UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE UNA PLATAFORMA DE ACCESO INALÁMBRICO WIFI DE ALTA DISPONIBILIDAD EN UN BANCO

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

JHON SANDY MUÑOZ MORALES

PROMOCIÓN
2006-I

LIMA-PERÚ
2010

IMPLEMENTACIÓN DE UNA PLATAFORMA DE ACCESO INALÁMBRICO WIFI DE ALTA DISPONIBILIDAD EN UN BANCO

A mis padres, porque creyeron en mí y porque me sacaron adelante,
dándome ejemplos dignos de superación y entrega,
porque en gran parte gracias a ustedes
hoy puedo ver alcanzada mi meta ya que siempre estuvieron impulsándome en los
momentos más difíciles de mi carrera,
y porque el orgullo que sienten por mi fue lo que me hizo ir hasta el final.
Va por ustedes, por lo que valen,
porque admiro su fortaleza y por lo que han hecho de mí.
A mis hermanos, tíos, primos, abuelos y amigos.
Gracias por haber fomentado en mí el deseo de superación
y el anhelo de triunfo en la vida.
Mil palabras no bastarían para agradecerles su apoyo,
su comprensión y sus consejos en los momentos difíciles.
A todos, espero no defraudarlos y
contar siempre con su valioso apoyo, sincero e incondicional

SUMARIO

El presente trabajo describe el diseñó e implementación de una plataforma de accesos inalámbrico WiFi de alta disponibilidad.

La solución es necesaria debido a que el creciente número de usuarios corporativos e invitados hacía ineficiente la administración de los puntos de accesos inalámbricos. También se detectó que tal cómo estaban configurados los puntos de acceso, los usuarios eran propensos a la pérdida de conectividad.

Para optimizar el trabajo de control y administración de estos recursos de red inalámbrica, se opta por un equipo, denominado controlador, el cual centraliza toda la administración de los parámetros de los puntos de accesos (AP o access point), los cuales pasan a denominarse puertos de acceso.

Esta solución se consideró sea aplicada en dos emplazamientos lejanos, cuya red de datos está conectada por fibra óptica. Para hacer más robusta la solución, se utilizó un controlador de puertos de acceso en cada emplazamiento, los cuales trabajan en simultáneo (cluster) balanceando el número de puertos de acceso administrados. Si uno falla, el otro controlador se hace cargo de la administración de los puertos de accesos inalámbricos.

La aplicación tecnológica se aplicó a una institución bancaria, sin embargo esta topología es aplicable a cualquier otra institución que lo requiera. La tecnología usada en la solución corresponde al estándar 802.11 a, b, g, con proyección a 802.11 n. estas tecnologías serán materia del marco teórico para una mejor comprensión.

ÍNDICE

INTRODUCCIÓN

La solución que es desarrollada en este informe surge de la necesidad optimizar el servicio y administración de los puntos de acceso inalámbricos para un gran y creciente número de usuarios corporativos e invitados, evitando las pérdidas de conectividad a las que era propenso el sistema.

También se consideró brindar una arquitectura robusta que permitiera la administración distribuida de los puertos de accesos, y que ante la falla de uno de los controladores de los puertos de accesos inalámbricos, otro controlador asumiera toda la administración de sus parámetros.

Dado el escenario, edificios de varios pisos y los terminales de usuario comunes en el medio (PDA, LapTop, etc.), se optó por implementar la plataforma de accesos inalámbrico mediante el estándar 802.11 a, b y g, haciendo una proyección para el tipo n.

La solución se llega a implementar por el uso de un controlador que centraliza la administración de los parámetros de los puertos de accesos inalámbricos, lo que no sucedía con los puntos de accesos originales. La robustez es lograda por la utilización de más de un controlador, los cuales trabajan de manera distribuida y simultánea, pudiendo en caso de falla de uno de ellos, hacerse cargo de las labores de administración los demás controladores.

El diseño presentado tiene cómo ámbito dos emplazamientos lejanos, la cantidad de puertos de acceso desplegados en total para ambas instalaciones son noventa y seis unidades (96) pero con capacidad de administrar hasta ciento veintiocho (128). El tiempo utilizado para el estudio e implementación fue de tres meses.

La disponibilidad tecnológica no fue problema por cuanto los equipos estaban disponibles comercialmente y no se requería de importaciones especiales. El balanceo incluye, el número de puertos de acceso en cada controlador, la asignación de frecuencias utilizadas, el número de usuarios registrados por puerto de accesos, etc.

Aunque la configuración del controlador podía ser realizada por cable serial o Telnet (línea de comandos), para hacer mucho más eficiente esta tarea se añadió para la solución, la utilización de un software propietario especializado WLAN Management Software (WMS) mucho más amigable e intuitivo.

El diseño fue posible gracias a la experiencia adquirida en la empresa CONVEXUS SAC, empresa dedicada al rubro de la telemática y telefonía. Cómo pasante en dicha

empresa se contribuyó en los esfuerzos de esta solución liderando el proyecto. Se analizó la situación de la necesidad, se identificaron las opciones de mejora y de diseño de la solución Inalámbrica. En conjunto con el equipo de trabajo aprendió como realizaban su trabajo. El equipo estaba conformado por jefes de proyecto, administradores de red y otros en una visión común.

La bibliografía utilizada en este trabajo es variada en cuanto a la teoría (Cisco), para la parte de diseño se contó con toda la documentación técnica requerida.

El presente informe de suficiencia, se divide de la siguiente manera: En el primer capítulo se expone el problema de ingeniería, haciendo hincapié en el objetivo y los alcances de la solución propuesta, en el segundo capítulo se exponen los conceptos necesarios que sustentan la explicación para la solución propuesta, en el tercer capítulo se describe la metodología de la solución, exponiendo los estudios preliminares para la cobertura, la localización de los puertos de accesos, y demás aspectos técnicos. En el capítulo final se hace un compendio de la programación de trabajos, el equipamiento usado, y los costos de dicha solución

Debo agradecer a la empresa Nortel por su excelente colaboración en el soporte tecnológico utilizado. A su vez a la empresa CONVEXUS SAC por haberme autorizado la presentación de mi trabajo, y la institución bancaria bajo sus términos de confidencialidad.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

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

1.1 Descripción del Problema

Un ineficiente servicio y administración de los puntos de accesos inalámbricos para el creciente número de usuarios corporativos e invitados en todos los emplazamientos de una empresa bancaria.

1.2 Objetivos del trabajo

Diseñar e implementar una plataforma de acceso inalámbrico WiFi (802.11) de alta disponibilidad que brinde seguridad de información a la empresa bancaria.

La solución se logrará mediante la utilización de equipos controladores (administradores) de los parámetros de los puertos de accesos. Estos controladores trabajan de manera distribuida (simultánea) balanceando el número de puertos de accesos, el número de usuarios registrados en cada acceso, las frecuencias, etc.

En caso de falla de uno de los controladores, los otros asumen toda la administración. Se diseña el sistema para 96 puertos de accesos, pudiendo ser capaces de servir el sistema hasta 128. Para la solución se debe determinar primero la ubicación ideal de estos puertos de acceso inalámbricos.

1.3 Evaluación del problema

El sistema inicial, si bien contaba con un número aceptable de puntos de acceso y cobertura, la labor de configurar cada uno de los AP era realizada de manera manual lo que hacía engorroso administrar a los usuarios, limitándolos a estos en su desplazamiento por las instalaciones (roaming).

El tema de cobertura fue constituyéndose en otro problema dado el mayor número de usuarios, así mismo el uso y asignación de frecuencias o canales. La caída de una punto de acceso no era advertido automáticamente por el personal de soporte técnico.

La solución propuesta es de suma importancia puesto que permite cubrir una mayor área y número de usuarios, así mismo una eficiente administración de los parámetros de

los puertos de accesos (usuarios, frecuencias, etc.).

La inclusión de controladores trabajando en simultáneo permite ahora un balanceo de los puertos de acceso y la redundancia, es decir que en caso de que uno de los controladores falle, los demás asuman el control de los puertos de acceso que estaban siendo administrados por el controlador caído.

1.4 Alcance del trabajo

Se diseña e implementa una plataforma de acceso inalámbrico WiFi (802.11) de alta disponibilidad que brinda seguridad de información a la empresa bancaria.

El diseño presentado abarca dos emplazamientos lejanos, la cantidad de puertos de acceso desplegados en total para ambas instalaciones son noventa y seis unidades (96) pero con capacidad de administrar hasta ciento veintiocho (128). El tiempo utilizado para el estudio e implementación fue de tres meses.

El balanceo incluye, el número de puertos de acceso en cada controlador, la asignación de frecuencias utilizadas, el número de usuarios registrados por puerto de accesos, etc.

1.5 Síntesis del trabajo

Para el diseño de la infraestructura de seguridad inalámbrica, como primer paso se escanearon todos los niveles de la entidad bancaria, donde cada nivel tiene aproximadamente 1500 m2, logrando así identificar la cantidad de punto de acceso (AP). Esto se llevo a cabo mediante una herramienta que puede ser instalada en Windows llamada Network Stumbler, lo cual facilito el trabajo de localización de los mismos, así como de los canales utilizados por estos equipos.

Después de realizado el análisis, se procedió a la detección de “Zonas Oscuras”, es decir zonas con mucha interferencia, o a las que no llega el servicio debido a obstáculos, que influirán en la calidad de la red. Con esta información se determino el lugar óptimo de emplazamiento de los puntos accesos Inalámbricos para asegurar una cobertura adecuada a todos los usuarios.

Una vez determinado la ubicación de los puntos de accesos, se procedió a identificar los equipos de comunicación (conmutadores de datos) para tal propósito la entidad financiera proporcionó dicha información que consistía en el tipo de Conmutadores de datos, diagrama de distribución de red, y sus ubicaciones físicas por nivel (wiring close). La topología de red desplegada en la Entidad Bancaria tiene una configuración estrella. Su entorno de red esta diferenciada en dos etapas de red: 1) Etapa acceso y 2) Core (núcleo).

1. En la etapa de acceso los equipos de comunicación son fabricación variada como Alcatel y Nortel. Estos equipos manejan VLAN (Redes virtuales de área local), cuentan

con 24 o 48 puertos, enlaces de fibra y también tienen la capacidad de manejo de etiquetas, también conocido cómo Tagging (IEEE 802.1Q)

2. En la etapa de Core de Red es el centro de red en la estrella, a esta llegan los enlaces de fibras procedentes de los distintos armarios (wiring close) repartidos por todo el edificio de la entidad bancaria. El Core esta compuesta por dos switches en configuración activo-activo con balanceo de carga.

Una vez entendida la topología de red se procedió a la configuración de los equipos de red, tanto alámbricos como inalámbricos bajo las siguientes condiciones:

a) La red inalámbrica como única finalidad es brindar acceso a la intranet e Internet inalámbrico a usuario conformados por trabajadores del banco (Corporativo) y los usuarios invitados solamente acceso a Internet no pudiendo accesar a la red corporativa, esto usuario serán los que el banco autorice.

b) Dos (2) SSIDs (Service Set Identifier) o números identificadores, uno para usuarios corporativos y otro para invitados.

c) El SSID estará modo oculto (los SSID no serán visibles)

d) Los tráficos en VLAN´s se han separado tanto para usuarios corporativos e invitados

e) Los SSID estarán vinculados a su respectiva VLAN, tanto para usuarios corporativos e invitados.

f) Para el caso de los usuarios invitados el controlador inalámbrico asignará dinámicamente una dirección IP dentro del pool (grupo de IPs disponibles) de IPs que el banco determine.

g) En el caso de los usuarios corporativos, las direcciones IP serán asignadas dinámicamente por el Servidor DHCP (Dynamic Host Control Protocol) del Banco

h) La autenticación de usuarios corporativos se realizará mediante Servidor RADIUS del banco y a la autenticación de los usuarios invitados será desde el controlador inalámbrico.

i) Los controladores inalámbricos estarán configurados en alta disponibilidad.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

En este capítulo se exponen los conceptos esenciales más importantes que faciliten el entendimiento de la solución descrita en el presente documento.

Los temas a tratar son 1) Introducción a las redes inalámbricas, 2) Normativa de frecuencias y estandarización tecnológica, 3) Conceptos de networking, 4) Servicios de red, 5) Redes privadas virtuales VLAN, 6) Power over Ethernet, 7) Arquitectura wireless LAN, 8) Seguridad en redes inalámbricas, 9) Sistema de administración distribuido.

2.1 Introducción a las redes inalámbricas

El creciente y sostenido desarrollo de las ciencias de la información, ha permitido a las organizaciones cubrir nuevas necesidades de conectividad para mantenerse competitivos en el escenario actual. Por este motivo es inconcebible que cualquier compañía no posea conexión a Internet, redes de computadores, centrales telefónicas propias y tampoco les haya brindado un adecuado servicio de correo electrónico para sus funcionarios.

Adicionalmente existe la necesidad de interconexión de servicios de comunicaciones y movilidad de funcionarios que les permitan aumentar su productividad. En tal escenario anterior, han aparecido tecnologías inalámbricas eficientes que permiten satisfacer los requerimientos.

No se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas, se considera que serán sólo un complemento. Las redes cableadas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes Inalámbricas actuales ofrecen velocidades de 11Mpbs, 54Mbps y 600Mbps, las redes cableadas ofrecen velocidades mayores de 100Gbps.

Sin embargo, se puede combinar las redes cableadas y las inalámbricas generando un Red Híbrida que resuelva los últimos metros hacia la estación base. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

Para lograr la implementación de sistemas de telecomunicaciones eficientes que permitan cubrir la demanda actual, es importante considerar dos objetivos claros: 1)

mantenerse a la vanguardia de la tecnología y 2) reducir los costos los costos. Esto es debido a que en la actualidad continúa el desarrollo de las redes de computadores e Internet, y el incremento de ancho de banda para diversas aplicaciones como: videoconferencia, VoIP y Telefonía IP.

2.1.1 Visión general

Una Red de Área Local Inalámbrica (WLAN) permite la interconexión entre dos o más puntos, nodos o estaciones, por medio de ondas electromagnéticas que viajan a través del espacio llevando información de un lugar a otro. Para lograr el intercambio de información existen diferentes mecanismos de comunicación o protocolos que establecen reglas que permiten el flujo confiable de información entre nodos. Por ejemplo, el conjunto de protocolos TCP/IP utilizado en redes de computadoras como Internet, permite que cualquier computadora que los implemente pueda comunicarse con otra que se encuentre conectada a la misma red.

Los estándares son una serie de normas que definen la forma en que se deben realizar ciertos procesos para garantizar la calidad y seguridad de su funcionamiento, sin importar el tipo de dispositivo o las diferencias en su fabricación. Los estándares facilitan además la interoperabilidad entre componentes aunque estos tengan características diferentes. Existen diferentes organismos internacionales que originan estándares; en el área de telecomunicaciones se encuentran, por ejemplo, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por su sigla en inglés) y la Unión Internacional de Telecomunicaciones (UIT).

2.2 Normativa de frecuencias y estandarización tecnológica

La gran mayoría de las redes inalámbricas utilizan tecnología Wi-Fi. Esta tecnología está definida en la familia de estándares inalámbricos 802.11 del IEEE, siendo las más representativas las enmiendas 802.11a, 802.11b, 802.11g, 802.11e y la 802.11n, que recientemente ha sido aprobada, pero de la cual ya existen versiones comerciales que se anticiparon a dicha aprobación.

Esta familia de estándares trabaja en las bandas de radiofrecuencia de 2.4GHz y 5GHz asignadas por la UIT para redes inalámbricas como uso secundario. En esta banda trabajan también los hornos de microondas domésticos y muchos otros dispositivos industriales que no requieren de licencia por parte de los entes reguladores del espectro en cada país; de aquí se deduce que el uso primario de estas frecuencias es para aplicaciones distintas a las de comunicación.

Debido a que estas frecuencias también han sido utilizadas para diferentes servicios de comunicaciones como teléfonos inalámbricos, intercomunicadores, transmisión de video y audio a corta distancia, etc. Por este motivo se debe tomar en cuenta los otros

usuarios de esta porción del espectro en un espacio físico determinado y establecer límites en los niveles de potencia máximos utilizables, para evitar interferencias con otras redes.

El estándar 802.11g usa la banda de frecuencias de 2.4GHz mientras que la 802.11a usa la banda de frecuencia de 5GHz. Esto hace que las redes que utilizan una u otra tecnología no sean interoperables a pesar de que utilizan las mismas técnicas de modulación y por ende la misma tasa máxima de transmisión de 54Mbps.

El estándar 802.11b tiene una tasa de transferencia de 11 Mbps y opera también en la banda de 2.4GHz por lo cual es compatible con la 802.11g, que hace posible la interoperabilidad de dispositivos y redes que los utilicen.

Cada variante del estándar utiliza cierto número de canales dentro de la banda de frecuencia de trabajo. Los canales están separados 5MHz, pero cada transmisión ocupa unos 20MHz, por lo que no se pueden utilizar canales contiguos sin causar interferencia.

El estándar 802.11n está definido para trabajar tanto en la banda de 2.4GHz como en la de 5GHz y ofrece una velocidad nominal de transmisión de hasta 600Mbps gracias a la incorporación de la tecnología MIMO (Múltiple Input, Múltiple Output). Ésta permite la utilización de varios flujos de datos al mismo tiempo entre el mismo par de estaciones, así como el uso de canales de 40MHz de ancho y de técnicas de modulación más avanzadas.

2.3 Conceptos de networking

Al implementar una solución de redes se debe identificar los elementos, así como los servicios y las alternativas de integración que presentan los dispositivos para realizar una configuración. Para el caso de las redes inalámbricas se tienen que diferenciar conceptos y funciones que pueden tenerse en equipos como los puntos de acceso o router inalámbricos, ya que dada su versatilidad permiten un mayor control de la red. Los aspectos que serán explicados a continuación son: a) Red de computadoras, b) Configuración de la red, c) Clasificación de las redes y d) Componentes básicos de una red.

a. Red de computadoras

Una red de computadoras es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a Internet, e-mail, chat, juegos), etc.

b. Configuración de la red

Para que un equipo determinado pueda acceder a la red y a Internet, es necesario configurar el acceso a la red. Algunos datos de acceso a la red deben ser suministrados

por el ISP (Internet Service Provider), que es la entidad con la que se tenga contratados los servicios de acceso a Internet.

Para conectarse a un LAN y a Internet, es necesario tener correctamente configurado el protocolo TCP/IP, en las propiedades de la conexión a la red. La dirección IP de un ordenador debe ser única dentro de la red a la que pertenece. Las direcciones IP que se tienen dentro de una LAN son privadas y las que comunican la LAN con Internet son públicas.

c. Clasificación de las redes

Las redes se pueden clasificar de acuerdo al área de cobertura en la que prestan servicios:

1. LAN (Local Area Network).- Son pequeñas redes como por ejemplo las que podemos crear en nuestro propio domicilio entre varios ordenadores. Son redes en las que cada equipo puede comunicarse con el resto de manera rápida debido a las pequeñas distancias que ha de recorrer la información. Son redes de uso privado.
2. MAN (Metropolitan Area Network).- De tamaño superior a las LAN, pueden abarcar una ciudad entera y la distancia entre puntos no sueles superar la decena de kilómetros. Un ejemplo sería la de que podría crearse una para unir varios comercios o entidades públicas de una ciudad.
3. WAN (Wide Area Network).- Redes de amplio alcance capaces de cubrir distancias de hasta miles de kilómetros. Las WAN puedes ser de tipo privado o público. De tipo privado puede ser la WAN de una empresa que permite la comunicación entre sucursales situadas en ciudades diferentes.
4. Internet.- Es una inmensa red de redes informáticos que están unidas entre si a nivel mundial.

d. Componentes básicos de una red

Los componentes básicos para una red local:

1. Servidor.- Es una computadora utilizada para gestionar el sistema de archivos de la red, da servicio a las impresoras, controla las comunicaciones y realiza otras funciones.
2. Estaciones de Trabajo.- Se pueden conectar a través de la placa de conexión de red y el cableado correspondiente. Los terminales "tontos" utilizados con las grandes computadoras y mini computadoras son también utilizadas en las redes, y no poseen capacidad propia de procesamiento.
3. Medio de transmisión (Cableado).- Permite la interconexión de dispositivos de red para la transmisión de datos.
4. NIC o adaptador de red Ethernet.- Permite el acceso de una computadora a una red. Cada adaptador posee una dirección MAC que la identifica en la red y es única. Una

computadora conectada a una red se denomina nodo.

5. Concentrador o hub: Funciona como un repetidor, pero permite la interconexión de múltiples nodos, además cada mensaje que es enviado por un nodo, es repetido en cada boca el hub.

6. Conmutador o switch: Funciona como el bridge, pero permite la interconexión de múltiples segmentos de red, funciona en velocidades más rápidas y es más sofisticado. Los switches pueden tener otras funcionalidades, como redes virtuales y permiten su configuración a través de la propia red.

