UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO Y SIMULACIÓN DE UNA RED INALÁMBRICA CON CRITERIOS DE SEGURIDAD

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

MAURO MIGUEL CASTILLO GRANADOS

PROMOCIÓN
2003-II

LIMA-PERÚ
2010

DISEÑO Y SIMULACIÓN DE UNA RED INALÁMBRICA CON CRITERIOS DE SEGURIDAD

A mi casa de estudios

la Universidad Nacional de Ingeniería

por la formación recibida

SUMARIO

En el presente informe se describe el diseño e implementación de una red inalámbrica con criterios de seguridad.

Para el caso de estudio, la empresa Bolsa de Valores de Lima (BVL) no contaba con una red inalámbrica para acceso a Internet a ninguno de sus cuatro niveles, impidiéndose así el desplazamiento y acceso tanto de personal autorizado cómo de invitados con dispositivos móviles (Lat Top, PDA, Celulares y otros).

La solución es implementada mediante el uso de controladores inalámbricos que gestionan a los Puntos de Accesos (AP) que están ubicados en los diferentes niveles. Los controladores configuran en los AP el SSID (Identificador de Red), la seguridad (encriptación y autenticación), las Redes Virtuales (una VLAN de invitados y otra de usuarios), los canales, la potencia transmitida. etc.

El diseño de la solución consta de una etapa previa de estudio de sitio apoyada en una simulación del escenario sobre el cual se desplegarán los APs. En una primera etapa se implementó un controlador y seis APs, en una segunda etapa (nueva necesidad de cobertura de BVL) se agregó otro controlador y seis APs.

La red inalámbrica aplicada a la solución es la IEEE 802.11 b/g. El protocolo de cifrado aplicado es el WPA (Acceso Protegido Wi-Fi) y el método de autenticación es el TKIP (Protocolo de integridad de clave temporal).

ÍNDICE

INTRODUCCIÓN

El trabajo surge por la necesidad del BVL de contar con un acceso permanentemente a la Internet que brinde comodidad a los usuarios para que no tuviesen que recurrir a modems GSM o el pago por servicios de valor agregado (VAS), además de la seguridad respectiva en general.

Por ello se determina diseñar e implementar una red inalámbrica (IEEE 802.11 b/g) con criterios de seguridad para la Bolsa de Valores de Lima (BVL) para sus cuatro niveles permitiendo el desplazamiento y acceso tanto de personal autorizado cómo de invitados con dispositivos móviles (Lat Top, PDA, Celulares y otros).

La solución inalámbrica se logra mediante la utilización de un controlador inalámbrico que gestiona a los Puntos de Accesos (AP) que están ubicados en los cuatro niveles que posee (sótano, mezzanine y dos pisos). En los APs, el controlador configura de manera centralizada: el SSID (Identificador de Red), la seguridad (encriptación y autenticación), las Redes Virtuales (una VLAN de invitados y otra de usuarios), los canales, la potencia transmitida, etc. La seguridad inalámbrica utiliza cómo protocolo de cifrado el WPA (Acceso Protegido Wi-Fi) y cómo método de autenticación el TKIP (Protocolo de integridad de clave temporal).

El diseño se aplica a un escenario que consta de cuatro niveles, cada uno de ellos con distintos ambientes de trabajo y salas de capacitación. En el último nivel o sótano se tiene una sala de capacitación, una sala de reuniones y un auditorio, en cada uno de ellos debe ir ubicado un AP. En el Tercer nivel o piso 3 se consideran 3 APs que darán cobertura a las oficinas de trabajo de ese nivel. En el área de Mezzanine se tiene el área de dirección de métodos, la sala de desarrollo de bolsa de productos y un salón protocolar, cerca de cada uno de ellos se considera un AP. La solución contempla 2 Wireless LAN Controller (WLC) de Cisco que administran hasta 6 APs cada uno y que serán ubicados en el data center de la BVL en el sótano.

El trabajo se desarrolla teniendo en consideración lo siguiente: a) Dimensionamiento de la solución, para ajustar el diseño a los requerimientos del cliente, etc., b) Estudio del sitio., para determinar las zonas oscuras y la obtención de las alternativas de la simulación, c) La propuesta de diseño, sobre la infraestructura de la red, la seguridad de la Red y el esquema final, y d) Equipamiento, describiendo los controladores, Puntos de acceso, las antenas y el software de gestión

El presente informe es desarrollado gracias a la experiencia adquirida como especialista en redes trabajando en la Unidad de Redes y Energía de la empresa COSAPI Data.

El presente trabajo se divide en cuatro capítulos. En el primer capítulo se plantea el problema de ingeniería estableciendo los objetivos y alcances, así mismo sustentando la solución propuesta y haciendo una síntesis del trabajo.

El segundo capítulo corresponde al Marco Teórico en el cual se definen los conceptos más importantes necesarios para la comprensión del informe. Este se divide en 1) Redes inalámbricas, 2) Estándares IEEE 802.11, y 3) Seguridad.

El tercer capítulo es la metodología para la solución del problema. En este capítulo se trata primero sobre el dimensionamiento de la solución, luego se hace el estudio de sitio, luego la propuesta de diseño y finalmente se describe el equipamiento utilizado.

Quisiera agradecer al Área de Tecnología Informática de la bolsa de Valores de Lima por facilitarnos el desarrollo de este informe, bajo el estrcito cumplimiento de sus normas de confidencialidad.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se realiza el planteamiento de ingeniería del problema, para ello primeramente se describe el problema y luego se expone el objetivo del trabajo, también se evalúa el problema y se precisan los alcances del informe, para finalmente presentar una síntesis del diseño presentado.

1.1 Descripción del Problema

Ineficiencia de las labores propias de la BVL por no contar con un sistema de acceso inalámbrico a Internet, para ninguno de sus cuatro niveles. Se veía así también impedido el desplazamiento y acceso tanto de personal autorizado cómo de invitados con dispositivos móviles (Lat Top, PDA, Celulares y otros).

Es muy importante para los involucrados estar conectados permanentemente a la Internet. La BVL brindaría la comodidad de que los usuarios no tuviesen que recurrir a modems GSM o el pago por servicios de valor agregado (VAS), además de la seguridad respectiva en general.

1.2 Objetivos del trabajo

Diseñar e implementar una red inalámbrica (IEEE 802.11 b/g) con criterios de seguridad para la Bolsa de Valores de Lima (BVL).

La solución inalámbrica es lograda mediante el uso de un controlador inalámbrico que gestiona a los Puntos de Accesos (AP) que están ubicados en los cuatro niveles que posee (sótano, mezzanine y dos pisos). En los APs, el controlador configura de manera centralizada: el SSID (Identificador de Red), la seguridad (encriptación y autenticación), las Redes Virtuales (una VLAN de invitados y otra de usuarios), los canales, la potencia transmitida, etc.

La seguridad inalámbrica utiliza cómo protocolo de cifrado el WPA (Acceso Protegido Wi-Fi) y cómo método de autenticación el TKIP (Protocolo de integridad de clave temporal).

1.3 Evaluación del problema

Actualmente la BVL viene desarrollando cursos en auditorios y salas de capacitación, por otro lado el avance de la tecnología informática y la aparición de diversos dispositivos de comunicación portátil crean la necesidad de brindar servicio de Internet inalámbrico a

los usuarios.

Existe además la necesidad de contar con una red inalámbrica segura que permita la movilidad dentro de las instalaciones de la BVL en sus diferentes niveles tanto a los usuarios que trabajan en la entidad como a los visitantes crea la necesidad de ampliar la red cableada aprovechando las ventajas que ofrece la tecnología inalámbrica.

El no contar con una red inalámbrica presentaba limitantes en cuanto a la movilidad de los usuarios, en el caso de los visitantes para acceder a Internet debían hacerlo por su modem GSM o sus celulares con las siguientes ventajas. (Cobro del servicio, limitación de tráfico).

El diseño e implementación de una red inalámbrica con criterios de seguridad constituye un vértice importante de crecimiento y desarrollo de infraestructura tecnológica para la BVL sin presentar riesgos o amenazas a la seguridad de la red actual, por el contrario la solución pretende acoplarse a la red sin afectar la seguridad que tiene la entidad actualmente.

1.4 Alcance del trabajo

El diseño se aplica a un escenario que consta de cuatro niveles, cada uno de ellos con distintos ambientes de trabajo y salas de capacitación.

En el último nivel o sótano se tiene una sala de capacitación, una sala de reuniones y un auditorio, en cada uno de ellos debe ir ubicado un AP.

En el Tercer nivel o piso 3 se consideran 3 APs que darán cobertura a las oficinas de trabajo de ese nivel.

En el área de Mezzanine se tiene el área de dirección de métodos, la sala de desarrollo de bolsa de productos y un salón protocolar, cerca de cada uno de ellos se considera un AP.

La solución contempla 2 Wireless LAN Controller (WLC) de Cisco que administran hasta 6 APs cada uno y que serán ubicados en el data center de la BVL en el sótano.

El tiempo total de la presente implementación, incluido entrega de materiales se detalla a continuación.

Tabla 1.1 Cronograma de trabajos para la implementación de WLAN

Actividades/Semanas	1	2	3	4	5	6	7	8	9
Entrega de materiales de cableado estructurado									
Implementación del cableado estructurado									
Entrega de equipamiento Cisco									
Instalación y configuración de Access Point									
Periodo de pruebas									

En general el proyecto constó de dos etapas, la segunda fue debido a una necesidad

de proporcionar mayor cobertura. En la primera etapa se implementó con un controlador y cuatro APs. En la segunda etapa se agregó otro controlador y seis AP En total son dos (02) controladores y diez (12) APs.

Se implementan dos Redes Virtuales de Área local (VLAN), una de invitados y otra de usuarios.

P/N	Descripción	Q	PU	PT
AIR-WLC2106-K9	2100Series WLAN Controller para hasta seis APs de carga ligera	2	2153.26	4306.52
AIR-LAP1142N-A-K9	802.11a/g/n AP, con antena integrada, configuración FCC	12	860.87	10330.44
AIR-PWRINJ4=	Power inyector – 1140/1250 Series; Spare	12	98.81	1185.72
TOTAL USD + IGV				15822.68

1.5 Síntesis del trabajo

El trabajo está organizado de tal manera que se comprendan los pasos de diseño e implementación, las consideraciones tomadas, los recursos usados (hardware, software, etc.). El trabajo se desarrolla en las siguientes fases

a) Dimensionamiento de la solución.- Para ajustar el diseño a los requerimientos del cliente, etc.

b) Estudio del sitio.- Consiste en la determinación de las zonas oscuras, y la obtención de las alternativas de la simulación.

c) Propuesta de diseño.- Sobre la infraestructura de la red, la seguridad de la Red y el esquema final.

d) Equipamiento.- Identificando los controladores, Puntos de acceso, las antenas y el software de gestión

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

En este capítulo se exponen las bases teóricas conceptuales más importantes para la comprensión del sistema descrito en el presente informe.

Los temas a tratar son;

1. Redes inalámbricas
2. Estándares IEEE 802.11
3. Seguridad

2.1 Redes inalámbricas

Las redes de área local inalámbricas (WLAN), redefinen la forma en que la industria contempla las redes de área local (LAN). La conectividad ya no implica conexión física. El networking inalámbrico proporciona todas las funciones y beneficios de las tecnologías de LAN tradicionales sin alambres ni cables. La libertad de movilizarse sin perder la conectividad ha ayudado a conducir las redes inalámbricas hasta nuevos niveles. Existen cuatro factores importantes a considerar antes de implementar una red inalámbrica.

1. Alta disponibilidad.
2. Escalabilidad
3. Gestionabilidad.
4. Arquitectura abierta.

2.1.1 Definición

Una red de área local inalámbrica (WLAN) proporciona todas las funciones y beneficios de las tecnologías LAN tradicionales, como Ethernet, pero sin las limitaciones impuestas por los alambres o cables. De esta forma, las WLAN redefinen la forma en la cual la industria contempla las LAN. Conectividad ya no significa conexión física.

Las áreas locales ya no se miden en pies ni en metros, sino en millas o kilómetros. Una infraestructura no necesita estar enterrada u oculta detrás de los muros, sino que puede desplazarse y cambiar según las necesidades de una organización.

Una WLAN, al igual que una LAN, requiere un medio físico a través del cual pasan las señales de transmisión. En lugar de utilizar par trenzado o cable de fibra óptica, las WLAN utilizan luz infrarroja (IR) o frecuencias de radio (RF). El uso de la RF es mucho más popular debido a su mayor alcance, mayor ancho de banda y más amplia cobertura.

Las WLAN utilizan la banda de frecuencia de 2.4 gigahertz (GHz) y de 5 GHz. Estas porciones del espectro de RF están reservadas en la mayor parte del mundo para dispositivos sin licencia. El networking inalámbrico proporciona la libertad y la flexibilidad para operar dentro de edificios y entre edificios.

2.1.2 Beneficios

Las redes de área local Ethernet cableadas actuales operan a velocidades de alrededor de 100 Mbps en la capa de acceso, 1 Gbps en la capa de distribución y hasta 10 Gbps en la capa principal. La mayoría de las redes de área local inalámbrica operan a una velocidad de 11 Mbps a 54 Mbps en la capa de acceso y no tienen como objetivo operar en la capa de distribución o en la capa principal.

El costo de implementar redes de área local inalámbrica compite con el de las redes de área local cableadas. Por lo tanto, ¿porqué instalar un sistema que se encuentra en el extremo mas bajo de las capacidades de ancho de banda actuales?

1. Una razón es que en muchos entornos LAN pequeños, las velocidades más lentas son adecuadas para soportar las necesidades de las aplicaciones y del usuario. Con muchas oficinas conectadas ahora a Internet por medio de servicios de banda ancha como DSL o cable, las redes de área local inalámbrica pueden manejar las demandas de ancho de banda.
2. Otra razón es que las WLANs permiten a los usuarios movilizarse dentro de un área definida con libertad y aun así permanecer conectados. Durante las reconfiguraciones de oficina, las WLANs no requieren un recableado ni sus costos asociados.

Las WLANs presentan numerosos beneficios para las oficinas hogareñas, los negocios pequeños, los negocios medianos, las redes de campus y las corporaciones más grandes. Los entornos que es probable que se beneficien de una WLAN tienen las siguientes características:

a. Requieren la velocidad de una LAN Ethernet estándar.
b. Se benefician de los usuarios móviles.
c. Reconfiguran la disposición física de la oficina a menudo.
d. Se expanden rápidamente.
e. Utilizan una conexión a Internet de banda ancha.
f. Enfrentan dificultades significativas al instalar LANs cableadas.
g. Necesitan conexiones entre dos o mas LANs en un área metropolitana.
h. Requieren oficinas y LANs temporales.

2.1.3 Tecnologías existentes y emergentes.

Muchas dependen del área de cobertura: PAN (de área personal), LAN (de área local), MAN (área metropolitana) y WAN (de área extendida), también poseen distintas

capacidades de servicio.

Las redes inalámbricas de nueva generación son redes experimentales, como lo era el Internet hace 10 o 12 años, utilizan nuevas tecnologías, son el banco de pruebas de nuevos protocolos de comunicaciones y nuevas aplicaciones y además en ellas se desarrollan los protocolos de internet del futuro.

En un inicio, las redes inalámbricas tenían como objetivo la transmisión de datos a mayores velocidades, hoy se busca transmitir información con calidad de servicio.

a. Calidad de Servicio (QoS)

QoS por sus siglas en ingles, Quality of Service, son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado, esto se denomina comúnmente (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de video o voz.

Inicialmente el objetivo de las redes era tener la capacidad de enviar información entre dos puntos. Se hacia el "mejor esfuerzo" para que la información llegara a cierta velocidad y en cierto tiempo.

El desarrollo de aplicaciones en tiempo real requiere adicionalmente que la información llegue. Esto permite transmitir datos, voz, videos, imágenes, etc.:

i. A una cierta tasa de bits (throughput)
ii. En un tiempo determinado (delay)
iii. Con una variación de demora determinada (jitter)
iv. Con pérdida de paquetes menor a cierto umbral

b. Redes Personales (PAN) IEEE 802.15

Desarrollado inicialmente por Ericsson para accesos a corta distancia. El objetivo es la eliminación de cables de mouses, teclados, teléfonos, cámaras digitales y cualquier dispositivo móvil. Permite utilizar múltiples medios como Radio Frecuencia (RF), celular, punto a punto, convencional. Se dispone de dos tecnologías:

i. Bluetooth
ii. UWB (Banda Ultra Ancha)

b.1 Bluetooth

Es una red de área personal inalámbrica (pico celdas). Normado por el estándar Bluetooth 802.15. Opera en la banda de 2.4 GHz. Sus velocidades de transmisión van de 1 a 20 Mbps. Su alcance hasta de 11 metros.

b.2 Banda Ultra Ancha (UWB)

Es una banda de 500 MHz en el espectro entre 3.1 y 10.6 GHz. Se transmite directamente sin modulación. Su alcance es de hasta 10 metros. Está normado por el

estándar 802.15.3ª. Es el futuro reemplazante de Bluetooth

c. Redes Inalámbricas de Área Local (WLAN) IEEE 802.11

Se dispone de la tecnología Wi-Fi que es parte del grupo de trabajo 802.11 de la IEEE Los cuatro estándares principales son:

a. 802.11a, 6 a 54 Mbps banda de 5 GHz
b. 802.11b, 11Mbps banda de 2.4 GHz
c. 802.11g, a 54 Mbps banda de 2.4 GHz (interoperable con 802.11b)
d. 802.11n, a 300 Mbps banda de 2.4 GHz o 2.2 GHz

El alcance de cada estándar varía de acuerdo a la frecuencia en la cual opera.

d. Redes Metropolitanas IEEE 802.16 (WiMax)

WiMax, es un estándar de transmisión inalámbrica de datos 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 (NLOS), sin línea de vista por sus siglas en ingles.

Integra la familia de estándares IEEE 802.16. Inicialmente se encontraba en la banda de 10-66 GHz y requería torres con línea de vista (LOS), por sus siglas en ingles, la nueva versión 802.16a, ratificada en marzo del 2003, utiliza una banda del espectro más estrecha y baja, de 2-11 GHz, facilitando su regulación.

Además, como ventaja añadida, no requiere de torres donde exista enlaces del tipo LOS sino únicamente del despliegue de estaciones base (BS) formadas por antenas emisoras-receptoras con capacidad de dar servicio a unas 200 estaciones suscriptoras (SS) que pueden dar cobertura y servicios a edificios completos. Su instalación es muy sencilla y rápida y su precio competitivo en comparación con otras tecnologías de acceso inalámbrico como Wi-Fi.

e. Tecnologías Móviles

Se encuentran a GSM, GPRS, UMTS.

e.1 GSM

El sistema Global para las comunicaciones Móviles (GSM), es un sistema estándar completamente definido, para la comunicación mediante teléfonos móviles que incorporan tecnología digital.

Por ser digital cualquier cliente de GSM puede conectarse a través de su teléfono con su computador y puede hacer, enviar y recibir mensajes por e-mail (correo electrónico), faxes, navegar por Internet, acceso seguro a la red informática de una compañía (Intranet), así como utilizar otras funciones digitales de transmisión de datos, incluyendo el servicio de mensajes cortos (SMS) o mensajes de texto.

GSM se considera, por su velocidad de transmisión y otras características, un

estándar de segunda generación (2G). Su extensión a 3G se denomina UTMS y difiere en su mayor velocidad de transmisión, el uso de una arquitectura de red ligeramente distinta y sobre todo en el empleo de diferentes protocolos de radio (W-CDMA).

e.2 GPRS

General Packet Radio Service (GPRS) o servicio general de paquetes vía radio, es una extensión del Sistema Global para comunicaciones Móviles o GSM, para la transmisión de datos no conmutada (o por paquetes).

Una conexión GPRS está establecida por la referencia a su nombre del punto de acceso (APN). Con GPRS pueden utilizar los servicios tales como Wireless Application Protocol (WAP), servicios de mensajes cortos (SMS), servicio de mensajería multimedia (MMS), Internet, y para los servicios de comunicación como el correo electrónico y la World Wide Web (WWW).

Para fijar una conexión de GPRS para un modem inalámbrico, un usuario debe especificar un APN, opcionalmente un nombre y contraseña de usuario, y muy raramente una dirección IP, todo proporcionado por el operador de red.

La transferencia de datos de GPRS se cobra por volumen de información transmitida (en kilo o megabytes), mientras que la comunicación de datos a través de conmutación de circuitos tradicionales se factura por minuto de tiempo de conexión, independientemente de si el usuario utiliza toda la capacidad del canal o está en un estado de inactividad. Por este motivo, se considera más adecuada la conexión conmutada para servicios como la voz que requieren un ancho de banda constante durante la transmisión, mientras que los servicios de paquetes como GPRS se orientan al tráfico de datos.

La tecnología GPRS como bien lo indica su nombre es un servicio orientado a radio enlaces que da mejor rendimiento a la conmutación de paquetes en dichos radio enlaces.

e.3 UMTS

Sistema Universal de Telecomunicaciones Móviles (UMTS), es una de las tecnologías usadas por los móviles de tercera generación 3G, también llamado W-CDMA, sucesora de GSM. Debido a que la tecnología GSM propiamente dicha no podía seguir un camino evolutivo para llegar a brindar servicios considerados de tercera generación.

Aunque inicialmente está pensada para su uso en teléfonos móviles, la red UMTS no está limitada a estos dispositivos, pudiendo ser utilizada por otros.

Sus tres grandes características son las capacidades multimedia, una velocidad de acceso a Internet elevada, la cual también le permite transmitir audio y video en tiempo real, y una transmisión de voz con calidad equiparable a la de las redes fijas. Además dispone de una variedad de servicios muy extensa.

2.2 Estándares IEEE 802.11

En esta sección se explicará el estándar en los siguientes ítems: 1) Descripción general, 2) Descripción de IEEE y del Comité 802, 3) Arquitectura lógica, 4) Clases, 5) Componentes y tecnologías.

2.2.1 Descripción general

Antes de que existieran los estándares inalámbricos, los sistemas inalámbricos estaban plagados de bajas velocidades de datos, incompatibilidades y elevados costos. La normalización proporciona los siguientes beneficios:

a. Interoperabilidad entre los productos de múltiples fabricantes.
b. Desarrollo más rápido de productos.
c. Estabilidad.
d. Capacidad para actualizar.
e. Reducciones de costos.

