POLITICAS DE GESTION PARA REDES INALAMBRICAS EN ENTORNOS EMPRESARIALES.

CHRISTIAN MAURICIO NAVAS M.
CLAUDIA LILIANA PACHECO L.

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2008

POLITICAS DE GESTION PARA REDES INALAMBRICAS EN ENTORNOS EMPRESARIALES.

CHRISTIAN MAURICIO NAVAS M.
CLAUDIA LILIANA PACHECO L.

Monografía presentada como requisito para optar al título de Especialista en Telecomunicaciones

DIRECTORA:
SHIRLEY PAOLA HERRERA HERNÁNDEZ
Especialista en Telecomunicaciones

CO-DIRECTORA:
LEYDI JOHANNA BARCO RINCÓN
Magíster en Ingeniería (c)

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2008

Dedicatoria

A Dios, por sus bendiciones.
A mis padres por las oportunidades que me brindan día a día, sin su amor y confianza, esto no sería posible.
A mis hermanos, por su cariño y apoyo, siempre están presentes en todos mis proyectos.
Y por supuesto a mis amigas, las incondicionales, porque con ustedes he aprendido el verdadero significado de la amistad.

Claudia Liliana Pacheco Luengas

D edicatoria

A mi familia fuente invaluable de apoyo, confianza y comprensión.
A mi novia, cuyo afecto y apoyo permanentes, me permitieron culminar este proyecto contagiandome de su alegria.

Christian Mauricio Navas Muñoz

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

TITULO: Políticas de gestión para redes inalámbricas en entornos empresariales.[*]

AUTORES: Christian Mauricio Navas M., Claudia Liliana Pacheco L.[**]

PALABRAS CLAVES: Arquitecturas WLANs, Seguridad en WLANs, Políticas de gestión de WLANs, WLANs en entornos empresariales.

DESCRIPCIÓN O CONTENIDO

En los últimos años, la tecnología WLAN está siendo considerada seriamente como una forma de completar una red existente o de crear una nueva red. Antes limitadas a un sector muy específico de la demanda, las redes locales inalámbricas se están convirtiendo en una herramienta estratégica para todo tipo de empresas, sin importar su tamaño y actividad.

Uno de los grandes desafíos para una WLAN empresarial es proporcionar las elevadas capacidades de proceso que hoy ofrecen las redes cableadas 10/100 Mbps, no obstante la IEEE ha desarrollado estándares que permiten velocidades de hasta 100Mbps (Estándar 802.11n).

Sin embargo, cuando se trabaja en redes corporativas con aplicaciones de misión crítica y soportan un número elevado de usuarios, su despliegue debe ser mucho más robusto e "inteligente" que la simple instalación de puntos de acceso. Asimismo, la confidencialidad, integridad y autenticidad deben abordar las necesidades centrales de gestión, seguimiento y control de los puntos de acceso inalámbrico en conjunto con la red cableada.

Es aquí donde se hace esencial un diseño estructurado para este tipo de redes con el objeto de favorecer la distribución y el mantenimiento de forma centralizada de los puntos de acceso, en cuanto a información estática, como la configuración de hardware e información dinámica, como parámetros de seguridad, grupos de trabajo entre otros, lo que implica por supuesto una topología jerárquica, que solo se logra con un conocimiento sólido de la tecnología. Las políticas de gestión y las nuevas tecnologías que se sugieren en esta investigación posibilitan la creación de entornos inalámbricos administrables de un modo unificado, como si se tratasen de una sola entidad, con capacidad de crear grupos virtuales de usuarios con derechos de acceso y políticas definibles y gestionables, independientemente de la localización física o de los movimientos que hagan de un lugar a otro.

---

[*] Monografía

[**] Faculta de Ingenierías Físico-Mecánicas. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Directora Shirley Paola Herrera. Codirectora Leydi Johanna Barco.

ABSTRACT

TITLE: Management polices for wireless network in enterprise environments.[*]

AUTHORS: Christian Mauricio Navas M., Claudia Liliana Pacheco L.[**]

KEY WORDS: WLANs Architectures, WLANs Security, Management polices for WLANs, WLANs in enterprise environments.

DESCRIPTION:

In recent years, WLAN technology is being seriously considered as a way to supplement an existing network or create a new network. Before limited to a very specific demand, wireless local area networks (WLAN) are becoming today a strategic tool for businesses of all kinds, regardless of their size and activity.

One of the great challenges for WLAN business is to provide a high processing capability that now offer wired networks 10/100 Mbps, however, the IEEE has developed standards that allow speeds of up to 54 Mbps and even 100Mbps (802.11n Standard).

However, when working in corporate networks with mission-critical applications and supports a large number of users, their deployment should be much more robust "intelligent" and that the simple installation of access points. Also, confidentiality, integrity and authenticity must address the needs of central management, monitoring and control of wireless access points in conjunction with the wired network.

This is where a design is essential for this kind of structured networks in order to promote the distribution and maintenance of a centralized access points, in terms of static information, such as hardware configuration and dynamic information, as parameters safety, working groups among others, which means of course a hierarchical topology, which will only be achieved with a solid knowledge of technology. Management policies and new technologies that are suggested in this research enable the creation of wireless environments manageable a unified way, as if it were a single entity, capable of creating virtual groups of users with access rights and policies definable and manageable, regardless of physical location or movements that make one place to another.

---

[*] Monograph

[**] Faculty of Physic-Mechanical Engineering. Electric, Electronic Engineering and Telecommunication's School. Director Shirley Paola Herrera. Co-Director leydi Johanna Barco

INTRODUCCION

A pesar del auge y la incidencia de las comunicaciones inalámbricas en la vida de los seres humanos, su implementación en ambientes empresariales sigue siendo un gran reto, no solo en cuanto a velocidades de transmisión sino a su vez en aspectos relacionados con la seguridad y gestión de las mismas frente a sus homólogas cableadas.

Asimismo, el espectro que utiliza la tecnología inalámbrica no tiene licencia, se puede saturar y ser susceptible a las interferencias, generando molestias y complicaciones en las conexiones. El mayor obstáculo para solucionar estos inconvenientes radica en que los efectos generalmente son intermitentes y, en consecuencia, más difíciles de detectar. Las señales pueden tener interferencias y crear un nuevo ataque de tipo de rechazo de servicio.

Si bien los inconvenientes relacionados con la seguridad, interferencia, estabilidad y desempeño, han sido una constante en esta tecnología, el estándar 802.11 ha evolucionado de tal manera que se han mejorado la gran mayoría de las características fundamentales, y de igual forma se han incorporado muchos beneficios para brindar eficientemente todos los servicios.

Sin embargo, el desconocimiento de los estándares y sus mejoras, así como de la infraestructura de estas redes, ha llevado a malos manejos tanto técnicos como administrativos de los equipos que las componen, haciendo más caótica su implementación en entornos de continua expansión.

Es precisamente esto lo que se pretende abordar en este proyecto, analizar el impacto y adaptación de estas redes y buscar mediante políticas de gestión una buena administración de los recursos que componen esta tecnología, de tal forma que brinde servicios complementarios a los sistemas cableados ya existentes en las

compañías, permitiendo la movilidad de sus usuarios, facilitando oficinas y LANs temporales, entre otros privilegios. La intención es responder si ¿Las quejas de la funcionalidad de las redes inalámbricas obedecen a problemas de la tecnología como tal?, o por el contrario son desaciertos en cuanto a diseño, implementación y administración de los dispositivos?

OBJETIVOS

OBJETIVO GENERAL

Formular políticas administrativas que faciliten la gestión de redes WLAN en infraestructuras corporativas.

OBJETIVOS ESPECÍFICOS

- Comprender las capacidades y limitaciones así como los riesgos de integrar redes inalámbricas a sistemas cableados ya existentes.
- Evaluar la seguridad de las redes WLAN y su impacto dentro de la organización.
- Proponer una arquitectura que facilite la administración de los recursos.

1. GENERALIDADES

Estándares 802.11. Despliegue y retos en redes empresariales.

Con la aprobación de la norma 802.11 por la IEEE en 1997, las WLAN iniciaron una lenta entrada en las redes de las empresas. La escasa velocidad de transmisión de la norma original 802,11, tan sólo 1 y 2 Mbps, limitó la aceptación generalizada de la tecnología, sin embargo se presentó un despliegue en aplicaciones verticales tales como los entornos de fabricación, almacenes y comercio minorista, como guía para la experimentación.

En 1999, el IEEE aprobó el 802.11a y 802.11b a la base estándar, lo que aumenta la velocidad de transmisión de datos disponibles a 54 y 11 Mbps, respectivamente, y la ampliación a una nueva banda de radio, sin mencionar el 802.11n que espera superar en casi 10 veces la velocidad del estándar 802.11a; esto, por consiguiente eliminó uno de los factores significativos que restringían la adopción del 802,11 en las grandes redes corporativas. No obstante, es importante destacar que la expansión de las WLAN 802,11 se ha concebido como la implementación y administración de un gran número de Access Points (APs) en dichas redes. Todo esto ha generado un estudio minucioso sobre la definición y la funcionalidad del Punto de Acceso (AP), así como de las técnicas de “bridging” de la capa 2 y de las VLANs para garantizar el correcto funcionamiento de los protocolos de capa superior.

Lo anteriormente descrito, pone en relieve ciertos retos al estándar 802.11. Como se ha mencionado, el eje de esta tecnología es el Acces Point o Punto de Acceso, por ende la gestión, el seguimiento y el control de un gran número de estos dispositivos en la red, puede resultar una carga significativa para la administración de la red. Igualmente, la distribución y mantenimiento de forma centralizada de los puntos de acceso, en cuanto a información estática como la configuración de hardware, e información dinámica como los parámetros de seguridad, grupos de trabajo entre otros, implica un buen diseño jerárquico de la arquitectura de la red, que solo se logra con un conocimiento sólido de la tecnología.

La naturaleza dinámica y compartida del medio inalámbrico, también exige una coordinación eficaz entre los APs para minimizar interferencias de radio y maximizar el rendimiento de la red. Del mismo modo, las consideraciones de seguridad que han sido una constante preocupación en redes WLAN, presenta incluso considerables desafíos en los grandes despliegues y las nuevas arquitecturas.

Recientemente, para hacer frente a algunos de los problemas, múltiples proveedores han comenzado a ofrecer soluciones propietarias que combinan los aspectos de la

red de conmutación, control y gestión centralizada entre otros, en una variedad de arquitecturas.

En este orden de ideas, este capitulo presenta una taxonomía de las arquitecturas existentes empleadas en los productos WLAN para entornos empresariales y sus desafíos, analizando por supuesto los conceptos concernientes a las funciones y servicios de este tipo de redes; cabe aclarar que no se ahondará en las nociones básicas relacionadas al manejo del medio en si.

1.1 FUNCIONES DE LAS REDES IEEE 802.11

El IEEE 802.11 es un estándar que define el uso de los dos niveles inferiores de la arquitectura TCP/IP (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN, por lo tanto establece las interfaces entre un cliente inalámbrico o estación (STA) y un Punto de Acceso (AP), así como entre los clientes inalámbricos. De igual forma describe cómo los dispositivos móviles pueden asociarse a un conjunto de servicios básicos (BSS) y este a su vez es identificado con un nombre o ID acreditado con las siglas en inglés (BSSID).

Dado que el propósito de la norma es proporcionar conectividad inalámbrica, la arquitectura WLAN puede ser considerada como un tipo de arquitectura de 'células', en el que cada célula es la base del conjunto de servicios (BSS), y cada BSS está controlado por un AP. Cuando dos o más AP están conectados a través de la capa 2 de la red y todos ellos están utilizando el mismo SSID, se dice que se ha creado un extenso conjunto de servicios (ESS). De la misma manera, para interconectar conjuntos de servicios BSSs se necesita del sistema de distribución (DS). El DS habilita el soporte a dispositivos móviles proporcionando los servicios necesarios para manipular el mapeo de dirección a destino y la integración sin fisuras de múltiples BSSs. Los datos se desplazan entre un BSS y el DS a través de un AP. Nótese que todos los APs son también STAs, lo cual los convierte en entidades direccionables.

El IEEE 802,11 no especifica los detalles de manera explícita de las implementaciones del sistema distribuido. En lugar de ello, la norma define los servicios que proporcionan las funciones que requiere la capa LLC para el envío de Unidades de Datos de Servicio MAC (MSDUs) entre dos entidades en la red. Estos servicios pueden clasificarse en dos categorías: servicio de estación de (SS) y el sistema de servicios de distribución (DSS). Los últimos, se relacionan con la administración de membresías dentro de la celda y con la interacción con estaciones que están fuera de la celda. En contraste, los servicios de estación se relacionan con la actividad dentro de una sola celda. Ambas categorías son utilizadas por la subcapa MAC. El sistema servicios de distribución se fundamenta en los siguientes cinco servicios:

- Asociación: El servicio es utilizado por las estaciones para conectarse ellas mismas al AP. Por lo general, se utiliza después de que una estación se mueve dentro del alance de radio del Access Point. Una vez que llega, anuncia su identidad y sus capacidades. Estas incluyen las tasas de datos soportadas y los requerimientos de administración de energía.

- Disociación: Elimina una asociación existente. Una estación podría utilizar este servicio antes de apagarse o de salir, asimismo el AP podría utilizarlo antes de su mantenimiento.

- Reasociación: Establece una asociación (entre el AP y una estación STA) para ser trasladados de un AP a otro o el mismo AP.

- Distribución: Proporciona transmisión de MSDU de los Access Points a las estaciones asociadas con ellos. Las Unidades de datos de servicio MAC (MSDUs) pueden ser transmitidas a destinos inalámbricos o a redes cableadas (Ethernet) o ambos a través del concepto de "Sistema de Distribución".

- Integración: Traduce los MSDU recibidos del sistema de distribución a un no-formato 802,11 y viceversa. Cualquier MSDU que se recibe del Sistema de Distribución DS invoca la «integración» de los servicios de DSS antes de la "distribución" de servicios. El punto de conexión entre el DS y la red LAN se denomina “Portal”.

Los servicios de estación, se utilizan después de que ha ocurrido la asociación y constan de las siguientes prestaciones:

- Autenticación: Establece la identidad de una estación como miembro del conjunto de estaciones que están autorizadas a asociarse unos con otros.

- Des-autenticación: eliminación de una relación existente de autenticación.

- Confidencialidad: Evita que el contenido de los mensajes puedan ser leídos por personas distintas de los destinatarios. Este servicio maneja la codificación y decodificación. Un algoritmo especificado es RC4.

- Entrega MSDU: Entrega de unidades de datos de servicio MAC (MSDU) para las estaciones.

Aparte de estos servicios, el IEEE también define adicionales que deben ser generados por el Access Point AP. Entre ellos encontramos:

- Generación de Beacons o frames de administración: Ésta trama contiene parámetros de sistema BSS y de frames almacenados en los Access Points.

Se transmite de la misma manera que los frames de datos pero no se envían a las capas superiores.

- Prueba: respuesta/transmisión: relacionada con el manejo de los frames de control para el acceso al medio con el fin de establecer una sesión y comenzar la transmisión de datos.

- Procesamiento de frames de control: RTS/CTS/ACK/PS-Poll/CF-End/CF-ACK: Los frames de control, como la Solicitud para Enviar (RTS), Despejado para Enviar (CTS) y Confirmación (ACK), controlan el acceso al medio utilizando frames RTS, CTS y ACK. En cuanto al PS-Poll, éste es utilizado por una estación para recuperar cualquier frame almacenado en algún buffer de un Access Point mientras estuvo en stand-by por motivos de ahorro de energía. CF-End/CF-ACK también pertenecen al proceso de manejo del medio y a los mecanismos de control del mismo.

- Sincronización

- Retransmisiones

- Adaptación de la tasa de transmisión

- Seguridad: Encriptación/Des-encriptación.

Como se mencionó, el estándar no detalla con precisión, cómo estas funciones se deben ejecutar, ni tampoco especifica que se apliquen en un dispositivo físico en sí. Tan sólo exige que los Access Points APs y consecuentemente el sistema de distribución DS trabajen en conjunto de tal forma que apliquen todos estos servicios.

Normalmente, los proveedores implementan no sólo los servicios definidos en el estándar IEEE 802,11, sino también una variedad de servicios o funciones de valor agregado, como el balanceo de cargas, Calidad de Servicio QoS, entre otros.

Sin embargo, se ha demostrado que estas funciones no son suficientes, motivo por el cual el IETF ha realizado estudios con el objeto de hacer frente a los problemas que se citaron en lo relacionado a la administración, configuración, control y seguridad. Estas funciones son especialmente importantes especialmente cuando se aplican a lo largo de varias entidades en una red a gran escala. Estas funciones incluyen:

- Monitoreo RF, tales como detección por radar, detección de ruido e interferencia y medición.

- configuración RF, para la retransmisión, selección de canal, ajuste de potencia de transmisión.

- Configuración de Access Point.

- Carga de firmware para AP (actualización de firmware para amplia consistencia de la red).

- Base de datos de información de estado de las estaciones de la red, incluida la información necesaria para apoyar los servicios de valor agregado, como la movilidad y el balanceo de cargas.

- Autenticación mutua entre entidades de red.

Los servicios mencionados se refieren a la configuración y el control de los recursos de radio (Monitorización y Configuración), a la gestión y configuración del Punto de Acceso (Configuración AP, Actualización de Firmware), y a la seguridad, con el registro de un AP en una entidad de control centralizado, este ítem se retomará mas adelante. Como un adicional ha tomado el IEFT la información de estado en relación con los STA (s) asociados a la red inalámbrica, con el objeto de favorecer la gestión de la movilidad a través de subredes y balanceo de carga. Este servicio fue tomado en cuenta con base en las diferentes propuestas de los proveedores de los dispositivos WLAN.

En lo concerniente al control y la gestión de radio, relacionados con las funciones de un AP, se encuentran especificadas en la norma y se describen implícitamente en el MIB (base de información de gestión), en temas relacionados con:

- Canal de asignación
- Control de potencia de transmisión
- Medición del recurso de radio. (Perteneciente al estándar 802.11k)

Asimismo, el estándar 802.11h, especifica la aplicación de un protocolo MAC de gestión para cumplir con los requisitos de algunos órganos reguladores (principalmente en Europa, pero en expansión a otros) en las siguientes áreas:

- Detección de RADAR
- Control de potencia de transmisión
- Selección dinámica del canal.

1.2 ARQUITECTURAS WLAN

A continuación se enumerarán las diferentes arquitecturas que ha desarrollado la comunidad de proveedores en un intento para hacer frente a la mayoría de problemas expuestos al inicio del capítulo, obviamente estas han sido depuradas y clasificadas con base en las características de los sistemas de distribución que se emplean para proporcionar las funciones 802.11, por el Network Working Group CAPWAP del IETF a fin de lograr la interoperabilidad en el mercado.

1.2.1 Arquitectura Autónoma:

La primera familia es la arquitectura tradicional autónoma, en el que cada Punto de Acceso es un único dispositivo físico que implementa todos los servicios 802.11, incluyendo los servicios de distribución, integración y de “Portal”. Esta estructura se llama Autónoma debido a que cada AP es autónomo en su funcionalidad, y no es necesario un apoyo de productos distintos complementarios.

El Punto de Acceso o Access Point es típicamente configurado y controlado de manera individual y pueden administrado a través de redes típicas de gestión de protocolos como el SNMP. Este tipo de dispositivos también se les conoce "Stand-alone AP".

1.2.2 Arquitectura Centralizada:

Esta es una nueva arquitectura jerárquica que utiliza uno o más controladores centralizados para la gestión de un gran número de dispositivos AP. Dicho controlador es comúnmente referido como un controlador de acceso (AC), cuya función principal es gestionar, controlar y configurar los Puntos de Acceso que están presentes en la red.

Además de ser una entidad centralizada en el plano del control y la gestión, también puede convertirse en un punto natural de agregación para el plano de datos, ya que suele ser situado de forma centralizada en la red de acceso inalámbrico. El AC es a menudo instalado con un puente capa 2, un switch, o un router capa 3, y puede ser denominado puente de acceso o router de acceso en esos casos particulares. Por lo tanto, un controlador de acceso podría ser un dispositivo capa 2 o capa 3.

También es posible que múltiples ACs estén presentes en una red con fines de redundancia, balanceo de carga, etc. Esta arquitectura tiene varias características que vale la pena señalar. En primer lugar, la estructura jerárquica y centralizada del AC brinda una mejor capacidad de administración de redes a gran escala. En segundo lugar, las funciones IEEE 802.11 y las funciones de control son proporcionadas por el AP y el AC en conjunto, por lo tanto, se puede decir que todas las funciones y servicios se ejecutan a través de múltiples dispositivos de red.

Dado que los dispositivos AP implementan sólo una parte de las funciones que poseen aquellos que trabajaran como stand-alone, en esta arquitectura se les denominan “APs de peso ligero”.

1.2.3 Arquitectura Distribuida:

La tercera arquitectura emergente es la arquitectura distribuida en la que participan nodos inalámbricos que son capaces de formar una red distribuida entre sí, a través de medios cableados o inalámbricos.

Una malla de red inalámbrica es un ejemplo dentro de la familia de arquitectura distribuida, donde la unión de los nodos forma una malla de redes, así que como la conexión de mallas con nodos vecinos a través de enlaces inalámbricos. Algunos de estos nodos también tienen conexiones con cable Ethernet que actúan como puertas de entrada a la red externa.

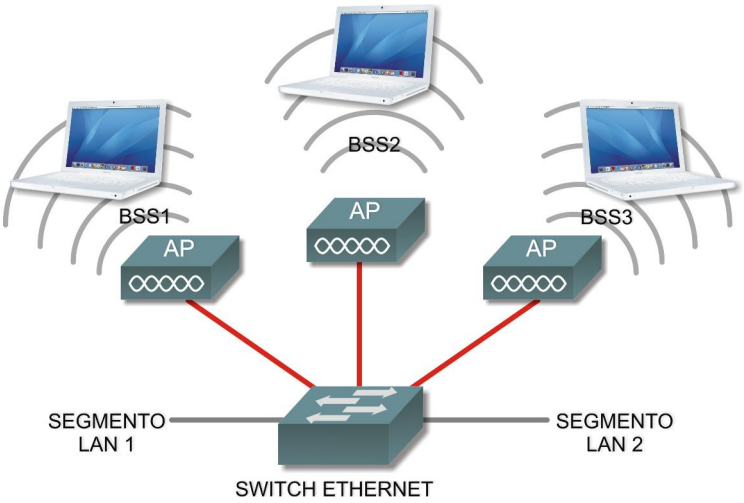
1.3 CARACTERIZACIÓN DE LAS ARQUITECTURAS

Una vez clasificadas las arquitecturas en tres grandes grupos, se expondrán a profundidad las particulares de cada una de ellas.

1.3.1 Arquitectura Autónoma:

La figura 1 muestra un ejemplo de una red Autónoma. Esta arquitectura implementa toda la funcionalidad en un único dispositivo físico, el Punto de Acceso AP. En este caso el AP traduce frames 802.11 a/desde su interfaz de radio y tramas 802.3 a/desde una interfaz Ethernet. También puede proporcionar portales para la integración de segmentos de LAN 802.3.

Figura 1. Ejemplo de una arquitectura autónoma



Fuente: CAPWAP.Architecture Draft

Un solo dispositivo AP, puede opcionalmente ser administrado como múltiples APs virtuales soportando múltiples SSID para que los clientes puedan ser asociados. En algunos casos esto implicará poner una etiqueta del tipo 802.1Q VLAN en cada paquete transmitido a la infraestructura de Ethernet y la eliminación de etiquetas 802.1Q antes de transmitir los paquetes hacia el medio inalámbrico.

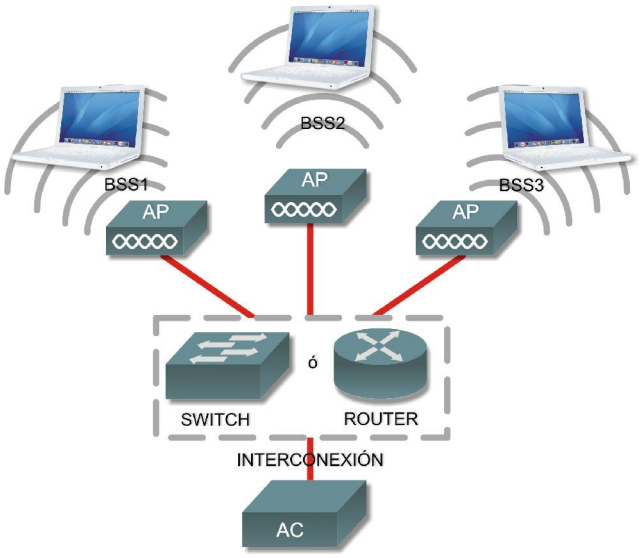
La interconexión de varios conjuntos de servicios básicos BSS, se confinará con base a las limitaciones impuestas por la infraestructura de Ethernet.

La autenticación de clientes pueden ser llevadas a cabo a nivel local por el Punto de Acceso AP o usando un servidor de autenticación centralizada. Dado que tanto las funciones y servicios están estrechamente integrados en un único dispositivo físico, las cuestiones de seguridad con esta arquitectura se limitan al AP. Este punto de conexión se vale de las técnicas empleadas por el estándar 802.11i para la autenticación de clientes. No obstante, es necesaria la autenticación mutua entre el AP y la infraestructura Ethernet, esto puede lograrse mediante el empleo de mecanismos existentes, tales como 802.11x permitiendo de esta forma la verificación mutua a las parte interesadas (el AP y el conmutador Ethernet a la que se conecta).

Otro aspecto importante y poco considerado, es el de la seguridad física del dispositivo, sobre todo porque allí se concentra la información relacionada a la gestión (SNMP) y a la seguridad (AAA). El robo de estos dispositivos, podría comprometer la red cableada.

1.3.2 Arquitectura Centralizada:

Figura 2 Esquema de la Arquitectura Centralizada



Fuente: CAPWAP Architecture Draft

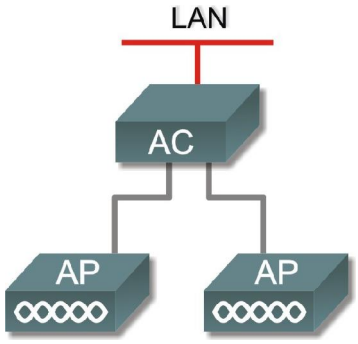
La arquitectura centralizada es relativamente nueva en el mercado de la familia WLAN. Contrariamente a la arquitectura autónoma, donde las funciones 802.11 y las funciones de control se manejan en un solo punto de terminación (AP), esta arquitectura dispone de uno o más controladores centralizados, denominados Controladores de Accesos (AC), permitiendo así, optimizar la supervisión, la escalabilidad en la gestión, y por consiguiente la dinámica de configuración.

La figura 2, exhibe el diagrama de la arquitectura centralizada de red, donde el controlador de acceso (AC) se conecta a múltiples puntos de acceso (APs) a través de un medio de interconexión. Este enlace puede realizarse con una conexión directa, o a través de un switch, o un router. El AC intercambia información de configuración y control con los dispositivos AP, proporcionando un punto centralizado para la gestión de la red.

A pesar que el AC se concibe como una sola entidad que ofrece las funciones de control, esto no necesariamente tiene que ser así. Es claro que este tipo de funciones demandan ciertos recursos en cuanto a CPU, memoria, almacenamiento, entre otros, por lo que se hace necesario distribuir roles u oficios entre los dispositivos que la componen la red.
En este orden de ideas, la entidad de red "AC", debe ser pensada como una multiplicidad de funciones lógicas, y no necesariamente como un único dispositivo físico. Los AC pueden optar también por aplicar algunas funciones de control a nivel local, y proporcionar interfaces para acceder a otras funciones globales de gestión de red, tales como SNMP Network Management Station y AAA de servidor (por ejemplo, autenticación Radius Server).

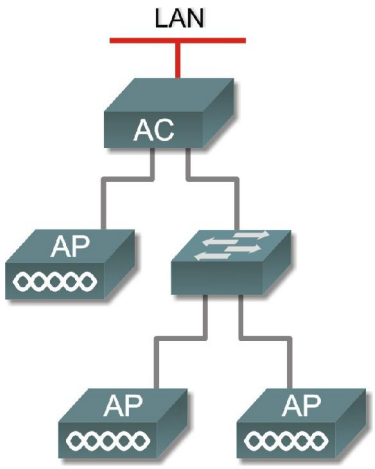
En lo que a la conectividad entre el AC y el Punto de Acceso se refiere, se ilustrará a continuación las diferentes alternativas:

Figura 3 Conexión Directa entre el AC y los APs



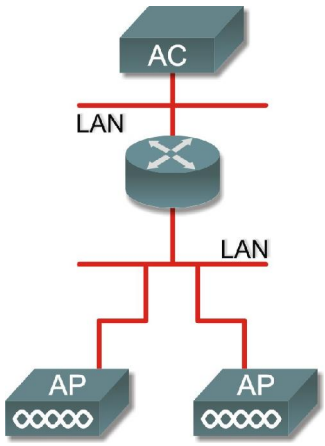
Fuente: CAPWAP Architecture Draft

Figura 4 Conexión conmutada



Fuente: CAPWAP Architecture Draft

Figura 5 Conexión con Router



Fuente: CAPWAP Architecture Draft

Uno de los aspectos más relevantes de las redes empresariales, es la gestión de las mismas, consecuentemente con ello, esta arquitectura propone algunas variantes con el objeto de atender distintos escenarios de despliegue, éstas se conocen bajo el nombre de MAC Local, MAC Dividida y MAC Remota.

Como se ha señalado a lo largo del capitulo, estas opciones son el resultado directo de la flexibilidad inherente al estándar 802.11 sobre la aplicación de las funciones lógicas que, a grandes rasgos se describe bajo el término "Punto de Acceso (AP)".

Lo que seguidamente se definirá hace parte de la recopilación que los diferentes proveedores han hecho a este esquema. La figura 6, ilustra la forma como cada alternativas precisa las funciones de control.

1.3.2.1 MAC Local.

El propósito principal de este modelo, es mitigar la carga de las políticas de acceso y las funciones de gestión de red sin dividir la funcionalidad MAC entre los dispositivos, tal y como se muestra en la figura 6.

Las primitivas MAC reside en los APs a nivel local, incluida la gestión y control de procesamiento de frames para las estaciones. Por otro lado, la información relacionada con la gestión y configuración de los Access Point se maneja como un servicio centralizado del AC, simplificando la administración del sistema y perseverando la coherencia de configuración de los dispositivos AP en la red.

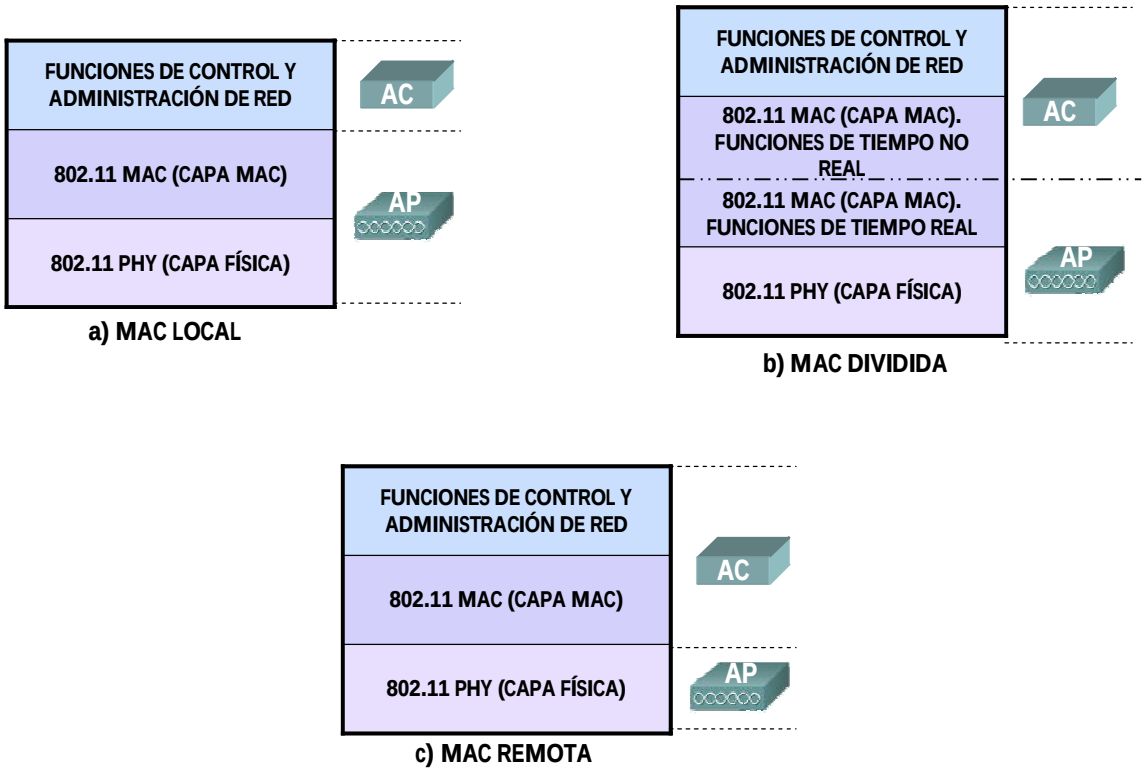
En este perfil, la conectividad entre el AP y el AC es de tipo capa 3. La gestión y el control de frames y todo lo que ese proceso conlleva se realizan a nivel de Punto de Acceso, esto hace referencia al control de acceso al medio utilizando tramas RTS, CTS y ACK. La agregación y entrega de frames de datos de una estación a otra (posiblemente a través de un DS) pueden ser enrutados a través del AC, lo que implica que el AC también actúa como router de acceso para esta red de acceso WLAN. Sin embargo existe otra alternativa donde la estación puede ser “puenteada” o enrutada localmente, sin dejar de mantener el control centralizado en la AC.

Las funciones y servicios de control y gestión de red, se aplican al AC con la ayuda de los Puntos de acceso para vigilar los canales de RF, y recopilar estadísticas e información de estado de la estaciones, ya que el AC ofrece las ventajas de visibilidad de toda la red, lo cual es esencial para de los servicios de control y configuración entre otros.

Asimismo, las funciones 802.11 se aplican en los Puntos de Acceso, no obstante, algunos proveedores difieren en la distribución de servicios, la programación de 802.11e (QoS), y 802.1X/EAP (autenticación). La diferencia en la distribución de servicio es coherente con el descrito anteriormente con respecto a la agregación y entrega de datos.

La tabla 1, resume las funciones que cada dispositivo a nivel lógico realiza en el modelo de MAC Local.

Figura 6 Variantes de la Arquitectura Centralizada



Fuente: CAPWAP Architecture Draft

1.3.2.2 MAC Dividida

Como se muestra en la Figura 6 (b), las funciones MAC se distribuyen en dos dispositivos, el AC y el AP. El Controlador de Acceso (AC) se encarga de las funciones de "tiempo no real" como parte de su servicio centralizado, conjuntamente con los ya mencionados de gestión y el control. Asimismo, las funciones de configuración, calidad de servicio QoS, balanceo de cargas y listas de control de acceso son manejadas por esta misma entidad.

Por otra parte, el AP administración las funciones de "tiempo real", provee conectividad y gestión del medio de transmisión y termina la infraestructura del enlace físico inalámbrico.

De acuerdo con lo expuesto, la diferencia fundamental entre la arquitectura local y la dividida, esta relacionada con las funciones de "tiempo no real". En este esquema, el AC termina las funciones de "baja criticidad", mientras que en la arquitectura local dichas funciones son terminadas por los AP enviando los mensajes apropiados al AC.

Tabla 1 Compendio de funciones del modelo MAC Local

FUNCIONES		
Procesamiento de frames de control.	✓	
Monitoreo RF	✓	✓
Base de Datos de estado	✓	✓
Autenticación de dispositivos. Mutuo	✓	✓
Generación de frames de admin	✓	
Configuración RF		✓
Actualización de firware AP		✓
Control de Energía	✓	
Fragmentación/Desfragmentación	✓	
Disociación/Asociación/Reasociación	✓	
Servicio de Integración	✓	
Servicio de Distribución		✓
Configuración de APs		✓
Control y administración de red		✓

Fuente: Autores del proyecto

Con base a lo anterior, se hace necesario definir cuales son las funciones de tiempo real y cuales no lo son. Cabe aclarar, que no existe una definición explícita en el estándar con relación a dichas funciones MAC. Sin embargo, el grupo IETF precisó, teniendo en cuenta a los proveedores de esta tecnología, los siguientes servicios de "tiempo real", aplicados en los Puntos de Acceso:

- Generación de BEACONS (tramas de administración)
- Prueba: Respuesta/Transmisión
- Procesamiento de frames de control RTS/CTS/ACK/PS-Poll/CF-End/CF-ACK
- Sincronización
- Retransmisiones
- Tasa de transmisión de adaptación

La siguiente lista son las funciones de “tiempo no real”:

- Autenticación / Des-autenticación
- Asociación / Disociación / Reasociación / Distribución
- Servicios de Integración: Puente entre 802.11 y 802.3
- Privacidad: 802,11 Cifrado / descifrado
- La fragmentación / desfragmentación

Sin embargo, algunos proveedores pueden optar por clasificar algunas de las anteriores funciones de "no-tiempo real" como funciones de tiempo real con el fin de apoyar aplicaciones específicas con requisitos estrictos de calidad de servicio QoS. Por ejemplo, a veces la reasociación es implementada como una función de apoyo de "tiempo real" para la Voz sobre IP (VoIP).

Este enfoque ha tenido gran aceptación, pues entre sus ventajas se encuentra el manejo preferencial que se les confiere a los servicios susceptibles a latencias, es decir aquellos que no pueden tolerar retrasos debido a la transmisión de tramas de control (o de algún tipo de información) a lo largo de múltiples saltos. Esto por consiguiente conlleva a otro beneficio ya que mitiga las labores del Punto de Acceso.

Finalmente, gracias a que las funciones de cifrado y des-cifrado no residen en el Access Point, se reducen las vulnerabilidades del mismo, facilitando la creación de nuevos esquemas de seguridad en el AC que simplifiquen la gestión y actualización de tareas.

La interconexión entre APs y ACs es del tipo capa 3, no obstante se aceptan las conexiones conmutadas debido a los limitantes de los retrasos, consecuencia de dividir MAC entre dos entidades físicas a través de una red.

La siguiente tabla (Tabla 2), sintetiza las funciones de cada dispositivo.

Al igual que en la Arquitectura MAC local, la mayoría de las funciones de control se aplican al AC. A excepción del seguimiento de RF y, en algunos casos la configuración RF, que se realizan a nivel local en los APs.

Tabla 2 Síntesis de funciones del modelo MAC Dividida.

FUNCIONES	AP	AC
Procesamiento de Frames de control	✓	
Monitoreo RF	✓	
Base de Datos de estado de las STAs		✓
Autenticación de dispositivos. Mutuo	✓	✓
Generación de frames de admin	✓	
Configuración RF	✓	✓
Actualización de firware AP		✓
Control de Energía	✓	
Fragmentación/Desfragmentación	✓	✓
Disociación/Asociación/Reasociación		✓
Servicio de Integración		✓
Servicio de Distribución		✓
Configuración de APs		✓
802.1x/ EAP. Autenticación y gestión de claves		✓

Fuente: Autores del proyecto

1.3.2.3 MAC Remota

Este enfoque es llamado MAC remota porque separa las funciones de capa física (PHY) de las funciones MAC en lo que a dispositivos se refiere, ver figura 6, es decir mantiene los APs con la menor carga posible, cediendo al Controlador el conjunto de funciones MAC (incluida las susceptibles a retrasos) y por consiguiente dejando todas las complejidades de la MAC y las funciones de control en general al AC.

