UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO DE FACTIBILIDAD DE REEMPLAZAR LA RED DE INTERCONEXIÓN WAN DEL IESP "NORBERT WIENER" CON TECNOLOGIA WIRELESS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

VÍCTOR RAÚL YUPANQUI MAURICIO

PROMOCIÓN
1986 - I

LIMA – PERÚ
2005

Dedico este trabajo a:

Mis Padres, ejemplos de disciplina, honradez y perseverancia,

Mi Esposa, por su tenacidad en la búsqueda del progreso familiar y aliento constante para lograr el mío,

Y mis hijos, fuentes de innovación y motivos de superación.

Agradecimientos a:

William, por su apoyo y confianza que me permitieron seguir el ciclo de actualización y elaborar el presente trabajo,

Pedro y Luis, por proporcionarme parte de la bibliografía utilizada en la elaboración del presente Trabajo

Jacqueline, por su ayuda en la redacción y revisión del Trabajo

Víctor y Andrés, por proporcionarme la información necesaria para el desarrollo del trabajo.

ESTUDIO DE FACTIBILIDAD DE REEMPLAZAR LA RED DE INTERCONEXIÓN WAN DEL IESP “NORBERT WIENER” CON TECNOLOGIA WIRELESS

SUMARIO

El presente trabajo tiene como objetivo establecer técnica y económicamente la factibilidad de reemplazar la red de interconexión WAN Punto-Multipunto del Instituto de Educación Superior "Norbert Wiener" con tecnología Wireless. Tecnología emergente que en teoría se presentaría como superior a la actual.

En el capitulo I se hace una evaluación descriptiva de la red de comunicación actual, indicando ancho de banda por sedes, equipos instalados, servicios cubiertos, alcances y limitaciones, requerimientos futuros y los costos de operación mensual.

En el capitulo II se da el fundamento teórico necesario, que nos permita establecer los parámetros de diseño del nuevo modelo con tecnología inalámbrica, como los estándares, protocolos, tecnologías y productos inalámbricos, así como las consideraciones de radiofrecuencias, que se deben tener en cuenta en el diseño de una red de comunicaciones inalámbrica.

El capitulo III presenta el diseño del nuevo modelo de comunicaciones basado en tecnología inalámbrica, estableciendo el requerimiento de equipos, así cómo la infraestructura y recursos humanos necesarios para su implementación.

El capitulo IV trata sobre los parámetros de evaluación técnica y económica del nuevo modelo, comparándolo con el modelo actual para determinar su factibilidad, resultado a partir del cual se decidirá la forma de su implementación.

ÍNDICE

CAPÍTULO II

FUNDAMENTO TEÓRICO DE REDES INALAMBRICAS

CAPÍTULO III

MODELO WIRELESS PROPUESTO

CAPÍTULO IV

EVALUACIÓN TÉCNICO-ECONOMICA DE LOS MODELOS

INTRODUCCION

La tecnología inalámbrica (*Wireless*) representa en la actualidad una nueva manera de comunicación, tecnología aun emergente, que está innovando la forma de interconexión de las redes de datos. Las redes inalámbricas utilizan ondas de radio para la transmisión de datos, denominada comunicación de datos por radiofrecuencias (RF). Este tipo de transmisión es empleada por una gran variedad de sistemas como: la telefonía celular, dispositivos periféricos; cada uno de ellos con sus propias características especiales. Para el caso de redes inalámbricas varios dispositivos ubicados localmente o distantes algunos kilómetros comparten información.

El numero de instalaciones de redes inalámbricas se está incrementando en los últimos tiempos en instituciones como universidades, aeropuertos, centros comerciales, hoteles, plazas publicas, sedes militares, entre otras; debido principalmente a su fácil adaptación a la movilidad de sus usuarios en el caso de redes LAN y constituir una red propietaria que no requiere de pago de alquiler por líneas de comunicaciones en el caso de redes WAN. Característica que implica un menor costo de implementación y mantenimiento por la no utilización de cables,

antecedentes y detalles que nos ha motivado a realizar el presente informe de ingeniería, que busca determinar la factibilidad de reemplazar la red de comunicaciones PPP (*Point to Point Protocol*) del Instituto de Educación Superior Privado "Norbert Wiener" perteneciente a la Corporación Educativa "Wiener Carrión", por tecnología inalámbrica, donde se incluye el análisis de los costos involucrados, así como las ventajas y desventajas de cada tecnología, tanto técnica como económicamente, planteando como hipótesis la consecución de un ahorro económico sustancial en un horizonte de 3 años.

Este estudio hace una descripción del sistema actual, el cual está basado por enlaces dedicados entre su local principal y cada una de sus sedes con diferentes anchos de bandas, proporcionados por Bellsouth, para luego, proponer un modelo de interconexión inalámbrico, determinando luego su costo de implementación a partir del cual se hace un análisis técnico económica comparando anchos de bandas, capacidad de prestación de servicios e inversiones mensuales para determinar la factibilidad.

