transición por los diferentes estados, ambas partes (cliente y PA) intercambian mensajes llamados *management frames.*

El proceso que realiza un cliente *wireless* para encontrar y asociarse con un PA es el siguiente:

Los PA transmiten *beacon frames* (anuncios de la red) cada cierto intervalo de tiempo fijo. Para asociarse con un PA y unirse a una red en modo de infraestructura, un cliente escucha en busca de *beacon frames* para identificar puntos de acceso. El cliente también puede enviar una trama *prove request* que contenga un SSID.

Después de identificar al PA, el cliente y el PA realizan autenticación mutua intercambiando varios *management frames* como parte del proceso. Hay varios mecanismos de autenticación que veremos más adelante.

Después de una autenticación realizada con éxito, el cliente pasa a estar en el segundo estado (autenticado y no asociado). Para llegar al tercer estado (autenticado y asociado) el cliente debe mandar una trama *assocciation request* y el PA debe contestar con una trama *association response*, entonces el cliente se convierte en un *host* mas de la red *wireless* y ya esta listo para enviar y recibir datos de la red.

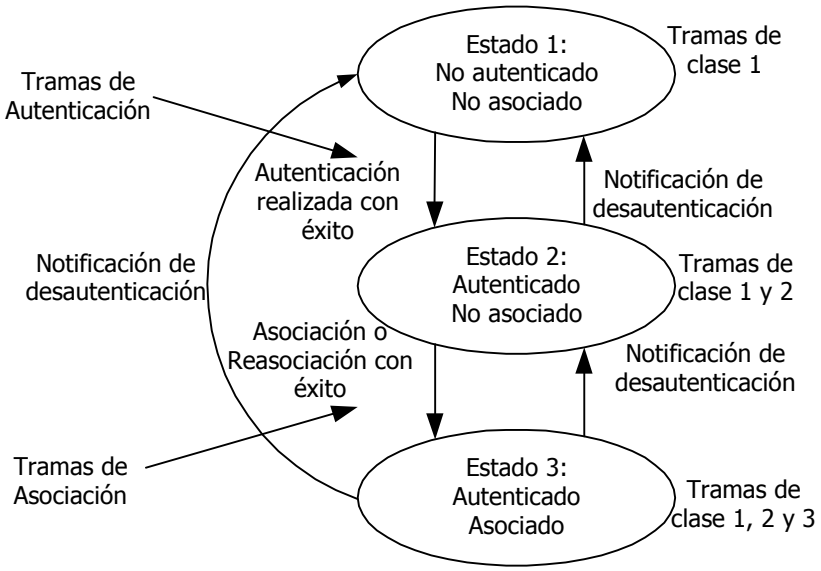


Figura 1-3 Pasos para asociarse a un PA

1.6 - Estándares para las redes WLAN

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso de la IEEE (*Institute of Electrical and Electronics Engineers*) [1], ETSI (*European Telecommunications Standards Institute*) [4], IETF (*Internet Engineering Task Force*) [5] y la *WI-FI Alliance (Wireless Fidelity Alliance*) [3]. Los tres primeros son grupos consagrados en el desarrollo de estándares y el último es la unión de un grupo de empresas interesadas en el desarrollo de la tecnología inalámbrica y la interoperatividad de los productos de diferentes empresas.

Estas normativas específicas definen de forma detallada los protocolos de la capa física y la capa de control de acceso al medio (MAC). Una vez desarrollados se convierten en la base de los fabricantes para desarrollar sus productos.

El comité IEEE 802.11 [1] es el encargado de desarrollar los estándares para las redes de área local inalámbricas.

El estándar IEEE 802.11 [1], se basa en el mismo marco de estándares que *Ethernet*. Esto garantiza un excelente nivel de interoperatividad y asegura una implantación sencilla de las funciones y dispositivos de interconexión *Ethernet* / WLAN. La especificación 802.11[1] original incluye características de seguridad muy elementales e insuficientes.

A finales del año 2000 y durante el 2001 se encuentran múltiples vulnerabilidades en las especificaciones de seguridad del estándar 802.11 [1]. Se crea el grupo de trabajo sobre seguridad 802.11i [2] para definir un nuevo marco de seguridad. Los fabricantes ofrecen soluciones (algunas propietarias y otras basadas en tecnologías bien conocidas) para solucionar los problemas de seguridad.

A finales del 2002, *Wi-Fi* [3] pretende unificar las soluciones de los fabricantes creando un «pre-estándar» compuesto por un subconjunto de las especificaciones en las que trabaja el proyecto 802.11i [2], a esta especificación (no estandarizada) la denomina *Wi-Fi Protected Access (WPA)*, en abril del 2003 aparecen los primeros productos certificados WPA.

El proyecto 802.11i [2] trabajó en el estándar llamado «*Robust Security Network* (RSN)», también denominado WPA2, que salió al mercado en el 2004.

Entre los principales estándares de IEEE 802.11 [1] se encuentran:

- **802.11 –** Fue el primer estándar disponible y permite dos variantes para el interfaz de aire: DS-SS (*Direct Sequence Spectrum*) y FH-SS (*Frequency Hopped Spread Spectrum*). Soporta de 1 a 2 Mbps (según fabricante).

- **802.11a** – Es una evolución del 802.11b, opera en una banda de 5 GHz. En la interfaz de aire utiliza multiplexación OFDM (*Orthogonal Frequency Division Multiplexing*). Soporta hasta 54 Mbps.

- **802.11b** – Es el estándar que lideró los primeros desarrollos masivos de WLAN. Emplea solamente DS-SS y utiliza modulación con forma de onda CCK (*Complimentary Code Keying*). Trabaja en la banda de 2.4 GHz. Soporta 11 Mbps.

- **802.11e** - Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio. Diseñado para el soporte multimedia mejorado,

garantizando la calidad de servicio (*QoS*) en comunicaciones de gran ancho banda y tiempo real.

- **802.11f** - Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.

- **802.11g** - Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps. OFDM: *Ortogonal Frequency Division Multiplexing*. Aprobado en 2003 para dar mayor velocidad con cierto grado de compatibilidad a equipamiento 802.11b.

- **802.11h** – Es una evolución del 802.11a que permite asignación dinámica de canales y control automático de potencia para minimizar los efectos inherentes. Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico. DFS: *Dynamic Frequency Selection*, habilita una cierta coexistencia con *HiperLAN* [4] y regula también la potencia de difusión.

- **802.11i** - Está dirigido a combatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X[6], TKIP (*Temporal Key Integrity Protocol*), y AES (*Advanced Encryption Standards*).

- **802.11j** - Permitiría armonización entre IEEE (802.11)[1], ETSI (*HiperLAN2*)[4], y ARIB (*HISWANa*)[4].

- **802.11m -** Mantenimiento redes wireless.

- **802.11n -** Diseñado para aumentar la capacidad efectiva de transmisión hasta 100 Mbps, siendo compatible con los estándares anteriores. La finalización del estándar esta prevista para finales del 2005.

- **802.1x** - Es el estándar de control de acceso a la red basados en puertos. En este estándar esta incluido el estándar EAP[6].

- **802.16 –** Es el estándar para las redes WiMax.

A continuación se muestra en la Tabla 1-1, las características principales de los estándares IEEE 802.11 [1].

Estándar	IEEE 802.11	IEEE 802.11b	IEEE 802.11g	IEEE 802.11a	IEEE 802.11h	IEEE 802.11n
Finalización	1997	1999	2003	2002	2003	2005
Frecuencia	2,4 Ghz ISM	2,4 Ghz ISM	2,4 Ghz ISM	5 Ghz	5 Ghz	2,4/5 Ghz
Velocidad	2 Mbps	11 Mbps	11/54 Mbps	54 Mbps	54 Mbps	100 Mbps
Interfaz aire	SS-FH/ SS-DS	SS-DS	SS-FH/ OFDM	OFDM	OFDM	OFDM
Otros aspectos	Superado por IEEE 802.11b	Disponible en el mercado	Disponible en el mercado	Disponible en el mercado	DCS *Power* control	Compatibilidad hacia atrás

Tabla 1-1 Comparativa de los estándares WLAN

1.6.1 - IEEE 802.11

El estándar IEEE 802.11[1] cubre las capas 1 y 2 del modelo OSI (*Open System Interconnection*).

La capa física de los estándares IEEE 802.11[1], se diseñó para cumplir con la regulación de radio frecuencia del FCC (*Federal Communications Commission*)[8]. Las mismas bandas de frecuencia, con algunas variantes, se utilizan en el resto del mundo.

Con respecto a la capa MAC (Control de Acceso al Medio), podemos mencionar que los estándares IEEE 802.11[1] utilizan dos posibles mecanismos de acceso:

- **CSMA/CA** (*Carrier Sense Multiple Access/ Collision Avoindance*) cada estación escucha a otros usuarios (*Carrier Sense*) y si el canal esta sin usar la estación está autorizada a transmitir (*Collision Avoidance*). Pero si está ocupada, cada estación espera hasta que la transmisión presente finalice, y después entra en un procedimiento de *random back*. Esto previene que múltiples estaciones intenten obtener el medio inmediatamente después de completarse la transmisión precedente. El proceso de transmisión es el siguiente, si el medio ha estado libre

durante un intervalo de tiempo (DIFS) entonces se transmite el paquete de datos. Una vez recibido, el receptor enviará una confirmación de recepción (ACK).

Si el transmisor ha encontrado el medio ocupado, espera a que se acabe la transmisión actual y, cuando vuelva a intentar transmitir tendrá que esperar el tiempo DIFS, más un tiempo de contención (*back-off*) seudo-aleatorio.

- **RTS/CTS** (*Request To Send/Clear To Send*), es un procedimiento opcional en el que el terminal que quiera transmitir tiene que enviar al PA una solicitud de envío (*Request To Send*) a la que el PA accede (*Clear To Send*) a la transmisión. De esta manera se soluciona el problema del "nodo oculto" en el que dos transmisores separados no detectan las transmisiones de terminales distantes y los paquetes llegan degradados al PA. En este caso el punto de acceso coordina el tráfico WLAN al ser el encargado de dar los permisos de transmisión.

Además de las especificaciones de las capas MAC y física, también se definen los formatos de los *frames* (*Data, Control, Management*), autenticación (*Open / Shared*) y privacidad (WEP).

1.6.1.1- Mecanismos de autenticación

IEEE 802.11 establece dos formas de autenticación:

Abierta (*Open System*)

El método de autenticación *Open System* es equivalente a no tener autenticación esta definido para las WLAN en topologías *ad-hoc*. Es otro mecanismo de autenticación definido por el estándar 802.11[1] para autenticar todas las peticiones que recibe. El principal problema, es que no realiza ninguna comprobación de la estación cliente, además, las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable.

En un *Open System*, cualquier cliente terminal puede solicitar la autenticación y el terminal que recibe esta solicitud puede otorgar la autenticación a las estaciones que se encuentran en su lista de usuarios definidos.

A primera vista, este método no parece tener ningún sentido, pero originalmente fue diseñado para obtener conectividad de forma rápida y para ser implementado en dispositivos portátiles como lectores de código de barra y *handhelds*. En estos dispositivos no se contaba con poder de procesamiento como para implementar algoritmos de autenticación fuerte.

El proceso de autenticación consta de dos transacciones (Ver Figura 1-4):

1. El Cliente envía un pedido de autenticación

2. El PA responde el pedido de autenticación.

Si la respuesta es satisfactoria, las dos estaciones están mutuamente autenticadas.

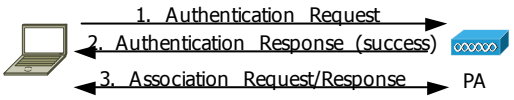


Figura 1-4 Proceso de autenticación *Open System*

Clave compartida (*Shared Key*)

Es un mecanismo de autenticación para las WLAN en topologías *ad-hoc*. El método de autenticación *Shared Key* utiliza un mecanismo de *challenge* y *encrypted challenge*, que sólo se puede configurar si el cifrado WEP está activo, y las claves WEP están correctamente configuradas.

En un sistema *Shared Key*, solamente las estaciones que comparten una clave secreta pueden ser autenticadas.

El proceso de autenticación consta de cuatro transacciones (Ver Figura 1-5):

1. El cliente envía un pedido de autenticación indicando *Shared Key*.

2. El PA responde el pedido de autenticación con un mensaje de texto.

3. El Cliente cifra el mensaje con la clave WEP que tiene configurada.

4. Si el PA puede descifrar el mensaje, con su clave WEP y coincide con el que envió originalmente, entonces responde dando acceso al cliente.

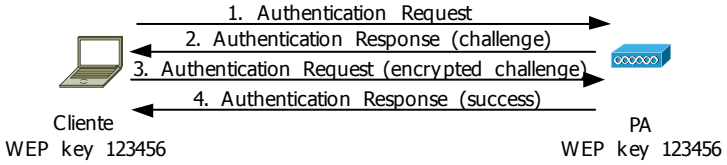


Figura 1-5 Proceso de autenticación *Shared System*

1.6.1.2- Encriptación y cifrado: WEP

WEP (*Wired Equivalent Privacy*) fue el primer protocolo de encriptación introducido en el primer estándar IEEE 802.11[1] en 1999. Es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11 [1]. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El algoritmo de encriptación utilizado es RC4 con claves, según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. El IV, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Se puede observar que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de WEP cifra de la siguiente manera (Ver Figura 1-6):

- A la trama se le computa un código de integridad (*Integrity Check Value*, ICV), mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

- Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.

- Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.

- La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo-aletorios. El generador RC4 es capaz de generar una secuencia seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.

- El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más de 32 bits (para cubrir la longitud de la trama y el ICV).

- Se hace un XOR *bit* por *bit* de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.

- El IV y la trama se transmiten juntos.

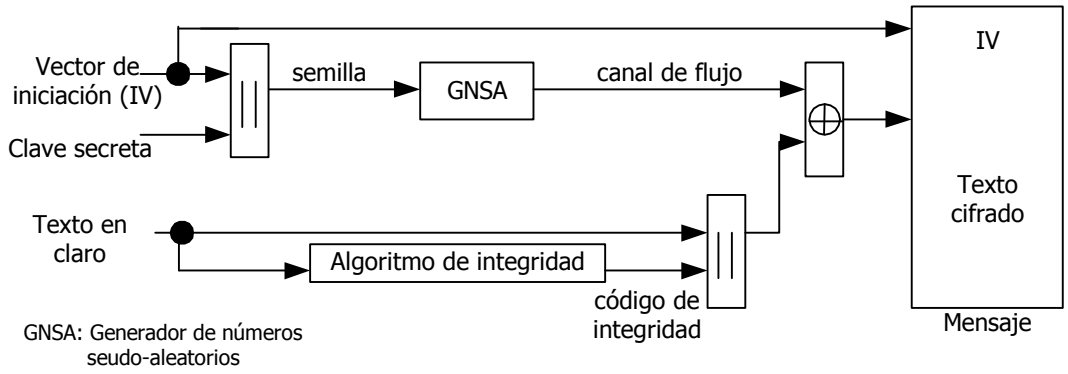


Figura 1-6 Funcionamiento del algoritmo WEP en modalidad de cifrado

En el receptor se lleva a cabo el proceso de descifrado (Ver Figura 1-7):

- Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.
- Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.
- Se efectúa un XOR *bit* por *bit* de la cifra de flujo y la trama cifrada, obteniéndose de esta manera la trama en claro y el ICV.
- A la trama se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.
- Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

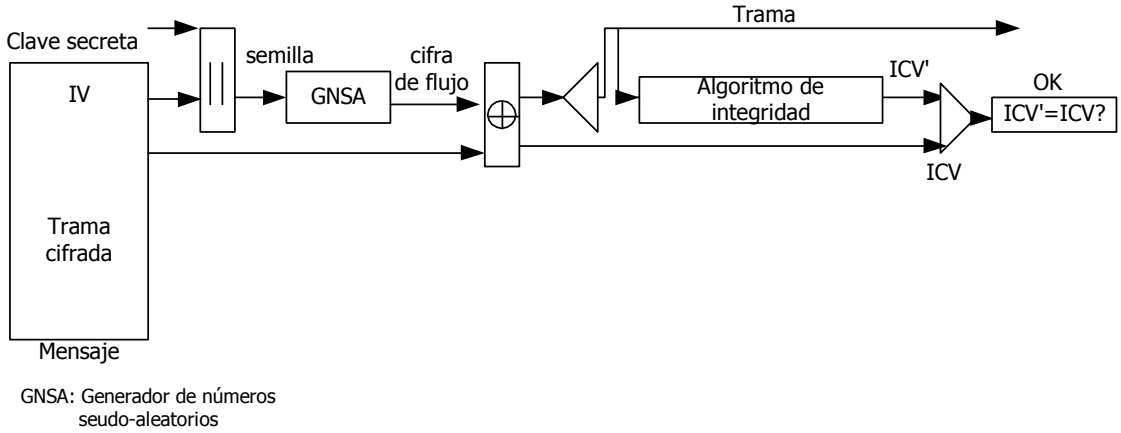


Figura 1-7 Funcionamiento del algoritmo WEP en modalidad de descifrado

El Vector de Inicialización (IV)

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que el IV es la parte que varía de la clave para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

Sin embargo, el estándar 802.11[1] no especifica cómo manejar el IV. Según se indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello. Queda abierta a los fabricantes la cuestión de cómo variar el IV en sus productos. La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama. Y esto ocasiona que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Más aún si tenemos en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

Por otro lado, el número de IVs diferentes no es demasiado elevado (2^24=16 millones aprox.), por lo que terminarán repitiéndose en cuestión de minutos u horas. El tiempo será menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se repitiese nunca, pero como vemos, esto es imposible en WEP. La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etc.) y de la carga de la red. Observemos que es trivial saber si dos

tramas han sido cifradas con la misma clave, puesto que el IV se envía sin cifrar y la clave secreta es estática.

La longitud de 24 *bits* para el IV forma parte del estándar y no puede cambiarse. Bien es cierto que existen implementaciones con claves de 128 *bits* (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 *bits*) pero el IV se conserva con 24 *bits*. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

¿Qué podemos hacer una vez hemos capturado varias tramas con igual IV, es decir, con igual *keystream*? Necesitamos conocer el mensaje sin cifrar de una de ellas. Haciendo el XOR entre un mensaje sin cifrar y el mismo cifrado, nos dará el *keystream* para ese IV. Conociendo el *keystream* asociado a un IV, podremos descifrar todas las tramas que usen el mismo IV. El problema es entonces conocer un mensaje sin cifrar, aunque esto no es tan complicado, porque existen tráficos predecibles o bien, podemos provocarlos nosotros (mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc.).

Con lo que hemos descrito no podemos deducir la clave secreta, aunque sí es posible generar una tabla con los IVs de los que sabemos su *keystream*, la cual permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla.

Sin embargo, podemos llegar a más y deducir la clave secreta. Una nueva vulnerabilidad del protocolo WEP permite deducir la clave total conociendo parte de la clave (justamente, el IV que es conocido). Para ello necesitamos recopilar suficientes IVs y sus *keystreams* asociados obtenidos por el procedimiento anterior.

1.6.1.3- Vulnerabilidades de WEP

WEP también adolece de otros problemas, además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4.

Entre los objetivos de WEP, como comentamos anteriormente, se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, por ejemplo, modificar algún número de la trama sin que

el destino se percatara de ello. En lugar del algoritmo de CRC se recomienda como ICV (*Integrity Check Value*) un algoritmo diseñado para tal fin como SHA1-HMAC [10].

El estándar IEEE 802.11 [1] incluye un mecanismo de autentificación de las estaciones basado en un secreto compartido. Para ello se utiliza la misma contraseña de WEP en la forma que describimos a continuación. Una estación que quiere unirse a una red, solicita al punto de acceso autentificación. El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió.

El mecanismo anterior de autentificación de secreto compartido tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad). El estándar es consciente de esta debilidad y aconseja no utilizar el mismo IV para el resto de transmisiones. Sin embargo, tanto si las implementaciones repiten ese IV como sino, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización explicadas anteriormente

WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autentificación es tan débil que la mejor opción es no utilizarlo sino es necesario para no ofrecer información extra a un posible atacante. En este caso tendríamos una autentificación de sistema abierto, es decir, sin autentificación.

Entre la larga lista de problemas de seguridad de WEP se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (*replay*). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica.

1.6.2 - WPA (*Wi-Fi Protected Access*)

WPA (*Wi-Fi Protected Access*), estándar desarrollado por la *Wi-Fi alliance* (WECA) [3], que trata de ser el sustituto de WEP. *Wi-Fi* [3] decidió, en colaboración con el IEEE[1], tomar aquellas partes del futuro estándar que ya estaba suficientemente maduras y publicar así WPA. WPA es, por tanto, un subconjunto de lo que seria IEEE 802.11i [2]. WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i [2]. Se mejora la protección de datos y control de acceso, pudiendo decirse que el nivel de protección es alto ya que mejora el cifrado de datos mediante TKIP (*Temporal Key Integrity Protocol*) con claves de sesión dinámica por usuario, sesión y paquete, pero es necesario acceder a través de un servidor de autentificación y que asegura la confidencialidad de datos. Y por otro lado, WPA también ofrece la autentificación de los usuarios mediante el estándar 802.11x y EAP (*Extensible Aunthentication Protocol*) [6], que permite controlar a todos y cada uno de los usuarios que se conectan a la red, aunque también permite, si se quiere, el acceso al usuario anónimo.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

1.6.2.1- Mecanismos de autenticación

PSK (Pre-Shared Key)

Este modo está orientado para usuarios domésticos o pequeñas redes. WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

EAP (Extensible Authentication Protocol)

EAP, definido en la RFC 2284 [6], es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad.

Como se muestra en la Figura 1-8, la autenticación del cliente se lleva a cabo mediante el protocolo EAP[6], y el servidor RADIUS, de la siguiente manera:

- El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso de ser cableada) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL (*EAP over LAN*), que es el requerido para efectuar la autenticación.

- La estación de trabajo envía un mensaje *EAPOL-Start* al autenticador, indicando que desea iniciar el proceso de autenticación.

- El autenticador solicita a la estación que se identifique, mediante un mensaje *EAP-Request/Identity*.

- Una vez recibida la información de identidad, el autenticador envía un mensaje *RADIUS-Access-Request* al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.

- El servidor de autenticación responde con un mensaje *RADIUS-Access-Challenge*, en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje *EAP-Request*.

- El cliente da respuesta al desafío mediante un mensaje *EAP-Response (Credentials)* dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje *RADIUS-Access-Response*.

- Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje *RADIUS-Access-Accept*, que autoriza al autenticador a

otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.

- El autenticador envía un mensaje *EAP-Success* al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS. En el caso del acceso inalámbrico, el servidor RADIUS despacha en el mensaje *RADIUS-Access-Accept* un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el punto de acceso. El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente (por ejemplo, cada cinco minutos), para evitar el ataque de rompimiento de la clave descrito en la sección referente a WEP. Ver Figura 1-8

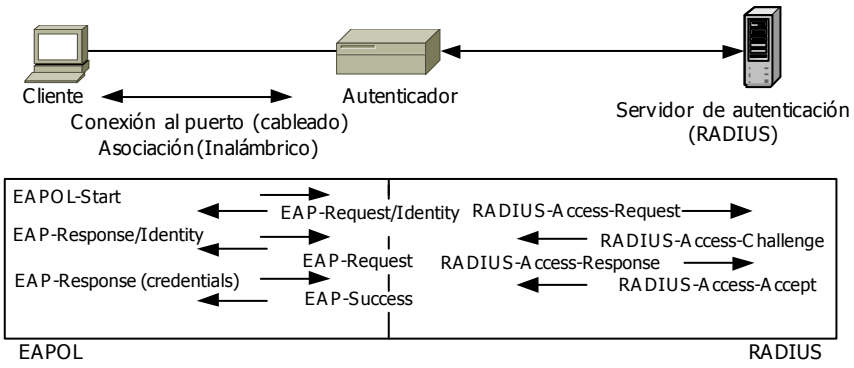


Figura 1-8 Diálogo EAPOL-RADIUS

Existen variantes del protocolo EAP[6], según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

Las variantes de EAP[6] que emplean certificados de seguridad son las siguientes:

- **EAP-TLS (*Extensible Authentication Protocol with Transport Layer Security)*:** Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (*Transparent Layer Substrate*)[11].

Los usuarios y el servidor de autenticación deben tener un certificado digital. El solicitante, tras la asociación y la creación del puerto de acceso por el autenticador, envía su identificación (nombre de usuario) hacia el autenticador y éste hacia el servidor de autenticación. Este último envía su certificado al cliente, al validarlo el cliente responde con su certificado. El servidor de autenticación comprueba si el certificado es válido y corresponde con el nombre de usuario antes enviado, si es así autentica al cliente. Cliente y servidor generan la clave de cifrado para esa sesión, y el servidor de autenticación la envía al punto de acceso, de forma que ya puede comunicarse el cliente de forma segura.

EAP-TLS exige que todos los clientes dispongan de un certificado digital lo que puede ser, en muchos casos, un inconveniente técnico y económico. Para evitar esta necesidad aparecen dos métodos: *Protected EAP* (PEAP) y *EAP-Tunneled* TLS (EAP-TTLS), que requieren únicamente del certificado en el servidor de autenticación.

- **EAP-TTLS (*EAP with Tunneled Transport Layer Security*):** Desarrollada por *Funk Software* y *Certicom*. Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor. Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establezca la sesión TLS[11], utilizando otro método tal como PAP[12], CHAP[13], MS-CHAP[15] o MS-CHAP v2[14]. También se basa en crear en primer lugar un túnel TLS pero los mensajes que intercambia son pares valor-atributo *(«attribute-value pairs»-AVPs*) muy similares a los que utiliza RADIUS.

- **PEAP (*Protected Extensible Authentication Protocol*):** Desarrollado por *Microsoft*, Cisco y RSA *Security*. Funciona de manera parecida a EAP-TTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador. Cuando el cliente ha validado el certificado del servidor de autenticación y creado el túnel, usando TLS se inicia una nueva autenticación donde negocian un método, por ejemplo MS-

CHAP v2[14], tras autentificar el servidor al cliente, ambos generan la clave de sesión.

El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas:

- La administración de los certificados de seguridad puede ser costosa y complicada, especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor. Es necesario comprar los certificados a una autoridad de certificación (CA) conocida, o montar una CA propia.

- El diálogo de autenticación es largo. Esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para los usuarios que tienen que reautenticarse con mucha frecuencia (por ejemplo, usuarios en movimiento que cambien de un punto de acceso a otro).

- La manipulación del certificado puede ser engorrosa para el usuario. En muchos casos se elige instalar el certificado en la terminal del usuario, con lo cual, si la terminal es robada y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo. Otra solución sería llevar el certificado en una tarjeta inteligente (*smart card*), lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas.

Las variantes de EAP que utilizan contraseñas son las siguientes:

- **EAP-MD5:** Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5[16]. Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5[16] hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente). Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está

conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.

- **LEAP (*Lightweigh EAP*):** Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.

- **EAP-SPEKE *(EAP with Simple Password-authenticated Exponential Key Exchange):*** Esta variante emplea el método SPEKE (*Simple Password-authenticated Exponential Key Exchange*), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso, una contraseña) a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servidor de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

En la Tabla 1-2, se resumen las características citadas anteriormente de EAP.

	EAP-MD5	LEAP	EAP-TLS	EAP-TLS	PEAP
Autenticación de servidor	Ninguna	Hash de la clave	Certificado digital	Certificado digital	Certificado digital
Autenticación de suplicante	Hash de la clave	Hash de la clave	Certificado digital	CHAP, PAP, MSCHAPv2, EAP	Cualquier EAP, tal como EAPMS-CHAPv2
Creación dinámica de claves	Si	No	No	No	No
Riesgos de seguridad	Identidad expuesta, ataques de diccionario, ataques de hombre en el medio, secuestro de sesiones	Identidad expuesta, ataques de diccionario, ataques de hombre en el medio	Identidad expuesta	Ataques de diccionario, ataques de hombre en el medio	Ataques de diccionario, ataques de hombre en el medio
Estándar abierto	Si, pero obsoleto ya por problemas de seguridad	No, método propietario	Si	Draft	Draft

Tabla 1-2 Comparativas de EAP

IEEE 802.1X

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red, es un estándar de control de acceso a nivel de acceso al medio (nivel 2), con lo que a diferencia de otros sistemas, el cliente no tiene una conexión efectiva con acceso al medio hasta que no se haya autenticado satisfactoriamente.

El protocolo fue inicialmente creado por la IEEE[1] para uso en redes de área local cableadas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x[6].

El protocolo 802.1x[6] involucra tres participantes (Ver Figura 1-9):

- El equipo cliente que desea conectarse con la red.

- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x[6] fue diseñado para emplear servidores RADIUS (*Remote Authenticatioin Dial-In User Service*), cuya especificación se puede consultar en la RFC 2058 [17]. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las redes LAN.

- El autenticador, que es el equipo de red (*switch*, enrutador, servido de acceso remoto entre otros) que recibe la conexión del cliente. El autenticador actúa como intermediario entre el cliente y el servidor de autenticación, y solamente permite el acceso del cliente a la red cuando el servidor de autenticación así lo autoriza.

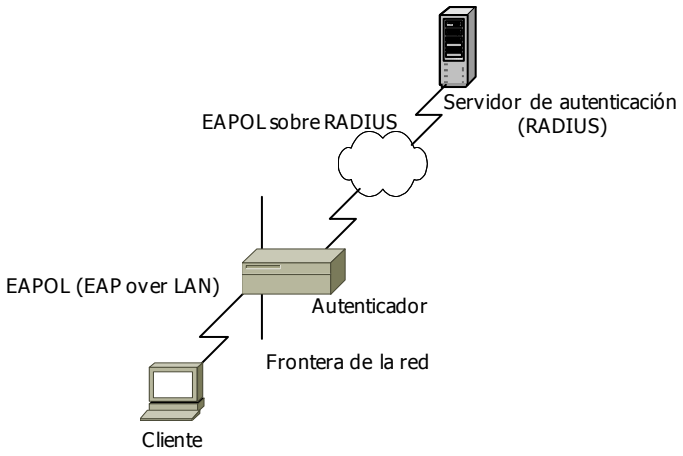


Figura 1-9 Arquitectura de un sistema de autenticación 802.1x

En IEEE 802.1x[6] se introduce un nuevo concepto, de puertos habilitado/inhabilitado, en el cual hasta que un cliente no se valide en el servidor no tiene acceso a los servicios ofrecidos por la red.

En sistemas 802.1x[6] activado, se generan dos llaves, la llave de sesión (*pairwise key*) y la llave de grupo (*groupwise key*). Las llaves de grupo se comparten por todas las estaciones clientes conectadas a un mismo punto de acceso y se utilizarán para el tráfico *multicast*, las llaves de sesión serán únicas para cada asociación entre el cliente y el punto de acceso y se creará un puerto privado virtual entre los dos.

IEEE 802.1x[6] mejora la seguridad proporcionando las siguientes mejoras sobre WEP:

- Modelo de seguridad con administración centralizada.
- La llave de encriptación principal es única para cada estación, por lo tanto, el tráfico de esta llave es reducido (no se repite en otros clientes).
- Existe una generación dinámica de llaves por parte del servidor de autenticación, sin necesidad de administrarlo manualmente.
- Se aplica una autenticación fuerte en la capa superior.