El Access Point actúa sólo como un canal entre los clientes de la LAN inalámbrica (STAs) y el AC, definiendo las características y métodos de transmisión y recepción, así como la adecuación de las capacidades del sistema para el servicio MAC. No obstante pueden asumir características adicionales para convertir los frames de un formato (802.11) a otro (puede ser Ethernet).

A nivel del Controlador se encuentra que entre sus labores, al igual que en las propuestas anteriores, están:

- Monitoreo y control de red
- seguridad.
- Gestión de los recursos
- Selección del canal de comunicaciones.
- Calidad del servicio a los usuarios.

Este tipo de arquitectura se despliega con especial atención a la conectividad entre los APs y el o los AC(s) a fin de que la demora se reduzca al mínimo.

Si bien, se presentaron tres orientaciones diferentes con respecto al manejo de la arquitectura centralizada en lo referente a las funciones 802.11, existen elementos comunes entre ellas:

- La mayoría de las funciones relacionadas con control de la red y la configuración residen en el AC.
- La capa física se establece en el Access Point.

Hay una clara diferencia entre los enfoques de MAC Local y Dividida con respecto al esquema de MAC Remota, las primeras mantienen una porción de las funciones MAC y las funciones de capa físicas en los APs. El impacto de esta separación se ve reflejado en el tipo de interconexión entre APs y ACs.

La ventaja de la Arquitectura MAC Remota es que no requiere de APs tan robustos, pues sus funciones se encuentran confinadas a la capa física (conectividad y soporte para la capa MAC).

La similitud de la MAC Local y la MAC Dividida está en el manejo de los frames de control, en ambos casos se da en el Access Point. La principal diferencia está en que el AP en la MAC Dividida es quien termina el procesamiento solo de los marcos control, mientras que en el esquema de MAC Dividida el AP finaliza todos los procesos de los diferentes tipos de frames. Una interesante consecuencia de esta diferencia es que la integración de servicios, que esencialmente se refiere a la vinculación entre 802.11 y 802.3, es ejecutado por el AC en el enfoque de MAC Dividida y por el AP en el MAC Local.

Asimismo, el Servicio de Distribución, aunque se atribuye siempre al AC, éste puede igualmente ser aplicado al AP en algunas arquitecturas locales, incrementándose así el rendimiento en la entrega de tráfico de datos, hacia y desde las estaciones (STAS), evitando túneles de comunicación con el AC, y disminuyendo la dependencia del AP con respecto al AC.

Aunque todo el tráfico 802.11 se agrega a los AC en el caso de la MAC Dividida, el plano de datos y control puede ser separado mediante el empleo de múltiples AC.

Un AC puede aplicar la mayoría de las funciones de control, mientras que otros ACs pueden encargarse de los frames de datos.

Cada una de las tres variantes de la arquitectura centralizada puede ser favorable para ciertos escenarios. La clave está en determinar el equilibrio deseado para centralizar o no ciertos servicios. El impacto de dicho equilibrio en la capacidad de administración de red es actualmente motivo de controversia dentro de la comunidad técnica.

Hasta el momento, solo se han presentado las funciones que desempeñan el AC y el AP de acuerdo al enfoque que se prefiera. Ahora bien, es igualmente importante conocer cómo estos dispositivos se comunican entre si.

Antes de que los mensajes puedan intercambiarse entre un AC y un AP, el Access Point necesita descubrir, autenticarse, y registrase primero con un AC, luego descarga el firmware y por último establecer un canal de control con el AC. Una vez se determina este canal se promueven los mensajes de configuración y control

La siguiente lista describe las operaciones básicas que suelen realizarse entre el AP y el AC:

1. Descubrimiento: El AP descubren el AC con el que quedarán ligado y por el cual será controlado. El procedimiento de descubrimiento puede emplear ya sea configuración estática o dinámica. En este último caso, un protocolo se utiliza para que el Access Point pueda descubrir el AC (s) candidato.

2. Autenticación: Después del descubrimiento, el AP se autentica con el AC y este último es autenticado también por el AP, sin embargo esto de la autenticación mutua no es ampliamente apoyado por algunos proveedores, ya que ellos prefieren baja carga de configuración en el AP. Esto no es recomendable en términos de seguridad pues deja la posible vulnerabilidad del AP atribuido a un AC.

3. Asociación: Después de la autenticación, el AP se registra con el AC con el fin de empezar a recibir la gestión y la configuración de mensajes.

4. Descarga de Firmware: Una vez asociado el AP puede ordenar, o el AC forzar el firmware, este puede ser protegido como la firma digital.

5. Establecimiento de canales de control: El AP establece ya sea un túnel IP, o realiza encapsulación Ethernet con el AC, para de transferir el tráfico de datos y frames de gestión.

6. Configuración de descarga: Tras el establecimiento de canales de control de proceso, el AC pueden imponer parámetros de configuración para los APs.

Dada la variada distribución de funcionalidades para la arquitectura centralizada, se hace necesario recurrir a técnicas avanzadas de seguridad, donde se manejen los siguientes parámetros:

- Seguridad de los datos de clientes
- Control de Seguridad de canal entre el AP y el AC
- Seguridad física de APs y ACs.

Seguridad de los datos de clientes:

El cifrado 802,11 [x] pueden aplicarse ya sea en el AP o en el AC. Por otra parte, la funcionalidad 802.1X/EAP [x] se distribuye entre el AP y el AC cuando, en la mayoría de los casos, el AC lleva a cabo las funciones necesarias como la autenticación 802.1X en el intercambio de mensajes y/o datos.

Si la estación (STA) y el AC hacen parte del intercambio de mensajes de cuatro vías “four-way hadshake”, es decir si la estación solicita abrir una sesión, entonces el Pairwise Transient Key (PTK) que es la clave que se establece entre en las parte interesadas y se renueva constantemente, tiene que ser transferido del AC al AP. Dado que el material clave (la llave de la sesión) es parte del control y la provisión del AP, se debe emplear un túnel cifrado para transportar dicha clave. Estos algoritmos de encriptación y técnicas basadas en claves se explicarán con mayor detenimiento en el capitulo 2.

Este modelo centralizado alienta implementaciones AC para utilizar claves del tipo Pairwise Master Key (PMK) para diferentes Acces Point. Esta práctica facilita la rápida transición de una STA de un AP a otro que está conectado al mismo AC sin establecer una llave PMK. Sin embargo, esto deja a la estación (STA) en una posición difícil, ya que la STA no puede distinguir entre un acuerdo PMK y uno que es intencionalmente compartido. Esta situación aún se encuentra en estudio.

Cuando el cifrado/descifrado (802.11i) se realiza en el AC, el intercambio de claves y de transiciones de estado se origina entre el AC y la estación (STA) directamente. Por lo tanto, no hay necesidad de la transferencia de cualquier material encriptado entre el AC y el AP.

Independientemente de que el cifrado se de en el AP, la arquitectura WLAN centralizada registra dos prácticas para la seguridad de los datos en redes cableadas. En algunos casos se establece un túnel encriptado (IPsec o SSL) entre el Access Point y el Controlador, lo que supone que el límite de seguridad está en el AC. Otra opción, es crear un túnel VPN que se proyecte entre el cliente y un AC.

Control de Seguridad de canal entre el AP y el AC:

Con el propósito de cumplir este ítem, se llevan a cabo los siguientes mecanismos de seguridad:

1. Descubrimiento seguro del AP a su AC asociado.
2. Autenticación del AP con su respectivo AC (y posiblemente autenticación mutua).
3. Confidencialidad, integridad y protección del canal de control de frames.
4. Una gestión segura de APs y ACs.

El descubrimiento y la autenticación de APs se manipulan con herramientas como los certificados X.509, la autenticación AAA y la autenticación de credenciales (pre-shared).

En todos los casos, la confidencialidad, integridad y protección contra ataques del tipo “hombre en el medio” de los frames de control, están dirigidas por un túnel cifrado entre el AP y el AC, utilizando claves derivadas de los métodos de autenticación enunciadas anteriormente.

Seguridad física de APs y ACS:

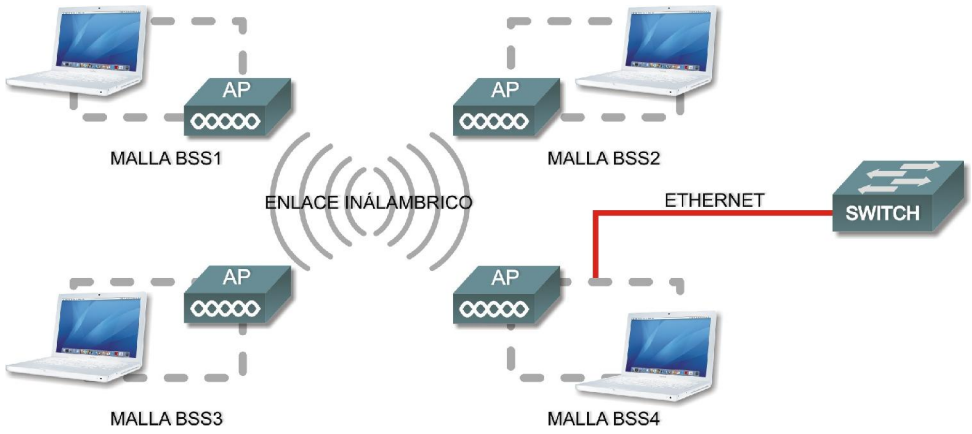
Para proporcionar cobertura de radio, los APs se instalan con frecuencia en lugares que son difíciles de proteger físicamente, pero si se emplean servidores RADIUS para los servicios de autenticación y soporte de seguridad, entonces la pérdida física de un AP no pondría en peligro esa información sensible (claves y usuarios).

1.3.3 Arquitectura Distribuida:

En esta arquitectura los nodos de malla en la red puede actuar como APs para estaciones cliente en sus respectivos BSS y proporcionar una mayor cobertura inalámbrica, así como enlaces para el tráfico a nodos vecinos a través de conexiones inalámbricas. También es posible que algunos nodos de malla en la red puedan servir sólo como enlaces inalámbricos de tráfico para otros nodos de malla, pero no como APs para cualquier estación cliente. En lugar de hacer conexiones del tipo Ethernet para cada AP, las mallas de redes inalámbricas ofrecen una alternativa atractiva a la transmisión de datos en el tráfico.

Dichos nodos pueden hacer un seguimiento del estado de sus nodos vecinos, o incluso más allá de sus nodos adyacentes, intercambiando información periódicamente entre ellos; De esta forma, ellos logran ser plenamente “conscientes” de la topología dinámica de la red y de las condiciones que les rodea

Figura 7 Ejemplo de una Arquitectura Distribuida



Fuente: CAPWAP Architecture Draft

La comunicación peer-to-peer permite a los nodos coordinar entre sí la auto-configuración y auto-restructuración. Esta es la principal diferencia entre la arquitectura distribuida de malla y la arquitectura centralizada, pues gran parte de las funciones de control y administración se pueden aplicar a través de la malla de nodos distribuidos sin la intervención de una entidad centralizada que tome el control de todas las decisiones.

Cabe señalar que las redes de malla no excluye necesariamente el uso de un control centralizado. Es posible que una combinación de centralización y control distribuido co-existan en este tipo de redes. Alguna configuración global o cambio de política puede ser mejor servido de manera coordinada por algún tipo de controlador de acceso (AC) disponible en la malla de red (incluso un AC, que no posea las características tal como se define en la arquitectura centralizada). Por ejemplo, una entidad de gestión centralizada se puede utilizar para actualizar la configuración por defecto de todos los nodos. Igualmente, puede ser más conveniente dejar ciertas funciones como la autenticación de usuarios a un único punto centralizado (como un servidor RADIUS), donde cada AP de malla, hable directamente con el servidor RADIUS, eliminando un único punto de falla y aprovechar mejor las estaciones de la red.

La comunicación de las mallas con la red LAN puede ser a través de un dispositivo capa 2 o capa 3, ver figura 7. Hasta donde se conoce, los vendedores están utilizando las tecnologías patentadas de malla en lo referente a los enlaces inalámbricos para que pueda existir comunicación peer-to-peer entre nodos de la malla. Por lo tanto, no existe una malla interoperable entre nodos de diferentes

fabricantes. El IEEE 802,11 WG inició un nuevo grupo de trabajo (GTs) en el 2004 para definir la malla estándar de 802.11.

A nivel de seguridad, la principal preocupación se encuentra en los datos del cliente y se aplican las mismas herramientas descritos en la arquitectura centralizada. Otra importante consideración de seguridad para las redes de malla, es que los nodos deben autenticarse mutuamente dentro de un mismo dominio administrativo. Para proteger a los usuarios y la gestión de datos entre nodos vecinos se debe emplear un mecanismo de capa 2 que ofrezca confidencialidad, integridad y protección de los servicios.

En conclusión podemos definir las tres categorías de la siguiente forma:

1. Autónoma: Propone una estructura donde las todas las funciones 802,11, y en caso de ser aplicable, las funciones de control se llevan a cabo en los APs.

2. Centralizada: Indica una familia de arquitecturas en las que las funciones se encuentran divididas entre el AP y el AC, donde el Controlador actúa como un punto de control centralizado para múltiples APs.

3. Distribuida: Plantea que parte de las funciones de control se ejecuten a través de una red distribuida de entidades pares.

Si bien se expuso este grupo de arquitecturas con un modelo funcional que permite de una u otra forma la integración de las redes inalámbricas WLAN a las redes LAN la decisión de escoger una con respecto a otra depende del entorno donde se pretenden adecuar.

Otro aspecto importante es la interoperabilidad entre equipos de diferentes fabricantes. La adopción de alguna de las opciones presentadas también depende de ello, sin embargo el estándar IEEE 802.11 y el grupo de trabajo del IETF están trabajando en la elaboración de normas y medidas para superar estos percances.

2 SEGURIDAD EN REDES INÁLAMBRICAS

El capítulo 1, presentó una serie de topologías a nivel físico que pretenden facilitar la integración de las redes inalámbricas con las redes cableadas ya existentes en entornos empresariales. Como se expresó al final del mismo, la elección de alguna de las arquitecturas depende de las necesidades y servicios así como las aplicaciones que la organización brinde a las estaciones y usuarios en general. Sin embargo, la adición de nuevos dispositivos a las actuales redes, trae consigo un conjunto de requerimientos esenciales para permitir su adaptación y que a su vez facilite a los administradores mantener el control y minimizar los riesgos de esta nueva implementación.

A nivel de riesgos en seguridad de redes inalámbricas, se da por manifiesto que estos equivalen a la suma de los inherentes a una red cableada y los nuevos generados por la portabilidad de los dispositivos inalámbricos. Para aminorar estos impactos, las organizaciones necesitan adoptar medidas de seguridad y prácticas que ayudan a reducir sus riesgos a un nivel manejable. Todas las características pertenecientes a la seguridad inalámbrica deberán ser configuradas en conformidad con la política de seguridad de la organización.

Por lo tanto la confidencialidad, integridad y autenticidad deben abordar las necesidades centrales de gestión, seguimiento y control de los puntos de acceso inalámbrico en conjunto con la red cableada. Igualmente, la seguridad física también debe abordarse para aquellos dispositivos que contienen los parámetros de seguridad que puedan comprometer al sistema, si esos parámetros fueron a caer en manos de un atacante.

Si se mira el principio de funcionamiento de estas redes, uno de los factores que más llama la atención de las WLAN es la facilidad de la conectividad, ya que solo es necesario estar dentro del rango de acción del punto de acceso para poder utilizar sus servicios. Esta flexibilidad a su vez, es la mayor debilidad en términos de seguridad de la información que por ella circula. Como es bien sabido, las redes inalámbricas permiten una gran movilidad al usar radiofrecuencia para propagar la información, esto hace que la señal que contiene la información no esté confinada ni a un computador ni a un área específica, pudiendo ser interceptada a varios metros de distancia disponiendo únicamente, en el mejor de los casos, de un computador y una buena antena si el Punto de Acceso no presenta protección alguna.

El contenido de este capítulo, aborda un compendio de las características más relevantes en seguridad para cualquier topología de WLANs, comenzando con los aspectos básicos que atañen a cualquier sistema en temas de seguridad y finalizando con los mecanismos actualmente empleados en soluciones inalámbricas.

2.1 VUNERABILIDADES DE LAS REDES INALÁMBRICAS

Dado que la implementación de seguridad en redes inalámbricas es relativamente nueva y que los protocolos de seguridad más usados no son los más seguros, esto hace que las redes WLAN sean vulnerables a ataques de personas con conocimientos especializados en el tema que cuentan con la capacidad de explotar estas vulnerabilidades.

Igualmente, en lo concerniente a la configuración usada en las redes WLAN también existen numerosas debilidades, ya que en la mayoría de las ocasiones las compañías o los encargados de la administración de una WLA no usan estrategias de seguridad en todos los equipos pertenecientes a la red.

Asimismo, el desconocimiento de los estándares y de la tecnología en sí, hace que se presenten debilidades en el diseño de las políticas de gestión y por consiguiente se evidencia poca claridad en la administración de las mismas.

Es precisamente esta falta de precisión en los procesos de control de la seguridad, lo que permite la creación de los llamados “huecos” en las redes, facilitando la exploración por parte de personas externas a dichas infraestructuras.

A continuación se enumeran las principales vulnerabilidades de una red inalámbrica:

- Débil encriptación de los datos: Muchos AP usan WEP (Privacidad Equivalente a la Cableada) como mecanismo de seguridad, sin embargo se ha probado que es ineficaz en la encriptación de los datos.
- Autenticación únicamente de dispositivo: Las técnicas empleadas solo autentican los dispositivos clientes, no se autentica a los usuarios.
- Falta de integridad de los mensajes: Se ha probado que el Valor de Control de Integridad (ICV) no es efectivo como medio para asegurar la integridad de los mensajes.

2.2 AMENAZAS A REDES INALÁMBRICAS

Así como las redes WLAN presentan vulnerabilidades por fallas no solo a nivel administrativo sino a su vez tecnológico, igualmente presentan amenazas relacionadas precisamente con las vulnerabilidades de dichas redes.
¿Cuáles son estas amenazas?

- Amenazas por parte de novatos que utilizan herramientas de hacking, para encontrar claves y tener acceso a la red.
- Amenazas que provienen de hackers más capacitados y son conocedores de las vulnerabilidades de las WLANs y de las posibles estrategias para explotar estas flaquezas.

- Amenazas por agentes externos u organizaciones ajenas a la compañía, estos intentan acceder a la red principalmente desde el exterior del edificio como estacionamientos, edificios adyacentes o áreas comunes.
- Amenazas por agentes internos, estos hacen referencia a personal autorizado que tiene acceso a la red con una cuenta en un servidor o con acceso físico al cableado. La mayoría de los incidentes reportados en las WLANs son causados por malos manejos y accesos internos.

El acceso inalámbrico puede ser una gran amenaza a la seguridad de la red. La mayoría de las WLANs tienen pocas o ninguna restricción para usuarios internos. Una vez asociado a un Access Point, un atacante puede recorrer libremente WLAN de la compañía.

2.3 ATAQUES

Una vez establecidas e identificadas las vulnerabilidades y las amenazas de las redes inalámbricas, es conveniente identificar los tipos de ataques existentes como apoyo para la elaboración de políticas de gestión de la seguridad.
Obviamente, estos ataques se originan posteriores al reconocimiento de la red que desean transgredir. Estas acciones pueden ser del tipo pasivo o activo.

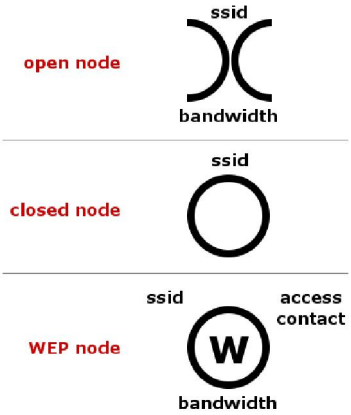
2.3.1 Ataques Pasivos

Los ataques pasivos son los más difíciles de identificar ya que el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información. Sus objetivos son la intercepción de datos y el análisis de tráfico.
Entre los ataques pasivos más conocidos y usados se encuentran:

- **Warchalking**

  El warchalking es un lenguaje de símbolos, normalmente escrito con tiza, en el cual una persona camina por la calle con su computador personal buscando redes inalámbricas, al encontrar una dibuja un símbolo en el piso o en una pared cercana.
  Dependiendo del símbolo se identifica si es un punto de acceso sin seguridad, con seguridad o con seguridad WEP. Aunque en este lenguaje existe una gran variedad de símbolos, cada uno con su significado particular, los tres más comunes y reconocidos son los mostrados en la Figura 8.

Figura 8 Simbología para reconocimiento de WLAN



Fuente: http://es.wikipedia.org/wiki/Warchalking

- **Wardriving**

  El término wardriving se refiere a la búsqueda de redes inalámbricas desde un vehículo en movimiento por medio de un dispositivo dotado de Wi-Fi, como un computador portátil o una PDA. Muchos practicantes de esta actividad usan GPS para ubicar la posición de los lugares con Internet inalámbrica y posteriormente registran estas ubicaciones en mapas de la ciudad o del sector en el que se hayan tomado los datos (Figura 9) y en muchas ocasiones registran estos mapas en un sitio web. El software necesario para este tipo de prácticas es de fácil consecución y se encuentra libremente en internet, siendo el mas conocida el Net Stumbler, el cual funciona en ambiente Windows.

Figura 9 Imagen satelital con ubicación de puntos de accesos

Fuente: http://www.home-network-help.com/wardriving.html

- **Espionaje**

  Es el ataque más simple que se puede realizar sobre una red inalámbrica. Consiste en observar el entorno y recolectar información relacionada con la topología de la WLAN, como localización de antenas, puntos de acceso, etc. Esta información puede ser usada posteriormente en ataques más estructurados. Para efectuar este ataque, únicamente es necesario tener acceso a la instalación en la que se encuentre la WLAN.

- **Escucha o sniffing**

  El sniffing o escucha es un ataque que tiene como fin obtener información, tales como MAC's, IP's origen y destino, contraseñas, claves WEP, etc.
  Este ataque es normalmente un paso previo a ataques activos posteriores como son la inyección y modificación de mensajes.

  Para llevar a cabo este ataque, se utiliza una tarjeta de red inalámbrica en modo promiscuo o modo monitor para poder recibir todo el tráfico que este circulando en ese momento por la red. Adicionalmente se necesita tener instalado algún programa "sniffer", los cuales monitorizan la información que circula a través de la red. Estos softwares son fácilmente encontrados y descargados de Internet. Este tipo de ataque resulta bastante sencillo y no requiere de conocimientos técnicos especializados. Algunos "sniffer's" conocidos son: Netstumbler, Airline, Airsnot, Kismet, por nombrar algunos.

- **Descubrimiento de contraseña**

  El objetivo de este ataque es descifrar la contraseña que un usuario legítimo utiliza para acceder a la WLAN, esto se logra, normalmente, después de llevar acabo durante cierto tiempo el proceso de escucha y recolección de información.
  Para obtener la contraseña se realizan principalmente dos tipos de ataques:

  - **Ataques por fuerza bruta.**

    En los ataques por fuerza bruta, el atacante intenta romper el cifrado mediante la prueba de todas las combinaciones posibles. Con este ataque es posible conseguir los nombres de usuario, las contraseñas de autenticación del usuario y las claves de los algoritmos de cifrado. Aunque el método siempre consigue su meta, su problema radica en el tiempo que se gasta en lograrlo, ya que con claves largas el número de combinaciones posibles, y por tanto el tiempo necesario, se eleva exponencialmente.

  - **Ataques diccionario.**

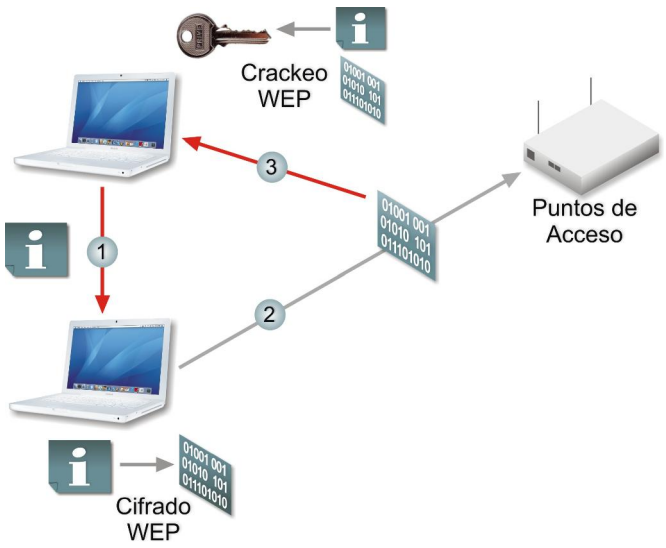
    En este ataque en lugar de intentar con todas las combinaciones posibles, como se hace en el ataque por fuerza bruta, se usan palabras probables, las cuales son tomadas de un diccionario de palabras y nombres. Si la clave

usada esta en el diccionario usado, se logra reducir considerablemente el tiempo de descubrimiento de la clave.

Estos dos tipos de ataques son los normalmente usados para descubrir claves de una WLAN que esté usando WEP como protocolo de seguridad.
Para lograr descubrir una clave WEP, se necesita un equipo con conectividad inalámbrica operando en modo promiscuo, capturando el tráfico de la red por medio de un software sniffer. El tiempo que se gasta en descubrir la clave WEP varia de acuerdo a la longitud de la clave y al hardware del equipo que se este usando para analizar la información capturada.

Los pasos para llevar a cabo del descubrimiento de una clave WEP son, normalmente, los siguientes:

Figura 10 Pasos para descubrir una clave WEP



Fuente: Autores del proyecto

1. Se realiza el envío de tráfico sin cifrar, a un usuario legítimo a través de la red WLAN.
2. El usuario legítimo cifra el tráfico y se lo envía al punto de acceso.
3. El atacante intercepta el tráfico cifrado, lo compara con su contenido y obtiene la clave WEP usada por el usuario legítimo.

2.3.2 Ataques activos.

Se denomina ataques activos a los ataques que implican la modificación en el flujo de datos o la creación de falsos flujos en la transmisión de datos. Pueden tener dos

objetivos diferentes: pretender ser alguien que en realidad no se es o colapsar los servicios que puede prestar la red.

- **Puntos de acceso no autorizados**

  Este ataque puede ser uno de los más perjudiciales para la seguridad de la red de la compañía, sin embargo es necesario tener acceso físico a la WLAN. Un punto de acceso no autorizado es un punto de acceso que se conecta sin permiso a la red existente.

  Este ataque permite el acceso a la red de la compañía a cualquier persona con posibilidad de acceso a una red inalámbrica y además vulnera todos los mecanismos basados en el cifrado de información entre extremos (WEP, WPA, etc), ya que el AP no autorizado se conecta físicamente a la red.

- **Spoofing**

  En un ataque de spoofing el atacante suplanta parámetros del usuario que permanecen invariantes antes, durante y después de la concesión de un privilegio, como son identificadores estáticos, credenciales y validadores.

  Para realizar ataques de este tipo es necesaria la realización con anterioridad de un ataque pasivo en donde se realice recopilación de información de la red a atacar. Mediante spoofing se puede suplantar la dirección MAC, la dirección IP, direcciones de correo electrónico, nombres de dominio y nombres de recursos compartidos. Mediante la suplantación de direcciones IP o MAC un atacante puede suplantar la identidad de algún usuario legítimo de la red WLAN.

- **Hombre en medio**

  En el ataque de hombre en medio (Man in the middle), el atacante intercepta los datos de la comunicación y selectivamente los modifica con el fin de suplantar la identidad de las personas implicadas en la comunicación. Es un ataque basado en el spoofing que consiste en interponerse entre dos sistemas. El agresor puede escuchar todos los mensajes intercambiados por las partes y los modifica sin que los extremos se enteren de que no se están comunicando realmente con quién creen.

  En redes inalámbricas se facilita la realización de este ataque, ya que una estación inalámbrica que transmite no detecta la presencia de estaciones adyacentes con la misma MAC o IP.

  Un caso muy frecuente es aquel en el cual, el atacante se hace pasar por un punto de acceso ante un usuario legítimo para conseguir credenciales válidas, luego de obtener la información emplea dos tarjetas de red inalámbricas, con una suplanta la identidad del punto de acceso ante un usuario final y, con la otra, suplanta la identidad de un usuario legitimo ante el verdadero punto de acceso.

- **Secuestro de sesiones**

  Este ataque al igual que el anterior se basa en spoffing. En el secuestro de sesiones el atacante se apodera de una conexión existente entre dos equipos. Monitorizando la red, el atacante esta en capacidad de generar tráfico que parezca venir de alguna de las partes involucradas en la comunicación robando de esta forma la sesión que mantenían las máquinas involucradas.

- **Denegación de servicio.**

  Es bastante diferente a los otros tres tipos de ataques tanto en la técnica usada como en el objetivo del ataque, ya que la intención en este caso, no es la de obtener información ni privilegios sino denegarlos y denegárselos no únicamente a los usuarios autorizados sino deshabilitar completamente los servicios del punto de acceso.

  El objetivo es impedir el funcionamiento de la red. El atacante usa, pasivamente, sin que los usuarios se den cuenta, gran cantidad de computadores generando cantidades gigantescas de tráfico hacia la red atacada, provocando que el punto de acceso se encuentre en imposibilidad de responder a esta gran cantidad de tráfico en la red y por tanto deniegue el servicio a los usuarios, tanto a los legítimos como a los ilegítimos.

2.4 MECANISMOS DE SEGURIDAD INALÁMBRICA

Para proteger la red contra ataques e intromisiones lo primero que debe establecerse es la adecuada ubicación de los Access Point, así como de las antenas de los mismos de tal forma que la señal inalámbrica se confine tanto como sea posible, tratando de que sean solo los usuarios deseados los que puedan ver la señal de radio.

Dado que confinar una señal de radio es bastante difícil y en ocasiones totalmente imposible, existen diversos mecanismos de seguridad para garantizar la seguridad de estas redes, a continuación se hablara de los más conocidos e implementados:

2.4.1 Filtrado de direcciones MAC

Este método consiste en la creación de una tabla de datos en los puntos de acceso a la red inalámbrica, esta tabla de datos contiene las direcciones MAC (Media Access Control) de las tarjetas que se pueden conectar a dicha red. Dado que la dirección MAC de una tarjeta de red es única se puede usar como método de autenticación.
Este método tiene varias desventajas entre las cuales se pueden nombrar:

- El aprenderse una dirección MAC no es fácil por lo que es necesario que el usuario sepa buscar su dirección dentro de su computador, lo cual no todos lo saben hacer.

- La dirección MAC es larga y su formato no es tan amigable, lo que puede ocasionar errores en la creación de las tablas.

- No es de fácil manejo en ambientes empresariales ya que cada vez que se introduce o se modifica un equipo hay que modificar o ampliar la tabla de datos, lo cual hace a esta técnica poco escalable y manejable.

- La dirección MAC viaja sin cifrar por el aire, lo que la hace vulnerable a que un atacante la capture y se identifique el mismo como propietario de esa MAC, variando el número MAC de su propia tarjeta de red, logrando de este modo hacerse pasar por un cliente válido.

- En caso de robo del equipo de un usuario, el ladrón dispondrá de la dirección MAC de un cliente válido con lo que podrá acceder a la red. En caso de robo de un Punto de Acceso el problema es mayor ya que el ladrón tendría acceso a las direcciones MAC de todos los usuarios legítimos de la red.

2.4.2 Protocolo WEP (Wired Equivalent Privacy)

El protocolo WEP o protocolo de privacidad equivalente a una red cableada forma parte de la especificación 802.11. Se diseñó para proteger los datos transmitidos en la red inalámbrica mediante cifrado. En el protocolo WEP se utiliza una clave estática tanto en las estaciones como en el punto de acceso, por lo tanto para autenticarse y entrar a la red se debe configurar la clave en el Punto de Acceso y posteriormente en el equipo del usuario.

EL protocolo WEP está basado en el algoritmo de cifrado RC4. Utiliza claves de 64 o 128 bits de los cuales 24 bits son para el vector de iniciación y los restantes corresponden a la clave.

Métodos de autenticación WEP

- Sistema de autenticación abierta

  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 método de Autenticación Abierta realiza el proceso de autenticación completo en texto abierto. En la Autenticación Abierta no hay una verificación del usuario o de la máquina. La Autenticación Abierta corresponde normalmente a un sistema de autenticación con clave WEP. Un cliente puede asociarse al Access Point con

una clave WEP incorrecta o incluso sin una clave WEP, sin embargo, el cliente con la clave WEP incorrecta no podrá enviar o recibir datos, ya que la carga de paquetes estará encriptada.

- Sistema de autenticación de clave compartida

El mecanismo se conoce como SKA (Shared Key Authentication), consiste en que: teniendo ambos dispositivos la misma clave de cifrado (WEP), el dispositivo transmisor pide al punto de acceso autenticarse, el punto de acceso le envía una trama al transmisor, si esta trama es correctamente codificada y devuelta, es posible establecer la comunicación. La clave compartida es vulnerable a un ataque por desconocidos, por lo que no es recomendada.

Estos mecanismos son poco fiables ya que no permiten la utilización de clave dinámicas. Poco tiempo después de ser presentado este protocolo se identificaron varias debilidades y fallos en su seguridad.

La principal desventaja del protocolo WEP es el uso de una pequeña clave estática de inicialización. La clave es introducida manualmente en el punto de acceso así como en cada dispositivo que vaya a acceder al él y no varía a menos que se modifique manualmente en todas las estaciones. Este proceso implica una labor bastante desgastante en ambientes empresariales donde se cuenta con muchos usuarios, razón por la cual, la clave no se renueva con frecuencia.

Otro aspecto importante está relacionado con la cantidad de tramas que pasan a través de un punto de acceso ya que estas son considerables. En ellas se pueden encontrar rápidamente dos mensajes con el mismo vector de iniciación y de esta forma lograr obtener la clave. Dado que ésta no es cambiada con cierta regularidad, un atacante que logre descifrar la clave obtendría acceso a la red por bastante tiempo, teniendo la posibilidad de efectuar una cuantía considerable de ataques o de reunir una cantidad muy significativa de información sin ser detectado ni bloqueado.

A pesar de estos inconvenientes, WEP incorporó a su esquema autenticación 802.1X, donde la estación cliente estaba obligada a solicitar acceso a la red utilizando EAP (Extensible Authentication Protocol, mencionado mas adelante)[1], tal como se establece en la norma. Sin embargo, esta solución no fue suficiente ya que sólo cubría las carencias en el ámbito de la autenticación, dejando sin resolver lo relacionado con la encriptación.

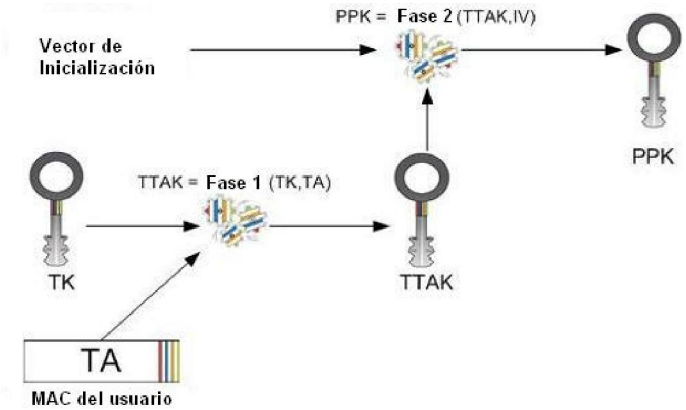
[1] EAP (Extensible Authentication Protocol): Extensión de Point-to-Point Protocol (PPP) que soporta múltiples métodos de autenticación, incluidos Kerberos, autenticación de clave pública (PKI) y tarjetas inteligentes. En 802.1X, EAP es encapsulado en el tráfico LAN o WAN, proporcionando el mecanismo para verificar la identidad de un usuario ante un servidor RADIUS u otra plataforma de autenticación.

En el año 2003 WEP fue reemplazado por WPA por presentar fallas en su objetivo de brindar seguridad. A pesar de esto WEP sigue siendo ampliamente utilizado y es la primera opción de seguridad que toman muchos propietarios para proteger sus redes inalámbricas.

2.4.3 Protocolo WPA (Wi-Fi Protected Access)

El protocolo WPA o Acceso Protegido Wi-Fi fue creado por la Alianza Wi-Fi (Wi-Fi Alliance). Debido a los errores encontrados por investigadores al protocolo WEP (como la reutilización del vector de iniciación) se ve la necesidad de sacar el protocolo WPA como medida intermedia y temporal mientras se concluía la implementación el protocolo 802.11i.
WPA es un estándar que opera a nivel MAC y está basado en un borrador del estándar IEEE802.11i. Aunque WPA tiene algunas carencias con respecto al definitivo IEEE 802.11i, los aspectos que se intentan optimizar mediante el uso de WPA son el proceso de autenticación y el de cifrado.
El protocolo WPA viene con distribución de claves dinámicas y un nuevo protocolo de autenticación más fuerte que su antecesor (WEP) con autenticación de usuario, característica con la que no contaba el protocolo WEP. Cuando es correctamente instalado este protocolo proporciona un nivel de seguridad bastante bueno, el cual asegura que la información estará protegida y que solo usuarios autorizados podrán acceder a la red.
WPA trabaja con el protocolo TKIP (Temporal Key Integrity Protocol), el cual es un esquema de encriptación más avanzado que el usado en WEP. TKIP inicia el proceso mediante una clave semilla de 128 bits compartida temporalmente entre los usuarios y los puntos de acceso. Después esa clave temporal se combina con la dirección MAC del usuario y se le añade un vector de inicialización de 16 bits para originar la clave que cifrará los datos, asegurando así que cada usuario manejará diferentes claves para la encriptación. Este procedimiento es mostrado en la Figura 11.

Figura 11 Manejo de claves por parte del protocolo TKIP



Fuente: http://www.vivasemfio.com/blog/category/tkip/

El protocolo TKIP junto al sistema de autenticación 802.1X/EAP emplean una jerarquía de clave que mejora la protección. También incluye el MIC (Message Integrity Check) o chequeo de integridad del mensaje, para la protección contra paquetes extranjeros a la red.

- **Encriptación en WPA**

El protocolo TKIP de WPA incrementa el tamaño de la clave a 128 bits y reemplaza el sistema de clave estática por un sistema de clave dinámica, la cual es generada y distribuida por el punto de acceso o el servidor de autenticación de la red. TKIP usa un manejo jerárquico de claves que elimina la posibilidad de descifrarlas de la forma en que se hacía en el protocolo WEP. El servidor de autenticación, después de aceptar la identidad del usuario usa el 802.1X para producir una única clave maestra o clave "pair-wise" para toda la sesión. TKIP distribuye esta clave al cliente y al punto de acceso e implementa una jerarquía de clave y un manejo de sistema usando la clave pair-wise para generar dinámicamente claves únicas y encriptar así cada paquete de datos que es transmitido durante la sesión. El manejo de clave jerárquico de TKIP cambia la clave estática usada en WEP por alrededor de 500 trillones de posibles claves las cuales pueden ser usadas en un paquete de datos.

