PROPUESTA DE UN ESQUEMA DE SEGURIDAD PARA LAS REDES INALÁMBRICAS (WLAN) DEL CAMPUS PRINCIPAL DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

LUZ STELLA GÓMEZ CADENA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO MECÁNICAS
ESCUELA DE INGENIERIAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2006

PROPUESTA DE UN ESQUEMA DE SEGURIDAD PARA LAS REDES INALÁMBRICAS (WLAN) DEL CAMPUS PRINCIPAL DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

LUZ STELLA GÓMEZ CADENA

Monografía para optar el título de Especialista en Telecomunicaciones

Director
SAMUEL GONZALO PINZÓN BARRIOS
Magíster en Ingeniería Electrónica

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO MECÁNICAS
ESCUELA DE INGENIERIAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2006

A, Dios por regalarme cada día y permitirme alcanzar las metas propuestas.

A, Mis padres por ser mi más grande apoyo.

A, mi Hermana, por estar a mi lado y de alguna manera apoyarme incondicionalmente.

AGRADECIMIENTOS

Expreso mis más sinceros agradecimientos:

Al Ingeniero Samuel Pinzón, director de la monografía, por su constante colaboración, aportando su experiencia y conocimientos.

A la Coordinación de la Especialización por ofrecerme la oportunidad y los recursos necesarios para llevar a cabo la Especialización.

Al Ingeniero Enrique Torres López, Jefe de la División de Servicios de Información por brindarme la oportunidad de realizar la monografía en esta dependencia.

A Libardo Lizcano, funcionario de la División de Servicios de Información por sus aportes, cooperación y dedicación.

A los docentes de la Especialización, por su interés en la formación de profesionales competentes de esta Institución.

A mis compañeros de la Especialización.

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

GLOSARIO

AAA: Abreviatura de Autenticación (Authentication), Autorización (Authorization) y Contabilidad (Accounting), sistema en redes IP para qué recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red.

ACCOUNTING: Es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión.

AD HOC: Una WLAN bajo topología "Ad Hoc" consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso.

AES: También conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bits desarrollado por los belgas Joan Daemen y Vincent Rijmen.

ALGORITMO DE ENCRIPTACIÓN: Codificadores de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma/producto modular y transformaciones lineales.

ATAQUES A PASSWORDS: Es un intento de obtener o descifrar una contraseña legítima de usuario.

ATAQUE DE DICCIONARIO: Método empleado para romper la seguridad de los sistemas basados en contraseñas en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles o recogidas en un diccionario idiomático.

ATAQUE DE FUERZA BRUTA: Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras (distinto del ataque de diccionario que prueba palabras aisladas).

AUDITORÍA: Análisis de las condiciones de una instalación informática por un auditor externo e independiente que realiza un dictamen sobre diferentes aspectos.

AUTENTICACIÓN: Es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña.

AUTORIZACIÓN: Es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito.

BRIDGE: Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar.

CHAP (Challenge Handshake Authentication Protocol): Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, lo cual lo hace un protocolo mucho más seguro que el PAP.

CIFRADO: Proceso para transformar la información escrita en texto simple a texto codificado.

CIFRADO ASIMÉTRICO: Cifrado que permite que la clave utilizada para cifrar sea diferente a la utilizada para descifrar.

CIFRADO DE ARCHIVOS: Transformación de los contenidos texto simple de un archivo a un formato ininteligible mediante algún sistema de cifrado.

CLIENTE INALÁMBRICO: Todo dispositivo susceptible de integrarse en una red inalámbrica como PDAs, portátiles, cámaras inalámbricas, impresoras.

CLAVE DE CIFRADO: Serie de números utilizados por un algoritmo de cifrado para transformar texto sin cifrar que se puede leer directamente en datos cifrados y viceversa.

CONFIDENCIALIDAD: Garantizar que la información sea asequible sólo a aquellas personas autorizadas a tener acceso a ella.

CONTROL DE ACCESOS: Se utiliza para restringir el acceso a determinadas áreas del PC, de la red, etc.

EAP - Protocolo de Autenticación Extensible (Extensible Authentication Protocol): Extensión del Protocolo Punto a Punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación.

ESTÁNDAR: Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos.

FAST (Flexible Authentication Secure Tunneling): Protocolo de seguridad WLAN del tipo EAP. Impide los denominados ataques de diccionario por fuerza bruta enviando una autenticación de contraseña entre el cliente WLAN y el punto de acceso inalámbrico a través de un túnel cifrado seguro. Elimina la necesidad de instalar servidores separados para tratar los certificados digitales empleados en otro sistema de seguridad WLAN (como el PEAP).

HOT SPOT: Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles) que proporciona servicios de red inalámbrica de banda ancha a visitantes móviles.

IEEE: Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización entre otras actividades, su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales

INFRAESTRUCTURA: Topología de una red inalámbrica que consta de dos elementos básicos: estaciones clientes inalámbricos y puntos de acceso.

ISP: Proveedor de Servicios de Internet.

LEAP (Lightweight Extensible Authentication Protocol): Protocolo del tipo EAP patentado por Cisco basado en nombre de usuario y contraseña que se envía sin protección.

MAC - Dirección de Control de Acceso al Medio (Media Access Control Address): Dirección hardware de 6 bytes (48 bits) única que identifica cada tarjeta de una red y se representa en notación hexademinal.

MD5: Algoritmo de cifrado de 128-bits del tipo EAP empleado para crear firmas digitales.

802.11: Familia de estándares desarrollados por la IEEE para tecnologías de red inalámbricas.

802.11a: Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de 5 GHz.

802.11b: Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 11 Mbps en una banda de 2.4 GHz. Utiliza la tecnología DSSS (Direct Sequencing Spread). La mayoría de los equipos utilizados en la actualidad son de esta tecnología. No es compatible con el 802.11a pues funciona en otra banda de frecuencia.

802.11e: Estándar destinado a mejorar la calidad de servicio en Wi-Fi. Es de suma importancia para la transmisión de voz y video.

802.11g: Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de frecuencia de 2.4 GHz. Una de sus ventajas es la compatibilidad con el estándar 802.11b.

802.11i: Estándar de seguridad para redes Wi-Fi aprobado a mediados de 2004. En el se define al protocolo de encriptación WPA2 basado en el algoritmo AES.

802.11n: Estándar para conseguir mayores velocidades de transmisión para Wi-Fi. Estas serán superiores a 100 Mbps.

802.16: Estándar de transmisión inalámbrica conocido como WiMAX. Es compatible con Wi-FI. La tecnología permite alcanzar velocidades de transmisión de hasta 70 Mbits en una banda de frecuencias entre 10 GHz y 66 GHz.

802.16d: Estándar de transmisión inalámbrica WiMAX que suministra una velocidad de entre 300 Kbps y 2 Mbps en una banda de frecuencia de 2GHz a 11GHz. Se utiliza para el cubrimiento de la “primer milla”.

802.1x: Estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.

PAP - Protocolo de Autenticación de Contraseñas (**Password Authentication Protocol):** El método más básico de autenticación, en el cual el nombre de usuario y la contraseña se transmiten a través de una red y se compara con una tabla de parejas nombre-clave, la no coincidencia provocará la desconexión.

PEAP (Protected Extensible Authentication Protocol): Protocolo del tipo EAP para la transmisión de datos autenticados, incluso claves, sobre redes inalámbricas 802.11. Autentica clientes de red Wi-Fi empleando sólo certificados del lado servidor creando un túnel SSL/TLS cifrado entre el cliente y el servidor de autenticación.

PKI - Infraestructura de Clave Pública: Sistema de certificados digitales, Autoridades Certificadores y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet.

PUNTO DE ACCESO (AP): Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles tanto para centralización como para enrutamiento.

RADIUS (Remote Authentication Dial-In User Service): Sistema de autenticación y contabilidad empleado por la mayoría de proveedores de servicios de Internet (ISPs)

RAS - Servidor de Acceso Remoto: Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta.

ROUTER: Es un conmutador de paquetes que opera en el nivel de red del modelo OSI, proporciona un control del tráfico y funciones de filtrado; está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP.

ROAMING: En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad

SERVIDOR DE AUTENTICACIÓN (AS): Servidor que gestiona las bases de datos de todos los usuarios de una red y sus respectivas contraseñas para acceder a determinados recursos.

SISTEMA DE CIFRADO: Colección completa de algoritmos que tienen su propia denominación en función de las claves que utilizan para cifrar.

SNIFFERS: Programa y/o dispositivo que monitorea la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información.

SSID: Identificador de red inalámbrica, similar al nombre de la red pero a nivel Wi-Fi.

TKIP - Protocolo de Integridad de Clave Temporal: Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

VLAN - Red de Área Local Virtual: Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares.

WAN – Red de Área Amplia: Tipo de red compuesta por dos o más redes de área local (LANs).

WARCHALKING: Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.

WARDRIVING: Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar puntos de acceso inalámbrico.

WARSPAMMING: Acceso no autorizado a una red inalámbrica y uso ilegítimo de la misma para enviar correo masivo (spam) o realizar otro tipo de acciones que comprometan el correcto uso de un sistema.

WEP – Privacidad Equivalente a Cableado: Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes inalámbricas que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del Vector de inicialización IV), de 128 bits (104 bits más 24 bits del vector de inicialización IV).

Wi-Fi (Wireless Fidelity): Es el nombre comercial con el cual se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica.

WiMAX - Interoperabilidad Mundial para Acceso por Microondas: Es un estándar de transmisión inalámbrica de datos (802.MAN) proporcionando accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa entre el punto transmisor y el receptor.

WPA - Acceso Protegido Wi-Fi: Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado).

WPA2 - Protocolo de Aplicación Inalámbrica: Protocolo de seguridad para redes Wi-Fi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Puntos de Acceso de última generación.

SUMMARY

TITLE: PROPOSAL OF A SECURITY SCHEME FOR THE WIRELESS NETWORKS (WLAN) OF THE MAIN CAMPUS OF THE 'UNIVERSIDAD INDUSTRIAL DE SANTANDER'. *

AUTHOR: LUZ STELLA GOMEZ CADENA**

KEY WORDS:

Information Security, Network Security, Wireless Networks.

DESCRIPTION:

At the moment the security in the wireless networks is a topic that has not been assumed with the necessary attention on the part of the administrators of the networks including of the users responsible for the information. Different elements contribute in the growing of this situation: the fact of using a shared means of transmission without controlling the access of people or devices, the vertiginous increase of this technology in the society, the novelty of the used technology, and the policy used in its implementation. All of the above have generated its expansion as priority and have put aside aspects relative to its security.

Nowadays is taking place a concerted effort in the development of standards and technologies that avoid these problems of security. Starting off this frame, this monograph presents a global vision of the security in the wireless networks, from the existing risks in the implementation of the present standards, to the proposed improvements to correct these risks. All of this with the purpose of obtaining as a final outcome a proposal of securing the wireless networks in the main campus of the 'Universidad Industrial de Santander'.

* Project of Degree

** Facultad the Engineering Physic – Mechanical School of Electrical, Electronic and Telecomunications. Project of Degree Master of Telecomunications, PINZON BARRIOS, Samuel Gonzalo, Mie.

RESUMEN

TÍTULO: PROPUESTA DE UN ESQUEMA DE SEGURIDAD PARA LAS REDES INALÁMBRICAS (WLAN) DEL CAMPUS PRINCIPAL DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER. [*]

AUTOR: LUZ STELLA GÓMEZ CADENA[**]

PALABRAS CLAVES:

Seguridad Informática, seguridad en redes, redes inalámbricas.

DESCRIPCIÓN:

Actualmente la seguridad en las redes inalámbricas es un tópico que no se ha asumido realmente con la atención necesaria por parte de los administradores de las redes e inclusive de los usuarios responsables de la información. Diversos elementos contribuyen en el crecimiento de esta problemática: el hecho de utilizar un medio de transmisión compartido sin controlar el acceso de las personas o dispositivos, el vertiginoso incremento de esta tecnología en la sociedad, la novedad de la tecnología empleada, y la política en su implementación, han generado como prioridad su expansión y se han dejado de lado aspectos relativos a su seguridad.

Hoy día se está efectuando un gran esfuerzo en el desarrollo de estándares y tecnologías que eviten estos problemas de seguridad. Partiendo de este marco, la presente monografía presenta una visión global de la seguridad en las redes inalámbricas, desde los riesgos existentes en la implementación de los estándares actuales, hasta las mejoras propuestas para subsanar dichos riesgos, con el fin de obtener como producto final una propuesta de aseguramiento de las redes inalámbricas a nivel del "Campus Principal de la Universidad Industrial de Santander".

---

[*] Proyecto de Grado

[**] Facultad de Ingeniería Físico Mecánicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones. Especialización en Telecomunicaciones. PINZÓN BARRIOS, Samuel Gonzalo, Mie.

INTRODUCCIÓN

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

La irrupción de esta nueva tecnología de comunicación ha proporcionado nuevas expectativas para el desarrollo de sistemas de comunicación, y así mismo el auge de nuevos riesgos en seguridad de la información. Esta seguridad de redes abarca un campo más amplio que la información sobre ataques y defensa. Un buen esquema de seguridad comienza por el nivel más alto de una organización, con un amplio plan que determine dónde concentrar los esfuerzos e inversión económica. Por consiguiente es un factor importante que debe estar presente en toda red inalámbrica especialmente en los lugares que pueden parecer más seguros y confiables, sitios que deben tener un sistema de seguridad robusto para proteger sus recursos más preciados.

Infortunadamente, la seguridad en redes Inalámbricas es un problema que, a pesar de su gravedad, no ha recibido la atención debida por parte de los administradores de redes y los responsables de la información, situación que no es ajena a la Universidad Industrial de Santander.

Es por esto, que el presente trabajo pretende definir un esquema de seguridad a ser aplicado en el Campus Principal del Alma Máter, basado en estándares de clase mundial y mejores prácticas de proveedores de la tecnología.

1. GENERALIDADES SOBRE REDES WLAN

1.1 CONCEPTO

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. Además, depende de ondas de radio para transferir datos, los cuales son sobrepuestos en una onda de radio por medio de un proceso denominado modulación, y en la cual la onda portadora, actúa entonces como el medio de transmisión, sustituyendo así el cable en un escenario LAN.

Las WLAN generalmente constan de un Punto de Acceso (AP, Access Point) que conecta una red cableada y un dispositivo remoto (cliente) a través de un enlace inalámbrico.

1.2 TOPOLOGÍA

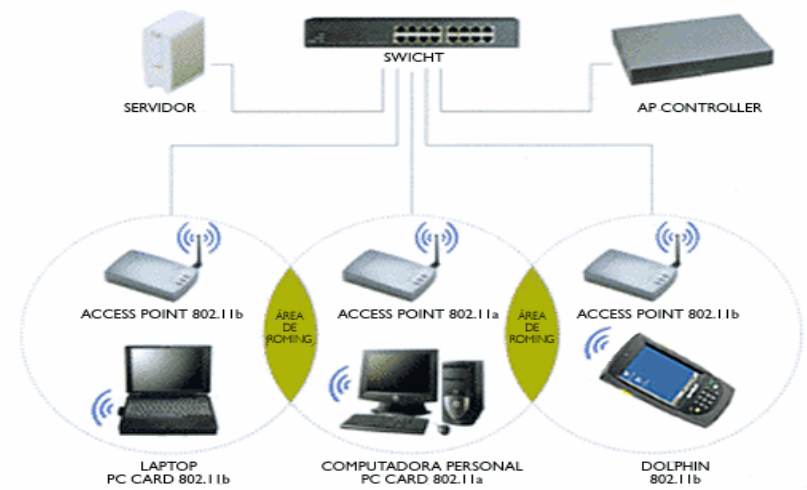
Se encuentran dos tipos de topología y/o modos de operación: Redes de tipo Infraestructura y Redes Ad Hoc.

1.2.1 Redes de tipo Infraestructura.

En este modo de operación, el Punto de Acceso controla toda la comunicación; es decir, todo se hace a través del Punto de Acceso. Los equipos se conectan a un Punto de Acceso quien controla el acceso a la red. Existe mayor cobertura porque el Punto de Acceso actúa como repetidor.

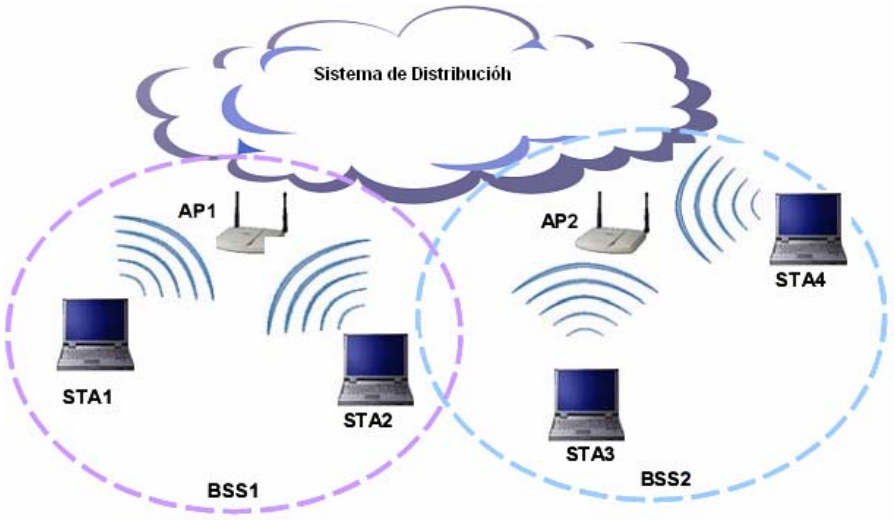
* De aquí en adelante se utilizará el término WLAN para hacer referencia a una red de área local inalámbrica 802.11

Figura 1 . Red Inalámbrica



Fuente: Tecnología Virtual. Disponible en Internet: <http://www.tvirtual.com/s-inalambricas.htm>

Figura 2. WLAN en modo Infraestructura



Fuente: Tecnología Virtual. Disponible en Internet: <http://www.tvirtual.com/s-inalambricas.htm>

1.2.2 Ad Hoc.

En esta configuración la comunicación se hace punto a punto, entre dos tarjetas WLAN. Cada estación posee una tarjeta de red inalámbrica mediante la cual se

conecta con todos los demás, no existe un dispositivo que controle el acceso a la red, y el alcance es limitado al cubrimiento de las tarjetas.

Figura 3. WLAN en modo Ad Hoc

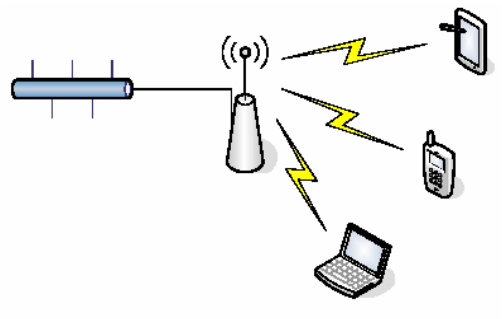
Fuente: Tecnología Virtual. Disponible en Internet: <http://www.tvirtual.com/s-inalambricas.htm>

1.3 APLICACIONES

Un sinnúmero de aplicaciones se pueden observar en la actualidad para las redes inalámbricas; la más común, son los llamados HotSpots. Entre las aplicaciones más relevantes están:

- **Punto de Acceso:** El punto de acceso es conectado a una LAN cableada ó actúa como nodo central en una red WLAN.