7. Enrutador o router: Funciona en una capa de red más alta que los anteriores el nivel de red, como en el protocolo IP, por ejemplo haciendo el enrutamiento de paquetes entre las redes interconectadas.

2.4 Servicios de red

En esta sección se mencionarán seis servicios de red importantes y vinculados a la solución propuesta en este informe; a) Web, b) DNS, c) DHCP, d) RADIUS, y e) LDAP.

a. Web

Son un conjunto de aplicaciones o de tecnologías con capacidad para interoperar en la Web. Estas aplicaciones o tecnologías intercambian datos entre sí con el objetivo de ofrecer unos servicios. Los proveedores ofrecen sus servicios como procedimientos remotos y los usuarios solicitan un servicio llamando a estos procedimientos a través de la Web.

Estos servicios proporcionan mecanismos de comunicación estándares entre diferentes aplicaciones, que interactúan entre sí para presentar información dinámica al usuario, brindando interoperabilidad y extensibilidad entre estas aplicaciones, y que al mismo tiempo sea posible su combinación para realizar operaciones complejas, es necesaria una arquitectura de referencia.

b. DNS (Domain Name System)

Es un servicio que permite resolver direcciones IP con relación a nombre de dominio, a través de una enorme base de datos de correspondencias con IP's. Existen una variedad de servidores DNS a través de Internet con tablas de correspondencias entre nombres y direcciones IP, que son gestionadas por los NIC (Network Information Center) de cada país.

Existen tres elementos indispensables en Internet para que sea posible mostrar una página web.

1. Servidor web.- Es un servidor que está acondicionado para servir páginas web las 24 horas del día.

2. Dominio.- Es el nombre del dominio que buscará la gente en Internet, introduciendo lo

la barra de direcciones del navegador.

3. Servidor DNS.- Es el encargado de transformar la IP de un servidor web, en el nombre del dominio.

El funcionamiento es el siguiente: 1) Cuando se pone por ejemplo, cdmon.com en la barra del explorador, este realiza la consulta en Internet de cómo está configurado este dominio; 2) El servidor DNS le indica al explorador que tiene que ir a buscar la información de la página web a la IP del servidor web; 3) El explorador envía la petición de la página web al servidor web, indicándole el nombre del dominio que desea; 4) El servidor web sirve la página web y el explorador la muestra. Todo esto pasa en cuestión de milésimas de segundo.

c. DHCP (Dynamic Host Configuration Protocol)

El protocolo de configuración dinámica de Host o DHCP es un protocolo que permite a los administradores de red automatizar y gestionar de manera centralizada la asignación de direcciones del protocolo Internet (IP) en una red de una organización o de un proveedor de servicios de Internet (ISP). Usando el conjunto de protocolos de Internet (TCP/IP), cada ordenador que puede conectarse a Internet necesita una dirección IP exclusiva. Cuando una organización configura los ordenadores de diferentes usuarios para que éstos se conecten a Internet, debe asignar una dirección IP a cada ordenador.

d. RADIUS

RADIUS (Remote Authentication Dial-In User Service) es un protocolo de autenticación, autorización y manejo de cuentas de usuario originalmente desarrollado por Livingston Enterprises y publicado en 1997 como los RFC 2058 y 2059. Es utilizado para administrar el acceso remoto y la movilidad IP, como ocurre en servicios de acceso por modem, DSL, servicios inalámbricos 802.11 o servicios de VoIP (Voice over IP o Voz sobre IP). Este protocolo trabaja a través del puerto 1812 por UDP.

La autenticación gestionada por este protocolo se realiza a través del ingreso de un nombre de usuario y una clave de acceso. Esta información es procesada por un dispositivo NAS (Network Access Server) a través de PPP (Point-to-Point Protocol o Protocolo Punto-a-Punto) siendo posteriormente validada por un servidor RADIUS a través del protocolo correspondiente valiéndose de diversos esquemas de autenticación, como PAP (Password Authentication Protocol o Protocolo de Autenticación de Clave de acceso), CHAP (Challenge-Handshake Authentication Protocol) o EAP (Extensible Authentication Protocol), y permitiendo el acceso al sistema

e. LDAP

LDAP (Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de

directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos.

Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos y/o organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas). Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

La versión actual es LDAPv3, la cual es especificada en una serie de Internet Engineering Task Force (IETF) Standard Track Request for Comments (RFCs) como se detalla en el documento RFC 4510.

2.5 Redes privadas virtuales VLAN

Los grupos de trabajo en una red, creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o hub, Trae como consecuencia directa, que estos grupos de trabajo compartan el ancho de banda disponible y los dominios de "broadcast", con la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Una VLAN es una lógica de red de área local (o LAN) que se extiende más allá de una sola LAN tradicional a un grupo de segmentos de LAN, habida cuenta de configuraciones específicas. Debido a que una VLAN es una entidad lógica, su creación y configuración se realiza completamente en software.

Las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de "broadcast".

La principal diferencia con la agrupación física, como se ha mencionado, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma.

Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico o VLAN.

2.6 Power over Ethernet

La tecnología Power over Ethernet permite que los dispositivos Ethernet, como puntos de acceso y cámaras IP, reciban alimentación y datos a través del cableado de la LAN existente. El estándar PoE, IEEE802.3af, es el primer estándar internacional de distribución de alimentación a través de una LAN Ethernet. Esto ha provocado un incremento de dispositivos e instalaciones Power over Ethernet, y que tras unos pocos años se han extendido completamente ya que el coste de agregar puertos Ethernet acordes con 802.3af a los dispositivos se ha ido reduciendo.

Los dispositivos se pueden apagar o reiniciar desde un lugar remoto. Tradicionalmente, los dispositivos de red, tales como teléfonos IP, LAN inalámbrica puntos de acceso, computadoras portátiles y cámaras Web, también han requerido los dos tipos de conexiones. Dado el creciente número de dispositivos de LAN en las empresas, las conexiones de cableado AC para cada uno de ellos es una tarea costosa.

La especificación 802.3af elimina la necesidad de puntos de venta adicionales y los gastos incurridos en laborales de contratación de electricistas para instalarlos. El adaptador Power Over Ethernet (PoE) proporciona alimentación a las cámaras de vigilancia y a los periféricos de redes locales inalámbricas, tales como puntos de acceso, puentes y routers. Permite la transmisión de corriente por medio del cable de red Ethernet, con lo que se evita tener que conectar directamente la alimentación al periférico de red local inalámbrica.

El estándar 802.3af define una forma de disponer de energía sobre Ethernet. La especificación incluye la entrega de 48 voltios de alimentación de CA sin blindaje más de par trenzado de cableado. Trabaja con los tipos de cables existentes, incluyendo la categoría 3, 5, 5e y 6; horizontal y patch cables, patch-paneles; puntos de venta y hardware de conexión, sin necesidad de modificación

2.7 Arquitectura Wireless LAN

La implementación de una red inalámbrica exige el uso de diversos dispositivos que permiten poner en funcionamiento el sistema de conexión. Cada uno de estos dispositivos presenta más de una presentación, función y servicio permitiendo la flexibilidad y facilitando la movilidad, es así que muchos dispositivos presentan mayor versatilidad al acoplar servicios y funciones de otros dispositivos.

A continuación se describen: 1) Adaptadores de red, 2) Antenas, 3) Puntos de acceso, 4) Controladores.

2.7.1 Adaptadores

Los Adaptadores de WLAN Cisco Aironet Inalámbricos también se denominan adaptadores clientes. Son módulos de radio que proporcionan comunicaciones de datos inalámbricas entre dispositivos fijos, portátiles o móviles y otros dispositivos inalámbricos o una infraestructura de red cableada. Los adaptadores clientes son completamente compatibles cuando se los utiliza en dispositivos que soportan la tecnología Plug-and-Play (PnP).

La función principal de los adaptadores de clientes es transferir paquetes de datos a través de la infraestructura inalámbrica. Los adaptadores operan de manera similar a un producto de red estándar, excepto en que el cable se reemplaza por una conexión de radio. No se requiere ninguna función de networking especial, y todas las aplicaciones existentes que operan a través de una red operarán utilizando los adaptadores.

Entre las aplicaciones mas corrientes están la de conectar un equipo con otros equipos de la red sin necesidad de instalar cables. Esto puede resultar especialmente útil en instalaciones no permanentes como ferias, congresos, demostraciones, etc. Otra aplicación muy usual es cuando se quiere compartir la conexión de Internet de banda ancha con otros miembros de la familia y no es posible o deseable instalar cables con todo lo que ello significa.

2.7.2 Antenas

Una antena es un dispositivo cuya misión es difundir y/o recoger ondas radioeléctricas. Las antenas convierten las señales eléctricas en ondas electromagnéticas y viceversa.

Existen antenas de distintos tipos, pero todas ellas permiten las mismas funciones, de servir de emisor receptor de una señal de radio. Cuando la comunicación fluye en ambas direcciones, se denomina bidireccional. Si dicha comunicación no se efectúa simultáneamente, sino alternativamente, se denomina comunicación semiduplex. Todas las comunicaciones dentro del ámbito WIFI son bidireccionales semiduplex.

Todas las antenas tienen un patrón de radiación. Muy relacionada con el patrón de radiación está la polarización de la antena. Las antenas pueden ser agrupadas en sistemas para lograr el patrón deseado. Estos sistemas pueden entonces ser dirigidos electrónicamente. Debido al diseño de baja potencia de las WLANs, todas las antenas usadas son pasivas. Una antena pasiva no tiene amplificadores conectados, y por lo tanto tendrá las mismas características sea que esté transmitiendo o recibiendo. Se mencionarán a continuación tres tipos de antenas según su patrón de radiación:

a. Antenas direccionales (o directivas)

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un foco que emite un haz de luz concreta y estrecha pero de forma intensa (más alcance). En su interior tienen unas barras de metal que cruzan el interior de ese tubo.

Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. Como todas las antenas exteriores hay que protegerla ante posibles descargas eléctricas. La señal que emiten es direccional y proporciona una ganancia que se encuentra en el rango de 15 a 30 dBi. Eat debe ser orientada directamente hacia el lugar con el que se quiere enlazar.

b. Antenas omnidireccionales

Se les llama también antenas de fuste vertical. Se utilizan principalmente para emitir la señal en todas las direcciones. En realidad la señal que emite en es forma de óvalo, y sólo emite en plano (no hacia arriba ni hacia abajo). Orientan la señal en todas direcciones con un haz amplio pero de corto alcance.

Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir, con menor alcance.

Teóricamente la información "se envía" a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

Se suelen colocar en espacios abiertos para emisión todas las direcciones. También se usan en espacios cerrados. En caso de colocarlas en el exterior es conveniente colocarle un filtro de saltos de tensión, para evitar problemas con tormentas eléctricas.

El alcance de una antena omnidireccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

c. Antenas sectoriales

Son una combinación de antenas direccionales y omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la

omnidireccional pero algo menor que la direccional. Siguiendo con el ejemplo de la luz, una antena sectorial sería como un foco de gran apertura, es decir, con un haz de luz más ancho de lo normal.

Para tener una cobertura de 360° (como una antena omnidireccional) y un largo alcance (como una antena direccional) se debe instalar tres antenas sectoriales de 120° ó 4 antenas sectoriales de 80°. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

2.7.3 Punto de acceso

El AP (Access Point) extiende la capacidad de una red Ethernet a los dispositivos en una red inalámbrica existente. El AP funciona cómo punto de acceso a redes de datos para los dispositivos inalámbricos.

Los dispositivos inalámbricos pueden estar conectados a un único punto de acceso (Access Point), o pueden moverse entre varios AP ubicados dentro de una misma área. A medida que los clientes inalámbricos se mueven de una celda de cobertura a otra, mantienen la conectividad de la red.

Para determinar la mejor ubicación de un AP, se recomienda realizar un estudio de sitio antes de colocar el dispositivo en su lugar definitivo.

El administrador de red tiene la labor de configurar cada unidad AP de acuerdo a los requisitos de la red, proporcionando a) Roaming (itinerancia) de clientes sin conflictos, b) Facilidad de instalación y funcionamiento, c) Cifrado de los datos enviados por radio, d) Enlaces de red de alta velocidad, etc.

El punto de acceso ofrece una gama completa de métodos de autentificación de usuario y seguridad inalámbrica basada en estándares para garantizar un acceso adecuado y seguro a los recursos de la red.

Los administradores de red pueden reducir los gastos implícitos de configuración mediante la implantación de una red unificada que ofrezca una gestión centralizada de las políticas y los dispositivos de redes cableadas e inalámbricas.

Los aspectos a tratar a continuación son 1) Seguridad, 2) Conectividad, 3) Calidad de servicio (QoS), y d) Gestión.

a. Seguridad

Se contemplan en esta categoría once ítems: 1) Posibilidad de elegir entre IEEE 802.11i Acceso Wi-Fi protegido 2 (WPA2) o WPA, 2) Seguridad y control de acceso, 3) Autentificación local mediante RADIUS, 4) Autenticación MAC basada en RADIUS, 5) Autentificación MAC local, 6) Filtro del tráfico del cliente de puente inalámbrico local, 7) Sistema cerrado, 8) SSL(Secure Sockets Layer), 9)SSHv2 (Secure Shell), 10)VLAN de gestión, 11) Control del acceso de gestión. Los que serán explicados a continuación.

a.1 Posibilidad de elegir entre IEEE 802.11i Acceso Wi-Fi protegido 2 (WPA2) o WPA

Bloquea el acceso inalámbrico no autorizado autenticando a los usuarios antes de conceder el acceso a la red; el sólido cifrado AES (Norma de codificación avanzada) o TKIP (Protocolo de integridad de clave temporal) garantiza la integridad de los datos del tráfico inalámbrico.

a.2 Seguridad y control de acceso

Comprenden a 1) Listas de control de acceso por usuario, 2) Asignación automática de VLAN, 3) Límites de velocidad, 4) IEEE 802.1X, 5) Detección de puntos de acceso colindantes (AP no autorizados) y redes inalámbricas "ad-hoc", y 6) Un número determinado de BSSID (Basic Service Set IDentifier) por radio con VLAN, seguridad y autentificación independientes.

1. Listas de control de acceso por usuario.- Permiten o deniegan el acceso de los usuarios a recursos específicos de la red en función de la identidad del usuario y la hora del día, permitiendo que varios tipos de usuario (empleados, visitas, trabajadores temporales) de la misma red tengan acceso a servicios específicos sin poner en peligro la seguridad de la red ni disponer de acceso autorizado a datos confidenciales.
2. Asignación automática de VLAN.- Asigna usuarios automáticamente a la VLAN adecuada en función de su identidad, comunidad y hora del día;
3. Límites de velocidad.- Aplican automáticamente límites de velocidad de entrada al tráfico de los usuarios en función de la identidad, comunidad y hora del día.
4. IEEE 802.1X.- Proporciona autentificación de usuario basada en puerto que admite el protocolo de autentificación extensible (EAP), TLS, TTLS, SIM, GTC y PEAP con la posibilidad de optar por cifrado AES, TKIP o WEP estático o dinámico para proteger el tráfico inalámbrico entre los clientes autentificados y el punto de acceso.
5. Detección de puntos de acceso colindantes (AP no autorizados) y redes inalámbricas "ad-hoc".- Se detecta periódicamente la existencia de puntos de acceso colindantes y redes inalámbricas "ad hoc". Para cada dispositivo inalámbrico detectado se captura la información recopilada durante la búsqueda, incluidos los ajustes de seguridad, BSSID, SSID, canal, RSSI y tipo de radio.

En algunos casos existen puntos de acceso que pueden funcionar en modo de búsqueda dedicada para realizar una exploración continuada en el entorno de RF cercano.

6. Un número determinado de BSSID por radio con VLAN, seguridad y autentificación independientes (1 o más).- Permite que el administrador controle el acceso de los usuarios a los recursos de la red en función de la autentificación de los usuarios y del nivel de seguridad fiable entre el sistema cliente y el punto de acceso.

a.3 Autentificación local mediante RADIUS

Proporciona seguridad inalámbrica 802.11i (WPA2) de categoría empresarial para pequeñas redes locales inalámbricas; sirve de método de autentificación auxiliar en caso de que los servidores RADIUS principal y secundario de la red no estén disponibles debido a una interrupción de la red. La función de autentificación de RADIUS local admite hasta una cantidad de cuentas de usuarios dependiendo de la marca y modelo.

a.4 Autenticación MAC basada en RADIUS

El cliente inalámbrico se autentica con un servidor RADIUS basado en la dirección MAC del cliente; esto resulta práctico para clientes sin interfaz de usuario o con una interfaz mínima.

a.5 Autentificación MAC local

Deniega o permite el acceso a la red basándose en la dirección MAC del cliente inalámbrico, que se compara con una base de datos almacenada en el punto de acceso.

a.6 Filtro del tráfico del cliente de puente inalámbrico local

Cuando está activado, evita la comunicación entre dispositivos inalámbricos asociados con el mismo punto de acceso.

a.7 Sistema cerrado

Restringe la difusión de SSIDs como medida de seguridad para ocultar la presencia de la red inalámbrica; el punto de acceso no responde a la solicitud de sondeo "ANY" del cliente inalámbrico.

a.8 SSL(Secure Sockets Layer)

Cifra todo el tráfico HTTP, permitiendo un acceso seguro a la interfaz de gestión basada en navegador de Web del punto de acceso.

a.9 SSHv2 (Secure Shell)

Cifra todos los datos transmitidos para proporcionar un acceso remoto seguro mediante el interfaz de línea de comandos (CLI) a través de redes IP.

a.10 VLAN de gestión

Garantiza la comunicación con el punto de acceso para realizar tareas de gestión; la VLAN de gestión se utiliza para gestionar el punto de acceso por medio de herramientas de gestión remota como la interfaz basada en Web, SSH, Telnet o SNMP.

a.11 Control del acceso de gestión

Para proporcionar más seguridad al punto de acceso, es posible desactivar interfaces de gestión que no sean necesarios, incluidos el navegador de Web, telnet y Secure Shell (SSH), así como el puerto de consola serie y el botón de reinicialización

b. Conectividad

Se contemplan en esta categoría nueve ítems: 1) Diseño de radio único o doble, 2) La

flexibilidad de uso de antenas permite una amplia gama de implantaciones de LAN inalámbrica, 3) Sistema de distribución inalámbrica (WDS) Bridging inalámbrico, 4) Compatible con el estándar IEEE 802.11h de la Unión Internacional de Telecomunicaciones (ITU), 5) Configuración internacional por país, 6) Selección automática de canales (ACS), 7) Potencia de salida ajustable, 8) Power over Ethernet IEEE 802.3af, 9) LLDP (Link Layer Discovery Protocol). Los cuales serán explicados a continuación

b.1 Diseño de radio único o doble

Dependiendo de las condiciones que tenga un equipo, se admite clientes inalámbricos de doble banda o solo una y se proporciona compatibilidad retroactiva con dispositivos inalámbricos.

Funcionamiento individual simultáneo de radio 802.11a, 802.11b o/y 802.11g; IEEE 802.11b en el caso del radio 802.11g.

Funcionamiento de radio IEEE 802.11b/g doble; permitiéndose en muchos casos proporcionar cobertura de LAN inalámbrica de voz y datos IEEE 802.11b/g de gran capacidad en redes en las que no se necesita compatibilidad con IEEE 802.11a.

1. Funcionamiento de radio única: proporciona un enlace inalámbrico con cada punto de acceso remoto; también sirve a los clientes inalámbricos locales;
2. Funcionamiento de radio doble: una radio proporciona un enlace inalámbrico con cada punto de acceso remoto. La segunda radio ofrece conectividad de red a clientes inalámbricos locales.

b.2 La flexibilidad de uso de antenas permite una amplia gama de implantaciones de LAN inalámbrica

1. Antena con diversidad integrada por radio con cobertura omnidireccional: proporciona sólida cobertura de LAN inalámbrica de doble radio para entornos de oficina abiertos;
2. Soporte de antena externa con diversidad por frecuencia de radio: permite configuraciones de antena externa para ampliar la cobertura inalámbrica o el bridging inalámbrico entre puntos de acceso.

b.3 Sistema de distribución inalámbrica (WDS) Bridging inalámbrico

Dado que amplía la conectividad de la red con puntos de acceso remotos ubicados fuera de la infraestructura cableada de la red, el bridging inalámbrico resulta ideal para aumentar la cobertura inalámbrica a edificios adyacentes, a lo largo de grandes salas de conferencias o entornos de campus exteriores. Cada punto de acceso puede o no soportar esta opción, variando la admisión del número de enlaces inalámbricos con puntos de acceso remotos. La distribución inalámbrica es compatible con los modos operativos de radio 802.11a, b y g.

b.4 Compatible con el estándar IEEE 802.11h de la Unión Internacional de Telecomunicaciones (ITU)

Utiliza la selección dinámica de frecuencia (DFS) y el control de potencia de transmisión (TCP) para seleccionar automáticamente otro canal y ajustar la potencia de transmisión con el fin de reducir la interferencia con sistemas tales como radares, si se detectan en el mismo canal

b.5 Configuración internacional por país

Se selecciona el país en cuestión y el punto de acceso configura automáticamente el funcionamiento para cumplir los requisitos normativos.

b.6 Selección automática de canales (ACS)

Ayuda a reducir al mínimo las interferencias entre canales al seleccionar automáticamente un canal de radio sin ocupar.

b.7 Potencia de salida ajustable:

Control del tamaño de las celdas para instalaciones de puntos de acceso de alta densidad.

b.8 Power over Ethernet IEEE 802.3af

Simplifica la implantación y reduce de manera espectacular los costes de instalación al eliminar los costes y el tiempo que supone el suministro de alimentación eléctrica local a cada ubicación de punto de acceso.

b.9 LLDP (Link Layer Discovery Protocol)

Activa la asignación en tiempo real de nodos a puertos de conmutación; el protocolo de detección estándar (IEEE 802.1AB) LLDP carga automáticamente los MIBs LLDP y de detección patentados para los sistemas de gestión de red que dependen de estos MIBs (Management Information Database). El MIB es un tipo de base de datos usado para administrar los dispositivos en una red de comunicaciones.

c. Calidad de servicio (QoS)

Comprende la 1) Compatibilidad con Wi-Fi multimedia (WMM) y 2) Admisión de prioridad de voz SpectraLink (SVP).