Hemos considerado que la implementación de la red inalámbrica en la institución, permitirá a los profesores y los alumnos acceder a la red, desde cualquier punto del campus universitario o desde cualquiera de las sedes de la corporación, así como, un alto ejecutivo de una empresa "x" lo hace a la red de su empresa desde cualquier aeropuerto, el poder establecer una red de comunicaciones inalámbrica para conectar las diferentes sedes de una entidad educativa permitiría a sus integrantes aprovechar las ventajas antes mencionadas desde cualquiera de las sedes. Se debe destacar que

las redes inalámbricas representan la mejor solución para construcciones antiguas por no requerir de cableado y para instituciones que por su modo de operación necesitan de permanente movimiento de sus terminales de datos, minimizando los costos de operación.

Debemos destacar que las redes inalámbricas son relativamente nuevas, ya que el primer estándar inalámbrico IEEE 802.11 fue aprobado en Julio de 1997, fecha a partir de la cual se han hecho innovaciones a este estándar como el 802.11a, 802.11b y el 802.11g aprobado recientemente en el 2003 pasando de una velocidad de 1Mbps a 54Mbps, lo que representa un aumento considerable en la velocidad y capacidad de las redes inalámbricas. Indicándose, además que las primeras comunicaciones inalámbricas, se dan en 1901 con el descubrimiento del teléfono inalámbrico por Marconi, quien utilizo código Morse, pero no tuvieron una apreciada aceptación, ya que se consideraban como inseguras por utilizar el espectro radioeléctrico para su transmisión, así como su baja velocidad, razones que impidieron su rápido desarrollo hasta la actualidad, donde éstas limitaciones han sido largamente superadas, siendo las técnicas de transmisión inalámbricas más utilizadas hoy en día los DSSS (*Direct Sequense Spread Spectrum*), FHSS (*Frecuency Hopping Spread Spectrum*) y OFDM (*Orthogonal Frecuency Digital Multiplexing*).

Las fuentes bibliograficas consultadas, han sido básicamente, manuales técnicos de fabricantes, así como, sus páginas web, revisándose en estos *data sheet*, *white paper* y broshoure de los productos, ya que a nivel de literatura tradicional, como libros, se tienen en forma restringida para redes inalámbricas LAN (WLAN) basadas en

dispositivos *access point*, no así, para la interconexión de redes basadas en *bridge* y antenas.

El uso de la tecnología inalámbrica en el **ámbito educativo**, nos da un conjunto ilimitado de aplicaciones; como por ejemplo: Los laboratorios de informática podrían estar en cualquier lugar de la institución, ya que las computadoras con interfaces inalámbricas pueden ubicarse en cualquier lado de la sede educativa, teniendo los docentes y alumnos acceso a la red sin restricción alguna.

CAPÍTULO I

EVALUACIÓN DE LA RED PRIVADA ACTUAL

La Universidad "Wiener" y los Institutos de Educación Superior Privados "Daniel A. Carrión" y "Norbert Wiener", son instituciones que conforman la corporación educativa "Wiener Carrión" e integradas en sus Redes de comunicaciones LAN y WAN, para que sus aplicaciones visuales, no visuales y cliente/servidor den los servicios administrativos y pedagógicos a toda su comunidad educativa, bajo una sola administración, representada por la Dirección de Sistemas de la Universidad, en cuya sede se encuentra, los servidores de las principales aplicaciones de la Corporación. En las líneas siguientes, se hace una evaluación de la Red WAN actual para su reemplazo por tecnología inalámbrico (Wireless), dejando las redes locales LAN para un análisis posterior.

Las sedes de la Corporación, en la actualidad, se encuentran interconectadas con enlaces dedicados proporcionados por Bellsouth, con un ancho de banda de 2Mb y canales de voz en su local central, el cual tiene enlaces con las otras sedes de 64Kb, 128Kb, 256Kb y 1Mb por lo que se abona una renta mensual, cuyo análisis y descripción se hace en las siguientes secciones.

1.1. Descripción de la Intranet

La Intranet se constituye de 9 sedes interconectadas a través de routers (marca Cisco en su mayoría) y sus otras sedes conectadas vía módem. Estas sedes se encuentran ubicadas desde la Av. Emancipación en el cercado de Lima hasta la calle Grimaldo del Solar en Miraflores, siguiendo casi una línea recta entre sedes, cruzando las avenidas Tacna, Wilson y Arequipa, lo que favorece para el "establecimiento" de la línea de vista entre las sedes, elemento clave para la interconexión con tecnología inalámbrica.