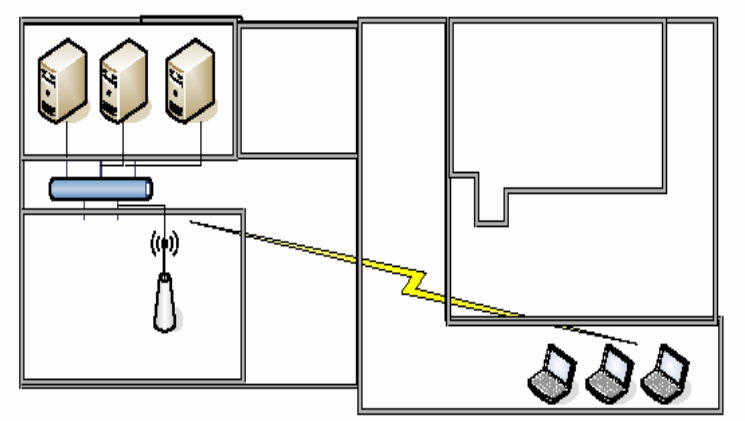
Figura 4. Punto de Acceso (Acceso a la red)



Fuente: Autor Proyecto

➲ **Extensión de una red cableada:** El punto de acceso amplia el área de cobertura de una red cableada.

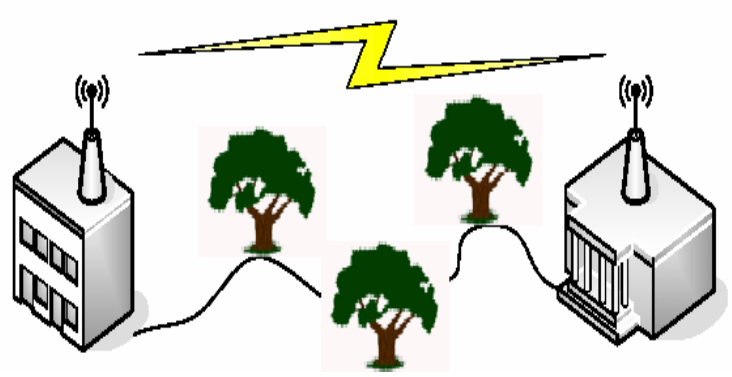
Figura 5. Extensión de una red cableada.



Fuente: Autor Proyecto

➲ **Conexión de edificio a edificio:** Diseñado para conectar dos LANs ubicadas en diferentes edificios.

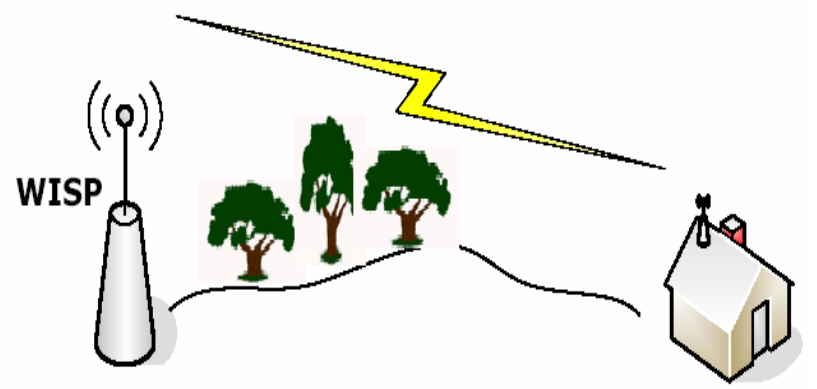
Figura 6. Conexión de edificio a edificio



Fuente: Autor Proyecto

➲ **Equipo de última milla:** Permite ofrecer servicios a zonas rurales de difícil acceso, a las que no llegan las redes cableadas proporcionando de este forma un servicio de telecomunicaciones.

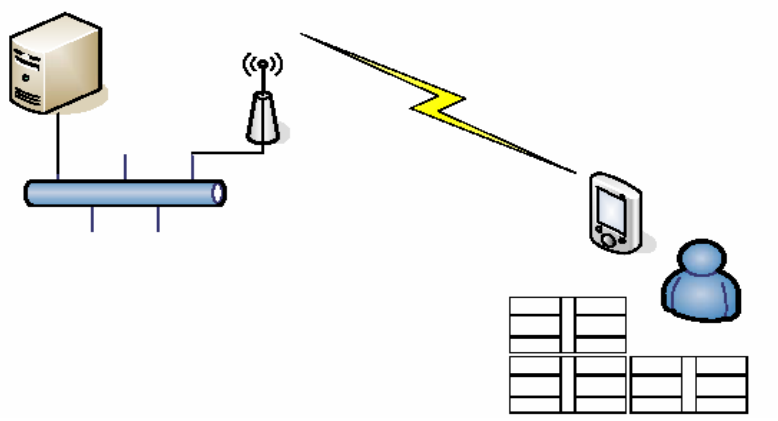
Figura 7. Equipo de última milla



Fuente: Autor Proyecto

➲ **Movilidad:** Las redes inalámbricas pueden proveer a los usuarios acceso a la información en tiempo real en cualquier lugar dentro de la organización.

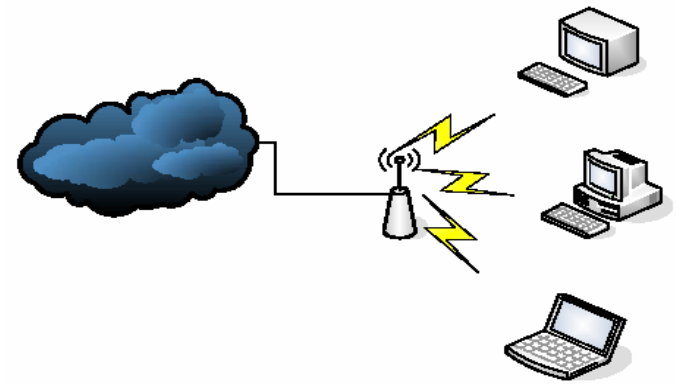
Figura 8. Movilidad



Fuente: Autor Proyecto

➲ **SOHO:** Estas redes se usan para conectar una red de una oficina pequeña o doméstica.

Figura 9. SOHO (Small Office – Home Office)

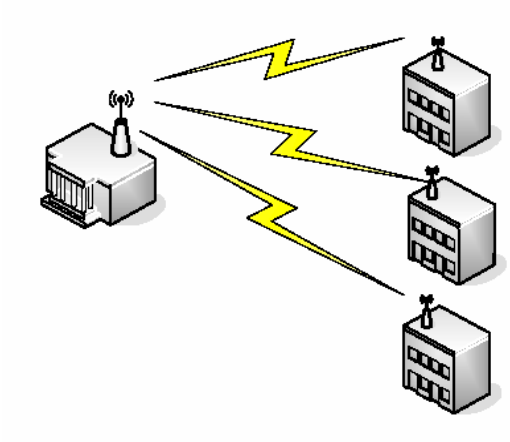


Fuente: Autor Proyecto

➲ **Oficinas Móviles:** Este tipo de aplicación, permite instalar oficinas temporales, evitando el cableado en áreas de difícil acceso.

Figura 10. Oficinas Móviles

Fuente: Autor Proyecto



Fuente: Autor Proyecto

1.4 ESTÁNDAR IEEE 802.11

La IEEE dividió sus estándares en varios comités. Al Comité IEEE 802 le correspondió hacerse cargo de las redes de área local LAN y las redes de área metropolitana MAN. Asimismo el comité 802 se subdividió en grupos de trabajo para tratar distintos temas específicos en las LANs y las MANs. De esta forma, el

grupo 802.1 se dedicó al tema del puenteo ("bridging") y administración, el grupo 802.2 se ocupó del control de la conexión lógica, al grupo 802.3 les correspondió el método de acceso CSMA/CD y de la misma forma, al grupo 802.11 le correspondió ocuparse de las redes inalámbricas (WLAN).

El grupo de trabajo 802.11 fue formado en septiembre de 1990. Su objetivo era crear la especificación de las LAN inalámbricas que operaran en el rango de frecuencia ISM*. Se definió inicialmente la velocidad de transmisión de 1 a 2 Mbps en el rango de frecuencia 2.4Ghz, usando: FHSS (Modulación por saltos de frecuencia) o DSSS (Espectro de extensión de secuencia directa).

El primer estándar 802.11 fue publicado en 1997. Las normas IEEE 802.11 forman una familia de especificaciones que definen cómo deben producirse los equipos de WLAN para que los equipos de los diferentes fabricantes puedan trabajar juntos. Seguidamente, el IEEE publicó las subdivisiones del estándar 802.11 de los cuales se muestran las principales características:

- **802.11a:** Revisión del protocolo 802.11 que proporciona 54 Mbps estandarizado y hasta 72 y 108 Mbps con tecnologías de desdoblamiento no estandarizado en el rango de frecuencia 5GHz, usando: OFDM (Multiplexión por División de Frecuencia Ortogonal), DSSS (Espectro Disperso de Secuencia Directa).

- **802.11b**: También llamado 802.11 High Rate o Wi-Fi, revisión del protocolo 802.11 que proporciona 11 Mbps con reducciones a 5.5, 2 y 1 Mbps en el rango de frecuencia 2.4 GHz, usando: DSSS.
- **802.11g:** Protocolo que proporciona 54 Mbps en el rango de frecuencia 2.4 GHz, manteniendo plena compatibilidad con el protocolo 802.11b.

* Son bandas reservadas internacionalmente para uso no comercial de Radio Frecuencia electromagnética en áreas industrial, científica y médica.

Otras especificaciones del estándar son:

- **802.11c**: Define características de puntos de acceso (AP) como Bridges.

- **802.11d:** Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias).

- **802.11e**: Calidad de servicio (QoS).

- **802.11f**: Protocolo de conexión entre puntos de acceso (AP), protocolo IAPP (Inter Access Point Protocol).

- **802.11h**: DFS (Dynamic Frequency Selection), habilita una cierta Coexistencia con HiperLAN y regula también la potencia de difusión.

- **802.11i:** Seguridad (aprobada en Julio de 2004).

- **802.11j:** Permitiría armonización entre IEEE (802.11), ETSI (HiperLAN2) y ARIB (HISWANa).

- **802.11m**: Mantenimiento redes inalámbricas.

- **802.11n**: Actualmente se está desarrollando, se espera que alcance los 500 Mbps.

1.5 ASPECTOS DE LA ARQUITECTURA WLAN 802.11

Según el estándar 802.11, en la arquitectura de red, se puede identificar los siguientes componentes en una red inalámbrica:

- Estación (STA - Station): Es el dispositivo que se conecta (Equipo de cómputo, PDA, móvil, etc.)

- Unidad de Servicio Básico (BSS Basic Service Set): Conjunto de STAs que se comunican unas con otras.

- Unidad de Servicio Básico Independiente (IBSS Independent BSS): Conjunto de STAs que se comunican unas con otras formando una configuración Ad Hoc.

- Unidad de Servicio Básico Infraestructura (Infrastructure BSS o simplemente BSS): Conjunto de STAs que se comunican unas con otras formando una configuración en modo Infraestructura.

- Punto de Acceso (AP Access Point): Es una STA especial que dirige las comunicaciones. Análogo a una BSS (estación base) en un sistema de comunicaciones móviles).

- Unidad de Servicio Extendido (ESS Extended Service Set): Varias BSS conectadas en modo infraestructura para extender la cobertura de la red.

- Sistema de Distribución (DS Distibution System): Medio por el que los APs y BSSs se comunican, puede ser cableado o también inalámbrico.

1.6 DISPOSITIVOS

Algunos dispositivos comunes en instalaciones de redes inalámbricas y sus modos de configuración, se muestran en la Tabla 1. Los accesorios adicionales en instalaciones de redes inalámbricas, son los siguientes: antenas RF, dispositivos PoE, amplificadores/ Atenuadores de RF, aterrizador, splitter, conectores RF, cables RF/Pig Tail.

Tabla 1. Dispositivos WLAN

DISPOSITIVO	MODO OPERACIÓN
Puntos de Acceso (Access Point)	Básico Puente (Bridge) Repetidor
Puentes Inalámbricos (Bridge Wireless)	Básico Puente (Bridge) Punto de acceso Repetidor
Dispositivos cliente WLAN	PCMCIA - Compact Flash Cards Ethernet - Conversores seriales Adaptadores USB Adaptadores PCI – ISA
Gateway residencial	Cable MODEM xDSL MODEM MODEM análogo MODEM satelital

Fuente: Autor Proyecto

2. SEGURIDAD INALÁMBRICA

Los tres aspectos fundamentales que se deben tener en cuenta al diferenciar una red WLAN de una cableada son:

- **Confidencialidad:** La información no es legible por terceros. Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos por medio de escucha pasiva.

- **Integridad:** La información no puede ser alterada en tránsito. Es decir que los datos que han sido enviados a través de la red no sean cambiados por intrusos.

- **Autenticidad:** El usuario es quien dice ser. Permite al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.

El aspecto crítico en las redes inalámbricas es que su medio de transmisión es el aire, por lo cual, no se puede controlar quien detecta o percibe la señal.

2.1 SEGURIDAD EN EL ESTANDAR 802.11

La seguridad en el estándar IEEE 802.11 se define en la forma de autenticación: Sistemas Abiertos y Sistemas de Clave Compartida. La autenticación del Sistema Abierto es la opción por defecto que se utiliza en todo dispositivo estandarizado bajo IEEE 802.11. Este tipo de autenticación permite que cualquier cliente forme parte de la red. La seguridad que nos proporciona un Sistema abierto es nula, por lo que cualquier cliente puede acceder la red sin ningún problema.

Las características incorporadas de seguridad del estándar IEEE 802.11, son propias y presentan sus limitaciones, de acuerdo a las recomendaciones planteadas. La especificación de IEEE 802.11 identifica varios servicios para proporcionar un ambiente de funcionamiento seguro. Los servicios de seguridad son proporcionados en gran parte por el protocolo WEP para los datos durante la transmisión inalámbrica entre los clientes y los puntos de acceso. WEP no proporciona seguridad, solamente la parte inalámbrica de conexión.

En la autenticación de Clave Compartida se requiere también la implementación del mecanismo de seguridad. Este mecanismo de seguridad utiliza una única clave secreta para todos los miembros de la red, la cual fue conocida por los miembros antes de entrar en la red. Esta clave compartida está contenida en un atributo de la MIB* a través del camino de gestión MAC. Este atributo es de sólo escritura así que el valor de la clave permanece interna en la MAC.

2.2 POSIBLES ATAQUES Y AMENAZAS A UNA WLAN

A continuación se presentan los ataques y/o vulnerabilidades existentes en redes inalámbricas†:

2.2.1 Ataques propios de una WLAN

2.2.1.1 Espionaje (surveillance)

Este tipo de ataque consiste en observar el entorno donde se encuentra instalada la red inalámbrica, no se necesita ningún tipo de hardware o software especial. Sirve para recopilar información y se puede combinar con otro tipo de ataques.

---

* Administración de la Base de Información. Es un esquema o un modelo que contiene el orden jerárquico de todos los objetos manejados en la base. Cada objeto manejado en un MIB tiene un identificador único.

† What Hackers Don´t Want You to Know About Your WLAN. Kathy Keenan. AIRMAGNET, www.airmagnet.com

Tabla 2. Espionaje

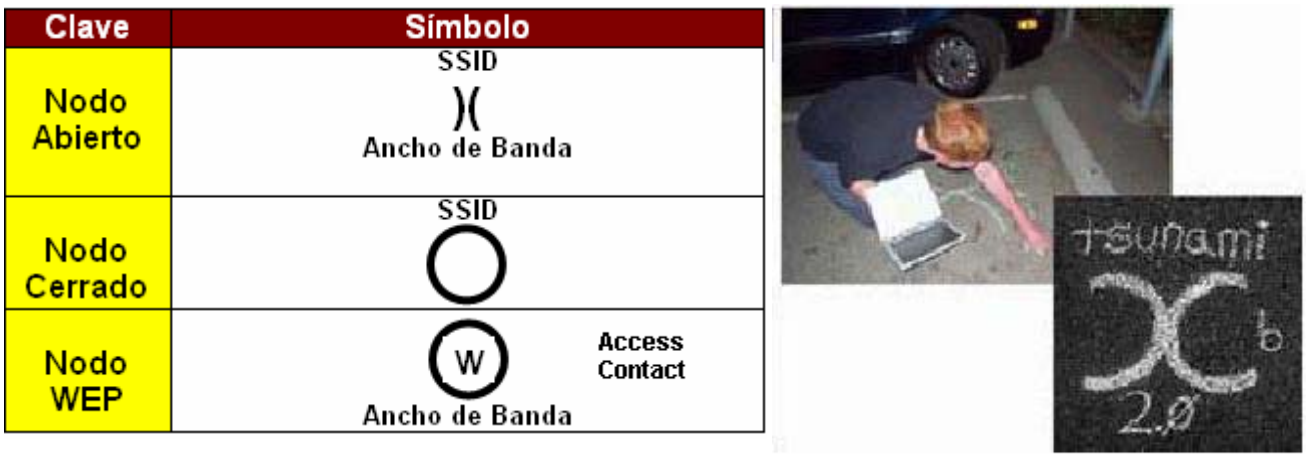
OBSERVACIÓN ENTORNO	LOCALIZACIÓN
Antenas	Muros, techos, tejados, pasillos, ventanas, entradas.
Puntos de acceso	Muros, techos, falsos techos.
Cables de red	Atraviesan techos, muros, paredes.
Dispositivos – scanner /PDAs	Personal de la empresa.

Fuente: Autor Proyecto

2.2.1.2 War-Chalking

Se trata de un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que pasen por allí. Consiste en dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico. En este tipo de ataque se utiliza tiza, pintura, spray de color, etc. El significado de cada símbolo es el siguiente:

Figura 11. War-Chalking



Fuente: Autor Proyecto

2.2.1.3 War-driving

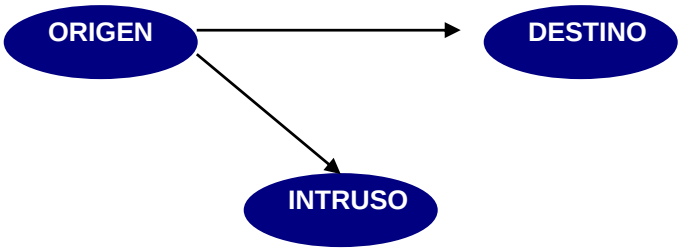
Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como un portátil o un PDA; el atacante pasea con el dispositivo móvil, y en el momento en que detecta la existencia de la red, se realiza un análisis de la misma. El dispositivo móvil puede estar equipado con un sistema GPS para marcar la posición exacta donde la señal es más fuerte, o incluso una antena direccional para recibir el tráfico de la red desde una distancia considerable.

Si la red tiene DHCP, el dispositivo móvil se configura para preguntar continuamente por una IP dentro de un cierto rango, si la red no tiene DHCP activado se puede ver la IP que figure en algún paquete analizado. Existen varias herramientas útiles para detectar redes inalámbricas, las más conocidas son el AirSnort o Kismet para Linux y el NetStumbler para sistemas Windows. Para realizar el War-driving se necesitan realmente pocos recursos. Los más habituales son una computadora portátil con una tarjeta inalámbrica, un dispositivo GPS para ubicar el AP en un mapa y el software apropiado (AirSnort para Linux, BSD- AriTools para BSD o NetStumbler para Windows). En la Figura 12 se aprecian un ejemplo de APs marcados con rojos y configurados con WEP.