Es importante comprender los dos tipos principales de estándares. Un estándar público no ha sido aprobado por una organización oficial de normalización, sino que es reconocido como estándar a causa de la difusión de su uso. También se denomina estándar de facto. A menudo, un grupo de estándares oficiales adoptaran posteriormente estándares de facto.

Un estándar oficial es publicado y controlado por una organización de normalización oficial como el IEEE. La mayoría de los grupos de normalización oficiales son financiados por el gobierno y la industria, que incrementa la cooperación y la implementación a nivel nacional e internacional. Por esta razón la mayoría de las compañías deberán implementar productos inalámbricos que sigan normas oficiales. Los estándares oficialmente aprobados se denominan estándares de jure. En la Figura 2.1 se muestran algunas organizaciones de normalización importantes.

Figura 2.1 Organizaciones de normalización importantes

Al implementar dispositivos de múltiples fabricantes, es importante que todos los

dispositivos se conformen al mismo estándar para asegurar la interoperabilidad. Por ejemplo, el cumplimiento con el estándar 802.11b actual puede crear una WLAN funcional, independientemente del fabricante del producto. El desempeño, la configuración y la capacidad de administración no son siempre los mismos, o iguales, entre fabricantes.

Un problema común en entornos móviles será que las tarjetas de interfaz de red (NIC) multi fabricante intenten acceder a una marca diferente de punto de acceso.

2.2.2 Descripción de IEEE y del Comité 802

El IEEE, fundado en 1884, es una organización profesional sin fines de lucro con más de 377,000 miembros en todo el mundo. El IEEE consiste en muchas sociedades y grupos de trabajo individuales. Desempeña un papel crítico en el desarrollo de estándares, la publicación de obras técnicas, conferencias de patrocinamiento y otorgamiento de acreditaciones el área de tecnología eléctrica y electrónica.

En el área de networking (redes), el IEEE ha producido muchos estándares ampliamente utilizados como el grupo 802.x de estándares de la red de área local (LAN) y los estándares de área metropolitana (MAN) los cuales se muestran en la Figura 2.2.

- 802.0 Sponsor Executive Committee (SEC)
- 802.1 High Level Interface (HILI)
- 802.2 Logical Link Control (LLC)
- 802.3 CSMA/CD (Ethernet)
- 802.4 Token Bus
- 802.5 Token Ring
- 802.6 Metropolitan Area Network (MAN)
- 802.7 BroadBand Technical Advisory Group (BBTAG)
- 802.8 Fiber Optics Technical Advisory Group (FOTAG)
- 802.9 Integrated Services LAN (ISLAN)
- 802.10 Standard for Interoperable LAN Security (SILS)
- 802.11 Wireless LAN (WLAN)
  - 802.11a, 802.11b, 802.11e, 802.11g, 802.11i
- 802.12 Demand Priority
- 802.14 Cable-TV Based Broadband Communication Network
- 802.15 Wireless Personal Area Network (WPAN)
- 802.16 Broadband Wireless Access (BBWA)
- 802.17 RPRSG Resilient Packet Ring Group (RPRSG)

Figura 2.2 Estándares LAN/MAN IEEE

El termino 802.11 se refiere realmente a una familia de protocolos, incluyendo la especificación original, 802.11, 802.11b, 802.11a, 802.11g, 802.11n y otros. El 802.11 es un estándar inalámbrico que especifica conectividad para estaciones fijas, portátiles y móviles dentro de un área local.

El propósito del estándar es proporcionar una conectividad inalámbrica para automatizar la maquinaria y el equipamiento o las estaciones que requieren una rápido

implementación. Estos pueden ser portátiles, handheld (dispositivos de mano) o montados en vehículos en movimiento dentro de un área local.

El estándar se denomina oficialmente Estándar IEEE para especificaciones MAC y PHY de WLAN (especificaciones de la IEEE de la capa física y la capa de enlace para las redes inalámbricas de área local). Define los protocolos por aire necesarios para soportar un networking inalámbrico en un área local.

2.2.3 Arquitectura lógica

La arquitectura IEEE 802.11 consiste en varios componentes que interactúan para proporcionar conectividad inalámbrica. Estos componentes pueden soportar movilidad entre estaciones transparentes para las capas superiores.

a. Conjunto de Servicios Básicos (BSS)

Es el bloque constructor básico de una LAN IEEE 802.11. La Figura 2.3 muestra un BSS con tres estaciones que son miembros del BSS, además del AP. El BSS abarca una única área RF, o celda, según lo indica el círculo. A medida que una estación se aleja del AP, su velocidad de datos disminuirá. Cuando sale de su BSS, ya no puede comunicarse con otros miembros del mismo. Un BSS utiliza el modo de infraestructura, un modo que necesita un AP, Todas las estaciones se comunican por medio del AP, y no directamente. Un BSS tiene una única identificación de conjunto de servicios (SSID).

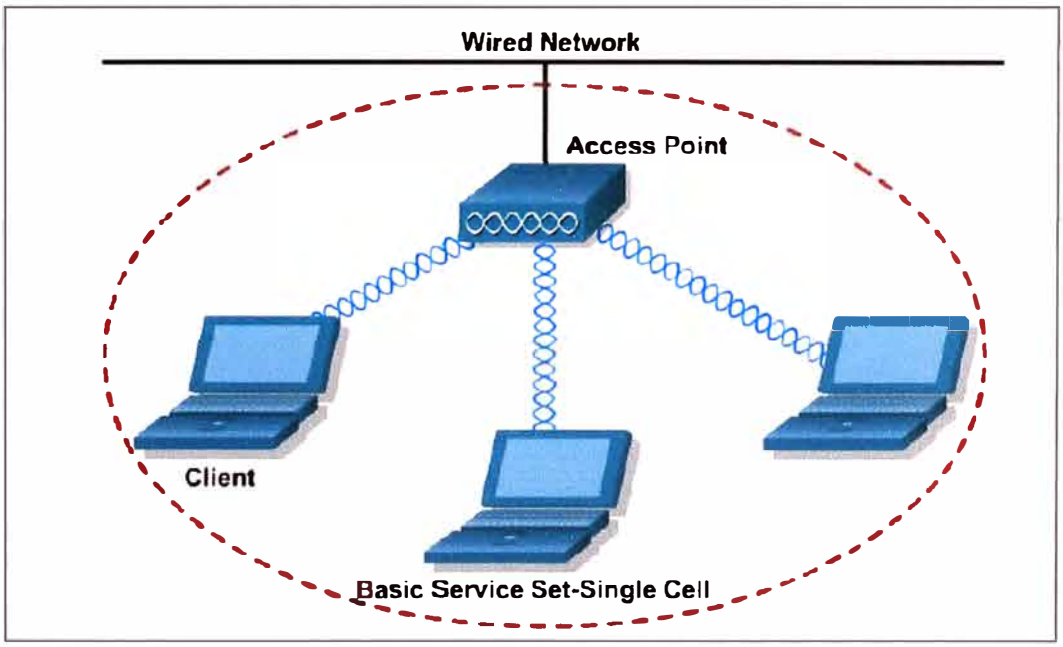

Figura 2.3 Conjunto de servicios básicos BSS

b. Conjunto de Servicios Básicos Independiente (IBSS)

Es el tipo más básico de LAN IEEE 802.11. Una LAN IEEE 802.11 mínima consiste solo en dos estaciones. En este modo de operación, las estaciones IEEE 802.11 se comunican directamente. Puesto que este tipo de LAN IEEE 802.11 se forma a menudo sin planificar solamente mientras es necesaria una WLAN, a menudo se denomina red

ad-doc.

Puesto que un IBSS consiste en STAs (Estaciones asociadas) conectadas directamente, también se denomina red peer-to-peer (punto a punto). Existe, por definición, solo un BSS y no hay un Sistema de Distribución (DS). Un IBSS con cuatro estaciones se muestra en la Figura 2.4. Un IBSS puede tener una cantidad arbitraria de miembros. Para comunicarse fuera del IBSS, una de las STAs debe actuar como Gateway o router.

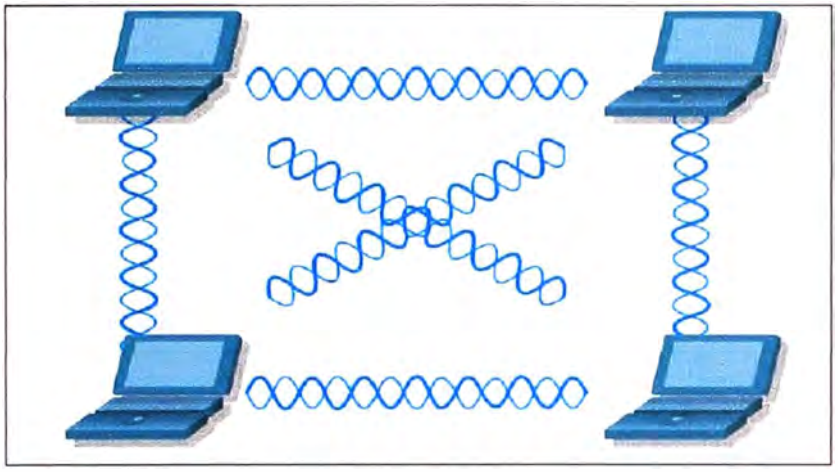

Figura 2.4 IBSS con cuatro estaciones

c. Sistema de distribución (DS)

Las limitaciones físicas determinan las distancias de estación a estación que pueden soportarse. En el caso de algunas redes esta distancia es suficiente. En el caso de otras, se requiere un incremento en la cobertura.

En lugar de existir independientemente, un BSS también puede formar un componente de un conjunto de servicios extendido (ESS). Un ESS se construye a partir de múltiples BSS, que se conectan a través de APs. Los APs se conectan a un DS común, como lo muestra la Figura 2.5. El DS puede ser cableado o inalámbrico, LAN o WAN. La arquitectura WLAN IEEE 802.11 se especifica independientemente de las características físicas del DS.

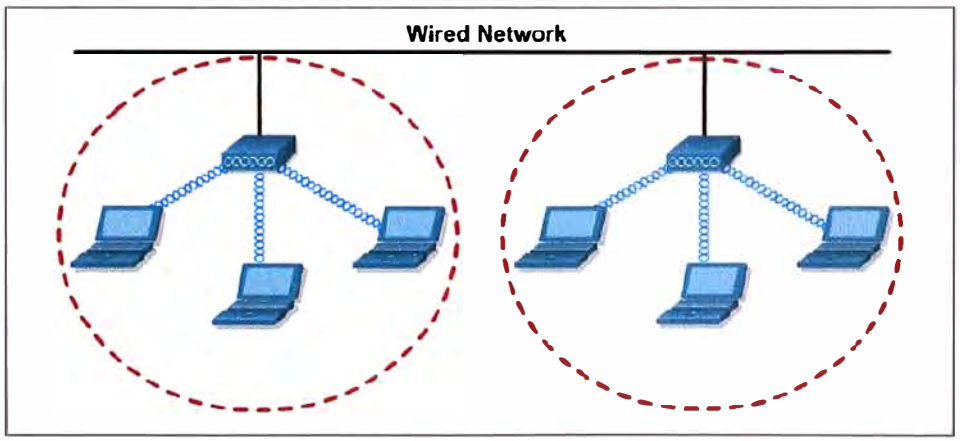

Figura 2.5 Sistema de Distribución.

d. Conjunto de Servicios Extendidos (ESS)

Se define como dos o más BSS conectados por medio de un DS común, como lo ilustra la Figura 2.5. Esto permite la creación de una red inalámbrica de tamaño y complejidad arbitrarios. Al igual que sucede con un BSS, todos los paquetes de un ESS deben atravesar uno de los APs.

2.2.4 Clases

En el momento existen distintos estándares para las WLAN, desarrolladas por la IEEE:

a. 802.11 b

Introducido en 1999, como extensión al estándar 802.11 publicado en 1997. Los equipos inalámbricos que operaban con la norma 802.11 nunca llegaron a tener una buena acogida, por que la máxima velocidad de conexión que ofrecían era de 2 Mbps. La norma 802.11b subsano este problema al permitir lograr una velocidad mas alta de transferencia de datos. Dicha velocidad tiene un límite de 11 Mbps (similar al de una red Ethernet convencional).

En la practica, se logran velocidades entre 2 y 5 Mbps, lo que depende del numero de usuarios, de la distancia entre emisor y receptor, de los obstáculos y de la interferencia causada por otros dispositivos.

El factor interferencia es uno de los que mas influye, porque los equipos 802.11b operan en la banda de 2.4 Ghz, en la que se presenta interferencia de quipos como teléfonos inalámbricos y hornos microondas. A pesar de sus problemas el estándar 802.11b se ha convertido en el más popular.

b. 802.11 a

Se introdujo al mismo tiempo que el 802.11b, con la intención de constituirla en la norma para redes inalámbricas para uso empresarial (802.11b se enfoco hacia las redes caseras y para pequeños negocios). Ofrece velocidades de hasta 54 Mbps (típicamente 22 Mbps) y opera en la banda de 5 Ghz. Su alto precio, el hecho de que la banda de 5 Ghz este regulada en algunos países, y su menor cubrimiento ha hecho que los equipos 802.11a sean menos populares que los 802.11b.

c. 802.11 g

Surgió en 2003, como la evolución del estándar 802.11b. Esta norma ofrece velocidades hasta de 54 Mbps (típicamente 22 Mbps) en la banda de 2.4 Ghz, y es compatible hacia atrás con los equipos 802.11b, por lo cual ha tenido una gran acogida, y se prevé que reemplace por completo al estándar 802.11b en un futuro no muy lejano.

d. 802.11 n

EEE 802.11n es una propuesta de modificación al estándar IEEE 802.11-2007 para

mejorar significativamente el desempeño de la red más allá de los estándares anteriores, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps.

Actualmente la capa física soporta una velocidad de 300Mbps, con el uso de dos flujos espaciales en un canal de 40 MHz. Dependiendo del entorno, esto puede transformarse a un desempeño visto por el usuario de 100Mbps. El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009.

2.2.5 Componentes y tecnologías

El elemento esencial de una red inalámbrica es el Acces Point (AP) o Punto de Acceso Inalámbrico.

Un Access Point (AP) actúa como un concentrador (Hub) de comunicaciones para los usuarios de redes inalámbricas. Un AP puede enlazar redes cableadas e inalámbricas. En grandes instalaciones, múltiples access points pueden configurarse para permitir a los usuarios inalámbricos hacer itinerancia (roaming) entre access points sin interrupción. Los access points también proporcionan seguridad. Finalmente, un AP puede actuar como repetidor inalámbrico, o punto de extensión para la red inalámbrica.

Un AP puede controlarse y configurarse a través de la línea de comandos (CLI) e interfaces de usuario grafico (Web). La administración también puede llevarse a cabo a través de protocolos tradicionales como el Protocolo Simple de Administración de Redes (SNMP). Una variedad de opciones de antenas puede proporcionar un alcance o velocidad adicional, dependiendo de la instalación. Un AP puede ser de banda única, como el AP 802.11a de 5 GHz. También puede ser de banda dual, como el AP 802.11a de 5 GHz o el 802.11b de 2.4 GHz.

A continuación se presentan dos puntos de acceso muy populares de la marca Cisco, se trata del Cisco Aironet 1130AG (Figura 2.6) y el Cisco Aironet 1240AG (Figura 2.7) y se describen sus principales características.

Cisco Aironet 1130AG

i. Diseño ligero y discreto para entornos de oficina
ii. Antena integrada
iii. Admite varios estándares de seguridad para la protección y autenticación de identidad
iv. Numero ilimitado de puntos de acceso
v. Funciona con la Solución Unificada para redes Cisco.

Cisco Aironet 1240AG

i. Diseñado para entornos menos decorativos cono fabricas, almacenes o áreas de comercio minorista.
ii. Admite varios estándares de seguridad para la protección

En ocasiones es necesario hacer uso de antenas especiales para cubrir cierta área o mejorar la cobertura. Las antenas generalmente se dividen en dos tipos. Antenas direccionales y antenas omnidireccionales. Las antenas direccionales, irradian energía de radiofrecuencia (RF) predominantemente en una dirección, algunos tipos comunes de este tipo de antenas son la antenas Yagi, las parabólicas las semiparabolicas y las antenas panel.

Las antenas omnidireccionales, irradian energía de radio frecuencia en todas las direcciones, algunos tipos comunes de antenas omnidireccionales son, la antena de mástil y la antena dipolo rubber.

Todas las antenas tienen un patrón de radiación. Muy relacionada con el patrón de radiación esta la polarización de la antena. Las antenas pueden ser agrupadas en sistemas para lograr el patrón deseado. Estos sistemas pueden entonces ser dirigidos electrónicamente. Debido al diseño de baja potencia de las LAN inalámbricas, todas las antenas usadas son pasivas. Una antena pasiva no tiene amplificadores conectados, y por lo tanto tendrá las mismas características sea que este transmitiendo o recibiendo. Algunos tipos de antenas se muestran en la Figura 2.8.

Figura 2.6 Cisco Aironet 1130AG

Figura 2.7 Cisco Aironet 1240AG

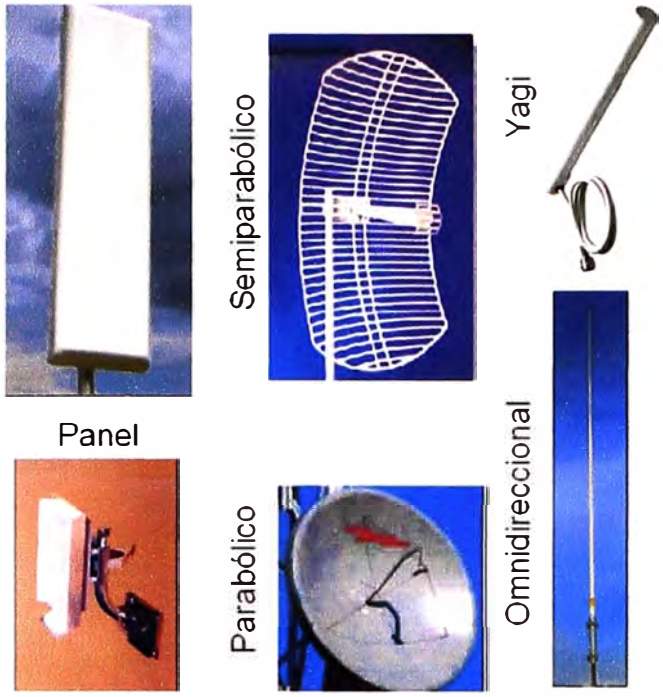

Figura 2.8 Tipos de antenas

2.3 Seguridad

La seguridad de la red es el proceso por el cual se protegen los recursos de información digital. Los objetivos de la seguridad son mantener la integridad, proteger la confidencialidad y asegurar la disponibilidad.

El crecimiento de la computación ha generado enormes avances en la forma en que las personas viven y trabajan. Por lo tanto, todas las redes deben estar protegidad para alcanzar su máximo potencial. Las WLANs presentan desafíos de seguridad única.

En esta parte del informe habalremos sobre los fundamentos de la seguridad de las WLANs. El crecimiento exponencial del networking, incluyendo als tecnologías inalámbricas, ha conducido a aumentare los riesgos de seguridad. Muchos de estos riesgos se deben al hacking (piratería), además del uso incorrecto de los recursos de la red.

2.3.1 Fundamentos de seguridad

Se explica este tema en cuatro ítems a) Definición de Seguridad, b) Vulnerabilidades de las WLANs, c) Amenazas a la WLAN, d) Métodos de ataque inalámbrico.

a. Definición de seguridad.

Un propósito principal de la seguridad es mantener afuera a los intrusos. En la mayoría de los casos, esto significa construir paredes fuertes y establecer puertas pequeñas bien protegidas para proporcionar acceso seguro a un grupo selecto de personas. Esta estrategia funciona mejor para las LANs cableadas que para las WLANs. El crecimiento del comercio móvil y las redes inalámbricas hace que los antiguos modelos sean inadecuados. Las soluciones de seguridad deben estar integradas sin fisuras y ser

muy transparentes, flexibles y administrables.

Cuando la mayoría de la gente habla sobre seguridad, hacen referencia a asegurar que los usuarios puedan realizar solo las tareas que tienen autorizado hacer y que puedan obtener solo la información que tienen autorizado tener. La seguridad también significa asegurar que los usuarios no puedan causar daño a los datos, a las aplicaciones o al entorno operativo de un sistema. La palabra seguridad comprende la protección contra ataques maliciosos. La seguridad también comprende el control de los efectos de los errores y de las fallas del equipo. Todo lo que pueda proteger contra un ataque inalámbrico probablemente evitara también otros tipos de problemas.

b. Vulnerabilidades de las WLANs.

Las WLANs son vulnerables a ataques especializados. Muchos de estos ataques explotan las debilidades de la tecnología, superadas hoy en día, también hay muchas debilidades de configuración, ya que algunas compañías, no están usando las características de seguridad de las WLANs en todos sus equipos.

En realidad, muchos dispositivos son entregados con passwords (claves de acceso) de administrador predeterminadas. Finalmente, hay debilidades de políticas. Cuando una compañía no tiene una política inalámbrica clara sobre el uso de la tecnología inalámbrica, los empleados pueden configurar sus propios APs. Un AP configurado por un empleado se conoce como AP escondido u oculto, que raramente es seguro.

Las vulnerabilidades de la seguridad del 802.11 pueden ser una barrera para el desarrollo de WLANs empresariales. Hay personas entusiastas, dispuestas y calificadas para tomar ventaja de cada vulnerabilidad de una WLAN. Ellas están constantemente tratando de descubrir y explotar nuevas vulnerabilidades. Se han escrito numerosos documentos sobre el tema de la seguridad del 802.11. Lo que sigue es un resumen de las principales vulnerabilidades:

i. Autenticación débil únicamente de dispositivo.- Se autentican los dispositivos clientes. Los usuarios no se autentican.

ii. Encriptación de datos débil.- Se ha probado que la seguridad equivalente a la cableada (WEP) es ineficiente como medio para encriptar datos.

iii. No hay integridad de mensajes.- Se ha probado que el valor de control de integridad (ICV) no es efectivo como medio para asegurar la integridad de los mensajes.

c. Amenazas a la WLAN.