En la Tabla 1.1, se dan las ubicaciones de las sedes interconectadas, el equipo de comunicación utilizado, el ancho de banda y los canales de voz utilizados en cada una de éstas sedes.

Ubicación de sedes interconectadas

SEDE	UBICACIÓN	ROUTER	ANCHO DE BANDA	CANALES DE VOZ
7801	Calle Grimaldo del Solar Cdra.7	Cisco 2600	64K	2
7802	Av. Wilson Cdra.12	Cisco 2600	64K	2
7803	Av. Arequipa Cdra.4	Cisco 3640	2MB	8
7804	Av. Emancipación Cdra.15	Cisco 2600	256K	2
7805	Av. Arequipa Cdra.15	Cisco 2600	256K	2
7807	Paseo Colon Cdra.2	Cisco 2600	256K	2
7809	Av. Arequipa Cdra.9	Cisco 2600	896K	2
7812	Av. Pardo Pardo Cdra.6	Red Web Rouger	64K	2
7814	Av. Arequipa Cdra.14	Red Web Rouger	128K	2

Tabla 1.1

En la figura 1.1, se presenta el diagrama de interconexión de las sedes. Se puede apreciar que la conexión de cada una de las sedes secundarias con la principal (7803) es una conexión punto a punto, por tanto, la conexión de la principal hacia los demás es punto – multipunto, lo que requiere disponer de líneas de comunicación dedicadas, considerando además, que algunos de los equipos instalados no son de propiedad de la Corporación, que implica el pago de alquiler de equipos y líneas de comunicación representando