Figura 12. Localización puntos de acceso WEP

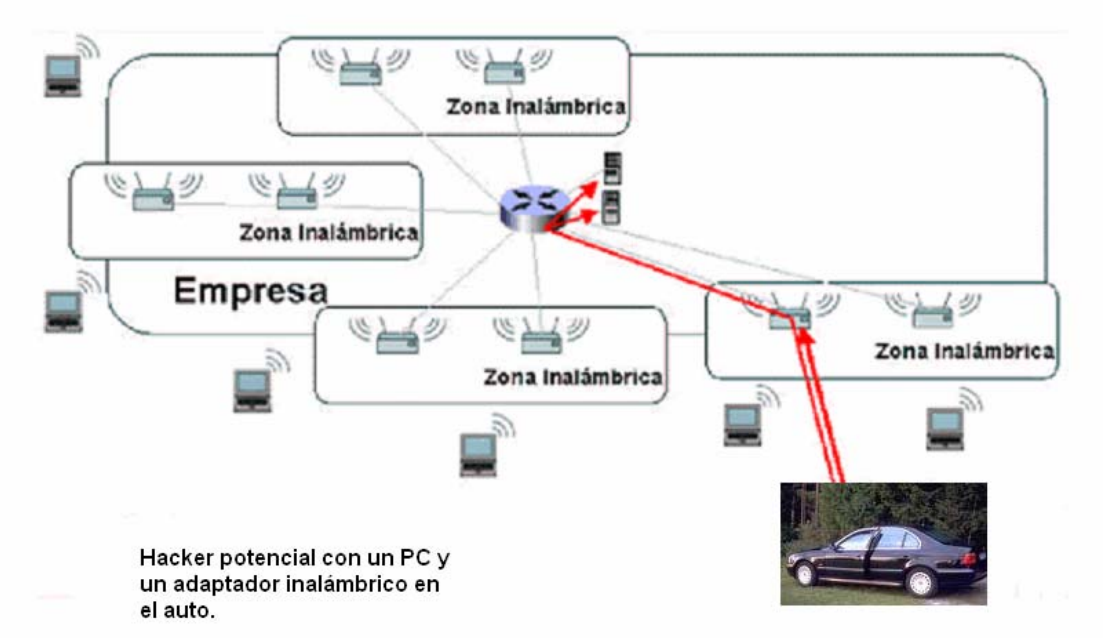
Fuente: Autor Proyecto

2.2.1.4 Interceptar una señal.



El atacante intenta identificar el origen y el destino que posee la información. Es decir, la toma de posesión y el uso del ancho de banda de las WLAN privadas y de los hot spot públicos, mediante un kit básico de war-driver, programas sniffer descargables de la Red. Tras haber interceptado la señal, el atacante intentará recopilar información sensible del sistema. El Wireless Hacking puede requerir que el war-driver tenga que exponerse peligrosamente, teniendo que acercarse a la red para poder capturar la señal. Esto puede provocar una probable tendencia a una mayor prudencia.

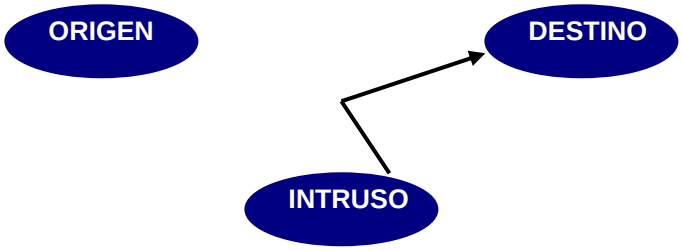
Figura 13. Intercepción de señal



Fuente: Seguridad Gíreles. Disponible en Internet: <http://documentos.shellsec.net/otros/SeguridadWireless.pdf>

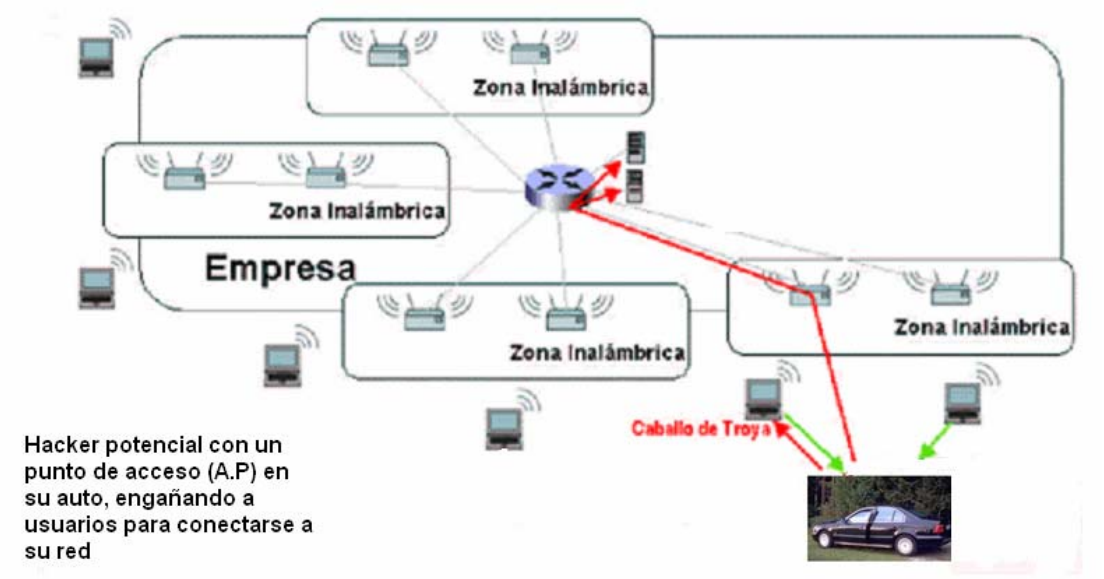
2.2.2 Técnicas de Intrusión

2.2.2.1 Suplantar una fuente real



En esta técnica el intruso pretende ser la fuente real u original.

Figura 14. Suplantación de fuente real



Fuente: Seguridad Gíreles. Disponible en Internet: <http://documentos.shellsec.net/otros/SeguridadWireless.pdf>

2.2.2.2 Sniffing – Eavesdropping

El programa monitorea los datos y determina hacia donde van, de donde vienen y qué son, siempre que haya una tarjeta de red que actúa en modo promiscuo. El modo promiscuo es un modo de operación en el que una computadora conectada a una red compartida captura todos los paquetes, incluyendo los paquetes destinados a otras computadoras. Es muy útil para supervisar la red, pero presenta un riesgo de seguridad.

2.2.2.3 MAC Spoofing (Suplantación de MAC) – Hijacking

Para este caso el intruso imita una dirección MAC de un cliente válido y trata de asociarse al Punto de Acceso. Existen dos formas de encontrar una dirección MAC, por fuerza bruta (aunque bastante complejo) ó simplemente monitoreando el canal y capturando paquetes.

2.2.2.4 DoS (Denial of Service, Denegación del Servicio) Flooding attacks

Se considera netamente vandalismo, en este tipo de ataque el intruso trata de bajar el servicio ofrecido por el Punto de Acceso. Se puede realizar de dos formas: Irradiando señales RF en la banda de 2.4GHz o 5 GHz hacia el Punto de Acceso ó enviando paquetes falsos de terminación de sesión Cliente – Punto de Acceso.

2.2.2.5 Asociación Maliciosa

En este tipo de ataque el intruso intenta obtener información valiosa de la red, haciéndose pasar por un Punto de Acceso válido y asociando clientes inadvertidos.

2.2.2.6 Ataque hombre en el medio

En este tipo de ataque, el intruso intenta insertarse, él mismo, en la mitad de una comunicación con el propósito de interceptar los datos de un cliente. De esta forma podría modificar los datos y enviarlos al destino real.

2.3 MECANISMOS DE SEGURIDAD

El hecho de tener un Punto de Acceso irradiando señal, se convierte en una vulnerabilidad si no se toman las acciones necesarias para garantizar la seguridad. Cualquier persona que detecte la señal y logre ingresar a la red podrá navegar gratis por Internet, en el mejor de los casos, o podrá robar información sensible, insertar un virus informático, bloquear servidores, entre otros. En general, algunos mecanismos son[‡]:

2.3.1 SSID.

Como uno de los primeros niveles de seguridad que se pueden definir en una red inalámbrica se cita al SSID ("Service Set Identifier" o identificador del servicio). Aunque se trata de un sistema muy básico (normalmente no se tiene por un sistema de seguridad), este identificador permite establecer o generar, tanto en la estación cliente como en el Punto de Acceso, redes lógicas que interconectarán a una serie de clientes.

Normalmente, los puntos de acceso difunden su SSID para que cada cliente pueda ver los identificadores disponibles y realizar la conexión a alguno de ellos simplemente seleccionándolos. Pero también se puede inhabilitar la difusión de este SSID en el punto de acceso, para dificultar el descubrimiento de la red inalámbrica por parte de personas ajenas a su uso.

[‡] MADRID MOLINA, Juan Manuel. Seguridad en Redes Inalámbricas 802.11. Sistemas & Telemática. Revista Facultad de Ingeniería UNIVERSIDAD ICESI.

2.3.2 Filtrado de direcciones MAC o ACL (Access Control List).

Este método consiste en la creación de una tabla de datos en cada uno de los Puntos de Acceso de la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los Puntos de Acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.
- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.
- Las direcciones MAC viajan sin cifrar por el aire. Un intruso podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador. De este modo, el atacante puede hacerse pasar por un cliente válido.
- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un Punto de Acceso el problema es más serio, porque el Punto de Acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

2.3.3 Protocolo WEP (Wired Equivalent Privacy).

Privacidad equivalente en una red cableada. Forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP utiliza una misma clave simétrica y estática en las estaciones y el Punto de Acceso; y no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de la red.

El algoritmo de cifrado 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.

Por otra parte, WEP no ofrece servicio de autenticación. El cliente no puede autenticar la red, ni al contrario; basta con que el equipo móvil y el Punto de Acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

2.3.4 OSA (Open System Authentication).

Es otro mecanismo de autenticación definido por el estándar 802.11 para autenticar todas las peticiones que el Punto de Acceso y transmisor reciben. Cualquier interlocutor es válido para establecer una comunicación con el Punto de Acceso. El mecanismo empleado se conoce con el nombre de SKA (Shared Key Authentication) y consiste en que ambos dispositivos disponen de la misma clave de cifrado, entonces, el dispositivo transmisor pide al Punto de Acceso autenticarse, el Punto de Acceso le envía una trama al transmisor, que si éste a su vez devuelve correctamente codificada, le permite establecer la comunicación. Lastimosamente, es un mecanismo poco fiable, dado que no permite tener claves dinámicas.

2.3.5 Protocolo de seguridad WPA (Wi-Fi Protected Access).

Es un estándar propuesto por los miembros de la Wi-Fi Alliance en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol - Protocolo de Clave Temporal de Integridad). Este protocolo se encarga de cambiar la clave compartida entre Punto de Acceso y cliente cada cierto tiempo, amplia su longitud de 40 a 128 bits. La clave 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. 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.

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. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs (Vector de Inicialización), con respecto a WEP. El mecanismo de autenticación usado en WPA emplea 802.1x/EAP. El estándar IEEE 802.1x define un protocolo para encapsular protocolos de autenticación sobre protocolos de la capa de enlace de datos. IEEE 802.1x permite utilizar diversos métodos para autentificar al usuario a través del protocolo de autenticación extensible (EAP).

IEEE 802.1x define 3 entidades:

- **El solicitante (supplicant**), reside en la estación inalámbrica, cuando pasa a estar activo en el medio selecciona y se asocia a un Punto de Acceso.

- **El autenticador (authenticator),** reside en el Punto de Acceso. Detecta la asociación del cliente y habilita un puerto para ese solicitante, permitiendo únicamente el tráfico 802.1x, el resto de tráfico se bloquea.

- **El servidor de autenticación**, reside en un servidor AAA (Authentication, Authorization, & Accounting), Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) o Diamater 802.1x utiliza un método de control de acceso basado en el concepto de puerto (PAE, Port Acess Entity). El autenticador crea un puerto lógico por cliente, existiendo dos caminos uno autorizado y otro no. Mientras el cliente no se ha autenticado con éxito únicamente se permite tráfico 802.1x/EAP hacia el servidor de autenticación.

Los métodos de autenticación definidos en WPA son: EAP-TLS, EAP-TTLS y PEAP. Estos métodos se basan en la infraestructura de clave pública (PKI) para autenticar al usuario y al servidor de autenticación, utilizando certificados digitales. La premisa es la existencia de una Autoridad de Certificación (CA) de confianza para la organización, que emita certificados para los usuarios y el servidor de autenticación. La CA puede ser privada (empresarial) o pública (basada en CAs de Internet como Verisign).

2.3.5.1 EAP-TLS (Transport Layer Security).

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.

2.3.5.2 PEAP Y EAP-TTLS.

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 2 métodos: Protected EAP (PEAP) y EAP-Tunneled TLS (EAP-TTLS), que requieren únicamente del certificado en el servidor de autenticación. La idea subyacente es que si el servidor de autenticación dispone de un certificado digital, el cliente podrá enviarle datos cifrados, creándose un "túnel de seguridad" por donde el cliente podrá enviar sus datos de autenticación.

PEAP fue diseñado por Microsoft, Cisco y RSA. 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, tras autentificar el servidor al cliente, ambos generan la clave de sesión.

2.3.6 WPA2 (IEEE 802.11i).

Es el nuevo Estándar del IEEE para proporcionar seguridad en redes WLAN. Incluye el nuevo algoritmo de cifrado AES (Advanced Encription Standard), desarrollado por el NIST. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requiere un hardware potente para realizar sus algoritmos. Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode/Cipher Block Chiang /Message Authentication Code Protocol) en lugar de los códigos MIC.

2.3.7 VPN (Redes Privadas Virtuales).

Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP. Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea dispositivos de capa 2 (Switch). Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

Tabla 2. Mecanismos para proteger redes inalámbricas.

	DESCRIPCIÒN	OBJETIVO
MECANISMOS BÀSICOS	Algoritmo de cifrado	Proporcionar privacidad de los datos. Ejemplo: TKIP-PPK o AES-CCM
	Integridad de los datos	Asegurar que no se han alterado los datos. Ejemplo: TKIP-MIC o AES-CBC-MAC
	Entorno de autenticación	Permitir el intercambio de mensajes entre los clientes, puntos de acceso y servidores AAA. Ejemplo: 802.1X/EAP
	Algoritmo de autenticación	Validar las credenciales de los clientes. Ejemplo: EAP-TTLS, PEAP, EAP-TLS
MECANISMOS AVANZADOS	Gestión segura de la red	SSH, SNMPv3, RADIUS, etc.
	Wireless IDS	Detectar puntos de acceso no autorizados, ataques activos, etc.
	Buenas practicas de integración entre la red cableada y la red inalámbrica	- Correspondencia de políticas de seguridad - Múltiples grupos de usuarios/dispositivos diferenciados (SSIDs, VLANs, túneles) -Uso de funcionalidades de seguridad tradicionales aplicados a los despliegues inalámbricos.

Fuente: Autor Proyecto

2.4 RSN (Robust Security Network)

El estándar IEEE 802.11i introduce el concepto de una RSN (Robust Security Network), red de seguridad robusta, que se define como una red inalámbrica que admite solamente la creación de RSNAs* (Robust Security Network Associations), es decir asociaciones robustas de seguridad que proporcionan niveles de aseguramiento medios a altos contra amenazas de seguridad con el uso de una variedad de técnicas criptográficas, además de permitir la protección de datos y ofrecer seguridad sobre WEP.

Las RSNAs permiten las siguientes características de seguridad para el estándar IEEE 802.11 en WLANs:

- Mecanismos de autenticación del usuario basados en 802.1x
- Administración de claves criptográficas
- Confidencialidad de los datos
- Autenticación e integridad del origen de los datos
- Protección contra la reproducción de tráfico

Los tres tipos de componentes de una RSN son las estaciones (STA), los puntos de acceso (AP) y servidores de autenticación (AS), siendo estos últimos un componente nuevo de la tecnología RSN.

2.4.1 Marco de Seguridad para una RSN.

Las RSNAs usan claves criptográficas que soportan derivado de claves, cifrado, autenticación y funciones de integración. El estándar IEEE 802.11i define dos claves jerarquías para RSNAs:

* Asociaciones de seguridad usada en una RSN

- **La clave de sesión (pairwise key).** Es única para cada asociación entre el cliente (STA) y el punto de acceso (AP), se diseña para la protección del tráfico unicast, creando un puerto virtual privado entre los dos.
- **La clave de grupo (groupwise key).** Se comparte por todas las estaciones clientes conectadas a un mismo punto de acceso y está prevista para la protección del tráfico multicast o broadcast.

Las claves de sesión, pueden ser instaladas en los dispositivos RSNA de dos formas:

- **Pre-Shared Key (PSK). Clave inicial compartida:** Es una clave estática compartida en las estaciones y punto de acceso; sólo se utiliza como punto de inicio para la autenticación, pero no para el cifrado de los datos.

  El estándar IEEE 802.11 no específica cómo PSKs debe ser generado o distribuido, así que estas decisiones se dejan a quien la implementa. Consecuentemente, se debe revisar cuidadosamente cualquier aproximación de PSK para las posibles vulnerabilidades y evaluar sus implicaciones de funcionamiento. PSK está orientado para usuarios domésticos o pequeñas redes.

- **Authentication, Authorization, and Accounting (AAA) - Key (AAAK).** También conocido como Master Session Key – MSK (clave de sesión principal), que se entrega al punto de acceso por medio de EAP (Protocolo Extensible de Autenticación) durante el proceso de creación de la RSNA.

  Cada vez que un usuario se autentica en la WLAN, la clave del AAA cambia; la nueva clave entonces se utiliza para la duración de la sesión del usuario. Las decisiones sobre los métodos apropiados de autenticación de

EAP se dejan para su implementación, teniendo en cuenta la revisión de este método.

El estándar 802.11i define dos protocolos para proporcionar confidencialidad e integridad a los datos para la RSNAs:

- **TKIP (Temporal Key Integrity Protocol). Protocolo de clave temporal de integridad:** TKIP es una solución de cifrado que mejora el protocolo WEP en cuanto al hardware basado en el estándar 802.11, para tratar las numerosas insuficiencias de WEP. TKIP se puede poner en ejecución a través de actualizaciones de software; no requiere el reemplazo del hardware de los puntos de acceso ni de los clientes. TKIP utiliza cifrado entre la estación cliente y el punto de acceso con clave simétrica, usa cuatro claves distintas para tráfico unicast y dos claves para tráfico broadcast y/o multicast.

- **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).** Este protocolo es complemento al TKIP y representa un nuevo método de cifrado basado en AES (Advanced Encryption Standards), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC. Así como el uso de TKIP es opcional, la utilización del protocolo CCMP es obligatorio si se está utilizando 802.11i.

  CCMP se considera la solución a largo plazo para el estándar IEEE 802.11 WLANs. CCMP requiere actualizaciones de hardware y es necesario sustituir el hardware de 802.11 WLAN.