Existen cuatro clases principales de amenazas a la seguridad inalámbrica: Amenazas no estructuradas, Amenazas estructuradas, Amenazas externas, Amenazas internas

i. Las amenazas no estructuradas

Consisten principalmente en individuos inexpertos que están usando herramientas de

hacking disponibles fácilmente como scripts de Shell y crakers de passwords.

iii. Las amenazas estructuradas

Vienen de hackers que están mucho más motivados y son técnicamente competentes. Estas personas conocen las vulnerabilidades de los sistemas inalámbricos y pueden comprender y desarrollar explotación de códigos, scripts y programas.

iii. Las amenazas externas

Son individuos u organizaciones que trabajan desde el exterior de la compañía. Ellos no tienen acceso autorizado a la red inalámbrica. Ingresan a la red principalmente desde el exterior del edificio como estacionamientos, edificios adyacentes, o áreas comunes. Estos son los tipos de amenazas por los que la gente gasta la mayor parte del tiempo y dinero en protegerse.

iv. Las amenazas internas

Ocurren cuando alguien tiene acceso autorizado a la red con una cuenta en un servidor o con acceso físico al cableado. El acceso inalámbrico puede ser una gran amenaza a la seguridad de la red. La mayoría de las WLANs tienen pocas o ninguna restricción. Una vez asociado a un AP, un atacante puede recorrer libremente la red interna.

d. Métodos de ataque inalámbrico.

Los métodos de ataque inalámbrico pueden ser divididos en tres categorías, reconocimiento, ataque de acceso y negación de servicio.

i. Reconocimiento.

El reconocimiento es el descubrimiento y mapeo no autorizado de sistemas, servicios o vulnerabilidades. También es conocido como reunión de información y normalmente precede a un acuerdo real o ataque de negación de servicio, los cuales se expondrá más adelante.

El reconocimiento es similar a un ladrón que revisa un vecindario buscando casas fáciles donde entrar. En muchos casos, los intrusos llegan tan lejos como a probar el picaporte de la puerta para descubrir áreas vulnerables, a las que pueden explotar en un momento posterior. La realización del reconocimiento comprende el uso de comandos o utilitarios comunes para conocer tanto como sea posible el sitio de la víctima.

El snooping (simulación) inalámbrico y el sniffing (rastreo) de paquetes son términos comunes para los escuchas. La información reunida por las escuchas puede luego ser usada en futuros accesos o ataques de negación de servicio (DoS) a la red. El usar encriptación y evitar protocolos que son fácilmente escuchados puede combatir las escuchas.

Los analizadores de protocolo inalámbrico comerciales como AiroPeek, AirMagnet, o

Sniffer Wireless se pueden usar para escuchar las WLANs. Los analizadores de protocolos gratuitos como Ethereal o tcpdump soportan por completo las escuchas inalámbricas bajo Linux. Las escuchas inalámbricas se pueden usar para ver el trafico d ela red y descubrir los SSIDs (identificadores de la red inalámbrica) en uso, las direcciones MAC validas o para determinar si la encriptación esta siendo usada.

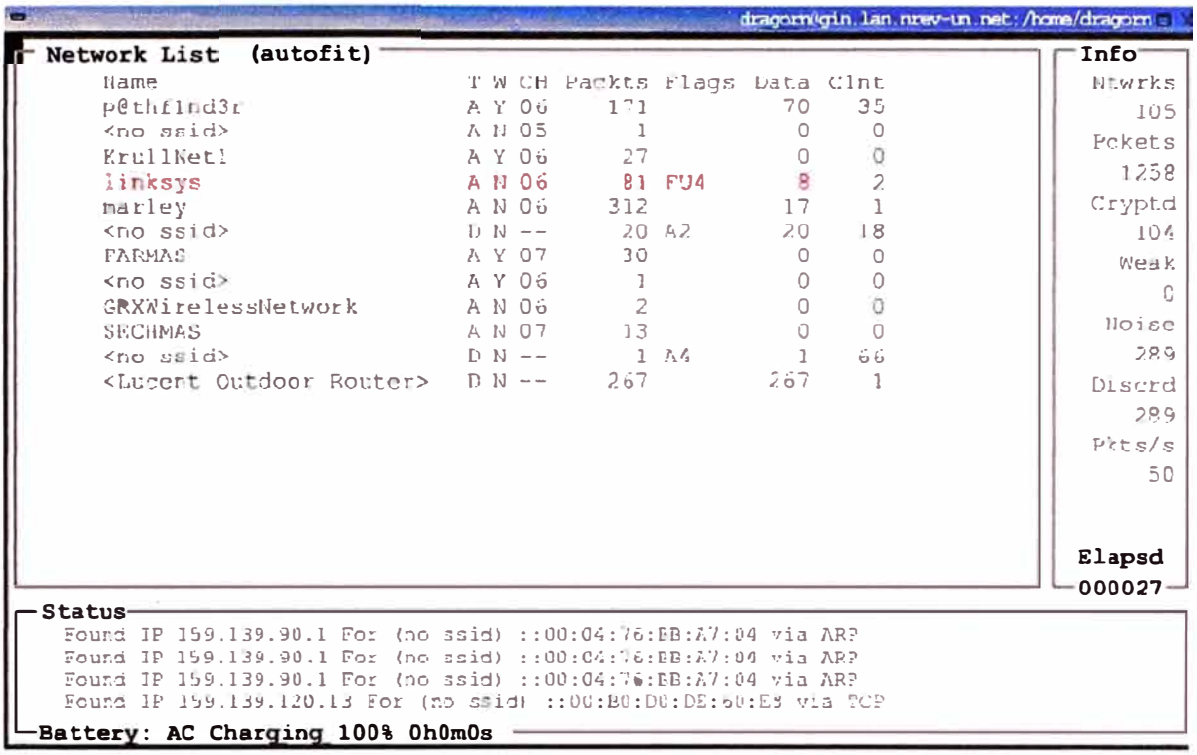

Figura 2.9 Kismet, herramienta utilizada para detectar redes inalámbricas.

El reconocimiento inalámbrico a menudo es llamado wardriving. Los utilitarios usados para explorar las redes inalámbricas pueden ser activos o pasivos. Las herramientas psivas, como Kismet, no tranbsmiten información mientras están detectando redes inalámbricas. Una pantalla de Kismit se muestra en la Figura 2.9.

Los utilitarios activos como el NetStumbler, transmiten pedidos de información adicional sobre una red inalámbrica, una vez que es descubierta. El sistema operativo Windows XP es sensible a la tecnología inalámbrica. Windows XP realiza una búsqueda activa. Intentara conectarse automáticamente a una WLAN descubierta. Algunas personas que usan herramientas WLAN están interesadas en recolectar información acerca del uso d ela seguridad inalámbrica. Otros están interesados en encontrar WLANs que ofrezcan acceso libre a internet o una puerta trasera fácil hacia una red corporativa.

ii. Acceso.

El acceso al sistema, en este contexto, es la capacidad para que un intruso no autorizado logre acceder a un dispositivo para el cual no tiene una cuenta o password. Para ingresar o acceder a los sistemas donde uno no tiene acceso autorizado normalmente se debe ejecutar un hack script o una herramienta que explote una

vulnerabilidad conocida del sistema o aplicación a ser atacada. Acceso es un termino demasiado abarcativo que hace referencia a la manipulación de datos, acceso a sistemas o escaladas privilegiadas no autorizadas. Algunos ejemplos d eacceso son los siguientes:

1. Explotacion de password débiles o no existentes.
2. Explotacion de servicios como HTTP, FTP, SNMP, CDP, Telnet.

El hack más fácil se llama Ingeniería Social. No comprende ninguna habilidad informática. Si un intruso puede engañar a un miembro de una organización para que le de información valiosa como ubicaciones de archivos y servidores o passwords, entonces el proceso de hacking resulta mucho mas sencillo.

El ataque de un AP furtivo (no autorizado) se da cuando la mayoría de los clientes se asocian al AP con la señal mas fuerte. Si un AP no autorizado, que por lo general es un AP furtivo, tiene una señal fuerte, los clientes se asociaran a el. El AP furtivo tendrá acceso al trafico de red de todos los clientes asociados. Por lo tanto, el AP furtivo puede ser usado para realizar ataques por desconocidos contra trafico encriptado como SSL o SSH. El AP furtivo también puede usar spoofing de ARP e IP para engañar a los clientes que envíen passwords e información confidencial. El AP furtivo puede también pedir sesiones no protegidas con la privacidad equivalente a la cableada (WEP) con clientes durante la asociación.

Los ataques contra la WEP incluyen Bit Flipping, Replay Attacks, y la coleccion Weak IV. Muchos ataques WEP no han salido del laboratorio, pero están bien docuemntados. Un utilitario, llamado AirSnort, captura Vectores de Inicializacion debeiles para determinar la clave WEP que se esta usando. La Figura 2.10. Muestra una pantalla del AirSnoft.

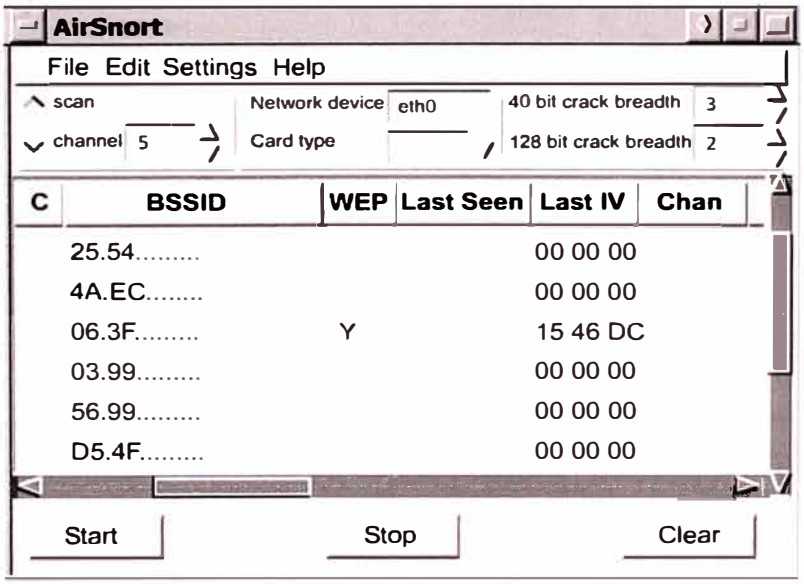

Figura 2.10 Pantalla del AirSnoft.

iii. Negación del Servicio.

La Negación del Servicio (DoS) ocurre cuando un atacante desactiva o corrompe las

redes, sistemas o servicios inalámbricos, con la intención de negar el servicio a usuarios autorizados. Los ataques DoS toman muchas formas. En la mayoría de los casos, la realización del ataque cpomprende simplemente ejecutar un hack, una script o una herramienta.

El atacante no necesita acceder previamente al objetivo, porque todo lo que se necesita normalmente es una forma de acceder a el. Por estas razones y a causa del gran daño potencial, los ataques de DoS son los mas temidos, ya que son los mas difíciles de evitar.

Muchos ataques DoS contra las redes inalámbricas 802.11 han sido teorizados. Un utilitario llamado Wlan Jack, envía paquetes de disociación falsos que desconectan a los clientes 802.11 del Access point. Siempre que se ejecute el utilitario de ataque, los clientes no pueden usar la WLAN. De hecho cualquier dispositivo que opere a 2.4 GHz o a 5 GHz puede se rusado como una herramienta DoS.

2.3.2 Tecnología de seguridad inalámbrica

Se tratarán los siguientes temas:

a. Seguridad Inalámbrica de primera generación

b. Privacidad equivalente a la cableada (WEP)

c. Autenticación y asociación

a. Seguridad Inalámbrica de primera generación

La seguridad no era una gran preocupación para las primeras WLANs. El equipo era propietario, costoso y difícil de conseguir. Muchas WLANs usaban el Identificador del Conjunto de Servicio [Service Set Identifier (SSID)] como una forma básica de seguridad. Algunas WLANs controlaban en acceso ingresando la dirección de control de acceso al medio (MAC) de cada cliente en los access points inalámbricos. Ninguna opción era segura, ya que el sniffing inalámbrico podía revelar las direcciones MAC válidas y el SSID.

El SSID es una cadena de 1 a 32 caracteres del Código Estándar Norteamericano para el Intercambio de Información ASCII (American Standard Code for Information Interchange) que puede ser ingresada en los clientes y en los access points. La mayoría de los access points tienen opciones como 'SSID broadcast' [difusión de SSID] y 'allow any SSID' [permitir cualquier SSID]. Estas características están normalmente activas por defecto y facilitan la configuración de una red inalámbrica.

El usar la opción 'allow any SSID' permite que un cliente con un SSID en blanco acceda a un access point. El 'SSID broadcast' envía paquetes que publican el SSID. El desactivar estas dos opciones no asegura a la red, ya que un sniffer inalámbrico puede fácilmente capturar un SSID válido del tráfico normal de la WLAN.

Los SSIDs no deberían ser considerados una característica segura. La autenticación basada en MAC no está incluida en las especificaciones del 802.11. Sin embargo, muchos fabricantes han implementado una autenticación basada en MAC. La mayoría de los fabricantes simplemente requieren que cada access point tenga una lista de direcciones MAC válidas.

Algunos fabricantes también permiten que el access point consulte una lista de direcciones MAC en un servidor centralizado. Controlar el acceso a una red inalámbrica usando direcciones MAC es tedioso.

Se debe mantener un inventario preciso y los usuarios deben reportar rápidamente la pérdida o el robo de equipo. Las direcciones MAC no son un verdadero mecanismo de seguridad, ya que todas las direcciones MAC no están encriptadas cuando se transmiten.

Un atacante sólo necesitaría capturar una dirección MAC válida para poder acceder a la red. En ciertos casos, la autenticación de direcciones MAC puede suplementar las características de seguridad, pero no debería ser nunca el método principal de seguridad inalámbrica.

b. WEP, Privacidad equivalente a cableada

El estándar IEEE 802.11 incluye a WEP para proteger a los usuarios autorizados de una WLAN de las escuchas ocasionales. El estándar WEP de IEEE 802.11 especificaba una clave de 40 bits, por lo que WEP podía ser exportado y usado en todo el mundo.

La mayoría de los fabricantes han extendido el WEP a 128 bits o más. Cuando se usa el WEP, tanto el cliente inalámbrico como el Access point deben tener una clave WEP idéntica. WEP está basado en un tipo de encriptación existente y familiar, la Rivest Cipher 4 (RC4).

El estándar IEEE 802.11 proporciona dos esquemas para definir las claves WEP a ser usadas en una WLAN. En el primer esquema, un conjunto de hasta cuatro claves predeterminadas son compartidas por todas las estaciones, incluyendo clientes y access points, en un subsistema inalámbrico.

Cuando un cliente obtiene las claves predeterminadas, ese cliente puede comunicarse en forma segura con todas las otras estaciones en el subsistema. El problema con las claves predeterminadas es que cuando llegan a estar distribuidas extensamente, es más probable que estén en peligro. El equipo WLAN de Cisco utiliza este primer esquema.

En el segundo esquema, cada cliente establece una relación de mapeo de clave con otra estación. Esta es una forma más segura de operación, porque menos estaciones tienen las claves. Sin embargo, la distribución de tales claves unicast se vuelve más difícil a medida que la cantidad de estaciones aumenta. La forma en que 802.11 utiliza la

encriptación WEP es débil en varias formas. Estas debilidades están siendo tratadas por el estándar 802.11i.

c. Autenticación y asociación

La Autenticación Abierta y la Autenticación de Clave Compartida son los dos métodos que define el estándar 802.11 para que los clientes se conecten a un access point. El proceso de asociación puede ser dividido en tres elementos, que son investigación, autenticación y asociación.

c.1 Autenticación Abierta

El método de Autenticación Abierta realiza el proceso de autenticación completo en texto abierto. Esto se muestra en la Figura 2.11. La Autenticación Abierta es básicamente una autenticación nula, lo que significa que no hay una verificación del usuario o de la máquina.

La Autenticación Abierta está normalmente ligada a una clave WEP. Un cliente puede asociarse al access point con una clave WEP incorrecta o incluso sin una clave WEP. Un cliente con la clave WEP incorrecta no podrá enviar o recibir datos, ya que la carga de paquetes estará encriptado. Tenga presente que el encabezado no está encriptado por el WEP. Sólo la carga o los datos están encriptados.

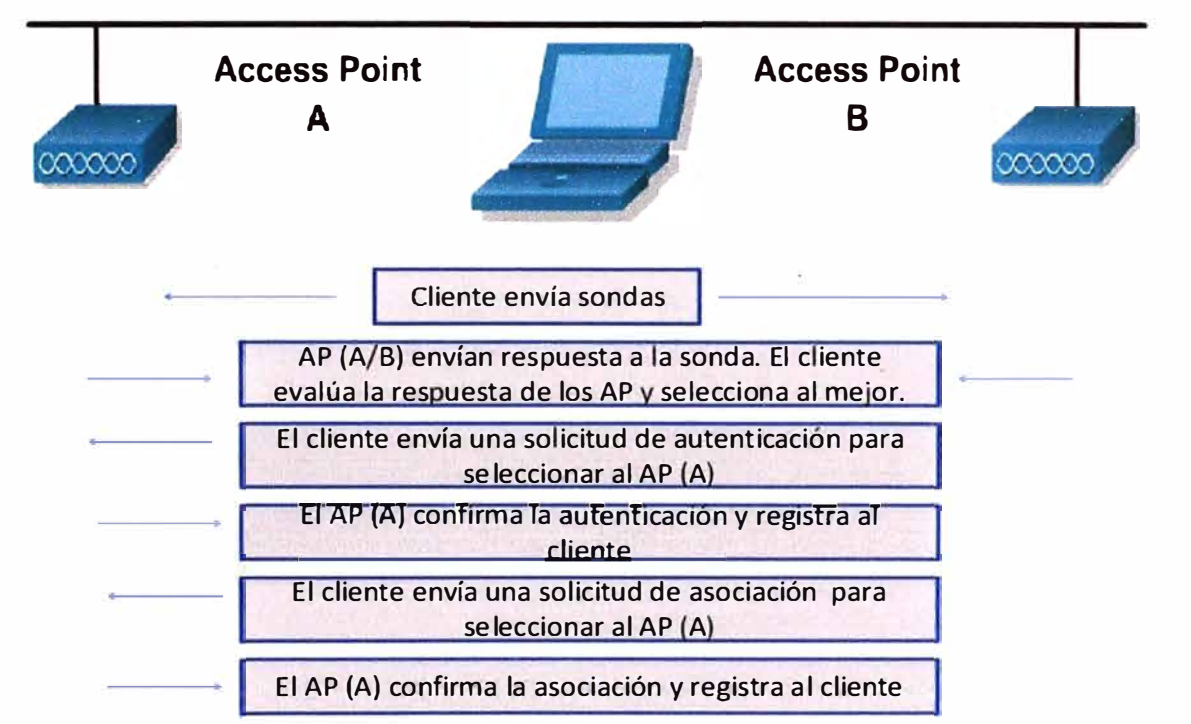

Figura 2.11 Autenticación abierta

c.2 Autenticación de Clave Compartida

La Autenticación de Clave Compartida funciona en forma similar a la Autenticación Abierta, excepto que utiliza la encriptación WEP para un paso. La clave compartida requiere que el cliente y el access point tengan la misma clave WEP.

Un access point que usa la Autenticación de Clave Compartida envía un paquete de texto de desafío al cliente, como muestra la Figura 2.12. Si el cliente tiene la clave equivocada o no tiene clave, fallará en esta parte del proceso de autenticación. El cliente no tendrá permitido asociarse al AP. La clave compartida es vulnerable a un ataque por desconocidos, por lo que no es recomendada.

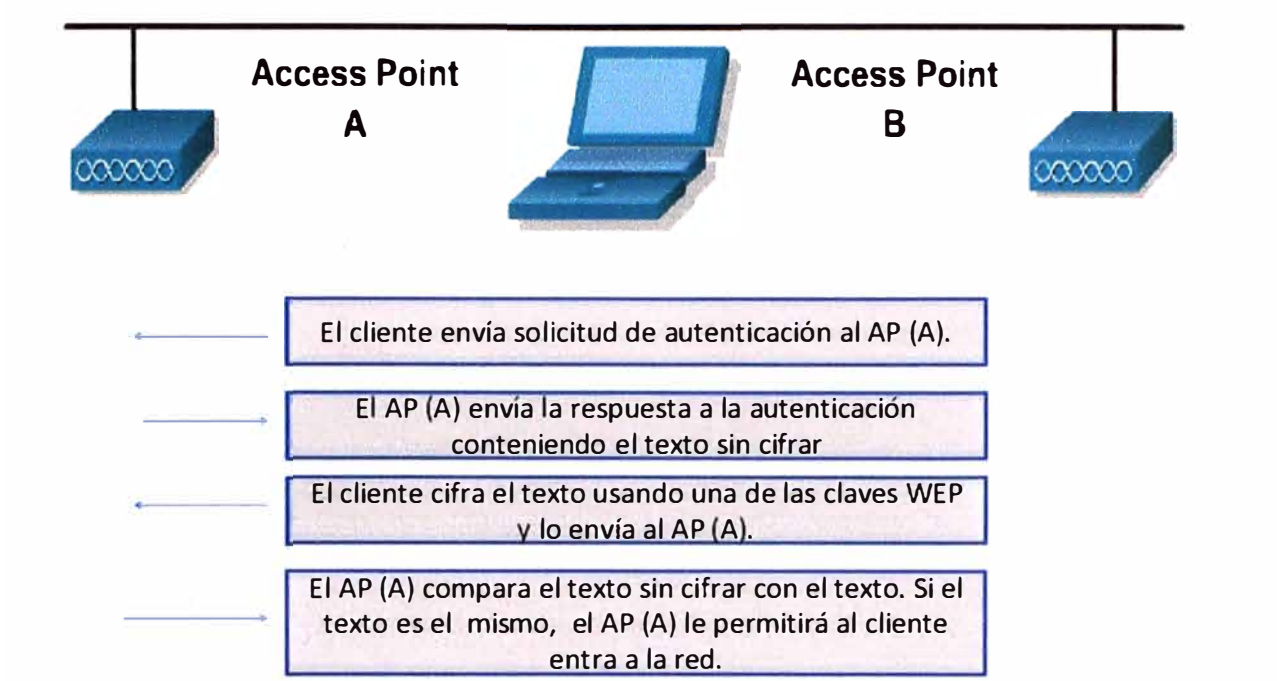

Figura 2.12 Autenticación con clave compartida

2.3.3 Configuración de seguridad WLAN básica

Se tratarán los siguientes temas: a) Seguridad WLAN Básica, b) Seguridad en clientes y APs, c) Supervisión del equipo WLAN y d) Desactivación de servicios no necesarios.

a. Seguridad WLAN Básica

Los access points y bridges inalámbricos deben estar asegurados. A menudo, la administración se realiza usando protocolos estándares, que no son seguros. Esta sección explicará los pasos básicos que se deben tomar para asegurar un equipo de infraestructura inalámbrica.