RED CORPORATIVA WIENER - CARRION

Diagrama Interconexión de Sedes

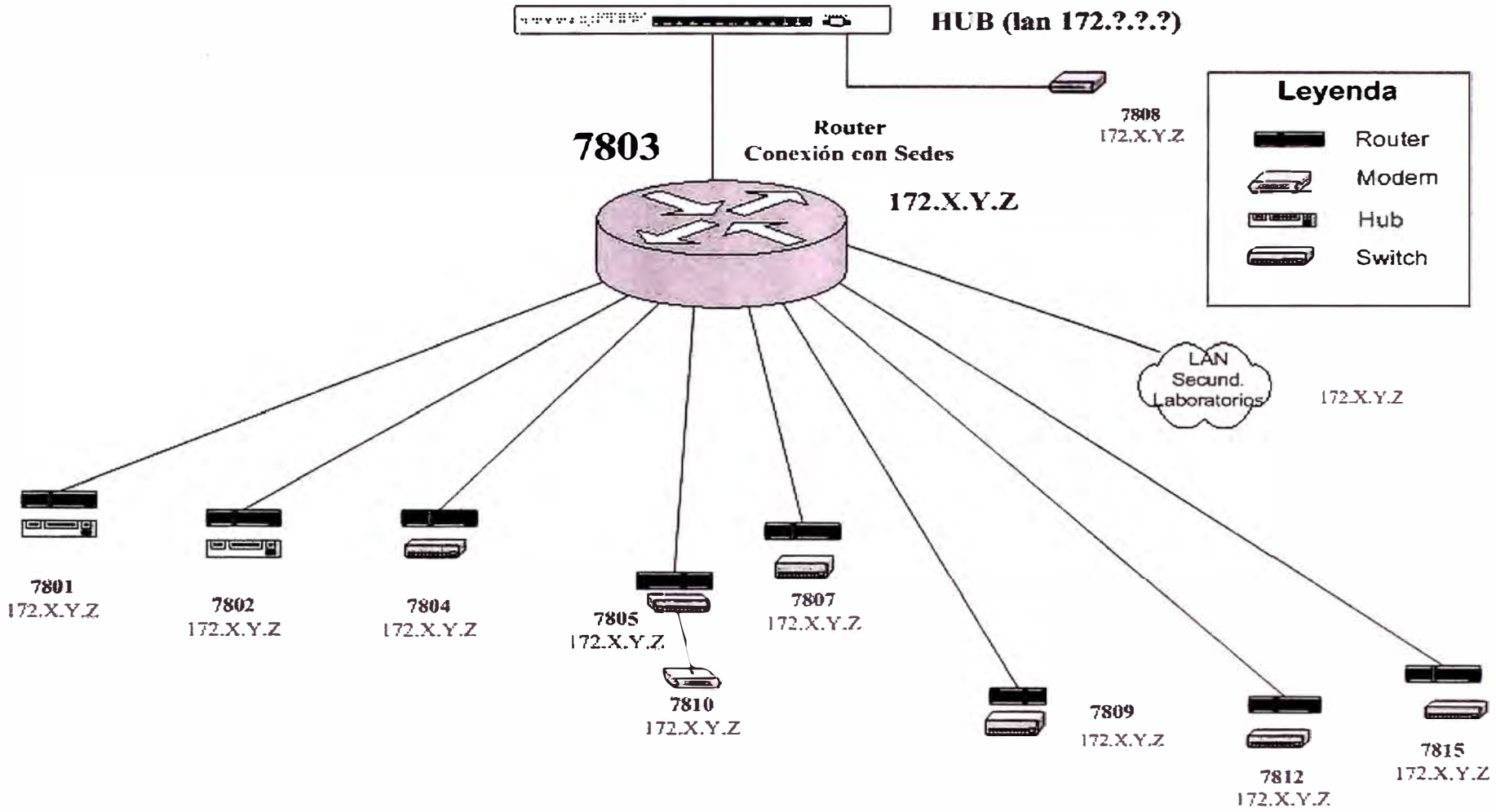


Figura 1.1

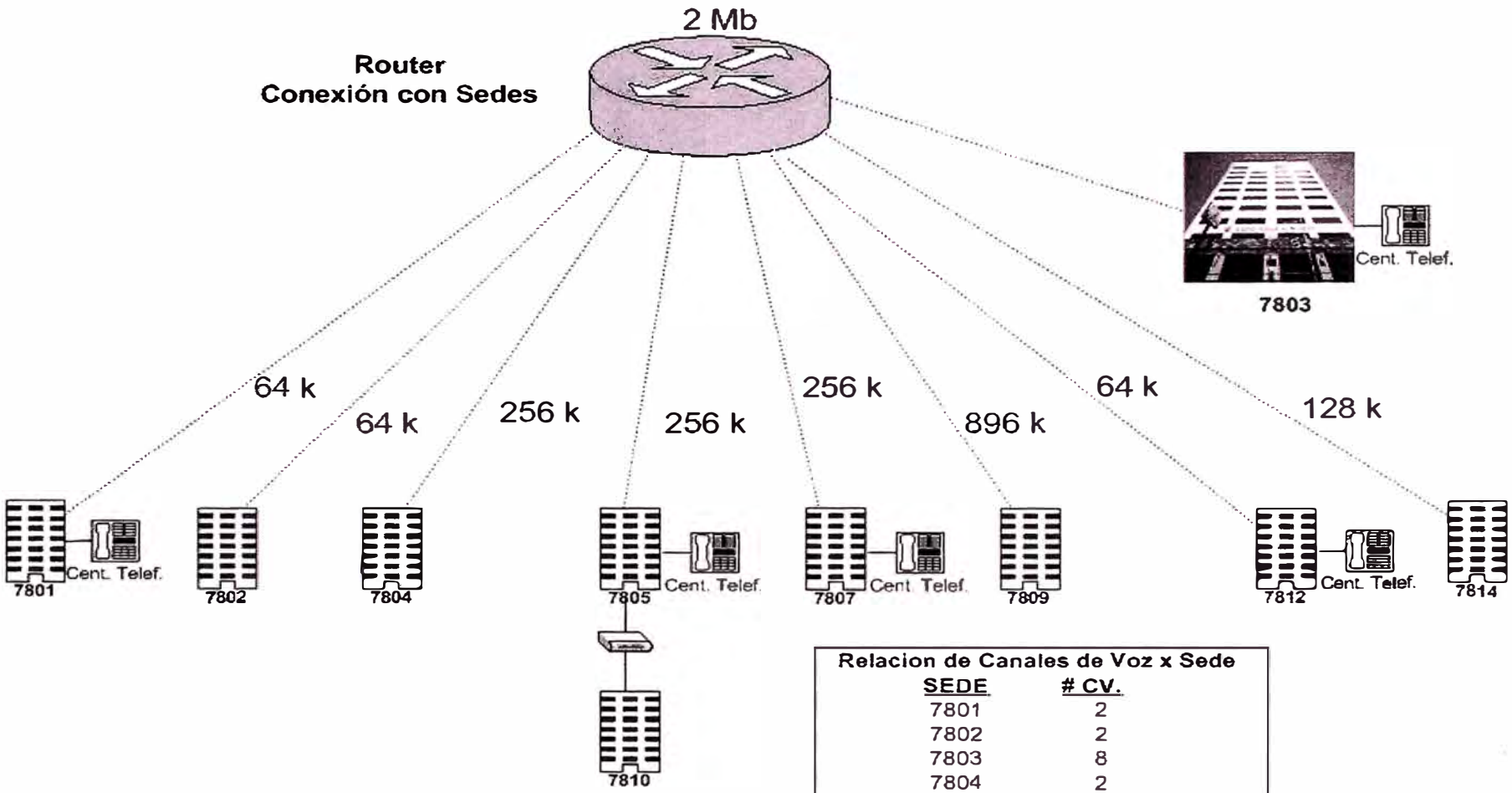
estos costos alrededor de US$ 6,000.00 mensuales (US$ 72,000.00 anuales), razón por la cual se planteó este proyecto.