Tabla 3. Protocolos de confidencialidad e integridad de datos

Características seguridad	WEP	TKIP (RSN)	CCMP (RSN)
Algoritmo criptográfico	RC4	RC4	AES
Tamaño clave	40 bits o 104 bits (cifrado)	128 bits (cifrado), 64 bits (protección integridad)	128 bits (cifrado y protección de integridad)
Función Per-Packet key	Creada a través de la concatenación de clave WEP y un IV de 24 bits	Creada con la función que mezcla TKIP	No es requerida, la clave temporal es lo suficientemente segura.
Mecanismo de integridad	Codificado CRC-32	MIC con contramedidas	CCM
Protección	Ninguna	Fuente y direcciones de destino protegidas por el algoritmo MIC (Message Integrity Code)	Fuente y direcciones de destino protegidas por CCM
Reproducción de tráfico	Ninguna	Cumplimiento de un VI secuencias	Cumplimiento de un IV secuencias
Autenticación	Sistema abierto o clave compartida	Método EAP con IEEE 802.1X o PSK	Método EAP con IEEE 802.1X o PSK
Distribución de claves	Manual	IEEE 802.1X o manual	IEEE 802.1X o manual

Fuente: Autor Proyecto

2.4.2 Principios de operación de una RSN.

IEEE 802.11 define cómo las tramas se intercambian entre STAs y el APs.

Hay tres tipos de tramas:

a) **Trama de datos**. Encapsulan los paquetes de la capa superior de protocolos, tales como IP, que alternadamente puede contener datos del uso (ejemplo: e-mail, páginas Web).

b) **Trama de administración.** Incluyen información de prueba y mensajes relacionados con la administración de eventos de asociación y autenticación.

c) **Trama de control.** Son usados para solicitar y controlar el acceso a los medios inalámbricos, por ejemplo como enviar un reconocimiento después de recibir una trama de datos.

Agrupando el intercambio de tramas por funciones, la operación podría ser como se aprecia en las siguientes fases:

2.4.2.1 Fase 1 Descubrimiento.

La STA identifica un AP* con el cual quiere comunicarse. La STA localiza el AP, mediante el intercambio de tramas de gestión, ya se recibiendo mediante las transmisiones periódicas un “beacon frame”, o enviando un “Probe Request”. Una vez el STA haya identificado el AP, se realiza la negociación para la comunicación. Para el final de la fase, el STA y el AP han establecido una política de seguridad que especifica capacidad de claves seguras, tales como confidencialidad en los datos e integridad de los protocolos para la protección del tráfico, un método de autenticación, y una clave de distribución.

* De aquí en adelante se utilizará la sigla AP para hacer referencia a un Punto de Acceso de una red inalámbrica

2.4.2.2 Fase 2 Autenticación.

Durante esta fase, el STA y AS prueban sus identidades para cada uno. Las tramas autenticadas pasan por el AP, con lo cual también los bloques de tráfico no autenticado del STA usando IEEE 802.1X. El mecanismo real de autenticación es puesto en ejecución por el STA y AS usando EAP, que proporciona una trama que permite el uso de múltiples métodos para alcanzar la autenticación, incluyendo claves estáticas, claves dinámicas, y certificados criptográfico de claves públicas. Después de que se haya terminado la autenticación, la clave AAA es instalada en el STA y AS; sirve como clave root para permitir la generación de otras claves usadas para asegurar comunicaciones entre el STA y el AP.

2.4.2.3 Fase 3 Generación y distribución de claves.

Durante esta fase el AP y el STA realizan varias operaciones que hacen que las claves criptográficas se generen y se coloquen en AP y el STA. Se emplean dos tipos de handshakes: Way handshakes y Group Key handshakes. Ambos emplean el cifrado y la integridad del mensaje que comprueban, usando uno de los dos algoritmos de confidencialidad e integridad. Para ambos tipos el NIST requiere el uso de claves AES con HMAC-SHA-1-128 en lugar del cifrado RC4 con HMAC-MD5 porque AES y SHA-1 son algoritmos aprobados y RC4 o MD5 no lo son.

2.4.2.4 Fase 4 Transferencia de datos protegidos.

El STA y el AP comparten datos con seguridad, usando políticas de seguridad y el cifrado de claves establecidas durante las primeras tres fases. Porque la transferencia de datos segura ocurre entre el STA y el AP solamente, se requiere considerar cuidadosamente la seguridad de los datos durante el resto de su tránsito, como por ejemplo en el DS (Sistema de distribución, permite la interconexión de forma transparente entre el STA y el AP)

2.4.2.5 Fase 5 Terminación de la conexión.

Durante esta fase, el STA y el AP terminan su conexión segura y eliminan su asociación, de tal modo terminando su la conexión inalámbrica.

El esquema de RSN introduce la fase de la autenticación, la fase de generación y distribución de claves, y la fase de la terminación de la conexión en la operación de IEEE 802.11. Antes de IEEE 802.11i, IEEE 802.11 operaba involucrando autenticación rudimentaria, pero solamente como parte de la fase del descubrimiento. RSN también introduce nuevos elementos y técnicas en las otras fases, pero la naturaleza básica del diálogo sigue siendo igual.

Si se desea establecer IEEE 802.11 RSNs, se deben configurar los APs de modo que permitan el establecimiento de RSNAs solamente. Durante la fase del descubrimiento, si un AP permite una asociación WEP en alguna STA, entonces esa asociación no es una RSNA, y por consiguiente la WLAN no es una RSN. Todas las asociaciones deben ser RSNAs para que la WLAN sea considerada una RSN. El permitir asociaciones basadas en WEP crea agujeros significativos de seguridad que pueden afectar negativamente la seguridad de los otros componentes de la WLAN. Las comunicaciones entre algún STAs y el APs no serán protegidas fuertemente, además, configurar el APs para permitir el uso de las capacidades de pre-RSN podría permitir que los atacantes dentro de la gama del AP establezcan conexiones no autorizadas a él, accediendo potencialmente a otros recursos.

3. SITUACIÓN ACTUAL DE SEGURIDAD EN LA WLAN DE LA UNIVERSIDAD

Las redes inalámbricas requieren medidas de seguridad superiores a las redes cableadas, debido a las vulnerabilidades físicas que posee esta tecnología. De este punto de visa, se definen las características necesarias para mantener el nivel de seguridad requerido para la WLAN.

Este documento presenta algunas generalidades sobre WLAN, los conceptos sobre redes inalámbricas, el estado actual de la infraestructura existente en la UIS, se incluyen los riesgos detectados, además se indica como se pueden ser tratados. Finalmente, se propone a la Universidad la migración hacia una RSN partiendo de una solución a corto plazo, y continuando con una solución a largo plazo para ofrecer un entorno inalámbrico con un nivel apropiado de seguridad.

3.1 ANTECEDENTES

En la actualidad se está viviendo una evolución acelerada de la tecnología inalámbrica con el fin de facilitar la movilidad manteniendo la conectividad a la red. En este sentido la Universidad Industrial de Santander, en el año 2005, decidió iniciar un proyecto para dotar a diferentes unidades académicas de conexión inalámbrica con el objetivo de mejorar la flexibilidad de la red y aumentar la productividad de su personal. La Universidad apostó en dicho momento por utilizar dicha tecnología para ofrecer servicios de conexión a la red LAN en determinadas situaciones o ubicaciones donde dicha solución generaba menores costos y aumento de la productividad.

El proyecto inició con la adquisición de dispositivos inalámbricos (Puntos de Acceso y Tarjetas inalámbricas), manejando marcas como D-Link, y

posteriormente con nuevos productos en el mercado se adquirieron equipos LinkSys y actualmente se adquirieron dispositivos inalámbricos de la marca 3com ; lo anterior basado en un análisis de las prestaciones que ofrecían los diferentes productos en ese momento disponibles en el mercado, así como la previsión de nuevas funcionalidades previstas por cada fabricante. De este análisis y de una prueba piloto destacando el funcionamiento de los equipos realizada en la División de Servicios de Información, se determinó la utilización de equipos de estos fabricantes.

Actualmente, en el Campus principal de la Universidad existen instalados 12 puntos de acceso, que hacen parte del inventario de la WLAN, relacionados en el Anexo A.

3.2 TIPOLOGÍA DE USUARIOS

El servicio inalámbrico de la Universidad permite la conectividad a la red de datos por parte del personal interno y en algunos casos de personal externo como visitantes debidamente autorizados para usar este servicio, que por reuniones programadas u otra circunstancia hacen uso de portátiles como estación de trabajo.

3.2.1 Perfil Externo.

Este perfil permite a los usuarios que visitan las instalaciones de la Universidad acceder a Internet para navegar o leer el correo electrónico o ingresar a los servicios de la Intranet. Generalmente se realiza el acceso con motivo de una reunión o conferencia.

El acceso a la red inalámbrica es inmediato por parte del usuario ya que no se requiere de autenticación alguna. El objetivo es facilitar el acceso a la red mediante el “broadcast” del identificador de la red inalámbrica y utilizando el método “Open Authentication” para asociarse al punto de acceso.

Las ubicaciones físicas que actualmente dan servicio al perfil externo son básicamente la Rectoría, sala de Consejos y salas alternas ubicadas en el edificio de Administración.

3.2.2 Perfil Interno.

Este perfil permite al usuario el acceso a la Intranet a la vez que a Internet, y a los diferentes sistemas de información que soportan los procesos de las Unidades Académicos Administrativas como es el caso del Sistema Financiero, Académico etc., permitiendo acceder a todas las aplicaciones al igual como se realiza cuando la red es cableada. En el perfil interno se contemplan los docentes, administrativos e incluso para el servicio de Internet proporcionado por la Biblioteca Central para los estudiantes. Estas dependencias y el esquema de seguridad pueden apreciarse en el Anexo A.

3.3 AMBIENTE DE TRABAJO DE LA WLAN

3.3.1 Métodos de Configuración.

Existen varios métodos para el esquema de seguridad actual de las WLAN de la Universidad entre estos se encuentran:

3.3.1.1 Filtrado de direcciones MAC.

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. Este proceso es realizado por un funcionario de la División de Servicios de Información encargado de configurar el equipo y actualizar esta información en el sistema de administración de la red. Para el caso de la Biblioteca, se tiene un formato (Anexo C), donde se registra los datos pertenecientes a los equipos que hacen uso del servicio de Internet.

3.3.1.2 Wired Equivalent Privacy (WEP).

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

Estos esquemas de seguridad son inadecuados e ineficientes, dado el esfuerzo en recurso humano destinado para la administración de las listas de control de acceso, y la vulnerabilidad descubierta en el protocolo WEP para descubrir la contraseña. En el anexo D. se aprecia una prueba para romper el cifrado wep en una WLAN.

3.4 ANÁLISIS DE RIESGOS DE LA INFRAESTRUCTURA INALÁMBRICA

De acuerdo al inventario y la configuración de los parámetros de seguridad de las redes inalámbricas, los posibles riesgos a los que está sometida la infraestructura WLAN de la Universidad son:

- No contar con registros de auditoria en caso de presentarse un incidente y/o para realizar monitoreo como acción preventiva.

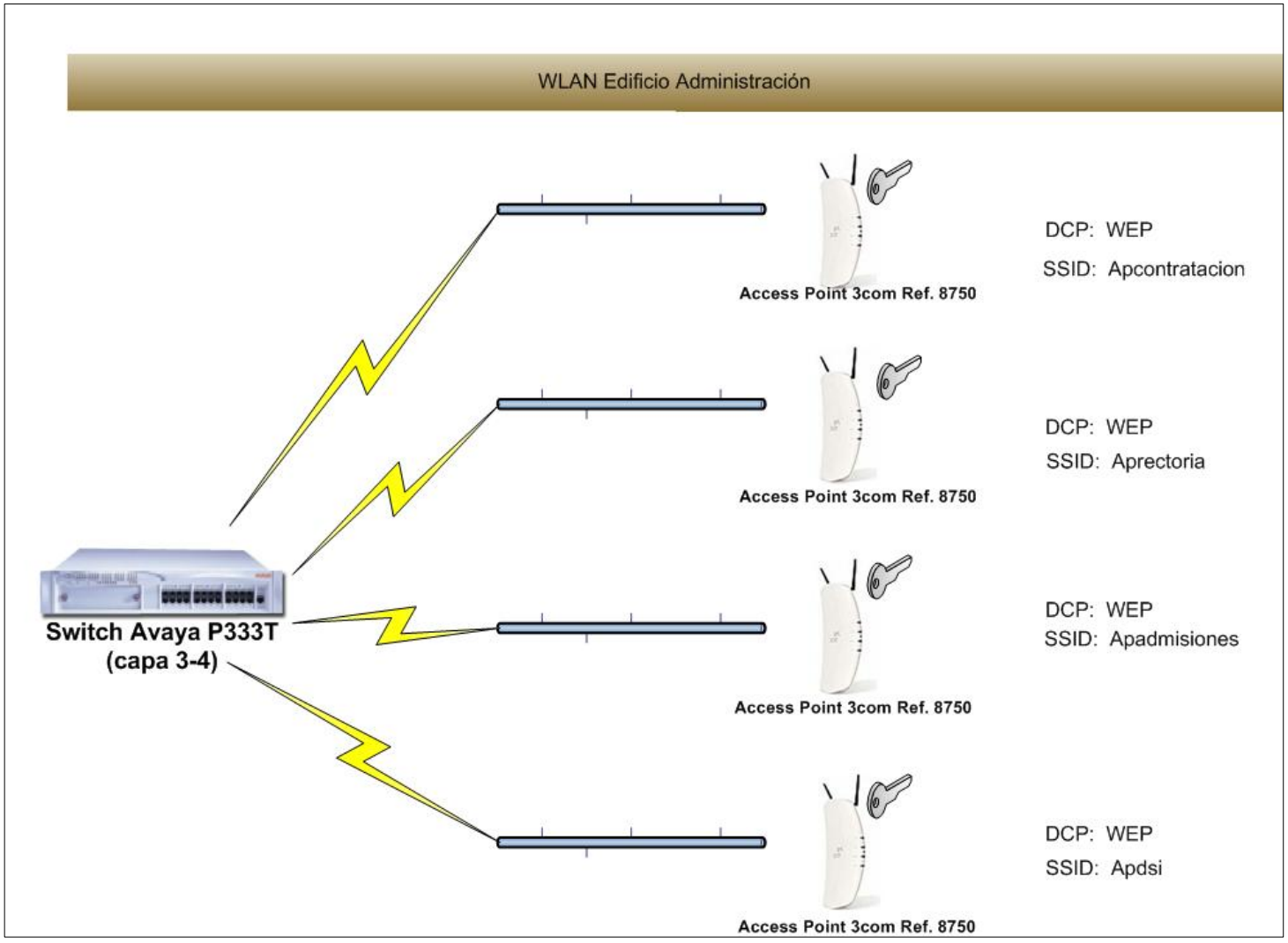
- Daño, pérdida de equipos o información por la falta de políticas, normas y procedimientos relacionados con la administración de las redes inalámbricas.

- Fuga de información por la falta de conciencia en seguridad por parte de los usuarios.

- Pérdida de confidencialidad, integridad o disponibilidad por la falta de una configuración adecuada de seguridad de las redes inalámbricas (Tanto equipos de red como clientes). Entre estos:
    - Configuración por defecto
    - SSID por defecto
    - SSID habilitado
    - Comunicación no cifrada
    - Sin autenticación de usuarios
    - DoS
- Multas por no licenciamiento del Software.
- Indisponibilidad del servicio y/o degradación del servicio.
- No contar con una protección física adecuada de los dispositivos de red (Punto de acceso).

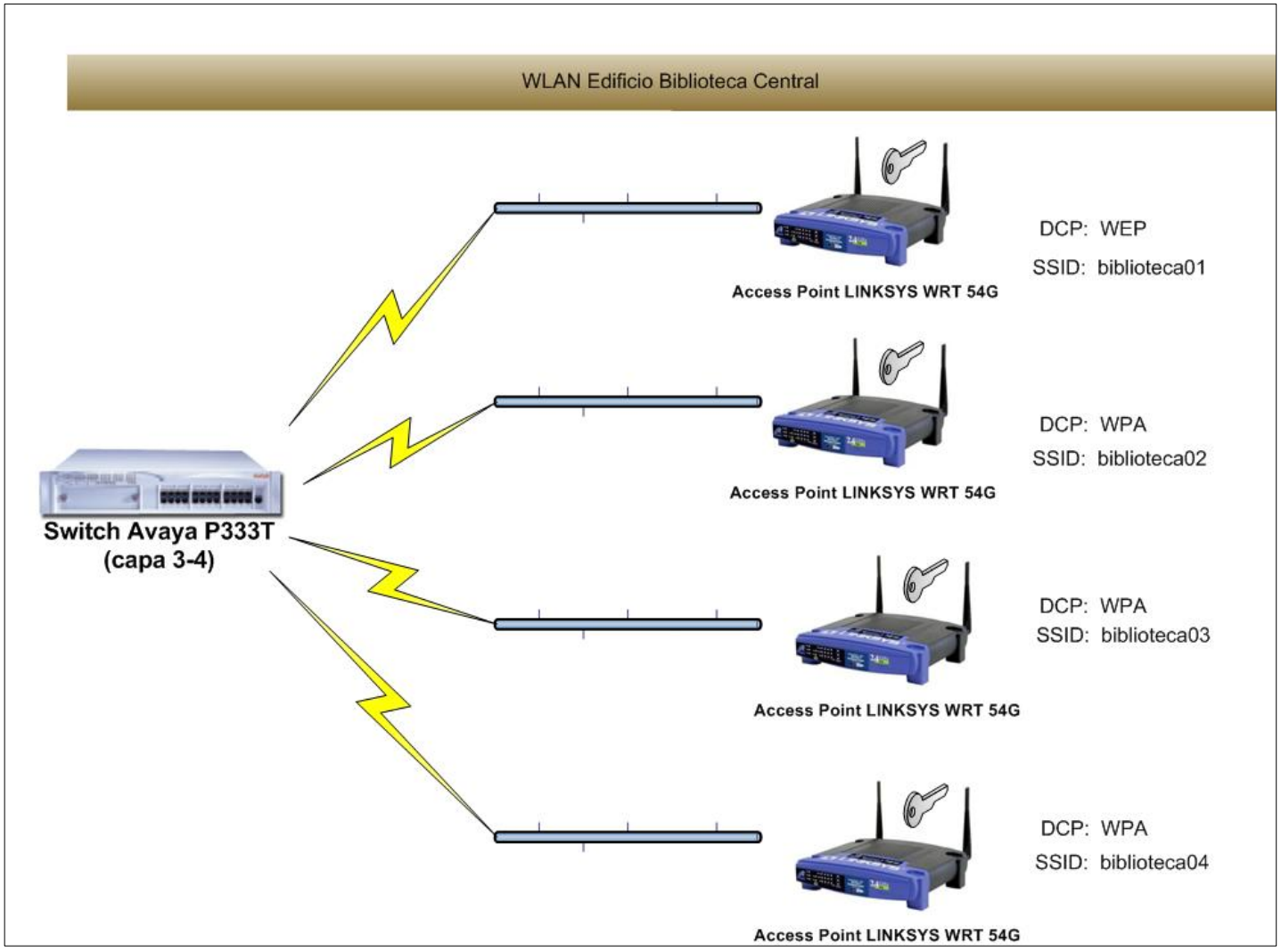
En las Figuras 15, 16 y 17 se presentan la infraestructura actual de seguridad de las WLANs en la Universidad.