El equipo de red ofrece muchos protocolos adicionales, lo que simplifica la administración de la red y el acceso de los usuarios. Dependiendo de la configuración de la red, sólo algunos de estos protocolos pueden ser necesarios. Esta sección hablará de protocolos que podrían no ser necesarios. Si un protocolo es necesario, es importante comprender sus debilidades y cómo puede ser asegurado.

a.1 Acceso Físico

La mayoría de los access points son fácilmente accesibles. Normalmente están ubicados cerca de los usuarios y fuera de habitaciones cerradas. Esto pone a los access

points en peligro de ser robados y al alcance de usuarios malintencionados. Se puede usar la supervisión de la red para determinar cuándo un access point se desactiva. Se necesitará seguir procedimientos apropiados para determinar lo que le sucedió al equipo.

Casi todos los fabricantes de tecnología inalámbrica publican los métodos para reconfigurar un access point usando botones de reset o el puerto consola.

a.2 Firmware

El último firmware normalmente será el más seguro. El firmware nuevo deberá ser probado y usado. Se deberán aplicar parches de seguridad o actualizaciones cuando se justifique.

a.3 Acceso por Consola

Las cuentas y los privilegios del administrador deberán estar configurados correctamente. El puerto consola debería estar protegido por una password. Elija una password segura. Ver Figura 2.13.

Administrators					
Username	Read-Only			Read-Write	
user1				✓	
user2				✓	
user3				✓	
ppatrick				✓	
tonorwoo				✓	
SSIDs					
SSID	VLAN	Open	Shared	Network EAP	
AP3	none	✓			
Server-Based Security					
Server Name/IP Address	EAP	MAC	Proxy Mobile IP	Admin	Accounting

Figura 2.13 Resumen de seguridad

a.4 Telnet/SSH

Telnet es un protocolo no encriptado e inseguro. Si es posible, se deberá usar un Shell seguro (SSH) para todas las funciones de la Interfaz de Línea de Comando (CLI). Telnet y SSH deberán estar protegidos con passwords. Para máxima seguridad, desactive Telnet y use sólo SSH.

Se necesita un cliente SSH en la PC de administración o en la estación de trabajo para conectarse a un AP que corre SSH. Hay varios programas freeware que están disponibles como PuTTY, Teraterm SSH y SecureNetTerm. Ver Figura 2.14.

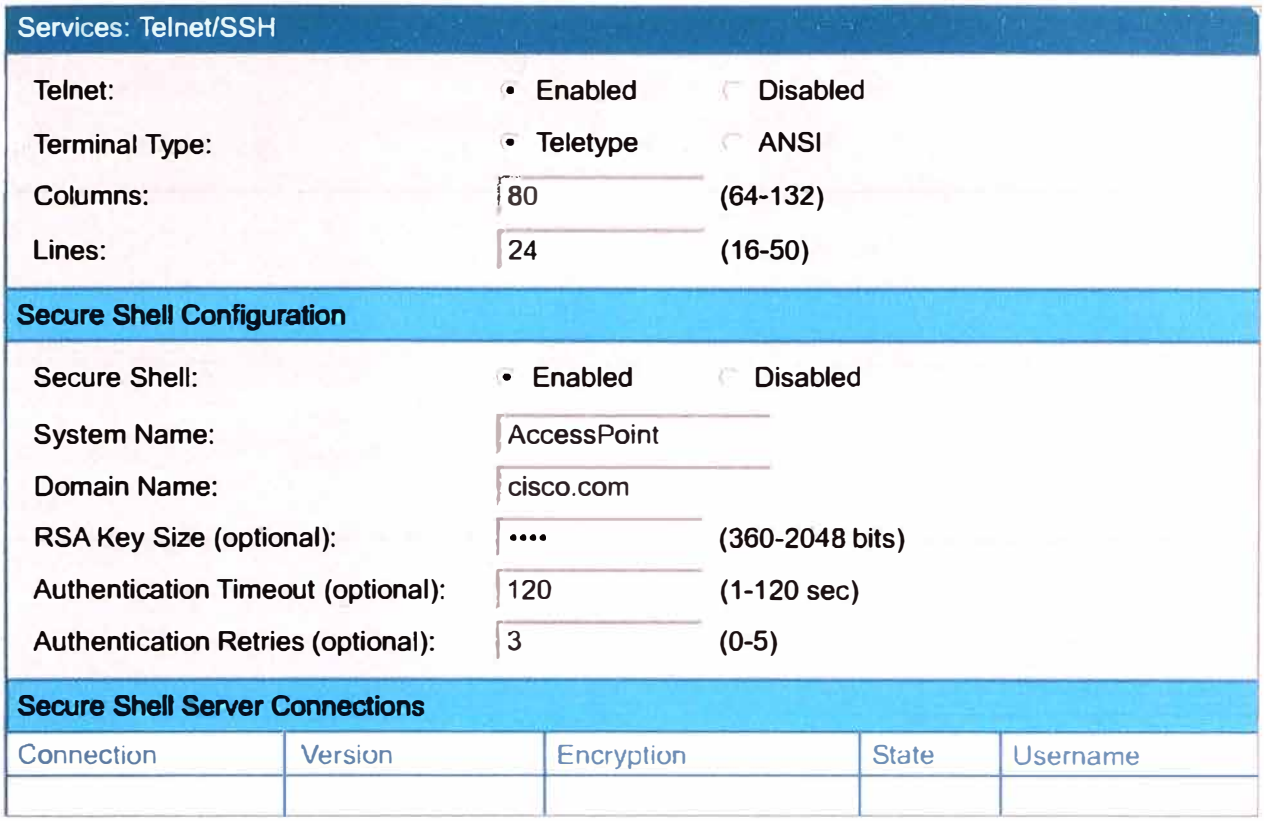

Figura 2.14 Servicios Telnet y SSH

a.5 TFTP/FTP

El Protocolo de Transferencia Trivial de Archivos (TFTP) y el Protocolo de Transferencia de Archivos (FTP) son usados para enviar y recibir archivos a través de una red. TFTP no permite que se utilicen passwords, y está limitado a archivos menores a 16 Mb. FTP permite nombres de usuario y passwords, pero aun es un protocolo no encriptado.

a.6 SSID

Como se mencionó antes, el SSID no debería ser considerado como una característica de seguridad. Los SSIDs pueden ser usados en conjunto con las VLANs para permitir el acceso limitado a invitados.

b.- Seguridad en clientes y APs

La seguridad del cliente es importante, porque asegurando simplemente a los access points no se protege a una red inalámbrica. Después de que estén protegidas las debilidades de los access points, el ataque a los clientes se convierte en la forma más fácil de obtener acceso a la red.

La seguridad apropiada para los clientes debería ser especificada en la política de seguridad inalámbrica. Esto incluye medidas de seguridad como búsqueda de virus, firewalls personales y mantener a los programas clientes y a los sistemas operativos actualizados.

Puede ser deseable el tener seguridad adicional para clientes inalámbricos. Por

ejemplo, WEP debería ser activado cuando sea posible. Como se dijo antes, la WEP estática tiene debilidades. Características de seguridad adicionales, como la clave por paquete de protocolo de integridad de clave temporal (TKIP) y el Control de Integridad de Mensajes (MIC), necesitan estar activas para la seguridad adicional.

Además de los clientes, los APs y los bridges deben ser asegurados usando WEP. No importa el tipo de autenticación que se esté usando, las claves WEP ingresadas en el cliente y en el access point deben coincidir. Las claves mismas deben coincidir, y el orden de las claves debe coincidir. Por ejemplo, una clave de 40 bits ingresada como Clave 1 en el cliente debe coincidir con la clave de 40 bits ingresada como Clave 1 en el access point.

c. Supervisión del equipo WLAN

El registro de eventos a través de SNMP o Syslog es muy importante en el proceso de seguridad general. CÓmo se muestra en la Figura 2.15, los niveles de notificación de eventos pueden ser definidos para SNMP y Syslog. Debe estar definido un servidor Syslog para que se puedan enviar mensajes Syslog a un servidor de supervisión central.

Event Log : Configuration Options

Disposition of Events (by Severity Level):

	Display on Event Log	Notify via SNMP/Syslog Trap	Record for SNMP/Syslog History Table	Displayon Telnet/SSH Monitor
Emergency	☑ Display	☑ Notify	☑ Record	☑ Monitor
Alert	☑ Display	☑ Notify	☑ Record	☑ Monitor
Critical	☑ Display	☑ Notify	☑ Record	☑ Monitor
Error	☑ Display	☑ Notify	☑ Record	☑ Monitor
Warning	☑ Display	☑ Notify	☑ Record	☑ Monitor
Notification	☑ Display	☑ Notify	☑ Record	☑ Monitor
Information	☑ Display	☑ Notify	☑ Record	☑ Monitor
Debugging	☑ Display	☐ Notify	☑ Record	☑ Monitor

Time Stamp Format for Future Events: • System Uptime ○ Global Standard Time ○ Local Time

Event Log Size: 4 (4-2147483) kilobytes

History Table Size: 1 (0-500) Messages

Figura 2.15 Visor de eventos SNMP

SNMP permite que los programas de administración de red vean y cambien configuraciones de equipos. SNMP puede ser usado para ver configuraciones usando un pedido Get. SNMP también puede ser usado para cambiar las configuraciones usando un pedido Set. Finalmente, los dispositivos SNMP pueden enviar alertas a las estaciones de administración usando la función Trap.

SNMP utiliza un secreto no encriptado llamado cadena o nombre de comunidad. Los nombres de comunidad de sólo lectura sólo permiten pedidos Get, mientras que los nombres de comunidad de lectura y escritura permiten pedidos Get y Set. Las versiones 1 y 2 de SNMP son inseguras, porque el nombre de comunidad puede ser visto en los pedidos.

La versión 3 de SNMP agrega seguridad adecuada, pero aun no está ampliamente usada o soportada. Nunca utilice public o private como nombres de comunidad porque son los predeterminados. Utilice un nombre de comunidad que cumpla con las pautas de passwords seguras.

d. Desactivación de servicios no necesarios

Es importante desactivar o asegurar todos los servicios no necesarios. Por ejemplo, si el protocolo de descubrimiento de Cisco (CDP) , el servicio de nombre de dominio (DNS), el protocolo de tiempo de la red (NTP) , el protocolo de transferencia de hipertexto (HTTP) , TFTP, SNMP y Telnet no son usados en la red, deberían ser desactivados

El uso de HTTP/Administración Web es útil, pero si se usa sobre el equipo de la red puede debilitar la seguridad de la red. Muchos fabricantes tienen serios problemas en su software de servidor Web. Para una máxima seguridad, HTTP deberá estar desactivado en una red de producción. Si se utiliza HTTP, deberá estar protegido con una password. Si la vulnerabilidad está publicada, deberá consultarse a asesores de seguridad del fabricante y se deberá aplicar nuevo firmware.

A menos que sean necesarios, TFTP y FTP no deberían estar activados. Algunos fabricantes usan esquemas TFTP muy débiles, lo que permite que el archivo de configuración sea bajado por cualquier usuario. Como el archivo de configuración contiene passwords y claves WEP, la seguridad puede estar comprometida.

2.3.4 Autenticación WLAN Empresarial

Se ven los siguientes temas.

a. Autenticación de segunda generación

b. Autenticación de usuarios inalámbricos

c. Fundamentos de 802.1x

d. Cómo funciona 802.1x

e. Tipos de autenticación de 802.1x

a. Autenticación de segunda generación

Los diseñadores de red y los expertos en seguridad saben que no es suficiente arreglar las debilidades de WEP. La Figura muestra algunos de los requisitos y soluciones para asegurar las WLANs. La verdadera seguridad inalámbrica requiere más que sólo hacer dinámicas las claves WEP o mejorar el WEP. La verdadera seguridad

inalámbrica debe poder autenticar a los usuarios, no sólo a los dispositivos.

Las organizaciones deben decidir cuánta seguridad necesitan e incluirla en la política de seguridad inalámbrica. Algunas redes dependerán de soluciones VNP existentes para proporcionar seguridad adicional.

Otras redes implementarán el control de acceso y los arreglos para WEP, que están incluidos en el Acceso Protegido Wi-Fi (WPA). WPA utiliza elementos de 802.11i, una solución de seguridad estandarizada de más largo plazo, para asegurar las WLANs. WPA también es llamado Networking de Seguridad Simple (SSN). Algunos administradores de red pueden decidir esperar al 802.11i antes de desarrollar las WLANs. Las secciones siguientes hablarán sobre lo que está mal en la seguridad WEP y qué está faltando.

b. Autenticación de usuarios inalámbricos

Una severa limitación de una WLAN con sólo WEP es que los usuarios no se autentican. WPA permite la autenticación de usuarios a través del protocolo IEEE 802.1x. 802.1x es un estándar terminado recientemente para controlar la entrada a las LANs cableadas e inalámbricas. 802.1x proporciona autenticación mutua. La autenticación mutua significa que la red y el usuario se intercambian las identidades, como se indica

1. Autenticación

Basada en dispositivo, no basada en usuario

Cliente no autentica red

2. Manejo de claves

Estáticas

Compartidas entre dispositivos y APs

Si el adaptador o dispositivo es robado, se deben cambiar las claves

3. Llaves RC4 basadas eb WEP

Algoritmo de encriptamiento es vulnerable a ataque

La integridad del mensaje no está asegurada

El estándar 802.11i también utiliza 802.1x y las mejoras TKIP para WEP. Una ventaja del estándar 802.1x es que puede soportar una variedad de tipos de autenticación. Un access point que soporta 802.1x y a su protocolo, el Protocolo de Autenticación Extensible (EAP), actúa como la interfaz entre un cliente inalámbrico y un servidor de autenticación como el RADIUS o servidor de Servicio al Usuario de Acceso Telefónico Remoto. El access point se comunica con el servidor RADIUS a través de la red cableada.

c. Fundamentos de 802.1x

802.1x requiere soporte en el cliente, en el access point y en el servidor de autenticación, cómo lo ilustra la Figura 2.16, 802.1X utiliza un proxy RADIUS para

autenticar a los clientes en la red. Este dispositivo proxy podría ser un switch o un access point. Este dispositivo trabaja en la capa de acceso.

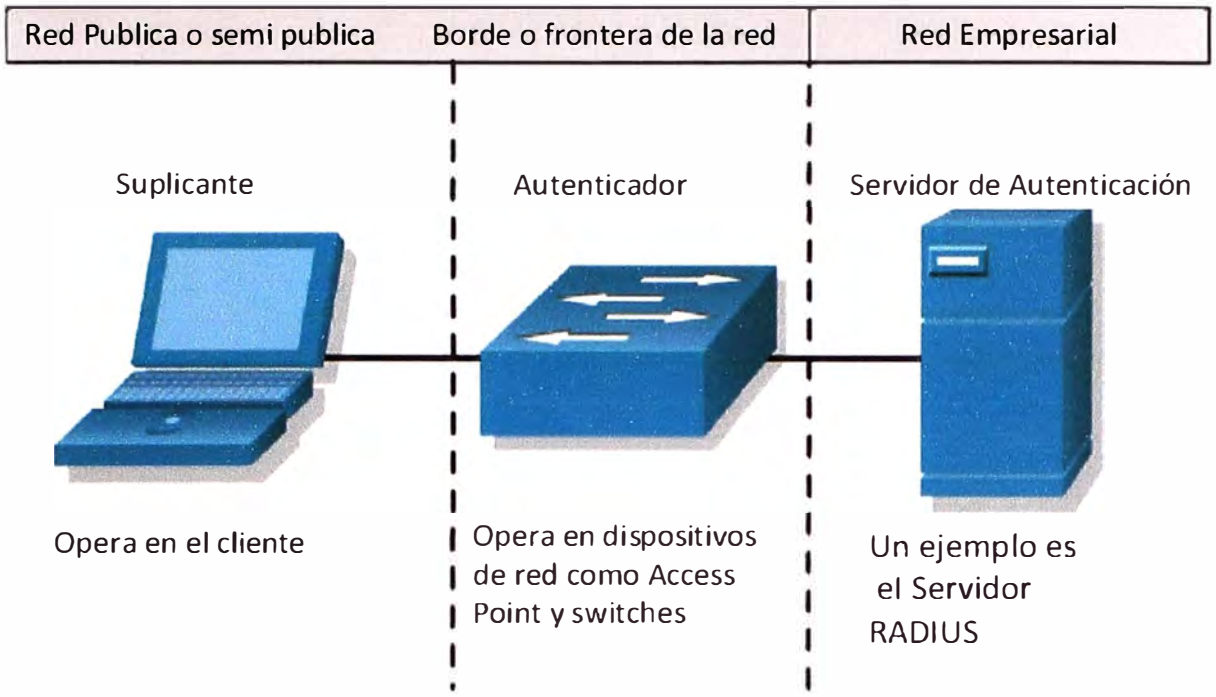

Figura 2.16 Suplicante, autenticador y servidor

El cliente o solicitante EAP envía las credenciales de autenticación al autenticador el que a su vez envía la información al servidor de autenticación, donde el pedido de ingreso es comparado con una base de datos de usuarios para determinar si el usuario puede obtener acceso a los recursos de la red, y a qué nivel. El access point recibe el nombre de autenticador.

El servidor de autenticación es normalmente un RADIUS o un servidor de autenticación, autorización y contabilidad (AAA). El servidor de autenticación necesita ejecutar un software extra para comprender el tipo de autenticación que está usando el cliente.

d. Cómo funciona 802.1x

La Figura 2.17 proporciona una descripción general de la forma en que trabaja el 802.1x. Después de que el cliente se ha asociado al access point, el solicitante comienza el proceso para usar EAPOL (EAP sobre LAN) pidiéndole al usuario su nombre y password.

El cliente responde con su nombre de usuario y password. Usando 802.1X y EAP el solicitante luego envía el nombre de usuario y un hash de un sentido de la password al access point. El access point luego encapsula el pedido y lo envía al servidor RADIUS.

El servidor RADIUS luego compara el nombre de usuario y la password con la base de datos para determinar si el cliente debería ser autenticado en la red. Si el cliente debe ser autenticado, el servidor RADIUS emite luego un desafío de acceso, que es pasado al

access point y después enviado al cliente.

El cliente envía la respuesta EAP para el desafío de acceso al servidor RADIUS a través del access point. Si el cliente envía la respuesta correcta entonces el servidor RADIUS envía un mensaje de acceso exitoso y una clave WEP (EAP sobre Inalámbrico) al cliente a través del access point.

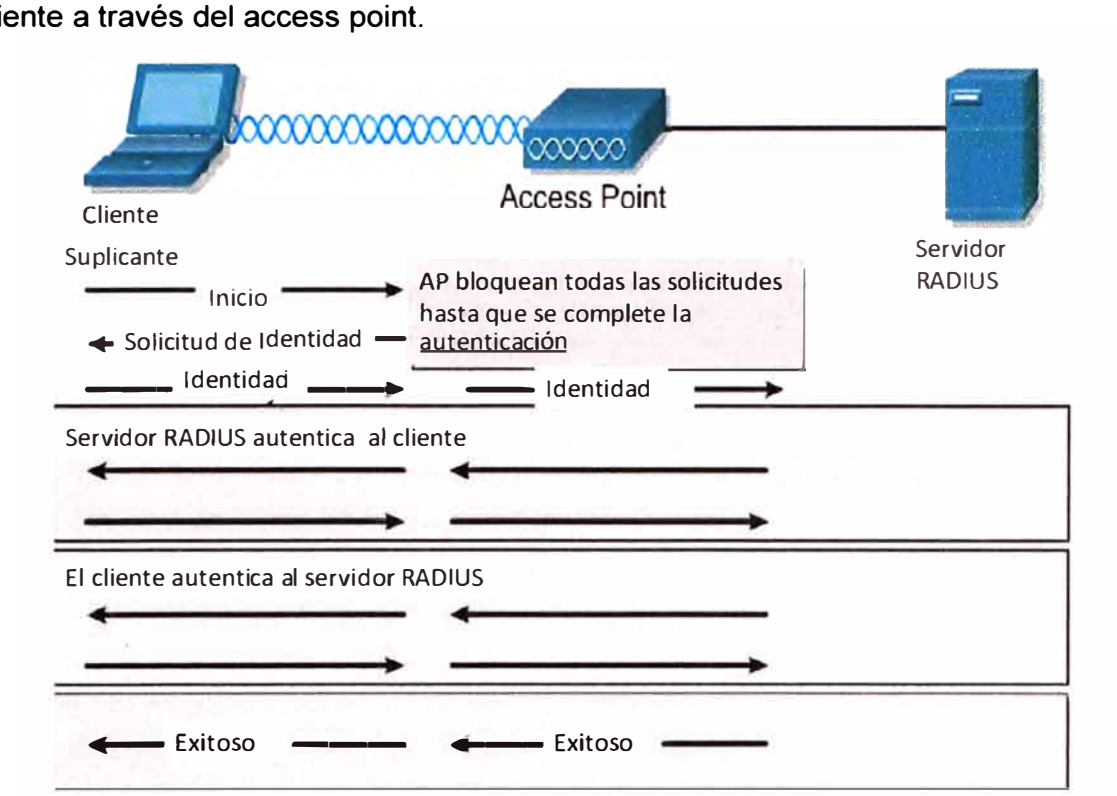

Figura 2.17 Forma de trabajo del 802.1X

La misma clave WEP de sesión también es enviada al access point en un paquete exitoso. El cliente y el access point luego comienzan a usar las claves WEP de sesión. La clave WEP usada para multicast es luego enviada desde el access point hacia el cliente. Es encriptada usando la clave WEP de sesión. Ante la desconexión del cliente, el access point vuelve al estado inicial, permitiendo que sólo pase tráfico 802.1X.

e. Tipos de autenticación de 802.1x

Cuando se utiliza 802.1x sobre una WLAN están soportados diferentes tipos de autenticaciones.