1. Compatibilidad con Wi-Fi multimedia (WMM): ofrece la funcionalidad de calidad de servicio (QoS) en redes inalámbricas estableciendo prioridades en el tráfico inalámbrico desde distintas aplicaciones.
2. Admisión de prioridad de voz SpectraLink (SVP): se brinda prioridad a los paquetes IP de voz SpectraLink enviados desde un servidor SVP a auriculares de voz inalámbricos SpectraLink para garantizar una excelente calidad de voz. El SpectraLink Voice Priority (SVP) es el estándar por defecto para la calidad de servicio (QoS) sobre redes Wi-Fi. Ha sido adoptado por los proveedores líderes de AP de las WLAN, SVP habilita la

convergencia de voz y aplicaciones de datos en una única infraestructura de red inalámbrica.

d. Gestión

Comprende: 1) Configuración y gestión remotas, 2) Compatibilidad con tarificación RADIUS, 3) SCP (Protocolo de copia segura) y 4) Gestión de redes.

1. Configuración y gestión remotas.- Mediante navegador Web seguro o interfaz de línea de comandos (CLI).
2. Compatibilidad con tarificación RADIUS: el soporte de servidor de tarificación RADIUS independiente para cada BSSID proporciona información detallada sobre la sesión, uso y eventual facturación de la actividad de cada cliente.
3. SCP (Protocolo de copia segura): permite una transferencia segura de archivos desde y en el punto de acceso; protege frente a descargas de archivos no deseados o la copia no autorizada del archivo de configuración.
4. Gestión de redes: muchos equipos presentan la funcionalidad para incluir funciones de control de autorización para el punto de acceso usando servidores RADIUS y autentificación MAC o protocolos de seguridad IEEE 802.1X. Se ofrece la capacidad de crear y asignar derechos de acceso, calidad de servicio e inscripción en VLANs que se asocian de forma dinámica con un usuario y se aplican en el punto de entrada o en el "perímetro" de la red. Entre las capacidades avanzadas cabe destacar la detección de dispositivos no autorizados, configuración y actualizaciones de firmware por grupos, supervisión de la actividad de las asociaciones de clientes inalámbricos y alertas por correo electrónico/buscapersonas.

2.7.4 Controladores de redes LAN inalámbricas

Los controladores de redes LAN inalámbrica (Wireless LAN Controller) proporcionan una gestión centralizada de LAN inalámbrica para servicios inalámbricos avanzados, lo que permite una red multiservicio de alta seguridad.

Son responsables de todas las funciones del sistema inalámbrico LAN, tales como las políticas de seguridad, prevención de intrusiones, gestión de RF, la calidad de servicio (QoS), y la movilidad. Trabajan en conjunto con Puntos de Acceso bajo un Sistema de Control (MC); Se emplean para servicios de voz y datos manteniendo un seguimiento para la ubicación de los clientes, proporcionan el control, escalabilidad, seguridad y confiabilidad de la red que necesitan los administradores para construir una red segura.

Incorpora una gestión de los derechos de acuerdo con la identidad, seguridad de datos inalámbricos e itinerancia segura en subredes, permitiendo a los administradores de redes aumentar la productividad empresarial mediante la ampliación del acceso seguro y adecuado de usuarios móviles a servicios de red sin incorporar nuevos riesgos.

Diseñada para reducir costes y complejidad al asegurar una LAN móvil, se integra de manera sencilla en los servicios de autenticación, red e infraestructura de WLAN, con lo que se consigue una estupenda rentabilidad de la inversión en TI (tecnologías de información).

Con una gestión centralizada de políticas y sistemas, los administradores pueden ajustar sin problemas las políticas de usuarios y seguridad en respuesta a las necesidades empresariales.

Un controlador admite:

Conexión inalámbrica: Con los dispositivos inalámbricos como teléfonos IP, portátiles y teléfonos los empleados se pueden comunicar y colaborar desde cualquier lugar.

Amplia cobertura: Con un soporte de hasta seis puntos de acceso, los empleados no están fuera de alcance ni desconectados.

Seguridad: La capacidad de soportar la mayoría de los estándares de seguridad significa que sus datos están siempre protegidos.

Integración: Como parte de las soluciones de redes inalámbricas unificadas de una marca en especial, permite su integración dentro de sus mismas soluciones.

Las características del controlador son agrupadas en a) Gestión, b) conectividad, c) Rendimiento, d) Capacidad de recuperación y alta disponibilidad, e) Gestión de políticas.

a. Gestión

Para esta tarea el controlador contempla las siguientes características: 1) Consola de administración, 2) Múltiples cuentas de administrador, y 3) Registro histórico completo de sesiones.

1. Consola de administración: simplifica la implantación y gestión de una LAN móvil segura al proporcionar un único lugar para crear y gestionar políticas de acceso de los usuarios, administrar la gestión de todo el sistema y supervisar todos los componentes del servidor de control acceso, así como la actividad de todos los usuarios.
2. Múltiples cuentas de administrador: aumentan la seguridad de la red al ofrecer tres niveles de acceso a la consola de administración, incrementando la seguridad de la red y la responsabilidad mediante la separación de las funciones de gestión de la red de la administración de las políticas de acceso, ambas asignadas y controladas mediante una cuenta de súper usuario.
3. Registro histórico completo de sesiones: proporciona información detallada para la identificación y solución de problemas.

b. Conectividad

Se caracteriza por poseer una conectividad backbone de alta velocidad Gigabit Ethernet. Gigabit Ethernet, también conocida como GigaE, es una ampliación del

estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet (También llamado 100-Base/T).

c. Rendimiento

Posee soporte para más de 50.000 usuarios simultáneos, proporcionando capacidad y escalabilidad de usuarios para grandes LANs inalámbricas.

d. Capacidad de recuperación y alta disponibilidad

Sus características en este ítem son:

1. Redundancia y recuperación automática del servidor de control del acceso: ofrece alta disponibilidad de red para implantaciones de LANs móviles de misión crítica; en caso de que el servidor de control de acceso principal falle o sea inaccesible, se activa inmediatamente un servidor secundario que se encarga de la gestión de todos los módulos de controlador de acceso Switch para ayudar a garantizar el acceso ininterrumpido a la LAN móvil.
2. Fuente Alimentación Redundante: Alimentación redundante contribuye a garantizar el funcionamiento interrumpido y la protección contra fallos de la fuente de alimentación al entrar en servicio sin interrupción en caso de fallo en los dispositivos. Cuando se detecta un fallo, la unidad proporciona instantáneamente alimentación al dispositivo defectuoso para que el equipo conectado no sufra una pérdida de función ni se reinicie. El Dispositivo afectado registra el evento de fallo de la fuente de alimentación en su archivo de registro local, así como en un gestor de eventos central mediante traps del protocolo de gestión de red simple (SNMP) o mensajes syslog.
3. Configuración Cluster N+1: Un método para conmutación por falla es agrupar los Controladores Wireless en redundancia N+1, con el fin de respaldar el Punto de Acceso (AP) como activo y backup en el mismo Cluster. Esto simplifica enormemente la configuración, gestión y también tiene en cuenta el hecho de que los Puntos de Acceso (AP) pueden conmutar por falla (failover) desde un Controlador Wireless a otro en el mismo cluster en el caso de una perdida temporal de conectividad durante una situación de avería en la red.
4. Redundancia en los Access Point: Los puntos de acceso pueden soportar una amplia variedad de opciones de flexibilidad ante un posible falla por ejemplo Redundancia para PoE, para las conexiones de enlace de datos y los servicios de seguridad puede ser proporcionada a la AP.
5. Redundancia PoE: Los puntos de acceso que tienen dos puertos Ethernet, PoE proporciona redundancia mediante la conexión de los dos puertos PoE que pueden estar

directamente conectada al controlador wireless o a través de un dispositivo llamado inyector PoE. Cuando los dos puertos Ethernet de los puntos de acceso están conectados, un puerto esta de modo activo y el otro de modo pasivo o backup (Dual-homing).

6. Redundancia en enlace de datos: Redundancia de enlace de datos de los puntos de acceso (AP) proporciona dos puertos Ethernet que conecta directamente a un controlador wireless, a dos controladores wireless, a un conmutador Ethernet (switch) intermediario, o una combinación de de controladores wireless y conmutador Ethernet. El homing Dual-link para redundancia de datos se activa automáticamente al conectar los dos puertos Ethernet de punto de Acceso (AP).
7. Itinerancia a través de subredes: ayuda a garantizar que los usuarios se mantengan conectados continuamente con la red y las aplicaciones.
8. Privacidad de datos inalámbrica: utiliza túneles IPSec, PPTP, L2TP/IPSec o SSH para cifrar el trafico inalámbrico con DES, 3DES, Blowfish, CAST o AES, para aportar la máxima confidencialidad de datos inalámbricos.
9. Secure Sockets Layer (SSLv3): cifra todo el tráfico HTTP en conexiones basadas en navegador.
10. Anti suplantación dirección MAC: evita acceso de usuarios sin permiso mediante la suplantación de de dirección MAC de un usuario de confianza.
11. Clasificación de paquetes: puede basarse en diversidad de criterios, incluyendo ID de VLAN, IP, puertos y direcciones IP de origen y destino, dirección MAC, identidad del usuario y Ethertype.
12. Admite IEEE 802.1Q VLAN: Permite etiquetado del tráfico en función del usuario o del punto de acceso a la red; Permite dirigir el tráfico inalámbrico por redes VLAN independientes; Permite la eliminación o reasignación de etiquetas de VLAN.
13. Clase de servicio (CoS): Las políticas de acceso permiten la reasignación de marcas de calidad de servicio, incluyendo el valor DiffServ, IP Precedente o tipo de servicio.

e. Gestión de políticas

Sus características en este ítem son:

1. Control y gestión del acceso a la red basada en identidades: permite a los administradores de red crear y mantener fácilmente políticas de acceso sólidas, incluido el acceso seguro e inalámbrico de invitados a los servicios de red adecuados, sin riesgo para la red.
2. Control preciso de quién ha accedido a qué y cuándo: las políticas de acceso gestionadas de forma centralizada combinadas con la inspección de paquetes forzada en la periferia permiten o deniegan el acceso de los usuarios a determinados servicios en el

extremo de la red, incluyendo servicios como Internet o el acceso por Web a intranets, FTP, Telnet, servidores de aplicaciones especializados o cualquier elemento de red que pueda identificarse mediante puertos y direcciones IP.

3. Servidor RADIUS integrado: puede realizar servicios de autentificación o actuar como servidor Proxy para un servicio de autentificación RADIUS remota; los servicios de autentificación activos permiten ahora la autentificación de usuarios y el control del acceso granular de tráfico de usuarios en LANs inalámbricas aseguradas con IEEE 802.11i o WPA.

4. Soporte de autentificación basado en normas para LDAP, Active Directory e IEEE 802.1X: se integra sin Problemas en servicios de autentificación existentes o utiliza la base de datos integrada.

5. Gestión de servicios mal configurados y redirección de proxy: permite un inicio de sesión transparente, seguro para invitados o usuarios que hayan cambiado sus configuraciones de redes cliente.

La Tabla 2.1 muestra un resumen de las características del controlador de red LAN inalámbrica.

Tabla 2.1 Características resumidas del controlador de WLAN

Características	**Beneficios**
Puertos Ethernet 10/100	Provee estos puertos para permitir una combinación con los puntos de acceso y establecer enlaces redundantes
Puertos habilitados con Power-over-Ethernet	Puede soportarse por lo general a través de uno o mas puertos Ethernet (802.3af Power over Ethernet (PoE)
Seguridad de cobertura Extendida	Extensión de cobertura más seguro para grandes tiendas y almacenes
Integración PCI	Soporte de PCI-certified architecture for retail customers
Suporte para 802.11n	Ofrece robusta cobertura con 802.11 a/b/g o ofrece fiabilidad sin precedentes utilizando 802.11n

2.8 Seguridad en redes inalámbricas

En la actualidad, gracias a la movilidad y reducción de costes que aporta la tecnología Wi-Fi, han surgido un gran número de redes inalámbricas en oficinas, centros de trabajo y lugares públicos (hot-spots). Sin embargo muchas veces no se tiene en cuenta la vulnerabilidad de estas redes tanto respecto a la privacidad de las comunicaciones como frente a intrusiones en la red.

Por tanto, a la hora de afrontar el reto de la movilidad, es imprescindible conocer los diferentes protocolos y mecanismos de seguridad existentes y tomar las medidas adecuadas. Una red inalámbrica tiene dos componentes principales: las estaciones (STA) y los puntos de acceso (AP).

Respecto a la protección de las redes inalámbricas existen una serie de medidas básicas y avanzadas para la protección de las redes inalámbricas. Siendo recomendado utilizar una combinación de, todas ellas.

2.8.1 Mecanismos de seguridad inalámbrica básicos

Los mecanismos de seguridad inalámbrico básicos son a) WEP, b) Firewall, c) Closed Network Access Control, d) Filtrado de direcciones MAC, e) Open System Authentication y f) Antivirus. Los cuales se verán a continuación.

a. Wired Equivalent Protocol (WEP)

Se trata del primer mecanismo de seguridad implementado, fue diseñado para ofrecer un cierto grado de privacidad, pero no puede compararse con protocolos de redes más seguros tales como IPSec para la creación de Virtual Private Networks (VPN). WEP comprime y cifra los datos que se envían a través de las ondas de radio. WEP utiliza una clave secreta, utilizada para el cifrado de los paquetes antes de su retransmisión. El algoritmo utilizado para el cifrado es RC4. Por defecto, WEP está deshabilitado.

b. Firewall

Sistema de defensa basado en la instalación de una "barrera" entre una computadora, un AP o un router y la Red por la que circulan todos los datos. Este tráfico es autorizado o denegado por el firewall, siguiendo instrucciones previamente configuradas.

Access Control List (ACL): Si bien no forma parte del estándar, la mayor parte de los productos dan soporte al mismo. Se utiliza como mecanismo de autenticación la dirección MAC de cada estación, permitiendo el acceso únicamente a aquellas estaciones cuya MAC figura en la lista de control de acceso (ACL).

c. Closed Network Access Control

Sólo se permite el acceso a la red a aquellos que conozcan el nombre de la red, o SSID. Éste nombre viene a actuar como contraseña.

d. Filtrado de direcciones MAC

Los puntos de acceso deben tener una relación de las direcciones MAC que pueden conectarse. No es un método que ofrezca un alto grado de seguridad, pero es una medida básica para evitar que el primero que pase por la calle pueda acceder a la red.

e. Open System Authentication

Es el mecanismo de autenticación definido por el estándar 802.11 y consiste en autenticar todas las peticiones que reciben. El principal problema de este mecanismo es que no realiza ninguna comprobación y, además, todas las tramas de gestión son enviadas sin ningún tipo de cifrado, incluso cuando se ha activado WEP.

f. Antivirus

Detecta y destruye virus, los cuales son software diseñados para dañar los sistemas

2.8.2 Mecanismos de seguridad inalámbrica avanzados

Los mecanismos de seguridad inalámbrica avanzados son a) TKIP, b) EAP-TLS, c) VPN, d) Estándar IEEE 802.1X, e) WPA, f) WPA2, g) Certificados digitales, h) Encriptador, i) Gestión de políticas, j) Detección de intrusos, k) Análisis de vulnerabilidad, l) Servidor RADIUS, m) EAP. Los cuales serán explicados a continuación

a. Protocolo de Integridad de Clave Temporal (TKIP)

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP, este protocolo posee un código de integración de mensajes (MIC) el cual cifra el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11 protegiendo con esto cualquier ataque por falsificación.

b. EAP-TLS (Extensible Authentication Protocol with Transport Layer Security)

Protocolo de autenticación basado en certificados digitales. Ofrece una autenticación fuerte mutua (es decir tanto de la estación como del punto de acceso), credenciales de seguridad y claves de encriptación dinámicas. Requiere la distribución de certificados digitales a todos los usuarios así como a los servidores RADIUS (Remote Authentication Dial In User service).

c. Virtual Private Network (VPN)

Sistema para simular una red privada sobre una pública, como por ejemplo Internet, La idea es que la red pública sea vista desde dentro de la red privada como un "cable lógico" que une dos o más redes que pertenecen a la red privada.

d. Estándar IEEE 802.1X

Utiliza el protocolo de autenticación extensible o EAP, para autenticar al dispositivo móvil, permitiendo a la Entidad de Autenticación de Puertos (Port Authentication Entity, PAE) un control del proceso de autenticación a la red.

e. Wifi Protected Access (WPA)

WPA utiliza el protocolo de integridad de clave temporal (TKIP) para codificar los datos, además Implementa el estándar 802.1x utilizando el protocolo de autenticación extensible (EAP).

f. Wifi Protected Access 2 (WPA2)

Recientemente aprobado por la Wi-Fi Alliance (1 de Septiembre del 2004), basado en el estándar de seguridad para 802.11, 802.11i cumpliendo con las normas del National Institute of Standards and Technology (NIST) FIPS 140-2. WPA2 implementa el algoritmo AES a diferencia de WPA que utiliza RC4, sin embargo WPA2 es totalmente compatible con WPA.

g. Certificados digitales

Software que acredita la identidad, autenticidad y seguridad de un sitio en Internet o

en Intranet para reducir los fraudes virtuales originados por la suplantación virtual de personas, empresas y sitios fantasmas.

h. Encriptador

Programa que convierte el texto a códigos indescifrables para que sea enviado por la Intranet o por Internet. Mediante otra contraseña el receptor convierte los códigos en texto.

i. Gestión de políticas

Sistema de administración proactiva o preventiva que verifica el funcionamiento del software de seguridad, generando alertas y reportes.

j. Detección de intrusos

Identifica el ingreso no permitido de intrusos internos y externos a determinadas áreas de la red y los sistemas informáticos.

k. Análisis de vulnerabilidad

Detecta debilidades de seguridad y prioridades de solución en las redes informáticas y sus equipos.

l. Servidor RADIUS

Es un protocolo ampliamente usado en el ambiente de redes, para dispositivos tales como routers, servidores y switches entre otros. Es utilizado para proveer autenticación centralizada, autorización y manejo de cuentas para redes de acceso dial-up, redes privadas virtuales (VPN) y, recientemente, para redes de acceso inalámbrico.

Los sistemas embebidos generalmente no pueden manejar un gran número de usuarios con información diferente de autenticación. Requiere una gran cantidad de almacenamiento.

RADIUS facilita una administración centralizada de usuarios. Si se maneja una enorme cantidad de usuarios, continuamente cientos de ellos son agregados o eliminados a lo largo del día y la información de autenticación cambia continuamente. En este sentido, la administración centralizada de usuarios es un requerimiento operacional.

Debido a que las plataformas en las cuales RADIUS es implementado son frecuentemente sistemas embebidos, hay oportunidades limitadas para soportar protocolos adicionales. Algún cambio al protocolo RADIUS deberá ser compatible con clientes y servidores RADIUS pre-existentes.

Un cliente RADIUS envía credenciales de usuario e información de parámetros de conexión en forma de un mensaje RADIUS al servidor. Éste autentica y autoriza la solicitud del cliente y envía de regreso un mensaje de respuesta. Los clientes RADIUS también envían mensajes de cuentas a servidores RADIUS.

Los mensajes RADIUS son enviados como mensajes UDP (User Datagram Protocol).

El puerto UDP 1812 es usado para mensaje de autenticación RADIUS y, el puerto UDP 1813, es usado para mensajes de cuentas RADIUS.