Figura 15. Esquema de seguridad WLAN Edificio Administración



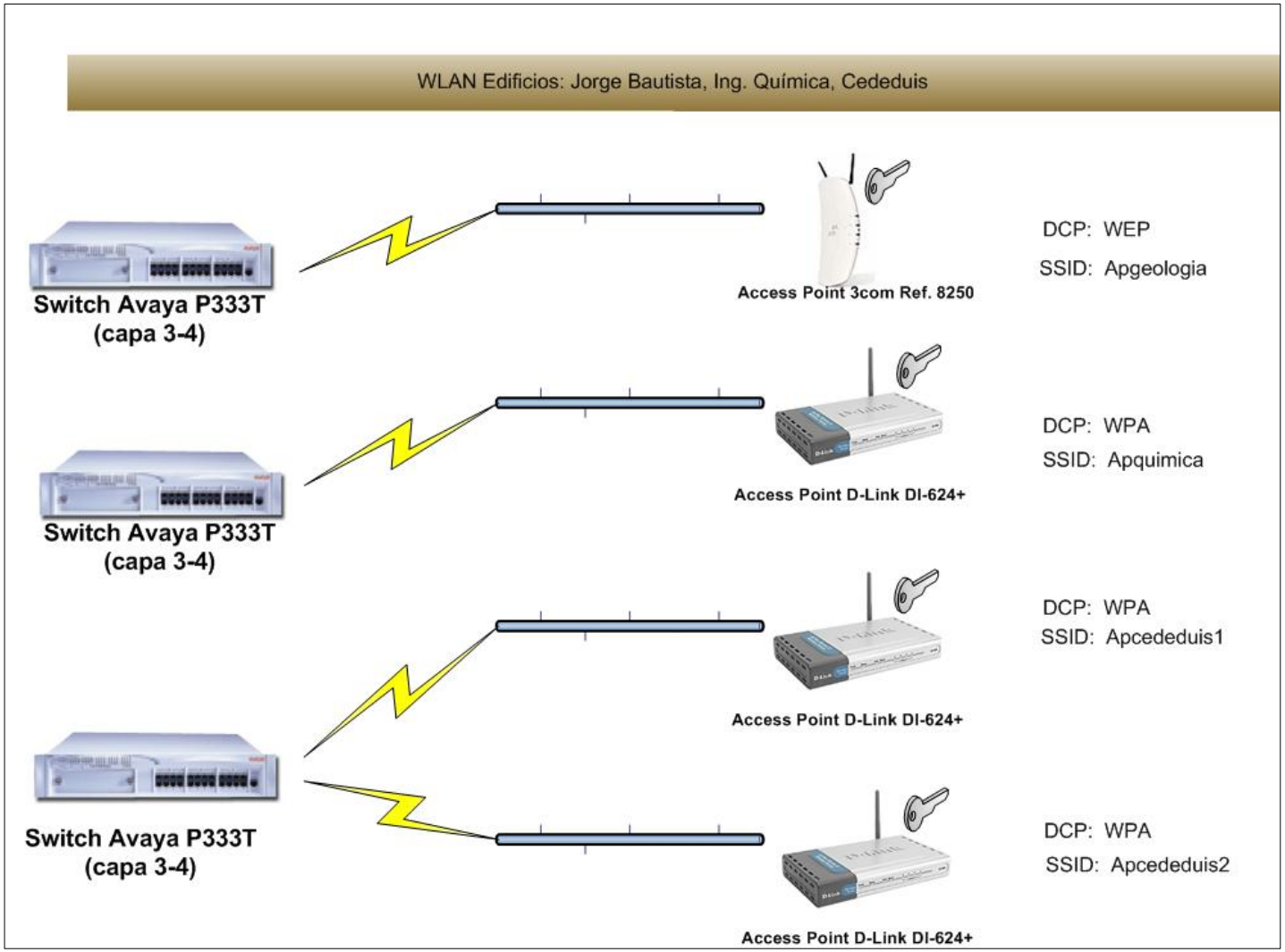
Fuente: Autor Proyecto

Figura 16. Esquema de seguridad WLAN Edificio Biblioteca Central



Fuente: Autor Proyecto

Figura 17. Esquema de seguridad WLAN Edificio (CDPA, Jorge Bautista Vesga, e Ingeniería Química)



Fuente: Autor Proyecto

4. ESQUEMA DE SEGURIDAD PARA LAS WLANs DEL CAMPUS PRINCIPAL DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

El estudio de las prestaciones y limitaciones del nuevo estándar 802.11 rápidamente lleva a determinar que el problema principal de esta tecnología no es la velocidad sino la seguridad.

Por consiguiente, la valoración de las distintas soluciones que se pueden adoptar para dotar a las comunicaciones inalámbricas del nivel de seguridad requerido por la Universidad, incluye aspectos completamente ajenos a la temática de la seguridad en las comunicaciones pero no por ello menos importantes como la complejidad del mantenimiento de la solución, la inversión inicial, la solución basada en estándares, la escalabilidad, integración con el software del punto de trabajo actual y el futuro de las WLAN de la Institución.

4.1 POLÍTICAS DE SEGURIDAD

Aparte de las medidas que se hayan tomado en el diseño de la red inalámbrica, se deben aplicar ciertas normas y políticas de seguridad que ayudan a mantener una red más segura:

- Emplear herramientas que permitan realizar controles periódicos para la detección de redes inalámbricas, análisis de tráfico y medir potencias irradiadas con cualquier tarjeta desde los perímetros de la red.

- Mejorar la seguridad física.

- Cancelar puertos que no se emplean.

- Limitar el número de direcciones MAC que pueden acceder. Esta actividad se realiza por medio de ACLs (Access List Control) en los AP.

- Satisfacer la demanda: Si se están empleando AP no autorizados por parte de los empleados, es porque les resulta útil, por lo tanto, se pueden adoptar las medidas para que se implanten, pero de forma segura y controlada, de otra forma, seguirán apareciendo, pero de forma clandestina.

- Controlar el área de transmisión: muchos puntos de acceso inalámbrico permiten ajustar el poder de la señal, colocando sus puntos de acceso tan lejos como sea posible de las paredes y ventanas exteriores. Verificando el poder de la señal para que usted únicamente pueda conectarse a estos sitios.

- Asegurar el cambio de contraseña predeterminada en todos los puntos de acceso, se recomienda utilizar una contraseña fuerte para proteger todos los puntos de acceso.

- Implementar la autenticación de usuario: Mejorando los puntos de acceso para usar las implementaciones de las normas WPA y 802.11i.

- Proteger la WLAN con la tecnología “VPN Ipsec” o tecnología “VPN clientes”: esta es la forma más segura de prestar servicios de autenticación de usuario e 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.

- Activar el mayor nivel de seguridad que soporta el hardware: incluso si se tiene un equipo de un modelo anterior que soporta únicamente WEP, asegurarse de activarlo. En lo posible, utilizar por lo menos una WEP con un mínimo de cifrado de 128 bits.

- Instalar firewalls personales y protección antivirus en todos los dispositivos móviles: la Alianza Wi-Fi recomienda utilizar la política de seguridad de redes corporativas para imponer su uso continuo.

- Adquirir dispositivos inalámbricos que respondan a los estándares y certificado por “Wi-Fi Alliance”.

- Utilizar mecanismos de intercambio de clave dinámica aportado por los diferentes productos comerciales.

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

- Actualizar el Firmware de los puntos de acceso para cubrir los posibles agujeros en las diferentes soluciones inalámbricas.

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

- Cambiar el SSID por defecto de los puntos de acceso, conocidos por todos.

- Inhabilitar la emisión broadcast del SSID

4.2 RECOMENDACIONES DE SEGURIDAD

Con base en la identificación de riesgos, en la siguiente tabla se aprecia una lista de comprobación de seguridad para redes inalámbricas, donde se presentan pautas y recomendaciones para limitar la probabilidad de ocurrencia del mismo. Cada recomendación, presenta tres columnas. La primera columna, “la mejor práctica”, si está seleccionada, significa que esta aplicada. La segunda columna, "debe considerar", si está seleccionada, propone la consideración de esta recomendación por tres razones:

- Implementar la recomendación puede proporcionar un nivel más alto de seguridad para el ambiente inalámbrico.

- La recomendación apoya una estrategia de defensa en profundidad.

- Puede tener impactos significativos en el funcionamiento, operación o costo.

Tabla 4. CheckList de seguridad WLAN

Recomendaciones de Seguridad		La mejor Práctica	Debería Considerarse	Estado
Recomendaciones de Administración				
1.	Dentro de las políticas de seguridad se contempla el uso de las tecnologías inalámbricas, incluyendo el estándar 802.11.	✓		✓
2.	Garantizar el entrenamiento a los usuarios de la red respecto al conocimiento de la seguridad de la computadora y los riesgos que están asociados a la tecnología inalámbrica.	✓		✓
3.	Realizar una valoración de riesgo para entender el valor de los activos que necesita la protección.	✓		
4.	Revisar que las tarjetas inalámbricas y los AP soportan actualizaciones de firmware mientras que los parches de seguridad pueden estar disponibles (antes de comprar)	✓		✓
5.	Realizar las evaluaciones respectivas de la seguridad en los intervalos regulares y al azar para verificar el estado de la seguridad inalámbrica en la red.	✓		✓
6.	Revisar la protección externa respecto al límite del perímetro de los edificios del Campus Universitario.	✓		✓
7.	Extender los controles de acceso físico al edificio y a otras áreas seguras	✓		
8.	Completar un Site Survey sobre el sitio para medir y para establecer la cobertura del AP.	✓		✓

Recomendaciones de Seguridad		La mejor Práctica	Debería Considerarse	Estado
9.	Realizar un inventario completo de todos los dispositivos inalámbricos y APs.	✓		✓
10.	Cerciorarse que las redes WLAN no sean utilizadas hasta tanto no se configuren con las políticas de seguridad establecidas.	✓		✓
11.	Localizar los APs en el interior del edificio en lugar de las paredes y ventanas exteriores cercanas.	✓		✓
12.	Colocar el AP en áreas aseguradas para prevenir el acceso y la manipulación física de usuarios desautorizados.	✓		
Recomendaciones Técnicas				
13.	Revisar los límites de la gama del AP para determinar el grado exacto de la cobertura inalámbrica.	✓		
14.	Cerciorarse que los APs sean apagados cuando no se usen.	✓		
15.	Garantizar que la función reset en el APs se esté utilizando solamente cuando es necesario y sea ejecutada por un grupo de funcionarios autorizados.	✓		
16.	Restaurar el AP a la configuración mas reciente de seguridad cuando se haya utilizado la función reset.	✓		✓
17.	Cambiar el SSID por defecto en el AP.	✓		✓
18.	Deshabilitar la característica de broadcast SSID de modo que el cliente SSID deba detectar el del AP.		✓	
19.	Validar que la cadena de caracteres del SSID no refleja el nombre de la Universidad (división, departamento, calle, etc.) o productos.	✓		

Recomendaciones de Seguridad		La mejor Práctica	Debería Considerarse	Estado
20.	Asegurarse que los canales del AP sean por lo menos cinco canales diferentes de otra red inalámbrica próxima para prevenir interferencia.	✓		✓
21.	Entender y cerciorarse que todos los parámetros de defecto deben ser cambiados.	✓		✓
22.	Deshabilitar todos los protocolos inseguros y no esenciales en el APs.	✓		
23.	Habilitar todas las características de la seguridad del dispositivo WLAN, incluyendo la característica criptográfica de autenticación y de aislamiento de WEP.	✓		✓
24.	Asegurarse de que los tamaños dominantes del cifrado sean por lo menos 128 bits o tan grandes como sea posible.	✓		✓
25.	Cerciorarse que las llaves compartidas por defecto sean substituidas periódicamente por llaves únicas más seguras.	✓		
26.	Instalar un firewall configurado correctamente entre la infraestructura cableada y la red inalámbrica.	✓		✓
27.	Instalar software antivirus en todos los clientes inalámbricos	✓		
28.	Instalar software personal firewall en todos los clientes inalámbricos	✓		
29.	Deshabilitar carpetas compartidas en clientes inalámbricos (especialmente en desconocidos ambientes).	✓		
30.	Utilizar las listas del control de acceso por MAC.		✓	✓
31.	Considerar la instalación de switches capa dos en lugar de hubs para la conectividad de los APs.	✓		✓

Recomendaciones de Seguridad		La mejor Práctica	Debería Considerarse	Estado
32.	Utilizar Ipsec basada en VPN para las comunicaciones inalámbricas		✓	
33.	Confirmar que el cifrado utilizado sea suficiente dado la sensibilidad de los datos sobre la red y de las velocidades del procesador de las computadoras.	✓		
34.	Experimentar y realizar parches y actualizaciones de software de forma regular.	✓		✓
35.	Corroborar que todos los APs posean contraseñas de administración fuertes.	✓		✓
36.	Controlar que todas las contraseñas sean cambiadas regularmente.	✓		✓
37.	Establecer la autenticación del usuario, por ejemplo: tarjetas inteligentes, autenticación de dos factores y PKI		✓	
38.	Constatar que el modo Ad Hoc haya sido deshabilitado en estándar 802.11, a menos que el riesgo en el ambiente sea tolerable. Algunos productos no permiten deshabilitar esta característica, usar con precaución.	✓		
39.	Usar direcciones IP estáticas en la red.		✓	✓
40.	Deshabilitar DHCP		✓	✓
41.	Habilitar los mecanismos de autenticación del usuario para los interfaces de administración de los APs.	✓		
42.	Examinar que el tráfico de administración destinado para el APs esté en una subred cableada.	✓		✓
43.	Utilizar SNMPv3 y/o SSL/TLS para la administración Web de los APs	✓		✓

Recomendaciones de Seguridad		La mejor Práctica	Debería Considerarse	Estado
Recomendaciones Operacionales				
44.	Configurar los ajustes del SNMP en el APs para menos privilegio (es decir, sólo lectura). Inhabilitar el SNMP si no se utiliza. SNMPv1 y SNMPv2 no se recomiendan.	✓		
45.	Establecer la seguridad para el tráfico de administración del AP usando SNMPv3 o un protocolo de protección criptográfica.	✓		
46.	Utilizar una interfaz local por puerto serial para la configuración del AP con el fin de reducir al mínimo la exposición de la información de administración.		✓	
47.	Considerar otras formas de autenticación para la red inalámbrica como por ejemplo: RADIUS, Kerberos.		✓	
48.	Revisar los agentes de detección de intrusos en la parte inalámbrica de la red para detectar el comportamiento sospechoso o acceso y actividad desautorizados.		✓	
49.	Adoptar la revisión de tecnología para analizar los expedientes producidos por RADIUS para la actividad sospechosa.		✓	
50.	Utilizar un producto de seguridad 802.11 que ofrezca características criptográficas realzando la autorización de la protección o del usuario.		✓	✓
51.	Habilitar la utilización de llaves key-mapping (802.1X) en lugar de las llaves por defecto de manera que las sesiones usen distintas llaves WEP.	✓		
52.	Conocer completamente los impactos de utilizar cualquier característica o producto de seguridad.	✓		✓

Recomendaciones de Seguridad		La mejor Práctica	Debería Considerarse	Estado
53.	Designar un funcionario para continuar con los productos y estándares de seguridad 802.11 (IETF, IEEE, etc.), amenazas y las vulnerabilidades de esta tecnología.		✓	✓
54.	Estar atentos a lanzamientos futuros de tecnología WLAN 802.11 que incorporen arreglos a las características de la seguridad.		✓	✓
55.	Cuando se disponga de APs que no tendrán un uso prolongado deshabilitar la configuración para prevenir el acceso a la configuración de red, de llaves, de contraseñas, etc.	✓		✓

Fuente: Autor Proyecto

4. 3 MITIGACIÓN DE RIESGOS

4.3.1 Contramedidas de Administración.

Las disposiciones de administración para asegurar las redes WLAN se inician con una política comprensiva de seguridad. Una política que integre entre otras, medidas de tipo operacional y técnico. Las políticas de seguridad de WLAN adoptadas por la Universidad debe contemplar lo siguiente:

- Identificar que dependencias pueden utilizar la tecnología WLAN.
- Determinar si el acceso del Internet es requerido.
- Definir quién puede instalar los puntos de acceso y las tarjetas inalámbricas.
- Proporcionar los límites en la localización de los puntos de acceso para su seguridad física.
- Detallar el tipo de información que se puede enviar sobre la red WLAN.
- Describir las condiciones bajo las cuales se permiten los dispositivos de red inalámbricos.
- Definir la configuración de los estándares de seguridad para los puntos de acceso.
- Especificar las limitaciones respecto a cómo el dispositivo inalámbrico puede ser utilizado.
- Precisar la configuración del hardware y del software de todos los dispositivos inalámbricos.
- Proporcionar las pautas en la divulgación de pérdidas de dispositivos y de incidentes.
- Aportar las pautas para la protección de clientes inalámbricos para reducir al mínimo el hurto de los mismos.

La Universidad debe asegurarse del entrenamiento de todo el personal crítico en el uso de la tecnología inalámbrica. Los administradores de la red necesitan estar

completamente informados de los riesgos de la seguridad WLAN. Se debe trabajar en asegurar las políticas de seguridad y saber qué decisiones tomar para contrarrestar el acontecimiento de un ataque.

4.3.2 Contramedidas operacionales.

La seguridad física es el paso más fundamental para asegurar que solamente los usuarios autorizados tengan acceso al material inalámbrico. La seguridad física combina medidas tales como:

- Controles de acceso.
- Identificación del personal encargado del área inalámbrica.
- Protección tanto externa como de las instalaciones que contienen redes cableadas, teniendo en cuenta el control de acceso físico. La protección externa puede incluir la fijación de puertas y la instalación de las cámaras de vídeo para la vigilancia alrededor del perímetro para controlar el acceso desautorizado a los componentes inalámbricos de la red.

Es importante considerar la gama del AP, para decidir en donde colocar un AP en un ambiente WLAN. Si la gama se extiende más allá de los límites físicos de las paredes del edificio de oficinas, la extensión crea una vulnerabilidad de la seguridad. En el exterior del edificio, se podría detectar la red usando un dispositivo inalámbrico que tome las emanaciones del RF.

Una consideración similar se aplica a la puesta en práctica de los bridges de edificio a edificio. Idealmente, el AP se debe colocar estratégicamente dentro de un edificio de modo que la gama no exceda el perímetro físico del edificio y no permita que el personal desautorizado lo detecte cerca del perímetro. En este caso se deben utilizar herramientas de pruebas en sitio para medir la gama de los dispositivos del AP, tanto en el interior como en el exterior del edificio donde se localiza la red inalámbrica. Además, se debe utilizar herramientas para seguridad

inalámbrica por ejemplo para determinar la vulnerabilidad de la WLAN, y regularmente programar controles de seguridad como auditorias a éstas.

Las herramientas de Site Survey están disponibles para medir y asegurar la cobertura del AP. Estas herramientas, que algunos vendedores incluyen con sus productos, permiten medir la fuerza recibida de la señal del AP. Estas medidas se pueden utilizar para planear el área de la cobertura. Sin embargo, los administradores de la seguridad deben tener cuidado al interpretar los resultados porque cada vendedor interpreta la fuerza recibida de la señal de diferente forma.

Algunos productos de los proveedores de AP también tienen características especiales que permiten el control de los niveles de energía y por lo tanto de la gama del AP. Esto es útil si la gama requerida para la cobertura no es amplia como es el caso cuando en el edificio o el cuarto el acceso a la red inalámbrica suele ser pequeño. Controlar la gama de la cobertura para este edificio o sitio más pequeño puede ayudar a evitar que las señales inalámbricas se extiendan más allá del área prevista. Se podría utilizar además las antenas direccionales para controlar emanaciones. Sin embargo, las antenas direccionales no protegen acoplamientos de la red; simplemente ayudan a controlar la gama de la cobertura limitando la dispersión de la señal.