1.- LEAP - EAP Liviano, es también llamado EAP-Cisco. LEAP es la versión de Cisco de EAP. Es para usar sobre redes que actualmente no soportan EAP. Las versiones actuales de EAP pueden no proporcionar la funcionalidad que se necesita y pueden ser demasiado exigentes.

Esto podría comprometer el rendimiento del equipo WLAN. LEAP es una buena opción cuando se utiliza equipo Cisco junto con sistemas operativos como Windows 95, Windows 98, Windows Me, Windows CE, Windows NT/2000/XP y Linux.

2.- EAP-TLS - La EAP-Seguridad de Capa de Transporte [EAP-Transport Layer Security

(EAP-TLS)] es una opción de seguridad de trabajo intensivo. EAP-TLS requiere que haya un certificado digital configurado en todos los Clientes WLAN y en el Servidor. EAP-TLS está basado en certificados X.509. Normalmente es más fácil de usar que PEAP, que está basado en EAP-TLS.

3.- PEAP - EAP Protegido [Protected EAP (PEAP)] es un tipo de autenticación EAP borrador que está diseñado para permitir la autenticación híbrida. PEAP emplea la autenticación PKI del lado del servidor. Para la autenticación del lado del cliente, PEAP puede usar cualquier otro tipo de autenticación EAP. Como PEAP establece un túnel seguro por medio de la autenticación del lado del servidor, se pueden usar tipos de EAP no mutuamente autenticables para la autenticación del lado del cliente.

Las opciones de autenticación del lado del cliente incluyen EAP-GTC para passwords ocasionales y EAP MD5 para autenticación basada en password. PEAP está basado en EAP-TLS del lado del servidor y soluciona los defectos de administrabilidad y escalabilidad de EAPTLS. Las organizaciones pueden evitar los problemas relacionados con la instalación de certificados

digitales en cada máquina cliente como lo requiere EAP-TLS. Ellas pueden luego seleccionar el método de autenticación del cliente que mejor les convenga.

4.- EAP-MD5 - El Protocolo de Autenticación Expandible MD5 [Extensible Authentication Protocol MD5 (EAP-MD5)] no debería ser usado, porque no proporciona autenticación mutua. EAP-MD5 es una autenticación de un sentido que esencialmente duplica la protección de password CHAP en una WLAN. EAP-MD5 se utiliza como un bloque de construcción en EAP-TTLS.

5.- EAP-OTP - EAP-Passwords Ocasionales [EAP-One Time Passwords (EAP-OTP)] también recibe el nombre de EAP-Tarjeta Token Genérica [EAP- Generic Token Card (EAP-GTC)]. No es recomendable, ya que las OTPs no son una forma de autenticación mutua.

6.- EAP-SIM - EAP-SIM utiliza la misma tarjeta inteligente o SIM que se utiliza en los teléfonos móviles GSM para proporcionar autenticación. EAP-SIM puede fácilmente montarse sobre EAP-TLS.

7.- EAP-TTLS - EAP-Seguridad de Capa de Transporte en Túnel [EAP-Tunneled Transport Layer Security (EAP-TTLS)] es un borrador IETF creado por Funk software y Certicom. EAP-TTLS provee una funcionalidad similar a PEAP. EAP-TTLS protege las passwords usando TLS, que es una forma avanzada de Capa de Socket Seguro [Secure Socket Layer (SSL)]. EAP-TTLS actualmente requiere un servidor RADIUS de Funk software.

8.- Kerberos - Kerberos no es parte del estándar 802.1x, sino que está siendo

promocionado por algunos fabricantes. Kerberos es un sistema de autenticación que permite la comunicación protegida sobre una red abierta, que utiliza una clave única llamada ticket. Requiere configuración del servicio. PEAP puede soportar Kerberos a través del EAP-Servicio de Seguridad Genérico [EAP-Generic Security Service (EAP-GSS)].

2.3.5 Encriptación Inalámbrica Empresarial

Se verá lo siguiente:

a. Fortalecimiento WEP.

b. Control de la integridad de los mensajes.

c. Rotación de clave de broadcast [Broadcast key rotation (BKR)].

d. Encriptación de segunda generación.

e. Uso de VPNs.

a. Fortalecimiento WEP

WPA incluye mecanismos del estándar emergente 802.11i para mejorar la encriptación de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente. Estas tecnologías son fácilmente implementadas usando la interfaz gráfica de usuario (GUI) del AP de Cisco.

TKIP es también llamado hashing de Clave WEP y recibió inicialmente el nombre WEP2. TKIP es una solución temporal que soluciona el problema de reutilización de clave de WEP. WEP utiliza periódicamente la misma clave para encriptar los datos.

El proceso de TKIP comienza con una clave temporal de 128 bits que es compartida entre los clientes y los access points. TKIP combina la clave temporal con la dirección MAC del cliente. Luego agrega un vector de inicialización relativamente largo, de 16 octetos, para producir la clave que encriptará a los datos.

Este procedimiento asegura que cada estación utilice diferentes streams claves para encriptar los datos. El hashing de clave WEP protege a los Vectores de Inicialización (IVs) débiles para que no sean expuestos haciendo hashing del IV por cada paquete.

TKIP utiliza el RC4 para realizar la encriptación, que es lo mismo que el WEP. Sin embargo, una gran diferencia con el WEP es que el TKIP cambia las claves temporales cada 10.000 paquetes. Esto proporciona un método de distribución dinámico, lo que mejora significativamente la seguridad de la red. Una ventaja de usar TKIP es que las compañías que tienen access points basados en WEP y NICs de radio pueden actualizarse a TKIP a través de patches de firmware relativamente simples. Además, el equipo sólo WEP aún interoperará con los dispositivos con TKIP activado usando WEP. TKIP es sólo una solución temporal. La mayoría de los expertos creen que aun es necesaria una encriptación más fuerte.

b. Control de la integridad de los mensajes

Las mejoras de TKIP, como MIC, proveen claves WEP más fuertes. MIC evita los ataques de bit-flip en paquetes encriptados. Durante un ataque bit-flip, un intruso intercepta un mensaje encriptado, lo altera levemente y lo retransmite.

El receptor acepta el mensaje retransmitido como legítimo. El controlador y el firmware del adaptador cliente deben soportar la funcionalidad del MIC, y MIC debe estar activo en el access point. Las mejoras de TKIP, como MIC y hashing de Clave WEP pueden ser activados usando claves WEP estáticas. No necesitan un servidor RADIUS para funcionar.

c. BKR, Rotación de clave de broadcast

La característica Rotación de Clave de Broadcast (BKR), descripta en la Figura , es también una mejora de TKIP. BKR protege al tráfico multicast del access point para que no sea explotado cambiando dinámicamente la clave de encriptación. El access point genera claves WEP de broadcast usando un generador de números pseudo aleatorios (PRNG) sembrados.

El Access point rota la clave de broadcast después de que se agota un temporizador configurado de clave WEP de broadcast. Este proceso por lo general debería estar en sincronía con los tiempos vencidos configurados en los servidores RADIUS para la re-autenticación de los usuarios.

La rotación de clave de broadcast es una excelente alternativa al hashing de clave WEP. Esto es cierto si la WLAN soporta dispositivos clientes inalámbricos que no son dispositivos Cisco o que no pueden ser actualizados con el último firmware para dispositivos clientes de Cisco.

Se recomienda que la rotación de clave de broadcast esté activa cuando el access point sirve a una LAN inalámbrica exclusiva de 802.1x. No es necesario activar la rotación de clave de broadcast si el hashing de clave WEP está activado. El uso de la rotación de clave y de hashing de clave provee de protección innecesaria. Cuando la rotación de clave de broadcast está activada, sólo pueden usar el access point los dispositivos clientes inalámbricos que usan autenticación LEAP o EAP-TLS.

Los dispositivos clientes que usan WEP estática con clave abierta compartida o autenticación EAP-MD5 no pueden usar el access point cuando la rotación de clave de broadcast está activada.

d. Encriptación de segunda generación

Además de la solución TKIP, el estándar 802.11i es muy probable que incluya al protocolo Estándar Avanzado de Encriptación (AES), como muestra la. AES ofrece una encriptación mucho más fuerte. En efecto, el Instituto Nacional de Estándares y

Tecnología (NIST) del Departamento de Comercio de los EE.UU. eligió al AES para reemplazar el DES obsoleto. El AES es ahora un Estándar de Procesamiento de Información Federal (FIPS) de los EE. UU., Publicación 197. Define un algoritmo criptográfico para ser usado por las organizaciones gubernamentales de los EE.UU. para proteger la información delicada no clasificada.

La Secretaría de Comercio aprobó la adopción del AES como un estándar oficial del Gobierno en mayo del 2002. Sin embargo, está el problema de que AES requiere un coprocesador o un hardware adicional para funcionar.

Esto significa que las compañías necesitan reemplazar los access points y las NICs clientes existentes para implementar AES. Basado en reportes de marketing, la base instalada actualmente es relativamente pequeña comparada con el desarrollo futuro predicho. Como resultado, habrá un porcentaje muy alto de nuevas implementaciones de WLAN que tomarán ventaja del AES cuando sea parte del 802.11. Por otra parte, las compañías que ya han instalado las WLANs necesitarán determinar si vale la pena los costos de actualizar para una mejor seguridad.

AES especifica tres tamaños de claves, que son 128, 192 y 256 bits. Utiliza el Algoritmo Rijndael. Si alguien fuera a construir una máquina que pudiera recuperar una clave DES en un segundo, entonces el penetrar una clave AES de 128 bits le tomaría a esa máquina aproximadamente 149 billones de años. Para ponerlo en perspectiva, se cree que el universo tiene menos de 20 mil millones de años de edad.

e. Uso de VPNs

La Seguridad IP (IPSec) es un marco de trabajo de estándares abiertos para asegurar la comunicación privada segura sobre redes IPs.

Las Redes Privadas Virtuales (VPNs) IPSec utilizan los servicios definidos dentro de IPSec para asegurar la confidencialidad, la integridad y la autenticidad de las comunicaciones de datos a través de redes como la Internet. IPSec también tiene una aplicación práctica para asegurar las WLANs. Logra esto superponiendo IPSec por sobre el tráfico inalámbrico de 802.11.

Cuando se implementa IPSec en un entorno WLAN, se coloca un cliente IPSec en cada PC conectada a la red inalámbrica. Se necesita que el usuario establezca un túnel IPSec y que enrute todo el tráfico hacia la red cableada.

Se colocan filtros para evitar que el tráfico inalámbrico llegue a cualquier destino que no sea el concentrador VPN y el servidor DHCP/DNS. Ver Figura 2.18.

Los clientes VPN también pueden ser terminados sobre un router IOS Firewall o un Aparato de Seguridad PIX. IPSec proporciona confidencialidad al tráfico IP. También tiene capacidades de autenticación y antirespuesta usando el Resumen de Mensajes 5

(MD5) o el Algoritmo Hash Seguro (SHA).

La confidencialidad se logra a través de la encriptación, que utiliza el Estándar de Encriptación de Datos [Data Encryption Standard (DES)], el Triple DES (3DES) o el AES.

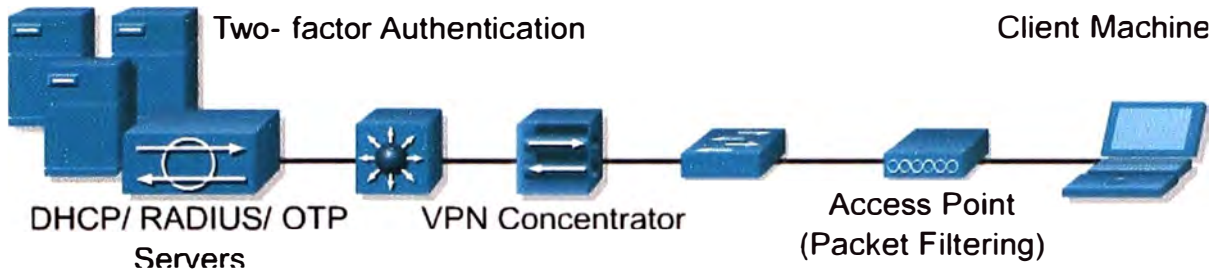

Figura 2.18 Implementación del VPN

El filtrado puede proporcionar una capa adicional de seguridad inalámbrica. Los filtros pueden ser creados para filtrar un Protocolo o un puerto IP. Cuando un access point está diseñado para utilizarse sólo en VPN, se pueden usar filtros

2.3.6 Otros servicios de seguridad empresariales

Se tratarán los siguientes temas:

a. Redes vistuales de área local, VLANs

b. Spanning tree

a. VLANs

Una red de área local virtual (VLAN) es una red conmutada que está segmentada en forma lógica por funciones, equipos de proyectos o aplicaciones en lugar de estarlo en forma física o geográfica. Por ejemplo, todas las estaciones de trabajo y los servidores usados por un grupo de trabajo en particular puede estar conectado a la misma VLAN, sin importar sus conexiones físicas a la red o el hecho de que puedan estar entremezclados con otros equipos. Usted utiliza VLANs para reconfigurar la red a través de software en lugar de hacerlo físicamente desconectando y moviendo dispositivos o cables.

Una VLAN puede imaginarse como un dominio de broadcast que existe dentro de un conjunto definido de switches. Una VLAN consiste en una cantidad de sistemas terminales, hosts o equipos de red (como bridges y routers), conectados por un único dominio de bridging. El dominio de bridging está soportado en varios equipos de red como switches LAN que ejecutan protocolos de bridging entre ellos con un grupo separado para cada VLAN.

Las VLANs proporcionan los servicios de segmentación tradicionalmente proporcionados por los routers en las configuraciones LAN. Las VLANs dirigen la escalabilidad, la seguridad y la administración de la red. Se debe considerar varios problemas claves cuando se diseña y construye redes LAN conmutadas:

1. Segmentación de la LAN

2. Seguridad
3. Control de broadcast
4. Rendimiento
5. Administración de la red
6. Comunicación entre VLANs

Las LANs se pueden utilizar en algunos equipos inalámbricos para separar el tráfico, como lo muestran la Figura 2.20. Esto puede ser útil para separar clientes WEP básicos en una VLAN de los usuarios que no están usando ninguna encriptación. Cuando están correctamente configuradas, las VLANs son seguras.

El tráfico de una VLAN no puede atravesar otra VLAN. Los SSIDs pueden utilizarse junto con las VLANs para permitir un acceso limitado a los invitados. Las VLANs pueden ser creadas usando la página de configuración de Servicios VLAN

b. Spanning tree

El Spanning tree es sólo necesario cuando se utilizan bridges inalámbricos. Debería permanecer desactivado para los access points y los repetidores, a menos que existan circunstancias especiales en la red. El algoritmo de Spanning Tree se utiliza para evitar bucles de bridging. El algoritmo computa las rutas de red disponibles y cierra las rutas redundantes, para que sólo haya una ruta entre cualquier par de LANs en la red.

Una configuración de spanning tree incorrecta puede desactivar conexiones necesarias. Desde una perspectiva de seguridad, un atacante podría desactivar puertos en una red configurada pobremente. Por favor revise y comprenda la información de spanning tree cuando tome decisiones de configuración.

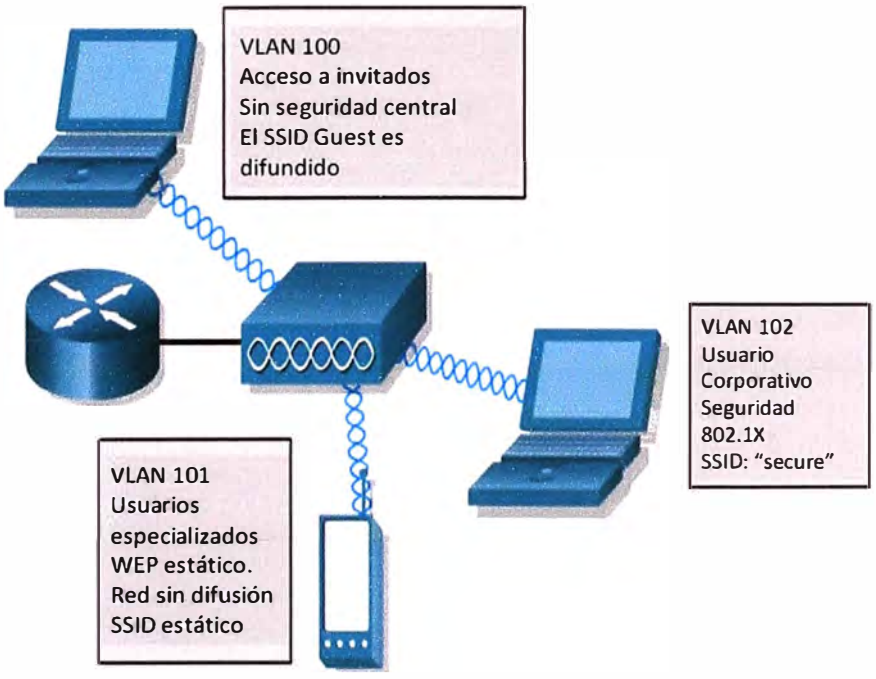

Figura 2.20 Uso de equipos inalámbricos para separación del tráfico

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

En el presente capítulo se describe la ingeniería del proyecto y las opciones tecnológicas para dar solución al problema. Se verán los siguientes aspectos

1. Dimensionamiento de la solución
2. Estudio del sitio
3. Propuesta de diseño
4. Equipamiento

3.1 Dimensionamiento de la solución

El proyecto consiste en la implementación, diseño y configuración de un sistema completo de comunicación inalámbrica para las instalaciones de la BVL, dicho sistema estará compuesto por 12 APs distribuidos de tal manera que se asegure una calidad de servicio optima para los usuarios y visitantes (11Mbps de tasa de transferencia de datos).

Para la evaluación y diseño del sistema de comunicación inalámbrico, se realizaron los estudios de campo necesarios para verificar la factibilidad del mismo, dando esta como resultado la cantidad necesaria de equipamiento a utilizar para brindar un servicio de interconexión optima.

3.2 Estudio del sitio

Antes de instalar los APs del sistema inalámbrico a implementar se deberá realizar el estudio de sitio, esto ayuda a establecer cuantos APs serán necesarios en todas las instalaciones para proporcionar la cobertura deseada, así cómo la ubicación de los APs y precisar la información necesaria para la instalación.

El estudio de sitio también determinará la factibilidad de la cobertura deseada ante obstáculos como limitaciones de la conectividad cableada y requisitos de las aplicaciones. Esto permitirá que la red de área local inalámbrica (WLAN) sea instalada correctamente y que se tenga un acceso inalámbrico consistente y seguro.

3.2.1 Consideraciones

Se tuvieron las siguientes consideraciones: a) Velocidad de datos, b) Tipo y Ubicación del AP, c) Entornos Físicos, d) Obstrucciones, e) Materiales de construcción.

a. Velocidad de datos

La sensibilidad y el alcance son inversamente proporcionales a la velocidad de los

bits de datos. El alcance máximo de la radio se consigue a la velocidad de datos mas baja viable.

b. Tipo y Ubicación del AP

La correcta configuración y ubicación del AP es un factor crítico en la maximización del alcance de la radio.

c. Entornos Físicos

Las áreas limpias o despejadas proporcionan un alcance de radio mejor que las áreas cerradas o llenas.

d. Obstrucciones

Una obstrucción física como una estantería o un pilar puede dificultar el rendimiento del AP. Se evita colocar el dispositivo de cómputo y el AP en una ubicación donde haya una barrera entre las antenas emisora y receptora.

e. Materiales de construcción

La penetración de la radio es influenciada enormemente por el material de construcción usado. Por ejemplo, la construcción de mampostería permite un alcance mayor que los bloques de concreto.

3.2.2 Planeamiento y simulación

Dado que el propósito de optimizar la red inalámbrica, proveyendo flexibilidad al desplazamiento a los usuarios y seguridad a la red, requiere de un controlador que administre los APs, se opta por buscar en el medio un software que pueda asistir en el planeamiento de la red inalámbrica simulando los patrones de cobertura. Este es el WCS (Cisco Wireless Control System)

La Figura 3.1 muestra una pantalla del WCS en donde se hace el planeamiento y diseño simplificado de LAN inalámbricas.

Las herramientas de planificación y diseño Cisco WCS simplifican el proceso de definición de punto de acceso y la determinación de áreas de cobertura de punto de acceso para los edificios de formas irregular y estándar.

Esta herramienta ayuda a los administradores a visualizar el ambiente ideal de RF, anticipándose a las necesidades de cobertura futuros y evaluar los eventos de LAN inalámbricos. Ayuda a los administradores de TI a reducir y eliminar, impropios diseños de RF y los problemas de cobertura que pueden conducir a tickets de problemas para el usuario final. Un ejemplo de ello puede verse en la Figura 3.2

3.2.3 Distribución

Los planos obtenidos de la ubicación de los APs en los distintos niveles se presentan a continuación. La Figura 3.3 corresponde al sótano, La Figura 3.4 a la mezzanine, la Figura 3.5 al tercer piso y la Figura 3.6 Plano Segundo Piso.