El MIC o chequeo de integridad del mensaje fue diseñado para prevenir que un atacante capturara paquetes de datos, los alterara y los volviera a enviar. El MIC provee una función matemática fuerte en la cual el receptor y el transmisor calculan y comparan el MIC. De no concordar, se supone que el paquete fue alterado y es rechazado.

Incrementando el tamaño de las claves, el número de las mismas y creando un mecanismo de chequeo de la integridad, TKIP aumenta considerablemente la complejidad y dificultad la decodificación de datos en una red inalámbrica que implemente WPA. Igualmente incrementa la complejidad en la encriptación inalámbrica, haciendo más difícil que un intruso penetre en la red.

A pesar de que TKIP constituyó probablemente en su momento la mejor solución disponible, debía operar sobre el hardware entonces existente y, por tanto, no puede introducir encriptación avanzada si antes dicho hardware no se actualiza con más potencia informática.

- **Autenticación**

En WPA es posible emplear dos modos de autenticación diferentes, conocidos como entornos personales y entornos empresariales:

- Entornos Residenciales

Dado que en este contexto no es posible contar con un servidor de autenticación centralizado o un marco EAP, WPA se ejecuta en un modo especial conocido como “home mode” o Pre-SharedKey (PSK) que permite la utilización de claves configuradas manualmente y facilita así el proceso de configuración al usuario residencial.

El usuario debe introducir una contraseña, que puede estar entre 8 y 63 caracteres en su punto de acceso residencial, así como en cada uno de los dispositivos que desea conectar a la red WLAN. A esta contraseña se le conoce como clave maestra.

Esta contraseña permite, en primer lugar, conectarse a la red únicamente a aquellos dispositivos con la clave adecuada, lo que evita ataques basados en escuchas así como acceso de usuarios no autorizados, y en segundo lugar, la contraseña provee una relación de acuerdo único para generar el cifrado TKIP en la red.

Por lo tanto, la clave maestra inicial para la autenticación es compartida por todos los dispositivos de la red, más no las claves de cifrado, las cuales son diferentes para cada dispositivo, siendo esta una mejora con respecto al mecanismo WEP.

Estando en operación normal y transmitiendo datos, el protocolo WPA es mucho más seguro que WEP. Sin embargo, WPA-PSK muestra una vulnerabilidad, incluso mayor que la del protocolo WEP, en el instante inicial en que la conexión se establece, se puede obtener la clave maestra de cifrado inicial con tan solo un menor número de tramas capturadas. Sólo es necesario capturar las seis primeras tramas intercambiadas entre el dispositivo usuario y el punto de acceso inalámbrico para llevar a cabo el descubrimiento de claves por medio de ataques de diccionario y de este modo comprometer la estación del usuario.

Esta fragilidad se debe principalmente a que el sistema utilizado en el intercambio de información para la generación de claves es débil, especialmente cuando la longitud de la clave maestra manipulada es inferior a 20 caracteres.
Dicho inconveniente se presenta solo en el momento en el que la conexión se establece, de no ser así, no es posible deducir la clave empleada durante la conexión, ya que esta es dinámica y varía en función de parámetros intercambiados durante el proceso inicial. Por lo tanto, a pesar de esta vulnerabilidad, el protocolo WPA-PSK es más seguro que WEP.

- Entornos Empresariales:

  En estos ambientes, los requerimientos estrictos de cifrado y autenticación hacen que sea más adecuada la utilización de WPA con la autenticación 802.1X y con alguno de los protocolos de autenticación extensibles EAP.

  802.1X es un método de control de acceso al medio basado en puertos para redes cableadas e inalámbricas. EAP maneja la presentación de tarjetas de usuario, en forma de certificados digitales, nombres de usuarios y contraseñas únicas, tarjetas inteligentes, IS's de seguridad o cualquier otra credencial de identidad que el administrador de la red considere adecuado utilizar.

  En WPA, EAP se emplea como transporte extremo-a-extremo para los métodos de autenticación entre el usuario y los puntos de acceso, mientras que IEEE 802.1X se usa como marco para encapsular los mensajes EAP. En pocas palabras, IEEE 802.1x define cómo enviar EAP sobre la red.

WPA es flexible en cuanto a que tipo de credencial y el tipo de EAP a utilizar, con respecto a este último los proveedores lo utilizan como medio para comunicar peticiones de acceso entre el cliente y un punto de acceso, sin embargo el protocolo no describe como gestionar la autenticación misma, por ello cada fabricante ha optado por algunas de las extensiones propietarias que definen la tecnología sobre la que se soportará esta gestión, dando lugar a una serie de implementaciones acordes pero, en ocasiones, incompatibles entre sí.

Las más conocidas y usadas son EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security) y PEAP (Protected Extensible Authentication Protocol), sin embargo existe una gran variedad de ellas, a continuación se describirán algunas:

- **LEAP** - EAP Liviano [Lightweight EAP (LEAP)] 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 los protocolos de autenticación (EAP) pueden no proporcionar la funcionalidad que se necesita y ser demasiado exigentes. Esto podría comprometer el rendimiento del equipo WLAN, por lo tanto, LEAP es una buena opción cuando se utilizan equipos Cisco.
- **EAP-TLS** – EAP- Seguridad de Capa de Transporte [EAP-Transport Layer Security (EAP-TLS)] utiliza el certificado de autenticación por clave pública TLS lo cual provee autenticación del servidor al cliente y del cliente al servidor. Ambos, tanto al servidor como al cliente se les asigna un certificado digital asignado por una entidad certificadora en la que ambos confíen. EAP-TLS está basado en certificados X.509. Normalmente es más fácil de usar que PEAP.

- **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 (autenticación de clave pública) 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 del lado del cliente incluyen EAP-GTC para passwords ocasionales, así como EAP-MD5 para autenticación basada en password. PEAP está basado en EAP-TLS del lado del servidor y soluciona los defectos de administración y escalabilidad de EAP-TLS. 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.

- **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.

- **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.

- **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.

- **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.

- **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)].

En la Tabla 3 se muestra un resumen de los EAP más conocidos y usados, así como sus características, similitudes y diferencias.

Tabla 3 Tabla comparativa de los diferentes métodos de autenticación EAP

EAP	CARACTERISTICAS								
	Propietario	**Autenticación del servidor**	**Autenticación del cliente**	**Tunelado**	**Generación claves dinámicas**	**Seguridad de las credenciales**	**Re-autenticación rápida**	**Compatible con WPA**	**Riesgos no mitigados**
MD5	No	No	Password Hash	No	Si	No	No	No	Exposición de identidad Ataque de diccionario Hombre en medio Secuestro de sesiones
LEAP	Si	Password Hash	Password Hash	No	No	Débil	No	Si	Exposición de identidad Ataque de diccionario
TLS	No	Certificado X509	Certificado X509	No	No	Fuerte	Si	Si	Exposición de identidad
TTLS	No	Certificado X509	PAP, CHAP, MS-CHAPv2, cualquier EAP	Si	No	Fuerte	Si	Si	Ataque de diccionario
PEAP	No	Certificado X509	Cualquier EAP	Si	No	Fuerte	Si	Si	Ataque de diccionario
SIM	No	Pre-shared key / key derivation	Pre-shared key / key derivation	No	No	Fuerte	Si	Si	No independencia de la sesión. Ataques de 64 bits.

Fuente: Autores del proyecto

Es importante destacar que con EAP, 802.1X crea un framework en el cual las estaciones clientes pueden autenticarse mutuamente con el servidor de autenticación. Esta autenticación mutua previene que los clientes se conecten accidentalmente a un punto de acceso en el cual no estén autorizados y también asegura que el usuario que esté entrando a la red es efectivamente el que debe entrar a dicha red. Cuando un usuario solicita acceso, éste envía su credencial al servidor de autenticación, si el servidor acepta la credencial, la llave maestra TKIP es enviada tanto al cliente como al punto de acceso. Posteriormente viene un proceso en el cual el cliente y el punto de acceso se conocen e instalan las claves.

En resumen, casi cualquier clase de certificado tiene cabida bajo 802.11X, como también casi cualquier protocolo de autenticación. Por eso, conviene que, aunque el responsable de seguridad de una empresa vea la certificación en un determinado producto, antes de adquirirlo, pregunte al proveedor para qué soluciones y funcionalidades de otros fabricantes están certificadas sus implementaciones de 802.1X.

2.4.4 IEEE 802.11i

Este protocolo fue lanzado en septiembre de 2004 por WI-Fi Alliance. Al igual que WPA, 802.11i soporta autenticación IEEE 802.1X/EAP e incluye un nuevo y avanzado algoritmo de cifrado utilizando como protocolos CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) y, opcionalmente WRAP (Wireless Robust Authentication Protocol), ambos basados en el cifrado AES[2] de 128bits. Mecanismo de encriptación usando el protocolo Counter-Mode/CBC-MAC (CCMP) llamado el sistema de encriptación avanzado (AES).

Aunque AES es más complejo y no sufre los problemas asociados a RC4. Requiere una gran capacidad de procesamiento, lo cual hace que algunos equipos como PDA's, no sean capaces de soportarlo obligando a los fabricantes a cambiar el hardware para tal fin.

El elemento del estándar IEEE 802.11i que negocia dinámicamente los algoritmos de autentificación y de cifrado que se utilizarán para las comunicaciones entre los puntos de acceso y los usuarios inalámbricos es conocido como RSN (Robust Security Network). RSN utiliza AES (Advanced Encryption Standard), junto con IEEE 802.1x y EAP. El protocolo de seguridad que RSN construye sobre AES es el CCMP.

Una ventaja del estándar IEEE 802.11i es que la negociación dinámica de los algoritmos de autentificación y de cifrado permite a RSN evolucionar según el estado del arte de seguridad, agregando nuevos posibles algoritmos para tratar nuevas

[2] AES (Advanced Encription Standar): Es el protocolo de encriptación estándar de la Administración de Estados Unidos. Reemplaza a Data Encryption Standar (DES).

amenazas y proporcionando la seguridad necesaria para proteger la información enviada a través de redes WLAN.

Otra mejora de IEEE 802.11i con respecto a WPA es que IEEE 802.11i, soporte todo tipo de infraestructura incluyendo las redes ad-hoc. Además, a diferencia de WPA, el estándar IEEE 802.11i soporta handoff rápido seguro, característica importante para teléfonos VoIP que empleen IEEE 802.11. Por último, IEEE 802.11i permite la des-autenticación y disociación segura de la red.

Ahora bien, ¿cómo funciona este estándar en ambientes corporativos?

Básicamente, 802.11i incrementa la seguridad WLAN utilizando algoritmos de encriptación y técnicas basadas en claves más avanzadas ya enunciadas. Cuando una estación inalámbrica solicita abrir una sesión con el punto de acceso, se establece en ambos extremos una clave denominada Pairwise Master Key (PMK). Para ello se utiliza típicamente el estándar LAN y WLAN 802.1X, que permite al responsable de seguridad aplicar un método de autenticación tan potente como desee, desde las simples combinaciones usuario/contraseña hasta certificados digitales. Se trata de un mecanismo de autenticación de usuario basado en plataforma RADIUS (o cualquier otro servidor de autenticación) y en el protocolo Extensible Authentication Protocol (EAP). El servidor RADIUS retorna la PMK al punto de acceso, y, entonces, éste y la estación intercambian una secuencia de cuatro mensajes, denominada “four-way hadshake” (algo así como saludo o reconocimiento de cuatro vías)

Durante el proceso “four-way hadshake”, se utilizan la PMK y diversos valores generados aleatoriamente tanto desde la estación como desde el Punto de Acceso, renovándose varias veces durante la sesión para asegurar el acuerdo de una nueva clave, denominada Pairwise Transient Key (PTK). Ésta se compone a su vez de tres subclaves: una para firmar los cuatro mensajes que intervendrán en el proceso, otra para asegurar los paquetes de datos transmitidos entre los dos dispositivos implicados y una tercera para encriptar la llamada “clave de grupo”, que será enviada desde el punto de acceso a la estación y que permitirá difundir tráfico multicast a todos los clientes asociados al Access Point, evitando el envío independiente de paquetes encriptados de forma diferente.

A lo largo del proceso, estación y Punto de Acceso negocian también el tipo de encriptación que utilizarán para cada conexión. De esta negociación resultarán dos cifras. Una de ellas es la clave de grupo ya mencionada; la otra, denominada cifra o clave pairwise (reconocimiento de pareja), se utilizará para las transmisiones de datos en modo unicast que sólo afectan al punto de acceso. A este respecto, 802.11i ofrece una importante ventaja, ya que permite la negociación de cualquier cifra de encriptación, aunque la tecnología de referencia para la especificación sea AES con clave de 128 bits en modo CCM (Counter with CBC-MAC). En un entorno puro, AES será utilizado normalmente tanto para la cifra de pareja como de grupo. Sin embargo, en caso de que del Punto de Acceso dependan tanto dispositivos 802.11i como pre-

estándar (WEP, WAP), podrá funcionar utilizando AES en el caso de los primeros para la cifra pairwise pero aplicar el mínimo denominador común (RC4 o TKIP) para la clave de grupo. Así, todas las estaciones podrán desencriptar el tráfico multicast, garantizándose el funcionamiento de los nuevos sistemas en entornos mixtos.

Entre las ventajas que 802.11i aporta hay que destacar también su capacidad para acelerar el "roaming" entre Puntos de Acceso, además de contar con la técnica conocida informalmente como Opportunistic Key Caching o Proactive Key Caching para acelerar dicho proceso (roaming). Si se hace que múltiples puntos de acceso compartan claves PMK, la estación puede asociarse entre ellos y acceder a puntos que no haya visitado antes reutilizando la PMK establecida con el punto de acceso al que hubiera estado asociada con anterioridad. Con WPA era necesario que la estación realizara la autenticación 802.1X completa cada vez que se asociaba a un nuevo punto de acceso. Ahora, cuando un cliente wireless retorna a un Punto de Acceso con el que ya está autenticado, puede reutilizar la PMK acordada con anterioridad, omitiendo el proceso 802.11x y pasando directamente al diálogo four-way-handshake. Además, la estación puede pre-autenticarse en un punto de acceso al que tiene intención de asociarse, sin perder su relación con el de origen.

2.4.5 WPA2

WPA2 fue lanzado en septiembre de 2004 por WI-Fi Alliance. Este protocolo es la versión certificada e interoperable del estándar completo IEEE 802.11i. Al igual que WPA, WPA2 soporta autenticación IEEE 802.1X/EAP. Asimismo incluye el mecanismo de encriptación Counter-Mode/CBC-MAC Protocol (CCMP) mencionado anteriormente.

El protocolo 802.11i y el WPA2 son muy similares. Ambos emplean como código de cifrado AES/CCMP en lugar de RC4/TKIP usado en WPA y añaden, opcionalmente, pre-autenticación a WPA.
Una de sus diferencias es la interoperabilidad con WPA. Si la migración no es una preocupación entonces WPA2 funciona según lo definido en IEEE 802.11i. Por ejemplo, un punto de acceso y una tarjeta de usuario que trabaja solamente con CCMP en WPA2, funcionarán igualmente en IEEE 802.11i. Sin embargo, un punto de acceso que permite a usuarios con CCMP y TKIP, actuará en modo mixto, IEEE 802.11i y WPA. Esto permite a los usuarios anteriores de WPA asociarse a los nuevos puntos de acceso WPA2.

La segunda diferencia que se podría mencionar, es que WPA y WPA2 están dispuestos para ser implementados en entornos empresariales, pero carecen de ciertos aspectos con los que cuenta IEEE 802.11i para proporcionar servicios de voz inalámbricos, como prevenir la latencia de la señal o la pérdida de información durante el roaming antes mencionadas.

2.4.6 VPNs

De todos los mecanismos de seguridad expuestos en este capítulo, VPN presenta una opción si la empresa emplea accesos remotos, proporcionando una conexión que tiene la apariencia y muchas las ventajas de un enlace dedicado pero trabaja sobre una red pública. Para este propósito utiliza una técnica llamada entunelamiento (tunneling), de tal forma que los paquetes de datos son enrutados por la red pública (Internet o alguna otra red comercial), en un túnel privado que simula una conexión punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura.

Básicamente la utilización de una VPN consiste en encapsular los paquetes de datos que salen de una LAN o del equipo del usuario remoto dentro de protocolos que trabajan a nivel 2 o 3 del modelo OSI. El usuario únicamente puede comunicarse con la red corporativa a través del túnel establecido con el concentrador VPN.

Desde el punto de vista del modelo OSI, se puede crear una VPN usando tecnologías de capa 2 (enlace de datos) y de capa 3 (red). Dentro de la capa de enlace de datos están PPTP y L2TP y en la capa de red se encuentra IPsec. IPsec es un marco de estándares abiertos para asegurar comunicaciones privadas sobre redes IP ideado y administrado por la IETF para aportar seguridad al actual estándar universal IP. IPsec puede proteger cualquier protocolo que se ejecute sobre IP, por ejemplo TCP, UDP e ICMP. IPsec proporciona servicios criptográficos para autenticación, seguridad, control de acceso y de confidencialidad.

Además, IPsec proporciona privacidad y/o integridad de los paquetes IP. Los paquetes normales de IPv4 están compuestos de una cabecera y carga, ambas partes contienen información útil para el atacante. La cabecera contiene la dirección IP, la cual es utilizada para el routing o enrutamiento, y puede ser capturada para ser usada más tarde con técnicas de spooffing, por otra parte la carga está compuesta de información que se supone confidencial para una empresa o una organización.

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPsec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta. Para proteger la confidencialidad de los datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico. El estándar IPsec exige la implementación de NULL y DES (56 bit). En la actualidad se suelen emplear algoritmos más fuertes: 3DES (168 bit), AES (168/128, 192, 256 bits) y Blowfish.

Para desarrollar IPsec se necesita que cada usuario disponga de un usuario IPsec instalado, además de hardware adicional, un gateway o controlador VPN. Se utilizan diversos filtros para eliminar todo el tráfico que no provenga del gateway/controlador VPN o de los servidores DHCP o DNS. La arquitectura IPsec se describe en el RFC2401.

Para que los participantes de una comunicación puedan encapsular y des-encapsular los paquetes IPsec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en asociaciones de seguridad (SA - Security Associations). Cada asociación de seguridad define los siguientes parámetros:

- Dirección IP origen y destino de la cabecera IPsec resultante. Estas son las direcciones IP de los participantes de la comunicación IPsec que protegen los paquetes.
- Protocolo IPsec (AH o ESP). A veces, se permite compresión (IPCOMP).
- El algoritmo y clave secreta empleados por el protocolo IPsec.
- Índice de parámetro de seguridad (SPI - Security Parameter Index). Es un número de 32 bits que identifica la asociación de seguridad.

Las asociaciones de seguridad, a su vez, se almacenan en bases de datos de asociaciones de seguridad (SAD - Security Asocciation Databases). Algunas implementaciones de la base de datos de asociaciones de seguridad permiten almacenar más parámetros como son:

- Modo IPsec (túnel o transporte).
- Tamaño de la ventana deslizante para protegerse de ataques por repetición.
- Tiempo de vida de una asociación de seguridad.

En una asociación de seguridad se definen las direcciones IP de origen y destino de la comunicación. Por ello, mediante una única SA sólo se puede proteger un sentido del tráfico en una comunicación IPsec full duplex. Para proteger ambos sentidos de la comunicación, IPsec necesita de dos asociaciones de seguridad unidireccionales.

Las asociaciones de seguridad sólo especifican cómo se supone que IPsec protegerá el tráfico. Para definir qué tráfico proteger, y cuándo hacerlo, se necesita información adicional. Esta información se almacena en la política de seguridad (SP - Security Policy), que a su vez se almacena en la base de datos de políticas de seguridad (SPD - Security Policy Database).

Una política de seguridad suele especificar los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En modo transporte, estas serán las mismas direcciones que en la SA. En modo túnel pueden ser distintas.

- Protocolos y puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico entre las direcciones IP indicadas.
- La asociación de seguridad a emplear para proteger los paquetes.

Por otro lado, IPsec emplea dos protocolos diferentes - Authentication Header (AH) e IP Encapsulating Security Payload (ESP) - para asegurar la autenticación, integridad y confidencialidad de la comunicación. Ambos son protocolos IP independientes.

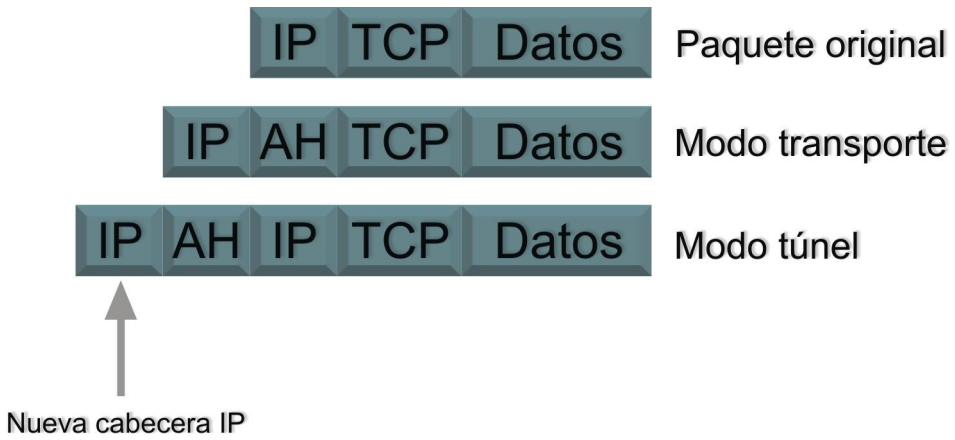
El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete.

El protocolo ESP asegura la integridad del paquete y la confidencialidad empleando cifrado. Tanto AH como ESP pueden ser aplicados ya sea en forma individual o en forma combinada. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC.

Cada protocolo puede, a su vez, ser operado en una de dos formas: modo transporte o modo túnel. IPsec puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo transporte.

En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En modo transporte IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores IP. En la Figura 12 se pueden observar los formatos de las tramas IPs de los distintos modos.

Figura 12 Formatos de tramas Ips



Fuente: Autores del proyecto

Por otro lado, como ya se ha comentado anteriormente, la configuración manual de la asociación de seguridad puede llevar a errores, y no es muy segura. Las claves secretas y algoritmos de cifrado deben compartirse entre todos los participantes de la VPN. Por ello, un problema crítico es el intercambio de claves simétricas cuando aún no se ha establecido ningún tipo de cifrado. Para esto, IPsec emplea Internet Key Exchange (IKE) que permite la autenticación de los participantes en la conexión y el intercambio de claves simétricas, permitiendo a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

El protocolo IKE funciona en dos fases. En la primera fase, autentica a los participantes. En una segunda fase se negocian las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de claves Diffie Hellmann. El protocolo IKE se ocupa también de renovar periódicamente las claves para asegurar su confidencialidad. Tras ello, crea las asociaciones de seguridad y completa la SAD.

En IPSec, el vector de inicialización (IV) es de 8 bytes y se usa para cifrar el primer bloque del texto plano y asegurar así la aleatoriedad entre mensajes que pueden comenzar con la misma información de texto plano.
Para protegerse contra ataques por denegación de servicio, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Entre las ventajas de IPsec están la modularidad del protocolo, ya que no depende de un algoritmo criptográfico específico. Sin embargo, es importante reseñar que este mecanismo cuenta con ciertas desventajas. En primer lugar, Las VPNs basadas en IPsec no proporcionan seguridad a nivel de enlace y sólo protegen tráfico IP. Además, todo el proceso de asegurar la información se lleva a cabo mediante software, con la utilización de recursos de dispositivos de usuario que esto implica.

Para unificar conceptos con base en lo expuesto a lo largo del capítulo, a continuación se muestra una tabla resumen con las características más importantes de los protocolos abordados:

Tabla 4 Tabla comparativa de los protocolos de seguridad

		WEP	WPA	802.11i	VPN
Autenticación	Autenticación	WEP	802.1X + EAP	802.1X + EAP	IKE de maquina, X-AUTH de usuario
	Pre-autenticación	No	No	802.1X (EAPOL)	Si
Cifrado	Negociación del cifrado	No	Si	Si	Si (DES, 3DES, AES)
	Cifrado	RC4 40-bit o 104-bit	TKIP: RC4 128-bit	CCMP: AES 128-bit	ESP: DES 56-bit, 3DES 168-bit, AES 168, 128, 192, 256
	Vector de inicialización	24 bits	48 bits	48 bits	DES-CBC 8 bytes
	Integridad de la cabecera	No	MIC	CCM	AH
	Integridad de los datos	CRC-32	MIC	CCM	AH/ESP
	Protección de respuesta	No	Fuerza de secuencia de IV	Fuerza de secuencia de IV	Si
	Gestión de claves	No	Basada en EAP	Basada en EAP	IKE (Diffie-Hellman)
	Distribución de clave	Manual	802.1X (EAP)	802.1X (EAP)	Diffie-Hellman
	Clave asignada a:	Red	Paquete, sesión y usuario	Paquete, sesión y usuario	Usuario
	Clave por paquete	Concatenación IV	Mezclado TKIP	No necesario	ESP
Otros	Seguridad ad-hoc	No	No	Si (IBSS)	No

Fuente: Autores del proyecto

En conclusión, al margen de los estándares de seguridad, los fabricantes están incorporando a sus productos características alternativas que pueden en algunos casos resultar suficientes para resguardar determinados entornos, como control de accesos, tecnologías VPNs (IPSec, por ejemplo) y herramientas que, al igual que los firewalls, localizan y bloquean usuarios no autorizados.

En el ámbito de la encriptación, una alternativa a las propias de WPA u 802.11i, es el protocolo de red privada virtual IPSec, especialmente si la red de la empresa en cuestión incluye una solución de acceso remoto, basada en este protocolo lo suficientemente robusta. Desde el punto de vista de la seguridad, IPSec aporta un modelo incluso más fuerte que WPA. Su inconveniente es que no puede aplicarse a usuarios que se encuentren fuera del área “militarizada” de la empresa. Además, la carga que suponen los procesos de “tunneling IPSec” puede llegar a comprometer el rendimiento en entornos de alta velocidad.

Obviamente la decisión de optar por uno de los mecanismos de seguridad o la combinación de los mismos, depende del tipo de información que maneje la organización, de los equipos que adquieran o dispongan y por supuesto de la infraestructura de la red.

3 POLÍTICAS DE GESTIÓN

Las secciones anteriores presentaron las arquitecturas y los temas de seguridad relacionados con las infraestructuras de redes WLAN. Si bien estos aspectos son fundamentales para el diseño e implementación de las redes inalámbricas, el mantenimiento y control de las mismas presenta igualmente desafíos sobretodo en entornos corporativos.

Como se mencionó a lo largo del primer capítulo, el crecimiento de este tipo de redes lleva consigo el aumento de los dispositivos que las componen y que necesitan ser administrados, pero ¿qué es lo que realmente se necesita para la formulación de políticas de gestión?

Para dar respuesta a esta inquietud, se debe comenzar por definir el concepto de gestión. Si este se concibe como "……el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio…" [3] se debe tener clara la infraestructura a nivel de arquitectura y dispositivos presentes en la red, así como de servicios y aplicaciones que brinden.

Por lo tanto, hay dos aspectos básicos que deben tenerse en cuenta antes de formular cualquier política de gestión y control. El primero esta relacionado con la implementación de redes inalámbricas en las organizaciones que ya poseen redes cableadas, pues estas no deben alterar dichas infraestructuras ni mucho menos las estrategias existentes. La segunda, es que éstas, las WLANs, deben concebirse como una extensión de la red existente aumentando la flexibilidad y la disponibilidad de la misma, sin ser sustitutas de las actuales arquitecturas.

Ahora bien, ¿cuáles serían las tareas que favorecen el despliegue y la integración de las redes inalámbricas dentro de la organización? Las siguientes son las labores que responden la citada inquietud

- Definir una topología a nivel de arquitectura (Diseño de la red WLAN)
- Definir ubicación e instalación de los dispositivos
- Configuración. Criterios de Seguridad
- Control, administración y mantenimiento

[3] T.Saydam and T. Magedanz, "From Networks and Network Management into Service and Service Management", *Journal of Networks and Systems Management*, Vol 4, No. 4 (Dic 1996).

3.1 TOPOLOGÍA O ARQUITECTURA

Esta topología hace referencia a las ya mencionadas en el capitulo 1. La decisión de tomar una de ellas permitirá definir que tipo de dispositivos intervendrán en el diseño de la red WLAN, así como las funciones que ejecutará cada uno de ellos.

Aunque en las redes cableadas la arquitectura, los dispositivos y sus funciones al igual que los servicios son más palpables, en el caso de las redes inalámbricas hay que comenzar eliminando la ambigüedad en relación a su funcionalidad en lo que dispositivos se refiere, para ello es necesario el establecimiento de una clasificación de las mismas, especialmente para la arquitectura centralizada.

La tabla a continuación exhibe un grupo de funciones asociadas con sus respectivas operaciones, que según los proveedores de dispositivos para WLAN y la IETF deben tenerse en cuenta para ser distribuidos entre los Controladores de Acceso (AC) y los Access Points (AP).

Tabla 5 Clasificación de Funciones

TIPO	DESCRIPCIÓN	GRUPO DE FUNCIONES
1	Funciones RF	• Transmisión/Recepción • Codificación, Modulación • Monitoreo de interfaces wireless
2	Funciones para datos	• Encriptación/des-encriptación • Fragmentación • Buffering (almacenamiento)
3	Funciones de gestión	• Autenticación • Asociación • Pruebas • Generación de Beacons
4	Funciones de control	• Frames de confirmación ACK • Control de errores
5	Funciones de supervisión para los APs	• Configuración de APs • Parámetros • Políticas de gestión • Gestión para Qos • Control de Acceso

Fuente: CAPWAP. Functionality Classifications

Las operaciones vinculadas con las funciones RFs, están relacionadas con aspectos comunes a las interfaces RF de los APs y los clientes móviles. Esto hace parte, por supuesto de la capa física. Las acciones sujetas a las funciones de datos, gestión y control hacen parte del procesamiento de la capa MAC. Las operaciones correspondientes a la supervisión de los APs hacen parte del nivel 7 del modelo TCP/IP, del tipo aplicación.

Las clasificaciones de la funcionalidad WLAN representan las unidades integrales que pueden aplicarse en el AC y el AP como parte de sus capacidades de servicio. Como se exhibe, estas acciones están orientadas hacia una arquitectura con control centralizado ya esta permite escalabilidad y simplificación en la administración entre otras bondades, siendo este el soporte de las políticas de control y gestión.

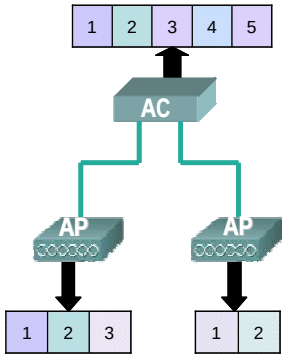
Teniendo como base este grupo funcional (tabla 5), la elección de los dispositivos de la red se puede tomar de acuerdo a como se desee estructurar su control, como tal, las empresas pueden optar por simplificar el AP realizando sólo funciones del tipo 1, es decir de Radio Frecuencia, dejando al AC realizar los demás grupos funcionales, distribuyendo de esta forma las operaciones de manera estructurada.

Las clasificaciones son igualmente una base para la identificación de diferentes tipos de APs, ACs y sus compatibilidades. Por ejemplo, la incorporación de la funcionalidad de APs del tipos 1 y 2 requerirá el apoyo de un AC correspondiente al tipo 3 y 4 o de un conjunto de ACs del tipos 3 y 4. En esencia, las clasificaciones actuales presentan oportunidades para los procesos de certificación entre APs y ACs.

Lo antedicho, representa un paso inicial para la gestión de la variedad de arquitecturas en especial para las de tipo de infraestructura centralizada, facilitando la configuración de distintos APs para operar conjuntamente dentro de una misma WLAN. De igual forma es necesario describir las interfaces de adaptación con la finalidad de gestionar la diversidad entre los APs.

La figura 13 servirá como ilustración para las diferentes políticas de adaptación de las interfaces. Se pone de manifiesto, para el asunto en cuestión, una red WLAN con un controlador central, AC1, capaz de ejecutar los cinco grupos funcionales. Cada uno de ellos se denota por un bloque con una numeración. Asociado al AC1 se encuentran dos APs, capacitados para realizar distintos grados de funcionalidades. El resto de operaciones complementarias necesarias para los dos APs se dejan al AC1.

Figura 13 Adaptación de interfaces entre el AC y los APs con diferentes grados de funcionalidad



Fuente: Autores del proyecto

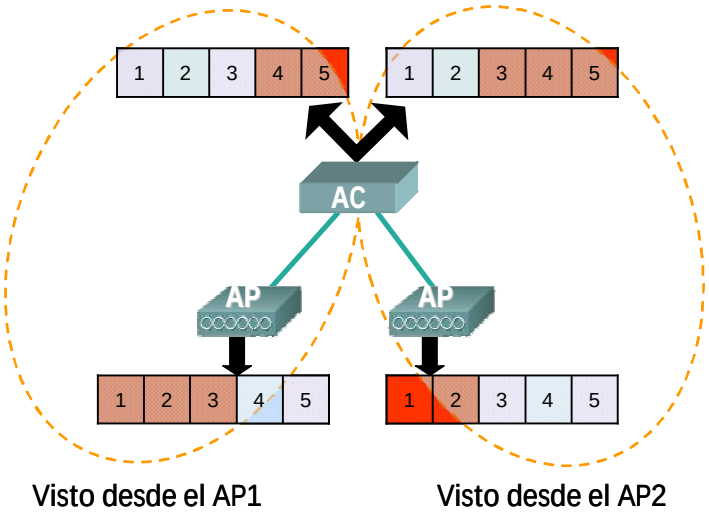
La primera estrategia es aquella en la que cada AP ejecuta todas sus funciones. En este caso, el conjunto de funciones complementarias necesarias son distintas para cada uno de los APs. Por lo tanto, con respecto a la figura 13, el AP1 ejecutar las operaciones concernientes al grupo 1, 2 y 3, dejando las del tipo 4 y 5 al AC1. El AP2, por otro lado, sólo puede ejecutar los tipos 1 y 2 del conjunto de funciones y se apoya en el AC1 para todas las demás.

Para la figura a continuación, los cuadros rojos representan las funciones que el AP o el AC ejecutan y los que no lo son, simboliza las que no se llevan a cabo. Los Access Point 1 y 2 efectúan la totalidad de sus funciones. El resto del conjunto de funciones complementarias se lo deja al AC1. El AC1, a su vez, ejecuta diferentes conjuntos de funciones complementarias para cada uno de los APs. El resultado de la primera estrategia es una adaptación de interfaz entre AC1 y los APs a su cargo. Donde requiere un AC1 para realizar diferentes tipos de procesamiento de frames recibidos de los diferentes APs.

También puede haber variaciones con respecto a las secuencias del procesamiento para los diferentes APs. En virtud de esta política, se da cabida a distintos APs al mismo tiempo y potenciar así sus capacidades individuales.

Cabe señalar aquí que un AC que operan al amparo del la de esta estrategia debe ser capaz de llevar a cabo partes sustanciales de las funciones WLAN completas. Teniendo en cuenta el contexto imperante del AC siendo potentes conmutadores o routers, las operaciones necesarias para esta política son marginales.

Figura 14 Funciones percibidas desde cada AP



Fuente: Autores del proyecto

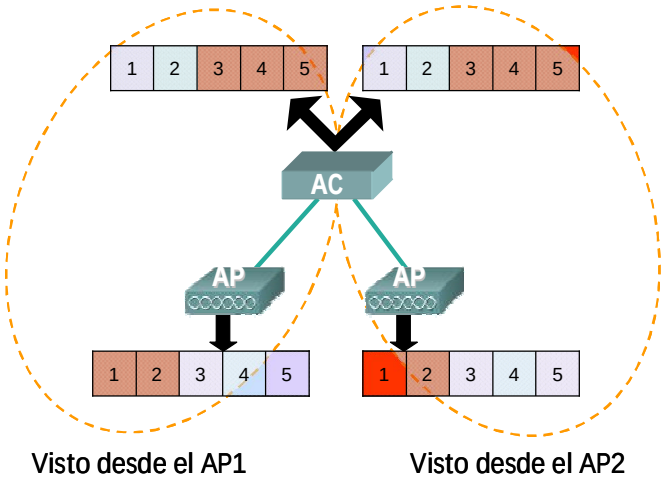
Una segunda política de interfaces de adaptación, implica la simplificación del AC. En este sentido, un administrador primero determina un subconjunto de las funciones que es común a todos los APs que se desean instalar, por lo tanto dichos APs sólo ejecutan esas funciones. De esta forma, el resto del conjunto de funciones complementarias, también común para los APs, son abstraídos por el AC.

Como se observa en la figura 15, el AP1 y el AP2 están obligados a ejecutar las funciones del tipo 1 y 2. Las restantes son idénticas para ambos, y por consiguiente son realizadas por el Controlador de Acceso. Esta política simplifica el proceso en el AC pues ejecuta las mismas funciones, es decir las operaciones relaciones con el grupo 3, 4 y 5 para diferentes Access Points, además de presentar la posibilidad de que algunos APs funcionen por debajo de su plena capacidad.

En este orden de ideas, una arquitectura que presente una jerarquía facilitará el control y manejo de la red y por supuesto la adaptación con las redes cableadas. En este caso el AC es el módulo fundamental, por manejar los aspectos fundamentales de la WLAN, esto significa que la elección de este dispositivo definirá la mayoría de las políticas de gestión.

El modelo del sistema de gestión para esta arquitectura se exhibe en la figura 16. El agente SNMP es el AC, pues permite de una forma centralizada monitorear los APs adscritos a él, su principal función es la configuración y administración de estos dispositivos manifestándose en el mapeo constante de sus enlaces.

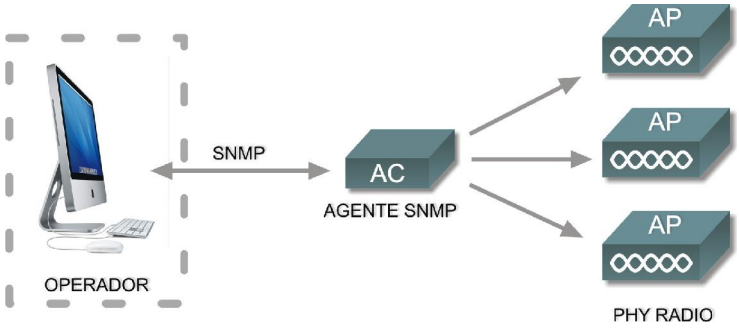
Figura 15 Funciones percibidas desde cada AP, con el mismo grado de funcionalidad



Fuente: Autores del proyecto

Aún se encuentra bajo estudio los diferentes módulos MIB que favorecerán la integración de diferentes tecnologías inalámbricas (802.11a/b/g, 802.11i, 802.11k, 802.11e), por el momento cada proveedor define sus MIBs para la administración de los Radios o APs.