En la figura 1.2, se presenta el diagrama de ancho de banda y canales de voz por sedes, habiéndose establecido el ancho de banda de cada sede, en función al numero de computadoras con que cuenta cada una de ellas; por ejemplo; la sede 7809 cuenta con un aproximado de 200 computadoras por lo que dispone de un ancho de banda de 896KB, ancho de banda utilizado por los canales de voz, la comunicación de datos (Intranet) y el acceso a Internet, cuya salida hacia el proveedor de servicios, está en la sede principal.

En la figura 1.3, se presenta el diagrama de servidores, ubicados en la sede principal como: el servidor DNS Interno, Servidor de Base de datos ORACLE, Servidor SIGU (Sistema Integrado de Gestión Universitaria), Servidor IDS, los servidores WEB www.uwiener.edu.pe (Universidad Wiener), www.acarrion.edu.pe (Instituto Daniel A. Carrión), idiomas.uwiener.edu.pe (Centro de idiomas de la Universidad) y el servidor de correos mail.wienergroup.com donde se configura la cuentas y cuotas de usuarios para toda la corporación. El servidor WEB para la Instituto Norbert Wiener se encuentra ubicado en la sede 7809 www.wiener.edu.pe. También se puede observar en el diagrama que como elementos de protección de la red corporativa, se ha configurado un firewall, servidor proxy y servidor proxy reverso.

RED CORPORATIVA WIENER - CARRION

Diagrama de Ancho de Banda y Canales de Voz por Sedes



Relacion de Canales de Voz x Sede	
SEDE	# CV.
7801	2
7802	2
7803	8
7804	2
7805	2
7807	2
7809	2