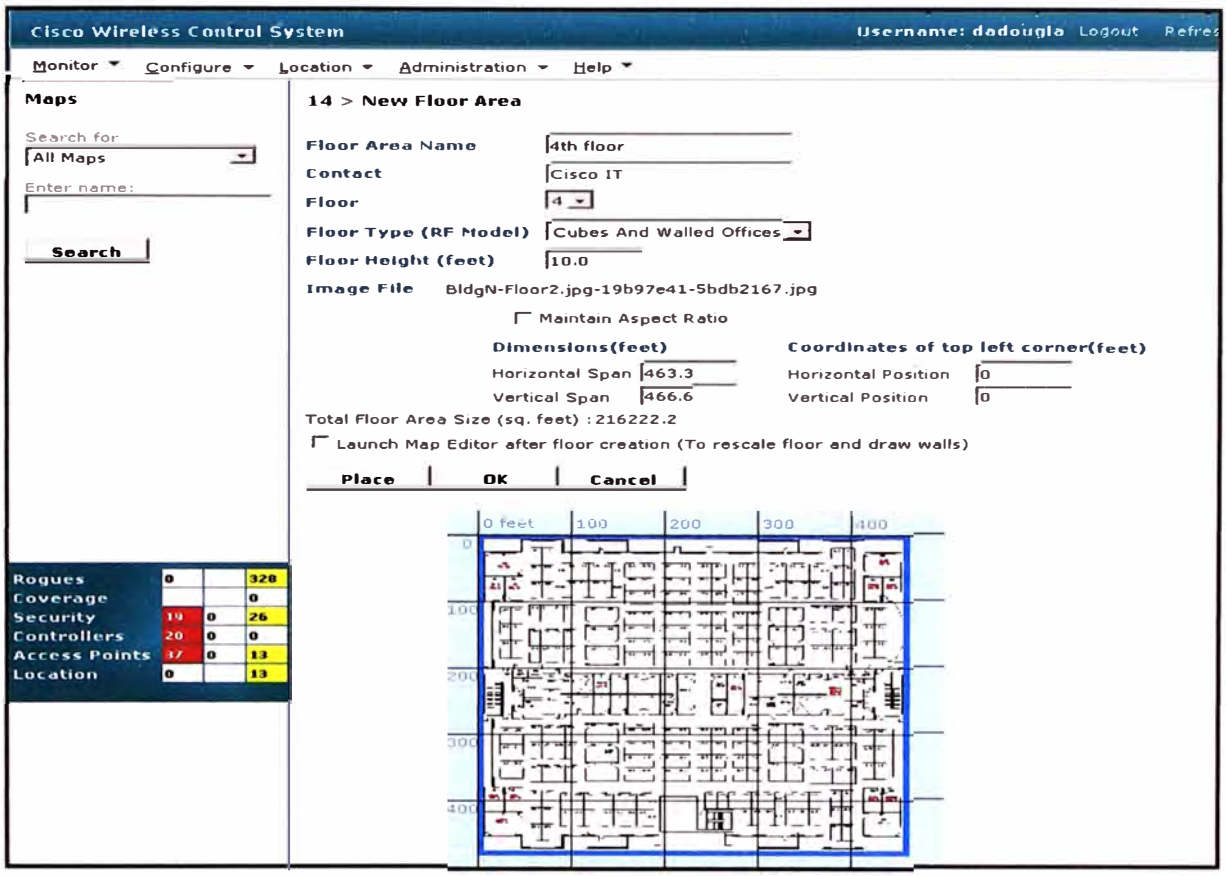

Figura 3.1 Planeamiento y Diseño Simplificado de LAN inalámbricas

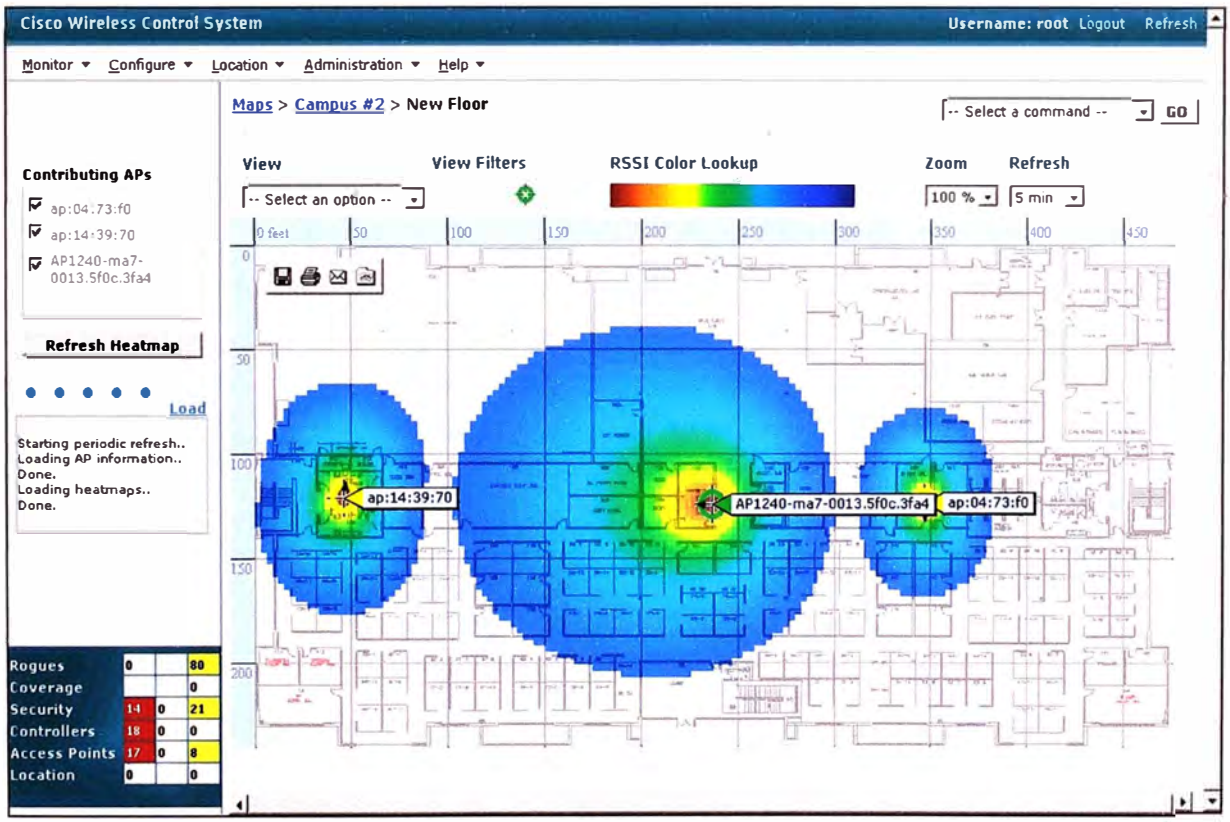

Figura 3.2. Visualización RF

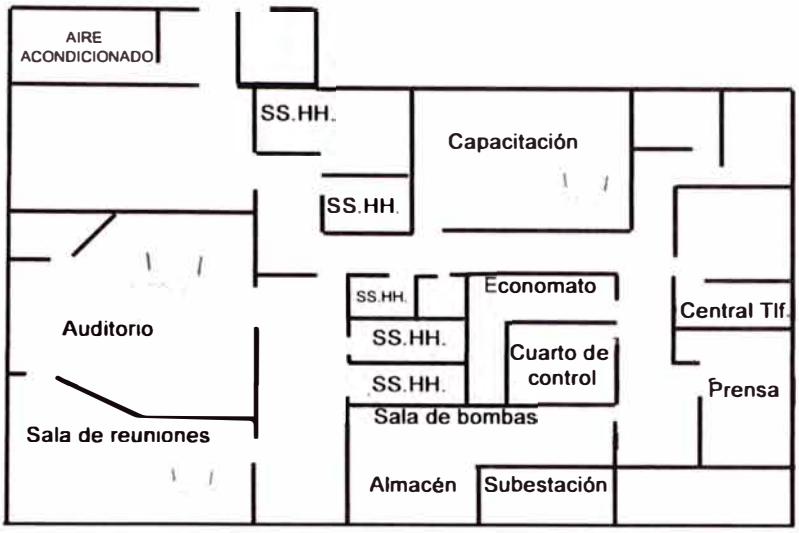

Figura 3.3 Plano sótano

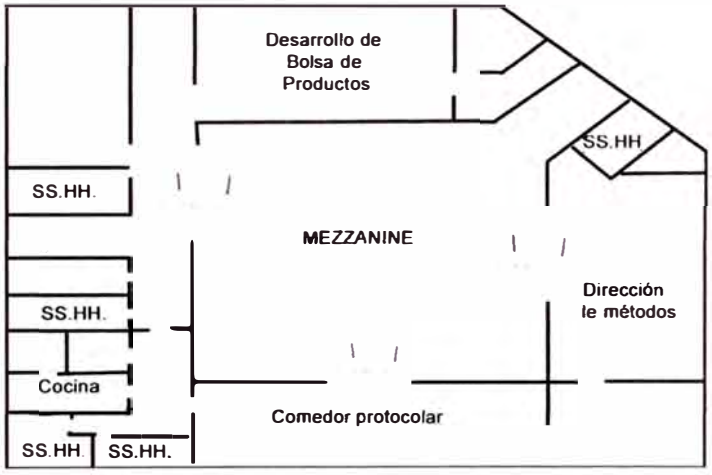

Figura 3.4 Plano Mezzanine

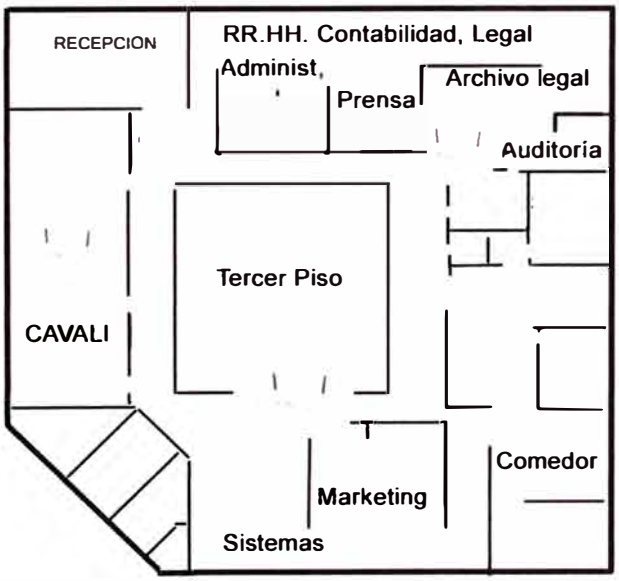

Figura 3.5 Plano Tercer Piso

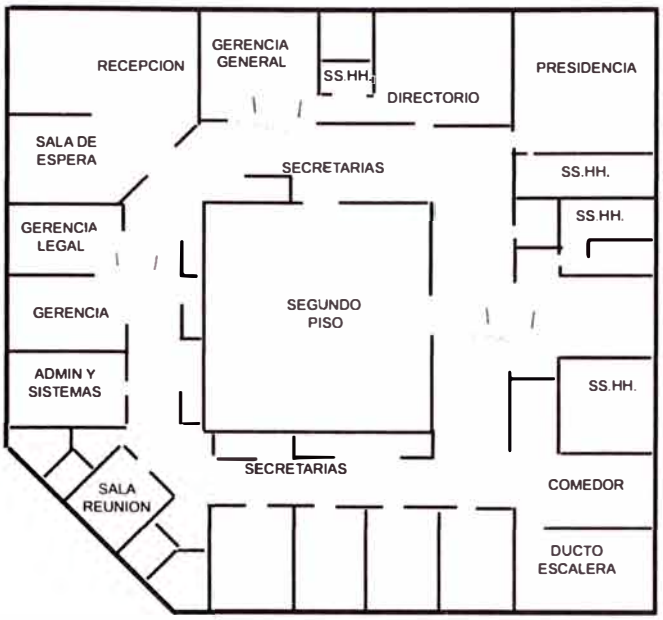

Figura 3.6 Plano Segundo Piso

3.2.4 Topología

Al igual que con las redes cableadas, se debe considerar que la topología de las WLANs puede tomar muchas formas, cómo se puede ver en la Figura 3.7.

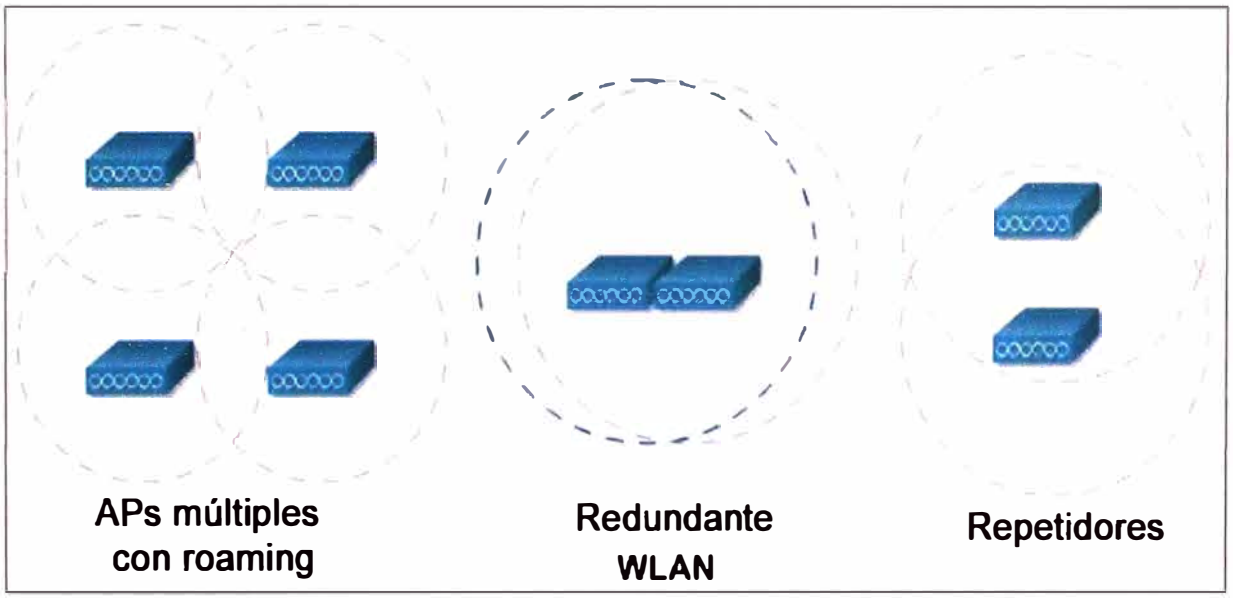

Figura 3.7 Diversas topologías inalámbricas

Con respecto a una WLAN, el termino topología no hace referencia a las arquitecturas como bus o anillo. En realidad hace referencia al Área de Servicio Básico (BSA) que esta compuesta por micro células. Cada AP tiene un área de cobertura llamada micro célula o célula. La topología que se usará en la presente implementación es la mostrada en la Figura 3.8.

3.3 Propuesta de diseño

En la Figura 3.9 se muestra el diseño de la solución propuesta para la BVL mediante el uso de 2 controladores Cisco y 12 APs también del mismo fabricante.

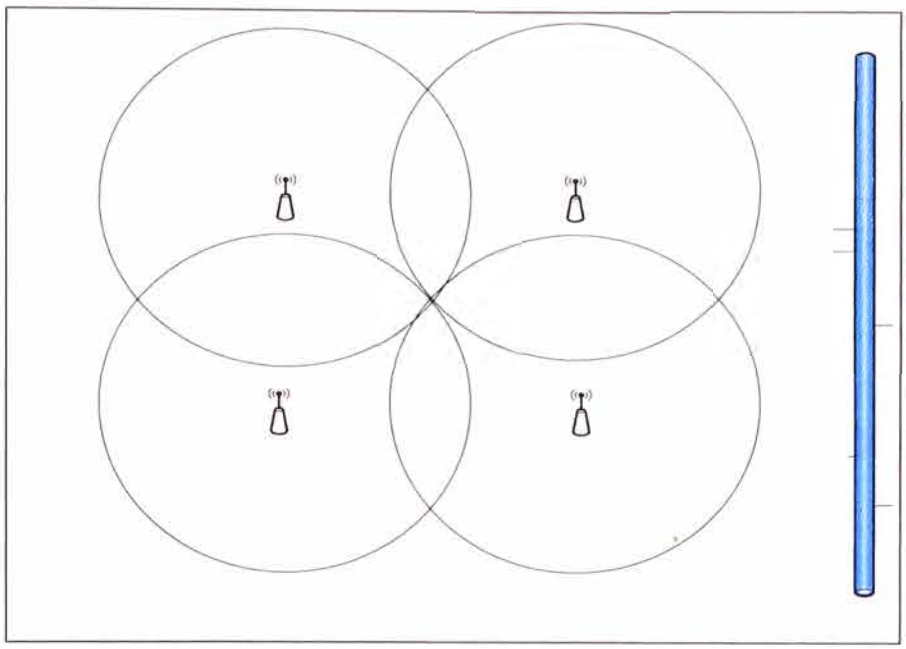

Figura 3.8 Topologías de la solución

3.3.1 Características ofrecidas por el WLC

Son las siguientes:

a. Tener la capacidad de publicar mediante SSID todas las VLAN (en caso de ser necesario)

b. Poder reenviar peticiones DHCP (relay)

c. Manejar patrones de seguridad apropiados:

-Asociación por MAC address (dirección física del host)

-Seguridad mediante WEP (40, 128 bits)

-Seguridad WPA, WPA2 (encriptación AES, autenticación: PSK, 802.1X)

-Autenticación WEB, etc.

d. Restricción y bloqueo de P2P

e. Habilitación de Roaming de Data

f. Funcionamiento de todos los AP en conjunto (como si fueran uno solo):

-Todos los AP pertenecientes al mismo grupo publican el mismo SSID.

-Ante la caída de un AP los otros automáticamente aumentan la intensidad en sus antenas para tratar de cubrir el área de cobertura inicial.

g. Seguridad optimizada en acceso, ya que solo el wireless controller estará conectado a un puerto de troncal y los APs a puertos de acceso comunes, logrando difundir las distintas VLANs mediante el uso del Protocolo LWAPP.

3.3.2 Configuración de los Wireless Lan Controller (WLC)

Se realizo la configuración básica, que consiste en habilitar las interfaces en el cual opera el WLC, es decir la interfaz de administración, la AP-manager, virtual, y cuatro interfaces dinámicas (VLANS), que justamente son para que se asigne de acuerdo a la

necesidad del cliente, uso interno y también para invitados (con acceso solo a Internet). Las direcciones se muestran en las Tabla 3.1 y la Tabla 32:

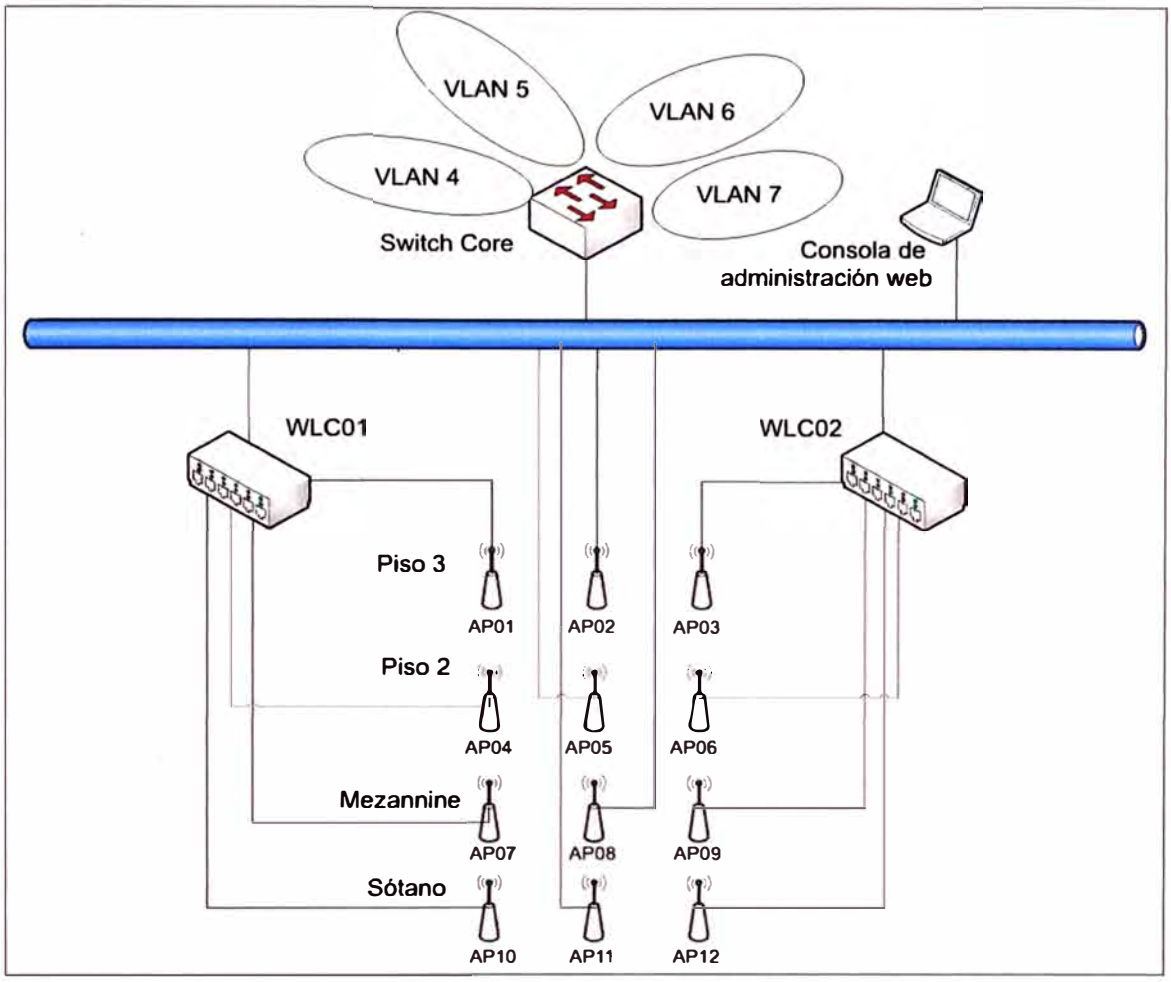

Figura 3.9 Esquema conexión solución inalámbrica BVL

Tabla 3.1 WLC 01 (master)

Nombre del interfaz	Puerto	Identificador de VLAN	Dirección IP
AP-Manager	1	Sin identificador	191.168.4.51
Administración	1	Sin identificador	191.168.4.50
Virtual	N/A	N/A	1.1.1.1
Vlan 4	1	4	0.0.0.0
Vlan 5	1	5	192.168.5.254
Vlan 6	1	6	192.168.6.254
Vlan 7	1	7	192.168.7.254

Tabla 3.2 WLC 02 (miembro)

Nombre del interfaz	Puerto	Identificador de VLAN	Dirección IP
AP-Manager	1	Sin identificador	191.168.4.53
Administración	1	Sin identificador	191.168.4.52
Virtual	N/A	N/A	1.1.1.1
Vlan 4	1	4	0.0.0.0
Vlan 5	1	5	192.168.5.254
Vlan 6	1	6	192.168.6.254
Vlan 7	1	7	192.168.7.254

Los Access Point trabajan en modo LIGHTWEIGHT, de tal manera que toda dependencia es hacia el Wireless Lan Controller (WLC). No se requiere realizar ningún

tipo de configuración en los Access point, ellos son gestionados por los controladores.