Aunque planear el área de cobertura puede generar alguna ventaja relativa a la seguridad, no debe ser visto como solución absoluta. Hay siempre la posibilidad que un individuo puede utilizar una antena high-gain para detectar el tráfico de la red WLAN. Debe existir claridad respecto que solamente con el uso de medios criptográficos fuertes se puede mantener un límite de seguridad contra los adversarios.

4.3.3 Contramedidas Técnicas.

Estas contramedidas implican el uso de soluciones de hardware y software de para ayudar a la seguridad de la red inalámbrica. Las contramedidas del software incluyen configuraciones apropiadas del AP (es decir, el ambiente operacional y de configuración de seguridad del AP), actualizaciones y mejoras del software, autenticación, sistemas de detección de intrusos y cifrado. Las soluciones de hardware incluyen las tarjetas inteligentes, VPNs, infraestructura dominante pública (PKI) y biometría. Como se observa más adelante, las soluciones de hardware, que tienen generalmente componentes de software se enumeran simplemente como soluciones de hardware.

4.3.3.1 Soluciones de software.

Las contramedidas técnicas implican el software, realizando una correcta configuración de los puntos de acceso, actualización del software, incluyendo la autenticación y soluciones de identificación, realizando intervenciones de la seguridad, y adoptando un cifrado eficaz.

Los administradores de la red necesitan configurar los APs de acuerdo con las políticas y requisitos de seguridad establecidos. La configuración correcta de las contraseñas administrativas, ajustes del cifrado, función de reset, función automática de conexión de red, listas del control de acceso, llaves compartidas, y los agentes de SNMP (Simple Network Management Protocol) ayudarán a eliminar muchas de las vulnerabilidades inherentes en la configuración por defecto del software.

a) Configuración de Access Point.

- **Actualización de contraseñas por defecto**. Cada dispositivo WLAN viene con su propia configuración por defecto, algunas de las cuales intrínsecamente contienen vulnerabilidades de seguridad. La contraseña del administrador es un ejemplo típico. En algunos APs, la configuración

por defecto de fábrica no requiere una contraseña (es decir, el campo de la contraseña está en blanco). Los usuarios no autorizados pueden acceder fácilmente al dispositivo si no hay protección de contraseña.

Los administradores deben cambiar esta configuración por defecto para reflejar la política de seguridad, que debe incluir como requisito (por ejemplo: una cadena de caracteres es decir, alfanumérica y especial por lo menos ocho caracteres en longitud) las contraseñas administrativas fuertes. Si el requisito de la seguridad es suficientemente alto, se debe considerar usar un generador automatizado de la contraseña. Una alternativa para la autenticación de la contraseña son los sistemas de autenticación de dos factores. Los sistemas de autenticación de dos factores superan los problemas de autenticación asociados a una sola clave solicitando un segundo dato secreto. En la autenticación de dos factores se utiliza una combinación de los siguientes elementos:

- Algo que posee el usuario, como un testigo (token) de hardware o una tarjeta inteligente.
- Algo que el usuario sabe, como un número de identificación personal (PIN).

Varios productos comerciales proporcionan esta capacidad. Sin embargo, el uso de un generador de la contraseña o de un mecanismo automatizado de la autenticación de dos factores puede no garantizarse en la inversión, pues depende de los requisitos de la seguridad que se establezcan, del número de usuarios, y del presupuesto destinado. Dada la necesidad de asegurar la buena autenticación y políticas de contraseña, es importante destacar la importancia crítica de asegurar protección criptográfica apropiada para prevenir el acceso desautorizado de las contraseñas. Existen mecanismos numerosos que se pueden explotar para asegurar el acceso cifrado tales como Shell seguro (SSH) y el SSL.

- **Establecer ajustes apropiados de cifrado**. Los ajustes de cifrado se deben configurar con el cifrado más fuerte disponible en el producto, dependiendo de los requisitos de la seguridad establecidos. Típicamente, el AP tiene solamente algunos ajustes de cifrado disponibles:

  - Ninguno
  - Llave compartida 40-bits
  - Llave compartida 104-bits (siendo el más fuerte).

  Es importante observar que los productos que usan 128-bits, no son compatibles con los que usan 104-bits.

- **Controlar la función de reajuste**. La función de reajuste plantea un problema particular porque permite que un individuo niegue cualesquiera de los ajustes de seguridad que los administradores hayan configurado en el AP, volviendo el AP a la configuración por defecto de fábrica. Los ajustes por defecto no requieren generalmente una contraseña administrativa, y se puede deshabilitar el cifrado. Un individuo puede reajustar la configuración por defecto, simplemente insertando un objeto acentuado tal como una pluma en el orificio del reset y presionando. Si un usuario malévolo tiene el acceso físico al dispositivo, ese individuo puede utilizar la característica del reajuste y cancelarla. La función de reajuste, si está configurada para borrar la información operacional básica tal como IP address o llaves, puede dar lugar más lejos a un DoS de la red, porque el AP no puede funcionar sin esta configuración.

  Tener controles de acceso físico en el lugar para prevenir los usuarios desautorizados del AP, puede atenuar las amenazas. Se puede detectar amenazas realizando intervenciones regulares de seguridad. Además, el reajuste se puede invocar remotamente sobre la interfaz de administración

en algunos productos. Por esta razón, hay una mayor necesidad de tener la administración y cifrado apropiados de las contraseñas.

b) **Usar la funcionalidad de control de acceso por MAC.** Muchos proveedores proporcionan las capacidades para restringir el acceso a las WLAN basados en el MAC ACLs, sin embargo no representa un mecanismo de defensa fuerte por sí mismo, porque las direcciones pueden ser capturadas fácilmente y el usuario malévolo puede cambiar la MAC address real en su computadora a un MAC address que tenga acceso a la red inalámbrica.

   Estas contramedidas pueden proporcionar un cierto nivel de seguridad, sin embargo los usuarios deben utilizar esto con precaución Los usuarios si desean, pueden considerar esto como parte de adición de niveles de estrategia de defensa en profundidad total de la seguridad para reducir la probabilidad de problemas. Sin embargo, los usuarios deben determinar la carga administrativa para permitir el MAC ACL (se asume están utilizando el MAC ACLs) contra la seguridad verdadera proporcionada. En una red grande, la carga del MAC que establece y que mantiene ACLs puede exceder el valor de las medidas de seguridad. Además, la mayoría de los productos mantienen solamente un número limitado de direcciones MAC en el MAC ACL. El tamaño del Access Control List puede ser escaso para las redes grandes.

c) **Actualizaciones de Software.** Los vendedores intentan generalmente corregir vulnerabilidades conocidas de seguridad del software (y hardware) cuando los han identificado. Estas correcciones se obtienen mediante actualizaciones y mejoras de seguridad; los administradores de la red necesitan comprobar regularmente con el proveedor para revisar si estas actualizaciones están disponibles para aplicarlas según lo requerido.

También, muchos vendedores tienen listas de correo de alertas sobre seguridad para aconsejar a clientes de las nuevas vulnerabilidades y ataques contra la seguridad.

d) **Autenticación.** En general, las soluciones eficaces de autenticación es una manera confiable de permitir que solamente los usuarios autorizados tengan acceso a una red. Las soluciones de autenticación incluyen el uso de nombres de usuario y contraseñas, siendo importante poseer políticas al especificar la longitud mínima y caracteres requeridos para la contraseña.

e) **Firewall personal.** Los recursos en redes inalámbricas públicas tienen un riesgo más alto de ataque, puesto que no tienen generalmente el mismo grado de protección que los recursos internos. Los firewall personales ofrecen cierta protección contra ciertos ataques. Los firewall personales son soluciones software que residen en la máquina del cliente, quienes pueden configurar el firewall y pueden no seguir ningunas pautas específicas de seguridad. Las soluciones centralmente manejadas proporcionan un mayor grado de protección porque los departamentos las configuran y maneja remotamente. Las soluciones centralmente manejadas permiten que las organizaciones modifiquen firewall del cliente para protegerse contra vulnerabilidades conocidas y para mantener una política constante de seguridad para todos los usuarios, aunque los firewall personales ofrecen una cierta medida de protección, no protegen contra formas avanzadas de ataque.

f) **Sistema de detección de intrusos.** El sistema de la detección de intrusos es una herramienta eficaz para determinar si los usuarios no autorizados están intentando tener acceso, han tenido acceso ya, o han comprometido la red.

g) **Cifrado.** Los usuarios de APs y los clientes 802.11 inalámbricos deben estar alertas sobre la comprobación con el proveedor respecto a mejoras en el soporte lógico.

h) **Auditorias de seguridad.** Las intervenciones de seguridad, son una herramienta esencial para comprobar el estado de la seguridad de una WLAN y para determinar la acción correctiva y cerciorarse de que sigue siendo segura. Es importante realizar intervenciones regulares usando analizadores de redes inalámbricas y otras herramientas. Los administradores de seguridad o los interventores de seguridad pueden utilizar analizadores de red, para determinarse si los productos inalámbricos están transmitiendo correctamente y en los canales correctos.

4.3.3.2 Soluciones de hardware.

Las contramedidas de hardware para atenuar riesgos en la WLAN incluyen colocar tarjetas inteligentes, VPNs, PKI, biométrica.

a) **Tarjetas inteligentes.** Las tarjetas pueden agregar otro nivel de protección, aunque también agregan otra capa de complejidad. Se pueden utilizar conjuntamente con el nombre de usuario o la contraseña o por sí mismos. Estas tarjetas son utilizadas en la autenticación y se pueden combinar con la biometría.

   En redes inalámbricas, las tarjetas proporcionan como valor agregado la autenticación; son beneficiosas en los ambientes que requieren autenticación más allá del nombre de usuario simple y de la contraseña. El certificado del usuario y la otra información se almacenan en las tarjetas y requieren generalmente a usuario recordar solamente un PIN, son también portables; por lo tanto los usuarios pueden tener acceso con seguridad a sus redes de varias localizaciones

b) VPNs. Es una tecnología que proporciona la transmisión de datos segura a través de las infraestructuras de la red pública. Hoy, se utilizan típicamente en tres panoramas: para el acceso de usuario distante, para la conectividad LAN a LAN, y para las extranets. Se emplean técnicas criptográficas para proteger la información del IP como pasa a partir de una red al siguiente o a partir de una localización al siguiente. Los datos que están dentro del VPN se aíslan del otro tráfico de la red.

c) PKI. Proporciona el marco y los servicios para la generación, producción, distribución, control, y la contabilidad de certificados de claves públicas. Provee el uso del cifrado y la autenticación segura en las transacciones de la red así como la integridad de los datos. Las WLANs pueden integrar PKI para la autenticación y asegurar transacciones de la red. Los fabricantes proporcionan PKI en dispositivos inalámbricos, los microteléfonos, y las tarjetas inteligentes que se integran con WLANs.

d) Biometría. Los dispositivos biométricos incluyen la huella digitaL, exploradores ópticos, faciales, y de reconocimiento de voz. La biométrica proporciona una capa agregada de protección cuando es utilizada sola o junto con otra solución de seguridad. Por ejemplo, para las empresas que necesitan niveles más altos de la seguridad, la biométrica se puede integrar con las tarjetas inteligentes, o las computadoras portátiles. Además, la biométrica se puede combinar con las soluciones de VPN para proporcionar autenticación y confidencialidad de los datos.

En la siguiente tabla se aprecia un resumen detallado de los diferentes riesgos en seguridad y su tratamiento.

Tabla 5. Mitigación de riesgos en WLANS

DESCRIPCIÓN DE RIESGOS	TRATAMIENTO DE RIESGOS
No contar con registros de auditoria en caso de presentarse un incidente y/o para realizar monitoreo como acción preventiva	Habilitar los registros de auditoria.
	Aplicar procedimiento de administración de logs.
Daño, pérdida de equipos o información por la falta de políticas, normas y procedimientos relacionados con la administración de las redes inalámbricas.	**Definir una política de seguridad que contenga los siguientes requerimientos:** ▪ Identificar quién puede usar la tecnología WLAN dentro de la organización ▪ Identificar si el acceso a Internet es requerido ▪ Describir quién puede instalar los AP y otros equipos inalámbricos ▪ Proveer los requerimientos de seguridad física y de ubicación para los AP ▪ Describir el tipo de información que puede ser transmitida por los enlaces inalámbricos ▪ Describir las condiciones bajo las cuales los dispositivos inalámbricos son permitidos ▪ Definir el estándar de seguridad para los AP ▪ Describir las limitaciones sobre cómo los dispositivos inalámbricos pueden ser usados (ej. la ubicación), ▪ Describir la configuración de hardware y/o software de todos los dispositivos inalámbricos ▪ Proveer las indicaciones para reportar la pérdida de dispositivos inalámbricos o incidentes de seguridad. ▪ Describir la configuración de los clientes inalámbricos ▪ Proveer la guía para la administración de claves y uso de cifrado ▪ Definir la frecuencia y alcance de operación de los AP ▪ Describir los procedimientos de auditoria, procedimientos para ingreso de terceros. ▪ Por otra parte, es importante contar un inventario actualizado de los APs, y en lo posible de los clientes.

Fuga de información por la falta de conciencia en seguridad por parte de los usuarios.	Entrenamiento a los usuarios en la operación de las WLAN internas y externas. Entrenamiento al Soporte Técnico en los procedimientos definidos. Campaña de cultura y conciencia en Seguridad de la Información
Pérdida de confidencialidad, integridad o disponibilidad por la falta de una configuración adecuada de seguridad de las redes inalámbricas (Tanto equipos de red como clientes). Entre estos: ▪ Configuración por defecto ▪ SSID por defecto ▪ SSID habilitado ▪ Comunicación no cifrada ▪ Sin autenticación de usuarios ▪ DoS, etc.	**Configurar el AP con los siguientes requerimientos:** ▪ Actualizar contraseñas por defecto y seguir la política de la organización en cuanto a contraseñas sensibles ▪ Activar el cifrado de la información (TKIP 256 bits - CCMP 128 bits) ▪ Controlar la función de reset ▪ Cambiar el SSID, Deshabilitar el broadcast del SSID ▪ Maximizar el intervalo de Beacon ▪ Usar SNMPv3 ▪ Utilizar un canal libre de interferencia ▪ Deshabilitar uso de DHCP ▪ Mantener actualizado el SW del dispositivo. **Otros:** ▪ Habilitar autenticación fuerte (AAA), habilitar Firewalls en los clientes ▪ Implantar WIDS, NIDS, Habilitar HIDS ▪ Deshabilitar archivos o directorios compartidos en los clientes ▪ Deshabilitar las opciones adicionales que no se vayan a utilizar ▪ Validar activación de antivirus en los clientes (cumplimiento de políticas de usuario final) ▪ Configurar el AP para evitar ataques de DoS la administración vía Web debe hacerse usando SSL/TLS o un protocolo equivalente (IPsec) ▪ Crear una VLAN de administración para los APs (y en lo posible para los usuarios) ▪ Instalar un firewall de red entre cada WLAN y el sistema de distribución ▪ Utilizar métodos EAP-TLS para el intercambio entre AP y el AS ó 802.1x, utilizar equipos con certificación WPA-2 ▪ Configurar la terminación de la sesión por un período de inactividad ▪ Especificar en los clientes el servidor de autenticación ▪ Emplear IPsec entre el SP y el AS ▪ Sincronizar los equipos por NTP con el servidor de tiempo de la organización. ▪ Utilizar contraseñas de tipo sensible para las cuentas de administración. ▪ Configurar GMX a 24 horas, Configurar un máximo de PMK no superior a 8 horas. ▪ Deshabilitar modo Ad Hoc de los equipos clientes.

Multas por No licenciamiento del Software	Validar el uso de licencias de administración y centralizar la operación.
Indisponibilidad del servicio y/o degradación del servicio.	Realizar/validar estudios de capacidad de los dispositivos inalámbricos en cuanto a usuarios concurrentes, tasas de transferencia, interferencia electromagnética.
No contar con una protección física adecuada de los dispositivos de red (Punto de acceso).	Incluir/validar controles en cuanto a control de acceso, identificación de personal y protección para evitar que señales RF generadas por AP de la red alcancen ubicaciones externas a la organización. En el último caso, realizar los estudios de planeación de WLAN y ajustar la potencia de salida del AP asegurando que sólo tenga cobertura en el área indicada. De igual forma validar a través pruebas de SITE SURVEY.

Fuente: Autor Proyecto

4.4 TRANSICIÓN DE LA INFRAESTRUCTURA WLAN A LA TECNOLOGÍA RSN

La Universidad debe cerciorarse de las consideraciones de seguridad incorporadas en cada fase del ciclo vital de las WLANs, durante el proceso de establecimiento e implementación de una RSN.

El planeamiento y la puesta en práctica de RSNs, describe un modelo de ciclo vital para WLANs y presenta las mejores recomendaciones relacionadas para cada fase. Estas consideraciones de seguridad WLAN incluyen:

- **Fase 1: Inicio**. Esta fase incluye las tareas que una organización debe realizar antes de comenzar a diseñar su solución de WLAN. Éstas incluyen desarrollar una política del uso de WLAN, la ejecución de una evaluación de riesgo de WLAN, y especificación de los requisitos funcionales para la solución.

- **Fase 2: Adquisición/desarrollo**. Esta fase se compone de dos fases siguientes:

  - **Fase 2a: Planeación y diseño**. En esta fase, los diseñadores de la red WLAN especifican características técnicas de solución, tales como métodos de autenticación, y los tópicos relacionados con los componentes de la red. También se debe tener en cuenta una Site Survey para ayudar a determinar la arquitectura de la solución y cómo la WLAN se debe integrar con la infraestructura existente de la autenticación, incluyendo PKI.

  - **Fase 2b: Consecución.** Esta fase implica el especificar el número y el tipo de componentes WLAN que deben ser adquiridos, los

sistemas deben presentar características y certificaciones como por ejemplo: WPA2.

- **Fase 3: Puesta en práctica**. En esta fase, los dispositivos se configuran para resolver requisitos operacionales y de seguridad, y posteriormente se instalan y activan en la red para su utilización.

- **Fase 4: Operaciones/mantenimiento**. Esta fase incluye las tareas de seguridad como evaluación periódica de la seguridad, revisiones de logs, etc.

- **Fase 5: Disposición.** Esta fase implica tareas que se ocasionan después de estar en funcionamiento el sistema o el retiro de alguno de sus componentes, incluyendo preservar la información para resolver requisitos legales, la esterilización de los medios que pudieron contener el material sensible, y disposición del equipo correctamente.

La política de aseguramiento dentro del Campus Principal de la Universidad está basada en las recomendaciones del Instituto de Estándares y Tecnología NIST (National Institute of Standards and Technology), para el establecimiento de una RSN.

La implementación de la RSN, se fundamenta en la construcción de RSNAs. La autenticación, como mínimo, apoyada en un nombre y una contraseña de usuario, aunque la autenticación compartida sería permitida por un período determinado, de acuerdo a las políticas que el administrador de la red designe. Los requerimientos soportados en WLAN no basada en RSNAs deben operar en un perímetro de la red separado por un firewall.