Algunos servidores usan el puerto UDP 1645 para mensajes de autenticación y, el puerto 1646, para mensajes de cuentas. Esto último debido a que son los puertos que se usaron inicialmente para este tipo de servicio.

m) EAP (Extensible Authentication Protocol)

La mayoría de los suministradores utilizan EAP como medio de comunicar peticiones de acceso entre cliente y punto de acceso. Pero este tipo de paquetes transportan sólo peticiones; el protocolo no describe cómo gestionar la autenticación misma. En consecuencia, cada fabricante ha optado por alguna de las extensiones propietarias que definen la tecnología sobre la que se soportará esta gestión, dando lugar a una auténtica sopa de acrónimos referidos todos ellos a implementaciones acordes con EAP pero, en ocasiones, incompatibles entre sí.

2.9 Sistema de administración distribuido

Las redes inalámbricas son propensas a los ataques, más aún, ya que su medio de transporte es el aire. Otro factor que contribuye a este riesgo es la fácil disponibilidad de herramientas de ataque.

Los gestores de la red constantemente tratar de garantizar la detección de accesos no autorizados en los puntos de acceso (AP) y otras intrusiones como ataques DoS (Denegación de Servicio), ataques de interferencia RF, etc. Una serie de factores como el ruido, interferencias, el aumento de tráfico y la atenuación de la señal de RF afectan a la topología de forma continua.

La detección de intrusos ayuda a: 1) Averiguar quién y qué es de su red., 2) Aplicar políticas de administración, 3) Cerrar todas las vulnerabilidades. Y 4) Disfrutar de una red inalámbrica libre de problemas.

2.9.1 Arquitectura distribuida

Los sistemas de administración realizan todo el proceso de vigilancia y seguridad de forma más simple para la LAN inalámbrica. Operan con sensores de hardware que pueden ubicarse en la red como cualquier otro dispositivo IP y pueden controlar de forma pasiva en el espectro de RF los paquetes 802.11.

Los elementos de la arquitectura para el sistema de administración distribuida vienen a ser los siguientes: a) Sensores de RF, b) Puntos de Acceso, c) Dispositivos inalámbricos, d) Software de administración.

a. Sensores de RF

Desempeñan las funciones de vigilancia de la RF en el espectro con parámetros como la fuerza de la señal, el ruido, los detalles del tráfico, errores y asociaciones. Estos

se remiten a los programas informáticos para darle una imagen completa de qué esta sucediendo en el lado de RF de la red.

b. Puntos de Acceso

Permiten el acceso a la red inalámbrica, son en algunos casos empleados como sensores o simples puntos inalámbricos para clientes.

c. Dispositivos inalámbricos

Están considerados los equipos clientes, cámaras IP, impresoras y entre otros equipos inalámbricos que trabajan en su mayoría de casos como agentes en ayuda de la seguridad, informando al servidor central sobre el estado de la red.

d. Software de administración

Permiten analizar toda la información recopilada a través de los sensores y dispositivos inalámbricos, toman decisiones de estrategias mediante diferentes técnicas configuradas al detectar fallos en la red, esta instalado en un equipo central (servidor central). La Figura 2.1 muestra a este software (WMS) y al Controlador de red inalámbrica (Wireless LAN Controller)

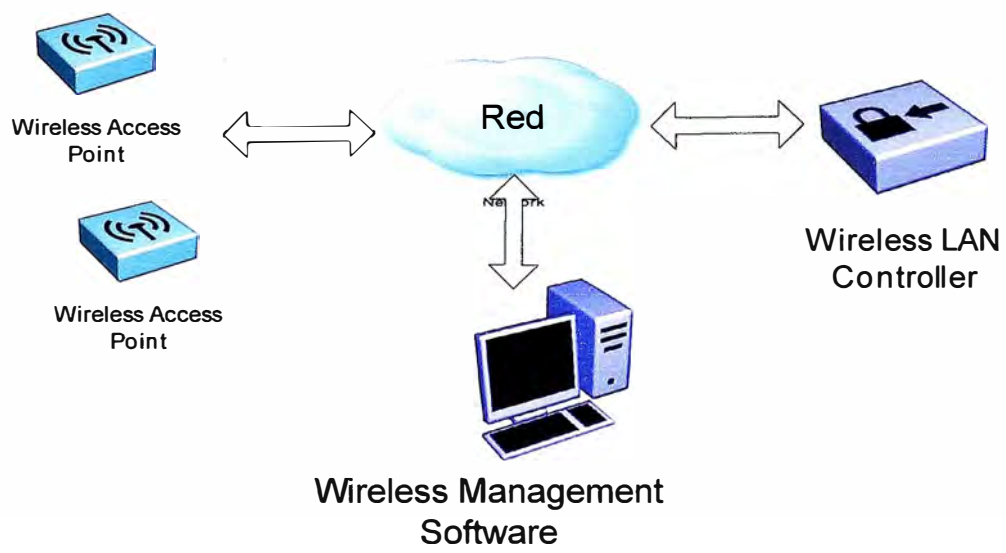

Figura 2.1 Diagrama de del Wireless Management Software (WMS)

2.9.2 Captura de paquetes

La captura de paquetes dentro de su gama 802.11, correlaciona y analiza diversas amenazas a la seguridad que se describen a continuación: a) Detección de intrusos, b) Los ataques de DoS, y c) Evaluación de la Vulnerabilidad

a. Detección de intrusos

La Detección de intrusos puede referirse a puntos de acceso-intrusos o equipos clientes-intrusos. Una vez que son detectadas por los sensores de RF la información pasa al servidor central (función principal). El software de administración correlaciona esta información con la información que ha recopilado desde el lado del cable de la red y alerta a los operadores de los posibles problemas.

b. Los ataques de DoS

Hay una serie de ataques de RF. Durante la autenticación los ataques afectan críticamente el funcionamiento de la WLAN. Estos sensores RF ayudan en la detección de estos ataques y pasan la información a un WiFi Manager.

c. Evaluación de la Vulnerabilidad

Existen algunas vulnerabilidades recurrentes en mantener una WLAN, por ejemplo.

La debilidad de WEP IV en uso, detección de Tráfico NetBIOS, etc. Los sensores RF identifican estas vulnerabilidades y el software reacciona inmediatamente y, por ende, impide eficazmente estas pequeñas vulnerabilidades.

Nota:
En el siguiente capítulo se describirá la metodología de la solución

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

En el presente capítulo se describe la metodología para la solución del problema. Se exponen los aspectos básicos a tomar en cuenta para el diseño, para luego explicar el antes y después de la solución implementada, mostrando seguidamente el aspecto conceptual del diseño y el equipamiento usado.

3.1 Aspectos básicos para el diseño e implantación

Con el propósito de diseñar e implementar una plataforma de acceso inalámbrico WiFi de alta disponibilidad en una entidad bancaria se realizaron una serie de tareas importantes que son descritas a continuación:

3.1.1 Identificación de puntos de acceso disponibles

Para el diseño de la infraestructura de seguridad inalámbrica, se escaneó la totalidad de niveles de la entidad bancaria (cada nivel tiene aproximadamente 1500 m2), logrando así identificar todos los puntos de acceso existentes.

Esta tarea llevo a cabo mediante una herramienta que puede ser instalada en Windows llamada Network Stumbler, lo cual facilito el trabajo de localización de los mismos, así como de los canales utilizados por estos equipos.

3.1.2 Detección de "Zonas Oscuras"

Después de realizado el análisis previo, se procedió a la detección de "Zonas Oscuras", es decir zonas con mucha interferencia o a las que no llega el servicio debido a obstáculos, que influirán en la calidad de la red.

Con esta información se determino el lugar óptimo de emplazamiento de los puntos accesos Inalámbricos para asegurar una cobertura adecuada a todos los usuarios.

3.1.3 Identificación de equipos de comunicación

Luego de haberse determinado la ubicación de los puntos de accesos, se procedió a identificar los equipos de comunicación (conmutadores de datos). Para tal propósito la entidad financiera brindó dicha información que consistía en: a) el tipo de Conmutadores de datos, b) diagrama de distribución de red, y sus ubicaciones físicas por nivel (wiring close).

La topología de red desplegada en la entidad bancaria tiene una configuración estrella. Su entorno de red esta diferenciada en dos etapas de red: 1) Etapa acceso y

2) Core (núcleo). Una descripción complementaria se muestra en las siguientes líneas:

1. En la etapa de acceso los equipos de comunicación son de fabricación variada como Alcatel y Nortel. Estos equipos manejan VLAN (Redes virtuales de área local), cuentan con 24 o 48 puertos, enlaces de fibra y también tienen la capacidad de manejo de etiquetas, también conocido cómo Tagging (IEEE 802.1Q)
2. En la etapa de Core de Red es el centro de red en la estrella, a esta llegan los enlaces de fibras procedentes de los distintos armarios (wiring close) repartidos por todo el edificio de la entidad bancaria. El Core esta compuesto por dos switches en configuración activo-activo con balanceo de carga.

3.1.4 Configuración de los equipos de red

Luego de recopilar toda la información sobre la topología de red se procedió a la configuración de los equipos de red, tanto alámbricos como inalámbricos bajo las siguientes condiciones:

a) La red inalámbrica como única finalidad es brindar acceso a la intranet e Internet inalámbrico a usuario conformados por trabajadores del banco (Corporativo) y los usuarios invitados solamente acceso a Internet no pudiendo accesar a la red corporativa, esto usuario serán los que el banco autorice.

b) Dos (2) SSIDs (Service Set Identifier) o números identificadores, uno para usuarios corporativos y otro para invitados.

c) El SSID estará modo oculto (los SSID no serán visibles)

d) Los tráficos en VLAN´s se han separado tanto para usuarios corporativos e invitados

e) Los SSID estarán vinculados a su respectiva VLAN, tanto para usuarios corporativos e invitados.

f) Para el caso de los usuarios invitados el controlador inalámbrico asignará dinámicamente una dirección IP dentro del pool (grupo de IPs disponibles) de IPs que el banco determine.

g) En el caso de los usuarios corporativos, las direcciones IP serán asignadas dinámicamente por el Servidor DHCP (Dynamic Host Control Protocol) del Banco

h) La autenticación de usuarios corporativos se realizará mediante Servidor RADIUS del banco y a la autenticación de los usuarios invitados será desde el controlador inalámbrico.

i) Los controladores inalámbricos estarán configurados en alta disponibilidad.

3.2 Criterios para el diseño

En esta sección se expondrán las necesidades propias de la empresa bancaria para la utilización de la solución implementada. Se describirá a la entidad financiera y sus principales requisitos técnicos.

3.2.1 Aspectos técnicos de la entidad bancaria

La entidad financiera tiene implementado una WLAN en algunas ubicaciones para reducir los costos de infraestructura de la red y aumentar la movilidad y productividad del personal.

La organización tiene una idea clara de sus necesidades de seguridad y ya ha implementado varias tecnologías para mejorar la seguridad de TI (Tecnologías de la información), por ejemplo, la autenticación de dominios, servidores de seguridad de Internet, programas de detección de virus y una solución VPN o de acceso remoto. Probablemente, tendrá planes a largo plazo para utilizar otras aplicaciones de alta seguridad, como el cifrado de archivos y el correo electrónico seguro.

El diseño de red lógico / físico simplificado de esta organización es definido en el diagrama siguiente (Figura 3.1) y corresponde a su situación antes de implementada la solución descrita. Una imagen con mayor detalle es mostrada en la Figura A.1 del Anexo A "Diagramas del sistema".

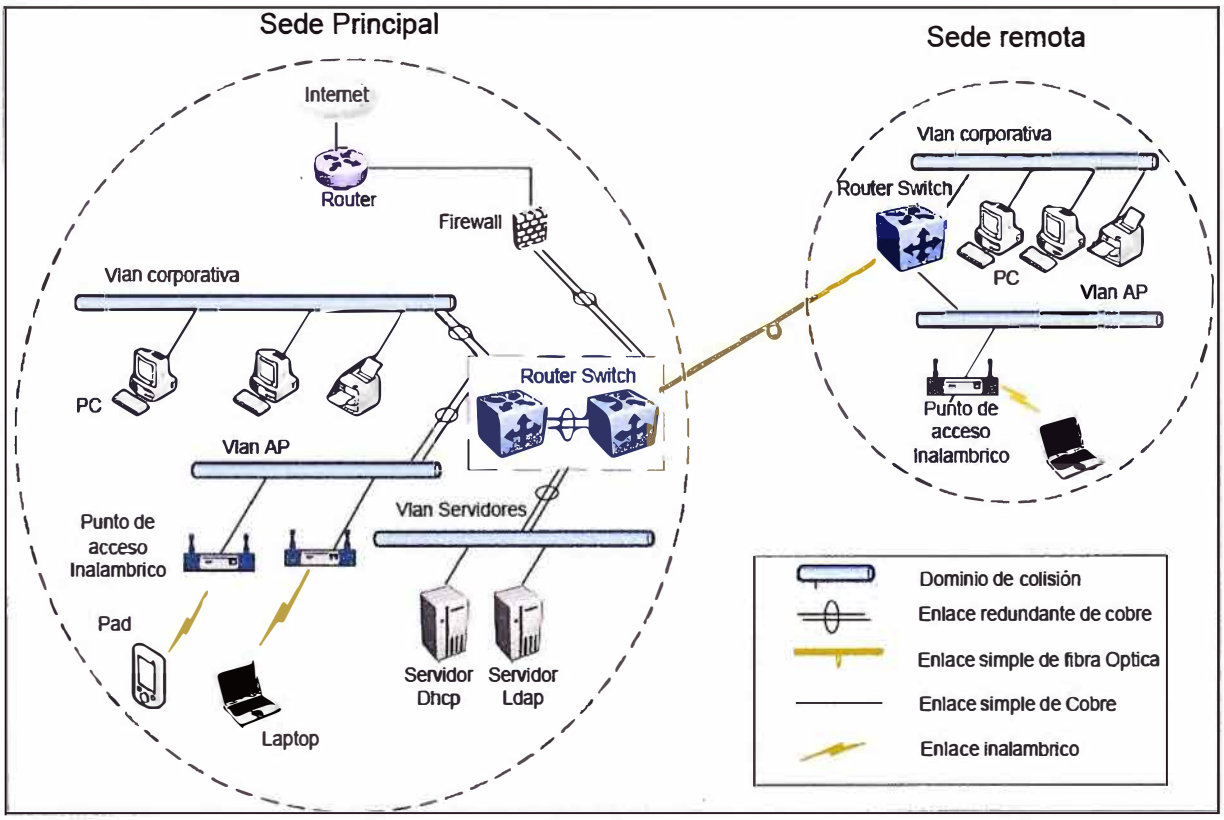

Figura 3.1 Esquema de red de Empresa Financiera previa a la solución implantada

La figura solamente incluye una oficina grande y una pequeña remota. En virtud de la claridad, sólo se muestran algunos servidores y clientes.

3.2.2 Requisitos de la organización

Los requisitos se aplicaran a la organización descrita en el escenario, se agrupan en a) Seguridad y b) Costos de implementación y administración:

a. Seguridad

La organización debe mejorar la seguridad de la WLAN para eliminar o reducir considerablemente las amenazas siguientes:

1) Intrusos que intercepten transmisiones de datos en la WLAN.
2) Intrusos que intercepten y modifiquen transmisiones de datos en la WLAN.
3) Intrusos u otros usuarios no autorizados que se conecten a la WLAN e introduzcan virus u otro tipo de código hostil en la red interna.
4) Ataques de denegación de servicio a nivel de la red (en lugar de a nivel de radio).
5) Intrusos que utilizan la WLAN corporativa para obtener acceso a Internet.

Las medidas de seguridad no deben tener un impacto negativo en la capacidad de uso de la red y no deben dar lugar a un incremento significativo de las llamadas al servicio de asistencia.

b. costos de implementación y administración

Deben ser lo suficientemente bajos como para ser justificables aunque solamente utilicen la solución de WLAN unos pocos usuarios (menos del 10% del personal).

El diseño debe ser compatible con gran variedad de clientes y dispositivos. Adicionalmente, suelen existir otros requisitos técnicos de naturaleza general:

1) Resistencia a errores de componente individual.
2) Posibilidad de escalabilidad para soportar niveles de uso superiores en el futuro, posiblemente de más del 100% del personal existente. El costo de la provisión de compatibilidad con números de usuarios cada vez mayores debería ser mínimo o, al menos, lo será en proporción a la ampliación requerida.
3) Posibilidad de reutilización de los componentes, siempre que sea posible. La solución debe reutilizar la infraestructura existente y los proyectos futuros deben poder reutilizar los nuevos componentes introducidos por la solución.
4) La infraestructura de administración y supervisión existente debería poder acomodar la nueva solución sin dificultad.
5) Capacidad de recuperación en caso de errores graves (por ejemplo, mediante la restauración de copias de seguridad en hardware alternativo).
6) Cumplimiento de los protocolos y formatos de los estándares del sector. Donde no existan normas actuales, la solución debería instaurarse según estándares futuros.
7) Seguridad sólida (incluyendo una renovación regular) de las credenciales y las claves utilizadas en la solución. Información de auditoría completa para la inscripción de usuarios y el acceso de clientes a la red.

c. Detalle de requerimientos

A partir de estos requisitos, pueden determinarse los criterios de compatibilidad con el

diseño de la solución en la Tabla 3.1.

Tabla 3.1 Compendio de requerimientos

Factor de diseño	Criterios
Seguridad	1) Autenticación sólida de los clientes inalámbricos. 2) Control de acceso que solamente permita el acceso de red a clientes autorizados. 3) Cifrado eficaz del tráfico de red inalámbrica. 4) Administración segura de las claves de cifrado. 5) Resistencia a ataques de denegación de servicio.
Escalabilidad	Diseño básico con escalabilidad ascendente y descendente para abarcar un amplio espectro de tamaños de organización
Número mínimo/máximo de usuarios admitidos	De 50 a 5000 (o más) usuarios de WLAN. (Esto se debe a que cada AP puede asociar hasta 50 usuarios, sin embargo es recomendable sólo 20 para un máximo desempeño)
Reutilización de componentes (uso de la infraestructura existente)	Utilización de Active Directory, servicios de red y clientes con Microsoft Windows® XP
Reutilización de componentes (capacidad de uso por parte de aplicaciones a futuras)	1) Compatibilidad con otras aplicaciones de acceso a la red (acceso a red por cable 802.1X y VPN) mediante la infraestructura de autenticación. 2) Compatibilidad con una amplia variedad de aplicaciones, como el sistema de archivos cifrados (EFS, Encrypting File System) y VPN, mediante PKI.
Disponibilidad	Resistencia a errores de componentes individuales o de vínculo de red.
Extensibilidad	1) Extensible para admitir capacidad y normas futuras (por ejemplo, 802.11n para WLAN). 2) Infraestructura de servicios de Certificate Server extensible para admitir la mayoría de los usos comunes de certificados de claves públicas (correo electrónico seguro, inicio de sesión con tarjeta inteligente, firma de código y Seguridad de servicio Web, entre otros).
Capacidad de administración	Integración con las soluciones de administración corporativa existentes (incluye la supervisión del sistema y del servicio, la creación de copias de seguridad, la administración de la configuración, etc.)
Estructura de la organización de TI	Favorece las TI centralizadas (departamento con un mínimo de cinco empleados y, normalmente, con 20 o 30 empleados de TI)
Cumplimiento de las normas	Cumplimiento de los principales estándares actuales y oferta de una ruta de migración clara a futuras normas importantes

3.2.3 Propuesta de diseño de la red

El diagrama de la Figura 3.1 muestra cómo se implementarán la WLAN, servidores físicos e Internet, cómo se vincularán y cómo se distribuirán entre los diferentes sitios de la empresa bancaria.

Es necesario recalcar que el número de servidores que se muestran en el diagrama de diseño de la red constituye una generalización.

Un diagrama con mayor detalle es mostrado en la Figura A.2 del Anexo A. Sin embargo en los siguientes ítems a) Sede Principal y b) Sede Remota, se muestra detalle de cada sede. Ambas sedes se encuentran enlazadas por fibra óptica.