1.6.2.2- Encriptación y cifrado: TKIP/MIC

Según indica *Wi-Fi* [3], es el protocolo encargado de la generación de la clave para cada trama. *Temporal Key Integrity Protocol* (TKIP) amplía y mejora a WEP, solucionando sus vulnerabilidades. TKIP amplía la longitud de la clave de 40 a 128 bits y pasa de ser única y estática a ser generada de forma dinámica, para cada usuario, para cada sesión (teniendo una duración limitada) y por cada paquete enviado.

Este esquema de encriptación surge como alternativa al WEP intentando solucionar sus problemas de seguridad. Uno de los requisitos principales de este nuevo esquema era que pudiera funcionar en el mismo hardware que el antiguo WEP, con una simple actualización del *firmware*. TKIP también utiliza un algoritmo de encriptación RC4, lo que implica nuevamente clave simétrica compartida entre el cliente y la estación base. En este caso las claves utilizadas (llamadas *Temporal Key*) son de 128 bits, que son actualizables cada cierto número de paquetes, y el vector de inicialización es de 48 bits, el cual es reiniciado a 0 cada vez que se fija una nueva clave temporal. Para la encriptación se pueden utilizar unas claves derivadas de la TK, llamadas PPK (*Per-Packet Key*) que son generadas de manera dinámica por cada paquete enviado.

Conceptualmente el vector de inicialización pasa de 24 a 48 bits, minimizando la reutilización de claves. También utiliza claves para tráfico de difusión y multidifusión. TKIP utiliza el algoritmo «*Michael*» para garantizar la integridad, generando un bloque de 4 *bytes* (denominado MIC) a partir de la dirección MAC de origen, de destino y de los datos, añadiendo el MIC calculado a la unidad de datos a enviar. Posteriormente los datos (que

incluyen el MIC) se fragmentan y se les asigna un número de secuencia. La mezcla del número de secuencia con la clave temporal genera la clave que se utilizará para el cifrado de cada fragmento.

El protocolo TKIP está compuesto por los siguientes elementos:

- Un código de integración de mensajes (MIC), encripta el *checksum* incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11. Esta medida protege contra los ataque por falsificación.

- Medidas fuertes para reducir la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.

- Utilización de un IV de 48 bits llamado TSC (TKIP *Sequence Counter*) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden. La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación. Pueden intercambiarse 2^48 paquetes utilizando una sola llave temporal antes de ser reusada.

La estructura de encriptación TKIP propuesta por 802.11i[2] sería la siguiente: (Ver Figura 1-10)

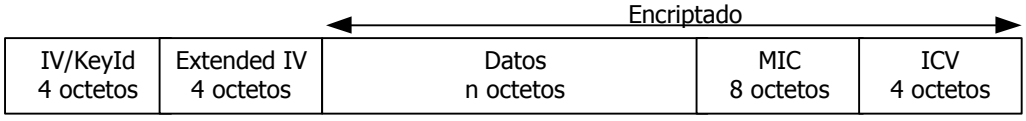


Figura 1-10 Estructura de encriptación TKIP

En el proceso de encriptación de TKIP (Ver Figura 1-11) se combinan dos fases la llave temporal, la dirección del emisor y el TSC para la obtención de una llave de 128 bits por paquete, dividido en una llave RC4 de 104 bits y en un IV de 24 bits para su posterior encapsulación WEP.

El MIC final se calcula sobre la dirección física origen y destino y el MSDU (MAC *Service Data Unit* o texto plano de los datos en la trama 802.11) después de ser segmentado por la llave MIC y el TSC.

La función MIC utiliza una función *hash* unidireccional, si es necesario, el MSDU se fragmenta incrementando el TSC para cada fragmento antes de la encriptación WEP.

En la desencriptación se examina el TSC para asegurar que el paquete recibido tiene el valor TSC mayor que el anterior. Sino, el paquete se descartará para prevenir posibles ataques por repetición. Después de que el valor del MIC sea calculado basado en el MSDU recibido y desencriptado, el valor calculado del MIC se compara con el valor recibido.

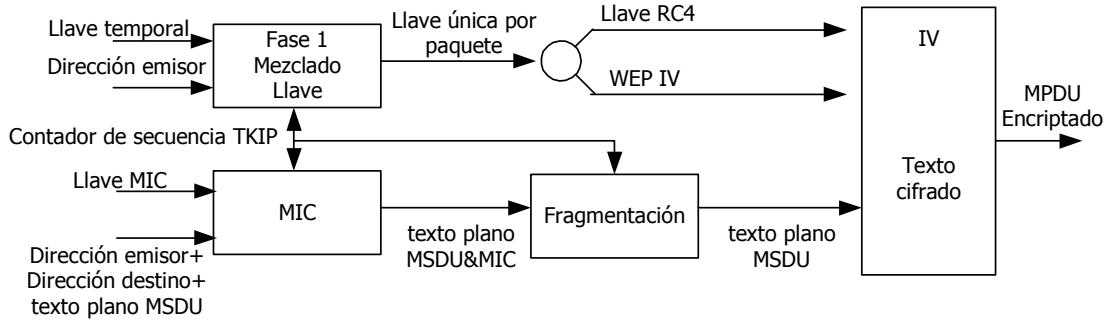


Figura 1-11 Proceso de encriptación WEP

1.6.2.3- Ventajas de WPA

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2^48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

1.6.2.4- Vulnerabilidades de WPA

- El sistema utilizado por WPA para el intercambio de la información para la generación de las claves de cifrado es muy débil.

- Cuando las claves preestablecidas utilizadas en WPA utilizan palabras presentes en el diccionario y la longitud es inferior a los 20 caracteres, el atacante sólo necesitará interceptar el tráfico inicial de intercambio de claves, es decir, únicamente es necesario capturar el tráfico de intercambio de claves para poder realizar el ataque de diccionario.

1.6.3 - IEEE 802.11i (WPA2)

En enero de 2001, el grupo de trabajo *i task group* fue creado en IEEE [1] para mejorar la seguridad en la autenticación y la encriptación de datos. En abril de 2003, la *Wi-Fi Alliance* [3] ,realizó una recomendación para responder a las preocupaciones empresariales ante la seguridad inalámbrica. Sin embargo, eran conscientes de que los clientes no querrían cambiar sus equipos.

En junio de 2004, la edición final del estándar 802.11i[2] fue adoptada y recibió el nombre comercial WPA2 por parte de la alianza *Wi-Fi* [3]. El estándar IEEE 802.11i[2] introdujó 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 *wireless* se llama

Robust Security Network (RSN) y utiliza autenticación 802.1X[2], 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 1-12):

Acuerdo sobre la política de seguridad, autenticación 802.1x, derivación y distribución de las claves, confidencialidad e integridad de los datos RSNA.

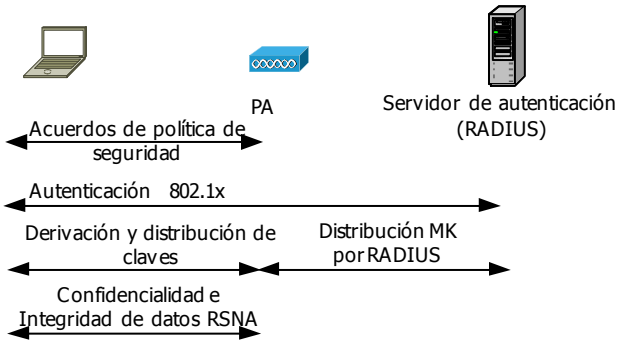


Figura 1-12 Fases operacionales de 802.11

WPA2 incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), desarrollado por el NIS [18]. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un *hardware* potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol*) en lugar de los códigos MIC.

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

1.6.3.1- Encriptación y cifrado: CCMP/AES

CCMP (*Counter Mode with CBC-MAC Protocol)*, es un protocolo complementario al TKIP y representa un nuevo método de encriptación basado en AES (*Advanced Encryption Standards*), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC[19]. En el caso de redes *Wi-Fi* este esquema se integra en el estándar WPA2, y utiliza claves de 128 bits, vector de inicialización de 48 bits y chequeo de integridad. Este esquema de encriptación hace necesario el cambio de hardware para su uso, por lo que no mantiene la compatibilidad con esquemas de anteriores, como ocurría con el TKIP.

En la Figura 1-13, podemos observar el formato de encriptación CCMP[19]:

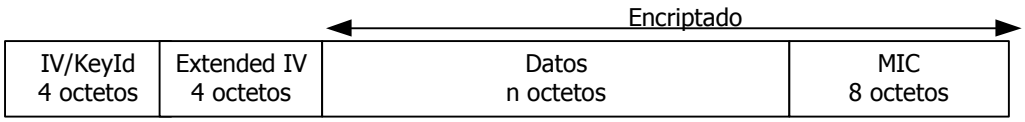


Figura 1-13 Estructura de encriptación CCMP

CCMP utiliza un IV de 48 bits denominado número de paquete (PN) utilizado a lo largo del proceso de cifrado, junto con la información para inicializar el cifrado AES para calcular el MIC y la encriptación de la trama.

En el proceso de encriptación CCMP, la encriptación de los bloques utiliza la misma llave temporal tanto para el cálculo del MIC como para la encriptación del paquete. Como en TKIP, la llave temporal se deriva de la llave principal obtenida como parte del intercambio en 802.1x[6]. Tanto el cálculo del MIC y la encriptación se realizan en forma paralela. El MIC se calcula a partir de un IV formado por el PN y datos extraídos de la cabecera de la trama. El IV se convierte en un bloque AES y su salida a través de la operación XOR conformará el siguiente bloque AES.

1.6.3.2- Vulnerabilidades de WPA2

Aunque se han descubierto algunas pequeñas debilidades en WPA/WPA2 desde su lanzamiento, ninguna de ellas es peligrosa si se siguen unas mínimas recomendaciones de seguridad. La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA/WPA2.

En la Tabla 1-3, podemos observar las características resaltantes de los estándares IEEE 802.11[1] y IEEE 802.11i[2], de acuerdo a su protocolo de encriptación/cifrado y mecanismos de autenticación.

Estándar	**IEEE 802.11**	**IEEE 802.11i**	
Protocolo de seguridad	WEP	WPA	WPA2
Encriptación y cifrado	Sistema de cifrado simétrico RC4 con clave estática	Encriptación: TKIP/MIC Sistema de cifrado simétrico RC4 con clave temporales	Encriptación: CCMP Cifrado AES
Integridad	Basada en CRC-32	Basadas en MIC	Basada en CCMP
Autenticación	Abierta Clave compartida	Redes grandes: IEEE 802.1x/EAP Redes pequeñas: PSK	IEEE 802.1x/EAP

Tabla 1-3 Resumen de IEEE 802.11 y IEEE 802.11i

1.7 - Ataques a WLAN

La seguridad WLAN abarca dos elementos: el acceso a la red y la protección de los datos (autenticación y encriptación, respectivamente). Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquellos instalados sin el conocimiento de los administradores de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).

Estos "hoyos" en la seguridad, pueden ser aprovechados por personal no autorizado (*hackers*), que en caso de que logren asociarse con el punto de acceso, ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la red inalámbrica a la cual se conecta.

Los puntos de acceso habitualmente ofrecen una configuración por defecto insegura, en la que están predefinidos los parámetros por defecto (SSID, canal, utilización de WEP). Generalmente no se suele habilitar WEP, y se usan SSID fijos y conocidos, predeterminados por el fabricante (Cisco, por ejemplo, utiliza la palabra "tsunami"). Además, muchos de ellos exponen sus interfaces de gestión a la red *wireless* (mediante web, snmp o telnet), permitiendo el acceso a cualquier usuario conectado a la red.

Los ataques se clasifican en, pasivos y activos. El ataque pasivo, es aquel en el cual el intruso monitorea el tráfico en la red (*eavesdropping*) para capturar contraseñas (*passwords)* u otra información para su uso posterior. En un ataque activo, el intruso interfiere con el tráfico legítimo que fluye a través de la red, interactuando de manera engañosa con el protocolo de comunicación.

Existen además ciertos ataques particulares en las redes *wireless*, que aprovechan algunas de las debilidades comentadas, y que pueden ser agrupados en varias categorías:

1.7.1 - Ataques al WEP

Los ataques al cifrado WEP pueden agruparse en:

Ataques pasivos, buscando ciertos paquetes específicos conteniendo "*weak IVs*". Requiere la captura de alrededor de cuatro millones de paquetes, lo que toma varias horas. Es un ataque totalmente pasivo e indetectable. Existen herramientas que implementan este ataque.

Ataques activos de modificación e inyección de paquetes, inyección de ARP, modificación de los IVC, *bit flipping*.

La finalidad de ambos tipos de ataques es obtener la clave WEP para acceder a la red.

Los ataques pasivos se llevan a cabo capturando tráfico cifrado de la red *wireless* y luego ejecutando una herramienta de *cracking* de WEP utilizando criptoanálisis (FMS) o por fuerza bruta. La cantidad necesaria para poder descubrir la clave WEP varía, no es una ciencia exacta, y dependerá del tipo de tráfico capturado. La herramienta *WEPCrack* fue la primera en implementar el ataque FMS, luego aparecieron otras como *AirSnort*. Las

herramientas *WepDecrypt* y *WepAttack* implementan ataques de fuerza bruta sobre un solo paquete capturado.

Los ataques activos se llevan a cabo capturando tráfico cifrado de la red *wireless* y reinyectándolo en la red para generar más tráfico y así obtener una gran cantidad de paquetes cifrados para luego ejecutar una herramienta de *cracking* de WEP. Para este tipo de ataques se utiliza la herramienta *Aireplay* de la *suite Aircrack*.

Un ataque activo al WEP es el ataque de fuerza bruta. La semilla de 32 bits que utiliza el PRNG es obtenida a partir de la *passphrase*. La *passphrase* normalmente contiene caracteres ASCII, por lo cual el *bit* más alto de cada carácter siempre es cero. El resultado de la operación XOR de estos *bits* también es cero y esto provoca una reducción de la entropía de la fuente, es decir, las semillas sólo podrán ir desde 00:00:00:00 hasta 7F:7F:7F:7F en lugar de hasta FF:FF:FF:FF.

El uso del PRNG con esta semilla también reduce la entropía. De la semilla de 32 *bits* sólo utilizan los *bits* del 16 al 23. El generador es un generador lineal congruente (LGC: *linear congruential generator*) de módulo 2^32, esto provoca que los *bits* mas bajos sean "menos aleatorios" que los altos, es decir, el *bit* 0 tiene una longitud de ciclo de 2^1, el *bit* 1 de 2^2, el *bit* 2 de 2^3, etc. La longitud de ciclo del resultado será por tanto 2^24. Con esta longitud de ciclo sólo las semillas que vayan de 00:00:00:00 a 00:FF:FF:FF producirán llaves únicas.

Como las semillas sólo llegan hasta 7F:7F:7F:7F y la última semilla que tiene en cuenta el PRNG es 00:FF:FF:FF, sólo necesitamos considerar las semillas desde 00:00:00:00 hasta 00:7F:7F:7F por lo que la entropía total queda reducida a 21 *bits*. El conocimiento de estos datos nos permite hacer ataques de fuerza bruta contra la encriptación WEP generando llaves de forma secuencial utilizando las semillas desde 00:00:00:00 hasta 00:7F:7F:7F. Utilizando este proceso, un procesador PIII a 500MHZ tardaría aproximadamente 210 días en encontrar la llave, aunque se puede usar computación en paralelo para obtener la llave en un tiempo más razonable.

También existe la posibilidad de utilizar un diccionario para generar sólo las semillas de las palabras (o frases) que aparezcan en el diccionario, con lo que si la *passphrase* utilizada

está en el diccionario se conseguirá reducir sustancialmente el tiempo necesario para encontrarla.

Además se tiene, el ataque inductivo *Arbaugh*. Se basa en explotar la vulnerabilidad de MIC independiente de la llave aprovechando también la redundancia de información producida por el CRC. Para realizar el ataque hay que conocer parte del texto plano que viaja encriptado en una trama, que se puede obtener por ejemplo identificando mensajes "*DHCPDISCOVER*" de los que se conoce que la cabecera IP tendrá como origen 0.0.0.0 y como destino 255.255.255.255 y tienen longitud fija. Una vez identificada la trama con el mensaje "*DHCPDISCOVER*" se realiza una XOR del texto plano conocido con el texto cifrado que hemos recibido, obteniendo así n (en este caso 24) *bytes* del *keystream* para el IV concreto del paquete.

Una vez que se tienen estos 24 *bytes* conocidos del *keystream* hay que generar un paquete de tamaño n-3, es decir 24-3 = 21 *bytes* de longitud. Este paquete debe ser algo de lo que podamos esperar una respuesta, por ejemplo un *ping* o un *ARP Request*.

Se calcula el ICV del paquete generado y se añade sólo los primeros 3 *bytes* del ICV que hemos calculado. Se realiza una XOR con el resto del *keystream* añadiendo el último *byte* del ICV en el *byte* n+1 (al final del paquete) tratando de adivinar el siguiente *byte* del *keystream.*

Una vez generado el paquete completo se envía y se espera una respuesta (*echo reply, ARP reply…*), si no hay respuesta se pueba las 255 posibilidades restantes modificando el último *byte* (n+1). Si hay respuesta se puede afirmar que el *byte* n+1 era el último *byte* del ICV, así que se tiene un texto plano que concuerda con el texto cifrado y que a su vez da el *byte* n+1 del *keystream* que es lo que interesa. Realizando este proceso repetidas veces obtendremos el *keystream* completo.

Asumiendo que un atacante puede realizar aproximadamente 100 pruebas por segundo, tardaría una media de 36 minutos en encontrar un *keystream* completo de 1500 *bytes* válido para un IV determinado.

Una vez que se tiene un *keystream* entero, los 2^24 – 1 restantes son fáciles de obtener: El atacante tiene que volver a generar un paquete del cual se le devuelva una respuesta,

(lo mejor es enviar *broadcast pings*, así recibimos múltiples respuestas por cada paquete que enviamos). El atacante conoce el texto plano de la respuesta y el que responde cada vez enviará el paquete con un IV diferente, así es posible construir una tabla de *keystreams* completos para cada IV que el atacante puede utilizar para descifrar el tráfico encriptado con WEP en tiempo real.

El atacante necesita almacenar 1500 *bytes* de *keystream* por cada IV, por lo que la tabla ocuparía 2^24 x1500 = 24GB y tardaría una media de 30 horas en construir la tabla. Si el ataque se realiza en paralelo 4 *hosts* atacantes tardarían 7,5 horas y 8 *hosts* atacantes 3.75 horas.

Cuando el atacante recibe un paquete mira en la tabla a que *keystream* corresponde el IV recibido y hace una XOR del *keystream* con el texto cifrado del paquete para obtener el texto plano.

1.7.2 - Ataques de escucha/monitorización pasiva (*eavesdropping*)

Las redes wireless son especialmente vulnerables a los ataques de monitorización, siendo el único requisito para su realización la conectividad, es decir, la posibilidad de acceso al flujo de datos.

El primer paso para obtener acceso a un sistema es conseguir una asociación con el mismo. En las redes que utilizan autenticación *Open System*, el proceso es transparente, aumentando su complejidad en los sistemas con autenticación *Shared Key*. En estos casos, la autenticación es posible tras la captura y *cracking* de cierto número de paquetes, existiendo diversas herramientas que facilitan dicha tarea. Por esto, es posible el acceso y monitorización del tráfico presente en el entorno como cualquier cliente autenticado.

También es posible realizar inyección y modificación de mensajes en este tipo de redes, sin necesidad de descifrar claves, SSID y demás.

La implementación práctica de los ataques escucha se conoce como *wardriving* (con su evolución de *drive-in hacking*), y consiste en localizar e identificar puntos de acceso a lo largo del territorio, cualquier ubicación puede ser rastreada. Adicionalmente, existen programas que pueden trabajar de forma conjunta con un receptor GPS, lo que permite

que pueda localizarse de manera muy precisa (latitud, longitud, datos adicionales como SSID) la ubicación de los distintos puntos de acceso.

1.7.3 - Ataques de intercepción/inserción (*main-in-the-middle*)

Los entornos que operan sobre redes *wireless* facilitan la captura y redirección de sesiones, ya que una estación que transmite no es capaz de detectar la presencia de estaciones adyacentes con la misma dirección MAC o IP.

El ataque de *Man in the middle*, también conocido como *Monkey in the middle* consiste en convencer al cliente (la victima) de que el *host* que hay en el medio (el atacante) es el punto de acceso, y hacer lo contrario con el punto de acceso, es decir, hacerle creer al punto de acceso que el atacante es el cliente.

Para realizar este ataque, primero debemos identificar el atacante y obtener:

- El SSID de la red (si esta ocultado, usaremos el método anterior)
- La dirección MAC del punto de acceso
- La dirección MAC de la victima

Una vez conocidos estos datos, utilizamos el mismo método que en el ataque *DoS*, para desautenticar a la victima del punto de acceso real, es decir, el atacante *spoofea* su MAC haciéndose pasar por el punto de acceso y manda tramas *deauth* a la victima. La tarjeta *wi-fi* de la victima empezará entonces a escanear canales en busca de un punto de acceso para poderse autenticar, y ahí es donde entra en juego el atacante.

El atacante hace creer a la victima que él es el punto de acceso real, utilizando la misma MAC y el mismo SSID que el punto de acceso al que la victima estaba autenticada anteriormente, pero operando por un canal distinto. Por otra parte, el atacante debe asociarse con el punto de acceso real, utilizando la dirección MAC de la victima.

De esta manera se ha conseguido insertar al atacante entre la victima y el punto de acceso.

Ahora todos los datos que viajan entre la victima y el punto de acceso pasan a través del atacante. Como el ataque es a nivel de capa de enlace (nivel 2), el atacante puede ver, capturar e incluso modificar las tramas en los niveles superiores del modelo OSI. Es muy fácil implementar este tipo de ataques utilizando el *driver air-jack* con la herramienta *monkey-jack*.

Hay que tener en cuenta que muchas soluciones de seguridad están pensadas asumiendo que las capas 1 y 2 son seguras, esto como se ha visto es incierto para las redes *wireless.*

1.7.4 - Ataques a la dirección MAC

Una de las medidas más comunes que se utilizan para securizar una red wireless es restringir las máquinas que podrán comunicarse con el punto de acceso haciendo filtrado por dirección MAC en éste. Para esto se suele crear una tabla en el punto de acceso que contiene todas las MACs de los clientes que están autorizados para conectar.

Aunque esto pueda parecer una medida de seguridad efectiva, no lo es, ya que es muy fácil cambiar la dirección MAC que aparece en los paquetes que un cliente envía, y hacerse pasar por uno de los equipos que si tienen acceso a la red.

Para llevar a cabo el ataque basta con buscar durante un momento el tráfico y fijarse en la MAC de cualquiera de los clientes, sólo hace falta que se ponga su misma MAC y ya se habra saltado la restricción. Esto es sencillo de implementar, por ejemplo en el sistema operativo Linux se puede realizar con el comando *ifconfig* dependiendo del tipo de tarjeta que tengamos. También existen otras utilidades para cambiar la MAC como por ejemplo *setmac*.

Hay que tener en cuenta que si hay dos máquinas en la red con la misma dirección MAC puede haber problemas, aunque generalmente en las redes *wireless* esto no suele ser un problema muy grave ya que el punto de acceso no puede distinguir que verdaderamente hay dos máquinas con la misma MAC. De todas formas, si se quiere "anular" a la máquina que han "robado" la dirección MAC. Para hacer esto, se debe implementar un ataque de denegación de servicio.

1.7.5 - Ataques Diccionario

Ataques buscando *hackear* una clave utilizando diccionarios de palabras, es decir, listas de palabras. Para combatirlo, lo mejor es utilizar claves que no contengan ninguna palabra común.

1.7.6 - Ataques de denegación de servicio (DoS - *jamming*).

Por las características propias del medio, es sencillo realizar ataques que afecten a la disponibilidad en los entornos *wireless*. Dichos ataques pueden ser abordados desde varios enfoques, siendo los más sencillos aquellos que utilizan un dispositivo de radiofrecuencia (RF) de alta potencia para generar interferencias, lo que prevendría que el usuario legítimo pudiera utilizar el servicio. Esto es consecuencia de la implementación de la capa MAC, que no transmitirá mientras detecte otra actividad de RF.

Para evitar las colisiones inherentes al protocolo CSMA/CD, se utiliza paquetes de reserva de bandas de tiempo (RST) a los que el punto de acceso contesta (CTS), obligando al resto de estaciones a no transmitir durante el intervalo definido en CST. Otro tipo factible de DoS, probado en entornos de laboratorio, es produce cuando una estación hostil envía mediante *spoofing* de forma ininterrumpida tramas CTS con los datos de origen (MAC e IP) del punto de acceso, y desemboca en una paralización gradual de las comunicaciones de la red.

1.7.7 - Ataque ARP *Poisoning*

El *ARP cache poisoning* es un ataque que sólo se puede llevar a cabo cuando el atacante está conectado a la misma LAN lógica que las victimas, limitando su efectividad a redes conectadas con *switches, hubs y bridges*, pero no *routers*. La mayoría de los puntos de acceso 802.11b actúan como *bridges* transparentes de capa 2, lo que permite que los paquetes ARP pasen de la red *wireless* hacia la LAN donde está conectado el punto de acceso y viceversa. Esto permite que se ejecuten ataques de *ARP cache poisoning* contra sistemas que están situados detrás del punto de acceso, como por ejemplo servidores conectados a un *switch* en una LAN a los que se pueda acceder a través de la WLAN.

1.7.8 - Ataques al SSID oculto

Como se ha comentado anteriormente, para que un cliente y un punto de acceso se puedan comunicar, ambos deben tener configurado el mismo SSID, es decir, deben pertenecer a la misma red *wireless*.

Una medida de seguridad bastante común es "ocultar" el SSID, es decir, hacer que el PA no mande *beacon frames*, o en su defecto no incluya el SSID en éstos.

En este caso, para descubrir el SSID se debe esnifar y esperar a que un cliente se conecte, y se verá el SSID en la trama *prove request* del cliente (en el caso de que no se manden *beacon frames*), o en la trama *prove response* del punto de acceso.

Pero también se puede "provocar" la desconexión de un cliente, utilizando el mismo método que en el ataque DoS, pero mandando sólo una trama de desasociación o de desautenticación en lugar de mandarlas repetidamente, es decir, se pone la dirección física del punto de aceso y se manda una trama *deauth o disassoc* a la dirección MAC del cliente (o a la de *broadcast*), entonces el cliente intentará volver a asociarse o autenticarse, con lo que se puede ver el SSID en los *management frames*.

1.7.9 - Ataques *bit-flipping* (volcado de bits) y *replay* (repetición)

El uso de un MIC frustra los ataques activos a la red diseñados para determinar la clave de cifrado empleada para cifrar los paquetes interceptados. Este ataque activo es una combinación de los ataques *bit-flipping* (volcado de bits) y *replay* (repetición). Si se implementa el soporte de MIC tanto en el punto de acceso como en todos los dispositivos cliente asociados, el transmisor de un paquete añade algunos *bytes* (el MIC) ha dicho paquete antes de cifrarlo y transmitirlo. Al recibir el paquete, el destinatario lo descifra y comprueba el MIC. Si coincide con el valor calculado (derivado de la función MIC), el destinatario acepta el paquete; en caso contrario, lo descarta.

Con MIC se eliminan los paquetes que se han modificado de forma malintencionada durante su tránsito. Quienes realizan los ataques no pueden utilizar los ataques *bit-flipping* o *active replay* para engañar a la red para que los autentique.

CAPÍTULO 2 - MARCO METODOLOGICO

Teniendo en consideración los objetivos especificos de este trabajo de investigación, se estableció el plan de trabajo, definido por etapas las cuales se describen a continuación:

2.1 - Etapa de evaluación preliminar de la red inalámbrica

2.1.1 - Revisión de documentación y normas de seguridad existentes en la empresa que hacen referencia al uso y administración de la red inalámbrica.

Es importante destacar que no hay prácticas de seguridad establecidas actualmente, no existe información documentada del uso de la red WLAN, ni existen manuales que describan los procesos principales de éstas. A su vez, no se ha desarrollado un procedimiento de seguridad a seguir por la gerencia de Tecnología de Información, que sirva como base para la seguridad inalámbrica. Las medidas existentes, en cuanto a estos aspectos, son resultado de iniciativas independientes previamente autorizadas.

En la estructura de la gerencia de Tecnología de Información no existe ningún área orientada específicamente a desarrollar y mantener programas y políticas de seguridad de la información. Las responsabilidades en cuanto a la seguridad de la información se comparten entre las demás áreas organizacionales, situación que origina divergencias en la canalización y conducción de las decisiones a seguir en materia de seguridad.

Los estudios realizados en materia de seguridad de la información se han enfocado, principalmente a la protección y seguridad física y lógica (*router, switches, ect*) de los bienes en los cuales se procesa, almacena o transporta la información manejada por la empresa sin tomar en cuenta la red inalámbrica. Estos se han basado en la implementación de herramientas tecnológicas a nivel de la red, sin contar con un estudio claro y conciso de las políticas de seguridad necesarias para la empresa.

Actualmente existe el esfuerzo en la empresa en las áreas encargadas de la seguridad de la información, para establecer y documentar las directrices de protección necesarias para garantizar un óptimo uso de este servicio. Estas áreas, encargadas de salvaguardar la integridad, confiabilidad y disponibilidad de la información, establecieron y desarrollaron normas y procedimientos que sirven de base para regular aspectos de la conducta de los usuarios de la red corporativa, vinculados con el manejo de la información, pero sin llegar

a profundizar en los aspectos necesarios que haría un efectivo plan de seguridad. Entre las normas y procedimientos que actualmente existen en la gerencia de Tecnología de Información están los siguientes:

- POL-IT-1001-00: Declaración de política de Seguridad Informática
- DIR-IT-1002-00: Directiva del uso aceptable de recursos informáticos y de comunicaciones.
- NPG-IT-0004-00: Procedimiento para el control y mantenimiento de inventario físico.

2.1.2 - Levantamiento de información de *software* y *hardware* de la plataforma WLAN consultando las configuraciones de los equipos inalámbricos.

En función de conocer la estructura física y lógica de la red inalámbrica de YPergas a continuación se describen cada uno de sus componentes:

Hardware

- Puntos de Accesos

  Actualmente hay 3 puntos de accesos, *Cisco Aironet Acces Point* 350 series (AIR-AP350 series) en la localidad de Caracas ubicados uno en el piso 16 y otro en el piso 17, como se indica en la Figura 2-1 (ver página 67) y Figura 2-2 (ver página 67). Además, hay otro punto de acceso que estaba guardado y que se utilizará para este proyecto.