Figura 1.2

RED CORPORATIVA WIENER - CARRION

Diagrama de Servidores

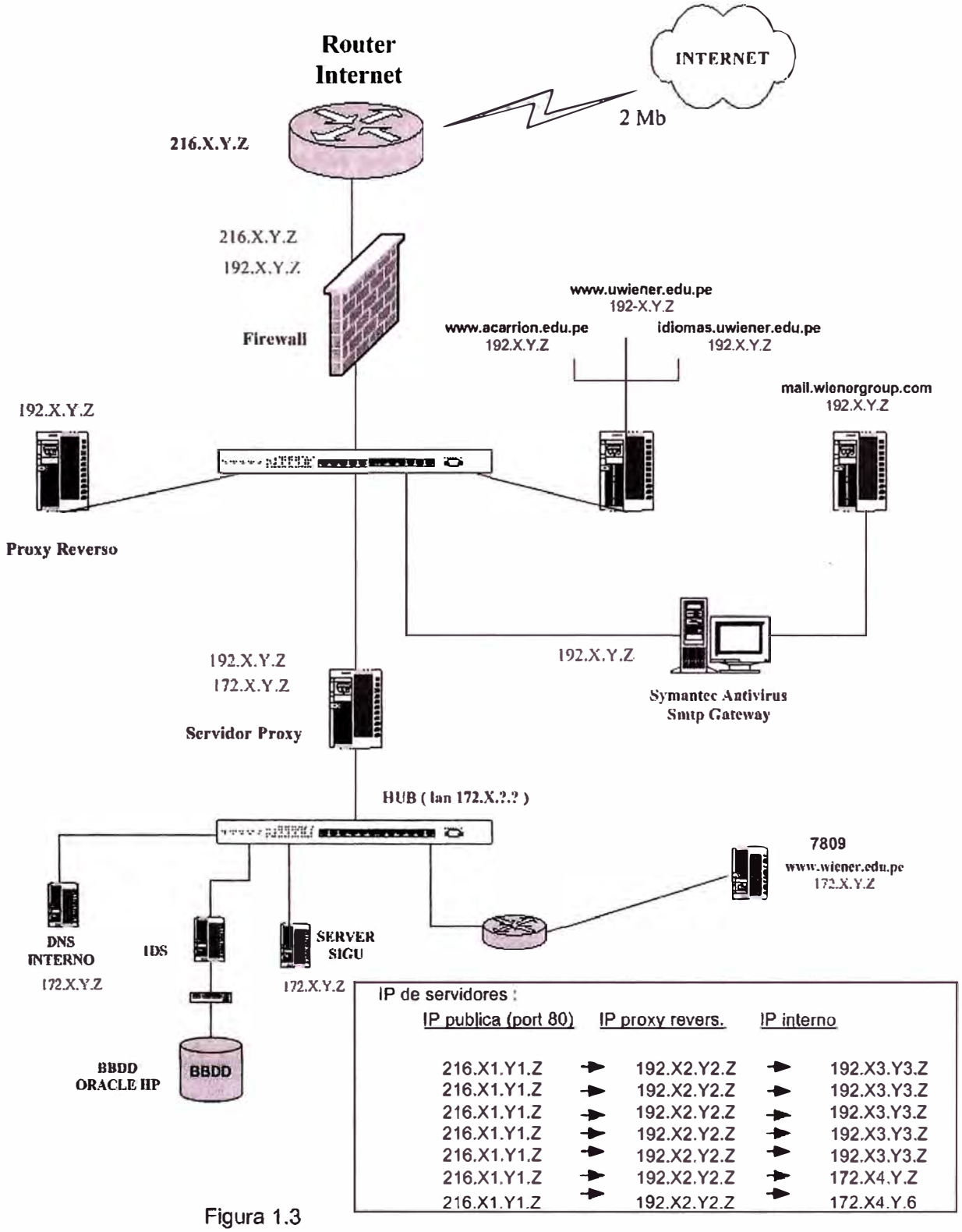


Figura 1.3

1.2. Alcances y limitaciones

La Red corporativa tiene un ancho de banda de conexión a Internet de 2MB a través de una conexión Frame Relay con su proveedor de servicios Bellsouth.

1.3. Servicios proporcionados por la Intranet

Los servicios del que hacen uso los miembros de la Corporación "Wiener Carrión", son los siguientes:

SIGU (Sistema Integrado de Gestión Universitaria)

Internet

Correo electrónico

Intranet Administrativa

Intranet Docente

Intranet Alumno

A continuación describiremos cada uno de los servicios

1.3.1 SIGU (Sistema Integrado de Gestión Universitaria)

Sistema con el cual se gestiona, supervisa y controla el proceso de matricula, la elaboración y modificación de horarios, así como los registros de notas de las tres instituciones miembros de la corporación: Universidad Wiener, Instituto Daniel A. Carrión e Instituto Norbert Wiener, siendo el sistema vital para el desarrollo de las actividades académicas y administrativas de la Corporación. Este sistema cuenta con 6 módulos:

a) **Académico 1:**

   Control de Horarios.

   Seguimiento Académico.

Asistencia de Alumnos.

b) **Académico 2:**

Informes.

Encuesta Personal Docente.

c) **Servicios al Estudiante:**

Practicas Pre-Profesionales.

Bienestar Estudiantil.

Deportes.

Bolsa de trabajo.

Biblioteca

Actividades Artísticas

Investigación.

d) **Administración:**

Tesorería.

Planillas.

Logística.

Tramite Documentario

e) **Estadísticos:**

Indicadores Gerenciales.

ISO.

f) **Institutos:**

Horarios.

Matricula

Registro de Notas.

Los cinco primeros módulos son de uso de la Universidad y el último modulo es utilizado por los institutos Wiener y Carrión, destacándose que a través de este sistema se controla todos los procesos de la Corporación.

1.3.2 Servicio de Internet

Para todos los integrantes de la Corporación, contándose con 4 servidores Web al cual tienen acceso el público interno como el externo, para conocer las actividades, carreras, cursos y otros servicios que las instituciones brindan:

Universidad Wiener – www.uwiener.edu.pe

Instituto Daniel A. Carrión – www.acarrion.edu.pe

Instituto Norbert Wiener – www.wiener.edu.pe

Centro de Idiomas Universidad – idiomas.uwiener.edu.pe

1.3.3 Servicio de correo electrónico

Se establece una cuenta y cuota de disco para cada uno de los integrantes de la corporación, teniéndose el servidor mail.wienergroup.com.

1.3.4 Intranet administrativa

Servicio que permite a cada usuario la solicitud de adelantos, verificar sus ingresos y egresos, verificar el inventario de equipos, entre otras, a través de las siguientes opciones activas:

Help Desk

Directorio telefónico

Inventario de equipos

Control de Asistencia

Cifras Estadísticas de Acceso a la Intranet.

Ingresos / Egresos.

Excelencias.

Solicitud de Adelanto

1.3.5 Intranet docente

A través de este servicio, los docentes verifican sus horarios, establecen su disponibilidad horaria, solicitan adelanto, así como el llenado de sus registros, teniendo las siguientes opciones:

Horarios de Clase.

Avance Académico.

Evaluación Académica.

Registro de Notas.

Ingresos / Egresos.

Solicitud de Adelanto.

1.3.6 Intranet alumno

A través de este servicio, los alumnos visualizan sus notas, pagos y horarios, lo que también puede ser observado por sus padres y tutores, siendo las opciones del menú las siguientes:

Registro Notas.

Control de pagos.

Horarios de Clases.

1.4. Requerimientos futuros

La corporación "Wiener Carrión", tiene como proyectos futuros implementar los siguientes servicios:

Universidad Virtual.

1.5. Costos de operación

En la tabla 1.2 se consigna la renta mensual abonada por la Corporación Educativa "Wiener Carrión" a Bellsouth por las líneas dedicadas para la interconectividad de sus sedes.