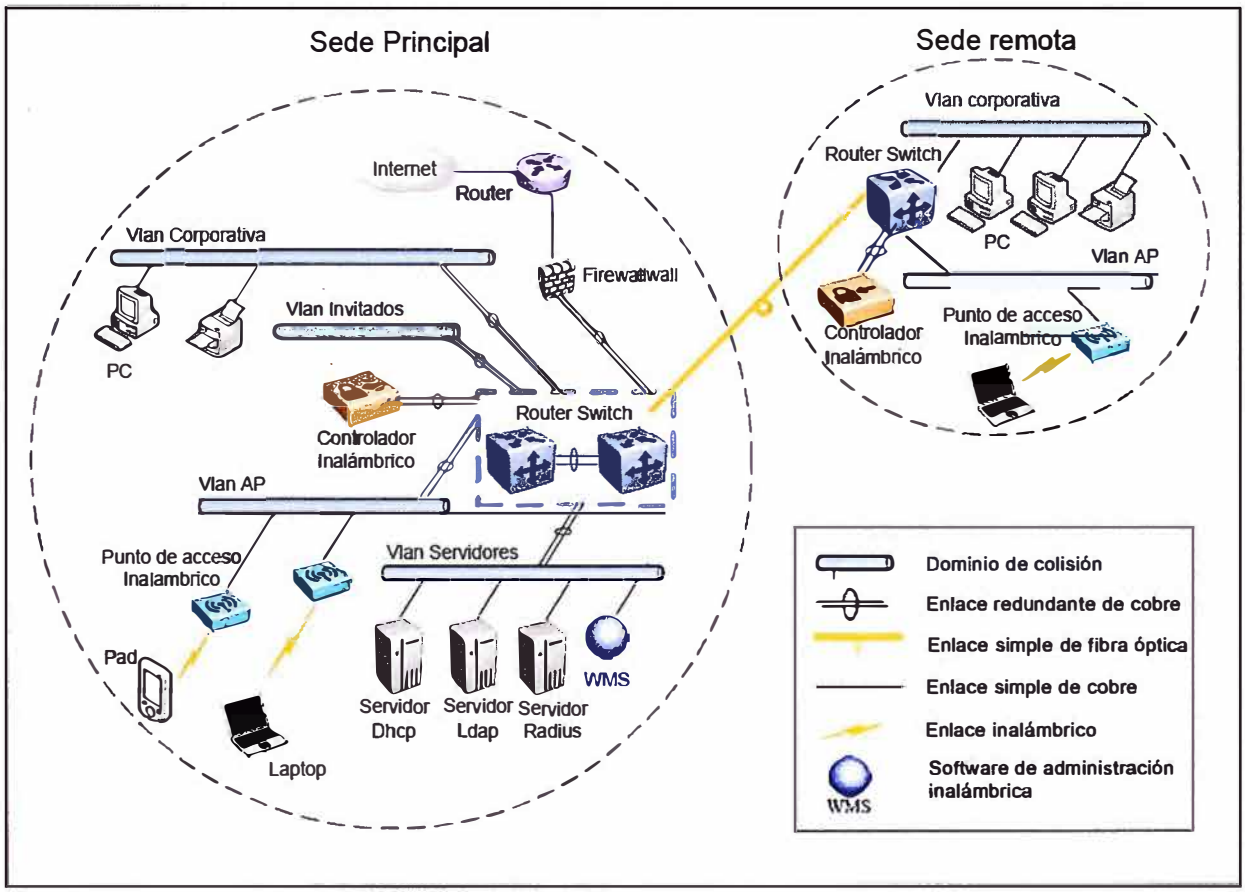

Figura 3.2 Esquema de red de luego de implantada la solución

a. Sede principal

La Figura 3.4 ilustra la implementación WLAN y servidores en la sede principal. Los componentes WLAN representan el componente nuevo: el controlador inalámbrico.

b. Sede Remota

La Figura 3.5 muestra lustra el diseño físico de una sede remota que se distingue por los servicios que son suministrados por la sede principal.

Bajo el marco de alta disponibilidad esta presente una controlador inalámbrico en dicha sede bajo el esquema de redundancia geográfica. La Figura 3.3 corresponde a la leyenda de los elementos mostrados en los diagramas

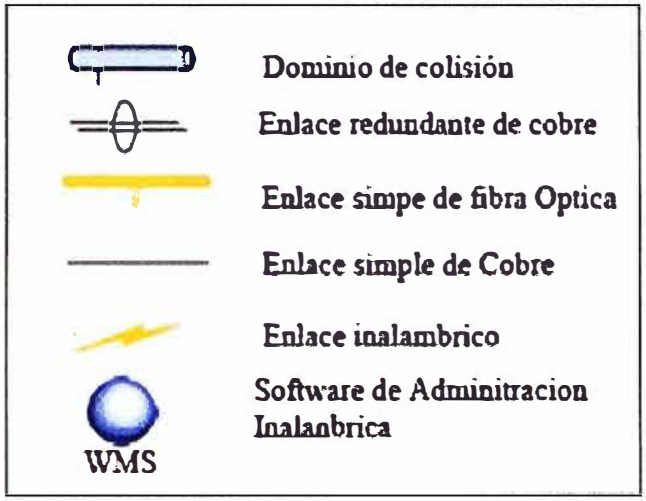

Figura 3.3 Leyenda

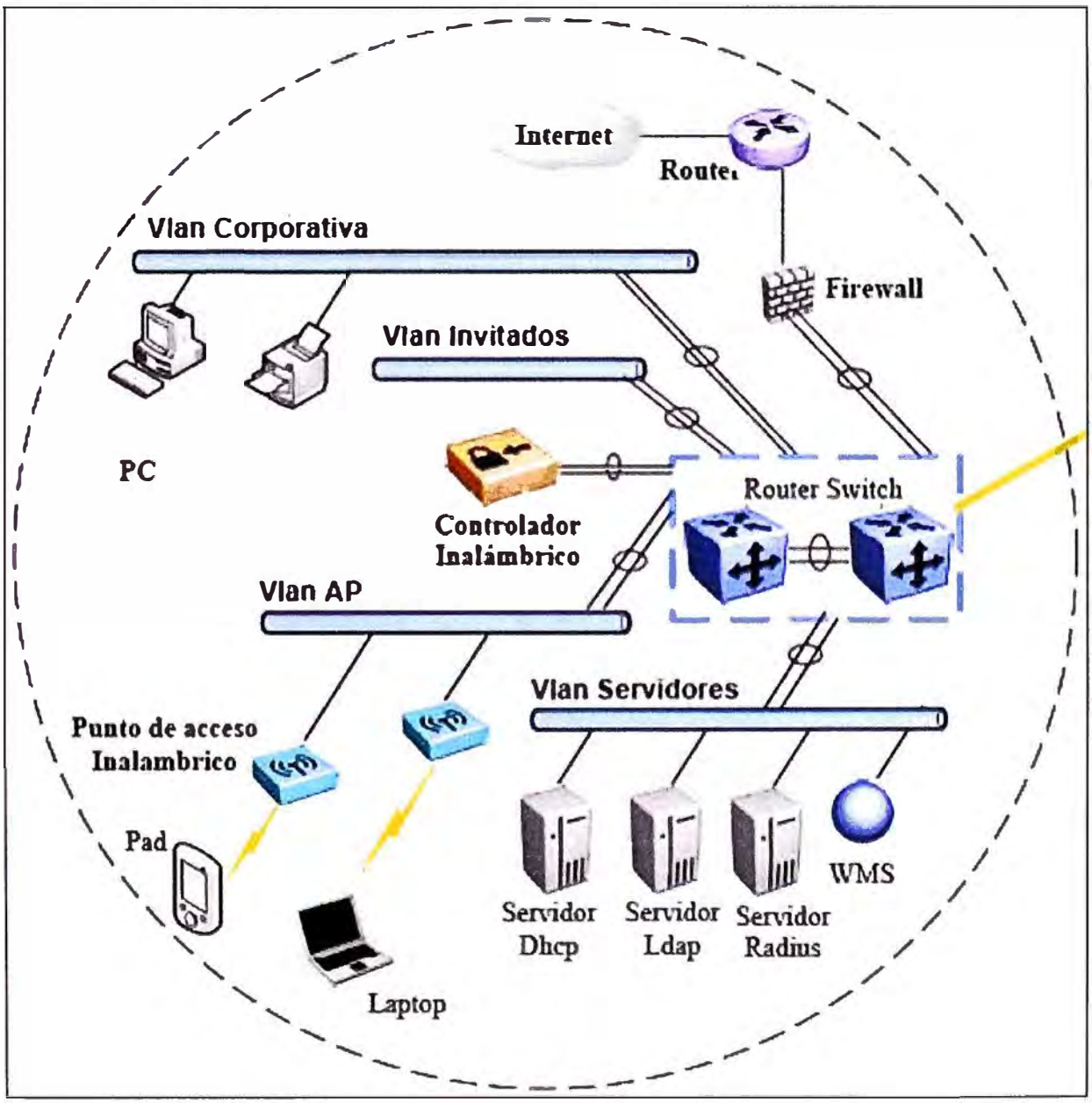

Figura 3.4 Sede Principal

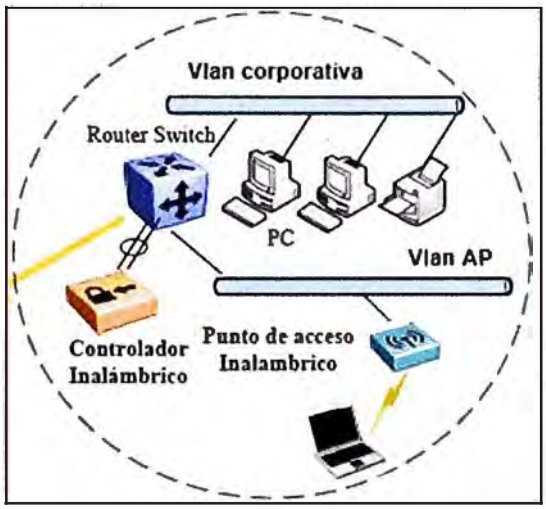

Figura 3.5 Sede Remota

3.2.4 Estrategia de escalabilidad

La solución es compatible con una amplia gama de tamaños de implementación a un costo apropiado para cada uno. Por ejemplo, una implementación para 500 usuarios debería costar proporcionalmente menos que una implementación para 5000 usuarios.

La complejidad de la implementación y administración también debe ser realista para esta gama de organizaciones. La Figura 3.6 muestra cómo puede escalarse el diseño en forma ascendente para abarcar una gran cantidad de usuarios en una sede principal y sedes remotas. La Figura A.3 del Anexo A la muestra en mayor detalle.

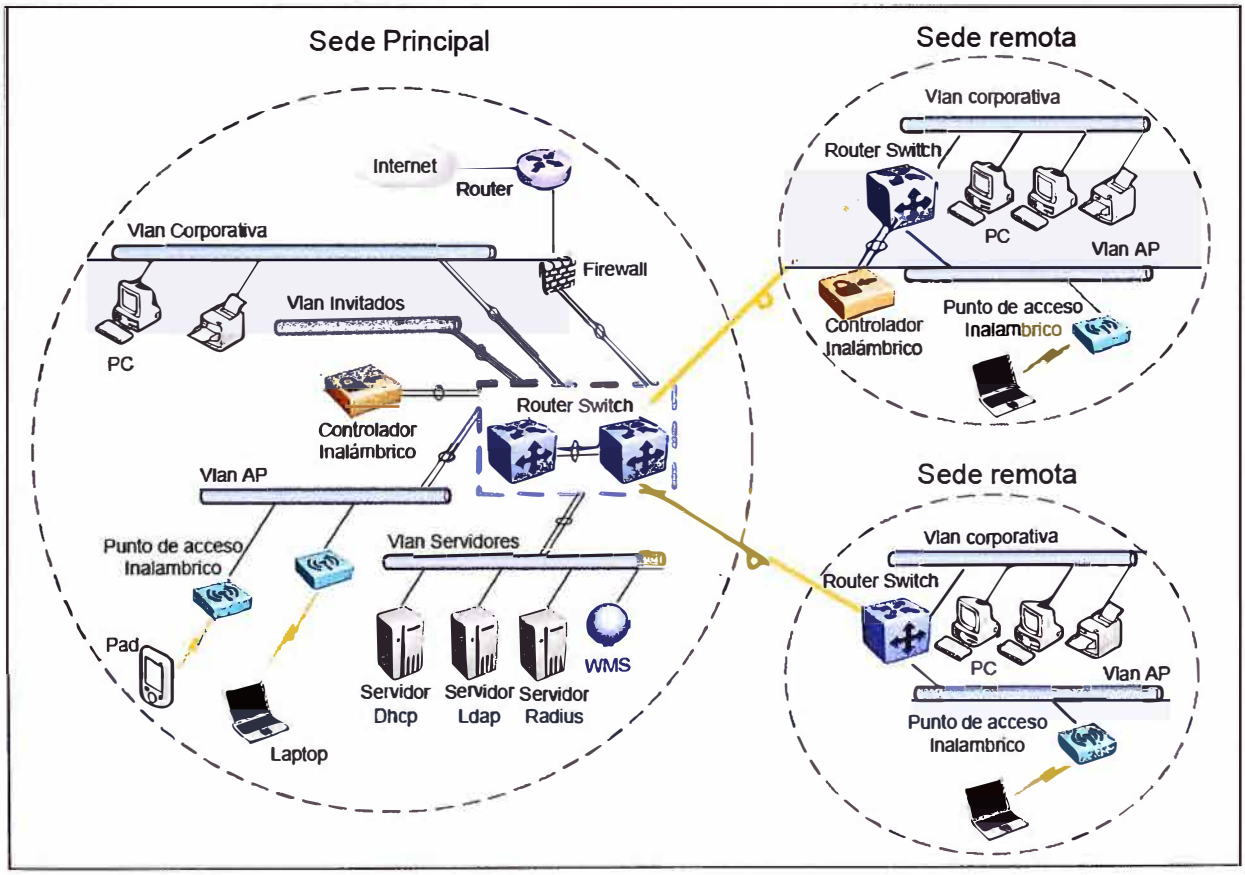

Figura 3.6 Escalabilidad del sistema

La reutilización de los componentes en aplicaciones futuras es un criterio clave en el diseño. Tanto los componentes como los servidores (DHCP, LPAD, RADIUS, WMS), controlador inalámbrico, pueden reutilizarse para proporcionar servicios para diversas aplicaciones.

El diseño de RADIUS utilizado en esta solución puede proporcionar autenticación, autorización y servicios contables para otros servidores de acceso a la red, como la autenticación de red por cable 802.1X y la autenticación de acceso remoto y VPN.

3.2.5 Reevaluación de los criterios de diseño

Resulta conveniente volver a examinar la lista de criterios para ver en qué grado el diseño propuesto cumple los objetivos establecidos anteriormente. Esta evaluación se resume en la lista a continuación.

1. Seguridad.- El diseño incluye servicios de autenticación, autorización y control de acceso sólidos. El cifrado de alta seguridad (de 128 bits) es una función del hardware de red compatible con la mayoría de los dispositivos disponibles actualmente. Se proporciona una administración segura de las claves de cifrado mediante la combinación del cliente 802.1X de Microsoft, el punto de acceso inalámbrico habilitado para 802.1X y las tarjetas de red inalámbrica y el servidor RADIUS.

El logro de una resistencia total a ataques de denegación de servicio constituye una tarea compleja; los estándares anteriores a 802.11i presentan vulnerabilidad a diversos ataques de este tipo.

2. Escalabilidad.- El diseño básico se ajusta a una gama de organizaciones con un costo asequible y una capacidad que oscila entre cientos y varios miles de usuarios. El diseño también es flexible en relación con el diseño geográfico y de red. Las oficinas pequeñas sin controlador de dominio local dependen de la fiabilidad de la WAN o de una solución de seguridad de menor calidad.

3. Reutilización de componentes (uso de la infraestructura existente).- El diseño utiliza el servicio de directorio de Active Directory y muchos servicios de red existentes, como el protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) y el sistema de nombres de dominio (DNS, Domain Name System).

4. Reutilización de componentes por parte de aplicaciones futuras.- El diseño de RADIUS, implementado mediante IAS (Servicio de autentificación de Internet, en ingles Internet Authentication Service), está listo para utilizarse o puede extenderse fácilmente para admitir otras aplicaciones de acceso a red (como VPN, acceso a red por cable 802.1X y acceso telefónico remoto).

De forma similar, la PKI (infraestructura de clave publica, en inglés, Public Key Infrastructure) es capaz de admitir aplicaciones sencillas de clave pública, como EFS

(Encrypting File System, sistema de archivos que, trabajando sobre NTFS, permite cifrado de archivos a nivel de sistema), y proporciona el entorno para aplicaciones más complejas, como el inicio de sesión con tarjeta inteligente. Este elemento también cumple el criterio de diseño de extensibilidad.

3.3 Arquitectura de la solución

En la presente sección se realizará una descripción de la arquitectura de la solución. En el capitulo anterior se explicó detalladamente los componentes necesarios para la solución. Los componentes clave son los siguientes: WLAN, DHCP, RADIUS y LDAP.

Los objetivos de esta sección son los siguientes:

1) Proporcionar una descripción conceptual del funcionamiento de una solución de WLAN segura, así como de los componentes principales de este tipo de solución.

2) Definir el diseño de la solución para el diseño lógico y las fases posteriores del diseño técnico detallado.

3) Producir un diseño lógico coherente que constituya la base para el diseño detallado

4) Explicar la forma en que puede modificarse la solución para cumplir los requisitos de organización de diferentes tamaños.

5) Explicar en detalle algunas de las formas en que puede ampliarse el diseño propuesto o utilizarlo como base para generar otras soluciones de acceso de red (por ejemplo, redes privadas virtuales control de acceso a redes por cable)

6) Examinar el proceso de diseño detallado para cada uno de los componentes principales del diseño lógico WLAN y Servidores como preparación para generar y poner la solución en funcionamiento.

3.3.1 Diseño conceptual

La solución necesita contar con las características siguientes:

1) Autenticación sólida de cliente inalámbrico. Esto debe incluir la autenticación mutua del cliente punto de acceso (PA) inalámbrico y el servidor RADIUS.

2) Un proceso de autorización para determinar quién tendrá o no tendrá acceso a la red inalámbrica

3) Control de acceso que solamente permita el acceso de residentes autorizados.

4) Cifrado eficaz del tráfico de la red inalámbrica.

5) Una administración segura de las claves de cifrado.

6) Una resistencia a los ataques de denegación de servicio (DoS).

3.3.2 Componentes principales

La Figura 3.7 muestra el diagrama conceptual de la solución con los elementos principales: a) El cliente inalámbrico, b) el AP, c) el AS y d) la red interna.

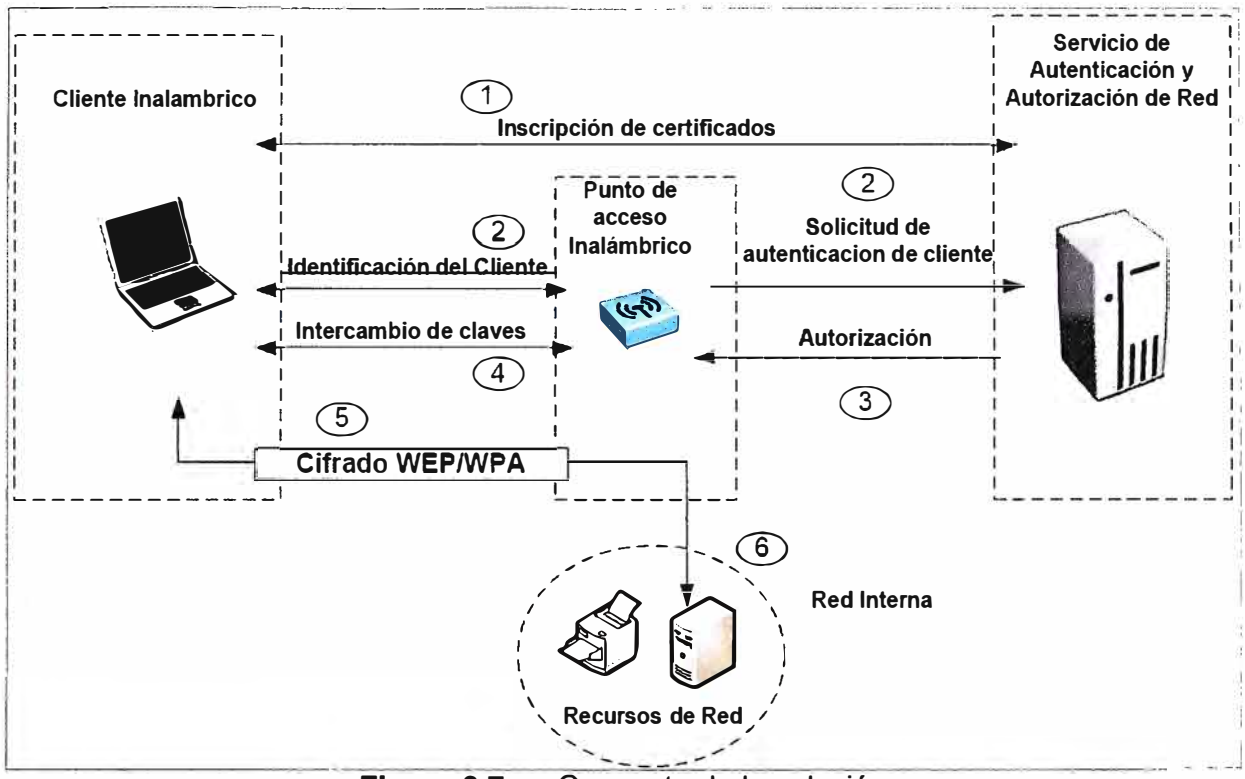

Figura 3.7 Concepto de la solución

a. El cliente inalámbrico

Se trata de un equipo o dispositivo que ejecuta una aplicación que requiere acceso a los recursos de red. El cliente tiene la capacidad de cifrar su tráfico de red, además ce guardar e intercambiar credenciales de manera segura (como claves o contraseñas).

b. El AP (Access Point)

O punto de acceso. En términos de redes más generales se conoce como "servicio de acceso a la red" (NAS, Network Access Service) pero en los estándares inalámbricos se hace referencia a este componente como "AP" o "punto de acceso".