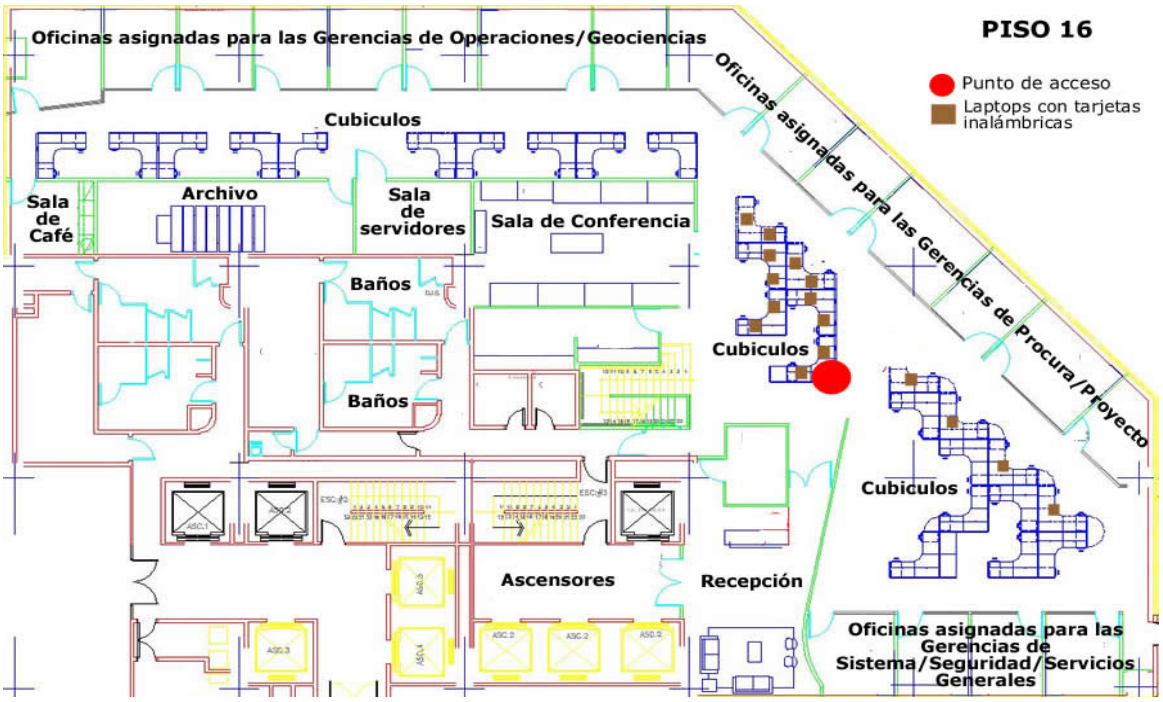


Figura 2-1 Ubicación física de PA - piso 16

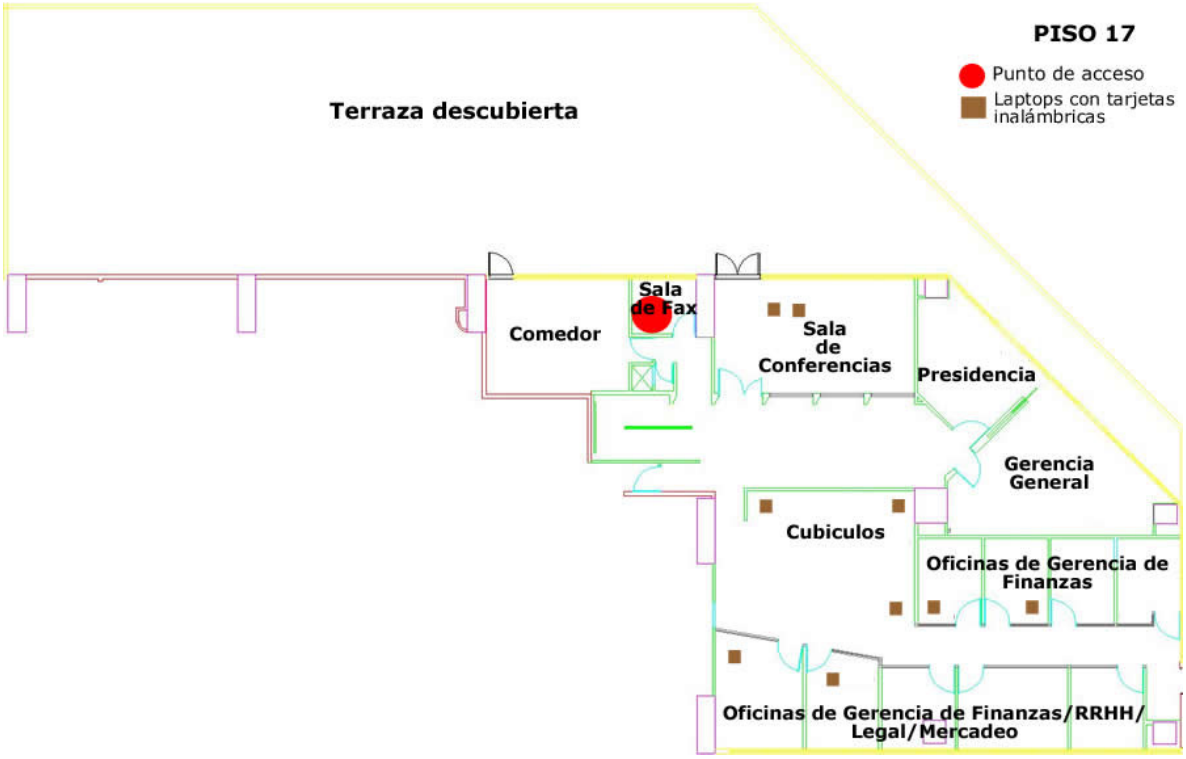


Figura 2-2 Ubicación física de PA - piso 17

- Tarjetas de accesos

  Actualmente se cuenta con 20 tarjetas de red, *Aironet AIR-PCI352* para *laptops* almacenadas y asignadas a los usuarios visitantes y personal temporal en Caracas, generalmente estas tarjetas sólo se utilizan en los equipos que no poseen tarjeta inalámbrica incorporada, como actualmente salen de fábrica.

Software

- El *software* instalado en los equipos *Cisco Aironet Acces Point* 350 series (AIR-AP350 series), es *Cisco 350 series* Ap con la versión de *VxWorks* 11.21 en un caso y en los otros casos *Cisco 350 series* AP con la versión de *VxWorks* 12.00T.

Las versiones de *VxWorks* que tienen los puntos de acceso *Cisco Aironet Acces Point* 350 series (AIR-AP350 series), están señaladas en Tabla 2-1, las mismas están desactualizadas con respecto a las nuevas versiones que existen en Internet para esos equipos. Cabe destacar, que los puntos de accesos están ubicados en la categoría *end-of-sale and end-of-life* [38] según las políticas de Cisco, esto significa que los productos ya han entrado en un ciclo en el cual, han salido del mercado por diversas causas, mucha demanda, innovación de tecnología y desarrollo del producto o simplemente los productos fueron reemplazados por otros con mayores y mejores funcionalidades.

Nro	Modelo	Versión de VxWorks
1	*Cisco Aironet Acces Point* 350 series (AIR-AP350 series	11.21
2	*Cisco Aironet Acces Point* 350 series (AIR-AP350 series	12.00T
3	*Cisco Aironet Acces Point* 350 series (AIR-AP350 series	12.00T

Tabla 2-1 Información de los puntos de accesos.

2.1.3 - Identificación de la topología física y lógica de los equipos inalámbricos, utilizando la documentación existente en la empresa y haciendo inspección visual de la red inalámbrica.

Como se indicó en el punto anterior 2.1.2 - los puntos de accesos se encuentran físicamente ubicados en los pisos 16 y 17 en la localidad de Caracas. Lógicamente están ubicados en una red plana, *fast ethernet* de 100Mbps y están conectados sobre la VLAN 1 que viene configurada por defecto en los equipos, sin establecer ninguna segmentación en los servicios de la red, en esta se encuentran todos los servidores, impresoras y estaciones de trabajo, como se muestra en la Figura 2-3.

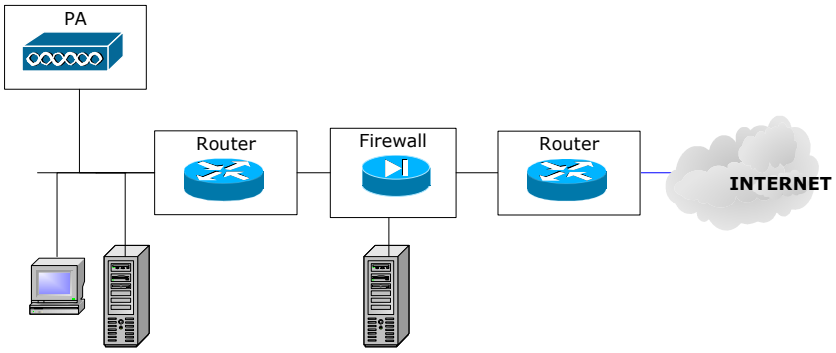


Figura 2-3 Diagrama lógico de la red inicial

Los puntos de accesos cumplen con el estándar 802.11b, ya que trabajan en la banda de 2.4 ghz y soportan 11 Mbps.

2.1.4 - Identificación del uso actual de las redes inalámbricas, realizando entrevista a personal técnico y usuarios de la empresa Ypergas.

La etapa está orientada a revisar el uso de la infraestructura actual. La técnica de recolección de información empleada, para recopilar los datos relacionados con los requerimientos fue la observación y las entrevistas.

Actualmente la plataforma WLAN se usa muy poco en la empresa, porque los empleados tienen asignado puestos de trabajo fijo y utilizan puntos de red *ethernet* a 100 Mbps, además esta red no ofrece los mecanismos de seguridad adecuados como para garantizar su buen funcionamiento.

Se realizaron 10 entrevistas, 2 entrevistas a personal técnico y 8 entrevistas a usuarios corporativos. Entre las preguntas que fueron formuladas tenemos las siguientes:

1.- ¿Para qué utiliza la red inalámbrica y con qué frecuencia la usa?

2.- ¿Le parece importante la red inalámbrica en la empresa?

3.- ¿Qué servicio cree ud. a su juicio sería necesario incorporar y mantener en la red inalámbrica?

La pregunta 1 y 2, estan enfocadas a determinar el uso de la WLAN en la empresa, mientrás que la pregunta 3, reflejará algunos requerimientos que se tomarán en cuenta en este proyecto.

Resultados de las entrevistas:

Pregunta Nro 1:

El 80% de los entrevistados, es decir, 8 personas no conocian de la red inalámbrica, por lo cual no la utilizaban.

El 20% de los entrevistados, es decir, 2 personas utilizaban la red inalámbrica para acceder a Internet, a la información departamental y a los correos internos, ya que son usuarios de la localidad de Altagracia y viajan con frecuencia a Caracas.

Pregunta Nro 2:

El 100% de los entrevistados mencionan que es importante la red inalámbrica por las siguientes razones:

- Pueden acceder desde cualquier zona de la empresa donde haya cobertura a Internet sin necesidad de estar fijos en sus puestos de trabajo.
- Pueden acceder a los correos internos vía Internet en una reunión en otra oficina.
- Pueden tener disponible la información departamental en otros equipos fuera de su puesto de trabajo.

Pregunta Nro 3:

Entre los servicios que los entrevistados consideraron importante de incluir y mantener en la red inalámbrica son los siguientes:

- Acceso a Internet para todos los usuarios corporativos y visitantes.
- Acceso a los correos internos vía Internet en caso de no estar en su puesto de trabajo o si es un usuario corporativo que proviene de la localidad de Altagracia de Orituco.
- Acceso a tráves de sus dispositivos móviles personales a Internet.

Conclusión de las entrevistas:

Las entrevistas determinaron en la pregunta 1 y 2, que el uso actual de la red inalámbrica es poco, por desconocimiento de la misma. Actualmente está provista para pocos usuarios, lo cual no garantiza que no haya brecha de seguridad a través de esos equipos.

Por otro lado, los administradores de la red, manifestaron no haber difundido el uso de esta red, ya que no garantiza todas las condiciones de seguridad, para permitir el acceso a Internet, y a la información de la empresa, ya que como se muestra en la Figura 2-3 (ver página 69), el punto de acceso (PA), se encuentra colocado directo en la red plana, donde estan los servidores y equipos, con fácil acceso a la información departamental, lo cual hace vulnerable la seguridad.

2.2 - Etapa de análisis y documentación.

2.2.1 - Documentación sobre recomendaciones, estándares y normas de seguridad en redes inalámbricas y mejores prácticas de la industria, a través del uso de Internet.

La actividad inicial de esta etapa contempló la investigación bibliográfica relacionada con recomendaciones, estándares y normas de seguridad en redes inalámbricas, y sus fundamentos teóricos, a tráves del uso de Internet.

Luego se establecieron dos enfoques para este proyecto:

- El enfoque del fabricante, el cual propone cuatro soluciones para su plataforma.
- El enfoque de la industria, el cual incorpora las mejores prácticas en las WLAN.

2.2.1.1- Soluciones para una WLAN según Cisco[39]

Estas investigaciones se realizaron directamente desde la página *web* de Cisco[39], ya que es la tecnología presente en la empresa.

Actualmente la seguridad para WLAN se centra en el control de acceso y en la privacidad. Un sólido control de acceso a la WLAN, también denominado autenticación, impide que los usuarios no autorizados se comuniquen a través de los puntos de acceso. Unas medidas estrictas de control de acceso a la WLAN ayudan a garantizar que las estaciones cliente se asocien solamente con puntos de acceso de confianza, en lugar de puntos de acceso falsos o no autorizados.

La privacidad de la WLAN ayuda a garantizar que sólo los destinatarios deseados entienden los datos transmitidos. La privacidad de los datos transmitidos por la WLAN se considera protegida cuando dichos datos se cifran con una clave que sólo puede utilizar el destinatario deseado. El cifrado de los datos ayuda a garantizar que éstos no resulten dañados durante el proceso de envío y recepción.

En la actualidad, las empresas que usan WLAN están empleando cuatro soluciones diferentes de seguridad en WLAN para solventar los problemas de control de acceso y privacidad de WLAN:

- Acceso abierto
- Seguridad básica
- Seguridad mejorada
- Seguridad del acceso remoto.

Igual que sucede en cualquier instalación de seguridad, Cisco recomienda a las organizaciones evaluar los riesgos de la red antes de seleccionar e implementar cualquier solución de seguridad de WLAN.

Solución Nro. 1:

Acceso abierto

Todos los productos para LAN inalámbrica con certificación *Wi-Fi*, como los productos de la serie *Cisco Aironet*, se envían en modo de "acceso abierto", con sus características de seguridad desactivadas. Aunque el acceso abierto o la falta de seguridad pueden ser apropiados y aceptables para lugares públicos como cafeterías, campus universitarios, aeropuertos, etc., no lo son para las organizaciones empresariales. La seguridad debe activarse en los dispositivos inalámbricos durante su instalación en los entornos empresariales. Algunas empresas no están activando sus características de seguridad de WLAN, con lo que están exponiendo sus redes a un riesgo importante.

Solución Nro. 2:

a) Seguridad básica: SSID, WEP y autenticación de direcciones MAC

La seguridad básica incluye el uso de *Service Set Identifiers* (SSID), de autenticación abierta o de clave compartida, claves WEP estáticas y autenticación MAC (control de acceso a medios) opcional. Esta combinación ofrece un nivel rudimentario de control de acceso y privacidad, pero todos los elementos pueden correr peligro.

SSID es un nombre de red común para los dispositivos de los subsistemas WLAN y sirve para segmentar lógicamente dichos subsistemas. El SSID impide el acceso por parte de cualquier dispositivo cliente que no tenga el SSID. Sin embargo, de forma predeterminada,

un punto de acceso difunde su SSID en su baliza. Aunque la difusión del SSID esté desactivada, un intruso puede detectar el SSID a través de lo que se conoce como "*sniffing*" (rastreo), o control no detectado de la red.

El estándar 802.11, que es un grupo de especificaciones para WLAN creadas por el IEEE, admite dos medios de autenticación de clientes: autenticación abierta y por clave compartida. La autenticación abierta implica casi exclusivamente la introducción del SSID correcto. Con la autenticación por clave compartida, el punto de acceso envía al dispositivo cliente un paquete de texto de reto que el cliente debe cifrar con la clave WEP correcta y devolver al punto de acceso. Sin la clave correcta, la autenticación fallará y el cliente no podrá asociarse con el punto de acceso. La autenticación con clave compartida no se considera segura, ya que cualquier intruso que detecte el paquete de reto sin formato y el mismo paquete de reto cifrado con una clave WEP puede descifrar la clave WEP.

Con la autenticación abierta, aunque un cliente pueda completar la autenticación y la asociación con un punto de acceso, el uso de WEP impide que el cliente envíe y reciba datos del punto de acceso, a menos que tenga la clave WEP correcta. Una clave WEP se compone de 40 ó 128 bits, y normalmente la define estáticamente el administrador de red en el punto de acceso y en todos los clientes que se comunican con dicho punto de acceso. Si se utilizan las claves WEP estáticas, los administradores de red deben realizar la laboriosa tarea de introducir las mismas claves en todos los dispositivos de la WLAN.

Si se pierde o roban un dispositivo que utilice claves WEP estáticas, el poseedor del dispositivo robado puede acceder a la WLAN. Ningún administrador puede detectar que un usuario no autorizado se ha infiltrado en la WLAN, a menos que informen del robo. En ese momento, el administrador debe cambiar la clave WEP en todos los dispositivos que utilicen la misma clave WEP estática que emplea el dispositivo que falta. En la WLAN de una gran empresa, con cientos o incluso miles de usuarios, esta tarea puede ser difícil. Y lo que es peor, si una clave WEP estática se descifra con una herramienta como *AirSnort,* el administrador no tiene forma de saber si un intruso ha puesto en peligro la clave.

Algunos fabricantes de WLAN admiten la autenticación basada en la dirección física, o en la dirección MAC, de la tarjeta de interfaz de red (NIC) del cliente. Los puntos de acceso

sólo permitirán que los clientes se asocien si las direcciones MAC de los mismos coinciden con alguna dirección de la tabla de autenticación que utiliza el punto de acceso. Sin embargo, la autenticación MAC no es una medida de seguridad adecuada, ya que se pueden crear direcciones MAC o las NIC se pueden perder o robar.

b) Seguridad básica con clave WPA precompartida

Otra forma de seguridad básica que ya está disponible es WPA con clave precompartida (PSK, *Pre-Shared Key*). La PSK verifica los usuarios a través de una contraseña o un código identificativo tanto en la estación cliente como en el punto de acceso. Los clientes sólo pueden acceder a la red si sus contraseñas coinciden con la del punto de acceso. La contraseña también proporciona el material de manejo de claves que utiliza TKIP para generar una clave de cifrado para cada paquete de datos transmitidos. A pesar de ser más segura que WEP estática, WPA con PSK se parece a ella en que la PSK se almacena en la estación cliente y puede correr peligro si la estación se pierde o la roban. Se recomienda utilizar una contraseña PSK sólida que emplee una mezcla de letras, números y caracteres alfanuméricos.

Resumen de la seguridad básica

La seguridad básica de WLAN, que confía en una combinación de SSID, autenticación abierta, claves WEP estáticas, autenticación MAC o WPA con PSK sólo es suficiente para empresas muy pequeñas o que no utilizan las redes WLAN para los datos más importantes. Las organizaciones restantes deben invertir en una solución de seguridad de WLAN robusta y de tipo empresarial.

Solución Nro. 3:

Seguridad mejorada: la ventaja del Conjunto de Seguridad Inalámbrica de Cisco

La seguridad mejorada es aconsejable para todos los clientes que necesiten seguridad de tipo empresarial con todos los equipos a nivel de *hardware* que garantizan un nivel de seguridad óptimo pero para esto es necesario invertir en equipos. El conjunto de seguridad inalámbrica de Cisco es una solución de seguridad mejorada que proporciona un

soporte total para WPA y sus componentes básicos de 802.1X y TKIP. Las siguientes características forman parte del conjunto de seguridad inalámbrica de Cisco:

- 802.1X para una sólida autenticación mutua y unas claves de cifrado dinámicas por usuario y por sesión
- TKIP para mejoras del cifrado basado en RC4, como el *hash* de claves (la generación de claves por paquete), la comprobación de la integridad de los mensajes (MIC), los cambios en los vectores de inicialización (VI) y la rotación de claves de difusión. Al ser una solución de seguridad mejorada, el conjunto de seguridad inalámbrica de Cisco proporciona a los administradores de red la certeza de que están instalando las WLAN con seguridad y protección de tipo empresarial.

Solución Nro. 4:

Seguridad en LAN inalámbrica de acceso remoto

En ciertas instancias, las empresas pueden necesitar seguridad de extremo a extremo para proteger sus aplicaciones empresariales. Con la seguridad del acceso remoto, los administradores configuran una red privada virtual (VPN) que permite a los usuarios móviles de puntos calientes públicos, como aeropuertos, hoteles y centros de convenciones, concertarse a través de un túnel seguro a la red de la empresa.

Algunas empresas, como las instituciones financieras, que requieren grandes medidas de seguridad, también pueden implementar una VPN para las WLAN en sus *intranets*, además de la seguridad mejorada. Sin embargo, una solución de seguridad mejorada, como el conjunto de seguridad inalámbrica de Cisco, cumple con los requisitos de seguridad de WLAN de las redes de la mayoría de las empresas. Para una WLAN interna no son necesarios los costes administrativos, las limitaciones y los gastos adicionales de una capa de VPN.

2.2.1.2- Mejores prácticas de la industria

Por otro lado, además de seleccionar el tipo de solución para la empresa, se deben emplear prácticas que son recomendables para minimizar los riesgos asociados al acceso

indebido en redes inalámbricas, para protegerla de los ataques [ver sección 1.7 - . Entre las principales recomendaciones o mejores prácticas tenemos:

1.- Control en el área de transmisión y cierre de todos los puntos de acceso: Muchos puntos de acceso inalámbrico permiten ajustar el poder de la señal. Se deben colocar los puntos de acceso tan lejos como sea posible de las paredes y ventanas exteriores y hacer pruebas del poder de la señal para que únicamente los usuarios indicados puedan conectarse a estos sitios. Luego, se debe cambiar la contraseña predeterminada en todos los puntos de acceso. Es importante emplear una contraseña fuerte para proteger todos los puntos de acceso.

2.-Para tener compatibilidad, el hardware debería ser del mismo distribuidor, mientras la norma IEEE tiene compatibilidad entre los dispositivos inalámbricos de diferentes fabricantes, las interpretaciones de las normas y las extensiones de propiedad exclusiva pueden impedir la integración total entre dispositivos de diferentes fabricantes.

3.-Uso del SSID inteligentemente. Se deben adquirir puntos de acceso que permitan deshabilitar la transmisión de los SSID para evitar que los puntos de acceso transmitan el nombre de la red y se asocie con clientes que no están configurados con su SSID. También es necesario cambiar el SSID predeterminado para el punto de acceso. (Y al mismo tiempo, cambiar también la contraseña del administrador y el nombre de usuario predeterminado).

4.-Explorar con regularidad los puntos de acceso atacantes. Las tarjetas de interfaz para las redes inalámbricas se pueden configurar como puntos de acceso y se requiere muy poco esfuerzo convertir un equipo cliente en un punto de acceso atacante. Con regularidad se debe explorar los puntos de acceso atacante en la red mediante el uso de una herramienta de exploración inalámbrica.

5.-Implementación de autenticación de usuario, es importante mejorar los puntos de acceso para usar las implementaciones de las normas WPA y 802.11i. Además, a medida que se implementa la autenticación de usuario en los puntos de acceso es más segura aunque está expuesta a ataques, se deben reutilizar los servidores existentes para

proporcionar autenticación a los demás servicios de la red para evitar que los empleados que ya no trabajan en la empresa utilicen antiguas cuentas de usuario de acceso a la red.

6.-Protección de la WLAN con la tecnología "*VPN Ipsec*" o tecnología "*VPN clientless*", es la forma más segura de prestar servicios de autenticación de usuario, integridad y confidencialidad de la información en una WLAN. La tecnología adicional VPN no depende del punto de acceso o de la tarjeta LAN inalámbrica; por consiguiente, no se incurren en costos adicionales de *hardware* puesto que las normas de seguridad inalámbrica continúan evolucionando.

7.-Uso de autenticación de direcciones MAC (Control de Acceso a Medios de transmisión). Si hay un número administrable de usuarios inalámbricos y pocos puntos de acceso, la dirección MAC le permite restringir las conexiones a sus puntos de acceso al especificar la única dirección de *hardware* de cada dispositivo autorizado en una lista de control de acceso y al permitir únicamente aquellos dispositivos específicos que se conectan a la red inalámbrica.

8.-Activación del mayor nivel de seguridad que soporte el *hardware*. Incluso si existe un equipo de un modelo anterior que soporte únicamente WEP, hay que activarlo. En lo posible, se debe utilizar por lo menos una WEP con un mínimo de encriptación de 128 bits.

9.-Instalación de *firewalls* personales y protección de antivirus en todos los dispositivos móviles. La Alianza *WiFi* recomienda utilizar la política de seguridad de redes corporativas para imponer su uso continuo.

10.-Instalación de tecnologías de protección de clase empresarial, implica emplear un *firewall* de Capa 7 en la zona desmilitarizada y clientes *firewalls* en todos los equipos de escritorio; los servicios VPN que cifran todo el tráfico desde y hacia los dispositivos inalámbricos; sistemas de detección de intrusos; *software* antivirus a nivel del *gateway*, servidores y equipos de escritorio; evaluaciones periódicas de vulnerabilidades de la red WLAN; y herramientas para el cumplimiento de las políticas.

2.2.2 - Identificación y análisis de los riesgos y vulnerabilidades que presenta actualmente la red inalámbrica en la empresa YPergas, utilizando la información recopilada.

El propósito de este análisis es identificar y documentar los puntos vulnerables de los equipos inalámbricos y su daño potencial, además de identificar los riesgos y vulnerabilidades que presenta la red inalámbrica de la empresa. Entre ellos tenemos los siguientes:

- Existe un filtrado de *MAC address*, que hace que el PA permita o impida el acceso a determinadas MACs, y en el momento que algún usuario filtrado intenta conectarse queda reflejado en el *log* para un futuro estudio y el usuario no podrá conectarse. Lo que se hace con esta funcionalidad es limitar el número de direcciones MAC que pueden acceder. Esta actividad se realiza por medio de ACLs (*Access List Control*) en los PA, en las cuales se especifica (a mano) las direcciones MAC de las tarjetas a las que se les permitirá el acceso, negando el mismo a cualquiera que no figure en ellas. Como se muestra en la Figura 2-4.

  Esta medida de seguridad no es muy efectiva, impedirá el acceso a usuarios pocos experimentados, pero se puede modificar la MAC de su adaptador *wireless*, conociendo una MAC válida del sistema, que este autorizada a entrar en ese PA y se puede ingresar al sistema, para obtener esa MAC válida, solo tienen que estar capturando paquetes de la red durante un pequeño tiempo, hasta que decodifique alguna trama en la que se pueda ver la MAC origen. Actualmente existen cantidad de programas para realizar estas capturas de paquetes, los *sniffer*.

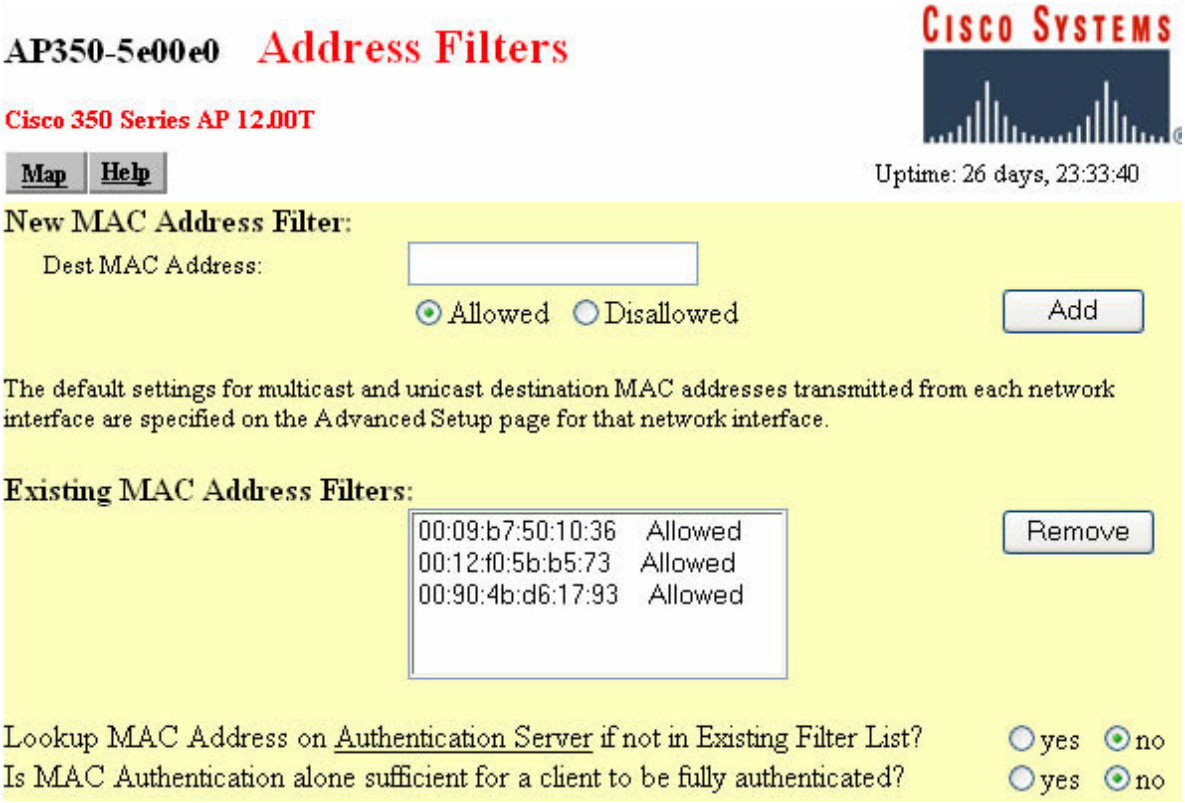


Figura 2-4 Filtrado de MACs address

- Los PA no tienen configuraciones VLANS. Como se muestra en la Figura 2-5 (ver página 81) . Aunque esto no se considera un riesgo, seria provechoso esta funcionalidad, ya que se pueden separar tanto el tráfico que llega a los usuarios inalámbricos con distintos esquemas de seguridad, como el que parte de éstos y asi se puede segregar en VLAN con distintas normativas de seguridad. En algunos casos, puede haber parámetros de seguridad diferentes para usuarios o grupos de usuarios diferentes de la red. Estos parámetros de seguridad pueden establecerse utilizando una VLAN en el punto de acceso. Por ejemplo, puede configurar políticas de seguridad diferente para grupos de usuarios diferenciados dentro de la empresa, como los de finanzas, legal, procura o recursos humanos. También, se puede configurar políticas de seguridad independientes para usuarios corporativos, no corporativos o visitantes que acceden a la LAN inalámbrica, incluso definir la administración de los equipos. La administración de los puntos de accesos se hace en la misma VLAN de usuarios, sin filtros de IP, bajo los protocolos de

HTTP/TELNET. El uso adecuado de las VLANS, permite utilizar un solo punto de acceso de forma económica para ofrecer soporte a varios grupos de usuarios con parámetros y requisitos de seguridad diferentes, mientras la red se mantiene segura y protegida.