El aseguramiento de las WLANs de la Institución parte de la evaluación de la infraestructura existente, con el propósito de migrar a un marco de tecnología RSN, en donde se propone una solución a corto plazo y posteriormente una solución a largo plazo.

La solución a largo plazo contempla la implementación de la seguridad basada en RSN usando IEEE 802.1x para el control de acceso y CCMP para la seguridad e integridad de los datos.

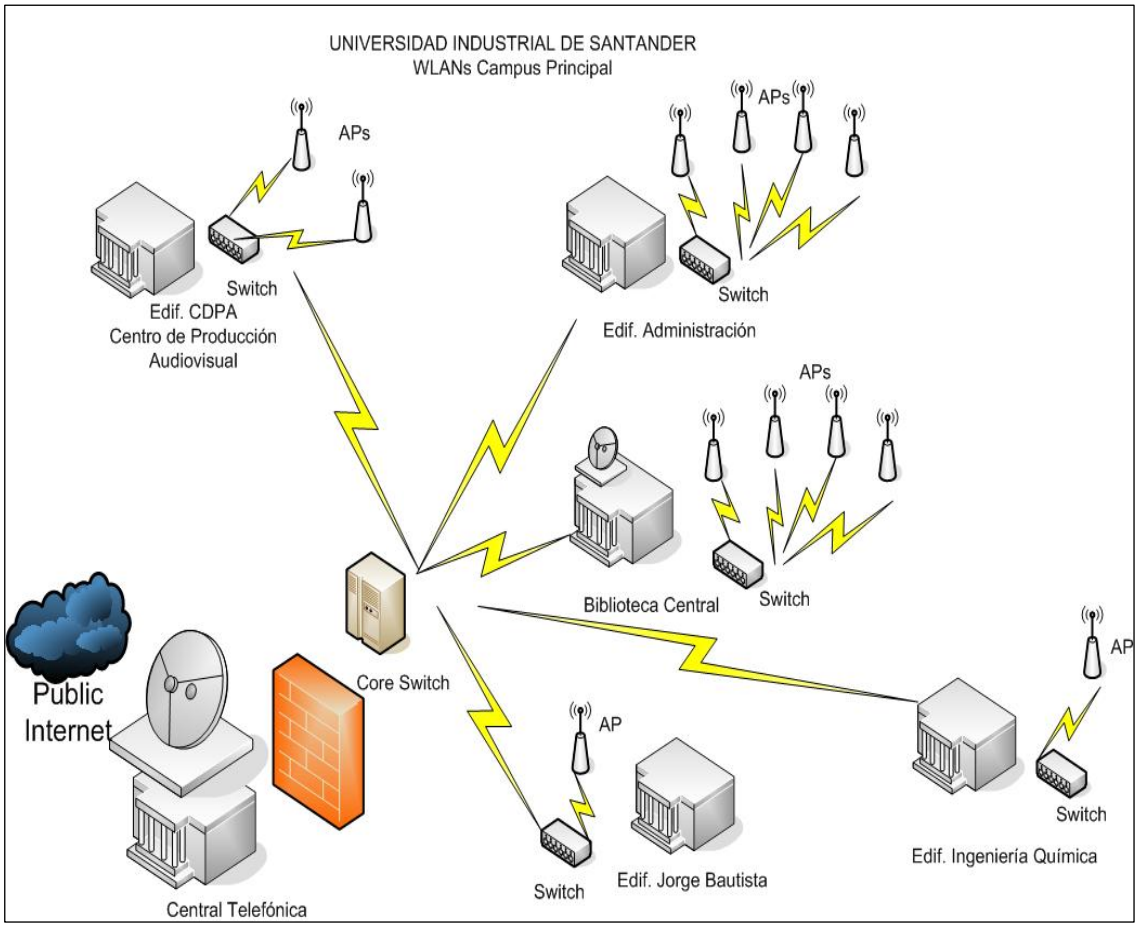
Sin embargo, dada la necesidad de establecer una seguridad inmediata con la diversidad de equipos y configuraciones existentes, se propone una solución a mediano plazo que significativamente aumenta la seguridad deseada.

4.4.1 Fase 1 Inicio.

El primer paso es la realización del inventario relacionado con la infraestructura existente (como se muestra en el Anexo A) y la ficha técnica del punto de acceso (Anexo B).

Consecuentemente, se puede realizar una evaluación para verificar si el software instalado en los equipos clientes (tarjetas inalámbricas) soporta TKIP, y posiblemente CCMP. También, se debe tener en cuenta el control de acceso físico, el cual puede ser proporcionado a través de una tarjeta electrónica utilizada para el ingreso. La infraestructura existente, se puede observar en la siguiente figura. Para este esquema de seguridad se manejan 12 APs con capacidad y configuraciones de seguridad que varían.

Figura 18. WLANs Universidad Industrial de Santander



Fuente: Autor Proyecto

4.4.2 Solución intermedia: Adquisición, desarrollo y puesta en práctica.

La planeación del aseguramiento de las redes inalámbricas, se inicia con una estrategia interna para la infraestructura actual. Entre los factores que se deben considerar se incluyen:

- Capacidad funcional del equipo actual
- Grado de afectación de los usuarios
- La buena voluntad de los usuarios para aceptar el cambio.

Para realizar esta practica, se pueden tener en cuenta la matriz siguiente:

Tabla 6. Estrategias para solución a corto plazo

VALORACIÓN AP	SOLUCIÓN CORTO PLAZO	SOLUCIÓN LARGO PLAZO
▪ No existe ninguna seguridad. ▪ No soportan upgrades. ▪ La certificación WPA2, pueden ser usada para la solución a largo plazo. ▪ Los usuarios insisten en el uso continuo de la WLAN sin importar nuevas medidas de seguridad, rechazan TKIP. ▪ Los Aps están localizados cerca de las ventanas.	▪ Colocar la ESS en un perímetro de la red fuera del firewall. ▪ Los usuarios requieren software VPN cliente para acceder a los recursos de internos de la red. ▪ Colocar el AP cerca del centro del área de trabajo, lejos de ventanas y de paredes.	
▪ WEP provee seguridad inadecuada. ▪ Todos los equipos pueden soportar TKIP pero no CCMP. ▪ No pueden soportar IEEE 802.1X, porque las aplicaciones de equipos WPA personales solo soportan PSK. ▪ Los usuarios están seguros con el uso de PSKs, porque se ha trabajado con la configuración de WEP.	▪ Configurar el AP para usar TKIP con PSKs. ▪ Establecer temporalmente una TSN (Transition Security Network) que permita asociaciones de WEP con TKIP. ▪ Promover la transición a TKIP ▪ Una vez se ha verificado que todas la STAs están usando TKIP, eliminar el soporte WEP	▪ Procurar que los nuevos equipos WPA2 soporten la solución a largo plazo. ▪ Deshabilitar TKIP.

	para establecer una RSN. ▪ TSN debe ser operacional por un periodo breve, preferiblemente no más de 72 horas.	
▪ ESS es una RSN usando IEEE 802.1X. ▪ RSN está basado en TKIP, no en CCMP, el cual se requiere una solución a largo plazo. ▪ Los APs no soportan CCMP y requieren ser reemplazados. ▪ Las tarjetas inteligentes proporcionan un alto nivel de aseguramiento de autenticación.	▪ Mantener la configuración.	▪ Reemplazar los AP con nuevos AP WPA2. ▪ Continuar apoyando, si es factible, el uso de tarjetas inteligentes. ▪ Deshabilitar TKIP.
▪ Los usuarios desconocen lo relacionado con PSKs pero son receptivos a la importancia de la seguridad.	▪ Familiarizar a los usuarios con las nuevas tecnologías.	▪ Reemplazar los AP con nuevos AP WP2. ▪ Deshabilitar TKIP.
▪ El AP puede soportar TKIP con un upgrade del firmware.	▪ Ejecutar el upgrade.	
▪ La ESS es una RSN usa CCMP con PSK.	▪ Mantener la configuración.	

Fuente: Autor Proyecto

Esta solución permite que se ejecuten rápidamente medidas de seguridad sin interrumpir el servicio o adquirir nuevos equipos o software, mientras se implementa la solución a largo plazo.

En esta solución intermedia se podría implementar una RSN con el equipo existente. El desarrollo de PSKs aumenta la complejidad administrativa de las operaciones de WLAN, sobre todo debido a la necesidad de rotar periódicamente claves, que es a menudo un proceso manual. Sin embargo, el uso de PSKs en esta solución permite proteger las WLANs, dando lugar a diseñar y poner una solución en ejecución a largo plazo.

4.4.3 Solución largo plazo: Adquisición, desarrollo y puesta en práctica.

Con la implementación de la solución a mediano plazo, la etapa siguiente para el aseguramiento es realizar la transición a largo plazo, en donde hay que tener en cuenta algunos aspectos importantes:

- Emigrar a una infraestructura centralizada de autenticación.
- Sustituir todo el APs que no son certificados WPA2 y por lo tanto no pueden soportar CCMP con control de acceso por puerto basado en IEEE 802.1X.
- Instalar el software en todas el STAs.
- Ampliar la solución de tarjetas inteligentes en las oficinas
- Utilizar un servidor Radius basado en AAA con EAP-TTLS y MD5-Challenge como método interno de EAP.

Esta solución implica software agente en cada STA que obtiene periódicamente un nuevo PSK de un servidor central.

En la solución a largo plazo, se contempla un servidor Radius basado en AAA, para integrarlo con el directorio LDAP del correo electrónico. También incorporar el sistema inteligente para la autenticación a través de tarjetas

para el uso del personal como seguridad adicional para acceder a la red. Para esta configuración se requiere el uso de EAP-TTLS con contraseña de MD5- Challenge, la autenticación basada para el ESS disponible para todos los usuarios, y la autenticación de EAP-TLS apta para el personal de soporte con requisitos adicionales de autenticación.

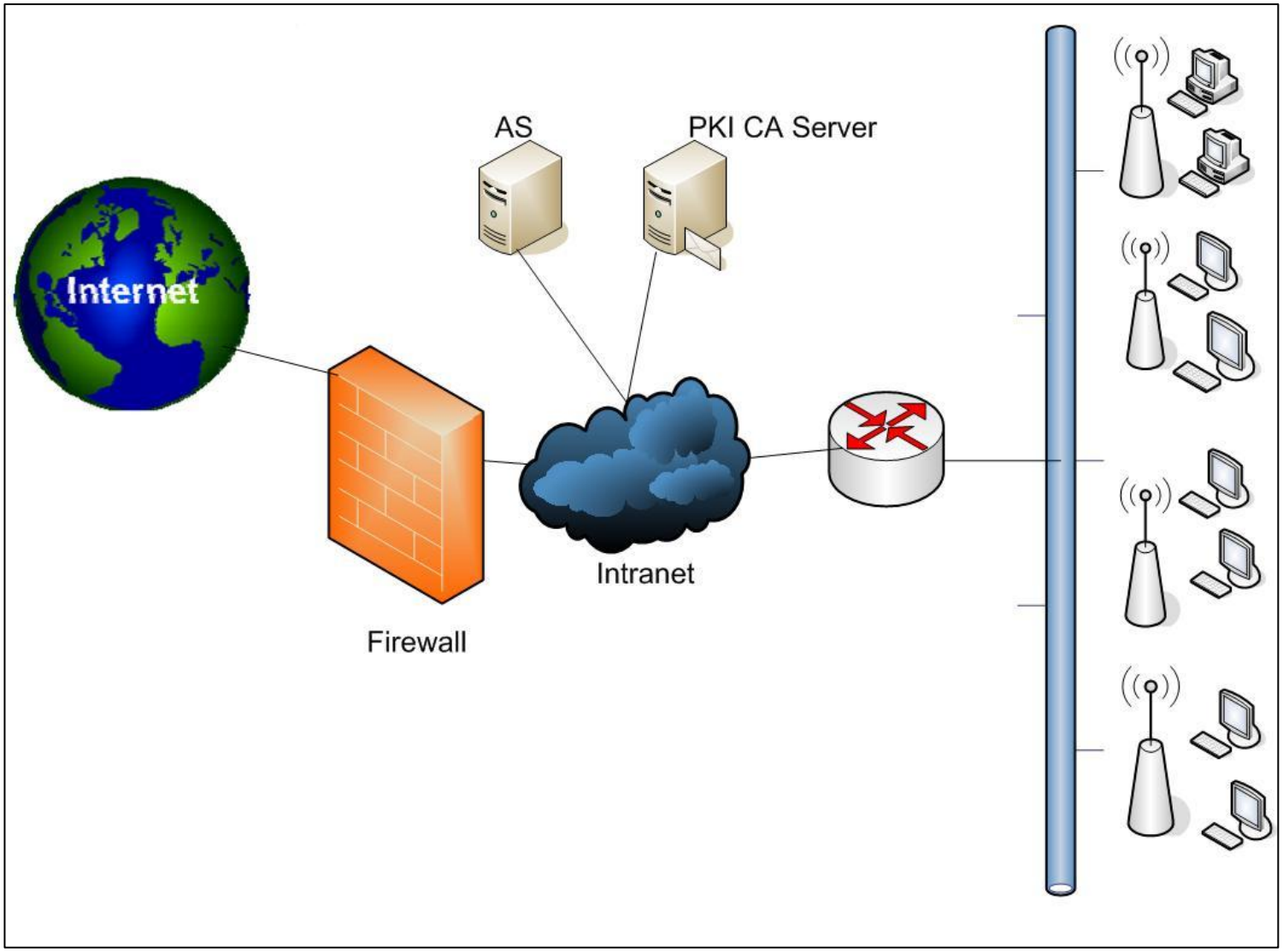
Establecer un firewall entre la red de los usuarios y la red de administración de los AP limita terminantemente los tipos de tráfico que puede fluir entre los dos: Además, se requiere sustituir todos los APs que no se apoyan en el estándar IEEE 802.1X y CCMP.

Para evitar interrupciones del servicio, siempre que un AP nuevo se instale, se debe dar un tiempo en días específico para la migración a la nueva RSN.

Es necesario instalar nuevo software para los clientes WLANs en cada STAm, debido a que los usuarios cuentan con diversidad en el ambiente de red, y es necesario que soporte RSN.

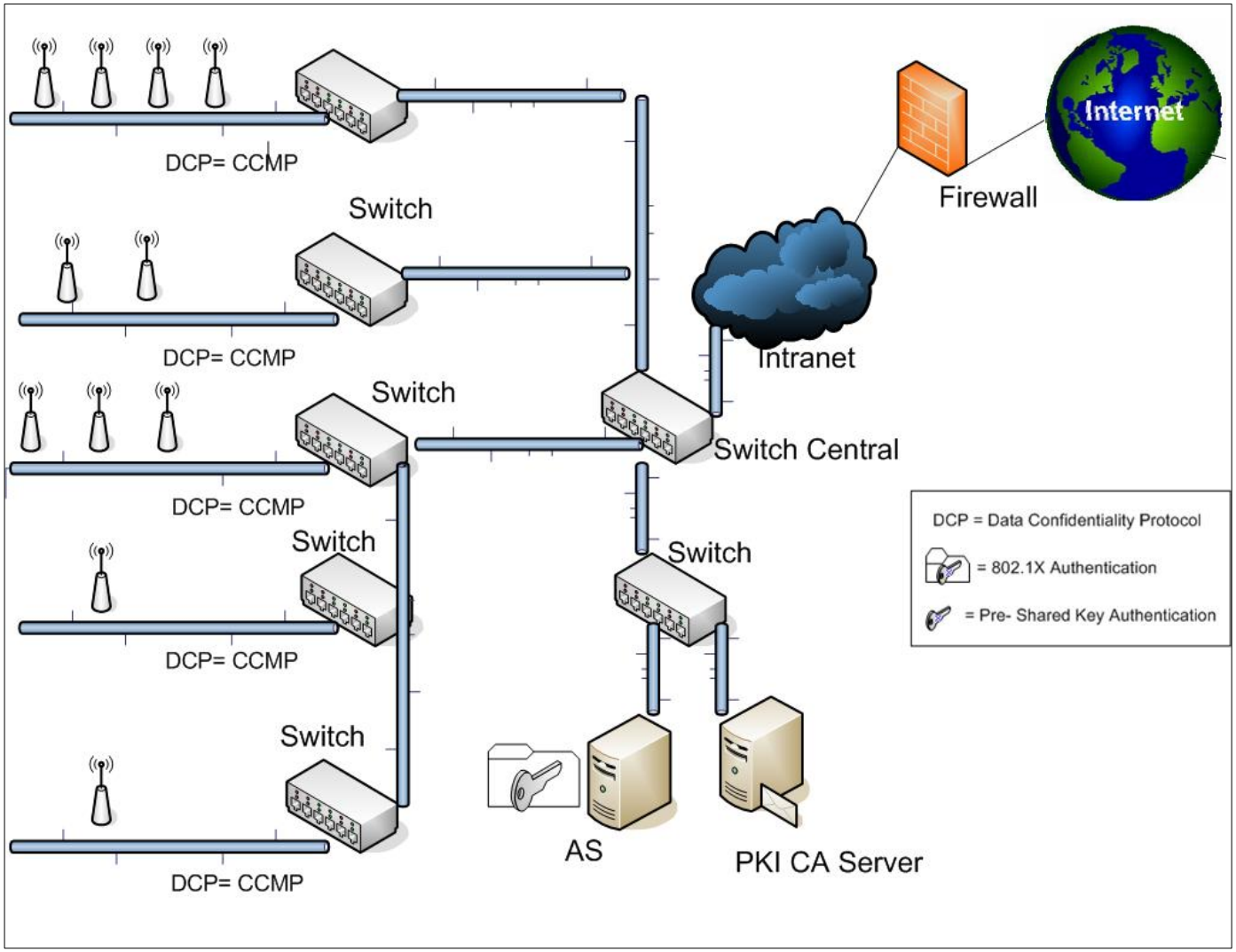
La solución a largo plazo se puede apreciar en la siguiente figura.

Figura 19. Esquema RSN



Fuente: Autor Proyecto

Figura 20. Esquema detallado RSN



Fuente: Autor Proyecto

4.4.4 Implicaciones en función del entorno.

La solución garantiza unos requisitos mínimos de seguridad:

- Privacidad de los datos del usuario (cifrado)
- Privacidad de las credenciales de los usuarios (autenticación)
- El despliegue se verá influenciado por los mecanismos de seguridad existentes previamente en la red.

4.4.5 Implicaciones en función de los clientes.

Diferentes tipos de usuario y clientes de acceso heterogéneos (PCs, PDAs, teléfonos, etc.) con diferentes sistemas operativos (Windows, Linux, MacOS, etc.).

Existen aplicaciones comunes entre alumnos y profesores, acceso a información de los estudiantes por parte del personal de la Universidad. Se debe escoger que mecanismos de seguridad se quiere ofrecer a cada tipo de usuario. Por ejemplo:

- Para los estudiantes y visitantes

  Seguridad: Sólo autenticación

  Entorno: Se permite la heterogeneidad de terminales
- Para los empleados y profesores:

  Seguridad: Autenticación de usuario y confidencialidad de los datos.