Figura 16 Modelo de sistema de Gestión WLAN



Fuente: Autores del proyecto

Sin embargo, a pesar que las preferencia estén hacia un arquitectura centralizada, eso no quiere decir que sea ésta la única opción a la hora de hacer un diseño, si por el contrario, se pretende trabajar con una red autónoma, se debe considerar que todas las funciones mencionadas en la tabla 5 o la gran mayoría se ejecutaran en los APs, de ahí su nombre “Stand Alone” o “Fat APs” por ser nodos direccionables con sus propias

interfases tanto para redes WLAN como para redes cableadas similares a los switch capa 2 y capa 3 o routers.

Otra arquitectura como la del tipo distribuida, se encuentra fuera del alcance de este documento, pues fue concebida para redes metropolitanas u otros desarrollos donde estén involucrados componentes del tipo “outdoor”

3.2 UBICACIÓN E INSTALACION DE EQUIPOS:

Este ítem obedece a los procesos de diseño relacionados con el radio de cobertura y el alcance de la misma para confinar la señal y proveer continuidad a los usuarios. Aquí juegan un papel importante el tipo de antena y la ubicación de los puntos de acceso, para dar conexión solo a áreas deseadas y de igual forma, que dichos dispositivos (antena y AP) se encuentren fuera del alance del personal no autorizado.

3.3 CONFIGURACIONES. CRITERIOS DE SEGUIRIDAD:

Dependiendo del nivel de seguridad exigido y existente en los sistemas de información de la empresa, es necesario aplicar medidas específicas de seguridad para proteger la información confidencial de la red cableada ante usuarios inalámbricos no autorizados.

Estas medidas van de la mano con el tipo de arquitectura de la red, no obstante a continuación se enumeraran algunas que pueden ser aplicadas a diferentes tipos de infraestructura.

1. Las redes WLAN deben ser asignadas a una subred dedicada y no compartidas con una red LAN.

2. Para proteger los servidores del núcleo de red de ataques DoS, los servicios que se desea prestar a los usuarios inalámbricos deben ubicarse en una DMZ (que retransmita estas peticiones de los servicios a los servidores de la empresa. Por lo tanto, es recomendable una red redundante para ofrecer alta disponibilidad).

3. Cambiar los parámetros por defecto de los equipos.

4. Comprobar regularmente si hay disponibles nuevas actualizaciones de seguridad para los equipos y aplicarlos.

5. Además de los puntos de acceso inalámbricos, también se deben tener en cuenta algunos elementos básicos :

- Firewalls: La red WLAN es considerada insegura, por lo que todo el tráfico entre ella y la red corporativa debe ser filtrada., algunos protocolos, direcciones IP origen y subredes destino.

- Servidor de DHCP. Proporciona la configuración de IP para los clientes inalámbricos. Su uso se recomienda por razones de escalabilidad.

- Servidor del DNS. Proporciona conectividad de IP a otras máquinas IP.

6. En cuanto a los mecanismos de seguridad a emplear, se prefiere, si la red inalámbrica que se diseña es nueva en su totalidad, que los Puntos de Acceso soporten el estándar IEEE 802.11i ya que permite un algoritmo de cifrado mas robusto. Sin embargo, si los Puntos de Acceso solo soportan el mecanismo de seguridad basado en WAP, esta implementación debe estar fundamentada en EAP que soporte un tipo de autenticación adecuado. Para dotar de mayor seguridad a la red, el tipo de EAP debe proporcionar una autenticación mutua, por lo tanto, no es aconsejable utilizar MD5. En caso de utilización de EAP-TLS, EAP-TTLS y PEAP se recomienda configurar los clientes inalámbricos con un certificado de un servidor seguro y evitar que el usuario pueda modificar estos parámetros. Únicamente el administrador debe tener privilegios para poder modificar el certificado empleado. Si no se configura el certificado, los ataques "Man in the Middle" son posibles.

   Para el manejo de las claves dinámicas y proporcionar autenticación tanto a los usuarios como a los puntos de acceso se puede disponer de un servidor RADIUS o DIAMETER[4]. En caso de utilización de certificados, se recomienda que el servidor RADIUS contraste el estado del certificado del cliente contra un autoridad CRL (las principales Autoridades Certificadoras internacionales actualmente son Verising y Thawte) ó un servidor OCSP.

   En función del método EAP de autenticación utilizado pueden ser empleados opcionalmente los siguientes elementos adicionales:

- Servidor PKI. Proporciona certificados X.509 para la autenticación de usuario y de servidor. Necesario en caso de emplearse EAP-TLS, EAP-TTLS y PEAP.

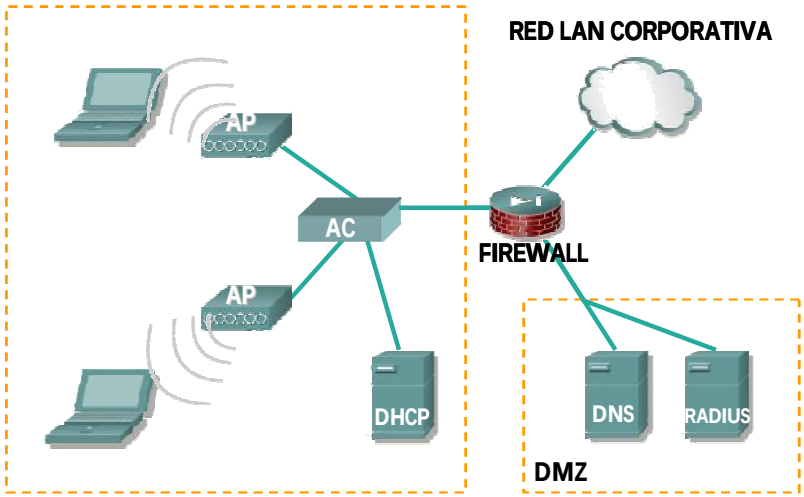
[4] Protocolo de AAA. Diameter es la nueva generación del protocolo RADIUS, interoperable con él y que incluye nuevas funcionalidades.

- Servidor OTP[5]. Proporciona autenticación OTP mediante servidores RADIUS. Puede emplearse con PEAP o EAP-TTLS.

Adicionalmente, es recomendable proteger el modo EAP empleado (LEAP, PEAP, EAP-TTLS) contra ataques de fuerza bruta. El servidor RADIUS debe bloquear las cuentas de usuario tras una serie de intentos de logueo fallidos. Cuando la cuenta de usuario está bloqueada el usuario no puede ser autenticado hasta que no se lleva a cabo una serie de acciones administrativas, lo que permite al administrador llevar a cabo un examen de la seguridad. Para evitar este riesgo, se puede exigir a los usuarios inalámbricos llevar a cabo autenticación tipo OTP.

Teniendo en cuenta las recomendaciones anteriores, la siguiente figura ilustra la arquitectura básica de una red WLAN:

Figura 17 . Arquitectura básica para redes WLAN



Fuente: Autores del proyecto

3.4 CONTROL, ADMINISTRACION Y MANTENIMIENTO

[5] El mecanismo One Time Paswword (OTP) es un método de autenticación simple en el que cada contraseña es válida para una única sesión. Un servidor OTP es aquel que genera contraseñas aplicando algoritmos criptográficos. El funcionamiento básico del método OTP consiste en obtener una contraseña de acceso a red válida mediante el envío de un mensaje de texto (SMS) al usuario. Será necesario repetir este proceso para conectarse en nuevas ocasiones.

Una vez se ha escogido la arquitectura con base a los servicios y aplicaciones teniendo en cuenta los aspectos de seguridad, se deben plantear las acciones de control que se llevarán a cabo para la administración y mantenimiento de la red inalámbrica.

¿Qué se debe controlar?

- La potencia de RF en cada Punto de Acceso Inalámbrico
- Balancear las cargas entre Puntos de Acceso vecinos
- Informar cuantos usuarios hay conectados a cada Punto de Acceso
- Detectar Interferencias y Obstáculos
- Calcular SNR. Relación Señal / Ruido
- Informar estándar 802.11 utilizado por cada usuario para conexión
- Informar sobre velocidades de transmisión
- Detectar bloqueos en el canal
- Detectar nodos ocultos
- Detectar Access Point, mal configurados
- Detectar Redes Ad-Hoc
- Detectar ataques de Denegación de Servicio -DoS
- Detectar Access Point maliciosos
- Detectar Access Point con fallos, que requieran mantenimiento
- Generar Alarmas ante situaciones que requieran intervención inmediata
- Generar Estadísticas.

El control de la potencia de radio frecuencia permite dos aspectos importantes, confinar la señal a sectores deseados y el balanceo de cargas. Este último consiste en transferir usuarios de un Access Point muy "colapsado" a otro contiguo que esté menos "ocupado". Esto se logra modificando el tamaño de las celdas. Si se aumenta la potencia de RF del que se encuentra mas libre se aumenta su radio de cobertura, así mismo si se reduce la potencia de RF del "colapsado" se disminuirá su cobertura. De esta manera se puede conseguir transferir usuarios de un AP a otro, compensando la carga de trabajo.

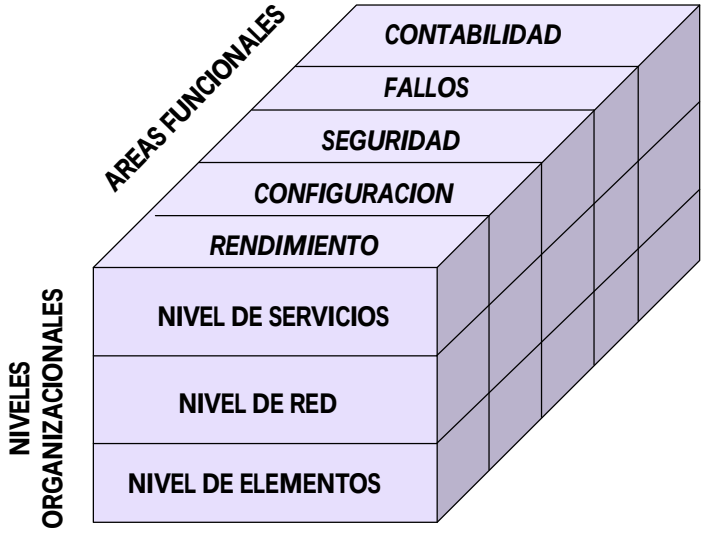
El cálculo del SNR, permitirá conocer si el sitio donde se encuentra ubicado el AP o hacia donde se pretenda ubicar presenta considerables obstáculos e interferencias, desmejorando por supuesto la calidad de la señal, por lo tanto se aconseja verificar al realizar el Site Survey, que en todos los puntos de la instalación, esta relación sea igual o mayor al 30%.

Todos estos aspectos y los mencionados a lo largo de esta sección, forman el conglomerado de políticas para la administración y mantenimiento de una red WLAN.

Si se toman los modelos de gestión existentes, se podrían ubicar las redes WLANs dentro de la arquitectura organizacional de la ITU-T TMN en los niveles de gestión de elementos, red y de servicios, pues ellas proporcionan conectividad y prestaciones con

base a sus homologas cableadas, es decir se administran dispositivos, se controla la red WLAN y se transfieren peticiones desde y hacia la red cableada, quien es la que concentra la información dentro de la organización. A nivel funcional, según el modelo OSI, el control y la administración, se promueve en congruencia con las áreas de gestión de fallos, configuración, seguridad y rendimiento, y si es el caso contabilidad. Esquematizando estos modelos se obtendría lo siguiente:

Figura 18 Esquema funcional de gestión



Fuente: Autores del proyecto

La proposición de la figura 18 indica que para cualquier nivel organizacional, se aplican diferentes áreas funcionales que traducido a las redes WLANs sería la aplicación al control mediante funciones en lo relacionado con la red y soportado por la gestión de los servicios establecidos en la red cableada corporativa existente.

Esto significa, teniendo en cuenta el estándar 802.11 que las políticas de gestión de WLANs están encaminadas al control y administración de los equipos inalámbricos a nivel de capa 2 y capa 3, ver tabla 5, y la evaluación de sus servicios se realizan a través de las políticas o estrategias que tenga la compañía ya estipuladas para el manejo de la red.

Todo lo enumerado en este capítulo, permite identificar las reglas necesarias para el control y mantenimiento de una red inalámbrica. Las siguientes son una propuesta para llevar a cabo tal fin, ver figura 19.

Dentro del esquema planteado en la figura 18 y las políticas generadas por el despliegue de redes WLAN en entornos corporativos, se encuentran enmarcadas las

funciones de cada estrategia, estas fueron seleccionadas como se muestra en la representación plasmada en la figura 20, donde los números hacen referencia a dichas políticas formuladas en la figura anterior.

Figura 19 Componentes de administración para redes WLANs.

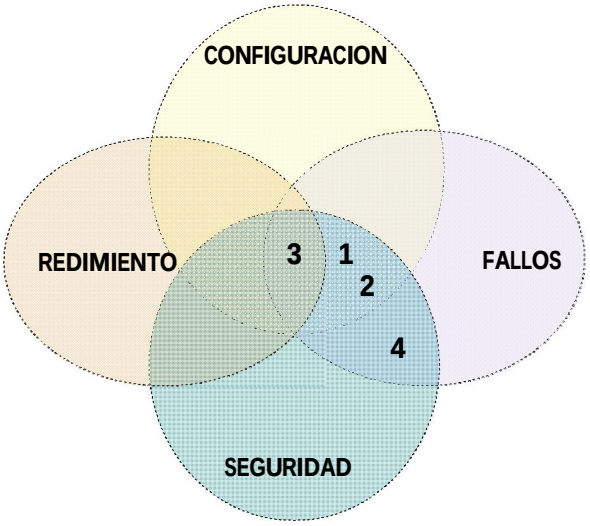
Fuente: Autores del proyecto.

Las acciones para el manejo de identidad y acceso a la red, son la recopilación de las áreas de aplicación concerniente a la configuración, seguridad y fallos. Asimismo dichas áreas cobijan las acciones vinculadas con el control de la radio frecuencia, identificadas en la figura con el número 1 y 2 respectivamente. Esto implica:

- Establecer los parámetros de operación
- Recoger información sobre el estado actual
- Recoger avisos de cambios significativos
- Cambiar la configuración del sistema. Si es necesario
- Crear, borrar y controlar los servicios y mecanismos de seguridad
- Distribuir la información de seguridad solo al personal autorizado.
- Informar de los sucesos relativos a la seguridad del sistema
- Mantener y examinar registros de errores
- Aceptar y actuar ante notificaciones de errores
- Localizar e identificar las averías.
- Llevar a cabo secuencias de pruebas de diagnóstico
- Corregir las averías

A nivel de políticas de movilidad, número 3 en la figura, se aplican todas las áreas del modelo, tales como rendimiento, configuración, seguridad y fallos, por ser un servicio fundamental de la WLAN base de las prestaciones de la misma.

Figura 20 Compendio de gestión con políticas de control



Fuente: Autores del proyecto

Así como en el caso anterior, el manejo de estas políticas obedece a las siguientes implicaciones:

- Reunir información estadística
- Mantener y explotar registros históricos del estado del sistema
- Determinar las prestaciones del sistema en condiciones naturales y artificiales
- Modificar la operación del sistema para una correcta gestión de prestaciones.

Ésto en cuanto a las estrategias de rendimiento, lo relacionado con la configuración, la seguridad y la gestión de fallos son las mismas que se formularon para las políticas de acceso y control RF.

Por último se tienen las políticas de intrusión, estas son producto de las acciones que se tomen frente al control de radio frecuencia y de acceso a la red, pues estas medidas favorecerán el control en la intrusión de acuerdo a los ataques, incluidos los APs “Rogue” o maliciosos. Por esta razón se encuentra ubicado en el área de intersección de la gestión de la seguridad y de fallos, ya que vela por la integridad de la red.

Las siguientes son las operaciones derivadas de la aplicación de los modelos de gestión para la administración de redes

3.4.1 Políticas de identidad y acceso a la red.

- Mantener una política de contraseñas adecuada.
- Utilizar perfiles de usuario que permitan el control de acceso para usuarios internos o empleados y usuarios invitados.
- Habilitar el cifrado sobre el tráfico enviado por el interfaz aéreo siempre que sea posible.
- Asegurar físicamente los puntos de acceso, para evitar que personal no deseado tenga acceso a él.
- Las redes WLAN serán sólo accesibles por aquellos dispositivos asociados al SSID adecuado. Para evitar el acceso por parte de usuarios no deseados es fundamental deshabilitar el broadcast de SSID que, en general, llevan a cabo por defecto los puntos de acceso. Aunque este mecanismo de seguridad es fácilmente vulnerable, tal y como han demostrado numerosos estudios, su práctica sigue siendo recomendable puesto que supone un primer nivel de defensa contra ataques y permite evitar la conexión de usuarios de manera automática a la red, ya que aunque no hagan uso de ella para transmitir información, degradan la conexión de otros usuarios.
- Emplear puntos de acceso inalámbricos que permitan activar la opción de 'intracell blocking' para evitar que un usuario conectado al mismo pueda acceder a máquinas de otros usuarios conectados a él.
- Emplear claves de usuario dinámicas, por ejemplo mediante autenticación OTP con PEAP y EAP-TTLS.
- Inhabilitar el modo ad-hoc.

3.4.2 Políticas de control de radio frecuencia

- Tipo y ubicación de antenas estudiada para restringir el área de cobertura radio dentro del radio deseado.
- Equipos inhibidores de señal en zonas que no se desea tener cobertura.
- Asignación de Potencia
- Manejo de canal

- Optimización del área de cobertura

- Balanceo de cargas

3.4.3 Políticas contra intrusión

- Llevar a cabo el bloqueo de cuentas de usuario por parte del servidor RADIUS tras una serie de intentos de autenticación fallidos.

- Detección de APs maliciosos

- Detección y manejo de ataques DoS

3.4.4 Políticas de movilidad

Estas acciones no solo son referentes a la movilidad dentro de la organización sino a su vez a los accesos a la red a través de servicios públicos.

- Para aumentar la seguridad de acuerdo a los escenarios de movilidad de determinados perfiles de usuarios, el uso de un IPsec VPN es altamente recomendado así como el uso de firewalls que filtren el tráfico entrante en la red de la empresa.

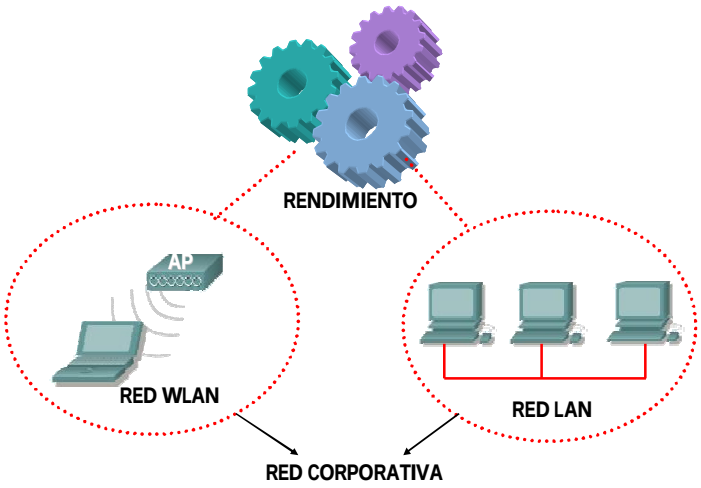
- Fast Roaming. Esto hacer referencia a la asociación de clientes o estaciones con los puntos de acceso cuando se desplazan dentro de la organización. La idea es que la autenticación de cada usuario con el punto de acceso no afecte la conectividad y no tenga impactos en los servicios y aplicaciones que se encuentre utilizando en ese momento. Uno de los mecanismos de seguridad que favorecen este requerimiento es el 802.1i, así como WPA2.

Estas fueron las políticas relacionadas con el manejo de la conectividad, es decir el acceso y uso de la red para servicios estipulados en la red LAN o cableada, sin embargo en estas estrategias no se encuentran concertadas las relacionadas con la interacción entre la red inalámbrica y la cableada en cuanto a rendimiento de la red corporativa, estas políticas deben ser concertadas con base a las existente para tal fin donde se debe incluir las siguientes:

- Número máximo de estaciones asociadas a un único punto de acceso al mismo tiempo, normalmente se maneja de 5 a 15 máquinas teniendo en cuenta el ancho de banda.

- Número máximo de octetos permitidos entre un punto de acceso y la red cableada, esto con el objeto de evitar la sobrecarga del Access Point en cuestión.

Figura 21 Esquema de integración con base en el rendimiento de la red



Fuente: Autores del proyecto

- Número máximo de octetos permitidos entre un punto de acceso y las estaciones individuales para advertir que una única estación consuma gran cantidad de ancho de banda afectando a otros usuarios.

- Establecer patrones de tráfico de la red LAN inalámbrica con el fin de obtener los detalles operativos de uso.

Como se puede concluir, el control y la administración de WLANs esta sustentada en los principios de flexibilidad y disponibilidad de la red, proporcionando una extensión de LAN existente, por lo tanto sus políticas de control y gestión entrañan aspectos de seguridad y conectividad desde y hacia la red corporativa cableada.

4 ANÁLISIS DE UNA RED CORPORATIVA

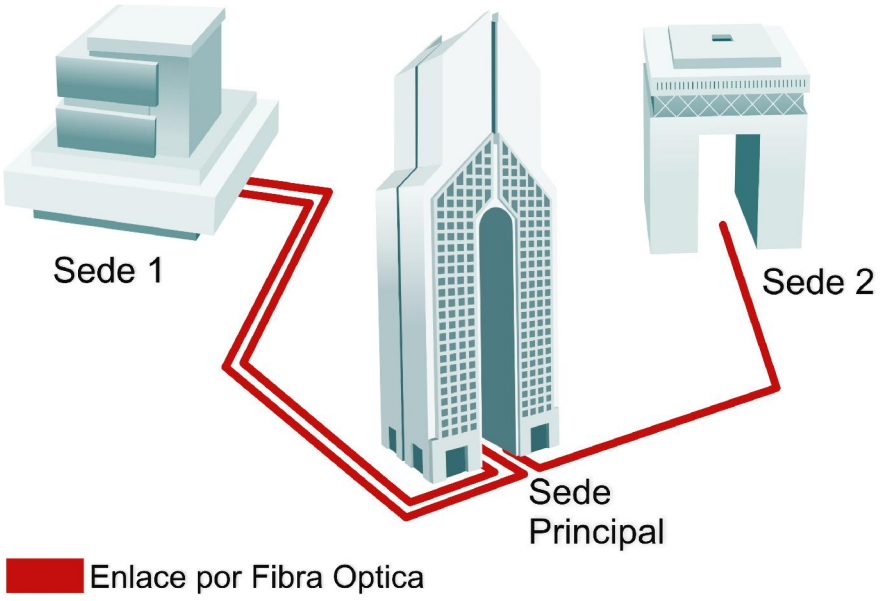
Con el objeto de aplicar todo lo expuesto en esta investigación a un entorno real, el presente capítulo expone el análisis realizado a una red corporativa existente.

4.1 DEFINICIÓN DEL ESCENARIO

La empresa cuenta con una sede principal y dos secundarias ubicadas en diferentes edificios en el mismo predio. En el edificio principal se localizan todos los servicios que proporciona la red, es la sede que posee la mayor cantidad de puntos de acceso inalámbricos y es donde se encuentra el personal encargado del control y gestión de la red de la organización.

La comunicación entre la sede principal y la sede 1, ver figura 22, es considerada de vital importancia para la compañía por manejar procesos críticos, razón por la cual entre las edificaciones se encuentra tendidos dos enlaces de fibra óptica, para efectos de redundancia. Caso contrario a la sede 2 que tan solo cuenta únicamente con un solo enlace de fibra óptica.

Figura 22 Distribución geográfica de la red



Fuente: Autores del proyecto

El edificio principal tiene 8 pisos de alto y cuenta con 18 puntos de acceso inalámbricos distribuidos de acuerdo con la tabla 6. Estos dispositivos se ubicaron con base a las necesidades particulares de cada piso y todos sus radios de acción se encuentran funcionando adecuadamente.

Todos los Puntos de Acceso, así como todos los equipos que hacen parte de la red de la compañía son marca CISCO. Las referencias de estos radios son: Aironet 1240 y Aironet 1242, que forman parte de la familia Aironet 1240. Actualmente cada punto de acceso inalámbrico va conectado a un Switch, y de esta forma se conecta con la red LAN.

Tabla 6 Distribución de puntos de acceso por piso en el edificio principal

PISO	CANTIDAD DE PUNTOS DE ACCESO	MARCA DE LOS PUNTOS DE ACCESO
1	3	Aironet 1240
2	2	Aironet 1240
3	2	Aironet 1240
4	2	Aironet 1242
5	2	Aironet 1240
6	3	Aironet 1242
7	2	Aironet 1242
8	2	Aironet 1240

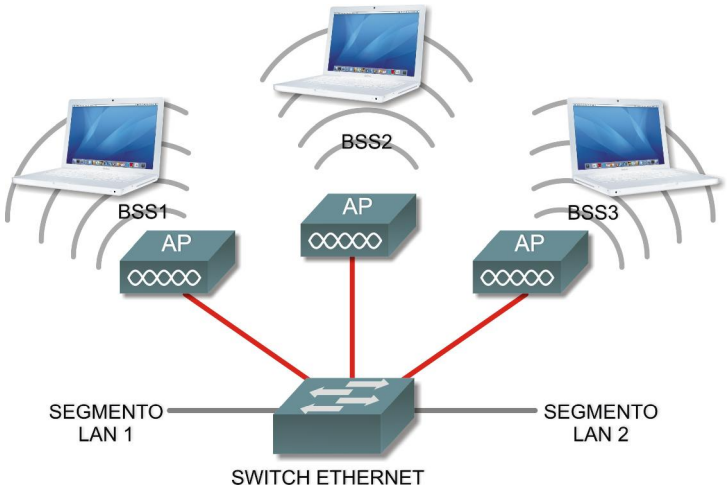
Fuente: Autores del proyecto

El edificio de la sede 1 cuenta con 3 pisos. Como el número de empleados es menor en comparación al resto de edificaciones así como el área de cobertura, disponen de tan solo un (1) punto de acceso en cada piso y dos en el primero, satisfaciendo los requerimientos de esas áreas.

La sede dos es un edificio de 5 pisos en el que se encuentran 10 puntos de acceso, dos (2) por cada piso. Del mismo modo que en los casos anteriores, estas distribuciones obedecen a las necesidades de cobertura y cumple con los exigencias.

La topología de la WLAN, tiene las características de una arquitectura autónoma como se ilustra en la figura 23 (explicada en el capítulo 1), los Access Points convergen a un switch LAN por piso. Son típicamente configurados y controlados de manera individual.

Figura 23 Esquema de Arquitectura Autónoma



Fuente: CAPWAP Architecture Draft

En materia de seguridad, el mecanismo implementado en la sede principal y en la sede 1 es WPA-PSK. Con respecto al edificio 2, los APs tienen configurado el protocolo WEP y como complemento a sus estrategias, la red inalámbrica tiene deshabilitado el broadcast de SSID en todos los APs, de esta forma la WLAN no es fácilmente vista por personas que no la tengan configurada en su equipo. Estas discrepancias en cuanto a protocolos de seguridad responden a los servicios que se manejan en las distintas zonas. Por tal motivo han estipulado diferentes VLANs, una para el personal de servicios informáticos, otra para los usuarios internos y una última para los externos y visitantes.

La configuración de la red inalámbrica para el acceso de las estaciones, es realizada por un técnico. Nunca se proporciona la clave ni el SSID a ningún usuario.

A continuación se muestra una tabla con el sumario de los aspectos más importantes recopilados de la red bajo el estudio.

Tabla 7 Resumes de las características actuales de la red

Distribución de la red (geográfica)	Tres edificios
Distribución de APs	En el edificio principal se cuenta con 18 puntos de acceso, en la sede dos con 10 y en la sede 1 con 4 puntos de acceso.
Topología empleada	Autónoma
Mecanismo de seguridad	WPA-PSK en la sede principal y sede 1, protocolo WEP en la sede 2.
Administración y control	No existe nada sólido al respecto, la

	configuración y manejo de problemas técnicos son solucionados de forma individual en cada estación de trabajo o en cada AP.
Equipos Usados	Cisco Aironet 1240 y 1242
Software de gestión de la red inalámbrica	Ninguno.

Fuente: Autores del proyecto

4.2 ANÁLISIS DE LA RED PRESENTADA

Antes de presentar cualquier propuesta es indispensable analizar la situación actual de la red, pues permite identificar las falencias de la misma así como sus aciertos. Esto por supuesto, beneficia el re-diseño ya que no solo se orienta hacia sus necesidades sino que a su vez se fundamenta en lo ya que se tiene preestablecido.

4.2.1 Puntos a Favor (Pros):

- El protocolo de seguridad configurado en la sede principal y la sede uno, es superior al protocolo WEP, favoreciendo ciertos aspectos en seguridad y confinando los ataques solo a personas con conocimientos en el tema.
- La configuración de VLANs favorece el manejo a nivel lógico de los usuarios y contribuye con las políticas de seguridad de la red en su totalidad, para el acceso restringido a ciertos servicios.
- Como estrategia, la desactivación del broadcast de SSID es conveniente, ya que la red no será vista tan fácilmente desde el exterior por cualquier persona ajena a la compañía. Aunque no es efectiva contra atacantes experimentales, es recomendable usarla como un primer nivel de defensa.
- El manejo de claves para la autenticación no es de conocimiento público y es única y exclusivamente conocida por personal capacitado de la empresa. Son ellos quienes realizan la configuración del equipo o las estaciones que necesiten conectarse a la red.
- El radio de cobertura de los puntos de acceso abarcan los espacios que precisan movilidad.
- Cuentan con personal competente para la administración y control de la red.

4.2.2 Puntos en Contra:

- No poseen una administración centralizada, la arquitectura autónoma adoptada por la compañía, no permite tener una visión general de la red, puesto que cada punto de acceso controla y gestiona su propio BSSID, con la intervención de un técnico, pero desconoce el estado de sus homólogos.
- El mecanismo de seguridad WPA-PSK empleado, fue creado como protocolo de seguridad para entornos caseros y no para ambientes empresariales, donde los niveles de seguridad son más exigentes. Asimismo el protocolo WEP presenta ciertas vulnerabilidades y debe ser reforzado con algún componente adicional.
- No existe un esquema estructurado para la configuración y autenticación de los usuarios de la red, el hecho de que únicamente los funcionarios delegados, puedan configurar las estaciones de trabajo, puede ocasionar, en ciertos casos, demoras y dificultades para su configuración y acceso a los servicios de la red.

4.3 PROPUESTA DE RE-DISEÑO

Con el reconocimiento y el diagnóstico de la configuración y administración actual de la red inalámbrica de la empresa, se procederá a realizar algunas recomendaciones.

Estas propuestas buscan mejorar el desempeño general de la red, a través de una distribución jerárquica que facilite el control y la gestión con la implementación de equipos y software apropiados.

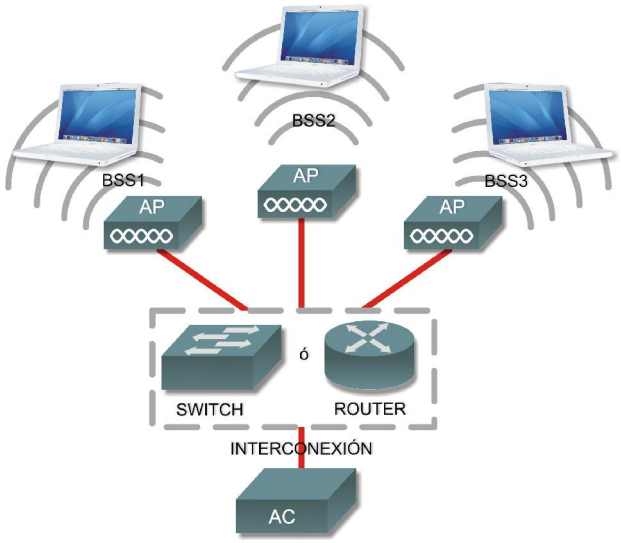
A continuación se enumeran las consideraciones y los puntos claves de análisis para las recomendaciones de diseño, con base a lo mencionado en el capítulo 3.

4.3.1 TOPOLOGÍA DE RED

Como se vio en el primer capítulo, la estructura jerárquica y centralizada, promueve la administración de redes a gran escala, pues los aspectos relacionados con la conmutación, control y gestión se delegan a un solo dispositivo, otorgando al administrador un dominio total de la red al optimizar la supervisión, la escalabilidad en la gestión, y por consiguiente facilitando la dinámica de configuración. Son estas razones las que conllevan a reestructurar la topología actual por una arquitectura centralizada como la mostrada en la figura 24.

Esta arquitectura se vale de uno o más controladores para la gestión de los puntos de acceso inalámbricos. Su función principal tal como su nombre lo indica, es controlar, gestionar y configurar los APs que están presentes en la red. Su conexión puede hacerse a través de un switch o un router, ver figura 24.

Figura 24 Esquema de la Arquitectura centralizada



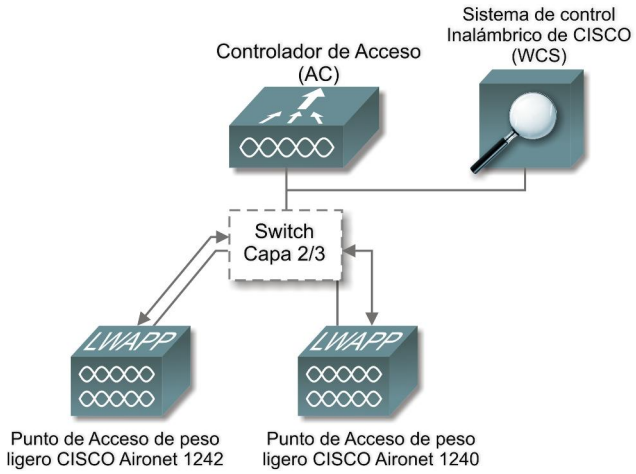
Fuente: CAPWAP Architecture Draft

Consecuentemente con lo planteado, podemos afirmar que la base de esta topología radica en el AC, por lo tanto uno de los aspectos a establecer es el tipo de conectividad del controlador con los puntos de acceso y evidentemente el tipo de AC. Para ello se tendrá en cuenta el proveedor que ha suministrado los equipos con el objeto de evitar engorrosas adaptaciones por efectos de interoperabilidad, máxime con el proceso de estandarización que aún continúa para algunas funciones y protocolos de la pila 802.11.

El esquema que se muestra a continuación, figura 25, obedece a ese deseo de mantener el mismo proveedor para las todos los dispositivos que conformarán la WLAN. Esta figura es el punto de referencia de este trabajo ya que el objetivo del mismo se basa en los equipos de gestión y control de la red inalámbrica y en el software de administración (Switches, Puntos de acceso, Controlador de redes inalámbricas y software de control y monitoreo).

A continuación se realizará un resumen general de las características más importantes de los equipos físicos necesarios para implementar una topología de red centralizada. Esto incluye, como se explicó anteriormente, los puntos de acceso actualmente utilizados (Aironet 1240 y 1242) y el o los controladores de acceso (Controladores de la serie 4400 de CISCO y el Sistema de Control Inalámbrico WCS de CISCO).

Figura 25 Conectividad entre el AC y el AP propuesta por CISCO



Fuente: CISCO

Para el controlador de acceso se prefirió una configuración stand alone, en la cual el controlador de acceso funcionara por si solo y no tuviera que ser integrado a ningún switch en particular, esto con el fin de que sea más fácil su implementación de la red y no haya necesidad de cambiar la configuración de los equipos actuales. Con configuración stand alone, Cisco posee únicamente dos series de controladores de acceso, la serie 2200 y la 4400, en este caso se escogió la serie 4400 ya que esta soporta mayor cantidad de puntos de acceso y permite un crecimiento mucho mayor que el ofrecido por la serie 2200

- **PUNTOS DE ACCESO**

La elección de este dispositivo depende precisamente de la arquitectura que se escoja para el montaje de la red, esto para definir si sus funciones son autónomas o por el contrario se rigen a través de otra máquina, una vez se establece la taxonomía se determinan ciertas características que apoyan la selección, tales como:

- Manejo de varios protocolos. Para este caso en particular la referencia incorpora el 802.11a y el 802.11g a 108Mbps.

- Simultaneidad de frecuencias de operación 2.4GHz y 5GHz.

- Mecanismos de seguridad altos 802.11i/WPA2.

Como se ha manifestado, la compañía cuenta con puntos de acceso CISCO Aironet 1240 Y CISCO Aironet 1242, ambos pertenecientes a la serie Aironet 1240 de CISCO, por lo que ambos tienen básicamente las mismas particularidades y cumple con las expuestas. Adicionalmente tiene la opción de ser autónomo o del tipo “light”, favoreciendo su adaptación en cualquier arquitectura. (Ver hoja de datos del anexo1)

Figura 26 Punto de acceso de la serie Aironet 1240 de CISCO

Fuente: CISCO

- **CONTROLADOR DE ACCESO**

Este es el elemento crítico y diferenciador de la red WLAN, no solo por el esquema de control que se pretenda implementar, sino porque a pesar de que la IEEE y la IETF hayan definido las funciones para una estructura centralizada y jerárquica, especialmente para el control de radio frecuencia, no especifica como deben efectuarse, este trabajo aún se encuentra en proceso, razón por la cual cada proveedor tiene protocolos propietarios para precisar estas acciones, una prueba mas para conservar la marca CISCO en el diseño.

De igual forma que la elección de los Access Points se hace a través de algunas recomendaciones, el controlador también obedece a ciertos criterios. Aquí alguno de ellos:

- Cubrimiento y desempeño de la red. Administración de Radio Frecuencia de los APs asociados a él.
- Manipulación de mecanismo de seguridad como WPA, WPA2 y 802.11i
- Empleo de técnicas de seguridad contra intrusión. Detección y localización de dispositivos no autorizados.

Otro aspecto importante es la capacidad que debe tener el dispositivo para manejar los Access Points que componen la WLAN. En este caso, la compañía, necesita un controlador que como mínimo administre los 42 puntos de acceso que hasta el momento tienen configurados.

Cisco ofrece equipos que cumplen con las exigencias, tiene la facultad de maniobrar 12, 25, 50 y 100 puntos de acceso. La referencia AIR-WLC4402-50-K9, puede controlar hasta 50 APs y sería la primera opción para esta red. (Hoja de datos anexo 2). Obviamente tendrían que contemplar y dimensionar el crecimiento de la WLAN para tomar otra ésta u otras opciones.

La siguiente tabla muestra las características del controlador de acceso de CISCO

Tabla 8 Características generales Controlador de Acceso de la serie 4400 de CISCO

CARACTERISTICA	DESCRIPCION
MANEJO INTELIGENTE DE RF	-Asignación dinámica de canal: Basado en los cambios en RF, el controlador varía los canales buscando optimizar el cubrimiento y desempeño de la red. -Detecta y evita interferencias. -El sistema realiza balanceo automático de cargas en la red, buscando el mejor desempeño de esta. -Detecta y corrige huecos de cobertura y los corrige aumentando la potencia de salida de los puntos de acceso.
ESTANDARES DE SEGURIDAD SOPORTADOS	- Soporta los estándares 802.11i, WPA, WEP, 802.11X y FIPS.
SEGURIDAD	-Detecta y evita interferencias, así como también evita la propagación no deseada de RF. -Detecta y localiza dispositivos no autorizados que estén operando dentro de la red. -Soporta diferentes permisos de acceso para poder dar a cada usuario o grupo de usuarios solo determinados permisos. -Soporta asignación de VLANs, listas de control de acceso, calidad del servicio, AAA y RADIUS y MFP. -Aplica políticas para que solo el usuario final con apropiadas condiciones de seguridad puede entrar a la red.
SERVICIOS DE VOZ	Provee voz sobre WLAN para comunicación empresarial usando Wi-Fi o celulares compatibles, brindando en la comunicación: alta confiabilidad, roaming y calidad de servicio.
SERVICIO DE LOCALIZACION	El sistema de localización ubica la posición física de los dispositivos Wi-Fi. Incluye la localización física de diversos equipos como portátiles, celulares compatibles, PDA’s y dispositivos intrusos.