El punto de acceso inalámbrico implementa funciones de control de acceso para permitir o denegar el acceso a la red y ofrece la capacidad de cifrar e tráfico inalámbrico. También cuenta con los medios para intercambiar claves de cifrado de manera segura con el cliente a fin de asegurar el tráfico de red. Finalmente, puede consultar un servido ce autenticación y autorización para tomar decisiones de autorización.

c. El AS (Authentication Service)

O servicio de autenticación. Guarda y comprueba las credenciales de los usuarios válidos y toma decisiones de autorización basándose en una directiva de acceso. También puede recopilar información contable y de auditoría sobre el acceso de los clientes a la red.

El servidor RADIUS es el componente principal de este servicio pero el directorio y la entidad emisora también contribuyen a esta función.

c. La red interna

Se trata de un área segura de servicios conectados a la red a los que la aplicación cliente inalámbrica debe obtener acceso.

3.3.3 Proceso de acceso a la red

Los números del diagrama de la Figura 3.8 ilustran el proceso de acceso a la red. El diagrama muestra los componentes individuales de forma más detallada. La Figura A.4 del Anexo A muestra el mismo diagrama en mayor escala.

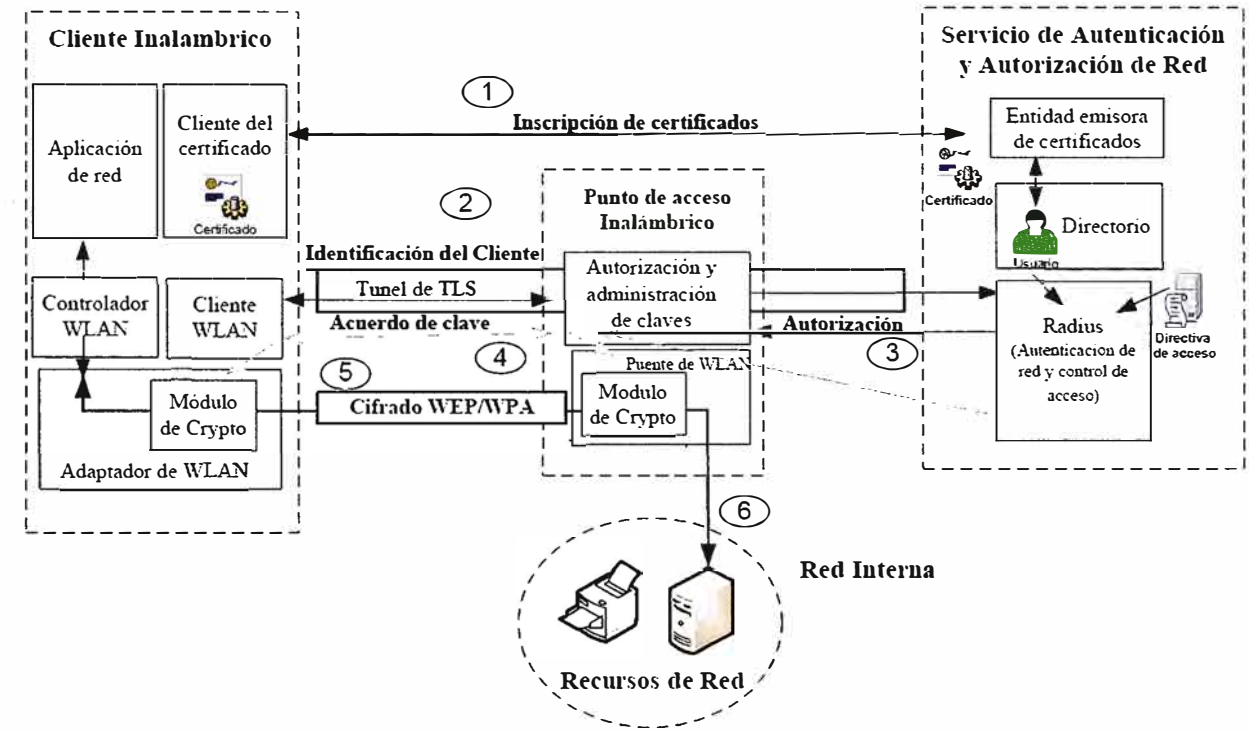

Figura 3.8 Arquitectura en detalle de la solución

Los pasos son los siguientes:

a. Paso 1

El cliente inalámbrico debe establecer credenciales con el servicio de autenticación antes de que se establezca el acceso a la red inalámbrica. (Esto podría realizarse con algunos medios fuera de banda como, por ejemplo, mediante un intercambio de disquetes, o bien podría realizarse en una red según por cable o de otro tipo.)

b. Paso 2

Cuando se encuentra al alcance del punto de acceso inalámbrico, el equipo cliente intenta conectarse a la WLAN activa en el punto de acceso. Para su identificación, la WLAN cuenta con un identificador del conjunto de servicios (SSID, Service Set Identifier). El cliente detecta el SSID de la WLAN y lo usa para determinar la configuración correcta y el tipo de credencial que debe utilizarse para esta WLAN específica.

El punto de acceso inalámbrico se configura para permitir únicamente conexiones seguras (autenticadas de 802.1X). Cuando el cliente intenta conectarse a

él, el punto de acceso envía un desafío al cliente. A continuación, el punto de acceso configura un canal restringido que permite cliente comunicarse sólo con el servidor RADIUS.

Este canal bloquea el acceso al resto de la red. El servidor RADIUS solamente aceptará una conexión de un punto de acceso inalámbrico de confiar o de uno que haya sido configurado como cliente RADIUS en el servicio de autenticación de Intranet (IAS, Internet Authentication Service) de Microsoft y que proporcione el secreto compartido para dicho cliente RADIUS.

El cliente intenta realizar la autenticación con el servidor RADIUS a través del canal restringido por medio de 802.1X. Como parte de la negociación EAP-TLS, el cliente establece una sesión de seguridad de la capa de transporte (TLS, Transport Layer Security) con el servidor RADIUS. El uso de una sesión de TLS tiene las finalidades siguientes:

1. Permitir al cliente llevar a cabo la autenticación del servidor RADIUS, lo que significa que el cliente solamente establecerá la sesión con un servidor que cuente con un certificado de confianza.
2. Permitir al cliente suministrar sus credenciales de certificado al servidor RADIUS.
3. Proteger el intercambio de autenticación frente a intrusiones contra paquetes.

La negociación de la sesión de TLS genera una clave que el cliente y el servidor RADIUS puede utilizar para establecer claves maestras comunes. Estas claves se usan para derivar las claves utilizadas en el cifrado de tráfico de WLAN.

Durante este intercambio, solamente el cliente y el servidor RADIUS pueden ver el tráfico en el túnel de TLS y no queda nunca expuesto al punto de acceso inalámbrico.

c. Paso 3

El servidor RADIUS valida las credenciales de cliente con el directorio. Si la autenticación del cliente se lleva a cabo de forma satisfactoria, el servidor RADIUS reunirá la información que le permitirá decidir si debe autorizarse el uso de la WLAN al cliente.

Utiliza información del directorio (por ejemplo, sobre la pertenencia a grupos) y las restricciones definidas en su directiva de acceso (por ejemplo, los períodos de tiempo en que se permite el acceso a la WLAN) para conceder o denegar el acceso del cliente. Seguidamente, el servidor RADIUS transmite la decisión al punto de acceso.

d. Paso 4

Si se concede acceso al cliente, RADIUS transmitirá la clave maestra del cliente al punto de acceso inalámbrico. Con ello, el cliente y el punto de acceso comparten información de clave común que pueden utilizar para cifrar y descifrar el tráfico de

WLAN que se desplaza entre ellos.

Cuando se utiliza WEP dinámica para cifrar el tráfico, las claves maestras deben cambiarse periódicamente para evitar ataques de recuperación de claves WEP. El servidor RADIUS realiza este proceso de forma regular, lo que obliga al cliente a repetir la autenticación y generar un conjunto de claves nuevo.

Si se utiliza WPA para proteger la comunicación, la información de la clave maestra se usa para derivar las claves de cifrado de datos, que cambian para cada paquete transmitido. WPA no necesita exigir la repetición frecuente de la autenticación para garantizar la seguridad de las claves.

e. Paso 5

A continuación, el punto de acceso establece la conexión de WLAN del cliente con la LAN interna, lo que ofrece al cliente un acceso sin restricciones a los sistemas de la red interna. Ahora, el tráfico transmitido entre el cliente y el punto de acceso está cifrado.

f. Paso 6

Si el cliente requiere una dirección IP, puede solicitar una concesión del protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) de un servidor en la LAN. Tras la asignación de la dirección IP, el cliente puede empezar a intercambiar información con los sistemas en el resto de la red de forma normal.

Nota:

Los subcomponentes del servicio de autenticación: la entidad emisora de certificados (CA), el directorio y el servidor RADIUS. Si bien conceptualmente estos subcomponentes llevan a cabo un conjunto de tareas relativamente simples, para hacerlo de manera segura, escalable administrable y fiable, necesitan una infraestructura auxiliar muy sofisticada.

3.4 Equipamiento utilizado

En esta sección se detallará al equipamiento (hardware y software) utilizado en el proyecto descrito: a) WLAN Access Point 2332, b) WLAN Security Switch 2382, c) WLAN Management Software 2300.

3.4.1 WLAN Access Point 2332

Los Switches de Seguridad 2300 WLAN ofrece varios modos de funcionamiento 802.11 a / b / g de servicios móviles para los clientes móviles. El 2332 está diseñado para despliegues densos y ofrece una conectividad de alto rendimiento móvil sin sacrificar la seguridad o la gestión. El 2332 es adecuado para las instalaciones en cielo raso y cuenta con una atractiva carcasa que se asemeja a un detector de humo común para mezclarse con los entornos de oficina. Ver Figura 3.9

a. Funcionalidades claves

Son las siguientes

1. Backhaul inalámbrico y puentes (bridging)

2. Reenvío de trafico local
3. Auto configuración
4. Puertos Ethernet dual-homed para el servicio de resistencia o auto recuperación
5. Continuo RF de escaneo para detectar actividad no autorizada
6. Priorización de voz y multimedia
7. Cifrado basado en Hardware
8. 802.3af PoE
9. Antenas Externas opcionales
10. WMM/802.11e QoS
11. Seguridad WEP/WPA/WPA2/802.11i

Figura 3.9 WLAN Access Point 2332

b. Especificaciones técnicas generales

Posee modo de ahorro de energía, transmisión de control de potencia en incrementos de 1 dB, hasta 32 SSID por radio. A continuación se especifican las características técnicas para la irradiación 802.11a, 802.11b, 802.11g:

b.1 Radio 802.11a

1. Banda de frecuencia: 5,15 a 5,25 GHz, 5,25 a 5,35 GHz, 5,470 a 5,725 GHz y 5,725 a 5,85 GHz, el funcionamiento de los canales es basado en las regulaciones de cada país. Las tasas son de 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 y 6 Mbps, con recuperación automática.
2. Modulación: Orthogonal Frequency Division Multiplexing (OFDM)
3. Potencia de transmisión: Se basa en el país de operación especificada por el administrador del sistema.
4. Tipo de antena: Omnidireccional integrado con (2) elementos radiantes para permitir así la utilización de la diversidad.
5. Ganancia de antena interna: Son las siguientes: a) 5,15 a 5,25 GHz pico = 3,18 dBi, b) 5,25 a 5,35 GHz pico = 2,83 dBi, c) 5,470 a 5,725 GHz pico = 2,50 dBi, d) 5,725 a 5,850 GHz pico = 2,44 dBi

b.2 Radio 802.11b

1. Banda de frecuencia: 2,4 GHz a 2,4835 GHz basado en las regulaciones de cada país.
2. Canales de funcionamiento: Es especificado por el administrador del sistema basado en las regulaciones de cada país.
3. Asociación de las tasas: 11 Mbps, 5,5 Mbps, 2 Mbps y 1 Mbps, con recuperación automática.
4. Modulación: BPSK, QPSK, CCK
5. Potencia de transmisión: Es especificado por el administrador del sistema basado en las regulaciones de cada país
6. Tipo de antena: omnidireccional integrado con (2) elementos radiantes para permitir asi la utilización de la diversidad.
7. Ganancia de antena interna: 3,86 dBi pico (azimut) y 2,48 dBi pico (elevación).

b.3 Radio 802.11g

1. Banda de frecuencia: 2,4 GHz a 2,4835 GHz es basado en las regulaciones de cada país.
2. Canales de funcionamiento: Es especificado por el administrador del sistema basado en las regulaciones de cada país.
3. Asociación de las tasas: 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 y 6 Mbps, con recuperación automática
4. Modulación: Orthogonal Frequency Division Multiplexing (OFDM)
5. Potencia de transmisión: Es especificado por el administrador del sistema basado en las regulaciones de cada país
6. Tipo de antena: omnidireccional integrado con (2) elementos radiantes para permitir la utilización de la diversidad.
7. Ganancia de antena interna: 3,86 dBi pico (azimut) y 2,48 dBi pico (elevación).

c. Especificaciones técnicas complementarias

c.1 Dimensiones y condiciones ambientales:

1. Tamaño Diámetro: 16,76 cm (6,6 pulgadas), Altura: 6,1 cm (2,4 pulgadas) y
2. Peso sin el soporte de montaje: 0,45 kg (16 onzas.
3. Peso con el soporte de montaje: 0,5 kg (17,5 onzas)
4. Temperatura de funcionamiento: 0 ° C a +50 ° C (32 ° F a 122 ° F)
5. Temperatura de almacenamiento: -20 ° C a +70 ° C (-4 ° F a 158 ° F)
6. Humedad: 10% a 95% sin condensación
7. Power over Ethernet (PoE): 42 VDC a 57 VDC (46 VDC nominal) IEEE 802.3af.

8. Indicadores de estado: Salud / LED WSS y radio

9. Puertos de red con conexión de cable: Dos puertos RJ-45 para Ethernet 10/100BASE-T y Power over Ethernet (PoE)

c.2 Cumplimiento de estándares

Soporta los estándares a) IEEE 802.11, b) IEEE 802.11a, c) IEEE 802.11b, d) IEEE 802.11g, IEEE 802.3af.

c.3 Seguridad y electromagnética

Se rige de acuerdo a los siguientes estándares:

a) FCC Part 15, UL 60950
b) IC Part 15, CSA 22.2 N0-950, RSS-139-1 and RSS-210
c) ETS 300-328 (2.4 GHz) and 301-893 (5 GHz), EN 301-489-17
d) R&TTE Directive 1999/5/EC
e) TELEC, ARIB T66
f) GBT-15941-1995, GBT-16841-1997
g) LP0002

c.4 Encriptación

Soporta las siguientes técnicas:

a) Wi-Fi Protected Access (WPA)
b) Estándar de cifrado avanzado (AES)
c) Privacidad 40-bit/104-bit Wired-Equivalent (WEP)

3.4.2 WLAN Security Switch 2382

El conmutador de seguridad WLAN 2382 proporciona el control, gestión y seguridad de hasta 128 puntos de acceso distribuidos y está diseñado para instalaciones centralizadas.

Figura 3.10 WLAN Security Switch 2382

a. Características y beneficios

Se agrupan en:

1) Rendimiento y recuperación del servicio y 2) Administración y seguridad

a.1 Rendimiento y recuperación

Diseñado para aplicaciones de voz y multimedia

1. QoS: Soporta WMM, SVP, 802.1p / DiffServ para voz y priorización de tráfico multimedia. SpectraLink VER certificados.
2. Roaming: Permite movilidad de los usuarios entre todos los puntos de acceso, incluidas las controladas por otros conmutadores WLAN de Seguridad.
3. Rápido Roaming: la información de autentificación de usuarios y las políticas asociadas, son compartidas con otros de la serie 2300, permitiendo así minimizar el retardo y jitter.
4. Administración Multicast: Soporta IGMP v1/v2 y miembros multicast contribuyendo para un alto rendimiento en los servicios inalámbricos Multicast.
5. Balanceo de carga de usuarios: Continuamente monitorea la carga de usuarios y automáticamente redirige a los usuarios nuevos a puntos de acceso alternativos para ofrecer un mejor rendimiento posible.
6. Administración dinámica de RF: óptimo calculo de las asignaciones de canales de radio 802,11 y los niveles de potencia de transmisión para todos los puntos de acceso asociados y se adapta a la carga de usuarios, interferencias, obstáculos y ataques de RF.
7. Diseño de Recuperación: fuentes de alimentación duales (WLAN conmutador de seguridad 2361/2380/2382), enlaces redundantes, opciones de arquitectura activo - pasivo, carga equilibrada AAA, backup de configuraciones elimina puntos de falla.
8. Compatibilidad VPN y Firewall: Para las implementaciones de sucursal, el WSS proporciona un control local de los puntos de acceso y no requiere ninguna nueva configuración de los routers WAN, gateways VPN o cortafuegos.

a.2 Administración y seguridad para las implementaciones a gran escala

1. Administración centralizada: Proporciona seguridad de red, QoS, gestión de RF y roaming para los puntos de acceso WLAN de la serie 2300.
2. Topología flexible: WLAN Security Switches pueden ser instalado en el armario de cableado, o en data centers. Los puntos de acceso se conectan en los switches L2 o L3.
3. Power over Ethernet: Cumple con el estándar 802.3af para proporciona energía a puntos de acceso conectados directamente al switch.
4. Las últimas normas de seguridad: Soporta estándares tales como WPA, WPA2, 802.11i/802.1x con WEP, Dynamic WEP, TKIP, CCMP, EAP-TLS, TTLS y PEAP, PEAP-TLS.
5. Políticas basadas en el usuario: Hace cumplir políticas de seguridad y QoS basado en un usuario o en grupo, no en el dispositivo, punto de acceso inicial o puerto físico.
6. Grupos de servicios virtuales: Puede soportar hasta 32 dominios de servicios independientes sobre una única infraestructura. Cada grupo de servicio puede tener su propia VLAN, subred, servidor AAA (s), la seguridad y las políticas de QoS.

7. Portales: Cada grupo de servicios virtuales puede ser asignado su propio portal de autenticación esto puede ser personalizado con mensajes únicos o anuncios.
8. Acceso a Invitados: Un personal de recepción tiene la capacidad de emitir rápidamente ID´s a invitados temporales.
9. Administración AAA: Puede cumplir múltiples opciones de autenticación basado en la dirección MAC Cliente, 802.1X o basado en autenticación Web con base local o RADIUS AAA.
10. Plug 'n Play: Reconoce nuevos puntos de acceso y de forma dinámica los incorpora al sistema WLAN.
11. Soporte AP 3 ª Party: Extiende muchos de los beneficios de la WLAN 2300 series de puntos de acceso existentes, incluyendo políticas de administración basada en usuario, rápido roaming.
12. Supervisión y Presentación de Informes: Proporciona estadísticas detalladas sobre RF y la actividad del usuario.
13. Protección contra rogue´s: Además de identificar, clasificar y localizar APs no autorizados, el sistema de WLAN 2300 puede avisar a los administradores, supervisar la actividad de puntos de acceso e incluso contener la amenaza frente a un ataque RF de los puntos de acceso vecinos.
14. Protección contra amenazas inalámbricas: Identifica los ataques de RF, las estimaciones de localización y alerta a los administradores.
15. WIDPS: (Wireless Intrusion Detection and Prevention System). Sistema de detección y prevención de intrusos. Utiliza el AirDefense Integration ® para un mejor escaneo, detección y prevención.

b. Especificaciones técnicas

La tabla 3.2 muestra las especificaciones técnicas del WLAN Security Switch 2382.

3.4.3 WLAN Management Software 2300

El sistema de gestión de Nortel WLAN Software es un instrumento de gestión para la WLAN 2300 de la serie que identifica lugares ideales para los puntos de acceso en los planos, configura todos los dispositivos con un solo clic y proporciona un control granular e informes para una completa visibilidad y control sobre toda la del sistema.

a. Funcionalidades

Sus funcionalidades clave son:

1. Un conjunto de herramientas integradas para la pre y post planificación a la implementación, configuración de todo el sistema y actualizaciones, monitoreo y presentación de informes.
2. Se ejecuta en las plataformas de servidores comunes, incluyendo Windows 2000,

Windows XP y Linux.