3.3.3 Canales, potencia y ganancia de antena

Se presenta un cuadro de acuerdo a los canales y frecuencias en cada canal, para América solo se admiten 11 canales. Tabla 3.3

Tabla 3.3 Canales

Id. de Canal	Frecuencia (MHz)	América
1	2412	X
2	2417	X
3	2422	X
4	2427	X
5	2432	X
6	2437	X
7	2442	X
8	2447	X
9	2452	X
10	2457	X
11	2462	X
12	2467	-
13	2472	-
14	2484	-

Las siguientes tablas muestran la máxima cantidad de potencia irradiada respecto a la velocidad de transmisión. Tabla 3.4 para 802.11b y Tabla 3.5 para 802.11g.

Tabla 3.4 802.11b

Tasa de datos Mbps	Máximo EIRP para una tarjeta PC-Cardbus con ganancia de antena 0 dBi y una tarjeta PCI con ganancia de antena 1 dBi	
	mW	dBm
1	100	20
2	100	20
5.5	100	20
11	100	20

Tabla 3.4 802.11g

Tasa de datos Mbps	Máximo EIRP para una tarjeta PC-Cardbus con ganancia de antena 0 dBi y una tarjeta PCI con ganancia de antena 1 dBi	
	mW	dBm
6	50	17
9	50	17
12	50	17
18	50	17
24	50	17
36	40	16
48	31.6	15
54	20	13

3.3.4 Resumen de configuración de los Wireless Lan Controler 2100

Se expresa en lo siguiente:

-Configuración básica (direccionamiento para interfaces)

-Creación de interfaces de acuerdo a las Vlans creadas en lo Switches

-Creación de SSIDs correspondientes a la Vlans ya establecidas

-Definición de políticas de Seguridad WEP, WPA, WPA2 y Layer 3

-Autenticación PSK (clave compartida); se sugiere implementar a futuro autenticación 802.1x (certificado digital)

-Descubrimiento de Vecinos (CDP v2)

-Encriptación AES

3.3.5 Acceso y monitoreo

Para acceder al equipo es necesario digitar la dirección web: https://191.168.4.50, aparecerá una ventana emergente, aceptar las condiciones y luego acceder al equipo con nombre de usuario bvladmin y contraseña xxxxxxxxx! (por razones de seguridad no será difundida). Ver Figura 3.10.

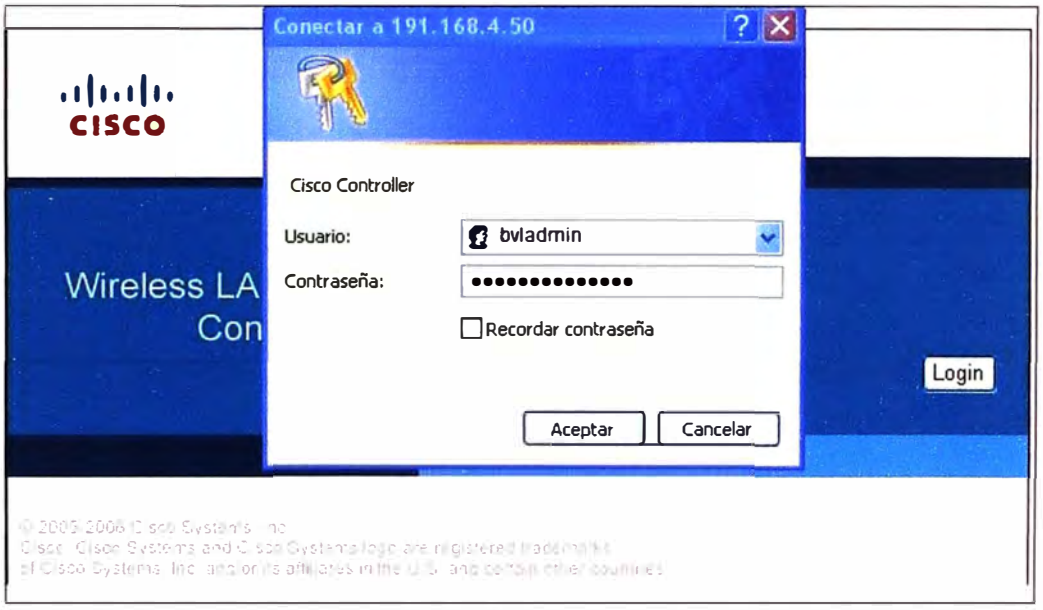

Figura 3.10 Ventana emergente para acceso

En la pantalla principal se visualizan los AP que se encuentran activos (Figura 3.11).

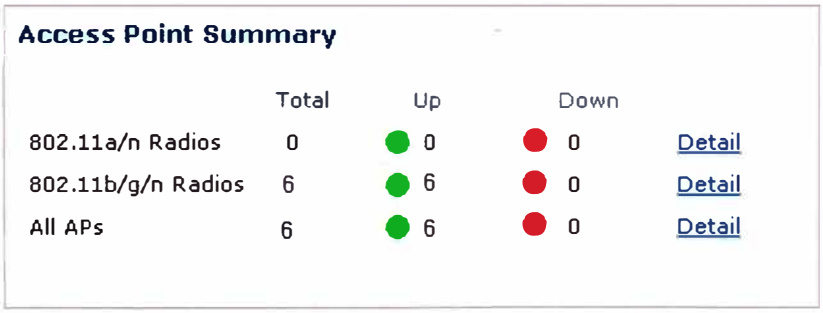

Figura 3.11 Ventana emergente para acceso

3.4 Equipamiento

Esta sección describe el equipamiento utilizado en la solución:

1. Controladores,
2. Puntos de acceso,
3. Software de gestión

Para complementar, el Anexo A muestra fotos de las instalaciones

3.4.1 Controladores

Son dispositivos de conmutación para administrar APs cuyo uso esta orientado a la clase empresarial. Soportan los protocolos 802.11a/b/g/n. Operan bajo el control de un sistema operativo, el cual incluye la administración de recursos de radio (RRM), creando una solución unificada de redes inalámbricas que puede automáticamente ajustar en tiempo real cambios en el entorno 802.11 RF.

El controlador LAN inalámbrico de la serie 2100 de cisco, trabaja en conjunto con APs cisco y con el Sistema de Control Inalámbrico (WCS por sus siglas en ingles) de cisco. Como un componente de la red inalámbrica unificada de cisco, el controlador de la serie 2100, presenta a los administradores de red la visibilidad y el control necesarios para administrar con eficiencia y seguridad las redes inalámbricas de clase empresarial y los servicios de movilidad tales como voz, acceso de invitados y servicios de localización.

Los controladores de la serie 2100 tienen 8 puertos de cobre Ethernet de 10 o 100 Mbps a través de los cuales el controlador puede soportar hasta 6, 12 o 25 APs. La Figura 3.12 muestra una topología de red típica para un controlador de la serie 2100. Se puede observar cómo se conecta un controlador LAN inalámbrico de la serie 2100, y seis APs (Puntos de acceso) Cisco.

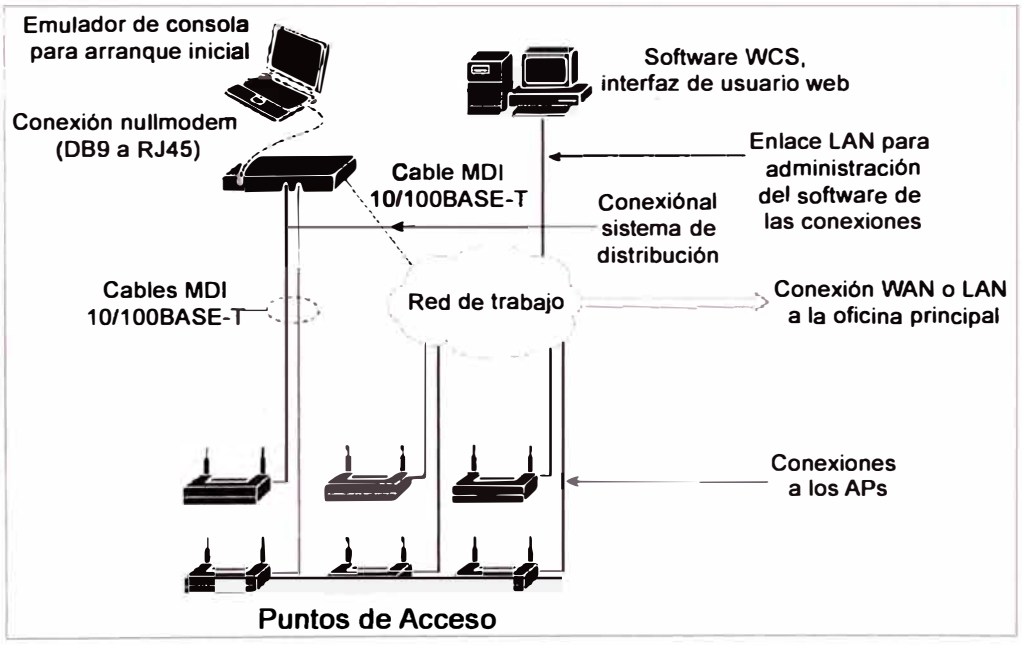

Figura 3.12 Controlador LAN en una topología básica

La Figura 3.13 muestra al controlador inalámbrico LAN de la serie cisco 2100. Se describirá los LEDs más importantes que aparecen en la vista mostrada.

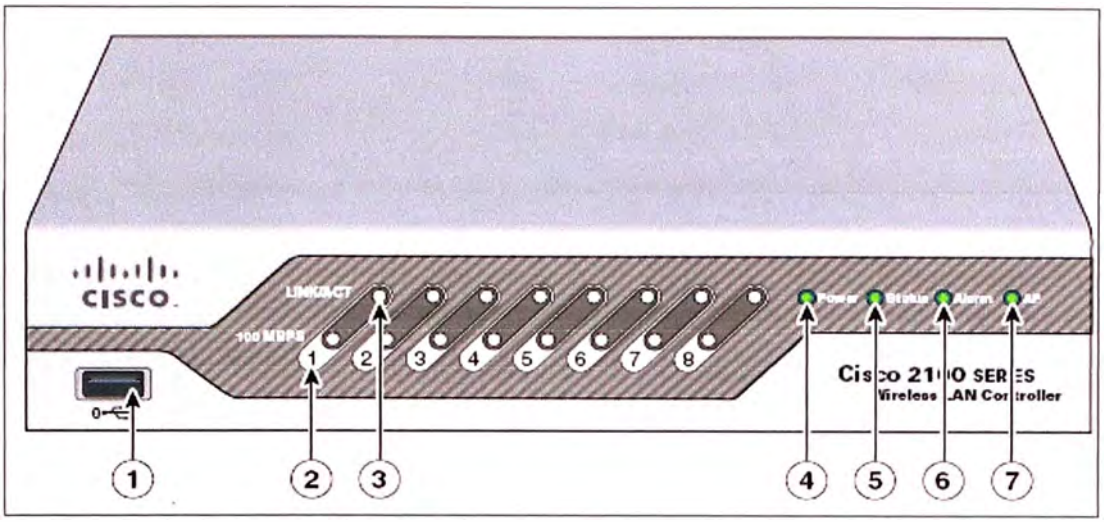

Figura 3.13 Vista frontal de un Controlador inalámbrico LAN de la serie cisco 2100

2: Indicador de velocidad, si esta apagado el LED, la velocidad es de 10 Mbps, pero si el LED esta encendido (color verde), la velocidad del puerto es de 100 Mbps.

3: Indicador de actividad del enlace, si el LED esta estoico en color verde, significa que el enlace se ha establecido, si esta de color verde y parpadeando, significa que hay actividad es la interfaz de red.

4: LED de encendido, verde significa que esta en línea, apagado significa fuera de línea.

5: LED de estado, verde significa que el controlador esta operando normalmente, color ámbar significa que hay un problema con el hardware (físico).

7: LED de información de los AP, si esta en verde significa que al menos un AP se ha asociado al controlador, apagado significa que el controlador no tiene ningún AP asociado.

La Figura 3.14 muestra la parte posterior del controlador. Se describe a continuación las partes más importantes.

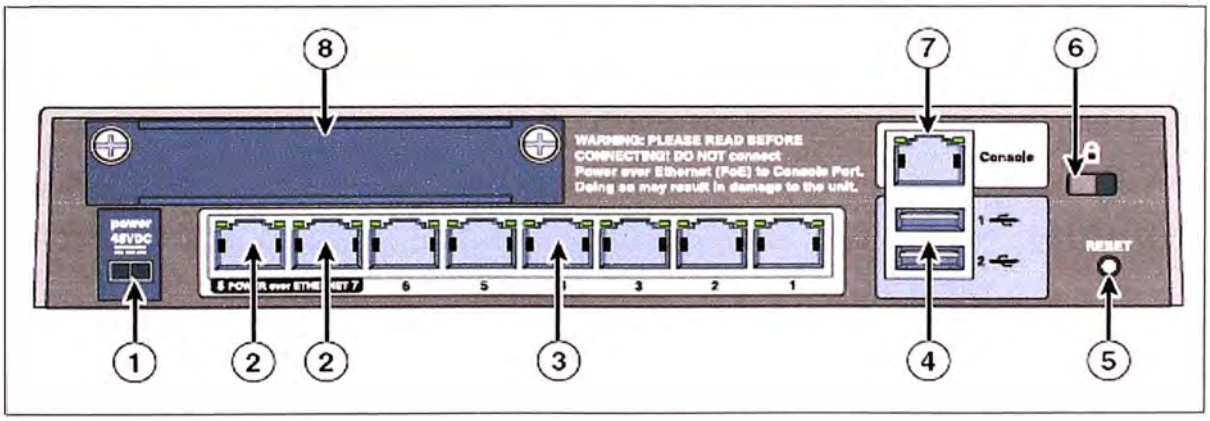

Figura 3.14 Vista posterior de un controlador inalámbrico de la serie cisco 2100

1: Conector de alimentación eléctrica 48 voltios continuos, se consiguen mediante el uso

de un transformador que viene con el equipo.

2: Puertos habilitados para entregar energia a través del puerto de red, comúnmente conocido como POE (Power over Ethernet).

3: Puertos distribuidos para los access point.

5: Boton de reinicio a configuración de fabrica del dispositivo (reset)

7: Puerto de consola

Los tres primeros controladores son stand-alone (autónomos). Los otros tres controladores son integrados a un switch o router.

3.4.2 Access Point (puntos de acceso)

Un Access Point (AP) actúa como un concentrador de comunicaciones para los usuarios de redes inalámbricas. Un AP puede enlazar redes cableadas e inalámbricas. En grandes instalaciones, múltiples APs pueden configurarse para permitir a los usuarios inalámbricos hacer roaming (pasar de un AP a otro sin perder conexión) entre APs sin interrupción. Los access point también proporcionan seguridad. Finalmente, un AP puede actuar como repetidor inalámbrico, o punto de extensión para la red inalámbrica. La Figura 3.15 muestra el access point Cisco modelo Aironet 1240G.

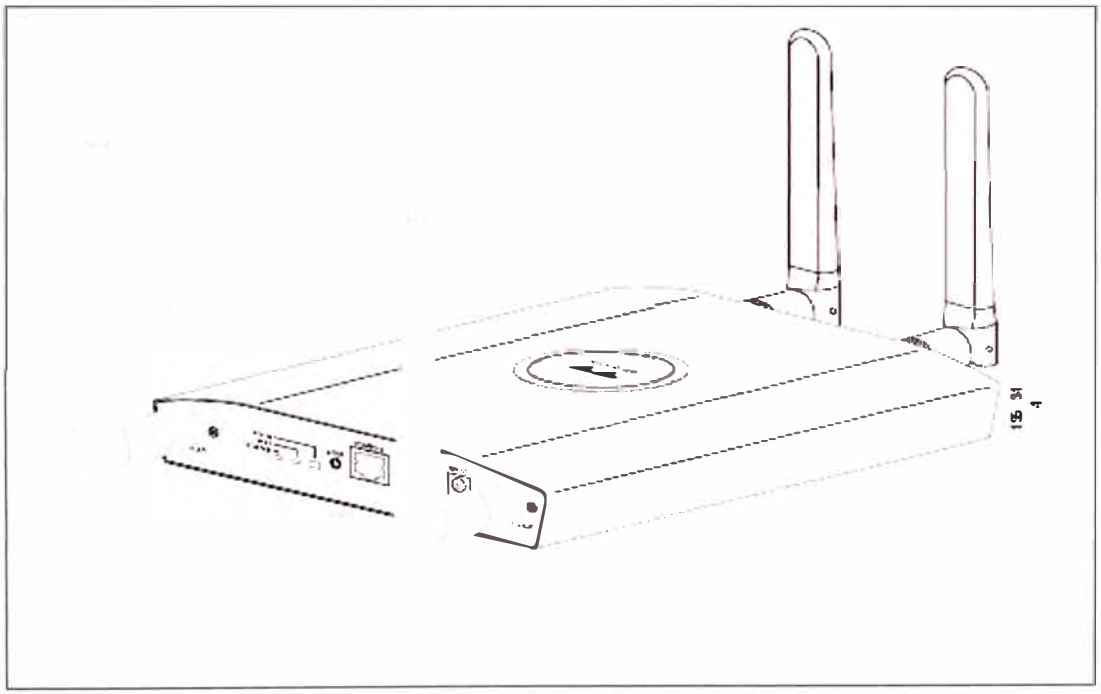

Figura 3.15 Access point con antenas

Las características del AP mostrado en la Figura 3.10 son las siguientes:

Modo de operación dual-radio: significa que opera en ambas frecuencias 2.4GHz y 5Ghz. Puede controlarse y configurarse a través de la línea de comandos e interfaces de la web.

La administración también puede llevarse a cabo a través de protocolos tradicionales como SNMP y syslog.

Una variedad de opciones de antena puede proporcionar un alcance o velocidad adicional, dependiendo de la instalación.

Un AP puede ser de banda única, como el AP 802.11a de 5Ghz. También puede ser de banda dual, como el AP 802.11a de 5Ghz o el 802.11b de 2.4Ghz.

3.4.3 Software de gestión

Cómo software de gestión es utilizado el Cisco Wireless Control System (WCS). Es la plataforma de administración más completa de la industria para la administración del ciclo de vida de 802. 11n y 802.11a/b/g, redes inalámbricas de clase empresarial. Esta plataforma de administración sólida ofrece una solución de administración rentable que permite que los administradores para planificar, implementar, supervisar, solucionar problemas y con éxito un informe sobre las redes inalámbricas interiores y exteriores La Figura 3.16 muestra el resumen de la configuración y la Figura 3.17 la ubicación mas apropiada de los clientes al punto de acceso que ofrece mejor señal.

Cisco WCS es una plataforma completa que escala para satisfacer las necesidades de pequeñas, medianas y a gran escala de redes LAN inalámbricas en todas las ubicaciones locales, remotas, nacionales e internacionales.

Esta solución TI da acceso inmediato de los administradores a las herramientas que necesitan, cuando ellos, necesitan más eficientemente implementar y mantener seguras las redes LAN inalámbricas, todo desde una ubicación centralizada que requiere un mínimo personal de TI.