Fuente: Autores del proyecto

Figura 27 Controlador de Acceso de la serie 4400 de CISCO

Fuente: CISCO.

4.3.2 UBICACIÓN DE LOS PUNTOS DE ACCESO

Este ítem está relacionado con el radio de cobertura y confinamiento de la señal. Por lo tanto la selección del tipo de antena y la ubicación de los puntos de acceso, son aspectos claves para dar conexión y permitir la movilidad de los usuarios, así como la protección física de los equipos.
Aquí es indispensable realizar el cálculo del SNR para examinar lo relacionado con los obstáculos e interferencias, se debe buscar que esta relación sea igual o mayor al 30%.

Para este caso de estudio, la administradora de la red de la compañía nos ha manifestado su interés de no modificar la posición actual de los puntos de acceso, pues cumple con todos los requerimientos y necesidades de la organización, sin embargo se recomienda realizar un análisis desde afuera del edificio para detectar si los APs están irradiando suficiente señal como para lograr una conexión desde el exterior, de ser así se deberán tomar las medidas pertinentes para confinar mas la señal.

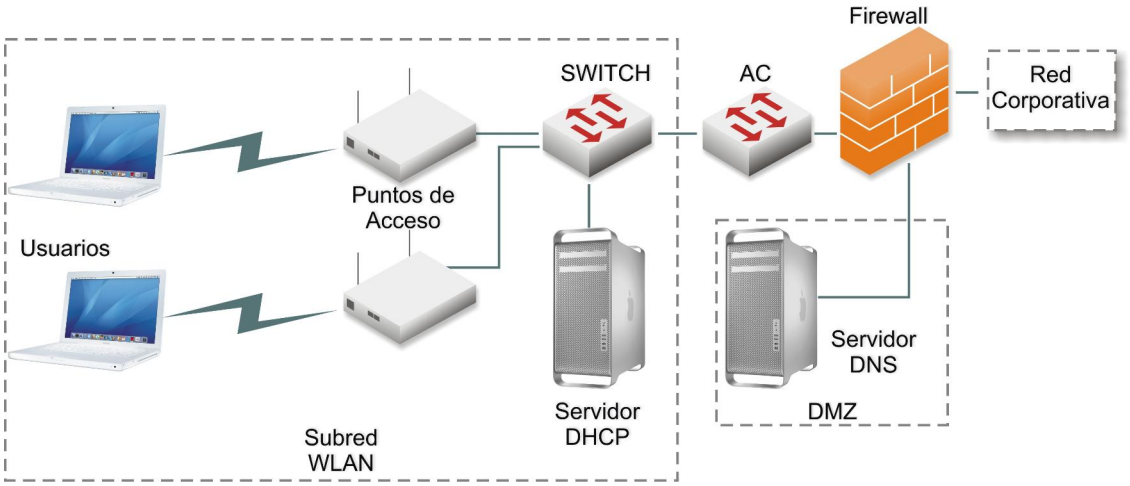
4.3.3 CRITERIOS DE SEGURIDAD

Una consideración elemental en la topología de la red por principios de seguridad, es su separación con respecto a su equivalente, la red LAN de la compañía. Tal como se comentó en el capitulo anterior esta debe ser aislada mediante un firewall que filtre el tráfico entre ellas. De igual forma debe establecerse una zona desmilitarizada que preste los servicios para los usuarios inalámbricos y retransmita las peticiones a los servidores de la empresa, por lo tanto a la arquitectura propuesta debe incluírsele estos aspectos como se ilustra en la figura 28.

En cuanto al mecanismo de seguridad, existen tres alternativas a implementar:

- IEEE 802.11i
- WPA2.
- WPA con soporte de autenticación IEEE 802.1X/EAP.

Figura 28 Arquitectura centralizada incluyendo firewall y servidores



Fuente: Autores del proyecto.

Las dos primeras alternativas, 802.11i y WPA2 tiene mayor aceptación porque poseen fuertes algoritmos de autenticación y cifrado, razón por la cual aún no han sido vulnerados, precisamente por estas características no se hace necesario la adecuación de firewalls en la red interna, pero pueden utilizarse para aumentar la seguridad en escenarios de movilidad. Una desventaja es la demanda de carga en procesamiento haciendo más lenta la red.

La última opción, WPA con IEEE 802.1X/EAP resuelve la desventaja que presentaba esta red con el uso de WPA-PSK en materia de autenticación, pues permite un manejo dinámico de las claves así como la definición de perfiles de usuario, no obstante su desventaja radica en el algoritmo de cifrado pues éste ya ha sido vulnerado.

A pesar de ello WPA es una buena alternativa pues el esquema propuesto en la figura anterior permite una integración de la parte inalámbrica con la cableada sin comprometer en gran medida la información.

Con respecto a la sede que maneja WEP, se recomienda hacer su migración a WPA. En caso de que no sea viable, se aconsejable aislar en lo posible estos sectores de los protegidos, ya que dejar una parte de la red expuesta y unida al resto, es similar a dejar toda la red desprotegida. Para aislar estos segmentos podrían crearse nuevas VLAN's, con políticas de seguridad acordes a los servicios que demanden éstas.

Para llevar a cabo el despliegue de una solución fundamentada en cualquiera de las opciones, La Wi-Fi Alliance recomienda seguir los pasos a continuación:

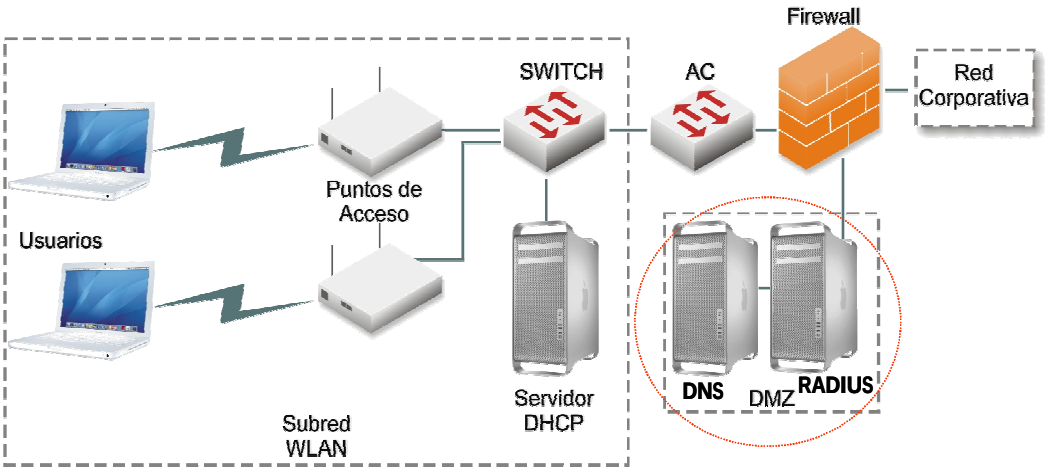
1. Seleccionar el mecanismo de seguridad y credenciales

2. Analizar las base de datos de autenticación de usuarios que se pueden emplear
3. Estudiar el Sistema operativo de los usuarios que van a utilizar esta solución
4. Seleccionar el Supplicant (software disponible en terminal de usuario para realizar la autenticación)
5. Seleccionar el tipo de EAP
6. Seleccionar el servidor de autenticación a utilizar.

Según lo anterior los elementos claves en este diseño para la implementación de políticas de autenticación basadas en IEEE 802.1x son:

- El Software específico en el dispositivo inalámbrico, ya que la solución debe estar basada en un tipo de EAP que soporte el tipo de autenticación seleccionado.
- Servidor AAA para proporcionar la autenticación de usuarios a la red WLAN. Este servidor dentro de la arquitectura mostrada en la figura 28, debe ubicarse también en la DMZ

Figura 29 Arquitectura de seguridad con servidor RADIUS



Fuente: Autores del proyecto.

Otro punto a examinar, es la seguridad física del AP, por lo que es prudente ubicarlos en lugares seguros o tenerlos monitorizados, para así evitar que tengan acceso a él personas no autorizadas.

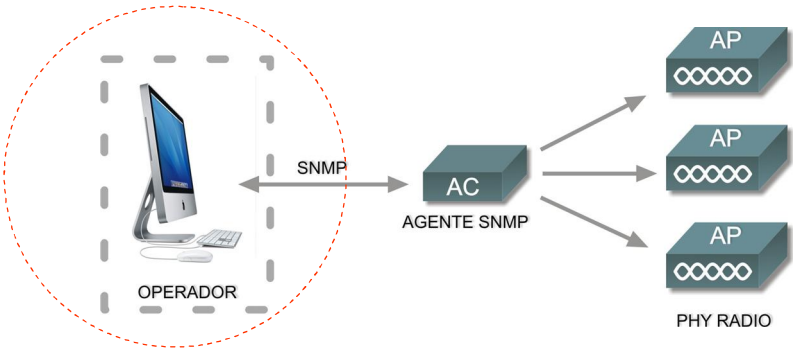
4.3.4 CONTROL Y ADMINISTRACIÓN

Aquí como en todos lo ítems de este análisis, tienen cabida las observaciones realizadas para este punto en el capitulo de políticas de gestión. Todo se encuentra enmarcado en las acciones de control de radio frecuencia, manejo de acceso e identidad de la red, movilidad e intrusión, por lo tanto esta administración requiere la búsqueda del gestor o software que interaccione con los agentes.

Siguiendo con una solución propietaria, se indagó por un software de administración de CISCO. La idea es adquirir una herramienta que permita planificar, configurar y realizar gestión de la red, de tal forma que facilite al administrador realizar el diseño, control y seguimiento de la misma, desde una ubicación centralizada, logrando la simplificación de operaciones y costos.

WCS (Wireless Control System) de CISCO, corre sobre una plataforma con una base de datos embebida, lo cual provee escalabilidad necesaria para manejar cientos de controladores de acceso como los mencionados anteriormente. El software WCS puede ser instalado ya sea en la misma red de la WLAN que se quiere controlar, o en alguna subred diferente o incluso a través de una red de área amplia.

Figura 30 Modelo de sistema de Gestión WLAN



Fuente: Autores del proyecto

Algunas de sus características más importantes son:

MANEJO GENERAL

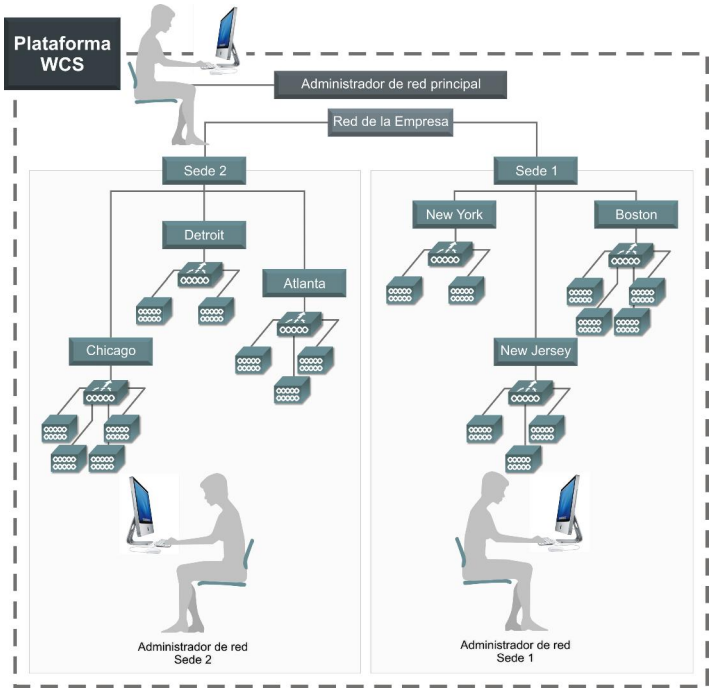
- Configuración de plantillas: Los administradores pueden asignar plantillas tanto a un punto de acceso en particular como a un grupo o a todos los puntos de acceso de un grupo de movilidad. Existe una variedad de plantillas para manejar sistemas WLAN, seguridad, control de acceso, 802.11 a/b/g/n, puntos de acceso inválidos y servidores TFTP

- Manejo del Software: Actualización del software de los puntos de acceso y de los controladores desde un solo punto.
- Manejo de privilegios de usuarios basado en grupos: Permite la creación de grupos y asignación de niveles de privilegios a cada grupo de trabajo.
- Auditoreo de la red: Los administradores pueden inspeccionar la red en busca de diferencias entre la configuración actual de los puntos de acceso y los controladores con respecto a la configuración guardada en el software. Al percibir discrepancias entre pueden elegir cual configuración dejar.
- SNMP: Soporta SNMP versión 1, 2 y 3.
- Interfaz HTTP y HTTPS: Puede ser visto desde cualquier navegador.
- Dominios Virtuales: Para redes inalámbricas de gran tamaño, el software WCS ofrece la posibilidad de segmentar esta gran red, en redes más pequeñas, dando la opción de que cada administrador se haga cargo de una parte específica de la red. Estos circuitos virtuales pueden bien ser creados para diferenciar ciudades, sedes de una empresa o simplemente sectores de la red con diferentes administradores. La figura 32 muestra un ejemplo de esta segmentación.
- Monitoreo de la Red: La propiedad de monitoreo permite la visualización del estado de las señales de radio frecuencia de la red, detectando así huecos de cobertura o puntos de acceso con poca cobertura.
- Solución de Problemas de la Red: Con el manejo de reportes de errores y facilitando la búsqueda por tipos de problemas, como nivel de ruido, radio de la señal de ruido, interferencia, amplitud de la señal, clientes, controladores, puntos de acceso o seguridad.
- Reportes: Se puede configurar la generación de reportes que mejoren el manejo de la información y aumenten el control del administrador sobre la red. La herramienta de generación de reportes del WCS incluye:

  - Posibilidad de exportar los reportes en formato CSV o PDF
  - Automatizar y programar el envío de reportes
  - Enviar notificaciones vía mail.
  - Especificar el grupo o la persona en particular que recibirá el reporte.
  - Configurar y modificar la frecuencia de los reportes.
  - Configurar el almacenamiento de información de los reportes.

Los reportes creados por el software WCS pueden ser acerca del inventario, el desempeño, seguridad, reportes detallados del cliente, puntos de acceso, malla y PCI.

Figura 31. Dominios virtuales creados con el WCS



Fuente: CISCO

- Solución de Movilidad: Determina a cual punto de acceso está vinculado un dispositivo inalámbrico en particular, dándole al administrador de la red una posición aproximada de donde se encuentra el dispositivo inalámbrico.

SEGURIDAD:

- Acceso seguro de invitados: Favorece el manejo de invitados a la organización, dándoles a las personas externas una entrada controlada a la red.

  Los permisos a los usuarios pueden programarse con anterioridad enviándole por mail al invitado un nombre de usuario y password. Es posible crear una interfaz HTML para la entrada del invitado a la red, se puede programar fecha y hora y lugar (edificio o piso especifico) a la cual el invitado tendrá permiso de entrar a la red de la organización, también existe la posibilidad de limitar el ancho de banda del invitado.
- Seguridad inalámbrica y protección de la red: El software WCS incluye diversas herramientas de seguridad de la red, entre las cuales se puede nombrar:

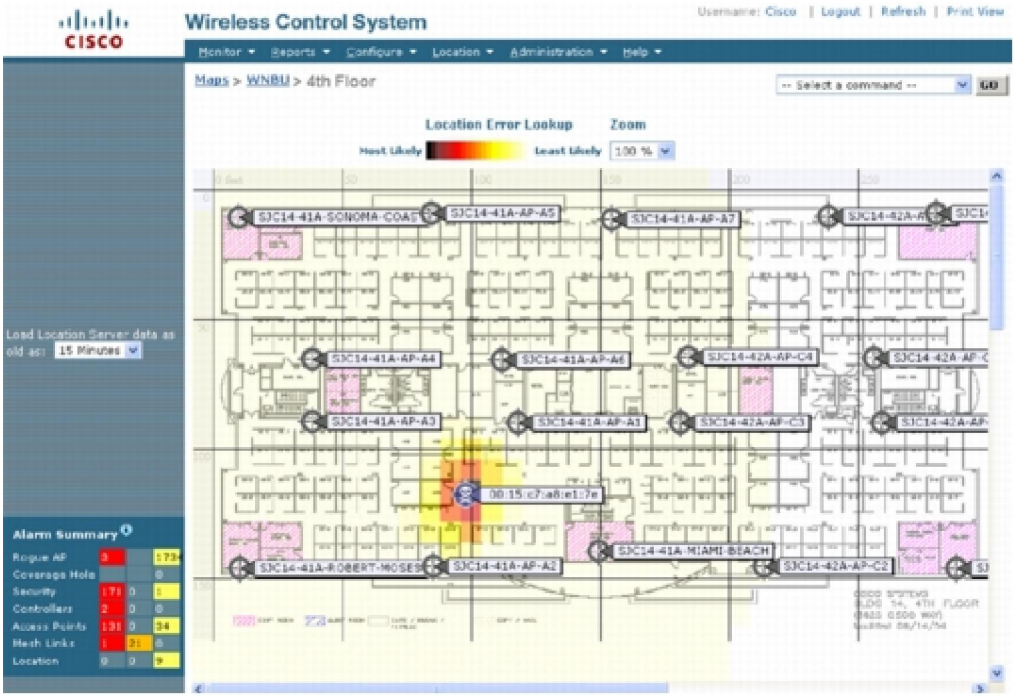
  - Sistema de detección y prevención de intrusos.

- Aviso de ataques RF y protección por manejo del frame.
- Detección, localización y contención de dispositivos inalámbricos no autorizados.
- Autenticación 802.1X.
- Lista de exclusión de usuarios.

Este software permite llevar a cabo un control estructurado a base de políticas como las planteadas en el capítulo 3, pues auxilia el desempeño relacionado con el servicio, la red como un todo y la inspección de elementos a nivel individual en lo concerniente al grado organizacional. Igualmente, sus características cumplen con los requerimientos funcionales del esquema de gestión.

Cabe aclarar que esta propuesta hace parte de un caso específico donde los equipos de la red son CISCO y la solución se planteó con el mismo proveedor, sin embargo se encuentran en el mercado software de monitoreo, entre otros, para el control de WLAN que no son el objeto de estudio del presente trabajo.

Figura 32 Captura de pantalla del programa WCS al detectar un AP no autorizado



Fuente: CISCO

5 CONCLUSIONES Y RECOMENDANCIONES

- Esta investigación permitió responder la inquietud que suscitó en primer lugar la elaboración de este trabajo; es claro ahora que los problemas que se presentan en las organizaciones con la integración de redes WLAN a las corporativas no son consecuencia de la tecnología como tal, sino desaciertos en cuanto a diseño y elección de equipos de red, implementación y administración de los mismos, a causa del desconocimiento de los estándares y por ende de la tecnología.

- Independientemente de las necesidades de la organización, la arquitectura centralizada facilita el despliegue de las WLAN en términos de administración y control, pues permite no solo tener una visión general de la red sino a vez particular de los elementos que componen el área de cobertura.

- La elección de los puntos de acceso juega un papel importante en materia de funcionalidad y operación ya que esto favorece la toma de acciones para el establecimiento de políticas de control y mantenimiento, así como de la selección del controlador que los administra.

- Como norma básica de seguridad en entornos corporativos y como complemento de la arquitectura jerárquica, se recomienda "aislar" la red WLAN de la empresa de la cableada y ubicar los servidores que gestionen los servicios que se desea prestar a los usuarios inalámbricos en una DMZ (DisMilitarized Zone) para que retransmita estas peticiones de los servicios a los servidores de la empresa.

- El mecanismo IEEE802.11i es el único mecanismo específico para redes WLAN que puede considerarse seguro para entornos corporativos. Sin embargo, en el caso de algunos fabricantes es necesario cambiar los puntos de acceso WLAN previamente instalados por un modelo que soporte IEEE802.11i. Además, actualmente los dispositivos PDA existentes no son compatibles con el algoritmo de cifrado AES empleado por el mecanismo IEEE802.11i por falta de capacidad de procesamiento.

  Una alternativa a IEEE802.11i es WPA. WPA aporta mejoras importantes con respecto a WEP, aunque el algoritmo de cifrado haya sido quebrantado sólo es posible realizar ataques que comprometan la información cifrada en el modo de operación personal (WPA-PSK). Por otra parte, WPA, al igual que IEEE802.11i, ofrece gestión dinámica de las claves.

- Como se puede concluir, el control y la administración de WLANs esta sustentada en los principios de flexibilidad y disponibilidad de la red, proporcionando una

extensión de LAN existente, por lo tanto sus políticas de control y gestión entrañan aspectos de seguridad y conectividad desde y hacia la red corporativa cableada.

- Aunque la red analizada en el presente trabajo, es una red, en su mayoría, confiable, además de contar con personal capacitado para su planeación y mantenimiento, se encontraron falencias en algunas zonas en cuanto a esquemas de seguridad, no solo en los mecanismos de protección es decir los protocolos empleados, sino a nivel de arquitectura. Se recomienda para este caso particular que emigren a nuevos diseños como los propuestos para que la WLAN esté a la altura de cualquier necesidad de seguridad y privacidad tanto para los usuarios de la empresa como para los visitantes.

- Se concluye que con la arquitectura propuesta en el capitulo cuatro, no solo se logra tener una mejor distribución y mayor seguridad en la toda la red de la empresa, al dividir la porción de red cableada de la parte de red inalámbrica. De igual forma con la introducción de los controladores de acceso y con la implementación del software de monitoreo, se logra un mejor desempeño, control, administración, gestión y apoyo a las medidas de la organización.

- Actualmente la empresa no cuanta con un software de monitoreo y gestión para la WLAN, precisamente por ello y tomando como base la arquitectura jerárquica propuesta, se investigó por un software que facilitara la integración y la administración de la red al realizar monitoreo y control del conjunto de controladores y los puntos de acceso asociados a él o ellos, el fin, favorecer las acciones de las políticas de control propuestas en el presente trabajo, sobretodo en lo concerniente a la detección de equipos intrusivos o no autorizados y el manejo de la potencia de radio emitido por cada punto de acceso.

BIBLIOGRAFÍA

- GAST, Mathew, 802.11 Wireless Netwoks: The Definitive Guide, O 'Reilly. April 2002.
- FLEXTRONICS, T. Sridhar. The Internet Protocol Journal, Wireless LAN Switches, Functions and Deployment. Volume 9, Number 3. Septembre 2006
- 59th IETF meeting, CAPWAP Architecture Draft, Lily Yang Intel Corp. March 3, 2004.
- MANI, Mahalingam (*Avaya),* O'HARA, Bob (*Airespace),* YANG, Lily (*Intel)* CAPWAP Architecture. 2003
- www.cisco.com
- PELLEJERO Izaskun, ANDREU Fernando, LESTA Amaia. Fundamentos y aplicaciones de Seguridad en redes WLAN, Febrero 2006.
- MADRID MOLINA, Juan Manuel. Seguridad en redes inalámbricas 802.11. Abril 2004
- ARÉVALO JIMÉNEZ, Fernando Andrés. Como Escoger e Implementar una VPN Conceptos Teóricos Y Prácticos. 2003
- WESLEY, Addison. Real 802.11. Security Wi-Fi Protected Access and 802.11i. 2003.
- www.enpresadigitala.net
- O'Reilly - 802.11 Security - Securing Wireless Networks. 2002.
- CAPWAP Functional Classifications Prepared for 59th IETF CAPWAP WG 03 March, 2004
- CLANCY, T. Charles. CAPWAP System Security. IETF 64, CAPWAP WG. Department of Computer Science University of Maryland, College Park. November 7, 2005.
- YANG, Shi and PERKINS, David T. CAPWAP Protocol and Dot11 Binding MIB. IETF 70th 3 Dec 2007, Vancouver.

ANEXOS

ANEXO 1

Cisco Aironet 1240AG Series 802.11A/B/G Access Point

Cisco® Aironet® 1240AG Series Access Points deliver the versatility, high capacity, security, and enterprise-class features demanded by WLAN customers. These IEEE 802.11a/b/g access points are designed specifically for challenging RF environments such as factories, warehouses, and large retail establishments that require the antenna versatility associated with connectorized antennas, a rugged metal enclosure, and a broad operating temperature range. The Cisco Aironet 1240AG Series provides local as well as inline power, including support for IEEE 802.3af Power over Ethernet (PoE).

The Cisco Aironet 1240AG Series is a component of the Cisco Unified Wireless Network, a comprehensive solution that delivers an integrated, end-to-end wired and wireless network. Using the radio and network management features of the Cisco Unified Wireless Network for simplified deployment, the Cisco Aironet 1240AG Series extends the security, scalability, reliability, ease of deployment, and manageability available in wired networks to the wireless LAN.

The Cisco Aironet 1240AG Series is available in two versions: unified or autonomous. Unified access points operate with the Lightweight Access Point Protocol (LWAPP) and work in conjunction with Cisco wireless LAN controllers and the Cisco Wireless Control System (WCS). When configured with LWAPP, the Cisco Aironet 1240AG Series can automatically detect the best-available Cisco wireless LAN controller and download appropriate policies and configuration information with no manual intervention. Autonomous access points are based on Cisco IOS® Software and may optionally operate with the CiscoWorks Wireless LAN Solution Engine (WLSE). Autonomous access points, along with the CiscoWorks WLSE, deliver a core set of features and may be field-upgraded to take advantage of the full benefits of the Cisco Unified Wireless Network as requirements evolve.

Award-Winning Security

The Cisco Aironet 1240AG Series has achieved National Institute of Standards and Technology (NIST) FIPS 140-2 level 2 validation and is in process for Common Criteria validation under the National Information Assurance Partnership (NIAP) program.

The Cisco Aironet 1240AG Series supports 802.11i, Wi-Fi Protected Access (WPA), WPA2, and numerous Extensible Authentication Protocol (EAP) types. WPA and WPA2 are the Wi-Fi Alliance certifications for interoperable, standards-based WLAN security. These certifications support IEEE 802.1X for user-based authentication, Temporal Key Integrity Protocol (TKIP) for WPA encryption, and Advanced Encryption Standard (AES) for WPA2 encryption. These certifications help to ensure interoperability between Wi-Fi-certified WLAN devices from different manufacturers.

The Cisco Aironet 1240AG Series hardware-accelerated AES encryption supports enterprise-class, government-grade secure encryption over the WLAN without compromising performance. IEEE 802.1X authentication helps to ensure that only authorized users are allowed on the network. Backward compatibility and support for WPA client devices running TKIP, the RC4 encryption algorithm, is also supported by the Cisco Aironet 1240AG Series.

Cisco Aironet 1240AG Series Access Points operating with LWAPP support Cisco Unified Intrusion Detection System/Intrusion Prevention System (IDS/IPS), a software feature that is part of the Cisco Self-Defending Network and is the industry's first integrated wired and wireless security solution. Cisco Unified IDS/IPS takes a comprehensive approach to security—at the wireless edge, wired edge, WAN edge, and through the data center. When an associated client sends malicious traffic through the Cisco Unified Wireless Network, a Cisco wired IDS device detects the attack and sends shun requests to Cisco wireless LAN controllers, which will then disassociate the client device.

Autonomous or unified Cisco Aironet 1240AG Series Access Points support management frame protection for the authentication of 802.11 management frames by the wireless network infrastructure. This allows the network to detect spoofed frames from access points or malicious users impersonating infrastructure access points. If an access point detects a malicious attack, an incident will be generated by the access point and reports will be gathered on the Cisco wireless LAN controller, Cisco WCS, or CiscoWorks WLSE.

Applications

Designed for rugged environments and installations that require antenna versatility, the Cisco Aironet 1240AG Series features antenna connectors for extended range or coverage versatility and more flexible installation options. Manufacturing applications, for example, can place WLANs in hazardous locations and remotely place antennas in the hazardous locations while securing the Cisco Aironet 1240AG Series Access Points. The access point without wired connection will use the 5-GHz radio to wirelessly connect to the other access point for backhaul to the network.

The metal housing and industrial-grade components of the Cisco Aironet 1240AG Series provide the ruggedness and extended operating temperature range required in factories, warehouses, "big box" retail environments, and similar facilities. High transmit power, receive sensitivity, and delay spread for both 2.4-GHz and 5-GHz radios provide the long range and large coverage area consistent with these applications. 5-GHz radios are used as wireless bridges between access points for backhaul to the network.

Access points may be placed above ceilings or suspended ceilings, allowing antennas to be discreetly placed below drop ceilings. The UL 2043 rating of the Cisco Aironet 1240AG Series allows the access points to be placed above ceilings in plenum areas regulated by municipal fire codes. Public access applications such as large hotel buildings may also present a challenging RF environment; the antenna versatility of the Cisco Aironet 1240AG Series, together with industry-leading range and coverage, provides reliable performance for the most demanding environments.

Features and Benefits

Table 1 lists the features and benefits of Cisco Aironet 1240AG Series Access Points.

Table 1. Features and Benefits of Cisco Aironet 1240AG Series Access Points

Feature	Benefit
Dual 802.11a and 802.11g Radios	Provides up to 108 Mbps of capacity in a single device for industry-leading capacity and compatibility with older 802.11b clients.
Dual RP-TNC Antenna Connectors for Both 2.4-GHz and 5-GHz Radios	Antenna connectors support a variety of Cisco 2.4-GHz and 5-GHz antennas, providing range and coverage versatility.
Link-Role Flexibility	Autonomous access points can function as an access point or bridge, whether set up as a single-band or dual-band platform, allowing each radio to be individually configured as an access point repeater, root bridge, non-root bridge, or workgroup bridge, enabling a broad array of applications.
Cisco Unified IDS/IPS	This integrated software feature is part of the Cisco Self-Defending Network and is the industry's first integrated wired and wireless security solution. When a trusted client acts maliciously, the wired IDS detects the attack and sends shun requests to Cisco WLAN controllers, which will then disassociate the client device.
Management Frame Protection	This feature provides for the authentication of 802.11 management frames by the wireless network infrastructure. This allows the network to detect spoofed frames from access points or malicious users impersonating infrastructure access points. If an access point detects a malicious attack, an incident will be generated by the access points and reports will be gathered on the Cisco wireless LAN controller, Cisco WCS, or CiscoWorks WLSE.
Security	**Authentication** Security Standards WPA WPA2 (802.11i) Cisco TKIP Cisco message integrity check (MIC) IEEE 802.11 WEP keys of 40 bits and 128 bits **802.1X EAP types:** EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) Protected EAP-Generic Token Card (PEAP-GTC) PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAP) EAP-Transport Layer Security (EAP-TLS) EAP-Tunneled TLS (EAP-TTLS) EAP-Subscriber Identity Module (EAP-SIM) Cisco LEAP **Encryption:** AES-CCMP encryption (WPA2) TKIP (WPA) Cisco TKIP WPA TKIP IEEE 802.11 WEP keys of 40 bits and 128 bits
Currently Supports 12 Non-Overlapping Channels, with Potentially up to 23 Channels	Lower potential interference with neighboring access points simplifies deployment. Fewer transmission errors deliver greater throughput.
Rugged Metal Housing	Metal case and rugged features support deployment in factories, warehouses, the outdoors (NEMA enclosure required), and other industrial environments.

Feature	Benefit
UL 2043 Plenum Rating and Extended Operating Temperature	Supports installation in environmental airspaces such as areas above suspended ceilings.
Multipurpose and Lockable Mounting Bracket	Provides greater flexibility in installation options for site surveys, as well as theft deterrence.
Both Local and Inline Power Supported, Including IEEE 802.1af PoE	Power can be supplied using the Ethernet cable, eliminating the need for costly electrical power line runs to remotely installed access points. The access points can be powered by IEEE 802.3af PoE, Cisco inline power switches, single port power injectors, or local power.
Hardware-Assisted AES Encryption	Provides high security without performance degradation.
Cisco Green Bulk Packaging	To reduce product packaging and preserve the environment, the Cisco Aironet 1240 Series may be ordered in a bulk package that includes 10 access points and 10 mounting kits.

Summary

Cisco Aironet 1240AG Series Access Points feature antenna connectors for greater range and coverage versatility using a broad selection of available Cisco antennas, as well as a rugged metal housing for operation over extended temperature ranges typical of industrial environments. Dual 802.11a and 802.11g radios offer a combined capacity of 108 Mbps, meeting the performance requirements of the most demanding applications, while hardware-assisted AES encryption provides uncompromised support for interoperable IEEE 802.11i and WPA2 security. The Cisco Aironet 1240AG Series delivers enterprise-class features for challenging RF environments.

Product Specifications

Table 2 lists the product specifications for Cisco Aironet 1240AG Series Access Points.

Table 2. Product Specifications for Cisco Aironet 1240AG Series Access Points

Item	Specification
Part Number for Individual Access Points	AIR-AP1242AG-x-K9 AIR-LAP1242AG-x-K9 **Regulatory domains**: (x = regulatory domain) • A = FCC • C = China • E = ETSI • I = Israel • J = Japan • K = Korea • N = North America (excluding FCC) • P = Japan2 • S = Singapore • T = Taiwan Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country, please visit: http://www.cisco.com/go/aironet/compliance Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.

Item	Specification
Part Number for Cisco Green Bulk Packaging	• AIR-AP1242-x-K9-10 (Cisco IOS Software) • AIR-LAP1242-xK9-10 (Cisco Unified Wireless Network Software) **Note**: The Cisco Aironet 1242AG Series may be ordered with Cisco IOS Software to operate as an autonomous AP with Cisco Unified Wireless Network Software using LWAPP. When the 1242AG is operating as a lightweight AP a WLAN controller is required. • Regulatory Domains: (x = Regulatory Domain) • A = FCC • E = ETSI • Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country please visit: http://www.cisco.com/go/aironet/compliance
Software	• Cisco IOS Software Release 12.3(8)JA or later (autonomous). • Cisco IOS Software Release 12.3(11)JX or later (Lightweight Mode). • Cisco Unified Wireless Network Software Release 4.0 or later.
Data Rates Supported	• 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
Network Standard	• IEEE 802.11a, 802.11b, and 802.11g
Uplink	• Autosensing 802.3 10/100BASE-T Ethernet
Frequency Band and Operating Channels	**Americas (FCC)** • 2.412 to 2.462 GHz; 11 channels • 5.15 to 5.35, 5.725 to 5.825 GHz; 12 channels **China** • 2.412 to 2.472 GHz; 13 channels • 5.725 to 5.825 GHz; 4 channels **ETSI** • 2.412 to 2.472 GHz; 13 channels • 5.15 to 5.35 GHz; 8 channels • 5470 to 5725 MHz; 11 channels **Israel** • 2.432 to 2.472 GHz; 9 channels • 5.15 to 5.35 GHz; 8 channels **Japan** • 2.412 to 2.472 GHz; 13 channels Orthogonal Frequency Division Multiplexing (OFDM) • 2.412 to 2.484 GHz; 14 channels Complementary Code Keying (CCK) • 5.15 to 5.25 GHz; 4 channels **Korea** • 2.412 to 2.472 GHz; 13 channels • 5.15 to 5.35, 5.46 to 5.72, 5.725 to 5.825; 19 channels **North America (not FCC)** • 2.412 to 2.462 GHz; 11 channels • 5.15 to 5.35, 5.725 to 5.825 GHz; 12 channels **Japan2** • 2.412 to 2.472 GHz; 13 channels OFDM • 2.412 to 2.484 GHz; 14 channels CCK • 5.15 to 5.35 GHz; 8 channels **Singapore** • 2.412 to 2.472 GHz; 13 channels • 5.15 to 5.35, 5.725 to 5.825 GHz; 12 channels **Taiwan** • 2.412 to 2.462 GHz; 11 channels • 5.25 to 5.35, 5.725 to 5.825 GHz; 7 channels
Non-Overlapping Channels	• 802.11a: 12 channels (FCC; other regulatory domains support different numbers of 802.11a channels) • FCC currently supports 12 non-overlapping channels, with potentially up to 23 channels via a future firmware release depending on FCC rules 802.11b/g: 3 channels

<table>
<tr><th>Item</th><th colspan="4">Specification</th></tr>
<tr><td>Receive Sensitivity (Typical)</td><td colspan="2">802.11a
6 Mbps: –88 dBm
9 Mbps: –87 dBm
12 Mbps: –86 dBm
18 Mbps: –85 dBm
24 Mbps: –82 dBm
36 Mbps: –79 dBm
48 Mbps: –74 dBm
54 Mbps: –73 dBm</td><td colspan="2">802.11g
1 Mbps: –96 dBm
2 Mbps: –93 dBm
5.5 Mbps: –91 dBm
6 Mbps: –91 dBm
9 Mbps: –85 dBm
11 Mbps: –88 dBm
12 Mbps: –83 dBm
18 Mbps: –81 dBm
24 Mbps: –78 dBm
36 Mbps: –74 dBm
48 Mbps: –73 dBm
54 Mbps: –73 dBm</td></tr>
<tr><td>Available Transmit Power Settings
(Maximum Power Setting will Vary by Channel and According to Individual Country Regulations)</td><td>802.11a
OFDM:
17 dBm (50 mW)
15 dBm (30 mW)
14 dBm (25 mW)
11 dBm (12 mW)
8 dBm (6 mW)
5 dBm (3 mW)
2 mW (2 dBm)
–1 dBm (1 mW)</td><td>802.11g
CCK:
20 dBm (100 mW)
17 dBm (50 mW)
14 dBm (25 mW)
11 dBm (12 mW)
8 dBm (6 mW)
5 dBm (3 mW)
2 dBm (2 mW)
–1 dBm (1 mW)</td><td colspan="2">OFDM
17 dBm (50 mW)
14 dBm (25 mW)
11 dBm (12 mW)
8 dBm (6 mW)
5 dBm (3 mW)
2 dBm (2 mW)
–1 dBm (1 mW)</td></tr>
<tr><td>Range (Typical)</td><td colspan="2">Indoor (Distance Across Open Office Environment):</td><td colspan="2">Outdoor:</td></tr>
<tr><td></td><td>802.11a:
85 ft (26 m) at 54 Mbps
150 ft (46 m) at 48 Mbps
210 ft (64 m) at 36 Mbps
230 ft (70 m) at 24 Mbps
260 ft (79 m) at 18 Mbps
280 ft (85 m) at 12 Mbps
310 ft (94 m) at 9 Mbps
330 ft (100 m) at 6 Mbps</td><td>802.11g:
105 ft (32 m) at 54 Mbps
180 ft (55 m) at 48 Mbps
260 ft (79 m) at 36 Mbps
285 ft (87 m) at 24 Mbps
330 ft (100 m) at 18 Mbps
355 ft (108 m) at 12 Mbps
365 ft (111 m) at 11 Mbps
380 ft (116 m) at 9 Mbps
410 ft (125 m) at 6 Mbps
425 ft (130 m) at 5.5 Mbps
445 ft (136 m) at 2 Mbps
460 ft (140 m) at 1 Mbps</td><td>802.11a:
100 ft (30 m) at 54 Mbps
300 ft (91 m) at 48 Mbps
425 ft (130 m) at 36 Mbps
500 ft (152 m) at 24 Mbps
550 ft (168 m) at 18 Mbps
600 ft (183 m) at 12 Mbps
625 ft (190 m) at 9 Mbps
650 ft (198 m) at 6 Mbps</td><td>802.11g:
120 ft (37 m) at 54 Mbps
350 ft (107 m) at 48 Mbps
550 ft (168 m) at 36 Mbps
650 ft (198 m) at 24 Mbps
750 ft (229 m) at 18 Mbps
800 ft (244 m) at 12 Mbps
820 ft (250 m) at 11 Mbps
875 ft (267 m) at 9 Mbps
900 ft (274 m) at 6 Mbps
910 ft (277 m) at 5.5 Mbps
940 ft (287 m) at 2 Mbps
950 ft (290 m) at 1 Mbps</td></tr>
<tr><td></td><td colspan="4">Measured with 2.2-dBi dipole antenna for 2.4 GHz, and 3.5-dBi omnidirectional antenna for 5 GHz.</td></tr>
</table>

Item	Specification
Compliance	**Standards** Safety: • UL 60950-1 • CAN/CSA-C22.2 No. 60950-1 • UL 2043 • IEC 60950-1 • EN 60950-1 • NIST FIPS 140-2 level 2 validation Radio approvals: • FCC Part 15.247, 15.407 • RSS-210 (Canada) • EN 300.328, EN 301.893 (Europe) • ARIB-STD 33 (Japan) • ARIB-STD 66 (Japan) • ARIB-STD T71 (Japan) • AS/NZS 4268.2003 (Australia and New Zealand) • EMI and susceptibility (Class B) • FCC Part 15.107 and 15.109 • ICES-003 (Canada) • VCCI (Japan) • EN 301.489-1 and -17 (Europe) • EN 60601-1-2 EMC requirements for the Medical Directive 93/42/EEC Security: • 802.11i, WPA2, WPA • 802.1X • AES, TKIP Other: • IEEE 802.11g and IEEE 802.11a • FCC Bulletin OET-65C • RSS-102
Antenna Connectors	2.4 GHz • Dual RP-TNC connectors 5 GHz • Dual RP-TNC connectors
Status LEDs	• Status LED indicates operating state, association status, error/warning condition, boot sequence, and maintenance status. • Ethernet LED indicates status of activity over the Ethernet. • Radio LED indicates status of activity over the radio.
Dimensions (W x L x H)	• 6.6 x 8.5 x 1.1 in. (16.76 x 21.59 x 2.79 cm)
Weight	• 2.0 lbs
Environmental	• Non-operating (storage) temperature: –40 to 185°F (– 40 to 85°C) • Operating temperature: –4 to 131°F (–20 to 55°C) • Operating humidity: 10 to 90 percent (non-condensing)
System Memory	• 32 MB RAM • 16 MB flash
Input Power Requirements	• 100 to 240 VAC; 50 to 60Hz (power supply) • 36 to 57 VDC (device)
Powering Options	• Local power • 802.3 AF switches • Cisco higher-power switches capable of supporting 13W or greater • Cisco Aironet power injectors (PWRINJ3 and PWRINJ-FIB) • Third-party PoE devices (must meet input power and power draw requirements)

Item	Specification
Power Draw	12.95W maximum **Note:** 12.95W is the maximum power required at the powered device. If the access point is being used in a PoE configuration, the power drawn from the power sourcing equipment will be higher by some amount dependent on the length of the interconnecting cable. This additional power may be as high as 2.45W, bringing the total system power draw (access point and cabling) to 15.4W.
Warranty	One year
Wi-Fi Certification	

System Requirements

Table 3 lists the system requirements for Cisco Aironet 1240AG Series Access Points.