3. Permite a los administradores que puedan realizar actualizaciones de todo el sistema y "ver" lo que está pasando a través de una interfaz gráfica.

4. Seguimiento y presentación de informes personalizables, proporciona todo lo necesario para manejar la solución de problemas.

5. Acepta múltiples niveles de acceso de administrador.

Tabla 3.2 Especificaciones técnicas

Item	Valores
Tamaño	Ancho: 44,2 cm (17,4 pulgadas) Profundidad: 30,7 cm (12,1 pulgadas) Altura: 4,4 cm (1,72 pulgadas)
Peso	Con suministros twpower: 4,99 kg (11,0 libras)
Temperatura de funcionamiento	0 ° C +50 ° C t (32 ° F t +122 ° F)
Temperatura de almacenamiento	-20 ° C +70 ° C t (-4 ° F t +158 ° F)
Humedad:	10% t95% sin condensación
Fuente de alimentación (cada uno):	150-240 AC ~ 50 Hz Hz t60 1 Armas en 120 AC ~ y Armas 0,51 a 230 AC ~ 17 A máx. en el 120 AC ~ y 32 A máx. en 230 AC ~
Indicadores de estado:	Estado de la gestión de la CPU LED LEDs de estado de suministro de energía La actividad de los puertos y LED de velocidad
Puertos de red:	Convertidor de interfaz gigabit (mini-GBIC) ranuras para 1000BASE-SX, 1000BASE-LX, o 1000BASE-TX Ethernet gigabit puertos Un puerto RJ-45 para Ethernet 10/100BASE-T (sin PoE) utilizado para administración del sistema.

b. Características y beneficios

Las características y beneficios se agrupan de la siguiente manera y son los siguientes:

b.1 Planificación y Diseño

1. Importa planos existentes en AutoCAD DXF ™, AutoCAD DWG, JPEG o GIF.

2. Incluye una biblioteca de las características de atenuación de RF para puertas, columnas, paredes, techos y otros obstáculos físicos.

3. Calcula el número ideal, la colocación y la configuración de puntos de acceso basados en los requisitos de capacidad y las características de RF.

4. Genera un detallado mapa que muestra la cobertura calculada.

5. Crea una lista de materiales, incluidos los puntos de acceso, switches y hasta

tendidos de cable.

6. Puede ser utilizado como una herramienta independiente para analizar los efectos de escenarios hipotéticos.

7. Puede importar datos de RF para una mayor precisión en el patrón de RF.

b.2 Configuración

1. Calcula WLAN topología, la colocación de puntos de acceso y configuraciones incluyendo el nivel de potencia y canal.

2. Proporciona todo el sistema de configuración y las actualizaciones en un solo paso.

3. Verifica los cambios del sistema con un motor de reglas y archivos con figuraciones pasadas.

4. Avisos a los administradores sobre los cambios conflictivos en la configuración.

5. Compatible con SNMP v3 y HP OpenView plug-in.

b.3 Supervisión y Presentación de Informes

1. Detecta y ubica APs no autorizados, usuarios y agujeros de cobertura.

2. Proporcionar información sobre la ubicación de usuarios, la tasa de ancho de banda, historial y estadísticas de uso.

3. Todas las estadísticas del sistema se pueden exportar en tablas y gráficos.

c. Requisitos de hardware para Windows y Linux

1. Procesador: Mínimo: Intel Pentium 4, 2 GHz o equivalente, Recomendado: Intel Pentium 4, 3,6 GHz o equivalente
2. RAM: Mínimo: 1 GB, Recomendado: 2 GB
3. Espacio en disco duro: Mínimo: 1 GB, Recomendado: 2 GB
4. Resolución del monitor: mínima: 1024 x 768 píxeles, 24-bit de color; Recomendado: 1600 x 1200 píxeles, color 32-bit

d. Requisitos de software para Windows y Linux

1. Plataforma de Windows: Microsoft Windows Server 2003, Windows XP (SP1) o Windows 2000 (SP4)
2. Plataforma Linux: Linex SUSE 9.1, Red Hat WS 3

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

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

En el presente capítulo se detallan los aspectos relacionados a los costos y al cronograma del sistema implementado.

4.1 Estimación de costos

En la estimación de costos sólo se considera al equipamiento utilizado en el sistema y es mostrado en detalle en la Tabla 4.1.

4.1.1 Elementos no considerados en la estructura de costos

No son considerados dentro de la estructura de costos lo descrito en los aspectos que se describen a continuación:

a. El servidor en donde reside el WMS

Es un equipo de cómputo provisto por la entidad bancaria.

b. El costo de la instalación y puesta en operación

Es parte de la propuesta técnico económico que sólo es manejada por el departamento de ventas de la entidad proveedora de la solución y que es considerada confidencial por la entidad bancaria.

c. El costo de capacitación del personal técnico

Que contribuya con la sostenibilidad de esta solución.- También es parte de la propuesta técnico económica, pero esta capacitación se brindó solamente a un grupo de cinco personas del departamento IT de la entidad bancaria, los que luego se encargaron de capacitar a todo su personal

4.1.2 Elementos considerados en la estructura de costos

Las características de los elementos considerados en el presupuesto son mostradas en la Tabla 4.2.

4.2 Cronograma de tareas

La Tabla 4.3 muestra el cronograma de tareas realizadas para la implementación del proyecto. El diagrama de Gantt correspondiente, dado su tamaño y detalle, es mostrado en el Anexo B “Diagrama de Gantt”.

Nota:
Con el propósito de hacer más didáctico el documento, se han reunido las Tablas mencionadas (Tabla 4.1 , 4.2 y 4.3), en las siguientes páginas.

Tabla 4.1 Presupuesto

Qty	Código de Parte	Detalle	Precio Unitario	Precio total
2	DR4001E80E5	**W**LAN **Security S**witch 2382 - 2 Gigabit SFP ports,	$7,733	$15,466
96	DR4001095 E6	**W**LAN **A**ccess **P**oint 2332 - 802.11a/b/g.	$357	$34,272
6	DR4011020-6.0.0	Licencias de software WLAN 2382 para 32 APs adicionales	$3,567	$21,402
4	AA1419043-E6	Tranceiver 1-port 1000Base-T SFP (Small Form Pluggable)	$210	$840
96	DR4005E08 E6	Inyector de energía Single-port 802.3af PoE para ser usado con WLAN 2300.	$90	$8,640
1	DR4011017-7.0	Programa de administración inalámbrica. **WMS**	$9,518	$9,518
			TOTAL	$90,138

Tabla 4.1 Presupuesto

ITEM	Características
El WSS o WLAN Security Switch 2382 - 2 Gigabit SFP ports	-Soporte 32 APs (por defecto), -Puede soportar hasta 128 APs – pero mediante licencia comprada aparte. -Posee dos fuentes de alimentación (DUAL PSU)
El WLAN Access Point 2332 - 802.11a/b/g (usado con el WSS serie 2300 y V.6.0 o superiores).	-Radios duales -PoE ETH Port dual, -Doble banda con diversidad de antena, 2 antenas R-SMA, tipo conector para extensión. (E4) - Licencias de software WLAN 2382 para 32 APs adicionales -Además múltiples licencias de actualización pueden ser usadas para el WSS 2382 hasta un máximo de 128 APs.
Licencias de software WLAN 2382 para 32 APs adicionales	Múltiples licencias de actualización pueden ser usadas para el WSS 2382 hasta un máximo de 128 APs. La licencia es aplicable al software del 2382 versión 6.0 o superior
Elementos complementarios	Tranceiver 1-port 1000Base-T SFP (Small Form Pluggable). Conector modular de 8-pins (RJ-45) Inyector de energía Single-port 802.3af PoE para ser usado con WLAN 2300. Programa de administración inalámbrica. WMS (Wireless Management Software) actualización Rel 7.0 – AC. Puede administrar desde 50 hasta 1000 APs

Tabla 4.2 Cronograma de tareas

Nombre de Tarea	Tiempo	Comienza	Fin
Proyecto banco.	21 días	01/07/2009 09:00	27/07/2009 19:00
Planificación.	3 días	01/07/2009 09:00	03/07/2009 19:00
Designación de responsables	0.25 días	01/07/2009 09:00	01/07/2009 11:00
Recopilación de información de aps(s/n & rsa)	1 día	02/07/2009 09:00	02/07/2009 19:00
Recopilación de información técnica	2 días	02/07/2009 09:00	03/07/2009 19:00
Entrega de equipos	1 día	03/07/2009 09:00	03/07/2009 19:00
Entrega de diseño de ubicación de ap´s	1 día	03/07/2009 09:00	03/07/2009 19:00
Wireless LAN.	7 días	06/07/2009 09:00	14/07/2009 19:00
Configuración de security switchs 2382	5 días	06/07/2009 09:00	10/07/2009 19:00
Pruebas de funcionalidad	2 días	13/07/2009 09:00	14/07/2009 19:00
LAN switching.	7 días	13/07/2009 09:00	20/07/2009 19:00
Configuración de VLANS	1 día	13/07/2009 09:00	13/07/2009 19:00
Configuración de trunk a wss 2382	1 día	13/07/2009 09:00	13/07/2009 19:00
Montaje de security switch 2382	2 días	18/07/2009 09:00	20/07/2009 19:00
Enlace - core a passport 8600.	1 día	17/07/2009 09:00	17/07/2009 19:00
Configuración de enlace a wss 2382	1 día	17/07/2009 09:00	17/07/2009 19:00
Despliegue/montaje de antenas indoor	17 días	04/07/2009 09:00	24/07/2009 19:00
Cableado TORRE	6 días	04/07/2009 09:00	12/07/2009 19:00
Sede principal	4 días	13/07/2009 09:00	16/07/2009 19:00
Cableado SEDE REMOTA	2 días	13/07/2009 09:00	14/07/2009 19:00
Sede remota	2 días	17/07/2009 09:00	18/07/2009 19:00
Herramientas de administración	1 día	16/07/2009 09:00	16/07/2009 19:00
Instalación/configuración del wms & integración con la red	1 día	16/07/2009 09:00	16/07/2009 19:00
Protocolo de pruebas.	1 día	27/07/2009 09:00	27/07/2009 19:00
Pruebas de funcionalidad entre wss 2382	1 día	27/07/2009 09:00	27/07/2009 19:00

Nota:
En el siguiente capítulo se presentan las conclusiones y recomendaciones relacionadas con presente trabajo.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La plataforma de acceso inalámbrico WiFi (802.11) implementada en la entidad bancaria ha demostrado desde su implantación un alto desempeño y alta disponibilidad brindando los niveles de seguridad de información requeridas para los empleados y usuarios foráneos.

2. Durante las pruebas de contingencia realizadas antes y durante la implantación de la solución (forzando la falla de uno de los controladores), la respuesta del controlador restante ha sido sumamente eficiente y rápida no habiéndose generado falla alguna en las comunicaciones de los usuarios.

3. El sistema diseñado para 96 puertos de accesos puede ser capaz de servir hasta 128 APs. Se dejaron habilitados 70 APs quedando los restantes para aspectos de escalabilidad y de respaldo.

4. La mayoría de los avances tecnológicos, las redes inalámbricas presentan ambas, oportunidades y riesgos a los usuarios y administradores. Esta tecnología puede ser un agregado útil para la infraestructura existente de la entidad bancaria ya que ofrece acceso de red a alta velocidad ayudando a ahorrar tiempo, costos, el trabajo de cablear la red y mecanismos de seguridad para prevenir que la red sea atacada.

5. Debido a la gran cantidad de información relacionada con las redes inalámbricas y puesto que es inverosímil abarcar todas sus áreas, así como estándares y profundizar en cada una de ellos, en este trabajo fueron expuestos sus conceptos básicos y fundamentos, para de esta manera cumplir con el objetivo del presente proyecto, que es el brindar un aporte que permita familiarizarse con este tipo de redes, su diseño, y los beneficios que aportan.

6. El sistema de red actual, enfrenta un problema con respecto a la movilidad de usuarios, y escalabilidad. La posible integración de nuevos usuarios, y las cambiantes necesidades departamentales, que eventualmente modifican la ubicación física de los empleados, podrían generar un gran problema en la creación de nuevos puntos de red, o movimiento de los mismos. Además, ante un cambio de sede, todos los cables y conexiones no podrán ser utilizados en la nueva oficina, con lo que la inversión realizada

no se recuperará. Sin embargo, todos los dispositivos que conforman una red inalámbrica pueden ser trasladados sin ningún tipo de problema, por lo que no volverá a tener que realizar ese gasto. El diseño expuesto, supera todas estas limitaciones, brindando escalabilidad, movilidad y asegurando la inversión.

7. Para el diseño se consideró las diferentes aplicaciones que utilizarán los usuarios de la red, basados en estadísticas del ancho de banda requerido por cada aplicación, con base en estos resultados, se concluye que al utilizar 802.11g, el ancho de banda supera lo necesario y se está garantizando un correcto desempeño de la red, y de las aplicaciones que sobre esta correrán.

8. En el tema legal, puesto que se trata de un proyecto para uso interno y exclusivo para la entidad bancaria, los equipos inalámbricos utilizados consumen potencias menores a 100 mw que no dañan la salud. Las frecuencias empleadas de la banda de 2.4Ghz no requieren licitación según por el MTC por lo tanto no será necesario realizar algún tramite con el MTC y ni con el municipio del distrito.

9. Se realizó un análisis de diferentes tipos de equipos existentes en el mercado y se procedió a la elección de la mejor alternativa tomando en cuenta aspectos técnicos y económicos, para lo cual se comparó sus características técnicas y se realizó un análisis de los precios del mercado actual y el costo que presenta el proyecto, optando con la mejor alternativa la Solución WLAN Nortel Corp.

10. Finalmente se concluye que el presente proyecto se perfila como una solución que se ajusta perfectamente a la realidad de nuestro medio, brindando soluciones con costos de inversión admisibles, satisfaciendo a los usuarios y permitiéndose a la entidad financiera en la medida de lo posible, ir a la par de los desafíos que representan los nuevos y sofisticados servicios de transporte de información.

Recomendaciones

1. Que el personal IT de la entidad bancaria realice periódicamente (cada cuatro meses) pruebas de contingencia a efectos de determinar aquellos elementos que puedan estar causan un bajo desempeño o riesgos de seguridad en la red Wireless.

2. Que el personal IT de la entidad bancaria realice efectúe la detección de “Zonas Oscuras”, ya sea por interferencia de otros emisores, o por la ubicación de nuevos obstáculos (cuando haya habido cambios en la infraestructura del edificio o de nuevos equipos de similar frecuencia).

3. Que el personal de soporte IT se mantenga capacitado y entrenado para las labores de soporte y reparación de eventualidades en la plataforma de acceso inalámbrico de alta disponibilidad.

4. Para los usuarios que necesiten instalar software se deben establecer políticas para definir los tipos de software permitidos, y las reglas que deben cumplir en cuanto a licencias. Además se debe planificar un intervalo de tiempo para la realización del mantenimiento del software de las estaciones de trabajo, con el fin de mantener los equipos libres de virus y espías informáticos (cada seis meses).

5. Es recomendable que el personal IT capacite periódicamente al personal de la entidad bancaria en cuanto a las políticas de seguridad por cuanto no es parte de la solución desarrollada (cada seis meses).

6. La administración de la red es la suma de todas las actividades de planeación y control, enfocada a mantener una red eficiente y con altos niveles de disponibilidad. Dentro de estas actividades hay diferentes responsabilidades fundamentales como el monitoreo, la atención a fallas, configuración, y seguridad, por lo que se debe contar con un buen sistema de administración, ya que esto ayudará a mantener la operatividad de los recursos y el buen estado de los mismos.

7. Se recomienda actualizar periódicamente el firmware de los equipos para tener disponibles las nuevas funcionalidades que los grupos de trabajo incorporen. Los grupos de trabajo se dedican a mejorar las redes inalámbricas, y así van apareciendo nuevas funcionalidades especialmente en el campo de seguridades que en el caso de nuestra red y en general de la redes inalámbricas es un campo de fundamental importancia..

8. Para este diseño se ha seleccionado los equipos del fabricante NORTEL, ya que sus características técnicas, rendimiento y garantías expuestas, están dentro de las necesidades de la red.

9. En primer lugar, como esquema básico de seguridad se planteó cambiar el SSID a uno que no tenga relación con el nombre de la entidad financiera y restringir su broadcast, esto hará a la red difícilmente identificable, luego se propuso el filtrado de direcciones MAC y la implementación de un servidor de autenticación RADIUS, lo que permitirá el acceso sólo a usuarios autorizados.

10. En la entidad bancaria, los datos con los que se trabajan son confidenciales, por lo que es primordial considerar el aspecto de la seguridad de esta información, si bien la desventaja fundamental de las redes inalámbricas es la seguridad, se han tomado las medidas de seguridad adecuadas para una red corporativa.

11. Es importante que existan equipos de protección contra sobrecargas y picos de tensión, como es el UPS, que además de brindar protección sirve como fuente de poder cuando existe algún corte de energía eléctrica, proveyendo durante algunos minutos energía para los elementos constitutivos de la red.

ANEXO A
DIAGRAMAS DEL SISTEMA

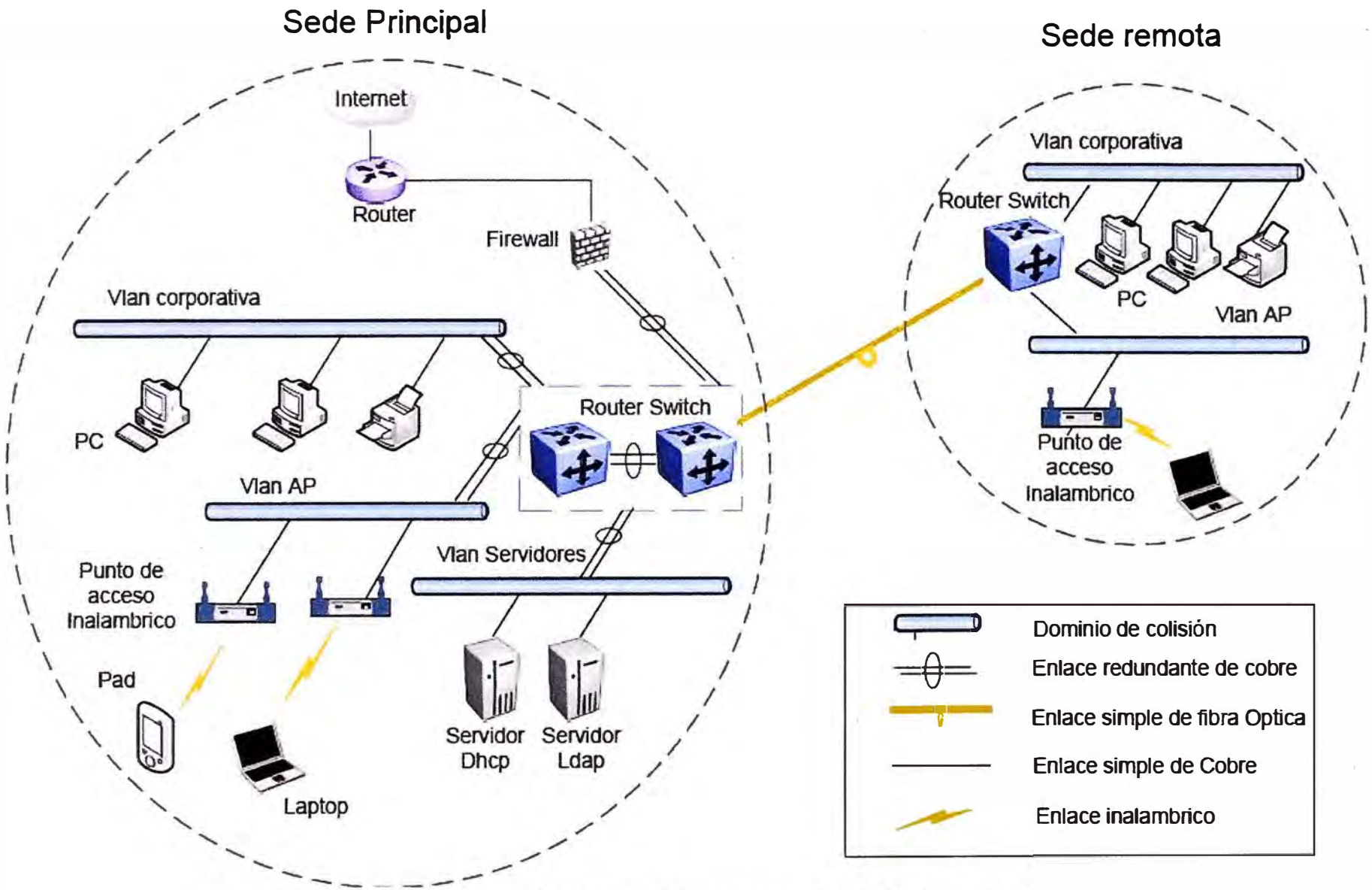

Figura A.1 Esquema de red de Empresa Financiera previa a la implantación de la solución