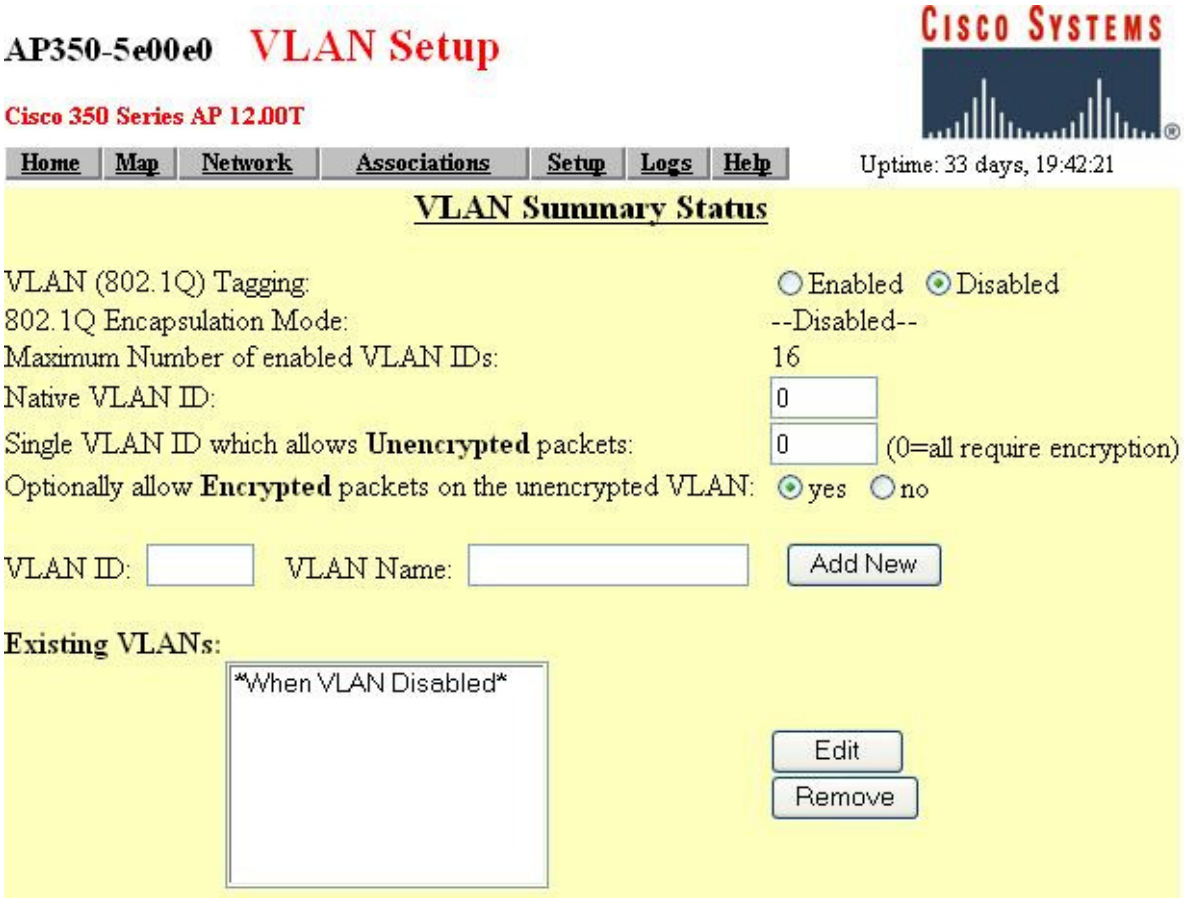


Figura 2-5 Configuración VLAN

- Los PA pueden manejar el estándar 802.1X (para autenticación EAP). Como se muestra en la Figura 2-6. Este protocolo 802.1X ofrece un marco en el que se lleva a cabo un proceso de autentificación del usuario, así como un proceso de variación dinámica de claves, todo ello ajustado al protocolo, denominado EAP (*Extensible Authentication Protocol*). Mediante este procedimiento, todo usuario que esté empleando la red se encuentra autentificado y con una clave única, que se va modificando de manera automática y que es negociada por el servidor y el cliente de manera transparente para el usuario. Pero en el caso de estos PA, no tienen configurado un servidor de autenticación para validar las cuentas de los usuarios y

verificar los datos suministrados mediante algoritmos, y otorgar acceso a la red en caso de validarse, lo cual hace vulnerable la seguridad a la red.

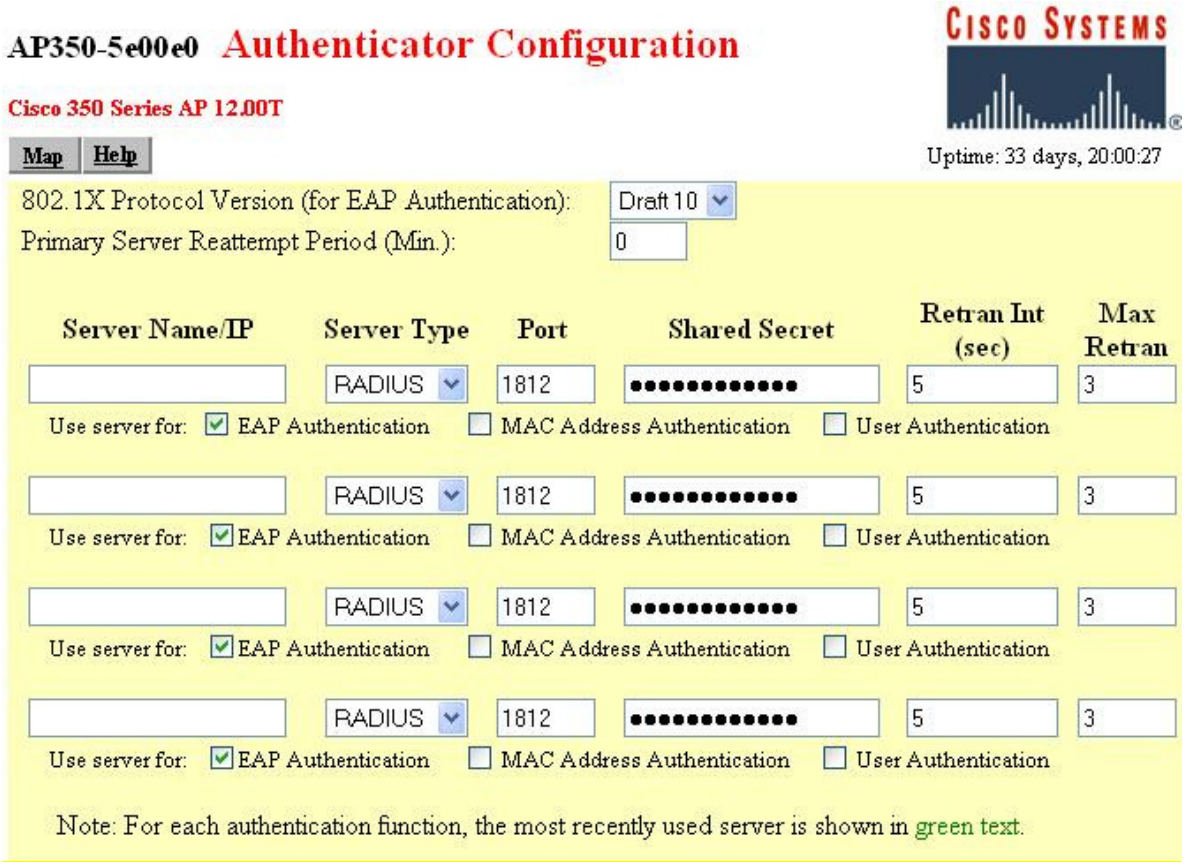


Figura 2-6 Configuración de autenticación en PA.

- Los PA tenian activado el SSID en *broadcast,* es necesario desactivar la publicación del SSID, sin embargo, un *sniffer* puede capturar en alguna trama el SSID aunque su publicación este desactivada, pero es necesario añadir esta funcionalidad porque sino tiene poca seguridad.

- Los PA no tenían una regulación de la potencia a transmitir, es necesario regular la potencia del PA para conseguir una cobertura exacta en el interior de las oficinas de la empresa, pero nos interesa que esa cobertura no se extienda innecesariamente a zonas donde no debemos tener usuarios. De esta manera, si alguien quiere buscar la red tendrá que aproximarse a las oficinas, y no lo podrá hacer desde los otros pisos o fuera del edificio. Al igual que las medidas de seguridad anteriores, es una medida que no garantiza nada pero ayuda.

- Los PA tenían un tipo de autenticación abierta con WEP a 128 *bit*, esto aporta mayor seguridad a la red. Como se muestra en la Figura 2-7, hay una encriptación completa de WEP a 128 *bits*, con una autenticación abierta. WEP utiliza un algoritmo de encriptación RC4, y clave de cifrado de 128 *bits*, utiliza una clave de cifrado asignada por el administrador tanto a los computadores como a los PA. El cifrado es simétrico con la misma clave tanto para cifrado como para descifrado, estas claves nunca se han cambiado siempre han sido las mismas, por lo que para alcanzar un nivel aceptable de seguridad las claves deben ser cambiadas con relativa frecuencia en todos los dispositivos por el administrador, se recomienda usar una clave (*Key* 1 - *Key* 2 - *Key* 3 - *Key* 4) por día o por semana, cambiando las claves cada mes, esto aporta un grado de seguridad mayor y hacemos que un futuro intruso tenga que trabajar mas en el intento de sacar o descodificar los paquetes que circulan por la red inalámbrica. Este procedimiento es imposible de llevar a cabo de manera automática, porque cualquier procedimiento que se intente, necesitaría que todos los computadores conectados se enterasen del cambio a la vez, ya que si por cualquier motivo un computador no estuviese conectado en el momento del cambio, se quedaría fuera de la red y tendría que ser reconfigurado manualmente. Otras vulnerabilidades de WEP es que verifica la máquina y no el usuario, los ataques criptográficos a WEP revelan la clave común, hay utilitarios especializados diseñados específicamente para romper el algoritmo de encriptación RC4 WEP, *AirSnort* y *WEP Crack* son dos de estas aplicaciones especializadas. WEP tiene algunas deficiencias de seguridad que lo hacen menos efectivo que WPA, de manera que se debería buscar soluciones que soporten codificación a través de WPA.

  Por otro lado, que los PA tengan configurado un sistema abierto de autenticación, indica que prácticamente no se restringe el acceso a la WLAN. Aunque debería tener configurado una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red, es el nivel más seguro. La autenticación mediante clave compartida funciona sólo si está habilitado el cifrado WEP, como es el caso de los PA de la empresa. Tener un sistema abierto, crea una ventana para que un intruso penetre en el sistema, después podrá enviar, recibir, alterar o falsificar mensajes.

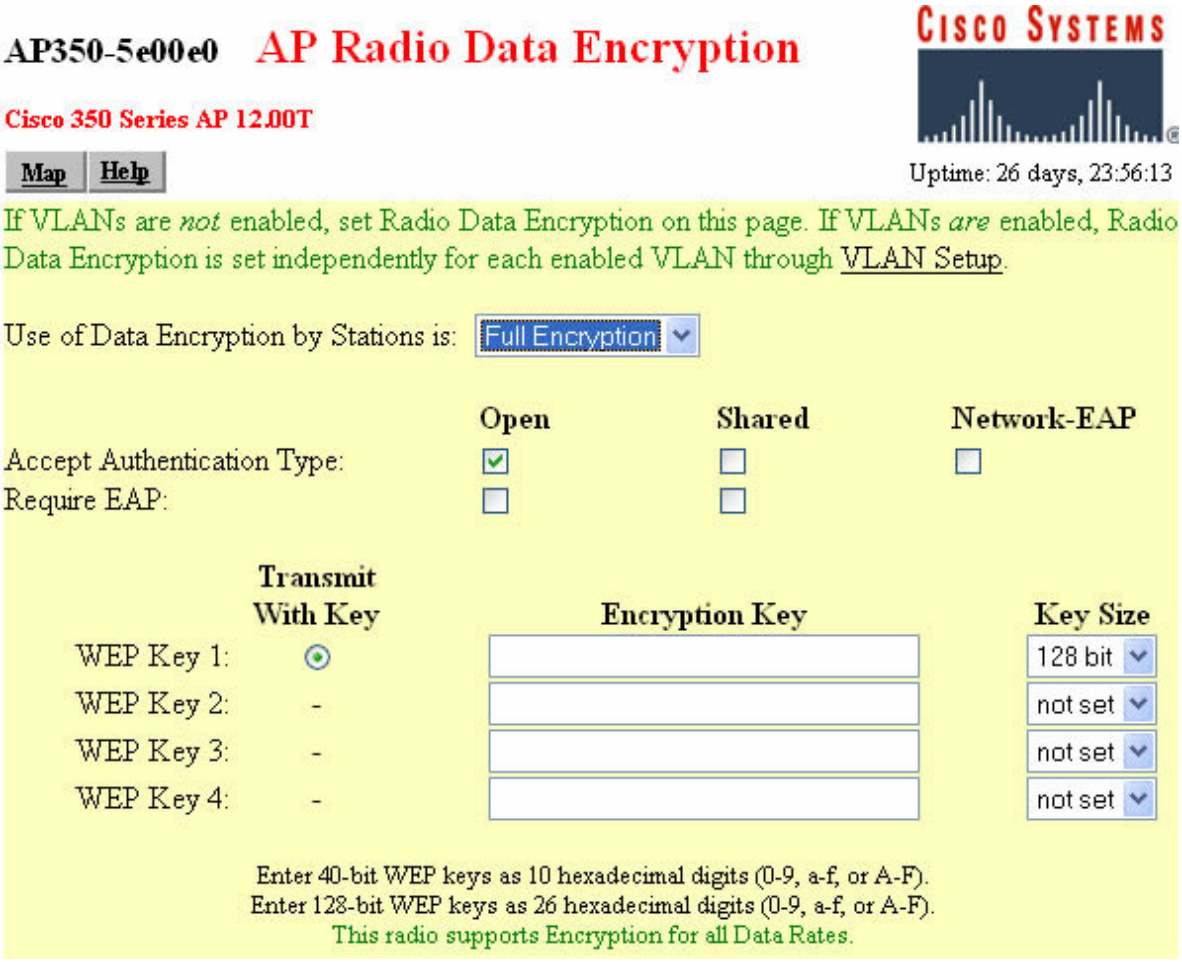
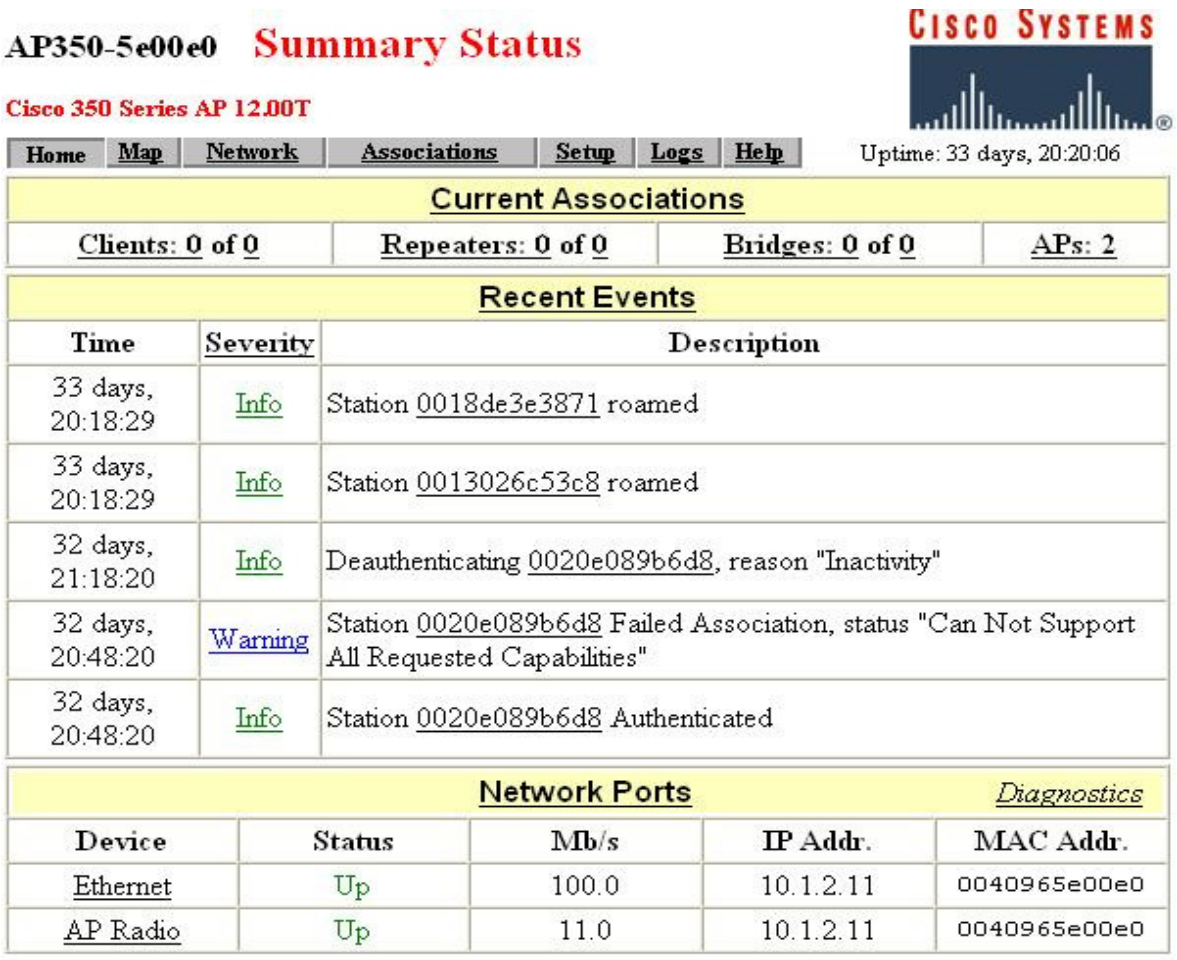


Figura 2-7 Autenticación abierta - WEP 128 bits

- Los PA se encuentran ubicados físicamente a la vista de los usuarios y en puestos de trabajos, por lo cual se considera necesario asignar una nueva ubicación física. Además, se encuentran ubicados lógicamente dentro de la misma red plana, donde están los servidores, impresoras, lo cual genera una brecha de seguridad, ya que pone en riesgo la información interna de la empresa.

- Los PA no tienen instalado un *firewall,* se debería instalar directamente en los dispositivos inalámbricos. Los atacantes que ingresen dentro de la cobertura de la red inalámbrica, pudieran evitar el paso a través del *firewall*.

- Los *logs* de eventos de los PA no son revisados frecuentemente por el administrador, lo cual trae como consecuencia que sea difícil aplicar medidas preventivas si existen acceso no autorizados. Como se muestra en la Figura 2-8



AP350-5e00e0 **Summary Status**

Cisco Systems

Cisco 350 Series AP 12.00T

Home | Map | Network | Associations | Setup | Logs | Help

Uptime: 33 days, 20:20:06

Current Associations

Clients: 0 of 0	Repeaters: 0 of 0	Bridges: 0 of 0	APs: 2

Recent Events

Time	Severity	Description
33 days, 20:18:29	Info	Station 0018de3e3871 roamed
33 days, 20:18:29	Info	Station 0013026c53c8 roamed
32 days, 21:18:20	Info	Deauthenticating 0020e089b6d8, reason "Inactivity"
32 days, 20:48:20	Warning	Station 0020e089b6d8 Failed Association, status "Can Not Support All Requested Capabilities"
32 days, 20:48:20	Info	Station 0020e089b6d8 Authenticated

Network Ports *Diagnostics*

Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	100.0	10.1.2.11	0040965e00e0
AP Radio	Up	11.0	10.1.2.11	0040965e00e0

Figura 2-8 Logs de eventos recientes del AP

A pesar de los riesgos y vulnerabilidades anteriormente expuestos, existen soluciones y mecanismos de seguridad mencionados en la sección 2.2.1 - que evitan el acceso de los intrusos a una red.

Una buena infraestructura de seguridad, con un plan adecuado que incluya políticas y procedimientos, así como la implantación de *firewalls* y sistemas de identificación con control de acceso, no garantiza una protección completa. La presencia de vulnerabilidades y brechas en un sistema informático significa que existe el riesgo que los datos

confidenciales puedan ser sustraídos o de que queden fuera de servicio operaciones vitales de la empresa, perdiéndose así tiempo, prestigio y dinero.

2.2.3 - Análisis de las posibles actualizaciones de *software* en los equipos inalámbricos, utilizando los documentos y recursos disponibles por parte del fabricante.

Inicialmente antes de realizar cualquier configuración en los equipos inálambricos era necesario hacer las actualizaciones del sistema operativo de los mismos, es decir, hacer un cambio de *VxWorks* a *Cisco IOS*.

Los puntos de accesos, como se mencionó en la sección 2.1.2 - (ver página 66), tienen versiones desactualizadas, y se debe hacer una actualización de sus sistemas operativos de *Vxworks* a *Cisco IOS*, para así proceder a realizar la actualización de la imagen que se adapte al equipo, ya que los equipos no soportaban el *Cisco IOS*.

Vxworks, es un sistema operativo basado en Unix, y *Cisco IOS* (*Internetwork Operating System*, Sistema Operativo de Interconexión de Redes) fue creado por *Cisco Systems*, para programar y mantener equipos de redes tales como *switches* (conmutadores) y *routers* (enrutadores).

La actualización de sistema operativo es recomendable, porque ofrece los siguientes beneficios:

- *Cisco IOS* es un *software* con soporte vigente, ya que desde el año 2000 *VXWorks* es un sistema que ingresó en la categoría EOL (*End of life*), es decir, que ya cumplió su ciclo de vida y soporte.

- Unificación de la administración, ya que este sistema operativo *Cisco IOS,* es el que se utiliza para la administración de los *routers y switches.*

- Incorpora nuevas y mejoras en las funcionalidades a nivel de sistema operativo.

- Eliminación de vulnerabilidades.

Durante el desarrollo de esta etapa, en cuanto al proceso de selección de las actualizaciones que se instalarían en los puntos de accesos, se procedió a realizar

comparaciones entre las actualizaciones que tienen los equipos actualmente y las que deberian tener de acuerdo a las investigaciones y revisiones realizadas en Internet, además de los mecanismos de seguridad que mas se adaptarían de acuerdo a la imagen que soporten estos equipos Cisco.

Se hicieron revisiones y descargas de las actualizaciones de las imágenes de los equipos inalámbricos (PA) *Cisco Aironet Acces Point* 350 series (AIR-AP350 series) modelo que se utiliza en la empresa.

Se observó que de acuerdo a la seguridad implementada en los equipos existentes se brinda una protección muy básica y sencilla a la red, en cuanto a tecnología se refiere. No obstante, se identificó la necesidad de incluir las actualizaciones pertinentes en los equipos para proceder a configurar y establecer los mecanismos de seguridad.

Luego de culminada la revisión de la actualización del sistema operativo a la versión *Cisco IOS*, se revisaron las imágenes disponibles en la página del fabricante para estos equipos, encontramos que las más actualizadas son: 12.3(8)-JEA3(LD) y 12.3(8)-JEA2(GD).

La nomenclatura JA/JEA implementada por Cisco en la versión de las imágenes, indica que el estándar se aplica en Japón-América/Japón-EMEA (Europa - Medio Oriente y Asia)-América respectivamente.

En el caso de LD (*Limited Deployment*) y GD (*General Deployment*), Cisco los define como designaciones a los *release* de las imágenes de IOS. LD, es un desarrollo limitado como su nombre lo indica, y el fabricante lo coloca a disposición para descarga en su página *web,* cuando incorpora una mejora significativa o soluciona un problema puntual en el sistema, no se recomienda implantar esta imagen como definitiva, ya que todavía esta a prueba en otras funcionalidades del *release.* Mientrás, GD, es la meta o hito del *release* e incorpora las funcionalidades definidas para el mismo.

En primer lugar, se realizó una comparación de las imágenes 12.3(8)-JEA3(LD) y 12.3(8)-JEA2(GD) señaladas en la página *web* del fabricante como las más recientes. La comparación determinaría cual era la más recomendable a instalar en los equipos. Esta se realizó con un utilitario llamado: *Cisco feature navigator[44]*, disponible en la página *web*

del fabricante, el cual permite realizar comparaciones de las imágenes, como se muestra en la Figura 2-9 (ver página 88).

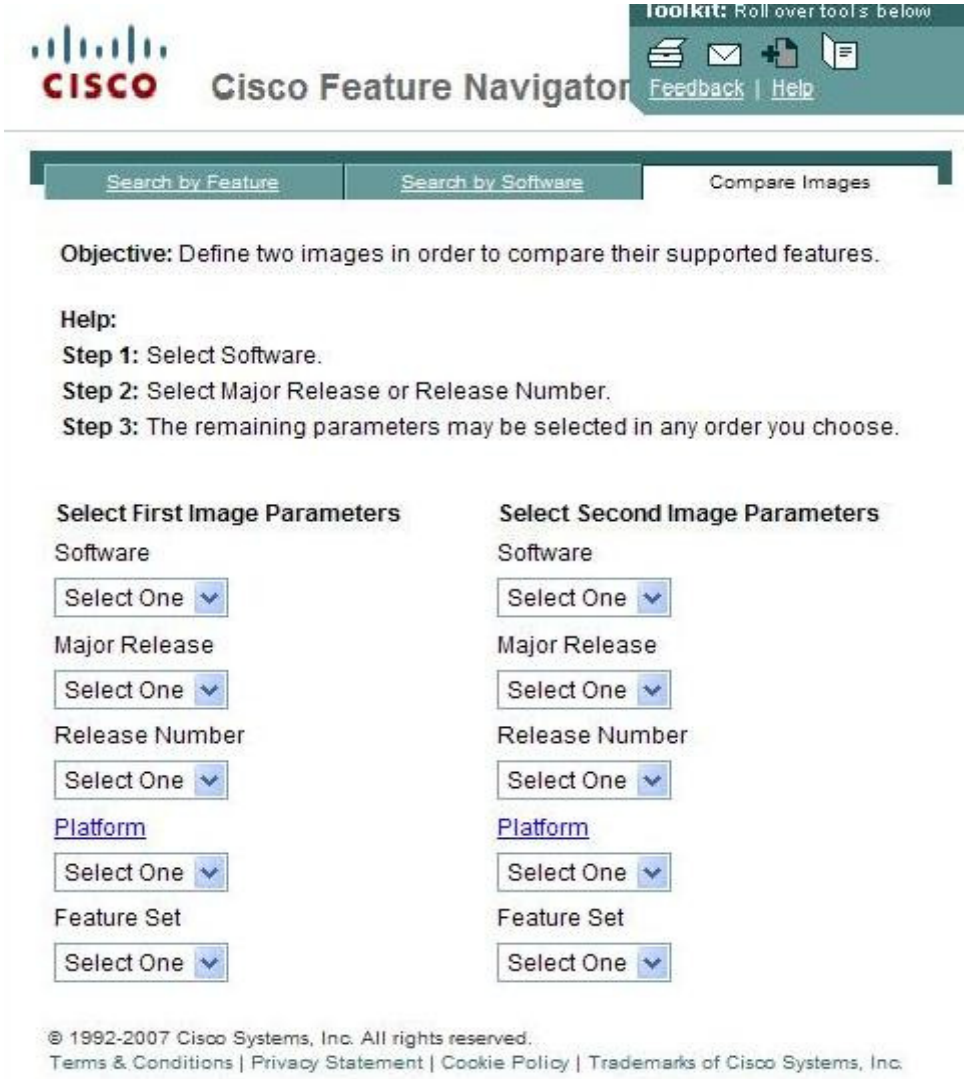


Figura 2-9 Pantalla del utilitario *Cisco Feature Navigator*

En la Tabla 2-2 (ver página 89), se pueden determinar las características principales de las imágenes 12.3(8)-JEA2(GD) y 12.3(8)-JEA3(LD). Además, en la Figura 2-10 (ver página 91), se muestra el resultado de la comparativa de las imágenes. Cabe destacar que cuando se realizó la comparativa a tráves del utilitario *Cisco feature navigator[44]*, las imágenes presentan las mismas funcionalidades, no hay nuevas agregadas en la imagen 12.3(8)-JEA3(LD) con respecto a la imagen 12.3(8)-JEA2(GD).

Descripción	12.3.8-JEA2(GD)	12.3.8-JEA3(LD)
Archivo para descargar	C350-k9w7-tar.123.8JEA2.tar	C350-k9w7-tar.123.8JEA2.tar
Fecha del *release*	26 de Julio del 2007	30 de Noviembre del 2007
Memoria Mínina / Tamaño del archivo	DRAM:16Mb, FLASH:8Mb / 4440Kb	DRAM:16Mb, FLASH:8Mb / 4440Kb

Tabla 2-2 Tabla comparativa de las imágenes 12.3(8)-JEA2 y 12.3(8)-JEA3

Sin embargo, en la guía: "*Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(8)JEA2*" [42], mencionan los problemas que están abiertos o por resolver y algunos de ellos son resueltos en la guía: "*Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(8)JEA3*" [44], entre ellos tenemos:

- CSCdz55178: Se pueden definir los nombres de perfiles en QoS que excedan más de 32 caracteres.
- CSCsj56438: Los paquetes EAP que identifican respuestas no son tan largos, lo cual ocasionaba reinicio.
- CSCsj66692: La integridad de los datos no se observa en el archivo encontrado en el directorio *voip/ccapi/ccapi_call.c*
- CSCsj81502: la salida del comando *show pagp neighbor* no es interrumpida en su ejecución.

Estos problemas reportados y resueltos en las guías no son relevantes para determinar cual imagen es mejor para la actualización de los equipos. De acuerdo a esta información, el criterio escogido en la toma de decisión de la imagen a instalar, fue basado en las designaciones a los *release* de las imágenes de IOS, es decir, si la imagen es *general deployment* (GD) o *limited deployment* (LD), una imagen designada como *general deployment* (GD), es más estable que una *limited deployment* (LD), por lo mencionado anteriormente. Además, la imagen 12.3(8)-JEA3(LD) no tiene nuevas funcionalidades con

respecto a la imagen 12.3(8)-JEA2(GD), los problemas resueltos en guía: "*Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(8)JEA3*"[43] ,no son importantes en la implantación de esta actualización. En conclusión, la imagen seleccionada a instalar en los puntos de accesos es 12.3(8)-JEA2(GD).