Table 3. System Requirements for Cisco Aironet 1240AG Series Access Points

Access Method	Description
Browser	Using the Web browser management GUI requires a computer running Internet Explorer Version 6.0 or later, or Netscape Navigator Version 7.0 or later.
PoE	Power sourcing equipment compliant with Cisco inline power or IEEE 802.3af, and providing at least 12.94W at 48 VDC

Ordering Information

To place an order, visit the Cisco Ordering Website at:
http://www.cisco.com/en/US/ordering/index.shtml

Service and Support

Cisco Systems® offers a wide range of services programs to accelerate customer success. These innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, visit Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about the Cisco Aironet 1240AG Series, visit http://www.cisco.com/go/wireless or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-338896-05 06/08

ANEXO 2

Cisco Wireless LAN Controllers

Delivering efficient and secure wireless control

Cisco® Wireless LAN Controllers work in conjunction with Cisco Lightweight Access Points and the Cisco Wireless Control System (WCS) to provide systemwide wireless LAN (WLAN) functions. As components of the Cisco Unified Wireless Network, Cisco Wireless LAN Controllers present network administrators with the visibility and control necessary to effectively and securely manage business-class WLANs and mobility services, such as enhanced security, voice, guest access, and location services.

Cisco Wireless LAN Controllers help reduce overall operational expenses by simplifying network deployment, operations, and management. The flexibility allows network managers to design networks to meet their specific needs, whether implementing standalone or highly integrated network designs.

Cisco 4400 Wireless LAN Controller

Cisco 2106 Wireless LAN Controller

Cisco Catalyst® 6500 Series Wireless Services Module (WiSM)

Cisco Catalyst 3750G Integrated WLAN Controller

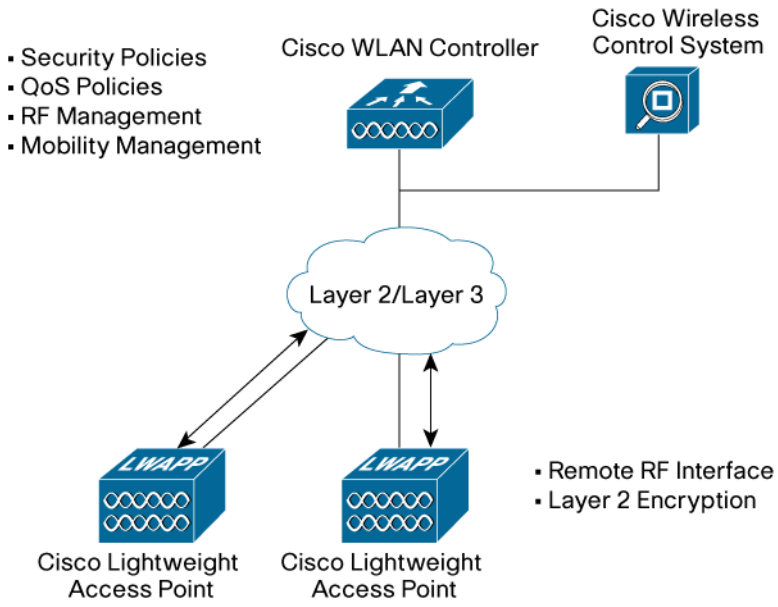
Cisco WLAN Controller Module for Cisco Integrated Services Routers

Features and Benefits

- Business-class RF security and WLAN security policy monitoring
- Clear visibility into and centralized control of the RF environment
- High performance through reliable coverage and optimized bandwidth
- Mobility features for uninterrupted network access for roaming users
- Scalability to meet the requirements of small businesses to large enterprises
- Investment protection
- Reduced overall operational expenses, achieved by simplifying network deployment, operations, and management

The Cisco Unified Wireless Network is designed to enhance productivity, collaboration, and responsiveness in organizations of all types and sizes. Cisco Wireless LAN Controllers (Figure 1) enable enterprises to create and enforce policies for business-critical applications such as mobile healthcare, inventory management, retail point of sale, video surveillance, real-time data access, asset tracking, and network visibility. Multiple WLAN controllers automatically discover each other and transparently coordinate WLAN services across themselves. In this way, Cisco Wireless LAN Controllers work together as a single, transparent system to deliver a scalable WLAN network with thousands of access points.

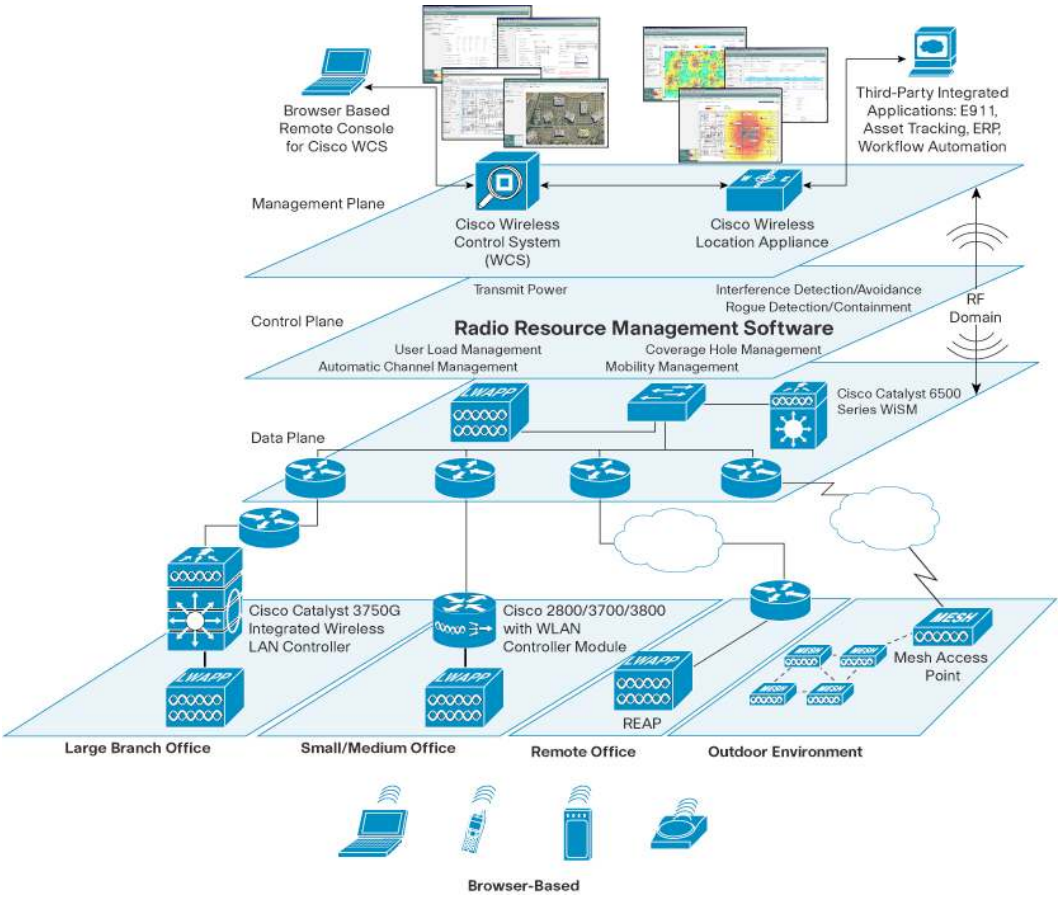
Figure 1. Cisco Unified Wireless LAN with Secure Communication Between Lightweight Access Points and Controllers



Intelligent RF Management

Cisco Wireless LAN Controllers take the complexity out of RF management by supporting a series of RF-specific management tools (Figure 2). These tools include dynamic channel assignment, RF interference mitigation, client load balancing, and power transmit control. The RF management tools provide visibility into the wired and wireless network, so network managers can view performance, usage, availability, and reliability statistics from a single interface. These features also support continuous site-survey services to help ensure that the wireless network provides optimal coverage and capacity.

Figure 2. Networkwide RF Intelligence



Specific intelligent RF capabilities managed by Cisco Wireless LAN Controllers include:

- **Dynamic channel assignment**—802.11 channels are adjusted to optimize network coverage and performance based on changing RF conditions.
- **Interference detection and avoidance**—The system detects interference and recalibrates the network to avoid performance problems.
- **Load balancing**—The system provides automatic load balancing of users across multiple access points for optimum network performance, even under heavy loads.
- **Coverage hole detection and correction**—Radio Resource Management (RMM) software detects coverage holes and attempts to correct them by adjusting the power output of access points.
- **Dynamic power control**—The system dynamically adjusts the power output of individual access points to accommodate changing network conditions, helping ensure predictable wireless performance and availability.

Enhanced Security

A unified network allows IT to maintain unified network security policies and detect and respond to alerts more quickly. Cisco Wireless LAN Controllers adhere to the strictest level of security standards, including:

- Standard 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, and Wired Equivalent Privacy (WEP)
- Standard 802.1X with multiple Extensible Authentication Protocol (EAP) types: Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunneled TLS (EAP-TTLS), EAP with Flexible Authentication through Secure Tunneling (EAP-FAST), EAP with subscriber identity module (EAP-SIM), and Cisco LEAP
- Management frame protection
- Federal Information Processing Standards (FIPS) 140-2 Level 2 validation

The result is the industry's most comprehensive WLAN security solution.

In the Cisco WLAN architecture, access points act as air monitors, communicating real-time information about the wireless domain to WLAN controllers. All security threats are rapidly identified and presented to network administrators through the Cisco WCS, where accurate analysis can take place and corrective action can be taken.

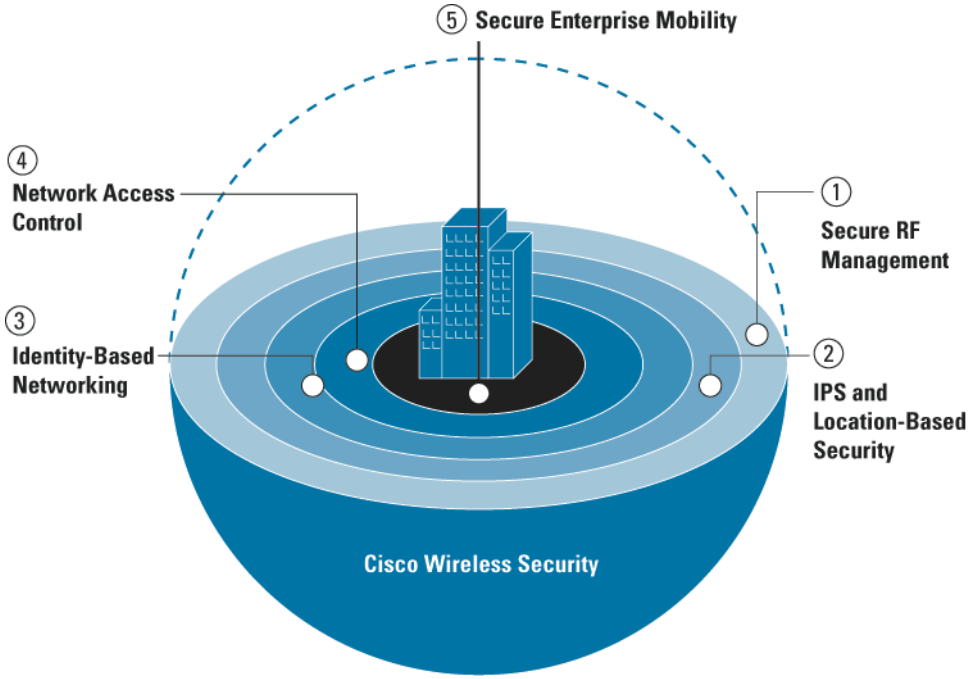
Cisco addresses WLAN security by offering multiple layers of protection, as Figure 3 shows. The multiple layers of WLAN protection include:

- **RF security**—The Cisco WLAN system detects and avoids 802.11 interference and controls unwanted RF propagation.
- **Wireless LAN intrusion prevention, location, and correlation**—The Cisco WLAN system not only detects rogue devices or potential wireless threats, but also locates these devices, enabling systems administrators to quickly assess the threat level and take immediate action to mitigate threats as required. The intrusion-detection-system (IDS) signature engine on controllers and on the Cisco WCS automatically eliminates duplicate alerts for rogue access points, rogue clients, and IDS signatures that previously occurred when two or more access points detected the same attacker. Now instead of one IDS alert from each detecting access point, a single alert is generated for the attack.
- **Identity-based networking**—IT staff must support many different user access rights, device formats, and application requirements when securing WLANs. The Cisco WLAN system enables enterprises to deliver individualized security policies to wireless users or groups of users, including:
  - **Layer 2 security**—802.1x (PEAP, TLS, TTLS, FAST, SIM, and LEAP), WPA, and 802.11i (WPA2)
- **Layer 3 security (and above)—**IP Security (IPsec) and Web authentication
  - **VLAN assignments**
  - **Access control lists (ACLs)**—IP restrictions, protocol types, port, and differentiated-services-code-point (DSCP) value
  - **Quality of service (QoS)**—Multiple service levels, bandwidth contracts, traffic shaping, and RF usage

- **Authentication, authorization, and accounting (AAA) and RADIUS user session policies and rights management**
- **Management frame protection**—Management frame protection (MFP) provides for the authentication of 802.11 management frames by the wireless network infrastructure, allowing the network to detect spoofed frames from access points or malicious users impersonating infrastructure access points.

- **Network Admission Control (NAC)**—The Cisco WLAN system enforces policies pertaining to client posture and configuration and behavior to ensure that only end-user devices with appropriate security utilities and health can gain access to the network.

Figure 3. Multiple Layers of Wireless LAN Protection



Reliability

Cisco delivers the highest level of reliability for mission-critical wireless networks. If an access point failure occurs, Cisco Wireless LAN Controllers automatically adjust power on adjacent access points to cover the area where the failed access point provided service. If an individual controller failure occurs, access points automatically find a backup WLAN controller to keep wireless service available. Cisco Wireless LAN Controllers can be deployed in an N + 1 redundant topology, allowing enterprises to scale their wireless networks while knowing that they are protected from both hardware and software disruptions. Only the Cisco Wireless LAN Controllers allow users to control wireless deployment costs without sacrificing reliability.

Mobility Services

The Cisco Unified Wireless Network is the first solution to provide true mobility services that enable business process improvement. Guest, voice, security, and location services can all significantly affect productivity, efficiency, and security when enabled organizationwide. The Cisco Wireless LAN Controller plays a critical role in supporting these mobility services.

Secure Guest Access

Guest access allows customers, vendors, partners, and others to wirelessly access network resources without compromising enterprise security. The WLAN controller ensures that client devices comply with security policies, and can be configured to automatically quarantine clients that pose a threat to network security. Guest access increases company productivity, facilitates real-time collaboration, and helps companies be more competitive in today's anywhere, anytime, business climate. The solution enables companies to:

- Manage guest access
- Monitor guest use of the network
- Automatically prioritize traffic to optimize network performance

Voice Services

Cisco Voice over WLAN provides business communications using Wi-Fi and cellular-compatible smart phones. Cisco Wireless LAN Controllers ensure enterprise voice services can be deployed by enabling:

- **High availability**—Real-time RF scanning and monitoring of the RF environment minimize interference and ensure high quality and availability for voice communications. Management tools for monitoring roam time, jitter, and client connectivity are critical to meet the requirements for high availability.
- **Roaming**—Cisco Wireless LAN Controllers support pervasive communications with fast (low latency) secure roaming for voice clients. They help clients optimize roaming and minimize disruption to communications.
- **Advanced QoS**—Cisco Wireless LAN Controllers support voice on the WLAN with advanced QoS features, industry-standard QoS, extended-talk-time battery life, and Call Admission Control.
- **Choice of client devices**—Cisco Wireless LAN Controllers securely interoperate with a diverse selection of wireless devices that support advanced features such as fast secure roaming and advanced QoS.

For more information about the Cisco Voice over WLAN solution, please visit: http://www.cisco.com/go/vowlan.

Location Services

Location services track the physical location of Wi-Fi devices, making possible applications such as real-time asset tracking, location-based security, and business policy enforcement. Interoperating with the Cisco WCS and Cisco Wireless Location Appliance, Cisco Wireless LAN Controllers can track the physical location of a variety of Wi-Fi devices—including laptops, voice handsets, personal digital assistants (PDAs), active Wi-Fi RF identification (RFID) tags, rogue client devices, and rogue access points. For more information about the Cisco Wireless Location Appliance, visit: http://www.cisco.com/en/US/products/ps6386/index.html

Network Management

The Cisco WCS is an optional network component that lets companies centrally plan, configure, and manage an enterprise wireless network. With an easy-to-use graphical interface, it simplifies management of multiple WLAN controllers and their associated access points. For more information about Cisco WCS, visit: http://www.cisco.com/en/US/products/ps6305/index.html

Deployment Flexibility for Branch Offices

Cost-effective Hybrid Remote Edge Access Point (REAP) functions allow remote deployment of the Cisco Aironet® 1240 AG and Aironet 1130 AG Series Access Points from the WLAN controller, making it ideal for branch office and small retail locations. With Hybrid REAP, users can choose whether they want to have traffic bridged locally or tunneled over the WAN over Lightweight Access Point Protocol (LWAPP) on a per-Service Set Identifier (SSID) basis. Because of bandwidth required, only 8 Hybrid REAPs can be used in any one location over a WAN connection. For more details, please visit: Cisco Unified Wireless Network Software Release 4.0.

Features and Benefits

All the Cisco Wireless LAN Controllers used in the Cisco Unified Wireless Network architecture offer the features described in Table 1. The main differences are in the number of access points supported, uplink capacity, and form factor.

Table 1. Features and Benefits of Cisco Wireless LAN Controllers

Feature	Benefits
Cisco Unified Wireless Network	The Cisco Unified Wireless Network reduces overall operational expenses by simplifying network deployment, operations, and management. The flexibility allows network managers to design networks to meet their specific needs, whether implementing highly integrated network designs or simple overlay networks.
Scalability	The scalable architecture of the Cisco Wireless LAN Controllers provides business-critical wireless services for locations of all sizes.
Integrated Radio Resource Management (RRM)	The system creates an intelligent RF control plane for self-configuration, self-healing, and self-optimization.
Zero-configuration deployment	The system is deployed without the need to modify existing routing and switching infrastructures or to configure access points.
Reliability	Automated recovery from lightweight access point and WLAN controller failures maximizes the availability of the wireless network.
Intuitive management interfaces	The Cisco WCS provides better visibility and control of your company's wireless network, resulting in ease of deployment and lower total cost of ownership.
Mobility management	Up to 24 Cisco Wireless LAN Controllers can be supported in a single mobility group for transparent, secure client roaming and high availability.
Enhanced security	• Enhanced security ensures authentication of clients for controlled access to network resources and encryption of client data to maintain privacy. • Intrusion detection, location, and containment preserve the integrity of wireless networks and sensitive corporate information. When an associated client sends malicious traffic, a Cisco wired IDS device detects the attack and sends shun requests to Cisco Wireless LAN Controllers, which then disassociate the client device. • The Cisco Unified Wireless Network integrates with the Cisco Self-Defending Network to limit damage from emerging security threats such as viruses, worms, and spyware. It also integrates with Network Admission Control to enforce security policy compliance on all wireless devices seeking to access network computing resources.
Mobility services	To facilitate integration with business processes, the Cisco Unified Wireless Network offers four mobility services: guest access, location, voice, and security.

Cisco Wireless LAN Controller Products

To meet a variety of deployment scenarios, the Cisco Wireless LAN Controller product line includes standalone controllers, integrated controllers, and modular WLAN controllers that work in conjunction with selected Cisco switches and routers.

- Cisco 4400 Series and Cisco 2106 Wireless LAN Controllers are standalone, 1-rack-unit devices.
- The Cisco Catalyst 3750G Integrated Wireless LAN Controller is integrated into a Cisco Catalyst 3750G Switch.
- The Cisco Catalyst 6500 Series WiSM and the Cisco Wireless LAN Controller Module (WLCM) are WLAN controller modules that slide into an existing Cisco Catalyst 6500 Series Switch or a Cisco Integrated Services Router, respectively.

All WLAN controllers deliver the same features and benefits, but each controller supports a different number of lightweight access points. Additionally, WLAN controller modules for the Cisco Catalyst 6500 Series Switch and Integrated Services Routers as well as the Cisco Catalyst 3750G Integrated Wireless LAN Controller can take advantage of the ACL, policies, and advanced features of the switch or router that they reside in.

Each controller can be managed centrally through the Cisco WCS or locally through the onboard WLAN controller GUI or CLI. Up to 24 controllers and 3600 lightweight access points can be clustered together to provide mobility and systemwide RF management (Table 2).

Table 2 lists specifications for the Cisco Wireless LAN Controller product line.

Table 2. Specifications for Cisco Wireless LAN Controller Products

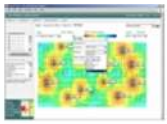
	Cisco 2106 Wireless LAN Controller	Cisco 4400 Series Wireless LAN Controller	Cisco WLCM[1]	Cisco Catalyst 3750G Integrated Wireless LAN Controller[2]	Cisco Catalyst 6500 Series WiSM[3]
Controller type	Standalone	Standalone	Module	Integrated	Module
Platform integration	–	–	Cisco 2800 and 3800 Series Integrated Services Routers	Cisco Catalyst 3750G Series Switches	Cisco Catalyst 6500 Series Switch
Number of lightweight access points supported	6	12, 25, 50, or 100	6	25 and 50	300
Deployment location	Remote location, branch office, or small office	Remote location, branch office, or campus	Remote location, branch office, or small office	Midsize organizations and enterprise branch offices	Large campus
Uplink interfaces	Two 10-/100-Mbps ports	Cisco 4402: Two 1-Gbps ports Cisco 4404: Four 1-Gbps ports	One 10-/100-Mbps port	24 Power over Ethernet (PoE) 10/100/1000 ports 32-Gbps, high-speed stacking bus	Eight 1-Gbps ports
Forwarding engine	Software	ASIC-based (Hardware)	Software	ASIC-based (Hardware)	ASIC-based (Hardware)

[1] Must be deployed with Cisco IOS® Software Release 12.4(2)XA1 or later.
[2] The Cisco Catalyst 3750G Integrated Wireless LAN Controller must be purchased as a complete unit. An existing Cisco Catalyst 3750G Switch cannot be upgraded to operate as a WLAN controller.
[3] Requires a Cisco Catalyst 6500 Series Supervisor Engine 720.

Table 3 lists ordering information for Cisco Wireless LAN Controllers, the Cisco Wireless Location Appliance, and the Cisco Wireless Control System.

Table 3. Ordering Information

Product	Features	Customer Requirements	Sales Advantages and Part No.
Wireless LAN Controllers			
Cisco 2106 Wireless LAN Controller 	• Supports up to six Cisco Aironet Lightweight Access Points. • 6 Fast Ethernet downlink Ethernet ports (2 of 6 provide power for lightweight access points). • 2 Fast Ethernet uplink Ethernet ports.	• Small to medium-sized deployments or enterprise • Branch or distributed offices	**Part Numbers** AIR-WLC2106-K9 Refer to the Cisco WLAN Controller data sheet for more details: http://www.cisco.com/en/US/products/ps7206/products_data_sheet0900aecd805aaab9.html
Cisco 4400 Series Wireless LAN Controller 	• Modular support of 12, 25, 50, or 100 Cisco Aironet Lightweight Access Points. • The Cisco 4402 with two 1-GB Ethernet ports supports configurations for 12, 25, and 50 access points. • The Cisco 4404 with four 1-GB Ethernet ports supports configurations for 100 lightweight access points. • IEEE 802.1D Spanning Tree Protocol for higher availability. • IPsec encryption. • Industrial-grade resistance to electromagnetic interferences (EMI).	• Midsize to large deployments • High availability	**Part Numbers** • AIR-WLC4402-12-K9 • AIR-WLC4402-25-K9 • AIR-WLC4402-50-K9 • ·AIR-WLC4404-100-K9 Refer to the Cisco WLAN Controller data sheet for more details: http://www.cisco.com/en/US/products/ps6308/products_data_sheet0900aecd802570b0.html
Wireless Integrated Switches and Routers			
Cisco Catalyst 6500 Series Wireless Services Module (WiSM) 	• Wireless LAN Controller for Catalyst 6500 in conjunction with up to 300 Cisco Aironet Lightweight Access Points. • IPsec encryption. • Industrial-grade resistance to electromagnetic interferences (EMI). • Intra-chassis and inter-chassis failover. • Interoperable with Cisco Catalyst 6500 Firewall and IDS Modules.	• Embedded system for the Cisco Catalyst 6500 Series infrastructure • Large-scale deployments • High availability	**Part Numbers** WS-SVC-WISM-1-K9 Refer to the Cisco Catalyst 6500 WiSM data sheet for more details: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet0900aecd80364340.html

Product	Features	Customer Requirements	Sales Advantages and Part No.
Cisco Catalyst 3750G Integrated Wireless LAN Controller 	• The Cisco Catalyst 3750G offers WLAN controller capabilities. • Modular support for 25 or 50 Cisco Aironet Lightweight Access Points per switch (and up to 200 lightweight access points per stack[4]). • IPsec encryption. • Industrial-grade resistance to EMI.	• Midsize to large deployments • High availability	**Part Numbers** • WS-C3750G-24WS-S25 • WS-C3750G-24WS-S50 Refer to the Cisco Catalyst 3750G Integrated Wireless LAN Controller data sheet for more details: http://www.cisco.com/en/US/products/ps6915/products_data_sheet0900aecd804b0879.html
Cisco Wireless LAN Controller Module for Cisco Integrated Services Routers 	• The Cisco Wireless LAN Controller Module is integrated into Cisco Integrated Services Routers. • Supports up to 6 Cisco Aironet Lightweight Access Points.	• Embedded system for the Cisco 2800 and 3800 Series Integrated Services Routers and Cisco 3700 Series Routers • Small to medium-sized deployments or branch offices	**Part Numbers** NM-AIR-WLC6-K9 Refer to the Cisco WLAN Controller Module data sheet for more details: http://www.cisco.com/en/US/products/hw/modules/ps2797/products_data_sheet0900aecd80364432.html
Wireless Location Appliance			
Cisco 2710 Series Wireless Location Appliance 	• Scalable location tracking and asset management for up to 2500 devices. • Enhanced network visibility. • Integration with a variety of technology and application partners through a rich and open application programming interface (API). • Enhanced WLAN security through accurate location of rogue access points. • Advanced planning and deployment tools for accurate calibration.	• Customers range from enterprises to vertical industries, such as healthcare, finance, retail, manufacturing, and federal organizations • Support for critical applications including high-value asset tracking, location-based security, enhanced network management, and business policy enforcement	**Part Numbers** AIR-LOC2710-L-K9 Refer to the Cisco Wireless Location Appliance data sheet for more details: http://www.cisco.com/en/US/products/ps6386/products_data_sheet0900aecd80293728.html
Wireless Network Management			
Cisco Wireless Control System (WCS) 	• Management of Cisco Wireless LAN Controllers, Cisco Aironet Lightweight Access Points, and the Cisco Wireless Location Appliance. • Modular support of 50, 100, 500, 1000, and 2500 Cisco Aironet Lightweight Access Points. • Supports up to 250 Cisco Wireless LAN Controllers. • Hierarchical maps. • WLAN planning,	• Easy management of Cisco Unified Wireless Networks • Businesses deploying mobility services • Base software for management • Additional software for location services • Compatibility with Windows and Linux	**Part Numbers** • WCS-APBASE-50 • WCS-APBASE-100 • WCS-APBASE-500 • WCS-APBASE-1000 • WCS-APBASE-2500 • WCS-APLOC-50 • WCS-APLOC-100 • WCS-APLOC-500 • WCS-APLOC-1000 • WCS-APLOC-2500 Refer to the Cisco WCS data sheet

[4] With 4 modules per stack and 50 access points per module

Product	Features	Customer Requirements	Sales Advantages and Part No.
	monitoring, configuring, and troubleshooting tools. • Policy management templates. • Centralized software upgrades. • Robust APIs. • Integrated location tracking (optional).		for more details: http://www.cisco.com/en/US/products/ps6305/products_data_sheet0900aecd802570d0.html

Summary

The Cisco Wireless LAN Controller eliminates the deployment and management complexity of wireless networks, and provides enhanced security, maximum network availability, and enhanced WLAN performance. Cisco Wireless LAN Controllers work in conjunction with the Cisco WCS and the Cisco Wireless Location Appliance to support mission-critical wireless data, voice, and video applications. As a component of the Cisco Unified Wireless Network, Cisco Wireless LAN Controllers provide network administrators with the visibility and control needed to effectively manage and secure enterprise-class WLANs.

Service and Support

Cisco offers a wide range of service programs to accelerate customer success. These innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, visit: http://www.cisco.com/en/US/products/svcs/ps2961/ps2738/serv_home.html

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

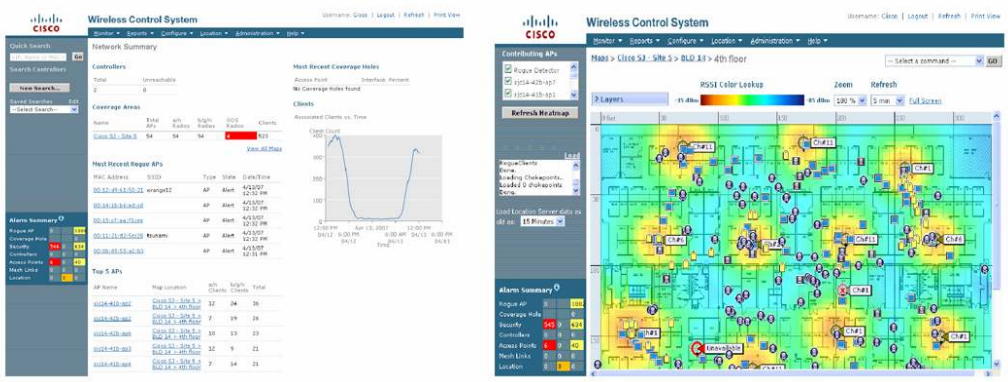
Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-384020-05 09/07

ANEXO 3

Cisco Wireless Control System (WCS)

Figure 1. Cisco Wireless Control System (WCS)



Product Overview

Cisco Wireless Control System (WCS)

Cisco® Wireless Control System (WCS) is the industry's leading platform for wireless LAN planning, configuration, management, and mobility services. It provides a powerful foundation that allows IT managers to design, control, and monitor enterprise wireless networks from a centralized location, simplifying operations and reducing total cost of ownership. Cisco WCS is a component of the Cisco Unified Wireless Network and supports the Cisco Motion vision.

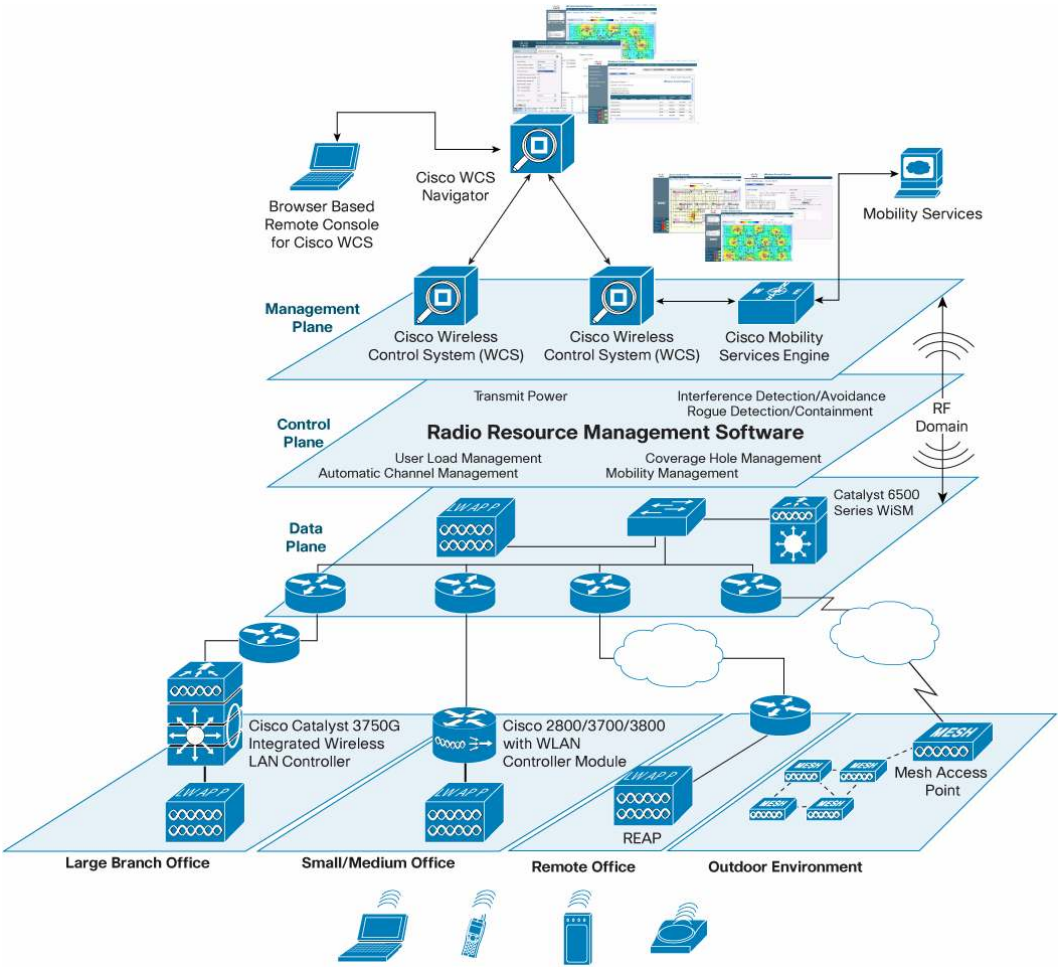
With Cisco WCS, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, device tracking, security monitoring, and wireless LAN systems management. Robust graphical interfaces make wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make Cisco WCS vital to ongoing network operations.

Cisco WCS runs on a server platform with an embedded database. This provides the scalability necessary to manage hundreds of Cisco wireless LAN controllers, which in turn can manage thousands of Cisco Aironet® lightweight access points. Cisco wireless LAN controllers can be located on the same LAN as Cisco WCS, on separate routed subnets, or across a wide-area connection. All Cisco wireless LAN controller models can be managed by Cisco WCS including enterprise-class stand-alone wireless LAN controllers such as the 4400 and 2100 Series as well as the Cisco Catalyst 6500 Series Wireless Services Module (WiSM), the Cisco Catalyst 3750G Integrated Wireless LAN Controller, and the Cisco Wireless LAN Controller Module (WLCM and WLCM-E) for Integrated Services Routers.

Cisco WCS also manages the Cisco 3300 Series Mobility Services Engine (MSE). Cisco MSE is an appliance-based platform that enables industry mobility solutions using a centralized, services engine with an open API for scalable mobility applications development. Cisco MSE serves as a single point of integration for a variety of value-added mobility services including Cisco Context-Aware Mobility Solution, Cisco Adaptive Wireless Intrusion Prevention System (IPS) and Cisco Mobile Intelligent Roaming Solution.

Multiple, geographically dispersed Cisco WCS management platforms can be cost-effectively and easily managed by the Cisco WCS Navigator. Cisco WCS Navigator supports up to 20 Cisco WCS management platforms with manageability of up to 30,000 Cisco Aironet lightweight access points from a single management console. Together, Cisco WCS and Cisco WCS Navigator are the ideal wireless LAN management solution for even the largest enterprise environments and outdoor deployments (Figure 2).