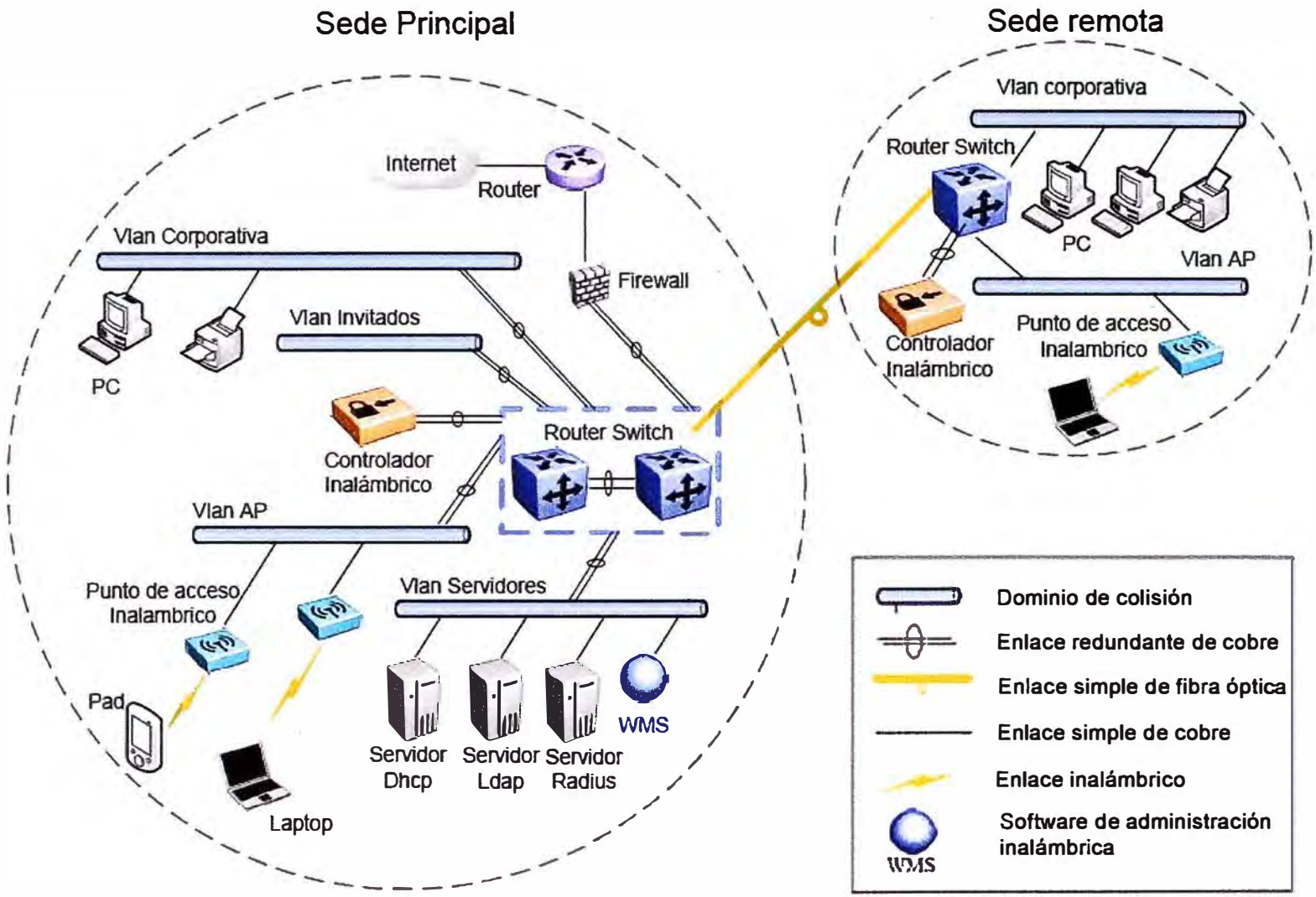

Figura A.2 Esquema de red de luego de implantada la solución

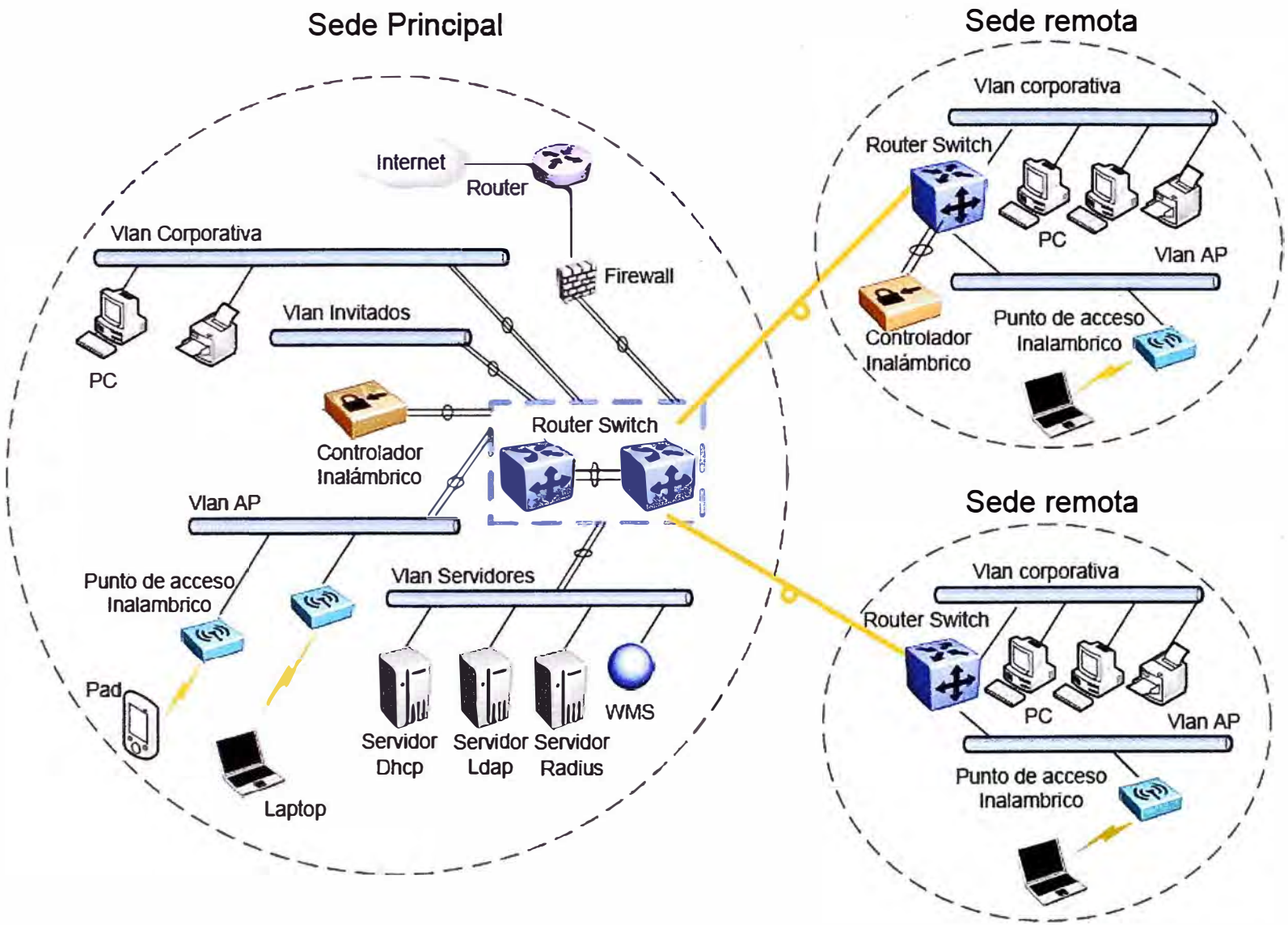

Figura A.3 Escalabilidad del sistema

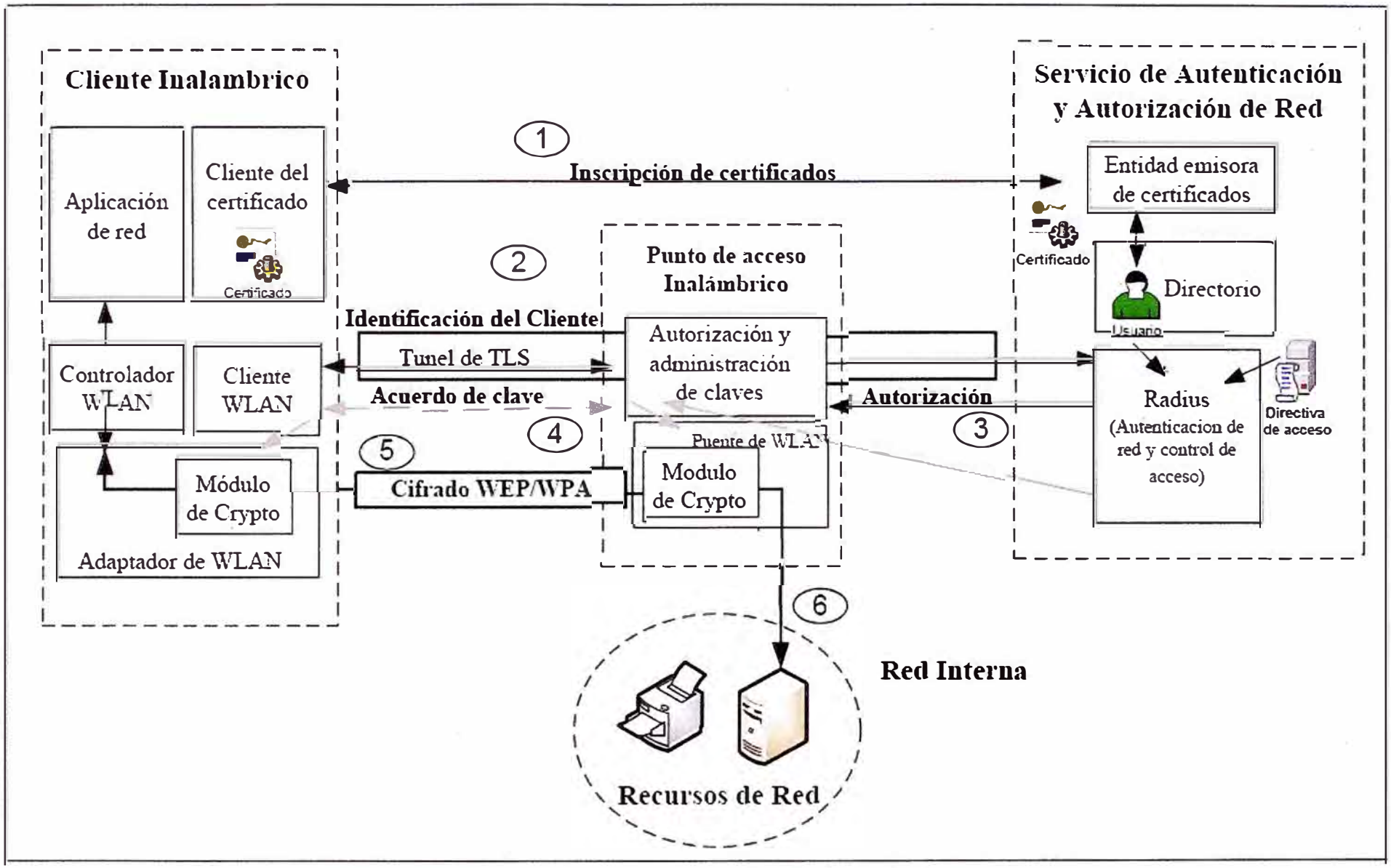

Figura A.4 Arquitectura en detalle de la solución

ANEXO B
DIAGRAMA DE GANTT

Id	Nombre de tarea
1	**PROYECTO BANCO.**
2	**PLANIFICACION.**
3	DESIGNACION DE RESPONSABLES
4	RECOPILACION DE INFORMACION DE APS(S/N & RSA)
5	RECOPILACION DE INFORMACION TECNICA
6	ENTREGA DE EQUIPOS
7	ENTREGA DE DISEÑO DE UBICACIÓN DE AP´S
8	
9	**WIRELESS LAN.**
10	CONFIGURACION DE SECURITY SWITCHS 2382
11	PRUEBAS DE FUNCIONALIDAD
12	
13	**LAN SWITCHING.**
14	CONFIGURACION DE VLANS
15	CONFIGURACION DE TRUNK A WSS 2382
16	MONTAJE DE SECURITY SWITCH 2382
17	
18	**ENLACE - CORE A PASSPORT 8600.**
19	CONFIGURACION DE ENLACE A WSS 2382
20	
21	**DESPLIEGUE/MONTAJE DE ANTENAS INDOOR**
22	Cableado SEDE PRINCIPAL
23	SEDE PRINCIPAL
24	Cableado SEDE REMOTA
25	SEDE REMOTA
26	**HERRAMIENTAS DE ADMINISTRACION**
27	INSTALACION/CONFIGURACION DEL WMS & INTEGRACIO
28	
29	**PROTOCOLO DE PRUEBAS.**
30	PRUEBAS DE FUNCIONALIDAD ENTRE WSS 2382

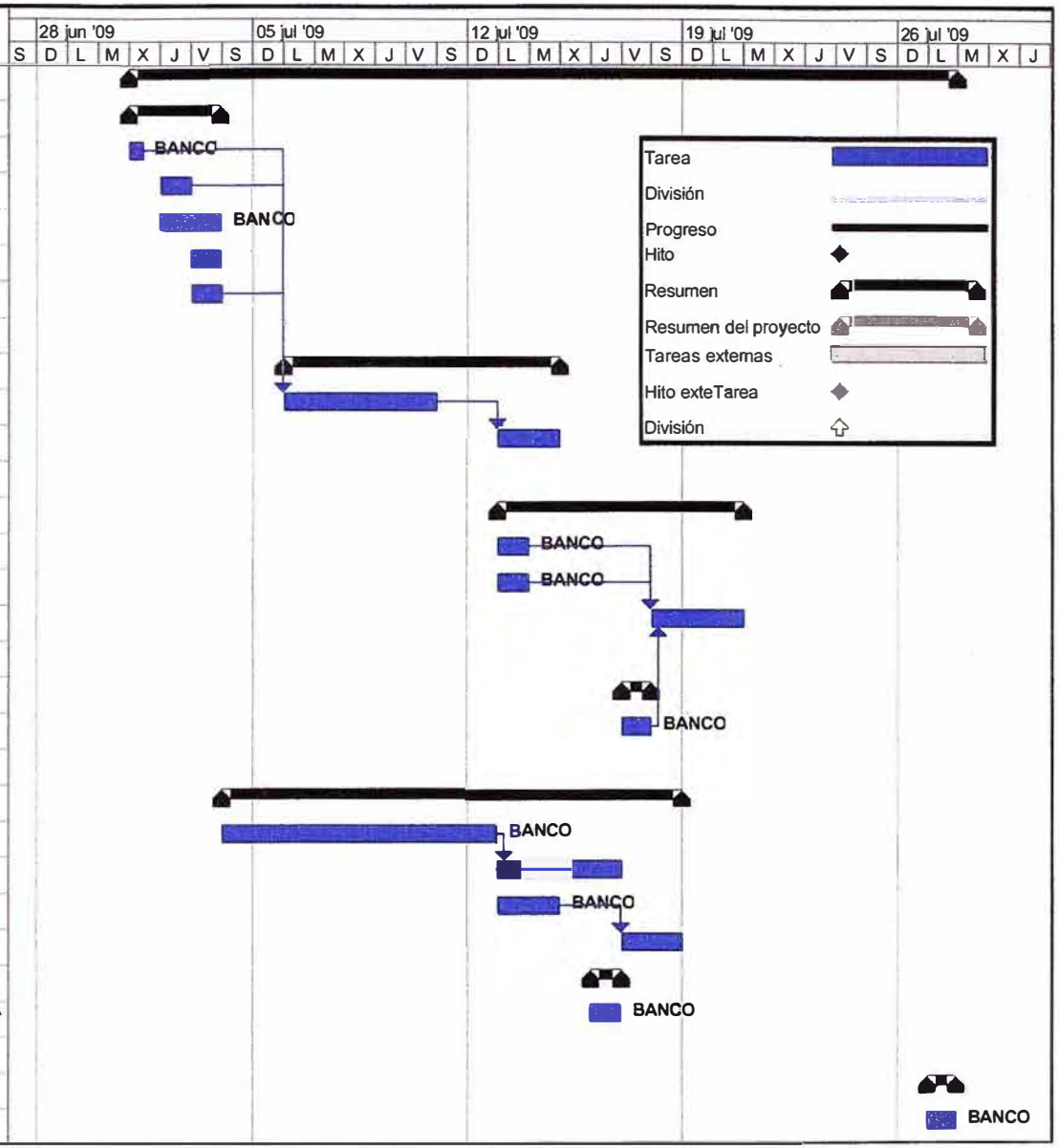

Figura B.1 Diagrama de Gantt

ANEXO C
GLOSARIO DE TÉRMINOS

ACS	Selección automática de canales
ACL	Lista de control de acceso
AES	Norma de codificación avanzada
AP	Punto de Acceso o Access Point
BSSID	Basic Service Set Identifier
CHAP	Challenge-Handshake Authentication Protocol
CLI	Interfaz de línea de comandos
Dos	Denegación de servicio
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol with Transport Layer Security
EFS	Encrypting File System
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IETF	Internet Engineering Task Force
IAS	Servicio de autentificación de Internet (Internet Authentication Service)
ISP	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol,
LLDP	Link Layer Discovery Protocol
MAN	Metropolitan Area Network
MIBs	Management Information Database.
MIC	Código de integración de mensajes
MIMO	Múltiple Input, Múltiple Output
NIC	Network Interface Card
NAS	Network Access Server
PAP	Protocolo de Autenticación de Clave de acceso (password)
PKI	Infraestructura de clave pública (Public Key Infrastructure)
PnP	Plug-and-Play
PPP	Point-to-Point Protocol o Protocolo Punto-a-Punto
QoS	Calidad de servicio
RADIUS	Remote Authentication Dial-In User Service
RFCs	Request for Comments
SCP	Protocolo de copia segura
SSHv2	Secure Shell
SSID	Service Set Identifier)

SSL	Secure Sockets Layer
STA	Estaciones
SVP	SpectraLink Voice Priority - Admisión de prioridad de voz SpectraLink
TCP/IP	Transmission Control Protocol/ Internet Protocol
TI	Tecnologías de la información
UIT	Unión Internacional de Telecomunicaciones
TKIP	Protocolo de Integridad de Clave Temporal
VLAN	Redes virtuales de área local
VPN	Virtual Private Network
WAN	Wide Area Network
WDS	Sistema de distribución inalámbrica o Bridging inalámbrico,
WEP	Wired Equivalent Protocol
WIDPS	Wireless Intrusion Detection and Prevention System
WLAN	Red de Área Local Inalámbrica (WLAN)
WMM:	Wi-Fi multimedia
WMS	WLAN Management Software
WPA	Wifi Protected Access
WPA2	IEEE 802.11i Acceso Wi-Fi protegido 2

BIBLIOGRAFÍA

[1] Nortel WLAN 2300 Series Design and Implementation Guide Rev 02.51, 2008, http://www142.nortelnetworks.com/mdfs_app/techdoc/enterprise/WLAN_7_0/pdf/NN47250-200_03.01_DSG.pdf

[2] WLAN Management Software 2300 Series Reference Guide Rev 02.51. 200823 http://www142.nortelnetworks.com/mdfs_app/techdoc/enterprise/WLAN_7_0/pdf/NN47250-102_03.01_RG.pdf

[3] WAP 2330/2330A/2330B Installation Guide Rev 02.51, 2008-06-13 http://www142.nortelnetworks.com/mdfs_app/techdoc/enterprise/WLAN_6_0_7/pdf/NN47250-302_02.51_INS.pdf

[4] WSS 2300 Series Configuration Guide Rev 02.01, 2008 http://www142.nortelnetworks.com/mdfs_app/techdoc/enterprise/WLAN_6_0/pdf/NN47250-500_CFG_02.01.pdf

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

[6] Richard Stevents. Addison- Wesley, "TCP/IP Ilustrated", volumen 1.

[7] Cisco, "Programa de certificacion CCNA" ver 4.0, 2007.

[8] WAP 2330/2330A/2330B Installation Guide, Rev 02.51, 2008http://www142.nortelnetworks.com/mdfs_app/techdoc/enterprise/WLAN_6_0_7/pdf/NN47250-302_02.51_INS.pdf

[9] WSS 2300 Series Configuration Guide Rev 02.01, 2008 http://www142.nortelnetworks.com/mdfs_app/techdoc/enterprise/WLAN_6_0/pdf/NN47250-500_CFG_02.01.pdf