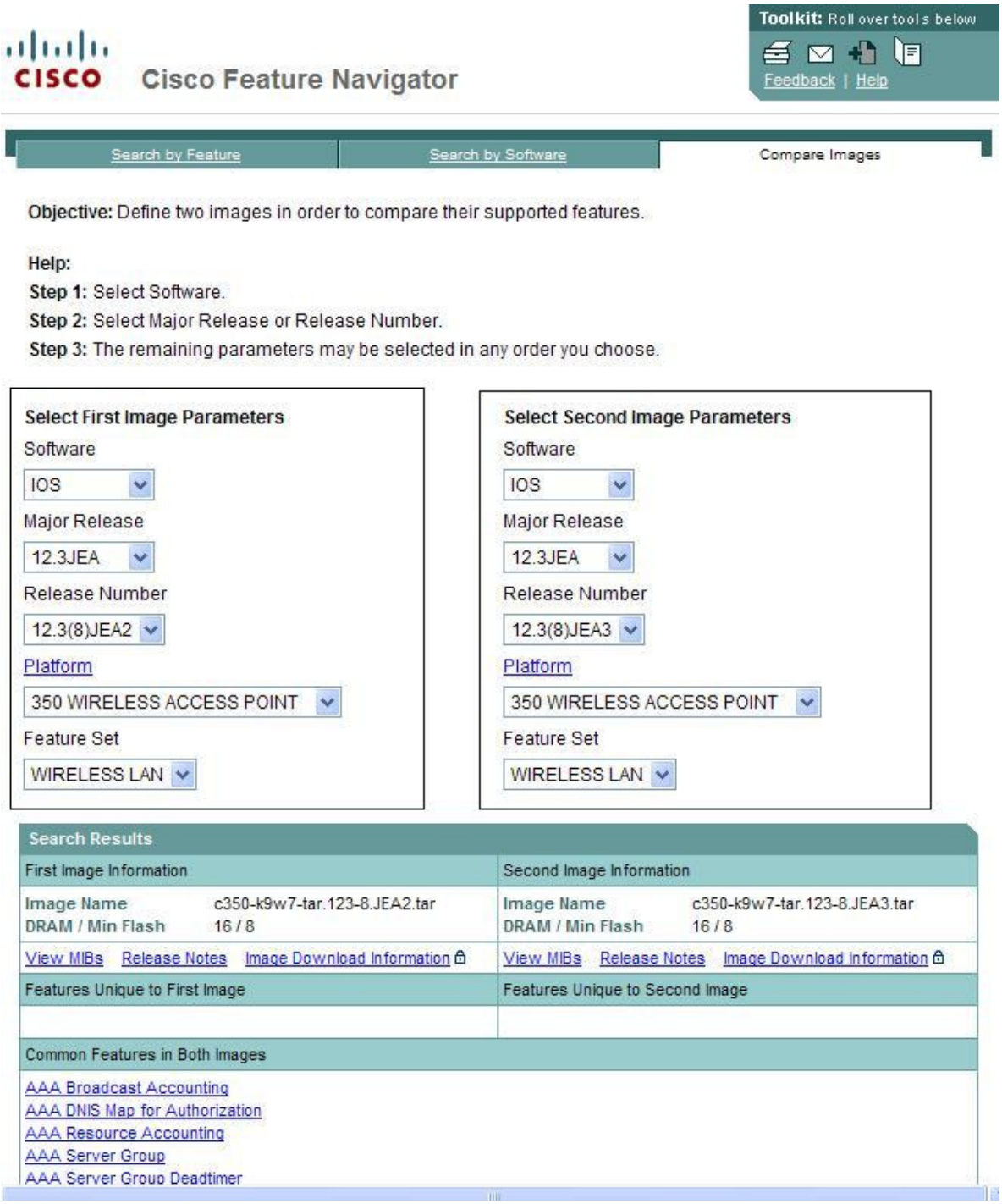


Figura 2-10 Comparativa en el *Cisco feature Navigator* de las imágenes 12.3(8)JEA2 y 12.3(8)JEA3

En la Figura 2-11 Comparativa en el *Cisco feature Navigator* de las imágenes 12.2(13)JA1 y 12.3(8)JEA2(ver página 94), muestra el resultado de la comparativa desde el utilitario *Cisco feature navigator[44]* entre las imágenes 12.2(13)JA1, imagen que tenian los equipos cuando se realizó la conversión de *Vxworks* a *Cisco IOS,* según señala la Tabla 2-4, y la imagen 12.3(8)-JEA2(GD) seleccionada a instalar en los equipos.

Las nuevas funcionalidades agregadas en la imagen 12.3(8)-JEA2(GD) con respecto a la imagen 12.2(13)JA1, son:

- Modo de escaneo en los puntos de accesos. En este modo, los puntos de acceso no pueden transmitir *beacons*, responden a posibles solicitudes o soportan mecanismos de asociación entre los clientes. Este modo funciona como un mecanismo de detención de intrusos.

- Rastreo de clientes. Esta nueva función permite ampliar la administración de la información de los puntos de accesos, incluyendo información de autenticación y eventos de *roaming*.

- Modo *frame* monitor. Un punto de acceso que trabaje en modo de escaneo puede ser configurado para operar en modo monitor. El modo monitor en los puntos de acceso, pueden enviar todos los *frames* recibidos y especifica la tercera parte en el servidor.

- Servidor *web* HTTP 1.1. El servidor *web* HTTP 1.1 esta integrado con Cisco IOS.

- HTTPS-HTTP con SSL 3.0. El servidor https-http y el cliente SSL 3.0 proveen funcionalidades con *Secure Socket Layer* (SSL) versión 3.0 soportado por el servidor y el cliente HTTP 1.1 con el *software* de Cisco IOS. SSL provee autenticación, encriptación, y mensajes de integración. HTTP sobre SSL es abreviado como HTTPS.

- Administración de clientes. Los clientes autorizados por el punto de acceso son detectados. El cliente puede forzar la disociación. Esta funcionalidad requiere el servidor *AirDefense*.

- Autenticación y protección de ataques. Esta característica cubre algunos mecanismos para identificar a un atacante que intenta comprometer la red en la fase inicial de la autentificación. Incluye los contadores en los frames de (Protocolo de 802.1x se denomina EAP *encapsulation over LAN*) EAPOL. La detección de *MAC spoofing*.

- Detección de *frames*. Algunos de los *frames* 802.11 son administrados por el punto de acceso. El contador de los *frames,* se pueden utilizar para detectar el comportamiento sospechoso que evidencian un ataque.

- IEEE 802.11d soporta modo *world*. El estándar 802.11d para el modo *world* permite informar a los puntos de accesos en sus dispositivos clientes 802.11d el ajuste del radio para las regulaciones locales.

- IEEE 802.1x Autenticación local para EAP-FAST. Esta característica permite que el servidor RADIUS soporte los tipos de autenticación EAP-FAST en el *software* de Cisco IOS, de tal modo que los puntos de accesos autentican al cliente *wireless* cuando el enlace WAN este apagado o el servidor RADIUS no este disponible.

- IEEE 802.1x para EAP-FAST. La suite de Cisco *wireless* soporta el estándar IEEE 802.1X, autenticación basada en EAP (*Extensible Authentication Protocol*) y EAP-Flexible, autenticación segura vía *tunneling* (EAP-Fast). EAP-FAST puede ser soportada en los puntos de accesos por la versión de Cisco IOS 12.2(11) JA o superior.

- Localización basada en servicios. Esta característica proporciona la capacidad para que los puntos de accesos Cisco localicen la etiqueta de los terceros que transfieren los paquetes especiales del tipo IEEE 802.11, al trabajar con un servidor de la localización.

- *Simple Network Time Protocol* (SNTP). SNTP es simplificado, la versión cliente utiliza NTP (*Network Time Protocol*).

- Asignación de VLAN por nombre. Esta característica proporciona la capacidad para que el servidor del RADIUS asigne a un cliente 802.11 una VLAN identificada por

nombre. Antes de la introducción de esta característica, VLANs tuvo que ser identificado por el " VLAN_ID".

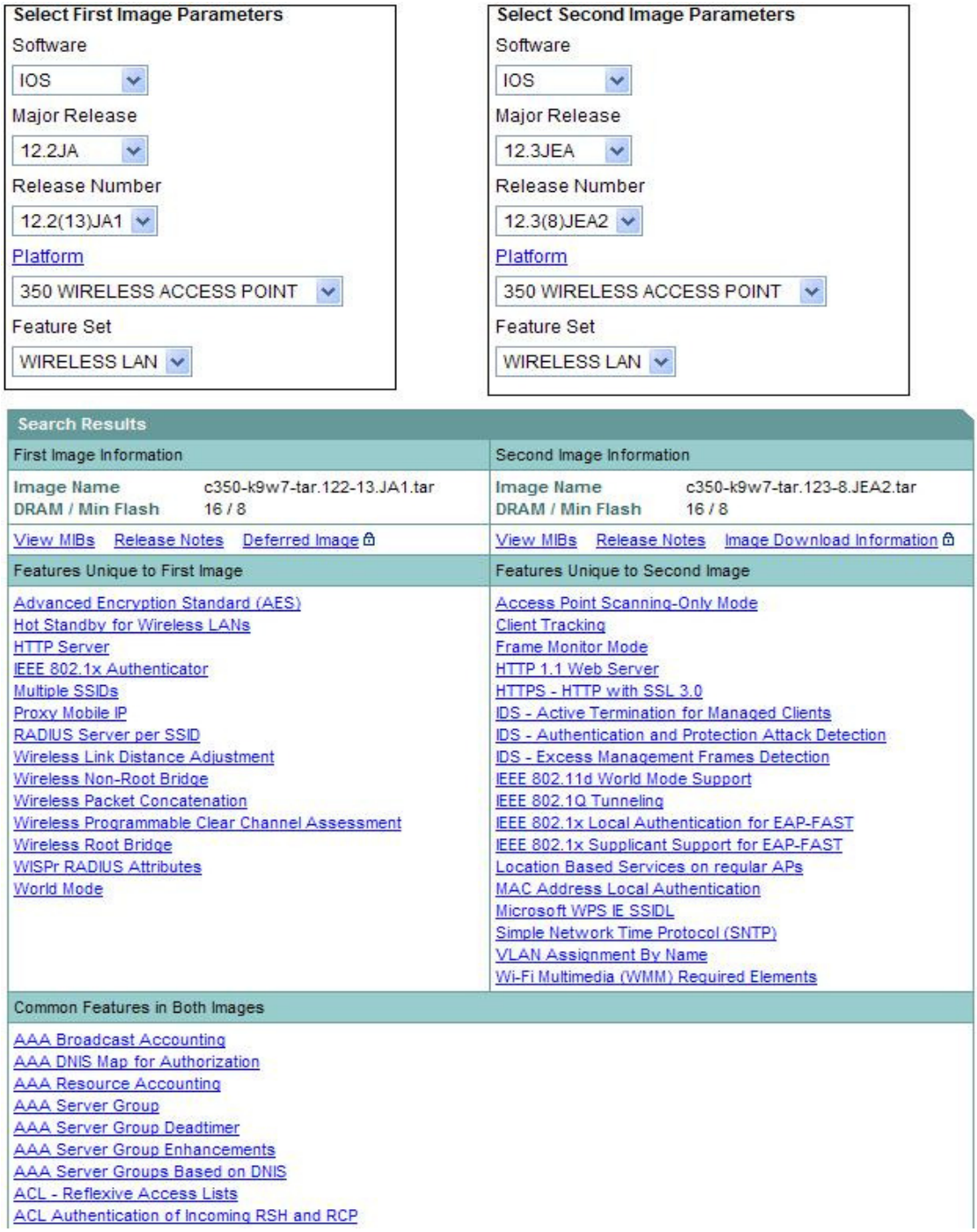


Figura 2-11 Comparativa en el *Cisco feature Navigator* de las imágenes 12.2(13)JA1 y 12.3(8)JEA2

2.3 - Etapa de implementación de cambios en los equipos inalámbricos.

2.3.1 - Evaluación de situación actual de la WLAN y diseño de solución a implementar, de acuerdo a la información recopilada en las etapas anteriores.

Inicialmente, se realizó una evaluación de la situación actual de la WLAN, posteriormente, se evaluó los posibles cambios a realizar en la red para garantizar el uso aceptable y definir el diseño de la solución a desarrollar para este proyecto.

2.3.1.1- Evaluación de la situación actual de la WLAN

En esta sección se resumió en varias premisas el escenario actual que presenta la red inalámbrica de la empresa, y que se analizó previamente en la sección 2.2.2 - (ver página 79):

- La seguridad implementada en los puntos de accesos es muy sencilla, basada en claves estáticas de 128bits para WEP, y en filtrado de direcciones MAC.
- Los puntos de accesos están ubicados lógicamente en el mismo segmento de la red interna, no se usan VLAN sólo la que viene predeterminada (VLAN 1).
- Los puntos de accesos se utilizan como redes separadas sin hacer *roaming* entre sí.
- La WLAN es utilizada esporádicamente por los usuarios, por desconocimiento y poca difusión de los administradores, ya que significa una brecha de seguridad para la empresa.
- La administración de los puntos de accesos se hace en la misma VLAN de usuarios, sin filtros de IP, bajo los protocolos de HTTP/TELNET.
- Los puntos de accesos están visibles a los usuarios y en algunos casos en los puestos de trabajo.

Además de las premisas que se señalaron anteriormente, se establecieron otras en la entrevista a los administradores que a continuación se mencionan:

- La empresa no está dispuesta a realizar inversión en *hardware,* ya que los equipos ofrecen el servicio básico que los usuarios necesitan, lo que consideraron importante es actualizar el *software* de los equipos y mejorar los mecanismos de seguridad para garantizar un mejor funcionamiento y buen uso de esta red dentro de la empresa, garantizando un nivel de seguridad aceptable.

- El acceso a Internet que se ofrece a tráves de la WLAN, es mediante el enlace dedicado de la empresa, lo cual afecta los servicios comunes que pueden ser críticos para los usuarios.

Este levantamiento de información sirvió como primer paso para poder involucrarse con la importancia de la seguridad inalámbrica de la empresa en cuanto a su uso adecuado y desempeño para las operaciones, al mismo tiempo que permitió clarificar algunos conceptos del tema y conocer los procesos básicos de la seguridad inalámbrica. Esta necesidad surgió debido a que la empresa mantiene relaciones con múltiples clientes y proveedores, por lo cual requiere manejar con cuidado la información confidencial o clasificada, ya que muchos de los negocios que se realizan pueden implicar el uso o la divulgación de información confidencial a través de sus redes.

Es necesario considerar la deficiencia, obsolescencia y ausencia de las medidas y controles identificados que pueden causar pérdidas de confidencialidad, integridad y disponibilidad de la información.

Otro punto importante a evaluar y analizar en esta sección fue las necesidades determinadas en las entrevistas con los usuarios y los administradores en referencia a la respuesta de la pregunta nro 3, de la sección 2.1.4 - (ver página 69), los cuales consideraron importante el uso de la WLAN, ya que la misma sería utilizada mayormente para:

- Ofrecer accesos a Internet a los usuarios visitantes/contratistas/auditores y al personal que viene asignado por tiempo limitado para la empresa y que no pueden ser ubicados en puestos de trabajos fijos por limitación de espacio.

- Ofrecer acceso a Internet a través de los dispositivos móviles personales (*iphone*, *palm*, *laptop*s no corporativas) a los empleados.

- Ofrecer conexión remota a las *laptops* corporativas a la red de los socios (socio Total).

El acceso de los usuarios corporativos por la WLAN a la información departamental, no se consideró importante por la baja necesidad manifestada por los usuarios, por lo cual no se justifica invertir tiempo y dedicación, en esta actividad además, compromete la seguridad de la empresa.

2.3.1.2- Diseño de solución a desarrollar en el proyecto

Luego de evaluar la situación actual de la WLAN y en discusión con el personal técnico de la gerencia de Tecnología de la Información, se definieron en conjunto lineamientos a implementar para proporcionar un uso aceptable de la WLAN, entre los cuales tenemos:

- Reubicación a nivel lógico de los equipos, se colocará detrás de un firewall perimetral, separados de la red plana.

- Actualización del sistema operativo en los puntos de accesos de *VxWorks* a *Cisco IOS* para que pueda soportar la actualización de la imagen que corresponde a estos equipos, la cual fue analizada en la sección 2.2.3 - (ver página 86).

- Actualización de la imagen en los puntos de accesos con la versión más actualizada que provee el fabricante, la cual fue analizada en la sección 2.2.3 - (ver página 86).

- Reubicación a nivel físico de los equipos, donde no sea un puesto de trabajo ni zona accesible a los empleados.

- Utilizar el acceso a banda ancha (ABA), provisto para los casos de contigencia en la empresa, para no saturar el enlace dedicado que afecta en los servicios críticos.

- Definición de tres VLAN, una VLAN para la administración segura de los equipos, otra para los usuarios corporativos que se conectan por VPN a las empresas de los socios, y por último la otra VLAN para que los usuarios puedan acceder a Internet.

- La VLAN para administración de los equipos se utilizará con filtros de acceso HTTPS/SSH.

- Establecer mecanismos de seguridad en las dos VLANS definidas como acceso en los equipos. WPA2 para los usuarios corporativos y no corporativos, y WEP para los usuarios corporativos que se conectan por VPN a las empresas de los socios.

- Establecer *roaming* entre los equipos.

- Definir una solución para los requerimientos de WLAN según el análisis del fabricante, señalada en la sección 2.2.1.1- (ver página2.2.1.1- 72).

- Brindar acceso a Internet a los usuarios corporativos con los equipos de la empresa y sus dispositivos o equipos personales.

- Brindar acceso a Internet a los usuarios corporativos mediante VPN a otras empresas (socios).

- Brindar acceso a Internet a los usuarios no corporativos.

En la Tabla 2-3 (ver página 99), se resume con párametros la situación actual de la WLAN, definido como escenario atual y los lineamientos a implantar, definidos como escenario propuesto.

Parámetros	Escenario Actual	Escenario Propuesto
Seguridad (CIA- Confiabilidad/ Integridad/ Disponibilidad)	Básica: (Clave WEP de 128bits con filtrado MAC)	WPA2 (guest mode) y WEP (VPN de los socios)
Acceso/ Administración	Los puntos de accesos están en el mismo segmento de la red interna. No usan VLAN, tiene configurada la predeterminada VLAN 1. Administración mediante HTTP/ TELNET, dirección IP en la misma VLAN de usuarios sin filtros IP.	Los puntos de accesos estarán detrás de un firewall perimetral. 3 VLAN (1 de administración con filtros de acceso HTTPS/ SSH, 2 de accesos para los usuarios)
Acceso a Internet	Se utilizan recursos comunes en ancho de banda a los servicios críticos de la empresa mediante el enlace dedicado.	Se utiliza el acceso a banda ancha (ABA) que está destinado sólo para contingencias en la empresa, sin afectar los servicios críticos.
Roaming	Se utilizan los puntos de accesos como redes separadas (no hay roaming)	Se establece roaming entre los puntos de accesos.
Costo de implementación	Sin costo de implementación	Horas / Hombre
Conectividad y acceso de usuarios	Pocos usuarios corporativos con los equipos de la empresa (uso esporádico)	Usuarios corporativos con equipos de la empresa y dispositivos personales. Usuarios corporativos mediante VPN a las empresas socias. Usuarios no corporativos con sus equipos personales.
Ubicación física	Visible a los usuarios en un puesto de trabajo	En un lugar no accesible a los usuarios.
Sistema operativos de los puntos de acceso	VxWorks	Cisco IOS
Imagen instalada en los equipos	11.21 y 12.00T	12.3(8)-JEA2(GD)

Tabla 2-3 Tabla escenario actual/escenario propuesto

2.3.2 - Actualizaciones que se realizaron de *software* en los equipos inalámbricos utilizando los recursos disponibles por parte del fabricante.

Inicialmente, como los puntos de accesos estaban en una versión desactualizada de su sistema operativo era necesario hacer una conversión, por lo cual se procedió a pasar de *Aironet VxWorks* a *Cisco IOS* , a traves de un utilitario de conversión llamada *conversion tool and image*, el cual es utilizado por los administradores para crear una configuración IOS usando la versión de *VxWorks* de los puntos de acceso de la serie 350 y 1200. Los pasos que se realizaron en la conversión estan documentados en el trabajo, basados en la guía de referencia: "*Cisco Aironet Conversion Tool for Cisco IOS Software 2-1 – Administrator guide for windows*" [40].

En la siguiente Tabla 2-4, podemos identificar los puntos de accesos, la versión de *VxWorks*, las imágenes que soporta el utilitario de conversión.

Punto de Acceso	Versión VxWorks	Archivo de la imagen	Versión de Cisco IOS (después de la conversión)
AP1200 AP1220	12.03T, 12.02T1, 12.01T1,12.00T, 11.56. or 11.54T	AP1200-Cisco-IOS-Upgrade-Image-v3.img	12.2(1.1)JA3
AP350	12.03T,12.02T1, 12.01T1,12.00T, 11.23T or 11.21	AP350-Cisco-IOS-Upgrade-Image-v2.img	12.2(13)JA1

Tabla 2-4 Versión de puntos de accesos, versión de *VxWorks* e Imágenes

Este utilitario, almacena la configuración del sistema operativo *VxWorks* en el computador, para luego utilizarla con el archivo imagen y generar la versión de *Cisco IOS*, dependiendo del modelo y serie del punto de acceso. En nuestro caso, utilizamos los puntos de accesos de la serie AP350, un equipo tenía la versión de *VxWorks* 11.21 y los otros equipos tenían 12.00T.

Existen dos maneras de realizar la conversión de *VxWorks* a *Cisco IOS,* una preservando la configuración actual del punto de acceso, y otra es sin preservar la configuración. En el primer caso, se puede revertir el proceso en cualquier momento utilizando el utilitario

conversion tool and image del punto de acceso, de la otra manera no se utiliza el utilitario *conversion tool and image,* sino la interfaz gráfica del punto de acceso (*browser*).

En este trabajo, se realizó la conversión preservando la configuración del punto de acceso, porque se puede revertir el proceso en caso de alguna falla, y además se puede determinar visualmente como se va ejecutando esta conversión, a través de la consola vía *hyperterminal*.

A continuación se explicarán los pasos para realizar la conversión en los puntos de accesos:

Antes de comenzar

1.- Verificar las configuraciones a nivel de *hardware* y *software* del computador donde se le instalará el *conversion tool and image,* este utilitario sólo opera con los sistemas operativos *Windows* 2000 o XP y necesita como mínimo los siguientes requerimientos a nivel de *hardware*: procesador Pentium III o equivalente, velocidad de 850 MHz, RAM de 128MB, espacio libre en el disco duro de 250 MB.

2.- Es importante que el usuario que realice la instalación tenga privilegios de administrador en el computador y en el punto de acceso, tenga todos los privilegios.

3.- Desactivar la opción del *firewall* del sistema operativo, para que permita ejecutar los procesos del utilitario.

4.- Habilitar la opción de SNMP en los puntos de accesos, ya que este utilitario usa los comandos de SNMP para obtener la configuración de los datos del punto de acceso. Tal como se muestra en la Figura 2-12.

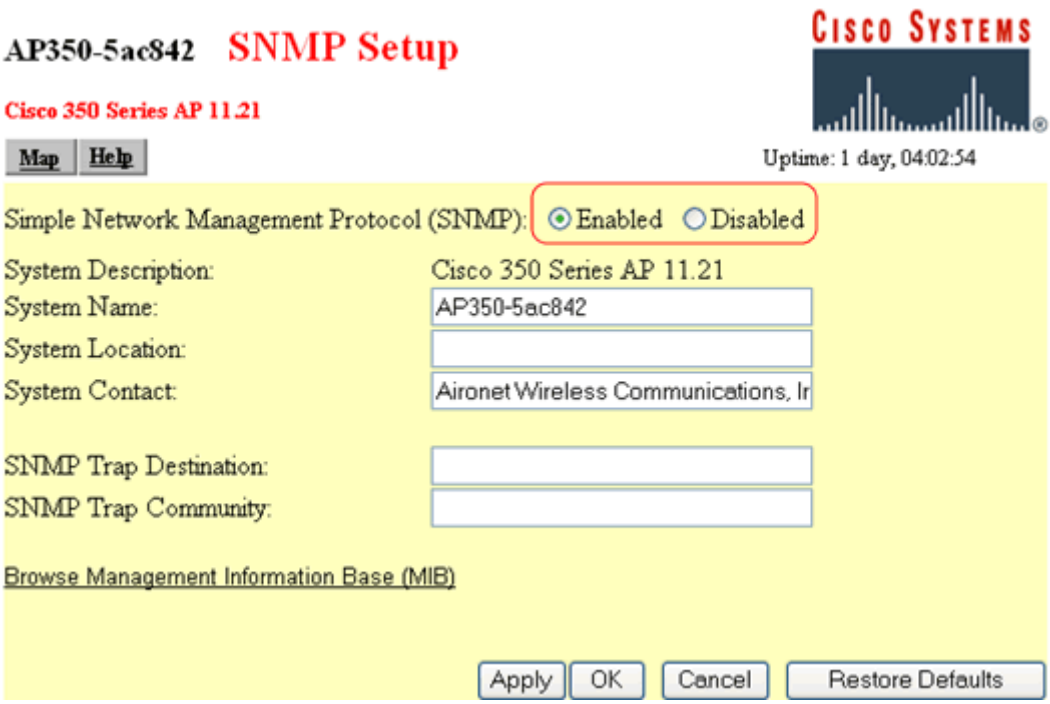


Figura 2-12 SNMP *Setup*

5.- El proceso de conversión requiere de espacio libre en el punto de acceso, como mínimo debería tener 4.2MB en los puntos de accesos de la serie 350, que es nuestro caso de estudio, para verificar el espacio de memoria disponible se establece una conexión por *hyperterminal* o una sesión de *telnet* y se verifica mediante el siguiente comando: *vxdiag_memshow*, la cantidad de memoria libre se lista en el *max block column*.

```
(Auto Apply On) :BOttom, :Down, :Back, :Forward, ^R, =, <ENTER>, or [Link Text]:
 :vxdiag_memshow
 status   bytes    blocks   avg block  max block
 ------ --------- -------- ---------- ----------
current
   free   6116384      669       9142    6033248
  alloc   7414352     7430        997          -
cumulative
  alloc  11266784    23057        488          -
(Auto Apply On) :BOttom, :Down, :Back, :Forward, ^R, =, <ENTER>, or [Link Text]:
```

Figura 2-13 Memoria disponible en los puntos de accesos

En este caso, el punto de acceso tenia 6MB de espacio libre en memoria, como se muestra en Figura 2-13. Si es necesario, se puede agregar memoria adicional al punto de acceso realizando los siguientes paso:

5.1 .-Acceder a la página *advanced*, del punto de acceso (*Setup – Associations - Advanced*), tal como se muestra en la Figura 2-14.

5.2.-Deshabilitar la opción de RFC 1493 802.1D *Statistics in MIB (dot1dTpFdbTable)* y la opción *Aironet Extended Statistics in MIB (awcTpFdbTable),* tal como se muestra en la Figura 2-14.

5.3.-Habilitar la opción *Map Multicast Entries to Broadcast Entry*.

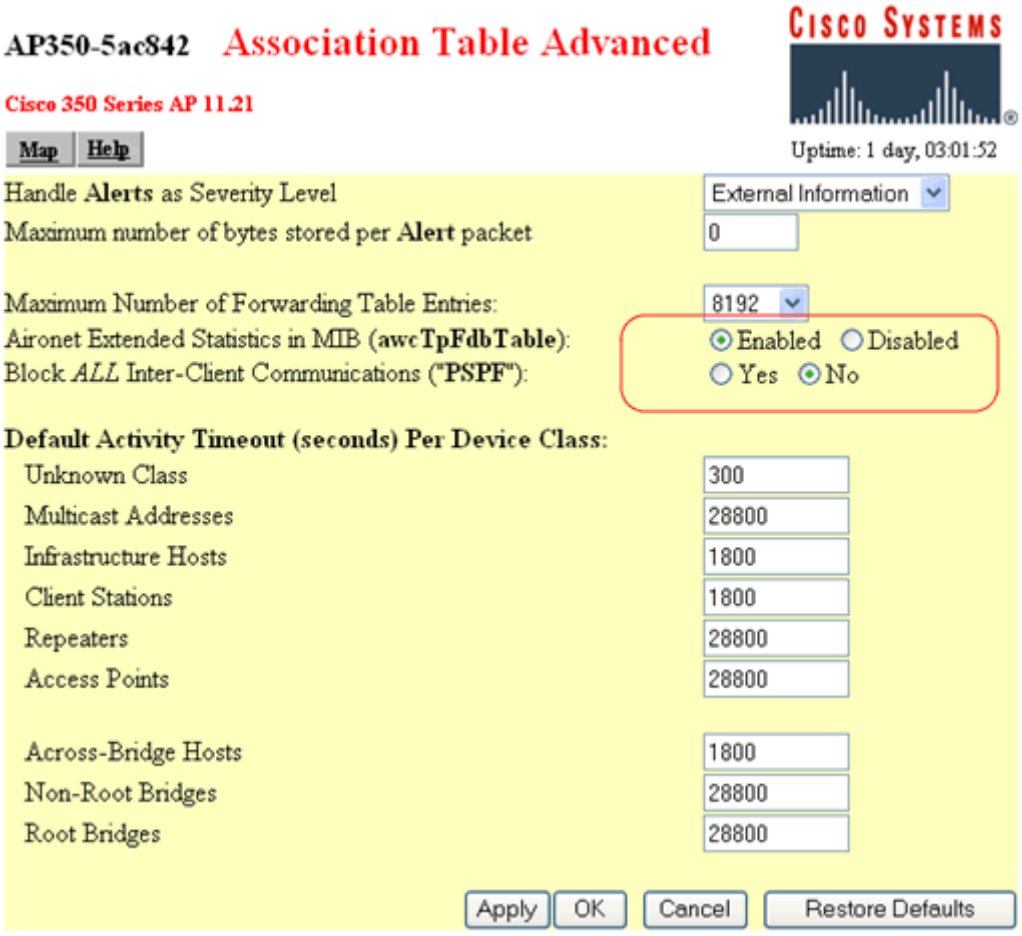


Figura 2-14 Tabla de asociaciones

6.- Descargar el utilitario *Aironet-AP-Cisco-IOS-Conversion-Tool-v2.1.exe* de la página *web* de Cisco.

7.- Descargar el *helper image file* de la página *web* de Cisco. Para identificar cual archivo corresponde en el punto de acceso, puede consultar en la Tabla 2-4. Para este caso, se descargó el *AP-350-Cisco-IOS_Upgrade-Image-v2.img*.

8.- Instalar el utilitario *conversión tool and image* .

Ejecutando el *conversión tool and image*

El *conversión tool* instala y utiliza un servicio de un servidor TFTP en el computador (*CACToolTFTPService*), cuando el utilitario esta activo, el servidor TFTP esta activo y cuando se sale del utilitario el servidor TFTP está desactivado.

1.- El utilitario se activa, ingresando a la opción *CAC Tool,* y aparece la ventana principal, como se muestra en la Figura 2-15, allí se muestran los botones de añadir, modificar y eliminar tareas, obtener la configuración de *IOS* y revisar los *logs* en caso de falla en alguna tarea.

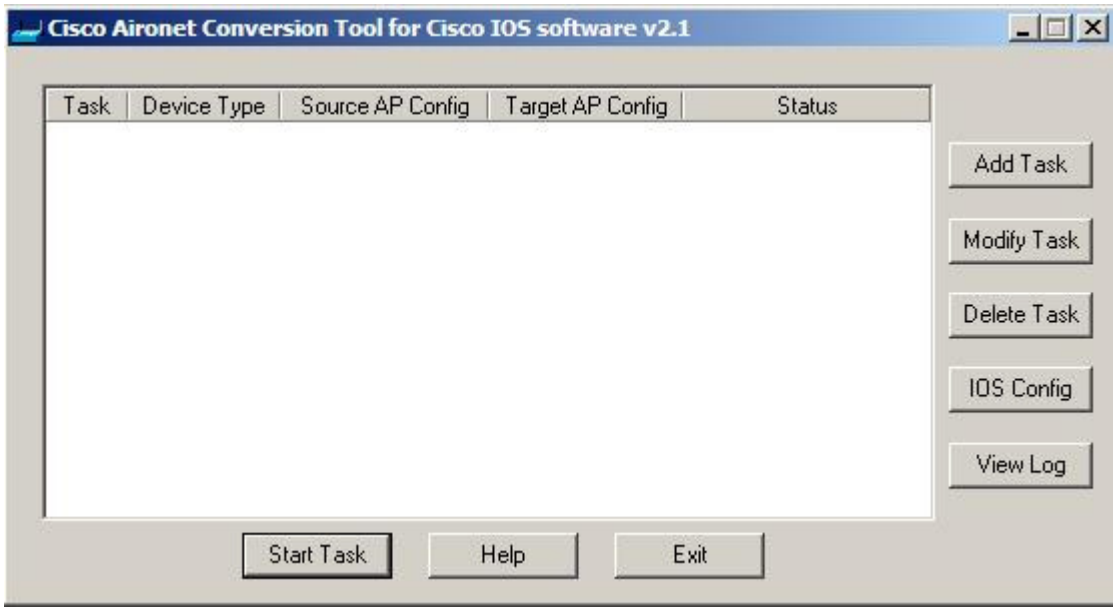


Figura 2-15 Ventana principal del *conversion tool*

2.- Cuando se añade una tarea, aparece la ventana de *device configuration*, alli se configuran los parámetros del origen (*source)* y destino (*target*). El origen o destino pueden ser configurados como un mecanismo o una ubicación en el disco duro, en este último caso se utiliza para guardar en el disco duro la configuración del punto de acceso creado por el utilitario, como se muestra en la Figura 2-16, donde se genera un archivo .cfg, en la ruta indicada en el disco duro del computador, más adelante se utilizará este archivo de configuración. Una vez ingresado todos los datos, se procede al siguiente paso

donde se observa el proceso de generación del archivo de configuración, como se muestra en Figura 2-17.