Figure 2. Enterprise Wide RF Intelligence



Cisco WCS enables the following functions across an entire wireless network:

General Management

Cisco WCS makes wireless LAN configuration, monitoring, and management as simple and as effective as wired systems management. This includes the following core capabilities:

- **Configuration templates:** With Cisco WCS, administrators can assign a template to one or all of the wireless LAN controllers or access points in a mobility group. They can then select the mobility group name and apply the template across the entire mobility group domain. A variety of wireless LAN controller templates are available to manage system, WLAN, security, access control, 802.11 a/b/g/n, mesh, rogue devices, TFTP servers, and management configurations (Figure 3 and Figure 4).

- **Bulk provisioning of Cisco wireless LAN controllers:** All Cisco wireless LAN controllers can be provisioned in bulk by importing a CSV file into Cisco WCS.
- **Software management:** With Cisco WCS, upgrades to Cisco wireless LAN controllers and access points can be performed from a centralized location, with a single click of a mouse.
- **User group-based privilege management:** Network administrators can create Cisco WCS user groups and assign management task level privileges to each individual user group.
- **Network auditing:** Network administrators can audit wireless LAN controller and access point configurations by network location, mobility group, or device. Discrepancies between the configuration stored in Cisco WCS and the current configuration of the access point or controller can be displayed. Network administrators can remediate configuration discrepancies by retaining either the Cisco WCS configuration or the configuration stored on the device. Using network auditing in conjunction with Cisco WCS configuration templates delivers powerful real-time configuration management of connected controllers and access points.
- **RADIUS and TACACS+ support for secure access:** Cisco WCS supports Simple Network Management Protocol (SNMP) version 3 and Terminal Access Controller Access Control System (TACACS+) for the highest level of network management capabilities and security. SNMP version 3 can be used for communication between a Cisco WCS server and individual wireless LAN controllers. Cisco WCS also supports SNMP version 1 and version 2, which allows other network management platforms to query it. TACACS+ is a Cisco protocol that supports authentication, authorization, and accounting (AAA) servers. Cisco WCS uses TACACS+ to authenticate and authorize access to specific Cisco WCS features.
- **HTTP and HTTPS interface:** Network administrators can access Cisco WCS via any standard browser running HTTP or Secure HTTP (HTTPS), which helps ensure anytime, anywhere access to Cisco's management capabilities.

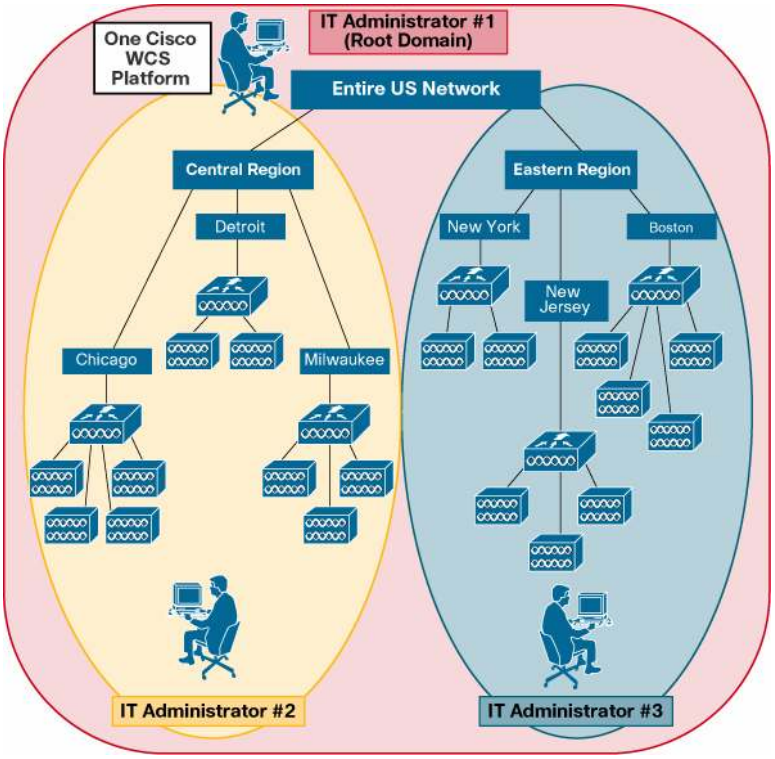
Figure 3. Cisco WCS Configuration Templates

Figure 4. Cisco WCS Configuration Group Templates

Virtual Domains

Organizations can segment Cisco WCS using virtual domains (partitioning). Cisco WCS virtual domains enhance network access control by allowing organizations to limit an individual IT administrator's access to only those wireless network segments that are under each IT administrator's individual responsibility. Cisco WCS virtual domains allows organizations to maintain super-user and root administrator control of the wireless LAN. Managed service providers can use this feature to easily manage multiple customer WLANs from a single, centralized, easy-to-use Cisco WCS platform (Figure 5).

Figure 5. Cisco WCS Virtual Domains Grouped by Hierarchical Domains



Cisco WCS virtual domains provide organizations with the flexibility to:

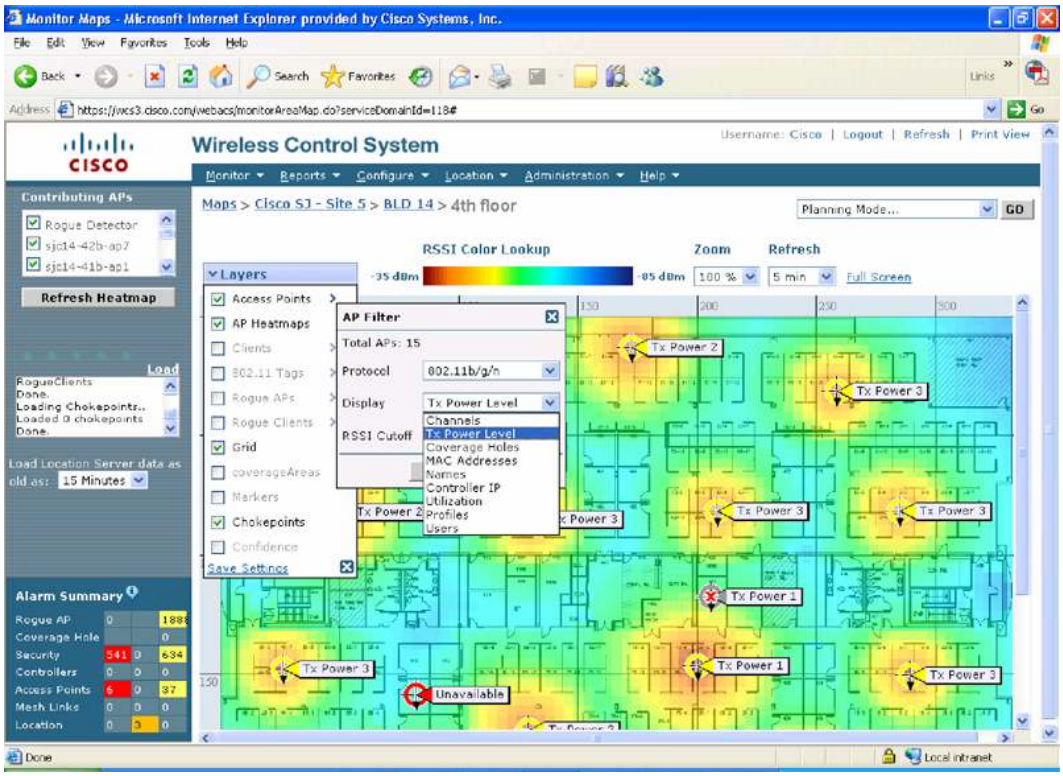
- Define the areas of the wireless network that individual IT administrators (users) can manage.
- Customize virtual domain names by geographical regions, customer names, building, campus, or other customized parameters to meet each organization's individual needs.
- Create up to 128 distinct hierarchical virtual domains.
- Maintain tight control of the wireless network infrastructure that is managed by each IT administrator.

Learn more about Cisco WCS virtual domains by reading the brochure: Cisco Wireless Control System Virtual Domains—Enhance Access Control and Simplify WLAN Management.

Network Monitoring

Cisco WCS provides tools that enable IT managers to visualize the layout of their wireless network and monitor ongoing WLAN performance. This includes detailed heat maps that show RF coverage on top of imported floorplans. Cisco WCS also provides a portal into the real-time RF management capabilities provided by Cisco wireless LAN controllers, including channel assignments and access point transmit power settings. In addition, Cisco WCS provides quick visibility into coverage holes, alarms, and key utilization statistics for easy WLAN monitoring (Figure 6).

Figure 6. Visualize RF Coverage

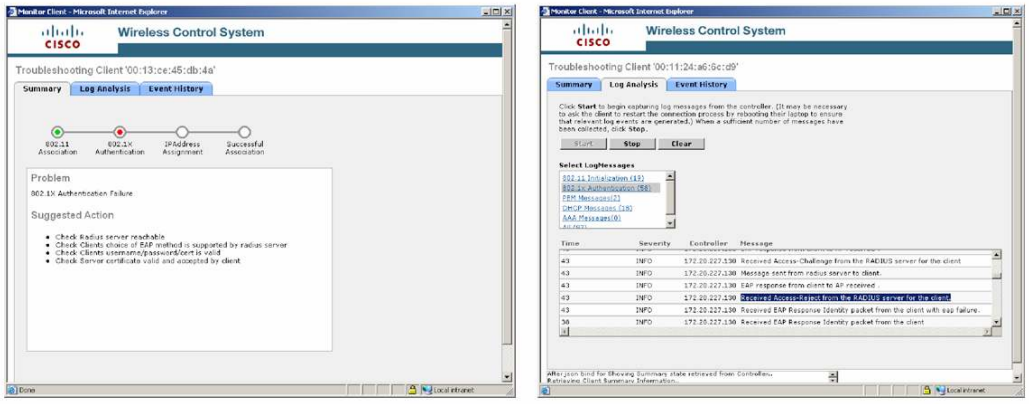


Network Troubleshooting

Cisco WCS facilitates network troubleshooting based on network reports and quick searches for areas such as noise levels, signal-noise ratio, interference, signal strength, clients, controllers, access points, security and performance. This allows network administrators to isolate and resolve problems at all layers of a wireless network. A client troubleshooting tool, client debugging logs, and integration with Cisco Spectrum Expert are also available for troubleshooting of client devices and non Wi-Fi interference.

- **Client Troubleshooting Tool:** A built-in client troubleshooting tool allows network administrators to quickly and easily troubleshoot problems with a client. Detailed client information is displayed on a troubleshooting dashboard to aide network managers in quickly troubleshooting client problems. This tool includes a summary page with a list of the defined problem and suggested troubleshooting actions as well as a log analysis to capture log messages from the controller and a detailed event history. This tool helps network managers debug Layer 1 to Layer 3 client problems using a step-by-step method (Figure 7).

Figure 7. Client Troubleshooting Tool



- **Client debugging logs and statistical reports:** Cisco WCS can collect, save, export and open debug logs for Cisco Aironet and Cisco Compatible Extensions version 5 client devices. These logs can facilitate the generation of client troubleshooting tickets. Real-time and historical statistical reports and a consolidated summary of the troubleshooting tests that were used on the diagnostic channel of these devices can be generated.
- **Integration with Cisco Secure Access Control Server (ACS) View Server 4.0:** The Cisco WCS client troubleshooting tool integrates with Cisco Secure ACS View Server 4.0 to provide aggregated client status information from multiple Cisco ACS Servers. This supports easy troubleshooting of client problems associated with client authentication failures.
- **Radio Resource Management (RRM):** Troubleshooting and maintenance of the WLAN network is simplified with the RRM tool. This tool provided visibility into wireless network performance and radio frequency statistics. The RRM dashboard is easy to read and enhances awareness of critical events, coverage, or lack of coverage, and configuration anomalies (Figure 8).

Figure 8. RRM Tool Dashboard

- **Integration with Cisco Spectrum Expert:** Cisco WCS supports integration with Cisco Spectrum Expert. This integration allows customers to use the Cisco Spectrum Expert tool to investigate non-Wi-Fi interference sources within the vicinity of the Cisco lightweight access points that are affected by interference. When the source of the interference is determined, customers can remove, move, shield, adjust, or replace the device that is generating the interference. This tool can be used to assist with network troubleshooting (Figure 9).

  Cisco WCS can be configured to receive non-Wi-Fi interference device traps from Cisco Spectrum Expert when a new device that is causing interference is discovered by Cisco Spectrum Expert. Cisco WCS can be configured to support the following actions:

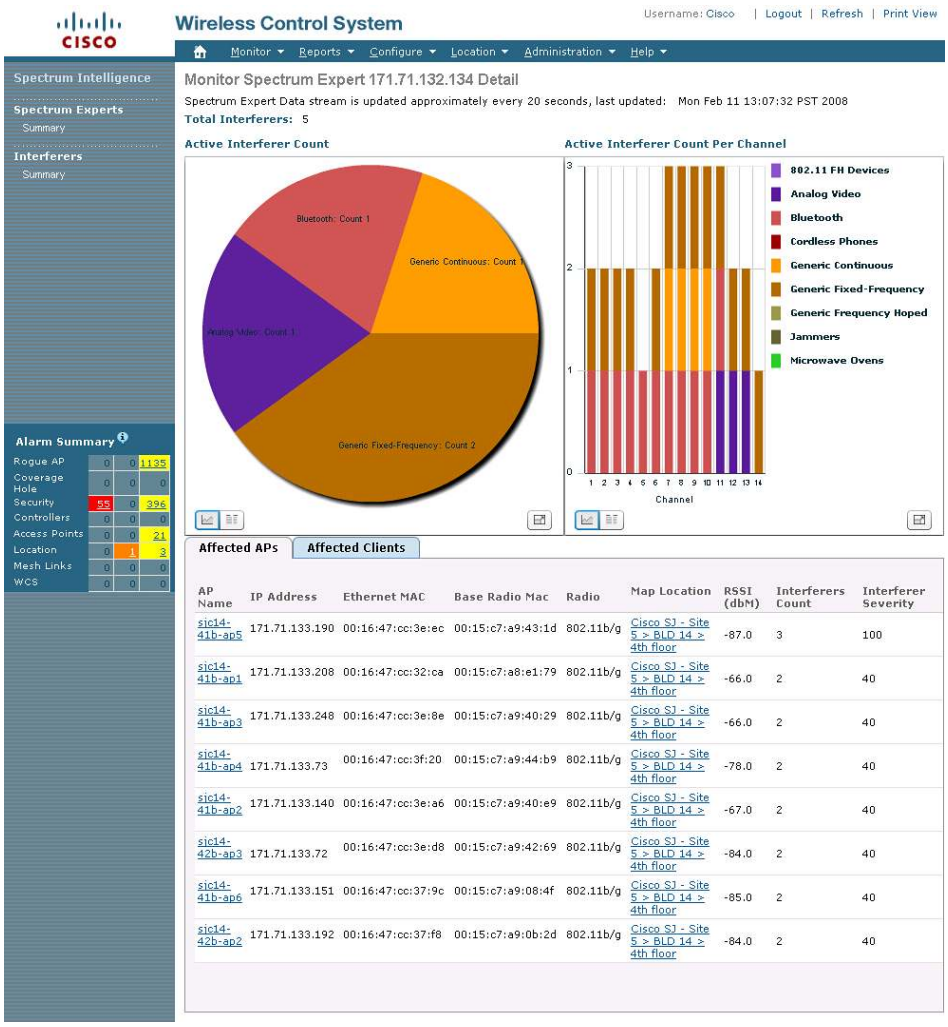
  - Enable the reception of a trap from Spectrum Expert (Cardbus). The authentication mechanism is set up by adding the laptop IP address as a valid trap transmitter to Cisco WCS.
  - Issue an interference alarm.
  - Configure the severity of the alarm, with a default value of minor.
  - Associate the alarm with a specific access point.

Users can set trap filters and threshold values within Cisco Spectrum Expert so that traps are generated only for significant interference events.

Learn more about the Cisco Spectrum Expert by visiting http://www.cisco.com/en/US/products/ps9393/index.html.

Learn more about spectrum intelligence by reading the brochure Cisco Spectrum Intelligence Solution Simplifies Detection, Classification, Location, and Troubleshooting of RF Interference.

Figure 9. Cisco WCS integration with Cisco Spectrum Expert



Reports

Reports that improve data management, simplify operations, and enhance network control can be generated by Cisco WCS on demand or for scheduled time increments. Cisco WCS general report features include:

- Exporting of reports into comma separated values (CSV) or PDF format.
- Automating and scheduling of exported reports.
- Sending e-mail notifications upon report generation.
- Specifying target or logical entity groups when generating a report.

- Configuring and customizing reports by frequency and polling to reduce the costs of unnecessary network polling and database storage
- Configuring data storage and saving parameters. Hourly aggregated data can be stored for up to 31 days. Daily aggregated data can be stored for up to 90 days. Weekly aggregated data can be stored for up to 54 weeks.

A summary of Cisco WCS reports can be found in Table 1. Sample reports are displayed in Figures 10, 11 and 12.

Table 1. Cisco WCS Report Summary

Cisco WCS Report	Description
Inventory	Inventory reports for wireless equipment deployed within the network (access points, controllers, and location appliances) can be generated for each hardware category or as a combined report for all categories. Reports can include the hardware type, software revision, and location by building or floor.
Performance	Memory and CPU usage can be tracked and reported at configurable intervals. Coverage hole alarms can be generated to provide a better view of the coverage hole problems experienced by client devices. Metrics for voice traffic streams are available to support Cisco Compatible Extensions clients running Version 4 and later.
Security	Security information can be downloaded as a report and the number of rogue devices detected by each access point per month can be automatically listed on the summary report. Intrusion detection system (IDS) reports display rogue devices and ad hoc events as a list or graph.
Detailed Client Report	Reports on the roaming history of all clients, the busiest clients and a list of unique clients that accessed the WLAN in a specific area for a specified duration of time can be generated. Trends in client counts can be displayed in a graph. A variety of client statistics can be displayed including MAC address, associated access point, transmit/receive throughout, RSSI, Cisco Compatible Extensions, and signal-to-noise ratio. Reports can be generated based on a variety of criteria including floor area, controllers, access point, and Service Set Identifiers (SSIDs). The display of this report can be customized.
Access Points	Traffic stream metrics for access points can be generated as a report or a graph. Access points can be reported by their location or SSID and the status of each access point by its profile listing can be reported. A listing of the busiest access points is available in a table format.
Mesh	A report on the number of alternate parents available to a mesh access point in case the parent is lost can be generated. Other mesh reports that can be generated for events overt time include: child and parent link statistics, node hop counts, packet error rate on the backhaul link, the number of transmitted neighbor packets, worst node hops, packet queue statistics, and worst SNR links.
Payment Card Industry (PCI) Assistance Report	An analysis of Cisco Unified Wireless Network security event data, such as rogue and attack events from Wireless IDS, as well as network-wide configurations and audit trails provide assistance in creating a PCI Assessment Report. Potentially non-compliant events and network configurations are summarized in this report.

Figure 10. Access Point Report and Inventory Report

Figure 11. Controller Utilization Performance Report and Busiest Client Report

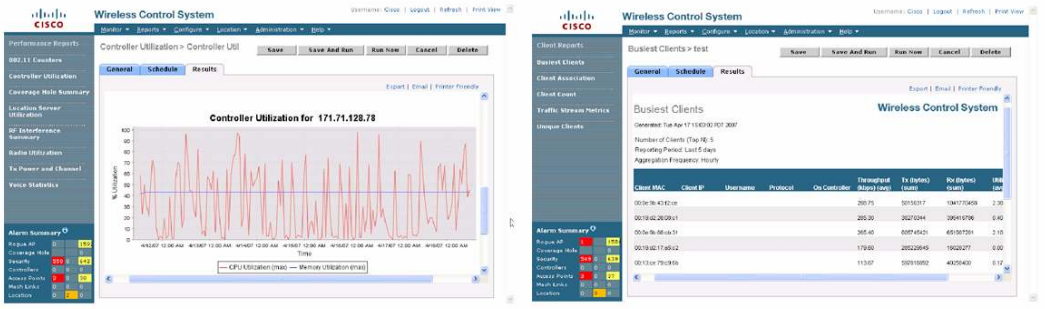
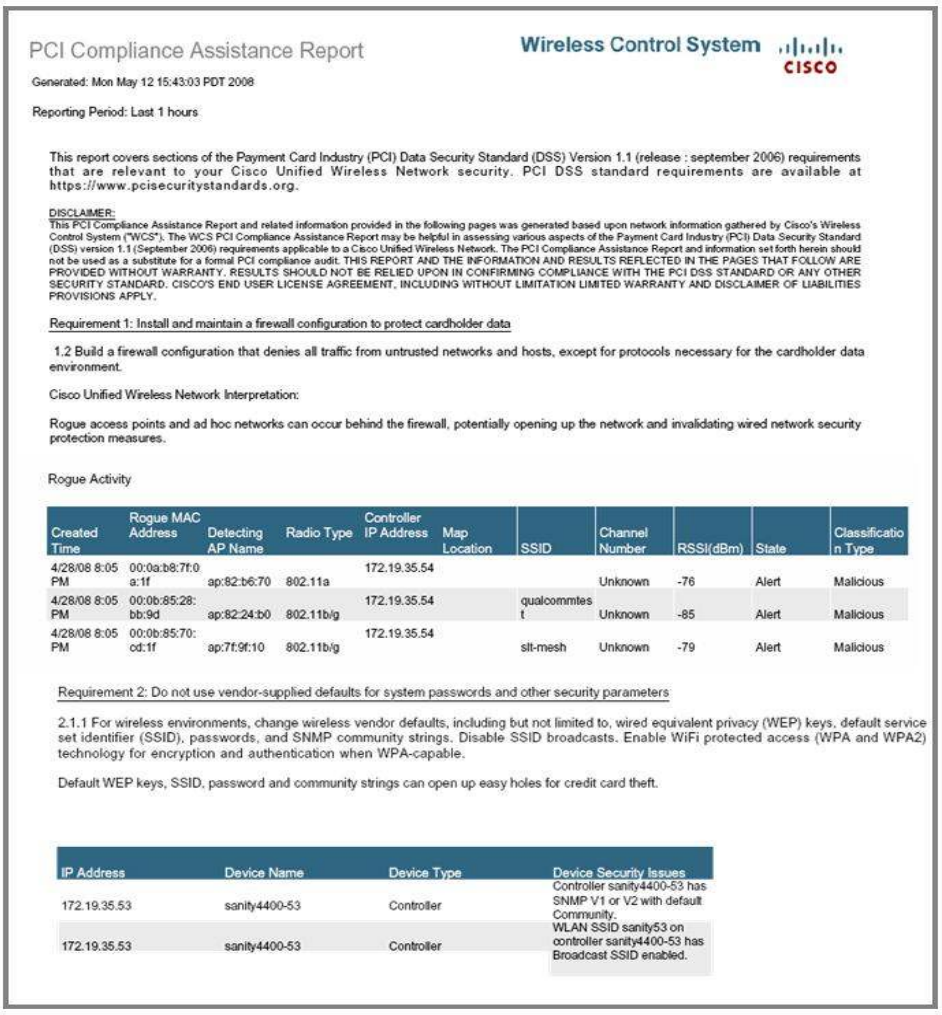


Figure 12. PCI Compliance Assistance Report



PCI Compliance Assistance Report

Wireless Control System

Generated: Mon May 12 15:43:03 PDT 2008

Reporting Period: Last 1 hours

This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.1 (release : september 2006) requirements that are relevant to your Cisco Unified Wireless Network security. PCI DSS standard requirements are available at https://www.pcisecuritystandards.org.

DISCLAIMER:
This PCI Compliance Assistance Report and related information provided in the following pages was generated based upon network information gathered by Cisco's Wireless Control System ("WCS"). The WCS PCI Compliance Assistance Report may be helpful in assessing various aspects of the Payment Card Industry (PCI) Data Security Standard (DSS) version 1.1 (September 2006) requirements applicable to a Cisco Unified Wireless Network. The PCI Compliance Assistance Report and information set forth herein should not be used as a substitute for a formal PCI compliance audit. THIS REPORT AND THE INFORMATION AND RESULTS REFLECTED IN THE PAGES THAT FOLLOW ARE PROVIDED WITHOUT WARRANTY. RESULTS SHOULD NOT BE RELIED UPON IN CONFIRMING COMPLIANCE WITH THE PCI DSS STANDARD OR ANY OTHER SECURITY STANDARD. CISCO'S END USER LICENSE AGREEMENT, INCLUDING WITHOUT LIMITATION LIMITED WARRANTY AND DISCLAIMER OF LIABILITIES PROVISIONS APPLY.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

1.2 Build a firewall configuration that denies all traffic from untrusted networks and hosts, except for protocols necessary for the cardholder data environment.

Cisco Unified Wireless Network Interpretation:

Rogue access points and ad hoc networks can occur behind the firewall, potentially opening up the network and invalidating wired network security protection measures.

Rogue Activity

Created Time	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Map Location	SSID	Channel Number	RSSI(dBm)	State	Classification Type
4/28/08 8:05 PM	00:0a:b8:7f:0a:1f	ap:82:b6:70	802.11a	172.19.35.54			Unknown	-76	Alert	Malicious
4/28/08 8:05 PM	00:0b:85:28:bb:9d	ap:82:24:b0	802.11b/g	172.19.35.54		qualcommtest	Unknown	-85	Alert	Malicious
4/28/08 8:05 PM	00:0b:85:70:cd:1f	ap:7f:9f:10	802.11b/g	172.19.35.54		slt-mesh	Unknown	-79	Alert	Malicious

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

Default WEP keys, SSID, password and community strings can open up easy holes for credit card theft.

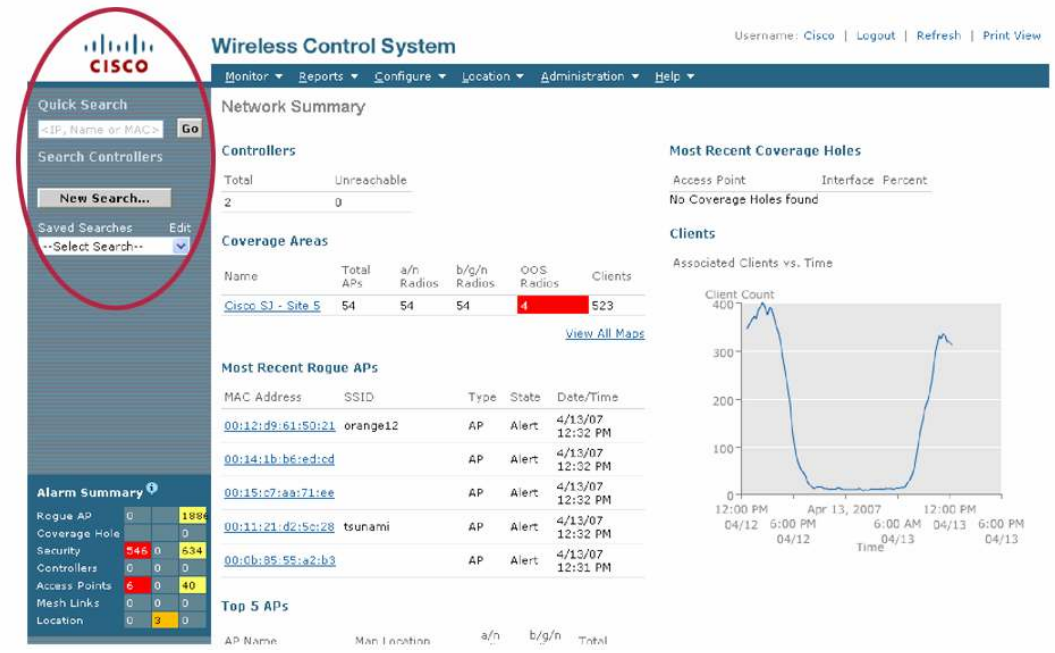
IP Address	Device Name	Device Type	Device Security Issues
172.19.35.53	sanity4400-53	Controller	Controller sanity4400-53 has SNMP V1 or V2 with default Community.
172.19.35.53	sanity4400-53	Controller	WLAN SSID sanity53 on controller sanity4400-53 has Broadcast SSID enabled.

Simplified Ease-of-Use

Cisco WCS is very easy to use and requires minimal training. This robust platform supports a variety of intuitive screens that streamline configurations and simplify daily operations and management of the WLAN including:

- A quick search box that enables searches across the entire WLAN for access points, controllers, or client devices by their MAC address, IP address, or name. This reduces the time required to identify and isolate devices with incorrect operations or security settings (Figure 13).
- Advanced searches with an option for saving
- Access control list (ACL) provisioning supports creating reusable grouped IP addresses and reusable protocols
- An extensive selection of access point and controller templates with specialized tab areas that simplify the selection and design of configuration parameters. These templates can be scheduled to be applied at a future day or time to support automated controller provisioning and software management at anytime, without manual intervention.
- Reuse and apply controller templates to one or all wireless LAN controllers.
- Configuration auditing supports auditing of the configuration of each wireless LAN controller to confirm that it's running configuration is identical to the configuration listed in Cisco WCS database.
- List page record sizes are configurable to up to 500 records per page
- Customizable dashboard with interactive real-time charts and tables to meet each organization's individual networking requirements
- Alarm configuration by severity level
- Scheduled shut off of WLAN and access point radios supports deactivation of the unified wireless LAN as needed to meet security requirements during business or non-business hours.
- Auto-provisioning of wireless LAN controllers supports remote configuration of controllers at branch offices or remote locations.
- Distinctive floor map icons indicate the device type including: authorized and unauthorized client devices, authorized and rogue access points, Wi-Fi tags, and chokepoints when the Cisco Wireless Location Appliance is deployed with Cisco WCS. The rogue access point icon also changes color to differentiate between a variety of states, including alert, pending, contained, threat, contained pending, trusted missing, on network, and off network.
- One-click software upgrade simplifies the process for upgrading Cisco WCS to run the latest software release.

Figure 13. Cisco WCS Quick Search and New Search



Cisco Context-Aware Mobility Solution

Cisco provides a variety of options for efficiently tracking wireless devices and managing contextual information from Wi-Fi enabled laptops, PDAs, voice handsets, telemetry-enabled devices and mobile assets equipped with 802.11 transceivers. Cisco WCS can determine which access point a wireless device is associated with, giving IT managers a general proximity of where wireless devices are situated. Wi-Fi devices and tags can also be divided into groups for simplified tracking and device control.

Environments that require more granular device location capabilities can implement Cisco Context-Aware Software in conjunction with Cisco MSE. This solution uses Cisco's patent pending "RF fingerprinting" technology. This technology compares real-time client RSSI information to known RF building characteristics, making Cisco the first WLAN infrastructure with the ability to accurately locate a wireless device, including rogue devices, to within a few meters (Figure 14).

Cisco WCS with location services supports "on demand" lookups of the most recent location information for a single Wi-Fi device or rogue device. With a Cisco WCS license deployed in conjunction with Context-Aware Software and Cisco MSE, real-time contextual information about mobile assets and users such as its location, temperature, availability, and applications in use can be supported to simultaneously monitor and track thousands of wireless clients (Figure 15).

Outdoor location is supported by Cisco WCS with Context-Aware Software and Cisco MSE to the nearest access point.

Figure 14. Cisco Context-Aware Mobility Solution —High Resolution Map for Rogue Device Detection

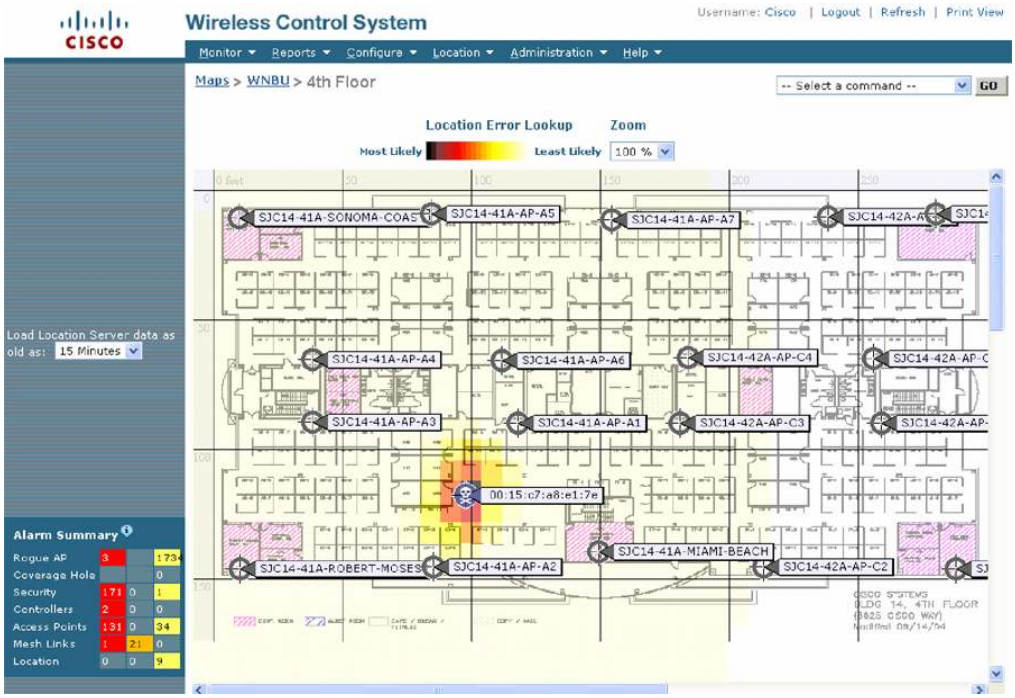
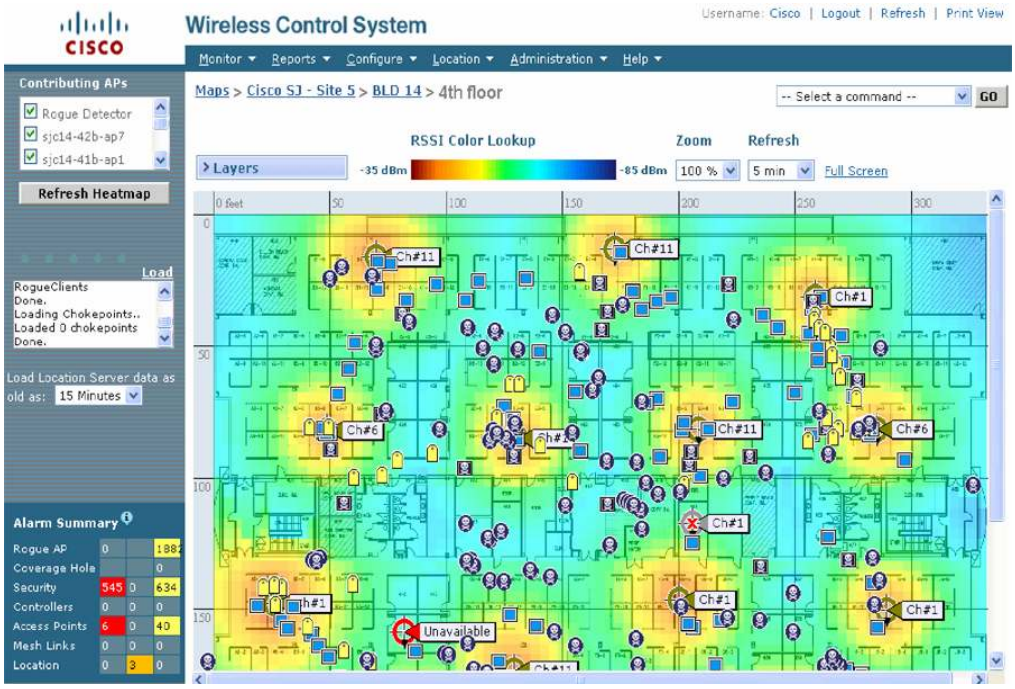


Figure 15. Cisco Context-Aware Mobility Solution—Location Services

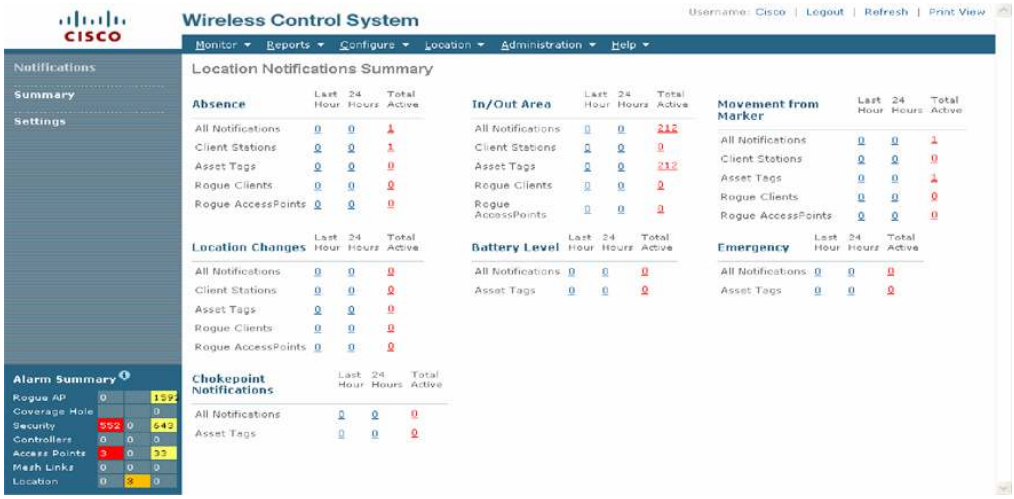


Cisco WCS also supports high-accuracy deterministic location-based notifications enabled through chokepoints. Chokepoint-based notifications are triggered by Cisco Compatible Extensions Wi-Fi tags as they come within range of a chokepoint. Notifications can be triggered by a variety of Wi-Fi tag actions, including entry or exit of a tag from a specified zone, doorway, or gate; and process control events such as those used in manufacturing environments. Chokepoint summary information is displayed on the Cisco WCS Location Notifications Summary. The Cisco WCS

Location Notifications Summary screen also displays a client's absence, movement in or out of an area, and marker or location change, battery level and emergency group notifications (Figure 16).

With these advanced location tracking capabilities, the Cisco Unified Wireless Network is an ideal platform for helping to enable key business applications that take advantage of wireless mobility, such as asset tracking, inventory management, and enhanced 911 (e911) services for voice. By incorporating indoor location tracking into the wireless LAN infrastructure itself, Cisco reduces the complexities of wireless LAN deployment and minimizes total cost of ownership.

Figure 16. Cisco WCS Location Notifications Summary



Secure Guest Access

Cisco WCS supports customizable secure guest access that allows organizations to keep their wired and wireless networks secure while providing customers, vendors, and partners with controlled access to their WLANs (Figure 17). The complexity and cost for guest access services is reduced because both wired and wireless access for guest users can be enabled through the wireless infrastructure and a single unified management interface.

The following features are supported by Cisco WCS secure guest access (Figure 18):

- Single-click guest provisioning that reduces errors made by provisioning personnel when they are issuing guest access credentials.
- An HTML image file that can be uploaded to the controller to replace the default Web authentication page that guests traditionally see when logging into a controller-based guest network. This customized page can be previewed prior to activation.
- Customized automated guest access by time of day and date.
- Customizable guest user login failure message and logout verification Web page helps enhance the overall guest-user experience and minimize help desk calls.
- Pre-provisioning of guests prior to their arrival at the site by sending them login credentials by email.
- Limits can be placed on the number of guest users that provisioning personnel can create during a given time period to help maintain network security.
- The existing LDAP infrastructure can be used to authenticate guest users via Web authentication.