  Entorno: Se estandarizan los terminales a usar

4.4.6 Implicaciones en función de los puntos de acceso

- El punto de acceso debe soportar WPA2 (o ser actualizable en un futuro breve)
- Cifrado AES muy exigente: Es deseable soporte de AES en hardware.
- Entorno heterogéneo :

  - Convivencia de múltiples esquemas de autenticación y cifrado

- Soporte de múltiples SSIDs en el AP
- Soporte de VLANs
- Correspondencia SSID a VLANs

- Deseable funciones de IDS en el propio AP
  - Detección de ataques
  - Terminación de sesiones de usuarios no deseados

5. CONCLUSIONES

La seguridad en las redes inalámbricas es una necesidad, por las características de la información que por ellas se transmite. Sin embargo la gran cantidad de las redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red, si es una red ya existente o una nueva, y del presupuesto disponible para implantarla, entre otros factores.

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

6. RECOMENDACIONES

El aseguramiento de las redes WLAN, requiere poner en marcha dos soluciones para la tecnología RSN, una solución a mediano plazo para establecer medidas inmediatas que contrarresten amenazas activas, y una solución a largo plazo donde se contempla un servidor RADIUS basado en AAA con control de acceso por puerto IEEE 802.1X.

En cuanto a los dispositivos inalámbricos existentes (puntos de acceso), es recomendable realizar actualizaciones del firmware, si están disponibles, para el caso de implementar la solución a mediano plazo. Para la solución a largo plazo se requiere el cambio de estos dispositivos.

BIBLIOGRAFÍA

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Citas y notas de pie de página. Bogotá: ICONTEC., 1996. 7 p. (NTC. 1487). COMPENDIO.

Secretaria de la función pública: Subsecretaría de tecnologías informáticas. Manual de seguridad en redes. 1998. 99 p.

SUBERCASEAUX, Miguel. Diccionario sinónimos y antónimos. Santa fe de Bogotá: Editar Ltda. 2000. 634 p.

MADRID MOLINA, Juan Manuel. Seguridad en Redes Inalámbricas 802.11. Sistemas & Telemática. Revista Facultad de Ingeniería UNIVERSIDAD ICESI.

RAMIO AGUIRRE, Jorge. Curso de seguridad informática y criptografía
Disponible en Internet:
<http://www.lpsi.eui.upm.es/SInformatica/SInformatica.htm>

FISHER, Dennis. Study Exposes. WLAN Security Risks.
Disponible en Internet:
<http://www.icesi.edu.co/es/publicaciones/publicaciones/contenidos/sistemas_telematica/3/jamdrid-seguridad_redes_inalambricas.pdf >

Practically Networket. Securing your wireless network.
Disponible en Internet:
<http://www.practicallynetworked.com/support/wireless_secure.htm>

Glosario de Informática y redes Wireless.
Disponible en Internet:
<http://www.virusprot.com/Glosarioc.html>

ANEXOS

ANEXO A. Inventario WLANs UIS, Campus Principal

Proyecto de Actualización y Ampliación de la Red Institucional FASE I

Ubicación	WLAN	Ref. AP	Estándar	Sw Versión	Dirección IP	*Clientes	Esquema Seguridad Actual
Edif. Administración División Serwicios de Información	administracion	3Com 8750	802.11 a/g	3.1	-	5	Autenticación WEP Shared SSID (enabled) Nombre Administrador (default) Listas de acceso por MAC Cifrado WEP
Edif. Administración Admisiones Recursos Humanos	administracion	3Com 8750	802.11 a/g	3.1	-	4	Autenticación WEP Shared SSID (enabled) Nombre Administrador (default) Listas de acceso por MAC Cifrado WEP
Edif. Administración Rectoría	administracion	3com 8750	802.11 a/g	3.1	-	10	Autenticación WEP OpenSystem SSID (enabled) Nombre Administrador (default) Listas de acceso por MAC (disabled)
Edif. Administración Contratación	administracion	3Com 8750	802.11 a/g	3.1	-	-	Autenticación WEP OpenSystem SSID (enabled) Nombre Administrador (default) Listas de acceso por MAC (disabled)
Edif. Jorge Bautista	geologia	3Com 8250	802.11 a/g	-	-	5	Autenticación WEP Shared SSID (enabled) Nombre Administrador (default) Listas de acceso por MAC Cifrado WEP
Edif. Ingeniería Química Escuela de Ingeniería Química	cisyc	D-Link DI-624+	802.11	2.05	-	9	WPA SSID (enabled) Nombre Administrador (default) Listas de acceso por MAC
Edif. **CDPA Cededuis	cededuis1	D-Link DI-624+	802.11	2.05	-	30	WPA SSID (enabled) Nombre Administrador (default) Listas de acceso por MAC

Ubicación	WLAN	Ref. AP	Estándar	Sw Versión	Dirección IP	*Clientes	Esquema Seguridad Actual
Edif. CDPA Cededuis	cededuis2	D-Link DI-624+	802.11	2.05	-	12	WPA SSID (enabled) Nombre Administrador (default) Listas de acceso por MAC
Edif. Biblioteca Biblioteca Central	biblioteca	LINKSYS WRT 54G	802.11g	DD-WRT #22 (prefinal3.2)	-	-	VPN (IPSec) Listado de acceso por MAC Firewall (disabled)
		LINKSYS WRT 54G	802.11g	DD-WRT #22 (prefinal3.2)	-	-	VPN (IPSec) Listado de acceso por MAC Firewall (disabled)
		LINKSYS WRT 54G	802.11g	DD-WRT #22 (prefinal3.2)	-	-	VPN (IPSec) Listado de acceso por MAC Firewall (disabled)
		LINKSYS WRT 54G	802.11g	DD-WRT #22 (prefinal3.2)	-	-	VPN (IPSec) Listado de acceso por MAC Firewall (disabled)

* La cantidad de clientes dependen de los requerimientos de las dependnecias

** Centro de Producción Audiovisual

NOTA: Los access point ubicados en la Biblioteca Central no son administrados por la División de Servicios de Información, estos equipos son de propiedad de Sisteco, y la configuración fue realizada por esta empresa. La administración de los usuarios está a cargo de la Biblioteca Central.

ANEXO B. Ficha técnica Access Point

UAA
WLAN
SSID
Channel
Ver. Fireware
Password
Marca
Referencia

Dirección IP														
MAC														
Puerta Enlace														
Rango Direcciones IP (														
Etiqueta toma datos														
No. Consec.	IP WIRELESS				MAC						Usuario	Marca PC	Ref. Tarjeta Inalámbrica	Inventario/ Service T

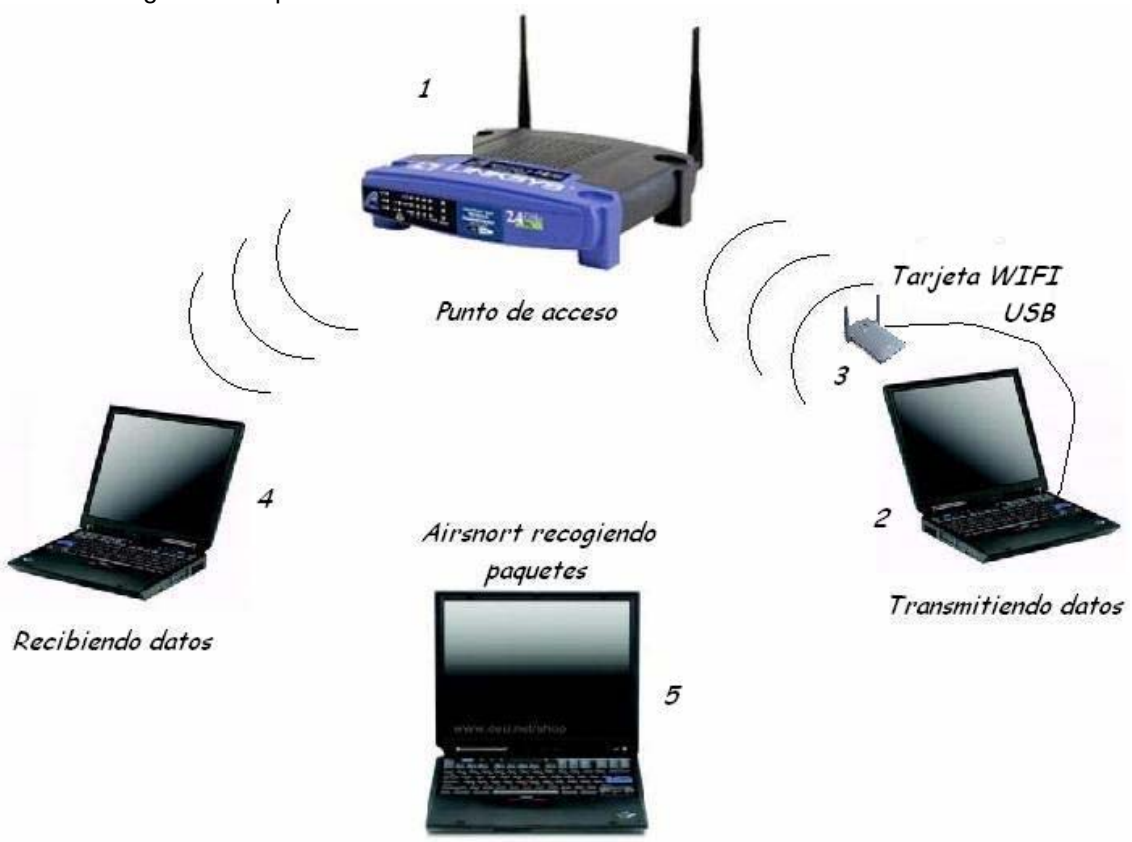
ANEXO C. Ficha inscripción servicio Internet Biblioteca

UNIVERSIDAD INDUSTRIAL DE SANTANDER
BIBLIOTECA - SECCION DE SERVICIOS AL PUBLICO
SERVICIO DE RED INALAMBRICA

Datos personales			
Nombres y apellidos:			
Código de estudiante:			
Carrera (Escuela):			
Dirección (correspondencia):			
Teléfono y/o E-Mail:			
EQUIPO			
MARCA:		DIRRECION MAC:	
SISTEMA OPERATIVO:		FECHA DE REGISTRO:	
Me comprometo a ser buen uso del servicio y me hago responsable de toda información y actividad que se genere desde este equipo.			
FIRMA: _____			
Observaciones:			

ANEXO D. Rompimiento cifrado WEP en una WLAN

Para esta prueba se utilizó el siguiente esquema de red[4]:



[4] Departamento de Sistemas Informáticos UCLM. Disponible en Internet <http://www.info-ab.uclm.es/asignaturas/42602/T8.doc>

Dispositivos utilizados:

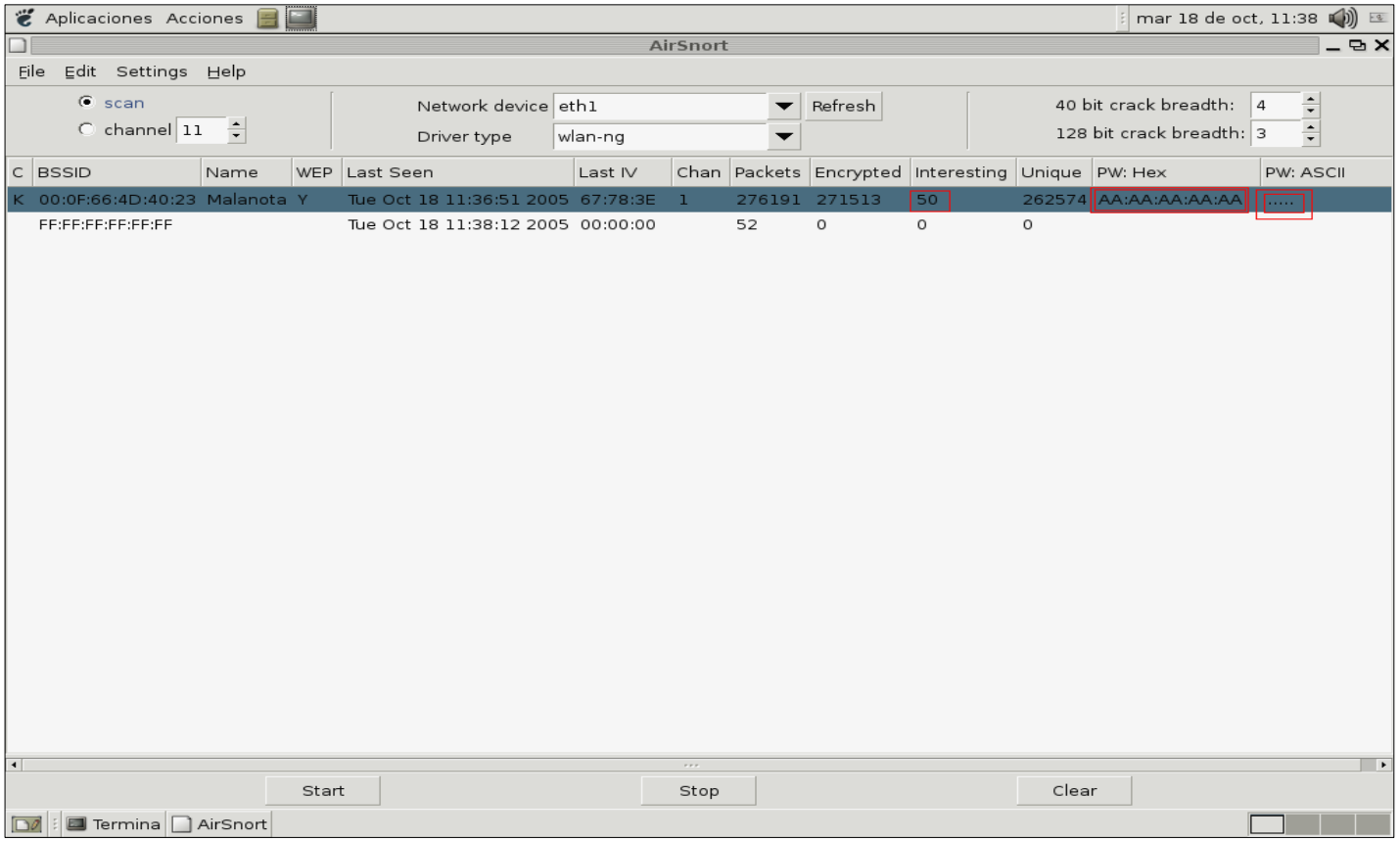
1- Router WIFI Lynksys
2- Portátil HP omnibook xe4500 para enviar datos.
3- Tarjeta WIFI USB Belkin en portátil HP omnibook xe4500.
4- Portátil IBM ThinkPad T41 para recibir datos.
5- Portátil IBM ThinkPad T41 con AirSnort para captura de paquetes.

Procedimiento:

Se preprara el Router wifi (1) para que utilice el protocolo WEP como protocolo de seguridad y se establece como password la secuencia **"….."** en ASCII ("AA AA AA AA AA" en hexadecimal) y se configuran los portátiles (2 y 4) para trabajar en la red creada.

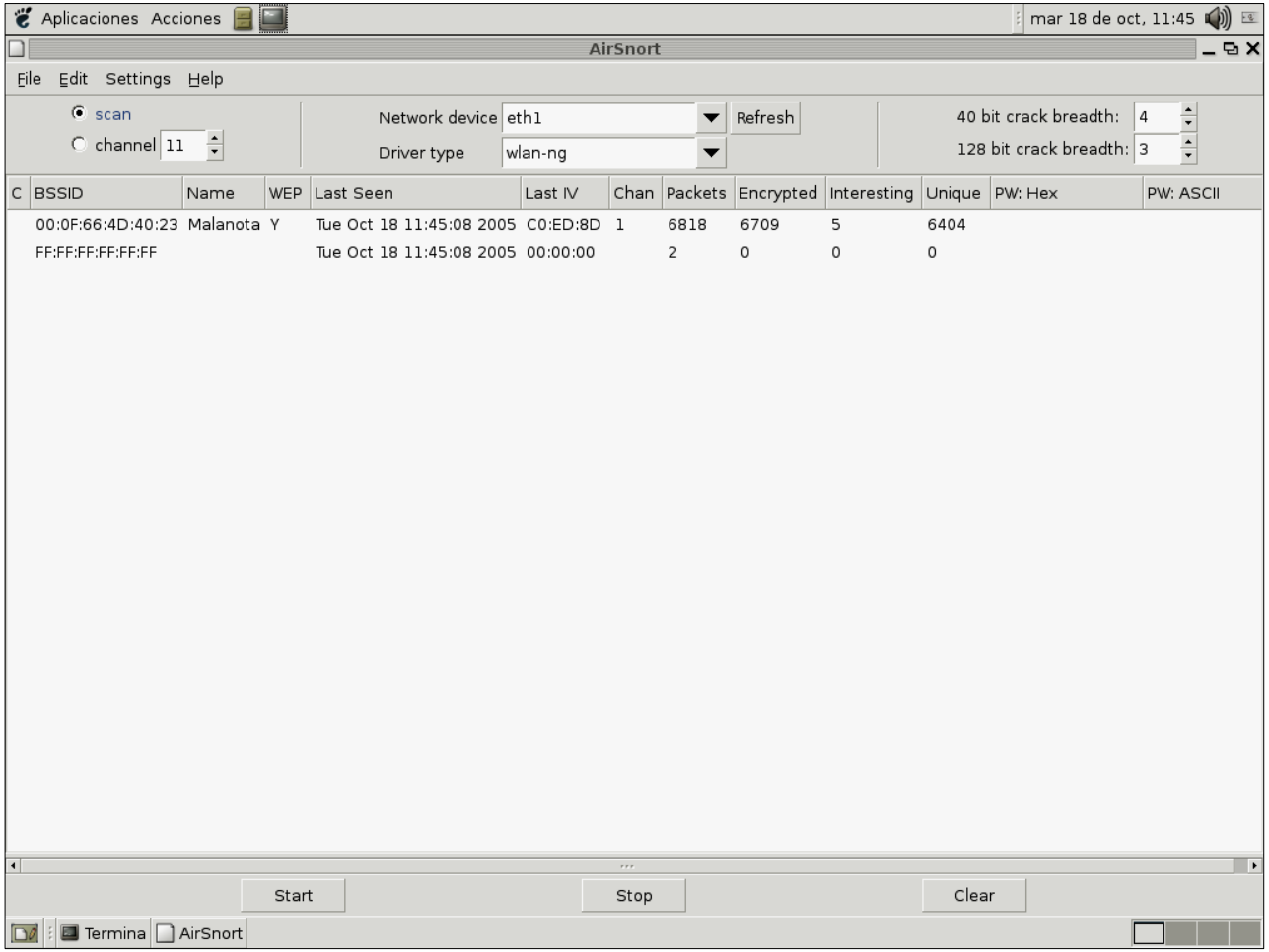
Desde uno de los portátiles (2), se comienza a enviar un archivo muy grande a otro (4). A continuación se nicia AirSnort en el tercer portátil (5) y se empieza a capturar paquetes con el botón "start" de AirSnort.

Se observa como al poco tiempo de empezar la captura, existen en la red 6818 paquetes, de los cuales 6709 estan encriptados y solo 5 son interesantes (de tipo débil) para romper la encriptación WEP, a los 271.513 paquetes ecriptados de los cuales 50 son interesantes, la clave WEP aparece decodificada como se puede ver en la imagen.



Como podría tratarse de una casualidad, se opta por repetir la prueba, pero esta vez con una clave más habitual para un usuario común, en concreto se utiliza la palabra “clave”.

De nuevo se realiza el mismo procedimiento, se comienza otra vez a transferir grandes cantidades de información.



En un tiempo muy corto (alrededor de 5 minutos) y con menos paquetes débiles que antes, AirSnort obtiene la clave de encriptación como se puede ver en la siguiente captura.