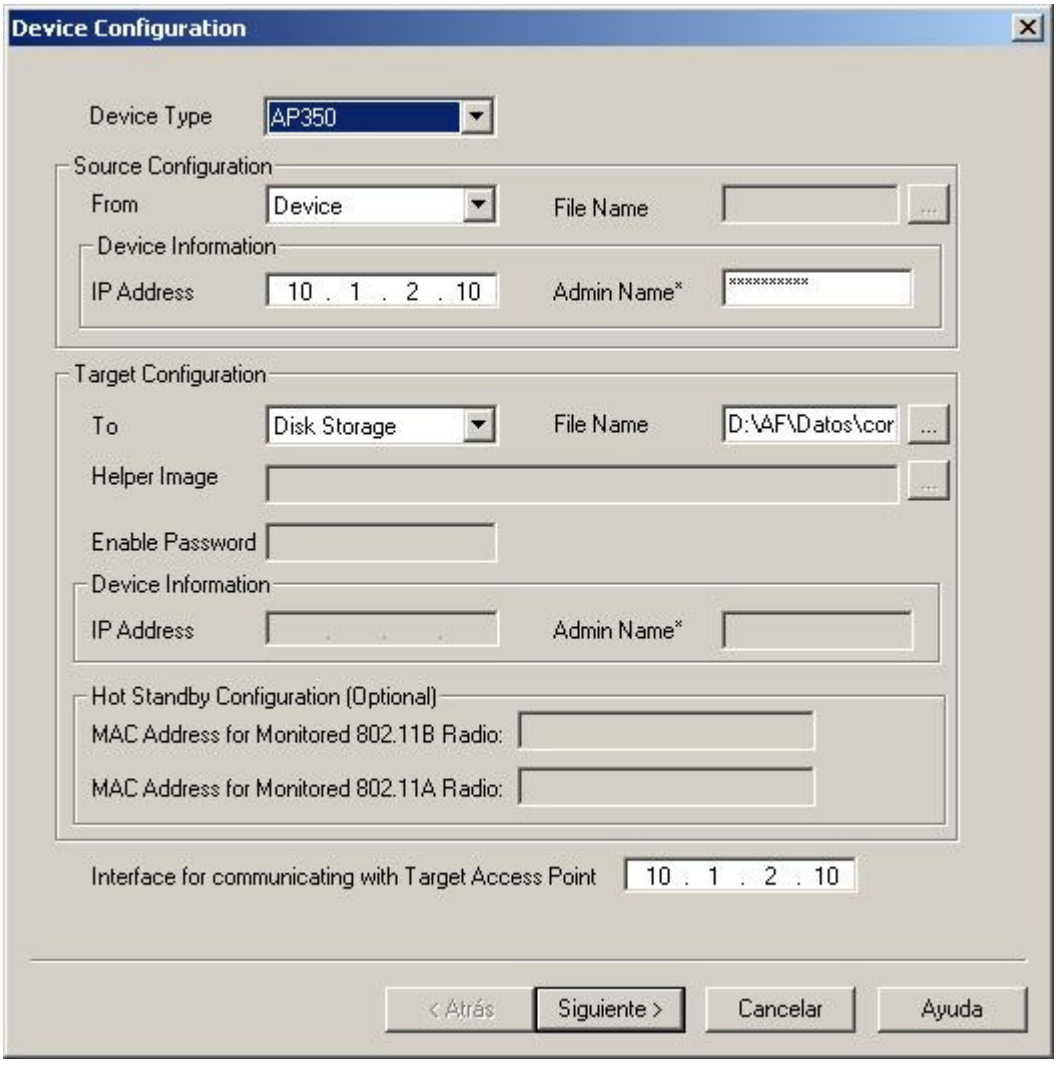


Figura 2-16 Ventana de "*device configuration"*

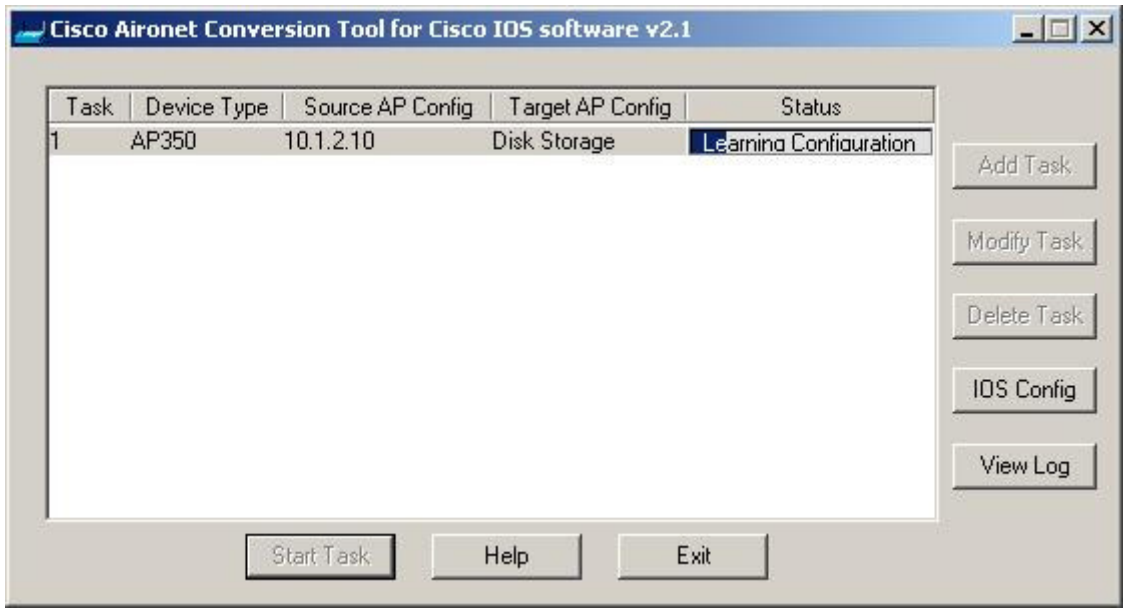


Figura 2-17 Generación de la configuración del punto de acceso

4.- Mediante el *conversion tool and image*, se extrae la configuración de seguridad del punto de acceso, se ingresa la clave del usuario para accesar a la configuración de seguridad (*security configuration*), es importante que el usuario sino es el administrador, debe tener privilegios en los puntos de acceso de administracion (*admin*), de escritura (*write*), y *firmware*, tal como se muestra en la Figura 2-18.

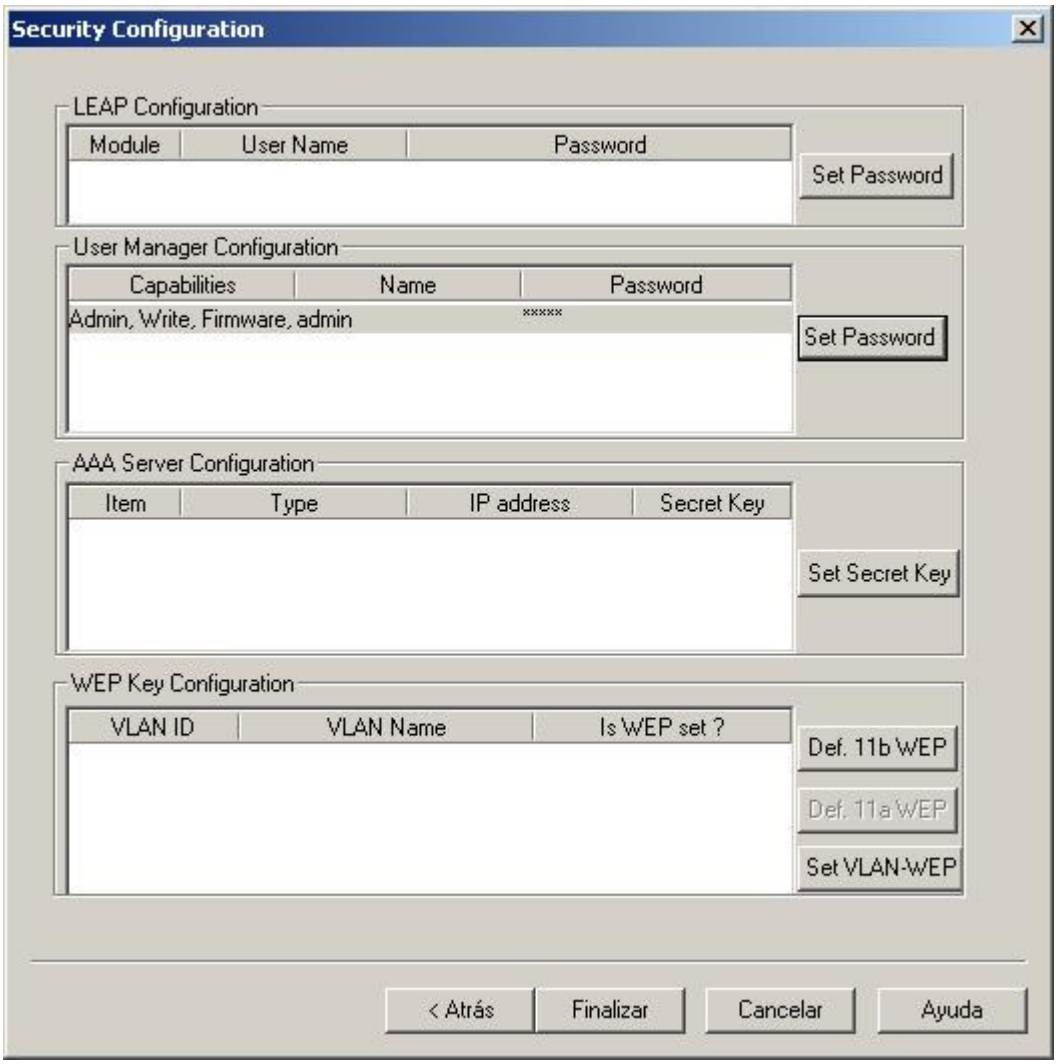


Figura 2-18 Ventana de *security configuration*

5.- Una vez generado y guardado el archivo de configuración (.cfg) en el disco duro del computador, se procede a realizar la conversión de *Vxworks* a *Cisco IOS* , ingresando la tarea en la ventana *device configuration*, como se muestra en la Figura 2-19.

Configuración fuente (*source configuration*)

Se utiliza el archivo de configuración que se generó anteriormente (.cfg) en el disco duro.

Configuración del destino (*target configuration*)

En este caso la fuente es el mismo punto de acceso, por lo cual se selecciona la opción *device*, y en la opción *helper image,* se indica la ruta en donde se descargó la imagen que corresponde al punto de acceso, que se señala en la Tabla 2-4.

Información del punto de acceso (*device information*)

Se ingresa la dirección ip del punto de acceso y la clave de administrador (admin).

Los demás campos de la ventana son opcionales.

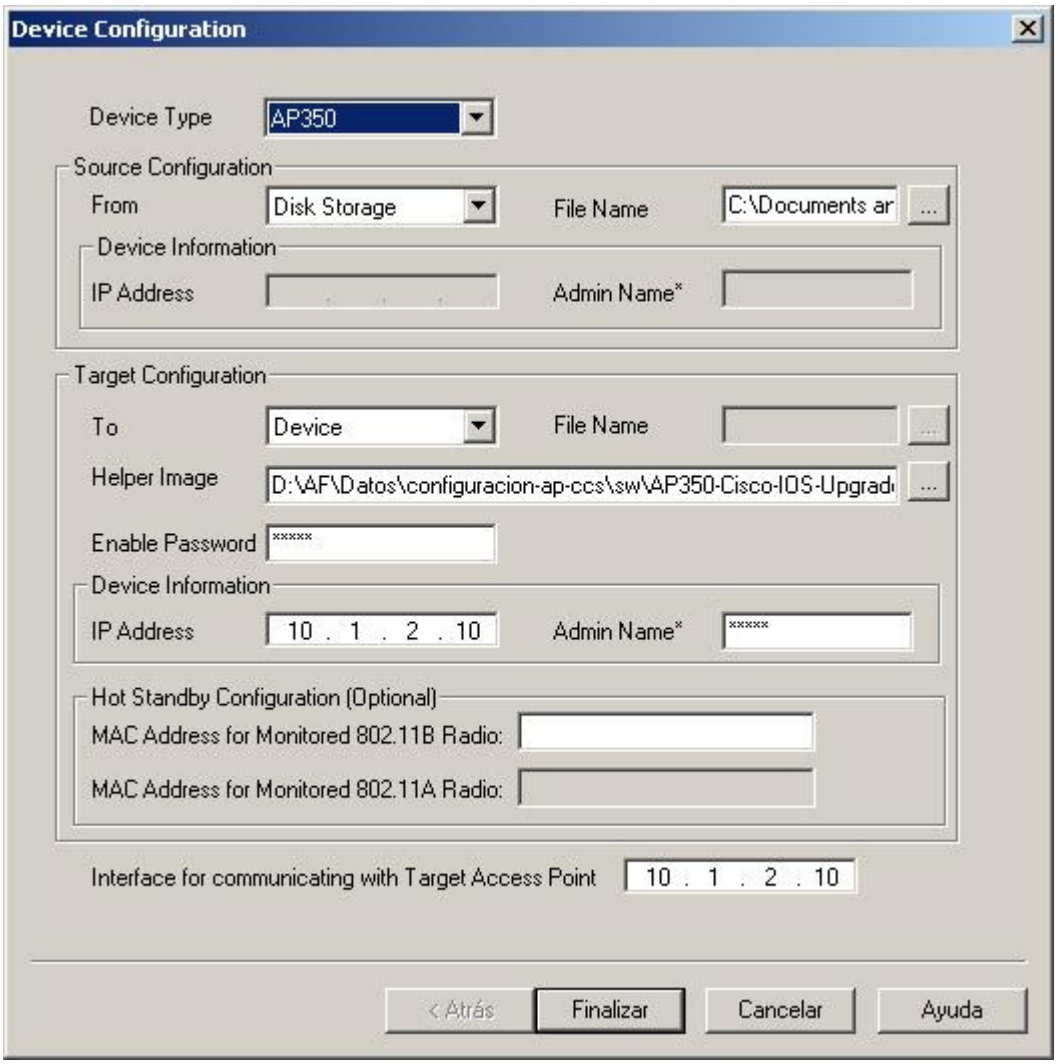


Figura 2-19 Conversión de *Vxworks* a *Cisco IOS*

6.- Luego que se han ingresado todos los parámetros señalados en la Figura 2-19, se procede a ejecutar la tarea como se muestra en la Figura 2-20. Cuando se realiza la conversión, es recomendable ver este proceso en consola, porque si ocurre un error es fácil de detectar.

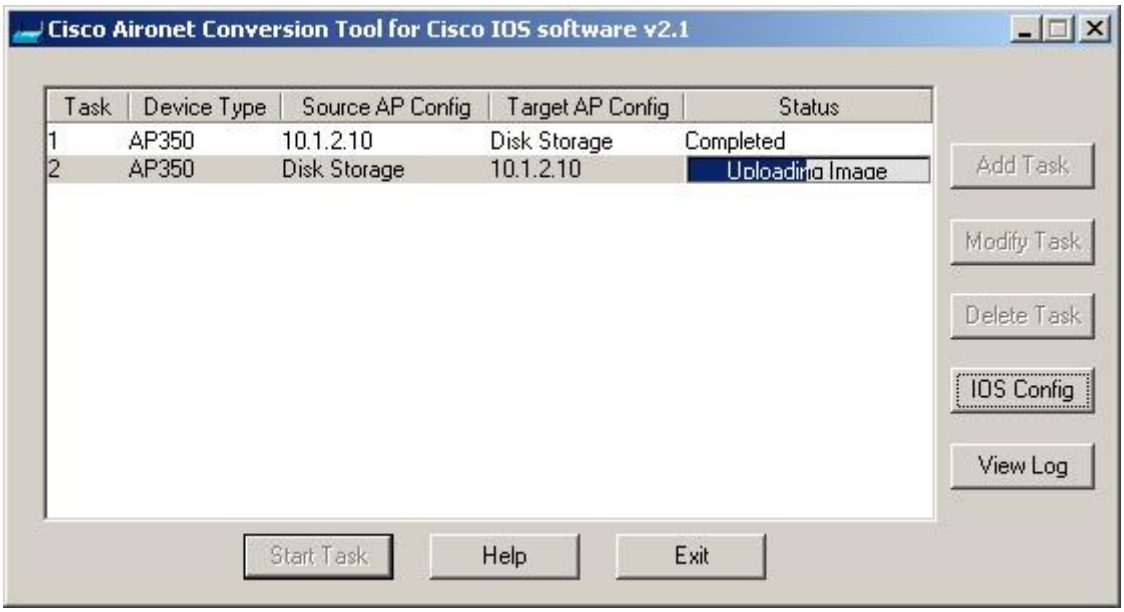


Figura 2-20 Tarea de conversión de *Vxworks* a IOS

7.- Cuando se ha completado la conversión la nueva versión del IOS del punto de acceso, es la documentada en la Tabla 2-4, y como se muestra en la Figura 2-21 y la Figura 2-22.

```
AP350-5e00e0>show version
Cisco Internetwork Operating System Software
IOS (tm) C350 Software (C350-K9W7-M), Version 12.2(13)JA1, EARLY DEPLOYMENT RELE
ASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Fri 14-Nov-03 15:08 by kellmill
Image text-base: 0x00003000, data-base: 0x00518D04

ROM: Bootstrap program is C350 boot loader
BOOTLDR: C350 Boot Loader (C350-BOOT-M) Version 12.2(13)JA, EARLY DEPLOYMENT REL
EASE SOFTWARE (fc1)

AP350-5e00e0 uptime is 4 minutes
System returned to ROM by power-on
System image file is "flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1"
```

Figura 2-21 Versión del IOS después de la conversión por consola

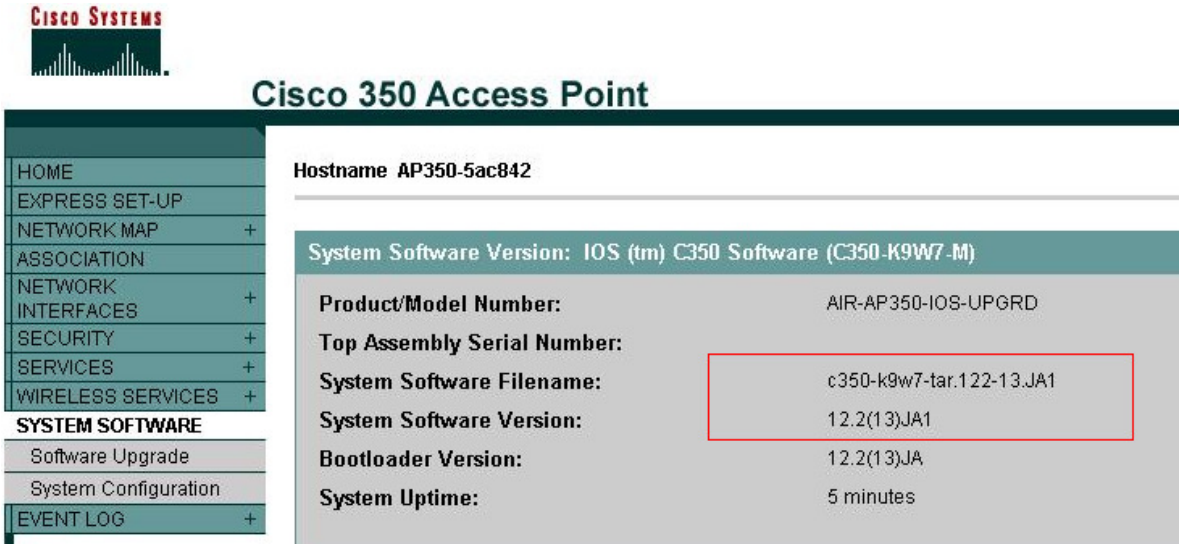


Figura 2-22 Versión del IOS después de la conversión por el *browser*

Una vez migrados los tres puntos de accesos a la versión de IOS correspondiente a la Tabla 2-4, y previo análisis documentado en la sección 3.2.3, se procedió a realizar la conversión del *firmware* correspondiente a la versión de IOS 12.3(8).JEA2 (GD). Los pasos que se realizaron en el proceso de actualización de *firmware* estan documentados en el trabajo, basados en la guía de referencia: "*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA*" [41] y el "*Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(8).JEA2"* [42].

Pasos realizados en la actualización de *firmware*:

1.- Descargar el *firmware* versión de IOS 12.3(8).JEA2 (GD), de la página de *web* de Cisco.

2.- Colocar el archivo descargado – c350-k9w7-tar.123-8.JEA2.tar, en el directorio del servidor tftp (*trivial file transfer protocol*), como se muestra en la Figura 2-23. TFTP, es un protocolo de transferencia muy simple semejante a una versión básica de FTP, se utiliza para transferir pequeños archivos.

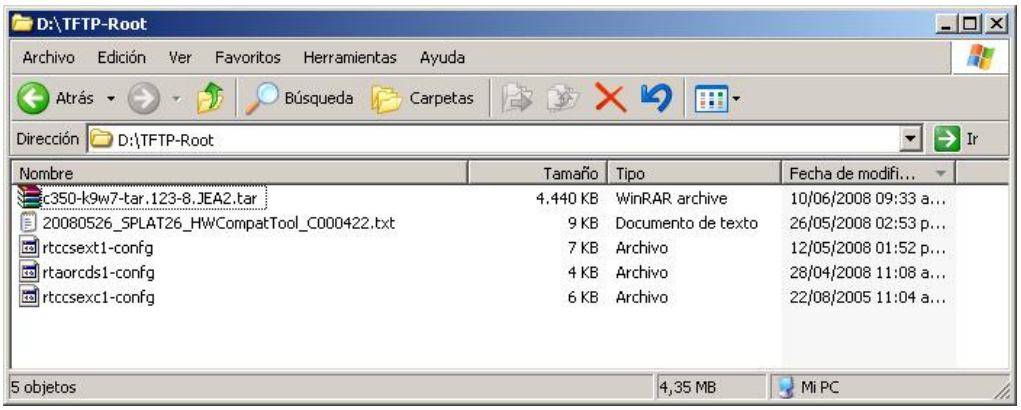


Figura 2-23 Carpeta de servidor tftp

3.- Levantar el servidor tftp para que se pueda transferir el *firmware* de la versión de IOS al punto de acceso y verificar que el archivo se encuentra en la carpeta *root* del servidor tftp, como se muestra Figura 2-24.

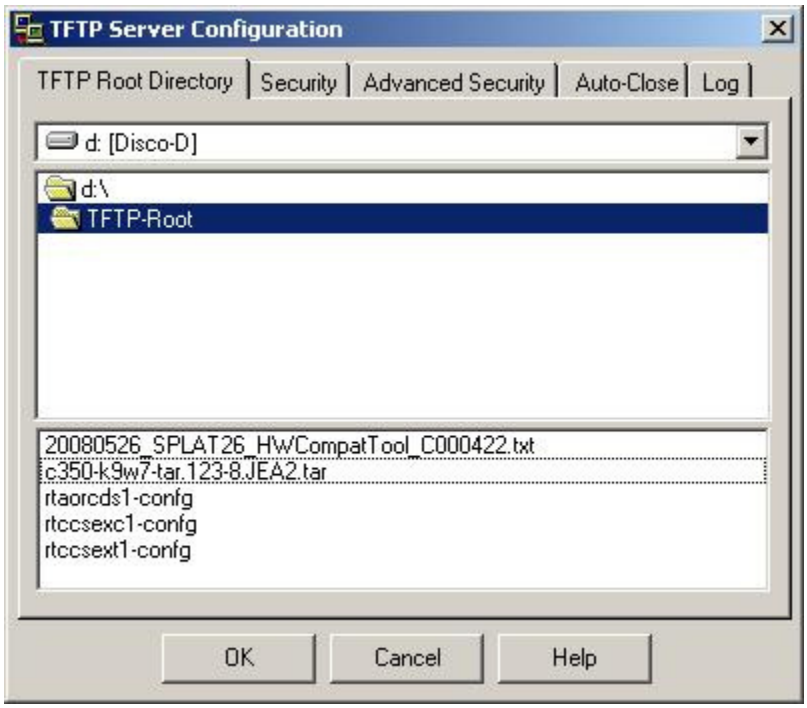


Figura 2-24 Servidor tftp

4.- Para ejecutar el *firmware* de la versión de IOS, no se debe descomprimir desde el *browser* sino desde consola, ya que se observa todo el proceso y en caso de alguna falla se determina la causa.

Desde consola, según señala la guía de referencia: "*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA*" [41], en la sección de "*working with software images",* si la transferencia del archivo se realiza vía tftp, se ejecuta el siguiente comando:

archive download-sw /overwrite /reload tftp:[[//location]/directory]/image-name ;

Lo que significa que se descarga la imagen al punto de acceso desde el servidor tftp y se sobreescribe la imagen actual, luego se realiza un reinicio automático del punto de acceso luego de la descarga de la imagen, si se han realizado cambios en el punto de acceso deberán salvarse antes porque sino se perderán.

En la Figura 2-25, se muestra el proceso del *upgrade* del *firmware* desde consola, la ejecución del comando antes mencionado, además de la carga de la imagen y la descompresión de archivos.

En la Figura 2-26, se muestra el final del *upgrade* del *firmware* , en este caso se realizaron cambios en el puntos de accesos que no se salvaron, por lo cual no se pudo realizar el reinicio del punto de acceso automáticamente sino manual.

```
AP350-5e00e0#$/reload tftp://10.1.2.15/tftp-root/c350-k9w7-tar.123-8.JEA2.tar
examining image...
Loading c350-k9w7-tar.123-8.JEA2.tar from 10.1.2.15 (via BVI1): !
extracting info (274 bytes)!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4546560 bytes]

Image info:
    Version Suffix: k9w7-.123-8.JEA2
    Image Name: c350-k9w7-mx.123-8.JEA2
    Version Directory: c350-k9w7-mx.123-8.JEA2
    Ios Image Size: 3891712
    Total Image Size: 4547072
    Image Feature: WIRELESS LAN
    Image Family: C350
Not enough free space to download w/o first deleting existing version...
Deleting flash:/c350-k9w7-mx.123-8.JEA2...done.
Extracting files...
Loading c350-k9w7-tar.123-8.JEA2.tar from 10.1.2.15 (via BVI1): !
extracting info (274 bytes)
c350-k9w7-mx.123-8.JEA2/ (directory) 0 (bytes)
c350-k9w7-mx.123-8.JEA2/html/ (directory) 0 (bytes)
c350-k9w7-mx.123-8.JEA2/html/level/ (directory) 0 (bytes)
c350-k9w7-mx.123-8.JEA2/html/level/1/ (directory) 0 (bytes)
extracting c350-k9w7-mx.123-8.JEA2/html/level/1/appsui.js (557 bytes)
extracting c350-k9w7-mx.123-8.JEA2/html/level/1/back.shtml (498 bytes)!
extracting c350-k9w7-mx.123-8.JEA2/html/level/1/cookies.js (5026 bytes)!
extracting c350-k9w7-mx.123-8.JEA2/html/level/1/forms.js (17542 bytes)!!!
extracting c350-k9w7-mx.123-8.JEA2/html/level/1/sitewide.js (15991 bytes)!!!!
extracting c350-k9w7-mx.123-8.JEA2/html/level/1/config.js (22242 bytes)!!!!
extracting c350-k9w7-mx.123-8.JEA2/html/level/1/stylesheet.css (3214 bytes)!
c350-k9w7-mx.123-8.JEA2/html/level/1/images/ (directory) 0 (bytes)
```

Figura 2-25 Proceso de *upgrade* del *firmware* desde consola

```
extracting c350-k9w7-mx.123-8.JEA2/info (274 bytes)00!
extracting info.ver (274 bytes)000000
[OK - 4546560 bytes]

New software image installed in flash:/c350-k9w7-mx.123-8.JEA2
Configuring system to use new image...done.
Requested system reload skipped due to unsaved config changes.
AP350-5e00e0#_
```

Figura 2-26 Final del *upgrade* del *firmware* desde consola

Además, del proceso que se ejecuta en la consola se puedo observar en el servidor tftp los eventos de envio del archivo, como se indica en la Figura 2-27.

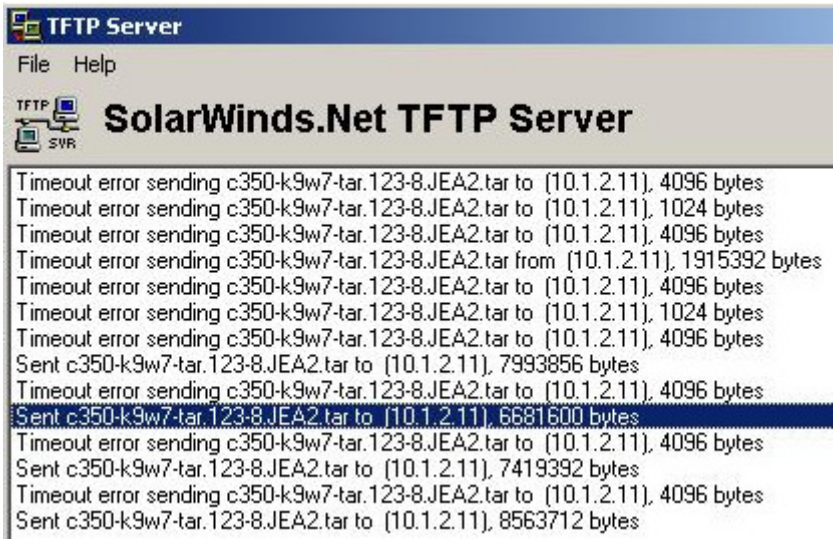


Figura 2-27 Eventos en el servidor tftp

Cuando ya ha finalizado el evento de *reload* (reinicio) del punto de acceso, todas las configuraciones quedan actualizadas en el equipo, se puede ejecutar el comando *show version* desde la consola o desde el *browser* se puede ver la nueva version del IOS que se actualizó 12.3(8).JEA2, como se muestra en la Figura 2-28 (ver página 114).