Costo mensual por puertos

CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO US$	PRECIO TOTAL US$
01	Puerto Dedicado a 2048 Kbps. En el punto principal de la Sede 7803.	790.00	790.00
01	Puerto Dedicado a 2848 Kbps. para el acceso a Internet, en la sede principal.	790.00	790.00
01	Acceso a Internet a 2048 Kbps. En el local de la Sede principal 7803.	1,800.00	1,800.00
01	Puerto Dedicado a 1024 Kbps. En el local de la Sede 7809.	550.00	550.00
01	Puerto Dedicado a 128 Kbps. En el local de la Sede 7814.	190.00	190.00
03	Puertos Dedicados a 64 Kbps. En los locales remotos de la Sedes 7805, 7807 y 7804.	245.00	735.00
03	Puertos Dedicados a 64 Kbps. En los locales remotos de la Sedes 7812, 7801 y 7802.	150.00	450.00
04	Alquiler de MODEM HDSL Sedes 7808 y 7810.	100.00	400.00
		Sub. – Total:	5,705.00
		Impuesto 19% (IGV):	1,083.95
		TOTAL US$:	6,788.95

Tabla 1.2

En la tabla 1.3 se presenta el cuadro de costos mensuales por sedes interconectadas y ancho de Banda.

Costos de operación por ancho de anda

Nº DE PUERTOS	SEDE	ANCHO DE BANDA	RENTA MENSUAL	
			PRECIO UNITARIO US$	PRECIO TOTAL US$
1	7803	2048 Kbps. Puerto Principal	790.00	790.00
1	7803	2048 Kbps. Puerto para Internet	790.00	790.00
1	7803	2048 Kbps. Acceso a Internet	1,800.00	1,800.00
1	7809	1024 Kbps. Puerto Remoto	550.00	550.00
1	7814	128 Kbps. Puerto Remoto	190.00	190.00
3	7805, 7807 y 7804.	256 Kbps. Puertos Remotos	245.00	735.00
3	7812, 7801 y 7802.	64 Kbps. Puertos Remotos	150.00	450.00
4	7808 y 7810.	Comunicación entre locales cercanos MODEM HDSL	100.00	400.00
			SUB TOTAL:	5,705.00
			IGV (19%):	1,083.95
			TOTAL	6,788.95

Tabla 1.3

CAPÍTULO II

FUNDAMENTO TEORICO DE REDES INALAMBRICAS

2.1. Redes inalámbricas términos y definiciones

El gran desarrollo actual de las comunicaciones inalámbricas y la computación móvil, determina la aceptación de las redes inalámbricas como una tecnología que permite resolver varios de los inconvenientes del usar cable como medio físico de enlace en las comunicaciones, relacionadas a actividades de vital importancia en el trabajo cotidiano de las empresas. En este capitulo se introducen algunos conceptos relacionados con las redes inalámbricas, indicando las características de las diversas tecnologías inalámbricas enmarcadas dentro del estándar IEEE 802.11 como bluetooth y homeRF. Luego, se establece, el uso de dispositivos inalámbricos como bridge y antenas para una comunicación inalámbrica WAN.

Los equipos inalámbricos otorgan la libertad necesaria para trabajar prácticamente desde cualquier punto del planeta e, incluso, permiten el acceso a todo tipo de información cuando se está de viaje. No importa que el sistema inalámbrico esté accediendo al correo electrónico desde un aeropuerto o recibiendo instrucciones desde el despacho para realizar alguna tarea, lo realmente relevante de esta

tecnología es la extremada efectividad que se logra al poder mantener una conexión de datos con una red desde cualquier remoto sitio del globo mundial. Por otra parte, las comunicaciones de radio han estado a nuestra disposición desde hace ya bastante tiempo, teniendo como principal aplicación la comunicación mediante el uso de la voz. Hoy en día, millones de personas utilizan los sistemas de radio de dos vías para comunicaciones de voz punto a punto o multipunto. Sin embargo, aunque los ingenieros ya conocían las técnicas para modular una señal de radio con la cual conseguir el envío de datos binarios, sólo recientemente han podido desarrollar y desplegar servicios de datos a gran escala.

La transmisión de datos en forma inalámbrica incluyen enlaces fijos de microondas, redes LAN inalámbricas, datos sobre redes celulares, redes WAN inalámbricas, enlaces mediante satélites, redes de transmisión digital, redes con paginación de una y dos vías, rayos infrarrojos difusos, comunicaciones basadas en láser, Sistema de Posicionamiento Global (GPS) y mucho más.

Como se puede ver, se tiene una variada y extensa gama de dispositivos con tecnología inalámbrica, los cuales son utilizados por millones de usuarios cotidianamente de forma transparente para ellos.