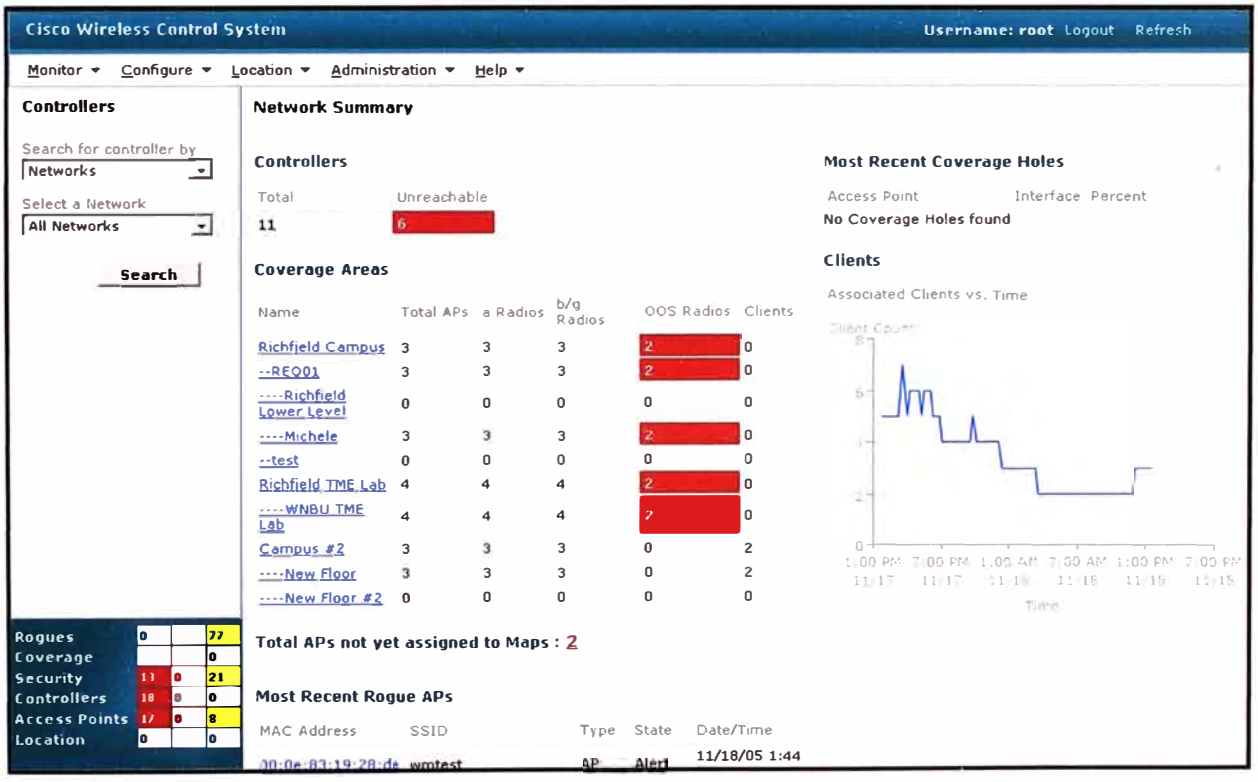

Figura 3.16 Consola de administración

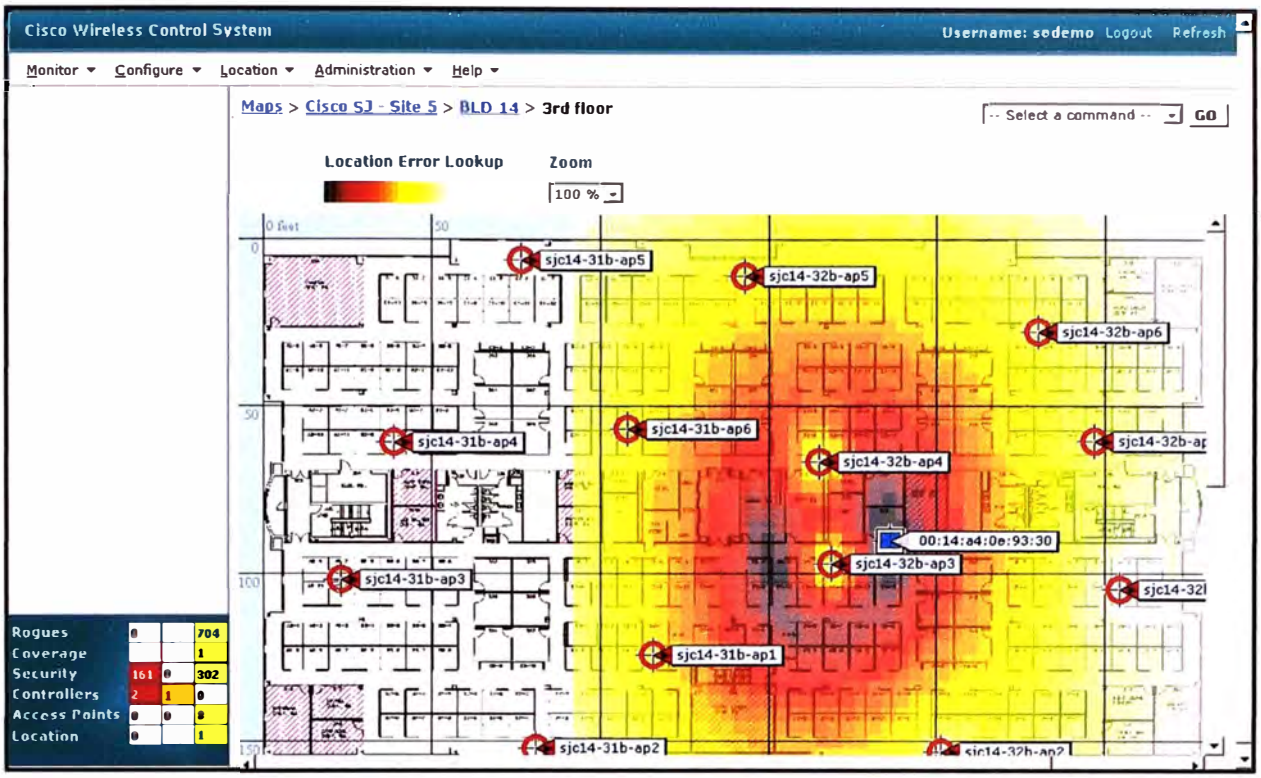

Figura 3.17 Mapa con la ubicación de los cliente

Los costos operacionales se reducen considerablemente a través de la interfaz gráfica intuitiva de Cisco WCS, herramientas simplificadas de facilidad de uso e integrados que ofrecen mayor eficiencia, disminuyen los costos de formación de TI y las necesidades de personal de TI son minimizadas, incluso cuando la red crece.

Administración integral de ciclo de vida de LAN inalámbrica

A continuación se desarrollan los aspectos principales: a) Administración integral de ciclo de vida de LAN inalámbrica, b) Monitoreo, c) Solución de problemas.

Figura 3.18 Ciclos de vida de la administración integral

a. Administración

Cisco WCS hace que las operaciones de LAN inalámbricas más eficiente y eficaz para todas las fases del ciclo de vida: Planeamiento (planning), Despliegue (deployment) Monitoreo (Monitoring), Solución de problemas (Troubleshooting), Reporte (Reporting). Estas se muestran en la Figura 3.18.

b. Monitoreo

Cisco WCS es la plataforma de administración ideal para la supervisión de la LAN inalámbrica completa para mantener un rendimiento sólido y ofrecer una óptima experiencia inalámbrica a móviles de los usuarios finales. La interfaz centralizada de Cisco WCS facilita acceso a la información donde sea necesario.

Cisco WCS es fácil de usar pues sirve como punto de partida para mantenimiento, seguridad, solución de problemas y capacidad futura planificación de las actividades. Acceso rápido a datos útiles acerca de los eventos insalubres y saludables que se producen en la red está disponible en una variedad de puntos de entrada, haciendo del Cisco WCS vital para las operaciones de la red actual.

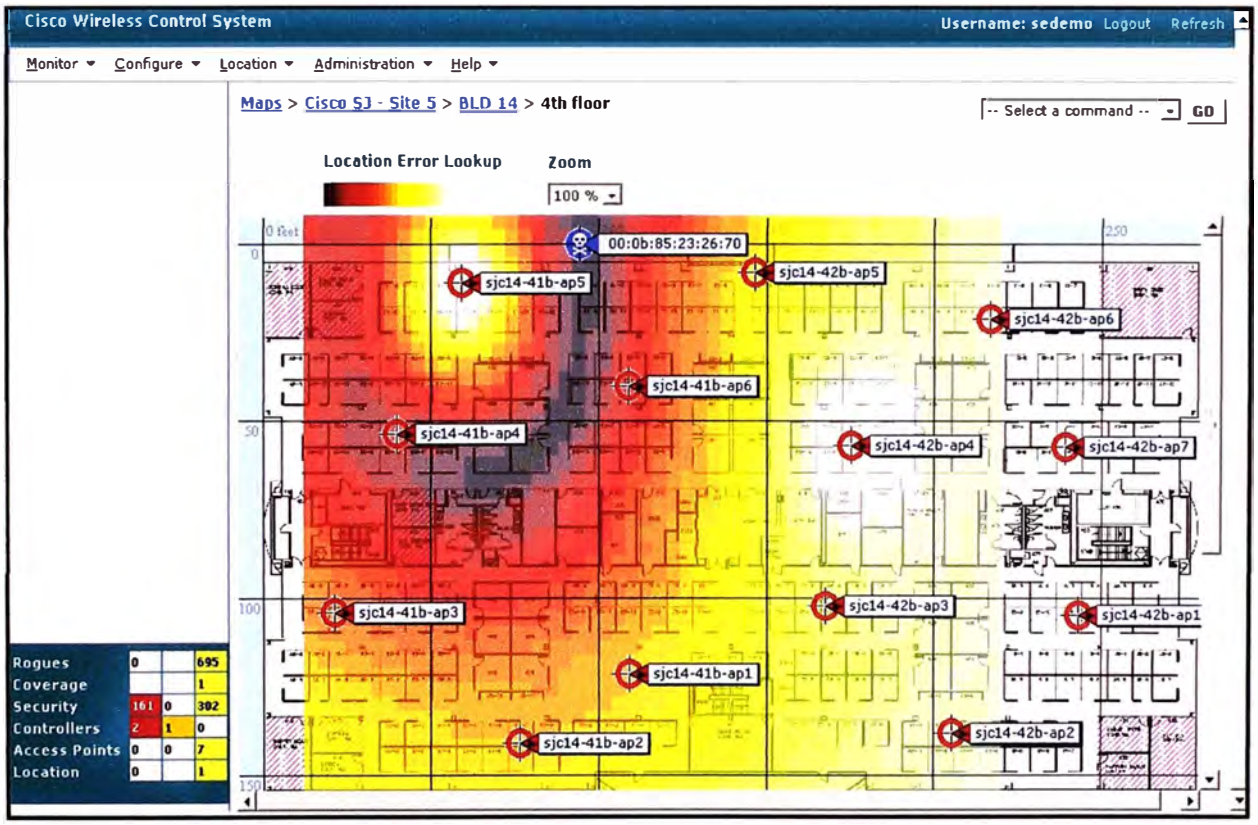

Figura 3.19 Mapa indicando ubicación de los puntos de acceso no autorizados

El resumen de alarma omnipresente en Cisco WCS simplifica el acceso a la información crítica, fallos y alarmas que se basa en su gravedad; facilitar la evaluación rápida de las notificaciones pendientes y apoyar una resolución más rápida de tickets de problemas. Las tareas de detectar, localizar y bloquear dispositivos no autorizados es

totalmente compatible cuando se habilitan servicios de localización (Figuras 3.19 y 3.20).

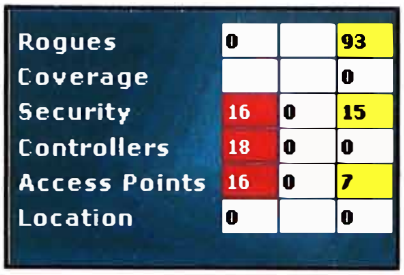

Figura 3.20 Monitor de alarmas para puntos de acceso no autorizados

c. Solución de problemas

Los flujos de trabajo integrados y la expansiva matriz de solución de problemas de herramientas en Cisco WCS ayudan a los administradores de TI rápidamente a identificar, aislar y resolver los problemas a través de todos los componentes de la red inalámbrica unificada de Cisco. Cisco WCS admite rápida solución de cualquier tamaño WLAN con mínimo personal de TI.

Cisco WCS facilita la evaluación rápida de las interrupciones del servicio, recibir notificaciones acerca de degradación del rendimiento, las resoluciones de la investigación y tomar medidas para paliar situaciones no óptimos. Los flujos de trabajo integrados admiten vínculo transparente entre todas las herramientas, alarmas, alertas, búsquedas e informes para todos los componentes de la infraestructura y dispositivos de cliente.

Una variedad de herramientas trabajan juntas para ayudar a los administradores de TI a comprender los matices operacionales que se producen en la WLAN y descubrir no óptimos de eventos que se producen fuera de los parámetros de línea de base, como la conexión de cliente o problemas de itinerancia.

La herramienta de búsqueda omnipresente en Cisco WCS facilita el acceso a la red a mediante la información histórica acerca de dispositivos ubicados en cualquier lugar de la red inalámbrica.

CONCLUSIONES Y RECOMENDACIONES

1. Se logró diseñar e implementar una red inalámbrica (IEEE 802.11 b/g) con criterios de seguridad para la Bolsa de Valores de Lima (BVL).

2. La solución inalámbrica fue implementada mediante el uso de dos controladores inalámbricos Cisco de la serie 2100 que son los encargados de gestionar los 12 Puntos de Accesos (de la familia Aironet 1130) que se ubicaron estratégicamente en los cuatro niveles que posee (sótano, mezzanine y dos pisos).

3. El uso de controladores a facilitado la gestión de la WLAN al personal que administra la red.

4. La seguridad aplicada fue WPA con encriptación AES, y cómo autenticación web no habiéndose producido hasta la fecha ninguna vulnerabilidad a la seguridad de la red de la empresa.

5. Se recomienda que los Wireless Controler estén en un área restringida y protegidos con energía estabilizada y en un ambiente temperado.

6. Se recomienda un mantenimiento físico y actualización de firmware de los APs a las últimas versiones existentes.

7. La empresa debe aplicar mecanismos de detección y contención frente ataques de red que proviene de una PC correctamente autenticada, así mismo proveer configuración de antivirus y IPS/firewall personal en cada computadora personal (PC) de le empresa.

ANEXO A
FOTOS DE INSTALACIONES

Los Access point están ubicados en el techo o falso techo de cada una de las oficinas tal como lo muestra la Figura A.1. Son ideales para oficinas y entornos similares que tienen poca variabilidad ambiental. Este punto de acceso ha integrado las antenas que proporcionan cobertura omnidireccional, patrones predecibles y puede operar en la frecuencia de 5GHz, según la norma 802.11a.

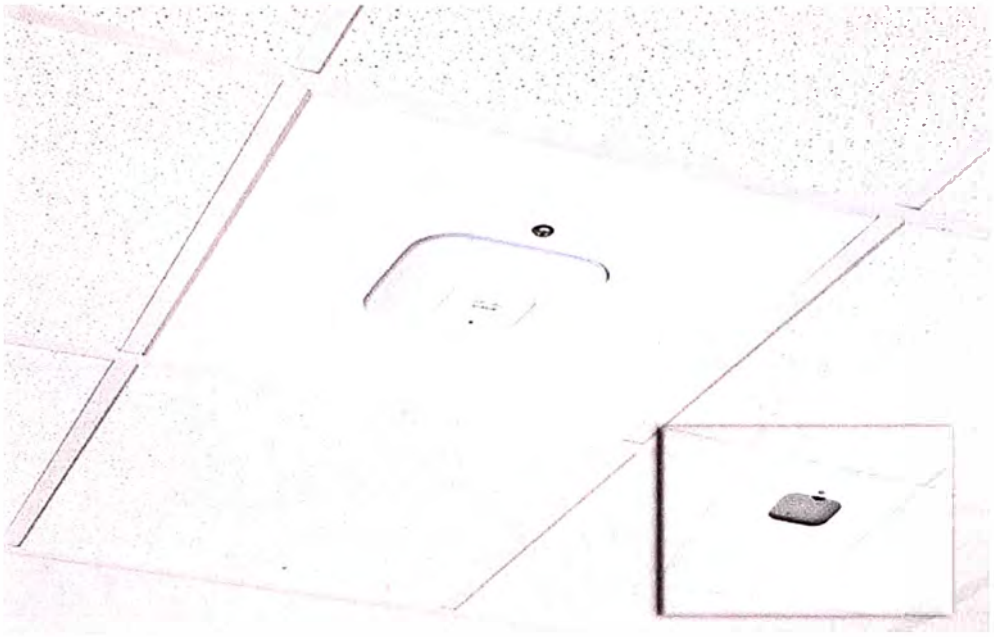

Figura A.1 Ubicación De Los Access Point

La Figura A.2 muestra los inyectores de corriente utilizados para energizar los ACCESS POINT utilizando el mismo medio por el cual circulan los datos, se observa que están conectados a la red eléctrica por medio de un adaptador de voltaje. Los inyectores se ubican en un gabinete ubicado en el centro de datos, en este mismo lugar se ubica el controlador inalámbrico que se muestra a continuación.

Figura A.2 Inyectores de corriente (POWER INJECTORS)

La Figura A.3 muestra uno de los dos controladores utilizados (AIRCon-WLC2106-K9 de Cisco)

Figura A.3 Controlador AIR-WLC2106-K9 Cisco

En la Figura A.4 se observa que el ACCESS POINT recibe la señal tanto de datos como eléctrica por medio de un cable de cobre de 8 hilos conocido como cable UTP que está conectado al inyector de energía. El inyector a su vez está conectado a un SWITCH por el cual recibe la señal de datos y también está conectado mediante un adaptador de voltaje a la red eléctrica por el cual recibe la corriente alterna y la convierte en continua para pasarla al inyector.

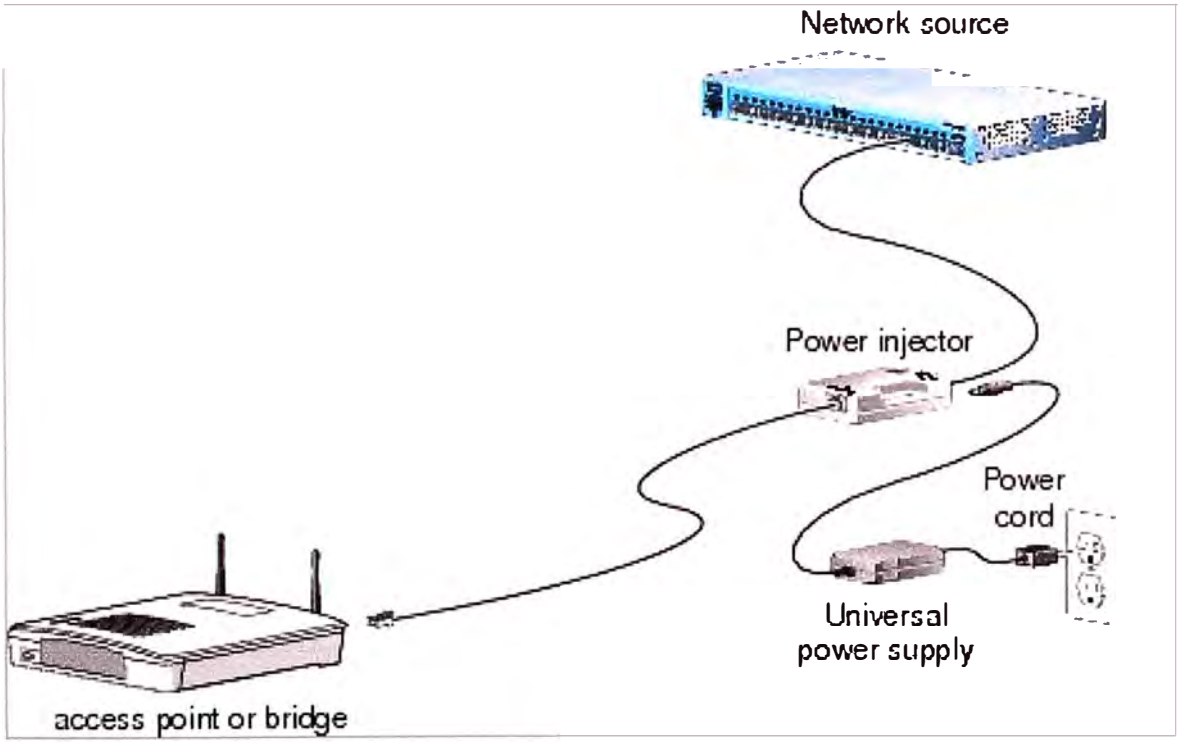

Figura A.4 Esquema de conexión de inyector de corriente a AP

ANEXO B
GLOSARIO DE TÉRMINOS

AES	Protocolo Estándar Avanzado de Encriptación
APN	Nombre del punto de acceso
APs	Access Point (Puntos de Acceso)
ASCII	American Standard Code for Information Interchange
BKR,	Rotación de clave de broadcast (Broadcast key rotation)
BS	Estaciones base
BSS	Conjunto de Servicios Básicos
BVL	Bolsa de Valores de Lima
CDP	Protocolo de descubrimiento de Cisco
CLI	Línea de comandos
DS	Sistema de Distribución
DoS	Ataques de negación de servicio
EAP	Protocolo de Autenticación Extensible
EAPOL	EAP sobre LAN
ESS	Conjunto de servicios extendido
FTP	Protocolo de Transferencia de Archivos
GPRS	General Packet Radio Service
GUI	Interfaz gráfica de usuario
GSM	Sistema Global para las comunicaciones Móviles
Hacking	Piratería
Hub	Concentrador
IVs	Vectores de Inicialización
IBSS	Conjunto de Servicios Básicos Independiente
ICV	Control de integridad
FIPS	Estándar de Procesamiento de Información Federal
HTTP	Protocolo de transferencia de hipertexto
IPSec	Seguridad IP
IR	Luz infrarroja
LAN	Redes de área local
LEAP	EAP Liviano (Lightweight EAP)
LOS	Línea de vista
MAC	Control de acceso al medio
MAN	Redes de área metropolitana)
MD5	Resumen de Mensajes 5
MIC	Control de Integridad de Mensajes
MMS	Servicio de mensajería multimedia

NIC	Tarjetas de interfaz de red
NIST	Instituto Nacional de Estándares y Tecnología
NTP	Protocolo de tiempo de la red
PAN	Redes de área personal
PRNG	Generador de números pseudo aleatorios
QoS	Calidad des servicio
RADIUS	Servidor de Servicio al Usuario de Acceso Telefónico Remoto Remote
RC4	Rivest Cipher 4
RF	Frecuencias de radio
SHA	Algoritmo Hash Seguro (Secure Hash Algorithm)
SMS	Servicio de mensajes cortos
SNMP	Protocolo Simple de Administración de Redes
SS	Estaciones suscriptoras
SSH	Secure Shell
SSID	Identificador de Red
SSL	Capa de Socket Seguro (Secure Socket Layer)
SSN	Networking de Seguridad Simple
STAs	Estaciones asociadas
TFTP	Protocolo Transferencia Trivial de Archivos
TKIP	Protocolo de integridad de clave temporal
UTMS	Sistema Universal de Telecomunicaciones Móviles
UWB	Banda Ultra Ancha
VAS	Servicios de valor agregado
VPNs	Redes Privadas Virtuales
WAN	Redes de área amplia
WAP	Wireless Application Protocol
WEP	EAP sobre Inalámbrico
WLAN	Redes de área local inalámbricas
WLC	Wireless Lan Controller
WPA	Acceso Protegido Wi-Fi

BIBLIOGRAFÍA

[1] Ing. Eduardo Tabacman, "Redes Inalámbricas (WiFi) Conceptos Básicos de Seguridad", 2006 http://www.virusprot.com/cursos/Redes-Inalámbricas-Curso-gratis.htm Ketterling,

[2] Cisco Networking Academy Program, "Fundamentos de redes Inalambricas" 2007.

[3] Certified Wireless Network Administrator, Official Study Guide, Mc Graw-Hill, Third Edition.

[4] Cisco Wireless LAN Controller, Configuration Guide, Cisco System Inc. Software Release 2007, Text Part Number OL-9141-03

[5] Cisco Aironet 1240AG Access Point Harware Installation Guide, 2007, Text Part Number OL-9141-03.

[6] Izaskum Pellejero, et al, "Fundamentos y aplicaciones de seguridad en redes WLAN", Marcombo Ediciones Tecnicas, 2006

[7] David Wall CCSI Technical Editor, "Managing and Securing a Cisco Structured Wireless Aware Network (SWAN)" Cisco System INC, 2005

[8] Building a Cisco wireless LAN Escrito por Eric Ouellet,Ron Fuller,Robert Padjen,Arthur Pfund,Tim Blankenship, Copyright 2002 by Syngress Publishing, Inc.

[9] John W. Rittinghouse,James F. Ransome, "Wireless operational security", Copyright 2004.

[10] Vijay Kumar Garg, "Wireless communications and networking",Morgan Kaufmann Publishers, 2007