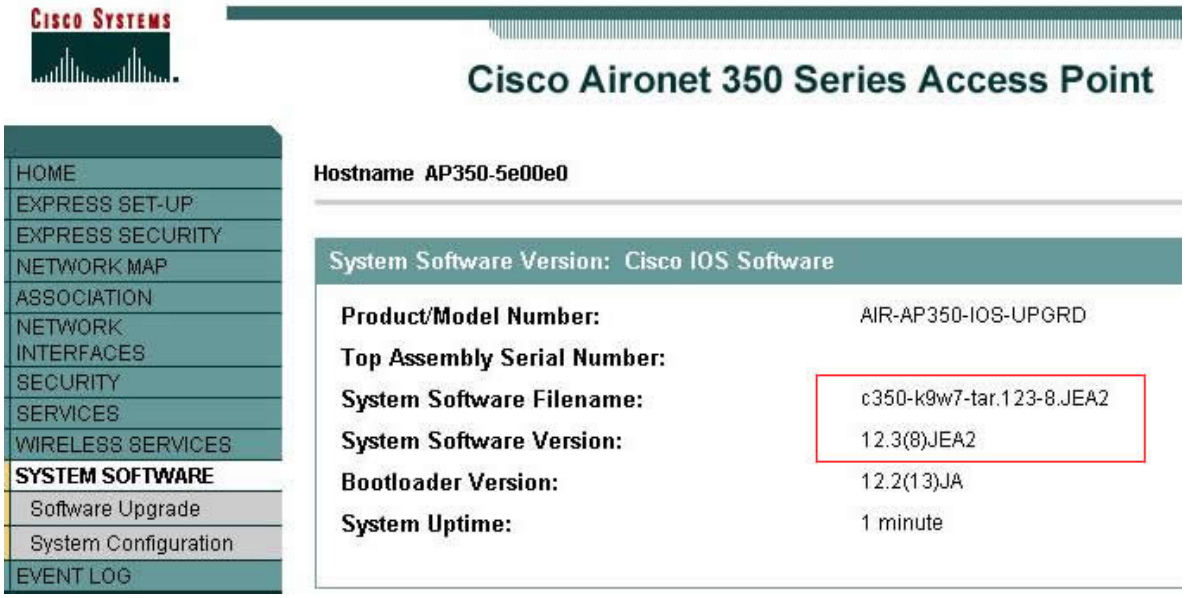


Figura 2-28 Versión de IOS 12.3(8).JEA2

2.3.3 - Evaluación e Implementación de normas, estándares, mecanismos de seguridad y mejores prácticas de la industria así como recomendaciones del fabricante en materia de redes inalámbricas que sean aplicables al proyecto en función de la información obtenida en la etapa de análisis y documentación.

El primer paso en la creación de una WLAN segura es establecer una estrategia empresarial para su instalación y utilización. Para este proyecto la estrategia abarcó las siguientes áreas:

- Determinar las necesidades de la empresa: ¿Cuáles son las motivaciones y necesidades de la empresa? Identificar claramente los objetivos y asegurarse de que los beneficios superan los riesgos.

- Integrar las políticas inalámbricas a las actuales políticas del departamento de TI. Las soluciones inalámbricas son una extensión de la red alámbrica.

- Definir claramente la propiedad de las WLAN: con ello se garantiza control y respuesta cuando se identifican las amenazas a la seguridad y se bloquean los ingresos de accesos furtivos.

- Proteger la infraestructura existente: es importante no poner los dispositivos inalámbricos directamente en la red interna, sino suministrar una WLAN separada con *gateways* muy controlados a la red principal.

- Educar a los usuarios sobre las políticas inalámbricas: incluye instruir a los empleados en la configuración de sus dispositivos para que tengan acceso de manera segura a la red.

Se pueden hacer varias recomendaciones para diseñar una red inalámbrica e impedir lo máximo posible el ataque de cualquier intruso. Lo más importante, es no utilizar excesivas normas de seguridad, porque podría reducir la rapidez y la utilidad de la red inalámbrica.

En la sección 2.2.1 - de documentación, se señalan las soluciones para una WLAN según el fabricante (Cisco) y las posibles mejores prácticas de la industria tecnológica, con esta información se definió cual es el esquema que se adapta a este proyecto. Además de seleccionar mecanismos de seguridad que minimicen los riesgos a un nivel aceptable y se pueda garantizar el acceso a la infraestructura WLAN.

2.3.3.1- Solución para WLAN según Cisco

Luego de analizar las soluciones que plantea el fabricante, se seleccionaron dos, de acuerdo a los requerimientos planteados en el escenario propuesto en la Tabla 2-3 (ver página 99), donde establece que se brindará acceso a Internet a los usuarios corporativos, a través de sus dispositivos personales y de la empresa, y además a los usuarios corporativos vía VPN a la empresa de los socios.

Por otro lado, el personal de la gerencia de Tecnología de Información, señaló que la empresa no disponía de capital para invertir en una solución que implicará un gasto que no estaba contemplado en su presupuesto, por lo cual la solución debía orientarse a reforzar la seguridad y los accesos con los equipos que están en este momento pero garantizando la confidencialidad de la información de la empresa.

Por esta razón se decidió implementar una solución que no implique ningún costo a nivel de *hardware* para la empresa, y que garantice un nivel de seguridad aceptable y entre las planteadas por el fabricante tenemos, la solución nro 2 definida en:

- A) Seguridad básica, basada en SSID, WEP y autenticación de direcciones MAC
- B) Seguridad básica con clave WPA precompartida

Para el caso de los usuarios corporativos que se van a conectar vía VPN, se decidió establecer la solución de seguridad nro 2.a, ya que el software para establecer la VPN con las empresas socias no soportaba WPA.

Para el caso de los usuarios corporativos que utilizaran sus dispositivos personales y los visitantes (proveedores, contratistas y otro usuario que no pertenezca a la empresa), se decidió establecer la solución de seguridad nro 2.b, ya que garantiza un buen nivel de seguridad que los puntos de accesos pueden soportar luego de realizar la migración de la imagen. La norma WPA tiene como objetivo solucionar todas las deficiencias de la WEP; combina la autenticación de usuario (que la WEP no suministró) con un elemento de encriptación más fuerte denominado Protocolo de Integridad Clave Temporal (TKIP).

2.3.3.2- Mejores prácticas y su configuración de seguridad

Obviamente la seguridad de las redes inalámbricas no se garantiza solo con normas. Los profesionales de seguridad de la información se preocupan con razón por muchos tipos de ataques que se pueden lanzar contra las WLAN, como por ejemplo la intercepción del tráfico, ataques de "tercero interpuesto", negación de servicio y secuestro de una sesión para nombrar unos pocos. Afortunadamente, muchos riesgos se pueden mitigar siguiendo prácticas básicas de seguridad inalámbrica con tecnologías de protección a clientes y a nivel empresarial.

Aparte de la solución definida en la sección anterior, se aplicaron ciertas normas y políticas de seguridad que nos ayudarían a mantener una red más segura y que están definidas como las posibles mejores prácticas de la industria tecnológica en WLAN, en la sección 2.2.1.2- , las cuales fueron aplicadas de la siguiente manera:

1.- Control en el área de transmisión y cierre de todos los puntos de acceso: se realizaron pruebas en las áreas externas de los pisos y los ascensores con el punto de acceso para determinar hasta donde llegaba su alcance, y se determinó que la señal no era fuerte en el área de ascensores y pasillo, una posible área de riesgo para la conexión de intrusos, lo importante era reducir la propagación de las ondas de radio fuera de la empresa.

2.- El *hardware* es del mismo distribuidor Cisco, todos los puntos de accesos son modelo 350 Cisco como se muestra en Tabla 2-1 (ver página 68).

3.-Uso del SSID inteligentemente. El SSID por defecto de los puntos de accesos, ya estaba cambiado, ya que por ser equipo Cisco, su SSID original era tsunami. Se configuró el SSID público denominado "CCC" (nombre ficticio en este documento por efectos de seguridad) para los usuarios corporativos y visitantes y el SSID "BBB" (nombre ficticio en este documento por efectos de seguridad) que no es visible para los usuarios. Además, se inhabilitó la emisión *broadcast* del SSID "BBB" que no es público pero si se dejó habilitada para el SSID "CCC" público. Se decidió colocar estos SSID con nombres muy coloquiales, que no hicieran referencia a la empresa ni tampoco al tipo de equipo inálambrico. Ver la Figura 2-31 (página 121).

4.-Explorar con regularidad los puntos de acceso atacantes. Este punto no se tomó en cuenta en el desarrollo de este proyecto.

5.-Implementación de autenticación de usuario. Este punto no se tomó en cuenta en el desarrollo de este proyecto, ya que no se disponía de una plataforma a nivel de *hardware*, es decir, no hay servidores que puedan servir para autenticar a los usuarios.

6.-Protección de la WLAN con la tecnología "*VPN Ipsec*" o tecnología "*VPN clientless*". Este punto no se tomó en cuenta en el desarrollo de este proyecto.

7.-Uso de autenticación de direcciones MAC (Control de Acceso a Medios de transmisión). Este control se realizaba en la imagen anterior del punto de acceso, luego de realizar la migración de imagen, también se decidió implantar este filtrado a través de direcciones MAC, ya que garantizaba un nivel de seguridad mínimo.

8.-Activación del mayor nivel de seguridad que soporte el *hardware*. Se implementó WEP con una encriptación de 128 bits para los casos de los usuarios corporativos que acceden a través de VPN a la empresa de los socios y WPA para los visitantes y usuarios corporativos que se conectan con sus dispositivos personales.

9.-Instalación de *firewalls* personales y protección de antivirus en todos los dispositivos móviles. Esta práctica se anexo como norma principal para la conexión de cualquier equipo a la WLAN corporativa.

10.-Instalación de tecnologías de protección de clase empresarial, implica emplear un *firewall* en la zona desmilitarizada y clientes *firewalls* en todos los equipos de escritorio. Este punto se desarrollará en la sección 2.3.4 - (ver página 118).

Además de evaluar e implantar las posibles mejores prácticas que se adaptaron para este proyecto, también se consideraron indispensables incluir las siguientes normas y/o estándares:

- Actualización de la imagen de los puntos de acceso para reforzar el sistema de seguridad de la solución *wireless*. Se visitó el sitio *web* del fabricante del dispositivo para conocer la versión más actualizada de la imagen para así garantizar que la red inalámbrica sea más segura y confiable. Esta actividad se realizó en la sección 2.3.2 -

- Proporcionar un entorno físicamente seguro a los puntos de accesos, en donde ningún empleado pueda acceder a ellos y desactivarlos cuando se haya un periodo de inactividad largo (ejemplo: vacaciones colectivas). Los equipos se ubicaron físicamente en un lugar donde los usuarios no pueden acceder fácilmente y se decidió no desactivarlos en ningún momento, sino reforzar la seguridad de los mismos, con los medidas mencionadas anteriormente.

- Protección lógica de los equipos, se reubicaron lógicamente los puntos de accesos, ya que los mismos se encontraban en el mismo segmento de red de los servidores y estaciones de trabajo. Este punto se ampliará más en la sección 2.3.4 - (ver página 118).

2.3.4 - Cambios físicos y lógicos que se aplicaron a la infraestructura de redes a fin de permitir las conexiones inalámbricas de usuarios corporativos así como usuarios no corporativos en todas las áreas de interés.

En la sección 2.1.3 - (ver página 69), se identificó la estructura lógica y física de la red inalámbrica, antes de realizar los cambios.

En esta sección, se analizarán los cambios físicos y lógicos que se realizaron en la infraestructura WLAN, para cumplir con los objetivos del proyecto. Entre los cambios físicos, esta la reubicación de los puntos de accesos, ya que anteriormente se encontraban en estaciones de trabajo visibles y al alcance de los usuarios, ahora están en un área donde no hay puestos de trabajos y no está visible a los usuarios, aunque no es la ubicación ideal para estos equipos, se estableció esta por efectos de ahorre de costos.

Los cambios lógicos que se realizaron fueron los siguientes:

- Reubicación de los puntos de accesos en otro segmento de red, con protección de un *firewall* y en una zona aislada de los servicios internos de la empresa, como se muestra en Figura 2-29. Implicando cambio de direccionamiento IP, máscara y restricciones de acceso para la administración en los puntos de accesos.

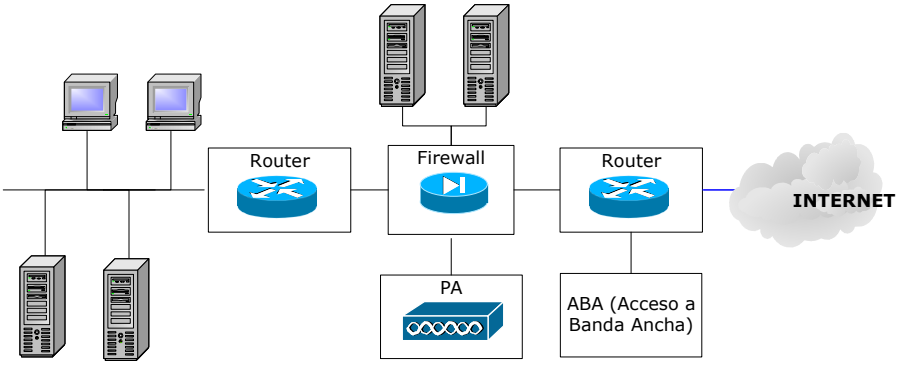


Figura 2-29 Diagrama lógico de la red final

- El *firewall*, que se muestra en la Figura 2-29 (ver página 119), funciona como enrutador y *firewall*, es decir el punto de acceso desvía el tráfico de la red inalámbrica a través del *firewall*, se dispone de un servidor DHCP instalado en el punto de acceso que asigna direcciones IP a los clientes inalámbricos entre el rango X.X.X.X - Y.Y.Y.Y con máscara Z.Z.Z.0. De esta manera el usuario que se conecte a la red inalámbrica no tiene que realizar ninguna configuración IP de su tarjeta de red, únicamente indicar que tome la configuración IP automática.

- El punto de acceso dispone de dos interfaces de red, una interfaz conecta con la red inalámbrica (interfaz LAN) y la otra con la red cableada directamente al servidor (interfaz WAN), por seguridad para la empresa no se puede anexar la

configuración de direcciones IP para ambas interfaces. Ver Figura 2-35 (ver página 124)

- En el punto de acceso, se realizó la configuración de los *bridge-groups* de la interfaz *Fast Ethernet* (*Fast 0*) con la interfaz radio (*Dot11Radio0*). En la Figura 2-30 (ver página 120), se muestra un diagrama lógico de la asociación de cada *bridge-group,* el cual esta identificado con un color para ver gráficamente como es esta asociación.

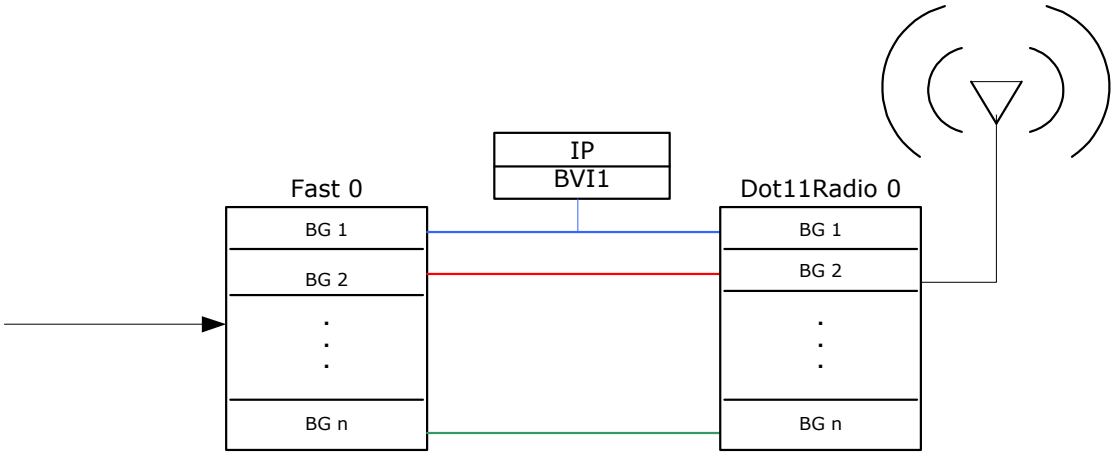


Figura 2-30 Diagrama lógico de los *bridge-groups*

- El tráfico de información viaja de forma separada a través del uso de VLANS, una en la categoría de administración (VLAN 3), otra de usuarios corporativos para conectarse con las empresas socias a través de VPN (VLAN 2) y otra en modo de visitante activada como *guest mode* (VLAN 4) y en los SSID configurados en los equipos. En la Figura 2-32 (ver página 122), se muestra la definición de esas VLANS

- El nombre asignado a la red inalámbrica (SSID) para visitantes o público se denomina "CCC" (nombre ficticio en este documento por efectos de seguridad), y el canal utilizado el 11. Lo único que tienen que hacer los usuarios es buscar la red desde la estación inalámbrica y asociarse a la misma con su clave WPA. El canal elegido es el 11 para no provocar interferencias con otras redes inalámbricas cercanas a la zona.

2.3.5 - Configuración de los equipos inalámbricos existentes tomando en consideración los requisitos físicos, lógicos y de seguridad anteriores.

En esta sección, se explicará en algunos segmentos de configuración de los equipos, los siguientes puntos:

- Los cambios que se realizaron en los puntos de acceso para mejorar la seguridad.
- Las configuraciones que se realizaron para que pudiesen conectarse los equipos corporativos y no corporativos dentro de la misma infraestructura inalámbrica.

Según lo señalado en la sección 2.3.3.1- y en la sección 2.3.3.2- se configuraron el SSID denominado "BBB" (nombre ficticio en este documento por efectos de seguridad) y SSID "CCC" (nombre ficticio en este documento por efectos de seguridad) público, como se muestra en la Figura 2-31 Configuración de SSIDspágina 121), con autenticación de seguridad WEP y WPA respectivamente.

```
! Configuración del ssid BBB, en la vlan 2, con autenticación abierta y con
! seguridad WEP (para usuarios con laptop de socios)
dot11 ssid BBB
   vlan 2
   authentication open
   authentication key-management wep
   wep ascii 7 [confidencial]

! Configuración del ssid CCC, en la vlan 4, con autenticación abierta y con
! seguridad WPA-PSK, en modo de visitante o de acceso público (para accesos a
! visitantes/usuarios corporativos)
dot11 ssid CCC
   vlan 4
   authentication open
   authentication key-management wpa
   guest-mode
   wpa-psk ascii 7[confidencial]
```

Figura 2-31 Configuración de SSIDs

Para segmentar el tráfico entre los usuarios empleados internos, los usuarios visitantes y la administración de los puntos de accesos se definieron 3 tipos de VLAN, solucionando la vulnerabilidad identificada en la sección 2.2.2 (ver página 79). En la Figura 2-32 (ver página 122), se identifican las VLAN 2, 3 y 4.

```
! Definición de la VLAN: XXX en la vlan 2 (para los usuarios empleados internos)
dot11 vlan-name XXX vlan 2
! Definición de la VLAN: YYY en la vlan 3 (para administración de la red inálambrica)
dot11 vlan-name YYY vlan 3
! Definición de la VLAN: ZZZ en la vlan 4 (para acceso a Internet a través del uso del
! acceso a banda ancha)
dot11 vlan-name ZZZ vlan 4
```

Figura 2-32 Definición de VLANS en los puntos de acceso

En la Figura 2-33 (ver página 122), mejora la protección de datos y control de acceso, pudiendo decirse que el nivel de protección es alto ya que mejora el cifrado de datos mediante TKIP, en la vlan 2 y vlan 4, según lo señalado en la sección 1.6.2.2- (ver página 50)

```
! Configuración de la interfaz radio 0, con encriptación tkip en la vlan 2 y 4, para los
! ssid BBB y CCC
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 2 mode ciphers tkip
 !
 encryption vlan 4 mode ciphers tkip
 !
 ssid BBB
 !
 ssid CCC
 !
 speed basic-1.0 2.0 5.5 11.0
 station-role root
 rts threshold 2312
 no dot11 extension aironet
```

Figura 2-33 Encriptacion tkip en las vlan 2 y 4

En la Figura 2-34 (ver página 123) y la Figura 2-35 (ver página 124), se identifican las configuraciones de las sub-interfaz radio y *fastEthernet* 0.25, 0.50 y 0.66, señalando, la VLAN de configurada en cada caso y el *bridge-group* al cual pertenecen, garantizando la segmentación de tráfico señalada anteriormente.

```
! Configuración de la sub-Interfaz radio 0.25, con vlan 2 y el bridge-group 2
!
interface Dot11Radio0.25
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
 bridge-group 2 spanning-disabled
!
! Configuración de sub-Interfaz radio 0.50, con vlan 3 nativa y el bridge-group 1
!
interface Dot11Radio0.50
 encapsulation dot1Q 3 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
! Configuración de sub-Interfaz radio 0.66, con vlan 4 y el bridge-group 4
!
interface Dot11Radio0.66
 encapsulation dot1Q 4
 no ip route-cache
 bridge-group 4
 bridge-group 4 subscriber-loop-control
 bridge-group 4 block-unknown-source
 no bridge-group 4 source-learning
 no bridge-group 4 unicast-flooding
 bridge-group 4 spanning-disabled
```

Figura 2-34 Configuración de la sub-Interfaz radio 0.25, 0.50 y 0.66

```
!
! Configuración de Interfaz fastEthernet 0 con full duplex y a una velocidad de 100
!(Interfaz física de la conexión del punto de acceso a la red cableada)
!
interface FastEthernet0
 no ip address
 no ip route-cache
 speed 100
 Full-duplex
!
! Configuración de la Sub-Interfaz fastEthernet 0.25, con la vlan 2 y bridge-group 2
!
interface FastEthernet0.25
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 no bridge-group 2 source-learning
 bridge-group 2 spanning-disabled
!
! Configuración de la Sub-Interfaz fastEthernet 0.50, con la vlan 3 y bridge-group 1
!
interface FastEthernet0.50
 encapsulation dot1Q 3 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
! Configuración de la Sub-Interfaz fastEthernet 0.66, con la vlan 4 y bridge-group 4
!
interface FastEthernet0.66
 encapsulation dot1Q 4
 no ip route-cache
 bridge-group 4
 no bridge-group 4 source-learning
 bridge-group 4 spanning-disabled
!
```

Figura 2-35 Configuración de las sub-interfaz fastEthernet

En los objetivos de este proyecto no contempla, la utilización de autenticación de usuarios con servidor TACACS o RADIUS, ya que no se dispone de una plataforma a nivel de *hardware* robusta que pueda soportar todas las configuraciones de seguridad necesarias en ese equipo, pero se realizaron algunas pruebas, configurando parámetros de autenticación, autorización y administración básicos que se muestran en la Figura 2-36 (ver página 125) y en la Figura 2-37 (ver página 125) que más adelante podrían servir de continuidad cuando se tenga la plataforma adecuada para seguir desarrollando este punto.

```
! Definición de los parámetros de autenticación, autorización y administración
!(autenticación en el servidor Tacacs para la administración del equipo)
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login AAA_LOCAL local
aaa authentication login AAA_REMOTO group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa session-id common
!
```

Figura 2-36 Definición de parámetros de AAA

```
! Indice de interfaz SNMP
!
snmp-server ifindex persist
!
! Acceso vía SSH al servidor Tacacs
!
tacacs-server host [confidencial] key [confidencial]
tacacs-server directed-request
!
control-plane
!
bridge 1 route ip
!
!
banner exec ^C
!
line con 0
 exec-timeout 5 0
!
! Autenticación al servidor Tacacs para efectos de administración con el usuario local y
! remoto
!
 login authentication AAA_LOCAL
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 login authentication AAA_REMOTO
 transport input ssh
 transport output none
line vty 5 15
 exec-timeout 5 0
 login authentication AAA_REMOTO
 transport input ssh
 transport output none
!
sntp server [confidencial]
end
```

Figura 2-37 Acceso vía SSH al servidor Tacacs

2.3.6 - Elaboración de documentos para usuarios y personal técnico, con el fin de facilitar el uso y administración de la red inalámbrica.

En el desarrollo de este trabajo, se realizaron dos guías rápidas:

- La "guía rápida para acceder a la WLAN de Ypergas (usuarios visitantes)", la cual indica paso a paso cómo deberían conectarse a la red los usuarios visitantes, muestra de manera gráfica y sencilla la conexión a la WLAN corporativa. Para mayor información consulte Anexo A.

- La "guía de configuración de los puntos de accesos de la WLAN (para personal de IT)", el propósito de esta guía es documentar la configuración realizada en los equipos inalámbricos para el personal técnico sin necesidad de acceder a los mismos. Para mayor información consulte Anexo B.

CAPÍTULO 3 - CONCLUSIONES Y RECOMENDACIONES

Al finalizar este trabajo se han obtenido importantes conclusiones, una de ellas y tal vez la más importante es que para el mejoramiento y actualización de la plataforma WLAN corporativa de YPergas, no se necesita grandes inversiones económicas ni tecnología de punta, pues contando con recursos limitados se ha logrado desarrollar el presente proyecto.

Con este fin, se habían propuesto la consecución de seis objetivos fundamentales:

1.-Describir el uso actual de las redes inalámbricas en la empresa YPergas.

2.-Precisar y determinar los potenciales riesgos de seguridad que presentan actualmente las redes inalámbricas en la empresa YPergas.

3.-Evaluar e implementar cambios necesarios en los equipos inalámbricos, tomando en cuenta la reutilización de equipos, mejoramiento de seguridad, facilidad de uso y administración y cobertura en las áreas de interés.

4.-Configurar conexiones de equipos corporativos y equipos no corporativos dentro de la misma infraestructura inalámbrica.

5.-Elaborar documentos para usuarios y personal técnico, con el fin de facilitar el uso y administración de las redes inalámbricas.

6.- Especificar el desarrollo general del proyecto.

En el objetivo 1, se realizó una revisión de la documentación existente en la empresa acerca de la plataforma WLAN, además se hizo un levantamiento de información de *software* y *hardware*, se identificó la topología física y lógica de la red y se determinó el uso que se le estaba dando a la misma. En esta parte del trabajo, se evalúo el escenario que estaba presente en ese momento, notando que existían equipos que no se le estaba dando el uso correcto dentro de la empresa, además muy pocos usuarios conocian la red, ya que los administradores, manifestaron no haber difundido el uso de ésta, porque no garantizaba las condiciones de seguridad, para permitir el acceso a Internet, y a la información de la empresa.

En el objetivo 2, se identificaron los potenciales riesgos de seguridad que presentaba la WLAN, identificando y analizando las vulnerabilidades presente en los equipos, para este punto se realizó una revisión de *hardware* y *software*, la cual reflejó que a pesar de que no se tienen equipos de última tecnología, se podían realizar actualizaciones de *software* que permitieran brindar un mejor esquema de seguridad en la WLAN, para lo que se hizo un análisis de las posibles actualizaciones de acuerdo a los equipos inálambricos presentes y se determinó la que mejor se adaptaría a los requerimientos de *hardware*.

En el objetivo 3, se evaluaron e implementaron los cambios necesarios en los equipos inalámbricos, reutilizando la misma plataforma de *hardware*, garantizando un mejoramiento de seguridad, para este punto se contempló la elaboración e implantación de un diseño orientado a las soluciones en materia de WLAN según el fabricante presente en la empresa, se eligieron las que se adaptaban a los requerimientos de conexión para usuarios corporativos y no corporativos, utilizando un esquema para cada caso, identificados en la sección 2.3.1.2- (ver página 97), además se realizaron actualizaciones de *software* y configuraciones de seguridad que se adaptaban a la nueva versión de *IOS* de los puntos de accesos. Además, se tomaron en consideración algunas mejores prácticas de la industria en materia de WLAN.

En el objetivo 4, se configuraron los equipos inálambricos y se realizaron cambios físicos y lógicos en la WLAN, para garantizar la conexión de usuarios corporativos y no corporativos a la misma red, se definieron esquemas de configuración en los equipos orientados a la segmentación de tráfico tomando en cuenta la protección de la información corporativa en el caso de usuarios no corporativos.

En el objetivo 5 y 6, se elaboraron guía rápidas documentadas en los anexos A y B, para facilitar el uso y la administración adecuada de la WLAN, además se documentaron las entrevistas realizadas al personal de la empresa en la etapa de evaluación, y el diseño, elaboración e implantación de la solución de este trabajo.

Se puede concluir que la estrategia definida, contempló la revisión detallada de los puntos de accesos a nivel de ubicación física, lógica, actualización de *software* y de los mecanismos de seguridad que presentaba en ese momento. En este trabajo se hicieron las actualizaciones necesarias en los equipos, además de seleccionar y configurar los

mecanismos de seguridad que se adaptaran a los mismos y la elaboración e implantación del diseño orientado a una solución según el fabricante y las mejores prácticas de la industria, tomando en cuenta los requerimientos de conexión para equipos corporativos y no corporativos, que definieron el nuevo ambiente de seguridad inalámbrico de la empresa.

Durante el desarrollo del trabajo fueron surgiendo ideas para incorporar al diseño para mejorar y actualizar la WLAN corporativa. Estas ideas fueron pasando a un segundo plano por no estar directamente relacionadas con el trabajo, éstas se resumen a continuación pues conforman un grupo importante de recomendaciones que pueden dar valor agregado:

- Se considera importante definir otra VLAN en los equipos inálambricos sólo para uso del personal de la gerencia de Tecnología de Información, que pueda acceder a la información.

- La empresa considere importante invertir en un servidor de autenticación robusto, para poder emplear autenticación entre usuarios con EAP-FAST, la cual es soportada por la imagen de los puntos de accesos.

- Se debería considerar incorporar este esquema de WLAN a la otra sede de la empresa ubicada en Altagracia de Orituco, ya que allí viajan muchos usuarios corporativos y no corporativos de Caracas y no existen muchos puntos cableados para brindar un servicio a todos.

- Se debería realizar la reubicación física de los puntos de accesos en zonas adecuadas y protegidas, aunque en el trabajo se realizó la reubicación de los equipos que se encontraban en puestos de trabajos visibles al público en zonas menos accesibles, se debe considerar una ubicación con precintos de seguridad o a nivel del techorazo para que no pueda influir el factor humano.

CAPÍTULO 4 - GLOSARIO DE TERMINOS

• PA – *Access Point*, punto de acceso, estación base de una red Wi-Fi que conecta clientes inalámbricos entre sí y a redes de cable.

• *Beacon frames*/*Beacons*/Balizas – tramas de administración o sondas que emiten los puntos de acceso para informar a sus clientes o a otros puntos de acceso de su presencia y de otros datos.

• CCMP – *Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol*, protocolo de encriptación utilizado en WPA2, basado en la suite de cifrado de bloques AES.

• CRC – *Cyclic Redundancy Check*, pseudo-algoritmo de integridad usado en el protocolo WEP (débil).

• EAP – *Extensible Authentication Protocol*, entorno para varios métodos de autenticación.

• EAPOL – *EAP Over LAN*, protocolo usado en redes inalámbricas para transportar EAP.

• GEK – *Group Encryption Key*, clave para la encriptación de datos en tráfico *multicast* (también usada para la integridad en CCMP).

• GIK – *Group Integrity Key*, clave para la encriptación de datos en tráfico *multicast* (usada in TKIP).

• GMK – *Group Master Key*, clave principal de la jerarquía de *group key*.

• GTK – *Group Transient Key*, clave derivada de la GMK.

• HiperLAN -- es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz.

• ICV – *Integrity Check Value*, campo de datos unido a los datos de texto para la integridad (basado en el algoritmo débil CRC-32).

• IV – *Initialization Vector*, vector de inicialización, datos combinados en la clave de encriptación para producir un flujo de claves único.

• KCK – *Key Confirmation Key*, clave de integridad que protege los mensajes handshake.

• KEK – *Key Encryption Key*, clave de confidencialidad que protege los mensajes handshake.

• *Keystream* – una secuencia de caracteres seudo-aleatorios.