- Per-user bandwidth limits on guest traffic to enhance network security and performance.
- Per-SSID guest portals to provision separate portals for different guest user groups.
- Restriction of guest users by their network location: campus, building, or floor area.
- Guest user passwords automatically generated or manually defined.

Figure 17. Cisco Unified Wireless Network Secure Guest Access

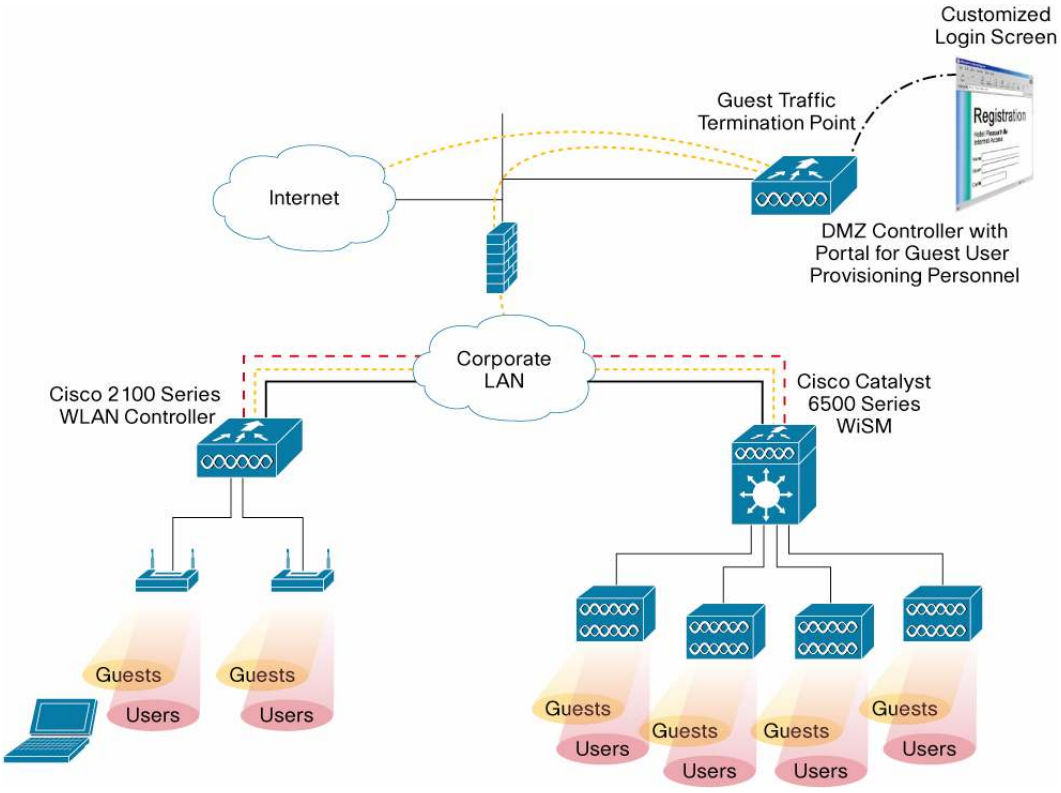
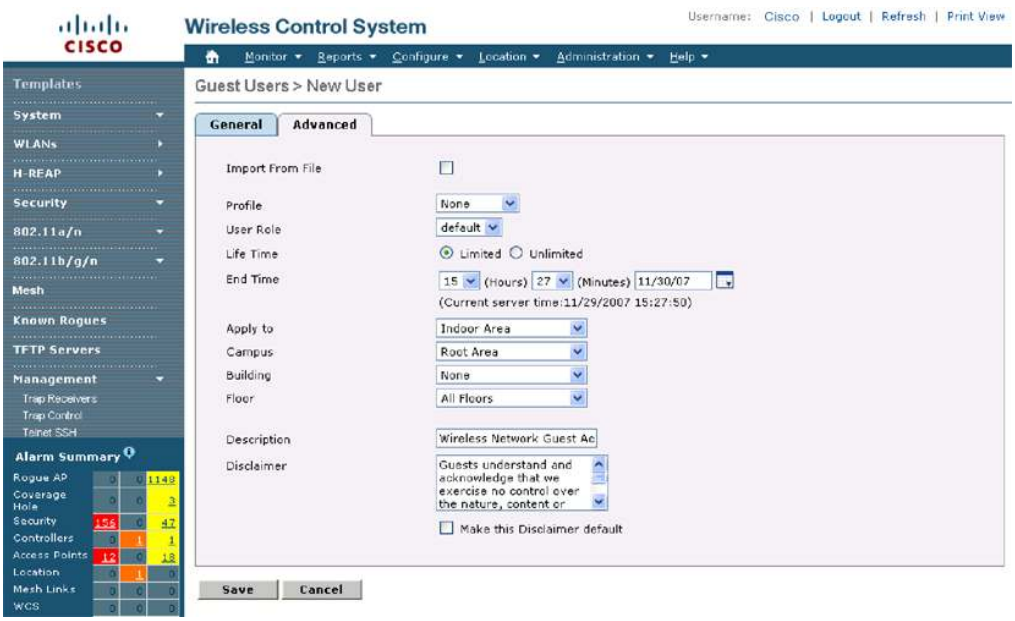


Figure 18. Cisco WCS Secure Guest Access Configuration

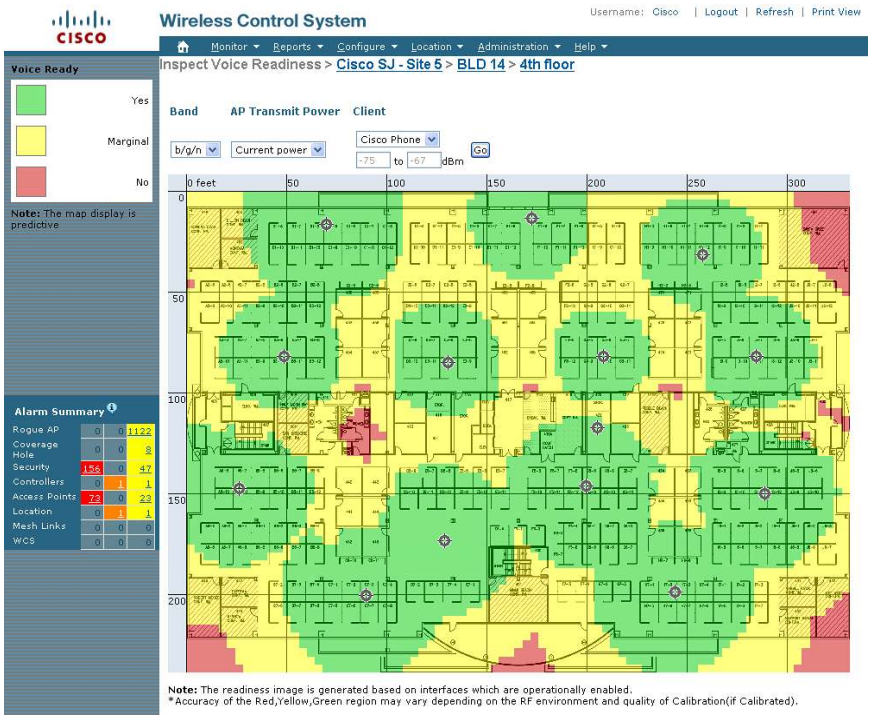


Voice over Wireless LAN

Cisco WCS includes a variety of advanced tools to plan, deploy, monitor, and optimize the WLAN for voice over wireless LAN (VoWLAN).

- **Voice WLAN parameter settings:** Voice is latency sensitive. Several WLAN parameters need to be modified to allow for both voice and data on the same network. Cisco WCS voice tools adjust critical WLAN parameters to support VoWLAN.
- **Voice troubleshooting tools:** Troubleshooting degraded voice quality problems can be difficult In a WLAN environment. Cisco WCS supports queries for traffic stream metrics (TSM) such as packet latency, packet jitter, packet loss and roaming time to determine the cause of voice quality problems.
- **Voice Readiness Tool:** The Cisco WCS Voice Readiness Tool (VRT) provides a visual indication of the RF coverage and provides an assessment of the readiness of the deployment for VoWLAN. The tool displays three distinct color-coded regions on the floor map highlighting areas of good, moderate and poor RF coverage (Figure 19). This helps identify insufficient coverage areas that could potentially experience voice quality issues. The VRT also takes advantage of calibration data, when available, to provide an estimate of the RF coverage levels and suitability of the network for VoWLAN. The tool can be queried for a visual representation of the RF coverage for current access point power levels or maximum access point power levels.
- **VoWLAN Audit Tool:** The Cisco WCS VoWLAN Audit Tool automates configuration checks and supports the definition of rules to validate Cisco wireless LAN controller configurations based on the VoWLAN deployment guide recommendations. Configuration violations can be presented as a report or an alarm. This tool helps organizations save time when performing configuration checks of Cisco wireless LAN controllers based on the suggested VoWLAN deployment guidelines.

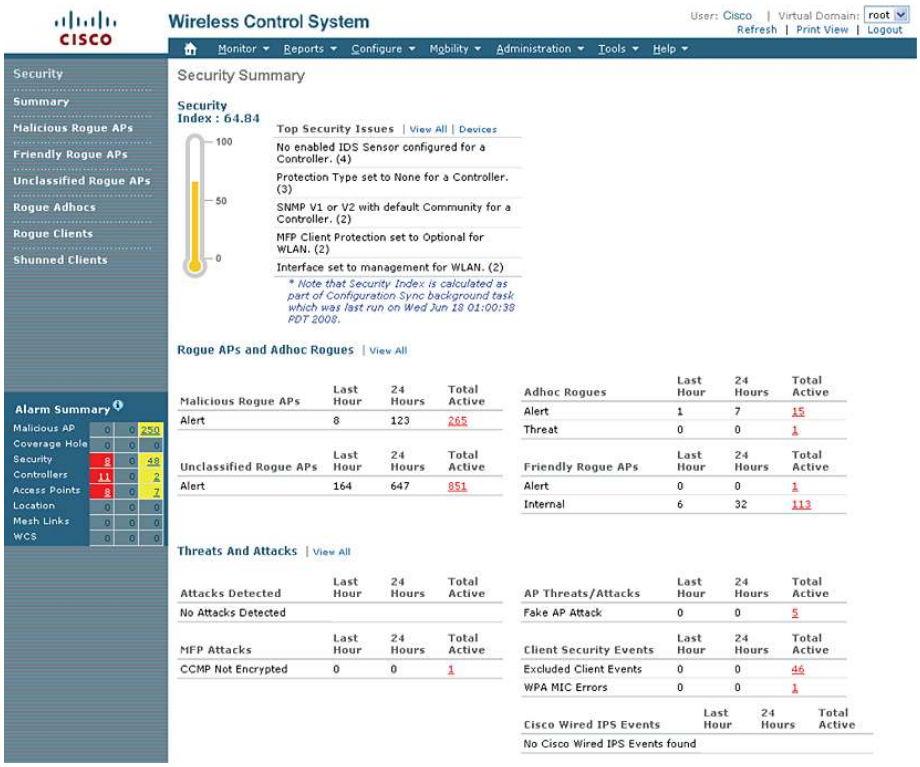
Figure 19. Cisco WCS Voice Readiness Tool (VRT)



Wireless Security and Network Protection

Cisco WCS streamlines administration and monitoring of security status across the wireless network by providing a single, comprehensive view of all security-related events and network conditions. The graphical at-a-glance format of the security summary greatly reduces the time needed for wireless network administrators to determine wireless network security status (Figure 20).

Figure 20. Cisco WCS Security Summary



Cisco WCS provides a full suite of tools for managing and enforcing security policies within a Cisco wireless infrastructure. These include:

- **Intrusion Detection System (IDS)/Intrusion Prevention System (IPS):** Cisco WCS supports robust IPS/IDS with the Cisco Secure Wireless Solution and Adaptive Wireless IPS that integrates with the Cisco Self-Defending Network and Network Access Control (NAC). This solution takes a comprehensive approach to security-at the wireless edge, wired edge, WAN edge, and through the data center. When an associated client sends malicious traffic through the Cisco Unified Wireless Network, a Cisco wired IDS device detects the attack and sends shun requests to Cisco wireless LAN controllers, which will then disassociate the client device.
- **wIDS signature tuning and management:** Cisco WCS reduces false alarms and increases event fidelity by supporting a configurable “interval” for all IDS signatures.
- **RF attack signatures and management frame protection:** Cisco WCS helps IT staff to create customizable attack signature files that can be used to rapidly detect common RF-related attacks, such as denial of service (DoS), Netstumbler, and FakeAP. Cisco WCS can be programmed to automatically generate alarms if an attack is detected. The detailed security summary enables IT staff to identify recurring security threats before they can cause significant harm.

- **Management frame protection:** Cisco WCS supports management frame protection (MFP) to monitor the authentication of 802.11 management frames by the wireless network infrastructure and client devices. MFP allows the network to detect spoofed frames from access points, malicious users impersonating infrastructure access points or Cisco Aironet client devices.
- **Rogue detection, location, and containment:** The Cisco WCS platform uses patent-pending technology to constantly monitor the RF environment looking for unauthorized access points and ad-hoc 802.11a/b/g/n networks. If unauthorized devices appear, Cisco WCS can be used to determine their location and assess the level of threat. The state of a rogue access point is easily determined by the color of the rogue access point icon displayed on the Cisco WCS floor plan map. If deemed malicious, IT managers can use Cisco WCS to properly contain these rogue devices. Detailed trending reports help to identify potential recurring problems. Standalone access points can be color-coded and marked as friendly or non-rogue.
- **Access point wired port authentication with 802.1X:** Cisco WCS also authenticates access points plugged into a wired network port using 802.1X to validate credentials. This helps to prevent wireless attacks on the wired network and reduces exposure to wireless security threats. It also eases installation and authentication of new access points on 802.1X-enabled networks.
- **Policy creation and enforcement:** Cisco WCS contains a service policy engine (Figure 21) that allows network administrators to easily create virtual LAN (VLAN), RF, quality of service (QoS), and security policies. With Cisco WCS, IT staff can create multiple unique service set identifiers (SSIDs) with individual security parameters. For example, a “guest” SSID can be secured with Web authentication; a “voice” SSID might be required to take advantage of the Wired Equivalent Privacy (WEP) capabilities inherent to voice handsets; and normal data traffic can be secured using 802.11i or IP Security (IPSec). Cisco WCS can be used to enforce security policies across an entire Cisco Unified Wireless Network, in individual Cisco wireless LAN controllers, or on individual lightweight access points.

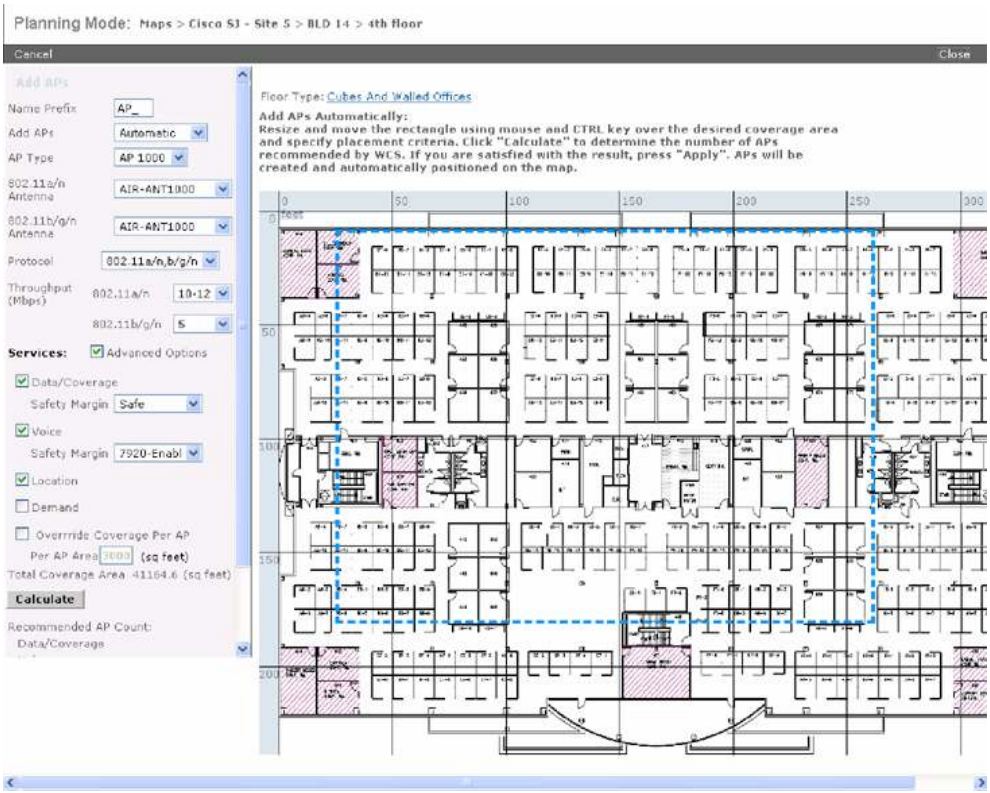
Figure 21. Policy Engine

- **User exclusion lists:** IT staff can use Cisco WCS to proactively exclude specific users from associating with the wireless network. In addition, if unusual activity is detected, offending devices can be flagged and excluded if they are considered to be malicious. These devices cannot access wireless LAN services until timing on the exclusion list expires, or the IT staff decides to grant them wireless LAN access.

Wireless LAN Planning and Design

Cisco WCS provides integrated RF prediction tools that can be used to create a detailed wireless LAN design, including lightweight access point placement, configuration, and performance/coverage estimates. IT staff can import real floor plans into Cisco WCS and assign RF characteristics to building components to increase design accuracy. Graphical heat maps help IT staff visualize anticipated wireless LAN behavior for easier planning and faster rollout. Drawing of irregularly shaped buildings using polygons is also supported to help organizations easily design and support WLAN deployments in such buildings (Figure 22).

Figure 22. Planning Tool



Google Earth Integration

Google Earth features and functionality can be used by Cisco WCS to assist with visualizing and managing Cisco Aironet outdoor wireless mesh deployments. A variety of Google Earth map features can be used within Cisco WCS, including zoom, pan, and tilt. Google Earth must be installed to enable this feature and Google Earth Pro is recommended.

Migrate CiscoWorks WLSE to Operate as a Cisco WCS

Organizations can simply and easily convert their existing CiscoWorks Wireless LAN Solution Engine (WLSE) Models 1130-19 or 1133 to operate as a Cisco WCS. This allows customers of CiscoWorks WLSE to migrate to the Cisco Unified Wireless Network architecture using their existing CiscoWorks WLSE platform.

A converted CiscoWorks WLSE becomes a server that runs Cisco WCS software using RedHat Linux ES v. 4.0. (A copy of RedHat Linux ES v. 4.0 is included with the CiscoWorks WLSE

migration CDs.) The converted CiscoWorks WLSE becomes a new Cisco WCS installation that supports lightweight access points and wireless LAN controllers running LWAPP.

Standalone (autonomous) access points are not supported by a converted CiscoWorks WLSE. A CiscoWorks WLSE that has been converted to Cisco WCS cannot be reverted back to operate as a CiscoWorks WLSE. CiscoWorks WLSE Express (Model 1030) and CiscoWorks WLSE (Model 1105) cannot be converted to operate as a Cisco WCS.

To simplify the CiscoWorks WLSE to Cisco WCS migration process, selected data can be migrated, in bulk, from CiscoWorks WLSE into Cisco WCS. CiscoWorks WLSE must be running software Release 2.15 or later in order to use this function. Learn more about converting a CiscoWorks WLSE to Cisco WCS by reading the Cisco WCS Licensing and Ordering Guide.

Simplified Standalone Access Point Migration and Monitoring

Cisco WCS simplifies the process of migrating standalone (autonomous) access points to operate as lightweight access points with a standalone access point migration tool and capabilities to monitor standalone access points.

- **Standalone Access Point Migration Tool:** Cisco WCS includes an easy-to-use migration tool that supports the simultaneous upgrading of up to 10 Cisco Aironet standalone access points of the same model number. Using this tool reduces the time required to migrate standalone access points.
- **Standalone Access Point Monitoring:** Organizations can now easily monitor their existing standalone access points from a Cisco WCS console in preparation for migration. Cisco WCS, running release 4.2 and later, can receive basic status and alarm information from standalone access points. These access points are then categorized as authorized access points on Cisco WCS heat maps. This helps optimize the WLAN and increase WLAN security.

  All Cisco Aironet standalone access point models can be monitored as well as the standalone access points of Cisco 800, 1800, 2800, and 3800 Series integrated services routers.

  Learn more about migrating to the unified architecture by reading the Feature Brief-Simplified Migration of Standalone Access Points to Operate as Lightweight Access Points in the Cisco Unified Wireless Network.

Cisco WCS Demonstration License

Customers can experience Cisco WCS, the industry's leading platform for wireless LAN planning, configuration, management, and mobility services, for free for 30 days by downloading the new full-featured, location-enabled Cisco WCS Demonstration License. This license supports 10 access points for up to 30 days. Network configurations and set up for the demonstration license are retained to make it easier to transition to a licensed Cisco WCS copy. Register to receive a license for free at http://www.cisco.com/go/license or https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?DemoKeys=Y. Select Network Mgmt Products > Wireless Control System > Wireless Control System 30 day trial license. Then, after registration, download Cisco WCS software from the Cisco Wireless Software Center (login required). **There is no Cisco Technical Assistance Center (TAC) support for the Cisco WCS Demonstration License**.

Features and Benefits

Table 2 lists the features and benefits of Cisco WCS.

Table 2. Features and Benefits of Cisco WCS

Feature	Benefit
Intuitive GUI and Simplified Ease-of-Use	IT staff can easily configure, monitor, and troubleshoot their wireless networks with minimal training.
Hierarchical Maps	IT staff can quickly access different geographies, campuses, buildings, floors, and regions for better visibility and control.
Virtual Domains	Enhanced access control is provided to organizations by allowing them to limit an individual IT administrator's access to only those wireless network segments that are under the IT administrator's individual responsibility. Managed service providers can use this feature to easily manage multiple customer WLANs from a single, centralized, easy-to-use Cisco WCS platform.
Policy Management Templates	Uniform QoS, security, and RF management policies can be easily created and enforced across an entire enterprise or outdoor deployment including outdoor mesh deployments. This can be done in a scalable fashion using global templates.
Robust Wireless Security and Network Protection	Cisco WCS streamlines administration and monitoring of security across the wireless network by providing a single, comprehensive view of all security-related events and network conditions. It supports built-in rogue detection, location, and containment as well as Adaptive Wireless IPS and robust security policy creation and enforcement.
Complete Wireless LAN Intrusion Protection	Customized signature files protect against unauthorized intrusion and RF attacks; automated alarms enable rapid response to mitigate risk.
Secure Access	Authentication and authorization to Cisco WCS is ensured with SNMP version 3 and TACACS+.
Client Troubleshooting	Network administrators can quickly and easily troubleshoot problems with a client, debugging Layer 1 to Layer 3 client problems using a step-by-step method. Integration with Cisco Secure ACS View Server 4.0 is supported for easy troubleshooting of client problems associated with client authentication failures.
Non-Wi-Fi Interference Detection	Integration with the Cisco Spectrum Expert allows customers to investigate non-Wi-Fi interference sources within the vicinity of the Cisco Aironet lightweight access points that are affected by interference. This tool assists with network troubleshooting.
Reporting	Extensive customizable reports allow network managers to monitor network activity and system information including inventory, performance, security, access points, clients, radio utilization, 802.11 counters, RF management, configuration history, and alarms.
Ease of Operation	Cisco wireless LAN controllers and Cisco Aironet lightweight access points remain up-to-date with no hands-on intervention. Flexible backups can be automatically scheduled for off-peak hours or run during normal business hours without impacting WLAN performance. Compressed backup files reduce file transfer times and disk space. Easily installed as a service on Windows, Linux or VMware systems.
Integrated High Accuracy Context-Aware Information	Real-time contextual information about mobile assets and users such as its location, temperature, availability, and applications in use can be supported with Cisco Context-Aware Software and Cisco MSE to simultaneously monitor and track thousands of wireless clients. High accuracy, deterministic location to within a few feet or several centimeters is supported by adding third party chokepoints.
Customizable Secure Wired and Wireless Guest Access	Organizations can keep their wired and wireless networks secure while providing customers, vendors, and partners with controlled access to their WLANs.
Voice over WLAN	Cisco WCS includes a variety of advanced tools to plan, deploy, monitor, and optimize the WLAN for VoWLAN including: voice WLAN parameter settings, voice troubleshooting tools, a voice audit tool, and a voice readiness tool.
Wireless LAN Planning Tools	Accurate RF prediction tools increase the effectiveness of wireless LAN planning and design. Three import file types are supported to generate maps: JPEG, PDF, and AutoCAD.
CiscoWorks WLSE Migration	Capital expenses can be reduced by converting an existing CiscoWorks WLSE (Models 1130-19 and 1133) to operate as a Cisco WCS. Selected data can be migrated in bulk from CiscoWorks WLSE into Cisco WCS.
Simplified Standalone Access Point Migration and Monitoring	The process of migrating standalone (autonomous) access points to operate as lightweight access points is simplified with a standalone access point migration tool and capabilities to monitor standalone access points.
Support for Large Scale Deployments	Up to 20 geographically diverse Cisco WCS management platforms can be cost-effectively and easily managed by Cisco WCS Navigator from a single management console.
Green Initiatives	Organizations can reduce power costs by using Cisco WCS to turn access points on or off at scheduled intervals. This feature can also be used to manage network security or restrict WLAN usage.

Summary

Cisco WCS is ideal for enterprise wireless LAN deployments and outdoor mesh networks. This easy-to-use solution simplifies the deployment and operation of wireless networks and helps to ensure smooth performance, enhance security, and maximized network availability. Cisco WCS centrally manages all Cisco wireless LAN controllers including Cisco Catalyst 6500 Series WiSM, the Cisco Catalyst 3750G Integrated Wireless LAN Controller, the Cisco WLCM, the Cisco WLCM-E and the 2100 Series and 4400 Series Cisco wireless LAN controllers. It also manages the Cisco Wireless Location Appliance, Cisco Aironet lightweight access points within campus environments and branch locations, and Cisco Aironet lightweight outdoor mesh access points, eliminating complexity and providing network administrators with visibility and full control of their indoor and outdoor wireless LANs.

Product Specifications

Table 3 lists the product specifications for Cisco WCS.

Table 3. Product Specifications for Cisco WCS

Item	Specification
Operating Systems (Customer Supplied Server)	**Cisco WCS can be deployed on a customer supplied server running one of the following operating systems:** • Windows 2003 SP1 or greater • Redhat Linux AS/ES v4.0 (Release 4.2 and later) and Redhat Linux AS/ES v5.0 (Releases 4.2.x or 5.0 or later) • VMware ESX Server 3.0.1 or later. (Minimum hardware requirements for a dedicated and guaranteed VMware server: Intel® Xeon Quad CPU; 3.15 GHz, 8 GB RAM, 200 GB HDD)
Minimum Server Requirements	Cisco WCS High-End Server • 3000 lightweight access points, 1250 standalone access points, 750 wireless LAN controllers • Two Intel® Xeon Dual Core CPU's; 3.0 GHz, 8 GB RAM, 200 GB HDD
	Cisco WCS Standard Server • 2000 lightweight access points, 1000 standalone access points, 450 wireless LAN controllers • Intel® Dual Core CPU; 3.2 GHz, 4 GB RAM, 80 GB HDD
	Cisco WCS Low-End Server • 500 lightweight access points, 200 standalone access points, 125 wireless LAN controllers • Intel® CPU; 3.06 GHz, 2 GB RAM, 30 GB HDD
	CiscoWorks WLSE Models 1130-19 or 1133 running Cisco WCS • 1500 lightweight access points, 161 wireless LAN controllers • Intel Pentium 4 CPU; 3 GHz, 3 GB RAM, 38 GB HDD
Minimum Client Requirements	Internet Explorer 6.0/SP1 or later
Management and Security	SNMP v1, v2c, v3 and TACACS+
Managed Devices	Cisco 2000, 2100, 4100 and 4400 Series Wireless LAN Controllers; Cisco Catalyst 6500 Series Wireless Services Module (WiSM), Cisco Catalyst 3750G Integrated Wireless LAN Controller, Cisco Wireless LAN Controller Module (WLCM and WLCM-E) for Integrated Services Routers; Cisco Aironet lightweight access points, Cisco Aironet lightweight outdoor mesh access points, Cisco 3300 Series Mobility Services Engine, Cisco Wireless Location Appliance, and Cisco Spectrum Expert. Monitoring and migration of selected Cisco Aironet standalone (autonomous) access points.
Database	Integrated Solid FlowEngine SQL

Cisco WCS Licenses

Ordering Guide

Please read the Cisco WCS Licensing and Ordering Guide for step-by-step instructions for ordering the correct Cisco WCS license SKUs as well as instructions for downloading, installing, and registering Cisco WCS software.

License Types

Cisco WCS base supports standard Cisco WCS capabilities. Cisco WCS location includes all base features plus the ability to track a single Wi-Fi device on demand or expand location capabilities by adding a Cisco Wireless Location Appliance to simultaneously track up to 2500 Wi-Fi devices. All purchasable Cisco WCS licenses can be ordered from the Cisco Ordering Tool.

Cisco WCS is available as a software-based license of two types: single server or enterprise.

Single Server Licenses

- License type: Standard, Location Upgrade and CiscoWorks WLSE migration to Cisco WCS.
- Typically suitable for customers deploying up to 500 Cisco Aironet lightweight access points.
- One Cisco WCS license key per Product Authorization Key (PAK) certificate.
- Available as Cisco WCS base or Cisco WCS location options in configurations of 50, 100, and 500 access points for the license families WCS-STANDARD-K9 and WCS-LOC-UPG-K9 to support new and expanded Cisco WCS deployments.
- Available as Cisco WCS base or Cisco WCS location options in configurations of 50, 100, 500, 1000, and 2500 access points for the license family WCS-WLSE-UPG-K9 to support the migration of CiscoWorks WLSE to operate as a Cisco WCS.

Enterprise Licenses

- License type: Enterprise.
- Available with Cisco WCS Software Release 4.1 or later.
- Typically suitable for customers deploying 500 or more Cisco Aironet lightweight access points.
- Multiple license files are linked to a single PAK certificate that can be deployed on one or multiple Cisco WCS servers.
- Location services are included with all enterprise licenses.
- Availability in configurations of 1000, 2500, 10,000 and 50,000 access points for the license family WCS-ENT-K9.
- Redeem licenses up to the maximum access point quantity associated with the SKU. As individual access point licenses under a PAK are redeemed, the access point quantity count tied to the PAK is decremented accordingly.
- With the licenses WCS-ENT-10000 and WCS-ENT-50000, a Cisco WCS Navigator license (WCS-NAV-20) is included to support up to 20 geographically diverse Cisco WCS management platforms.

Ordering Considerations

The following ordering considerations are applicable for Cisco WCS licenses. To select the correct Cisco WCS license SKU, please read the Cisco WCS Licensing and Ordering Guide.

- All Cisco WCS SKUs can be bought as a discrete SKU (first-time purchase) or as an expansion SKU (added to an existing deployment) unless otherwise noted.
- Cisco WCS base and Cisco WCS location licenses cannot be combined. Only Cisco WCS single server licenses of the same option (base or location) can be combined.
- If a single server license is upgraded from Cisco WCS base to Cisco WCS location, all of its associated access points must stay on the single server where the license was originally deployed.
- For single server deployments, it is more cost-effective to purchase Cisco WCS location initially rather than add location at a later date to a Cisco WCS base deployment.
- Single server licenses can be combined with an enterprise license. However, if single server and enterprise licenses are combined, the license for the single server must be deployed on one server.
- Single server and enterprise licenses can only be combined if the single server license supports location. If a Cisco WCS base license was purchased, this license must be upgraded to Cisco WCS location before the enterprise licenses can be added.
- A single server license cannot be upgraded to operate as an enterprise license.
- Cisco WCS licensing is not tied to the type of lightweight access point deployed since Cisco WCS licensing does not distinguish access point types. Each lightweight access point is counted as one access point license.
- All Cisco WCS SKUs, except for the Cisco WCS Demonstration License, are orderable from the Cisco Ordering Tool.

Downloading Cisco WCS Software

Customers can download Cisco WCS Software Release 4.0, 4.1 or later from http://www.cisco.com/cgi-bin/tablebuild.pl/Wireless_Control_System_Software (login required) or from the Product Upgrade Tool.

Cisco WCS licensing entitlement is applicable for new or expanded Cisco WCS deployments on single or multiple servers, CiscoWorks WLSE customers upgrading to Cisco WCS, Cisco WCS location upgrades, and existing Cisco WCS installations that are upgrading to Cisco WCS Software Release 4.1.

Customers running Cisco WCS Software Release 4.0 are encouraged to upgrade to Cisco WCS Software Release 4.1, but they are not required to do so.

Ordering Information

Table 4 provides ordering information for Cisco WCS. To place an order, for all Cisco WCS licenses except the Cisco WCS Demonstration License, visit the Cisco Ordering Website. To request a license for the Cisco WCS Demonstration License visit http://www.cisco.com/go/license.

Please read the Cisco WCS Licensing and Ordering Guide for step-by-step instructions for ordering the correct Cisco WCS license SKU as well as instructions for downloading, installing, and registering Cisco WCS software.

Note: Each license is orderable in specified quantity blocks. To add multiple quantities of license blocks, you must go back to the main screen and order additional family SKUs and then select the sub-SKU option and quantity block required. Repeat this process as needed, until the correct quantity of license blocks for your sub-SKU have been ordered.

Table 4. Ordering Information for Cisco WCS

Product Part Number	Product Description
WCS-STANDARD-K9 **New and Expanded Cisco WCS Deployments**	
Cisco WCS Base • Supports deployment of Cisco WCS on a single server	
WCS-APBASE-50	Cisco WCS Base License for 50 access points, Windows/Linux
WCS-APBASE-100	Cisco WCS Base License for 100 access points, Windows/Linux
WCS-APBASE-500	Cisco WCS Base License for 500 access points, Windows/Linux
Cisco WCS Location • Supports deployment of Cisco WCS on a single server • Includes location services to support tracking of a single Wi-Fi device on demand or expanded location capabilities by adding a Cisco Wireless Location Appliance. • Cisco WCS Location must be installed to support deployment of a Cisco Wireless Location Appliance.	
WCS-APLOC-50	Cisco WCS with Location License for 50 access points, Windows/Linux
WCS-APLOC-100	Cisco WCS with Location License for 100 access points, Windows/Linux
WCS-APLOC-500	Cisco WCS with Location License for 500 access points, Windows/Linux
WCS-LOC-UPG-K9 **Upgrading Cisco WCS Base to Cisco WCS Location**	
• Supports upgrading a Cisco WCS base license to support location services • Supports deployment of Cisco WCS on a single server • Includes location services to support tracking of a single Wi-Fi device on demand or expanded location capabilities by adding a Cisco Wireless Location Appliance. • Cisco WCS Location must be selected to support deployment of a Cisco Wireless Location Appliance.	
WCS-APLOC-UPG-50	Cisco WCS Location Upgrade License supporting 50 access points, Windows/Linux
WCS-APLOC-UPG-100	Cisco WCS Location Upgrade License supporting 100 access points, Windows/Linux
WCS-APLOC-UPG-500	Cisco WCS Location Upgrade License supporting 500 access points, Windows/Linux
WCS-ENT-K9 **Enterprise licenses for large-scale deployments**	
• Supports deployment of Cisco WCS on a single or multiple servers • Includes location services to support tracking of a single Wi-Fi device on demand or expanded location capabilities by adding a Cisco Wireless Location Appliance. • 10,000 and 50,000 enterprises licenses include a Cisco WCS Navigator (WCS-NAV-20) license • These licenses are operational with Cisco Unified Wireless Network Software Release 4.1 and later.	
WCS-ENT-1000	Cisco WCS Enterprise License with Location for 1000 access points, Windows/Linux on Multiple Cisco WCS Servers
WCS-ENT-2500	Cisco WCS Enterprise License with Location for 2500 access points, Windows/Linux on Multiple Cisco WCS Servers
WCS-ENT-10000	Cisco WCS Enterprise License with Location for 10,000 access points, Windows/Linux on Multiple Cisco WCS Servers. Includes Cisco WCS Navigator
WCS-ENT-50000	Cisco WCS Enterprise License with Location for 50,000 access points, Windows/Linux on Multiple Cisco WCS Servers. Includes Cisco WCS Navigator
WCS-WLSE-UPG-K9 **Converting an existing CiscoWorks WLSE to Cisco WCS**	
CiscoWorks WLSE Conversion to Cisco WCS Base • Supports deployment of Cisco WCS on a single server • Available for CiscoWorks WLSE Models 1130-19 and 1133 only	
WCS-WLSE-APB-50	Cisco WCS Base License for WLSE conversion supporting 50 access points, Linux

Product Part Number	Product Description
WCS-WLSE-APB-100	Cisco WCS Base License for WLSE conversion supporting 100 access points, Linux
WCS-WLSE-APB-500	Cisco WCS Base License for WLSE conversion supporting 500 access points, Linux
WCS-WLSE-APB-1000	Cisco WCS Base License for WLSE conversion supporting 1000 access points, Linux
WCS-WLSE-APB-2500	Cisco WCS Base License for WLSE conversion supporting 2500 access points, Linux
CiscoWorks WLSE Conversion to Cisco WCS Location • Supports deployment of Cisco WCS on a single server • Includes location services to support tracking of a single Wi-Fi device on demand or expanded location capabilities by adding a Cisco Wireless Location Appliance. • Cisco WCS Location must be installed to support deployment of a Cisco Wireless Location Appliance.	
WCS-WLSE-APL-50	Cisco WCS Location License for WLSE conversion supporting 50 access points, Linux
WCS-WLSE-APL-100	Cisco WCS Location License for WLSE conversion supporting 100 access points, Linux
WCS-WLSE-APL-500	Cisco WCS Location License for WLSE conversion supporting 500 access points, Linux
WCS-WLSE-APL-1000	Cisco WCS Location License for WLSE conversion supporting 1000 access points, Linux
WCS-WLSE-APL-2500	Cisco WCS Location License for WLSE conversion supporting 2500 access points, Linux
AIR-WCS-DEMO-K9 **Cisco WCS Demonstration License** • Only available from http://www.cisco.com/go/license. • After requesting the license, go to Cisco Wireless Software Center (login required) to download Cisco WCS software. • There is no Cisco Technical Assistance Center (TAC) support for the Cisco WCS Demonstration License.	
AIR-WCS-DEMO-K9	Free Cisco WCS full featured, location-enabled, 30 day demonstration license supporting ten lightweight access points

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, visit Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about Cisco WCS, contact your local account representative or visit http://www.cisco.com/en/US/products/ps6305/index.html.

For more information about the Cisco Unified Wireless Network, visit http://www.cisco.com/go/unifiedwireless.

For more information, read the Cisco WCS Licensing and Ordering Guide at http://www.cisco.com/en/US/products/ps6305/products_data_sheet0900aecd804b4646.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C78-341404-10 06/08