• MIC – *Message Integrity Code*, campo de datos unido a los datos de texto para la integridad (basdo en el algoritmo Michael).

• MK – *Master Key*, clave principal conocida por el suplicante y el autenticador tras el proceso de autenticación 802.1x.

• MPDU – *Mac Protocol Data Unit*, paquete de datos antes de la fragmentación.

• MSDU – *Mac Service Data Unit*, paquete de datos después de la fragmentación.

• OFDM–*Ortogonal Frequency Division Multiplexing*. División de frecuencia por multiplexacion ortogonal, Es una técnica de modulación FDM que permite transmitir grandes cantidades de datos digitales sobre una onda de radio.

• PAE – *Port Access Entity*, puerto lógico 802.1x.

• PMK – *Pairwise Master Key*, clave principal de la jerarquía de pares de claves.

• PSK – *Pre-Shared Key*, clave derivada de una frase de acceso que sustituye a la PMK normalmente enviada por un servidor de autenticación.

• PTK – *Pairwise Transient Key*, clave derivada de la PMK.

• RSN – *Robust Security Network*, mecanismo de seguridad de 802.11i (TKIP, CCMP etc.).

• RSNA – *Robust Security Network Association*, asociación de seguridad usada en una RSN.

• RSN IE – *Robust Security Network Information Element*, campos que contienen información RSN incluida en *Probe Response* y *Association Request*.

• SSID – *Service Set Identifier*, identificador de la red (el mismo que ESSID).

• STA – *Station*, estación, cliente wireless.

• TK – *Temporary Key*, clave para la encriptación de datos en tráfico unicast (usada también para la comprobación de la integridad de datos en CCMP).

• TKIP – *Temporal Key Integrity Protocol*, protocolo de encriptación usado en WPA basado en el algoritmo RC4 (como en WEP).

• TMK – *Temporary MIC Key*, clave para la integridad de datos en tráfico unicast (usada en TKIP).

• TSC – *TKIP Sequence Counter*, contador de repetición usado en TKIP (al igual que Extended IV).

• TSN – *Transitional Security Network*, sistemas de seguridad pre-802.11i (WEP etc.).

• WEP – *Wired Equivalent Privacy*, protocolo de encriptación por defecto para redes 802.11.

• WPA – *Wireless Protected Access*, implementación de una versión temprana del estándar 802.11i, basada en el protocolo de encriptación TKIP.

• WRAP – *Wireless Robust Authenticated Protocol*, antiguo protocolo de encriptación usado en WPA2.

CAPÍTULO 5 - REFERENCIA

[1] Institute of Electrical and Electronics Engineers:

http://www.ieee.org

[2] Grupo de trabajo de IEEE 802.11i:

http://grouper.ieee.org/groups/802/11/

[3] WI-FI Alliance.

http://www.wi-fi.org/

[4] European Telecommunications Standards Institute.

http://www.etsi.org/

[5] Internet Engineering Task Force.

http://www.ietf.org/

[6] RFC 2284. PPP Extensible Authentication Protocol (EAP).

http://www.ietf.org/rfc/rfc2284.txt

[7] FCC *Federal Communications Commission*

http://www.fcc.gov/

[8] RFC 3748. Extensible Authentication Protocol (EAP).

http://www.ietf.org/rfc/rfc3748.txt

[9] FCC *Federal Communications Commission*

http://www.fcc.gov/

[10] RFC 2058 Remote Authentication Dial In User Service (RADIUS)

http://rfc.net/rfc2058.html

[11] RFC 2404 Uso de HMAC-SHA-1-96 en ESP y AH

http://www.rfc-es.org/rfc/rfc2404-es.txt

[12] RFC 2246 *The TLS Protocol Version* 1.0

http://www.ietf.org/rfc/rfc2246.txt

[13] RFC 1334 *PPP Authentication Protocols*

http://www.ietf.org/rfc/rfc1334.txt

[14] RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)

http://www.ietf.org/rfc/rfc1994.txt

[15] RFC 2759 Microsoft PPP CHAP Extensions, Version 2

http://www.ietf.org/rfc/rfc2759.txt

[16] RFC 2548 Microsoft Vendor-specific RADIUS Attributes

http://www.ietf.org/rfc/rfc2548.txt

[17] RFC 1321 *The MD5 Message-Digest Algorithm*

http://www.ietf.org/rfc/rfc1321.txt

[18] RFC 2058 Remote Authentication Dial In User Service (RADIUS)

http://www.faqs.org/rfcs/rfc2058.html

[19] Computer Security Resource Center, National Institute of Standards and Technology:

http://csrc.nist.gov

[20] RFC 3610 Counter with CBC-MAC (CCM)

http://www.rfcsearch.org/rfcview/RFC/3610.html

[21] Seguridad en redes inalámbricas 802.11, por Juan Manuel Molina

http:// http://dspace.icesi.edu.co/dspace/bitstream/item/888/1/sist_telema3.pdf

[22] Protocolos de seguridad en redes inalámbricas, por Saulo Barajas

http://www.saulo.net/pub/inv/SegWiFi-art.htm

[23] Protocolos de seguridad en redes inalámbricas 2, por Saulo Barajas

http://www.saulo.net/pub/inv/SegWiFi-pre_archivos/frame.htm

[24] Seguridad en redes inalámbricas, por Vicent Alapont Miquel

http://documentos.shellsec.net/otros/SeguridadWireless.pdf

[25] Seguridad en redes inalámbricas, por Carlos Cervera Tortosa

http://www.uv.es/montanan/redes/trabajos/SeguridadWLANs.pdf

[26] WPA Seguridad en redes inalámbricas, por Francisco García López

http://www.coitt.es/antena/pdf/154/06c_Reportaje_Seguridad.pdf

[27] *Wireless LAN Solution.* Cisco Systems

http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_package.html

[28] Cisco EAP-FAST. Cisco Systems

http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/netqa09186a00802030dc.html

[29] *Cisco Wireless LAN Security Overview*. Cisco Systems

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html

[30] White Papers A Comprehensive Review of 802.11 Wireless LAN Securityand the Cisco Wireless Security Suite. Cisco Systems

http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_white_paper09186a00800b469f.shtml

[31] Redes Wireless 802.11b, por Javier Pascual Soriano

www.fistconference.org/data/presentaciones/ 802.11bwirelessnetworksvulnerabilities.pdf

[32] IEEE 802.11 (WI-FI). El estándar de facto para WLAN, por Fidel Ramón García

http://www.coit.es/publicac/publbit/bit138/wifi.pdf

[33] Seguridad en redes WLAN, por Alejandra Ruíz

http://www.eside.deusto.es/eventos/semana/eventos/inc/Semana_eside_seguridad_wifi.pdf

[34] Seguridad aplicada en despliegues wireless, por Diego Ramírez

http://www.red.es/actividades/documentos/satec.pdf

[35] Avanzando en la seguridad de las redes WIFI, por Rodrigo Castro

http://www.rediris.es/rediris/boletin/73/ENFOQUE1.pdf

[36] Introducción a la redes inalámbricas (WIFI), por Oscar Entrecanales Baratey

http://www.ciefp-santander.org/DOCUMENS/CurWiFi.pdf

[37] Soluciones de seguridad en redes inalámbricas, por María Victoria Figueroa

http://www.ciefp-santander.org/DOCUMENS/CurWiFi.pdf

[38] Seguridad en redes wireless 802.11, por Leandro Meiners

http://www.cybsec.com/upload/ER_Seguridad_en_redes_Wireless_80211_v20.pdf

[39] *Product Support, End-of-Sale and End-of-Life Products*, por Cisco Systems

http://cisco.com/en/US/products/hw/tsd_products_support_end-of-sale_and_end-of-life_products_list.html

[40] *Cisco Aironet 350 Series*, por Cisco Systems

http://www.cisco.com/en/US/customer/products/hw/wireless/ps458/index.html

[41] *Cisco Aironet Conversion Tool for Cisco IOS Software 2-1 Administrator guide for windows*, por Cisco Systems

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/ios/administration/guide/tool3ios.html

[42] *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA*, por Cisco Systems

http://www.cisco.com/en/US/docs/wireless/access_point/12.3_8_JA/configuration/guide/1238jasc.html

[43] *Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(8).JEA2*, por Cisco Systems

http://www.cisco.com/en/US/docs/wireless/access_point/ios/release/notes/b1238jea2.html

[44] *Cisco Feature Navigator*, por Cisco Systems

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

[45] *Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(8).JEA3*, por Cisco Systems

http://www.cisco.com/en/US/docs/wireless/access_point/ios/release/notes/12_3_8_jea3.html

ANEXOS

ANEXO A

ANEXO B

	Guía rápida para acceder a la WLAN de Ypergas (usuarios visitantes)	Sección: IT
YPERGAS		GUI-IT-1002-00
		Fecha de Vigencia 10 de noviembre del 2008

PROPÓSITO

Este documento define como los usuarios visitantes pueden acceder a la WLAN corporativa de la empresa YPergas. El uso aceptable de esta red garantiza la seguridad y continuidad operativa de la empresa en general. El uso no apropiado representa riesgos para la empresa como vulnerabilidad en los sistemas, pérdida de confidencialidad en la información, gastos elevados y problemas legales, entre otros.

RESUMEN DEL DOCUMENTO

Este documento establece los lineamientos necesarios para que los usuarios visitantes a la empresa YPergas S.A., puedan acceder a la WLAN corporativa.

REFERENCIAS

POL-IT-1001-00	Declaración de Política de Seguridad Informática
DIR-IT-1001-00	Política de Seguridad Informática
-	Decreto Nº 1.204 de Mensaje de Datos y Firmas Electrónicas (Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148)
-	Ley Especial contra los Delitos Informáticos (Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.313)

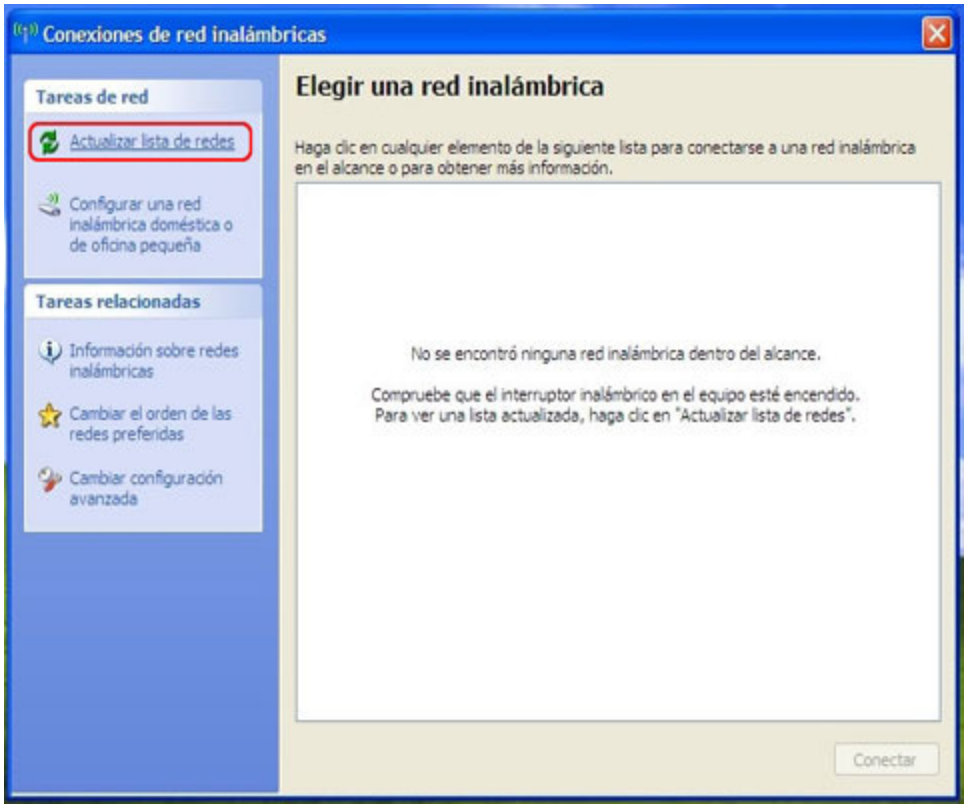
LINEAMIENTOS GENERALES

1.- Solicitar al personal de soporte técnico la información del SSID y la clave de acceso a la WLAN.

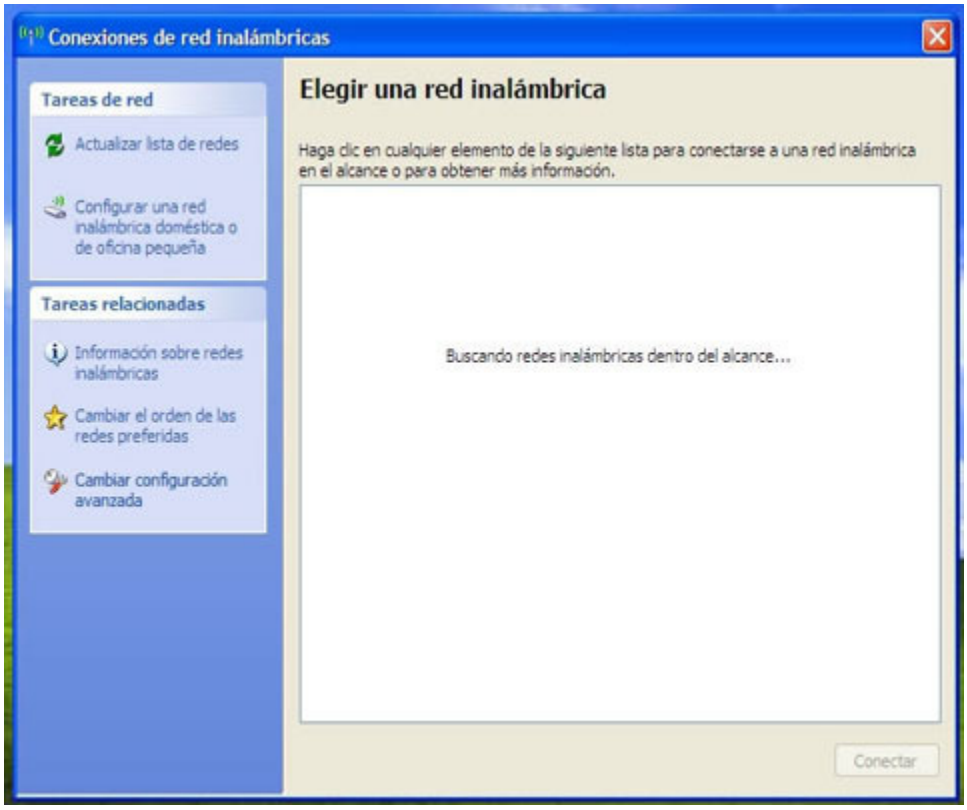
2.- Debe asegurarse tener activo el icono de la red inalámbrica, para buscar la señal de la WLAN de YPergas, buscando el icono de redes, que se encuentra en la barra de tareas, allí podrá saber si la máquina tiene la red desconectada o no ha sido instalada.

3.- Al encontrar el icono, damos clic derecho sobre él y a continuación nos saldrá un menú textual, con varias opciones, de las cuales debemos seleccionar “ver redes inalámbricas disponibles”.

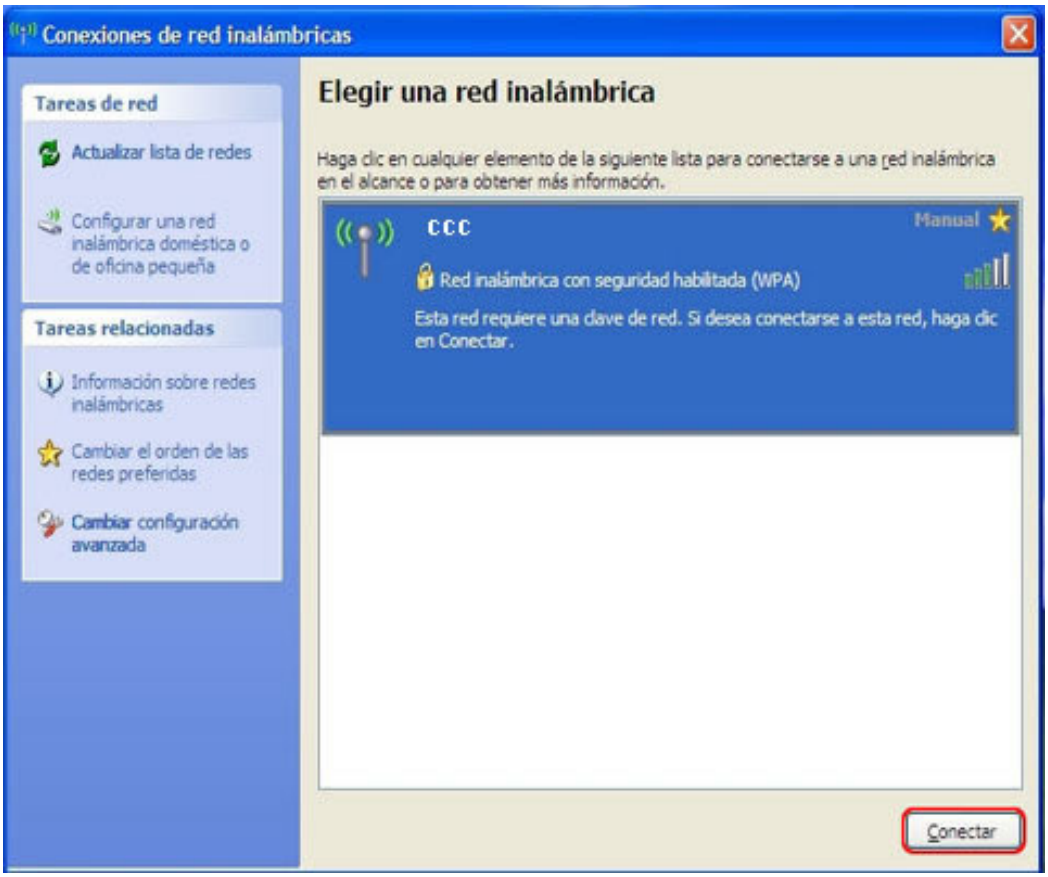
4.- En la ventana de conexiones de redes inalámbricas, debe seleccionar la opción “elegir una red inalámbrica”. Luego, seleccionar la opción “actualizar lista de redes” con esto podrá ver las redes inalámbricas a las cuales tenemos alcance.



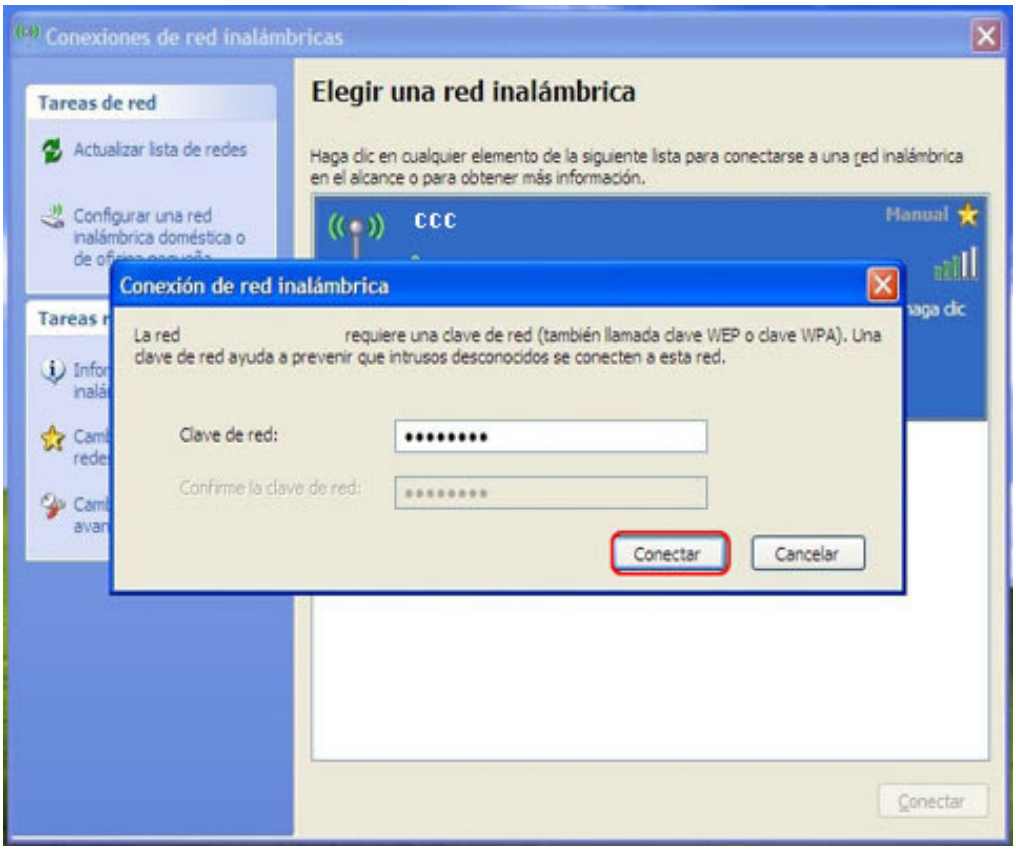
5.- Luego de realizar el tercer paso, aparecerá la ventana como la siguiente imagen que indica que está buscando las redes disponibles en su computadora. Para que puedas efectuar los pasos siguientes.



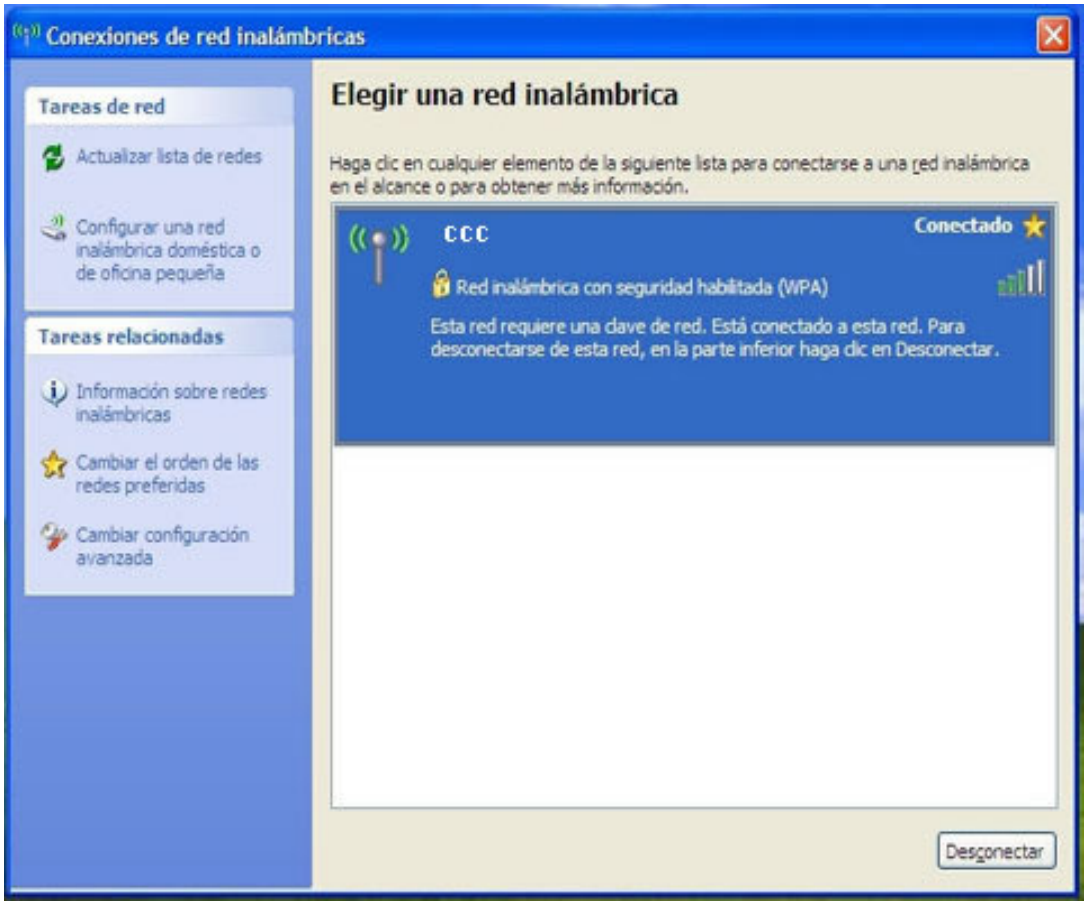
6.- Al encontrar la red inalámbrica disponible (ver lineamiento en el punto 1), en este caso el nombre de prueba es “CCC”. Luego, seleccionamos el botón “conectar”.



7.- Al intentar conectarse a esta red inalámbrica, le solicita la clave de red para acceder a ella (ver lineamiento en el punto 1), introduce la clave y luego selecciona nuevamente el botón “conectar”.



8.- Si la red ha sido conectada exitosamente, aparecerá los detalles de la conexión en la siguiente ventana, o en la barra de tarea notará que la red está activa.



PROPÓSITO

Este documento sirve para que el personal técnico de la gerencia de Tecnología de Información, tenga documentada la configuración de los puntos de accesos de la WLAN corporativa de Ypergas.

RESUMEN DEL DOCUMENTO

Este documento muestra la configuración realizada en los puntos de accesos, en el caso que sea necesario realizar alguna configuración adicional en los mismos.

CONFIGURACION DE LOS PUNTOS DE ACCESOS

```
! Ingreso al punto de acceso en modo EXEC (modo de ejecución) y solicitud de
! configuración del equipo APCCSP161

APCCSP161#show run
Building configuration...
!
Current configuration: 6160 bytes
!
! Últimos cambios realizados
!
! Last configuration change at 14:14:16 VST Fri Jun 13 2008
! NVRAM config last updated at 14:14:18 VST Fri Jun 13 2008
!
! Versión del software IOS almacenadas en memoria flash
!
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
! Nombre del host
!
hostname APCCSP161
!
enable secret 5 [confidencial]
!
clock timezone VST -4 30
ip subnet-zero
ip domain name [confidencial]
ip name-server [confidencial]
ip name-server [confidencial]
!
```

```
! Definición de los parámetros de autenticación, autorización y administración
!(autenticación en el servidor Tacacs para la administración del equipo)
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login AAA_LOCAL local
aaa authentication login AAA_REMOTO group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa session-id common
!
! Definición de la VLAN: XXX en la vlan 2 (para los usuarios empleados internos)
dot11 vlan-name XXX vlan 2
! Definición de la VLAN: YYY en la vlan 3 (para administración de la red
inálambrica)
dot11 vlan-name YYY vlan 3
! Definición de la VLAN: ZZZ en la vlan 4 (para acceso a Internet a través del uso
del
! acceso a banda ancha)
dot11 vlan-name ZZZ vlan 4

! Configuración del ssid BBB, en la vlan 2, con autenticación abierta y con
! seguridad WEP (para usuarios con laptop de socios)
dot11 ssid BBB
   vlan 2
   authentication open
   authentication key-management wep
   wep ascii 7 [confidencial]

! Configuración del ssid CCC, en la vlan 4, con autenticación abierta y con
! seguridad WPA-PSK, en modo de visitante o de acceso público (para accesos a
! visitantes/usuarios corporativos)
dot11 ssid CCC
   vlan 6
   authentication open
   authentication key-management wpa
   guest-mode
   wpa-psk ascii 7[confidencial]

! Configuración de pki
crypto pki trustpoint TP-self-signed-2522710326
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2522710326
 revocation-check none
 rsakeypair TP-self-signed-2522710326
!
! Usuario y password del equipo
!
username [confidencial] privilege 15 secret 5 [confidencial]
!
bridge irb
```

```
!
! Configuración de la interfaz radio 0, con encriptación tkip en la vlan 2 y 4, para
los
! ssid BBB y CCC
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 2 mode ciphers tkip
 !
 encryption vlan 4 mode ciphers tkip
 !
 ssid BBB
 !
 ssid CCC
 !
 speed basic-1.0 2.0 5.5 11.0
 station-role root
 rts threshold 2312
 no dot11 extension aironet
!
! Configuración de la sub-Interfaz radio 0.25, con vlan 2 y el bridge-group 2
!
interface Dot11Radio0.25
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
 bridge-group 2 spanning-disabled
!
! Configuración de sub-Interfaz radio 0.50, con vlan 3 nativa y el bridge-group 1
!
interface Dot11Radio0.50
 encapsulation dot1Q 3 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
! Configuración de sub-Interfaz radio 0.66, con vlan 4 y el bridge-group 4
!
interface Dot11Radio0.66
 encapsulation dot1Q 4
 no ip route-cache
```

```
 bridge-group 4
 bridge-group 4 subscriber-loop-control
 bridge-group 4 block-unknown-source
 no bridge-group 4 source-learning
 no bridge-group 4 unicast-flooding
 bridge-group 4 spanning-disabled
!
! Configuración de Interfaz fastEthernet 0 con full duplex y a una velocidad de 100
!(Interfaz física de la conexión del punto de acceso a la red cableada)
!
interface FastEthernet0
 no ip address
 no ip route-cache
 speed 100
 Full-duplex
!
! Configuración de la Sub-Interfaz fastEthernet 0.25, con la vlan 2 y bridge-group 2
!
interface FastEthernet0.25
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 no bridge-group 2 source-learning
 bridge-group 2 spanning-disabled
!
! Configuración de la Sub-Interfaz fastEthernet 0.50, con la vlan 3 y bridge-group 1
!
interface FastEthernet0.50
 encapsulation dot1Q 3 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
! Configuración de la Sub-Interfaz fastEthernet 0.66, con la vlan 4 y bridge-group 4
!
interface FastEthernet0.66
 encapsulation dot1Q 4
 no ip route-cache
 bridge-group 4
 no bridge-group 4 source-learning
 bridge-group 4 spanning-disabled
!
! Configuración de la Bridge-Group Virtual Interface, con la IP del PA
!
interface BVI1
 ip address [confidencial] [confidencial]
 no ip route-cache
!
ip default-gateway [confidencial]
```

```
no ip http server
ip http authentication local
no ip http secure-server
ip http help-path [confidencial]
ip radius source-interface BVI1
!
!
! Indice de interfaz SNMP
!
snmp-server ifindex persist
!
! Acceso vía SSH al servidor Tacacs
!
tacacs-server host [confidencial] key [confidencial]
tacacs-server directed-request
!
control-plane
!
bridge 1 route ip
!
!
banner exec ^C
!
line con 0
 exec-timeout 5 0
!
! Autenticación al servidor Tacacs para efectos de administración con el usuario
local y remoto
!
 login authentication AAA_LOCAL
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 login authentication AAA_REMOTO
 transport input ssh
 transport output none
line vty 5 15
 exec-timeout 5 0
 login authentication AAA_REMOTO
 transport input ssh
 transport output none
!
sntp server [confidencial]
end
!
! Indice de interfaz SNMP
!
snmp-server ifindex persist
```

```
!
! Acceso vía SSH al servidor Tacacs
!
tacacs-server host [confidencial] key [confidencial]
tacacs-server directed-request
!
control-plane
!
bridge 1 route ip
!
!
banner exec ^C
!
line con 0
 exec-timeout 5 0
!
! Autenticación al servidor Tacacs para efectos de administración con el usuario
local y ! remoto
!
 login authentication AAA_LOCAL
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 login authentication AAA_REMOTO
 transport input ssh
 transport output none
line vty 5 15
 exec-timeout 5 0
 login authentication AAA_REMOTO
 transport input ssh
 transport output none
!
sntp server [confidencial]
end
```