Tampoco hay que olvidar los numerosos beneficios que aporta la utilización de los dispositivos inalámbricos, ya que gracias a ellos se logran realizar conexiones imposibles para otro tipo de medio, conexiones a un menor costo en muchos escenarios, conexiones más rápidas, redes que son más fáciles y rápidas de instalar y conexiones de datos para usuarios móviles.

Como vemos, el panorama de las redes inalámbricas es casi tan extenso o más que el de las propias redes convencionales, a las que estamos más habituados. Debido a la impresionante variedad de tecnologías, configuraciones, dispositivos, topologías y medios, relacionados con las redes inalámbricas nos centraremos en el uso de dispositivos que nos permitan interconectar un conjunto de edificios ubicados entre el Cercado de Lima y el distrito de Miraflores utilizando ondas de radio para interconectar las redes LAN de computadoras ubicados en los edificios.

El fundamento de muchas de las actuales redes inalámbricas se encuentra basado en el estándar IEEE 802.11, y más concretamente en las especificaciones IEEE 802.11b, IEEE 802.11a y IEEE 802.11g. Un consorcio, el *"Wireless Ethernet Compatibility Alliance"* (WECA), formado por un grupo de empresas de renombre, ha creado una nueva línea de productos de mayores prestaciones y de plena compatibilidad. Con este estándar se pone fin a la larga tradición que siempre ha acompañando y se ha relacionado con el mundo de las redes inalámbricas, y donde, como todo en esta vida, hay parte de razón y otra parte fruto de la leyenda negra. Además, los productos acogidos a la normativa IEEE 802.11 tienen garantizada la interoperatividad entre fabricantes, consiguiendo al mismo tiempo una significativa reducción de los costes y abaratamiento de los dispositivos para el usuario final.

WECA ha establecido un estándar llamado Wi-Fi (*Wireless Fidelity*), que permite certificación de los productos acogidos a esta normativa para lograr que entre ellos existan una obligada interoperatividad y otros aspectos comunes de actuación como la facilidad de configuración, unanimidad de protocolos, modos de funcionamiento,

así como las más elementales normas. Pero, independientemente del prometedor futuro de las WLAN (*Wireless LAN*) acogidas al Wi-Fi, dentro de este particular sector de las redes inalámbricas hay otras tecnologías que también aprovechan parte de la infraestructura de la cual hacen uso casi todos los dispositivos WLAN. En general, los sistemas LAN sin cables basados en el protocolo 802.11 hacen un exhaustivo uso de la banda de frecuencias de los 2.4GHz. El porqué de este concreto rango de frecuencias no es difícil de explicar y puede resumirse en que en esta zona del espectro electromagnético no se requiere el uso de licencias tal y como se lleva a cabo la regulación de los sistemas de radio, ya que en ellas se permite la transmisión de información en bandas del espectro, concretamente en las bandas llamadas ISM (*Industrial Scientific Medical*) por su uso para aplicaciones industriales, científicas y médicas. Pero esta misma ventaja actúa a su vez de atractivo y poderoso reclamo para otras tecnologías, sistemas o dispositivos inalámbricos que también quieran basar su funcionamiento en esta área específica del espectro.

Las WLAN aunque son la base de la expansión y flexibilidad de muchas de las actuales redes LAN, pecan quizá de ser una solución más bien general y dirigida a entornos de trabajo en grupo y empresas que puedan sacar el máximo partido a sus capacidades. Precisamente, esta generalidad ha dado pie a que nuevas tecnologías como bluetooth y homeRF, surjan en torno al protocolo 802.11, y aprovechando igualmente el rango de frecuencias de 2,4GHz han optado por especializarse en ofrecer una conectividad inalámbrica, pero enfocada a unos usos mucho más particulares y en relación directa con los requerimientos tecnologicos de las empresas

y personas pertenecientes a una sociedad económicamente globalizada como es la sociedad actual.

Bluetooth es, a grandes rasgos, una especificación para la industria informática y de las telecomunicaciones que describe un método de conectividad móvil universal con el cual se pueden interconectar dispositivos como teléfonos móviles, Asistentes Personales Digitales (PDAs), ordenadores y muchos otros dispositivos, ya sea en el hogar, en la oficina o, incluso, en el automóvil, utilizando una conexión inalámbrica de corto alcance. Es un estándar que describe la manera en la que una enorme variedad de dispositivos pueden conectarse entre sí, de una forma sencilla y sincronizada, con cualquier otro equipo que soporte dicha tecnología utilizando las ondas de radio como medio de transporte de la información. Técnicamente, la implementación de esta novedosa tecnología no entraña ninguna complicación técnica especialmente problemática ni sofisticada. Tampoco supone que los nuevos dispositivos equipados con esta tecnología deban sufrir profundas revisiones o modificaciones, todo lo contrario.

En sí, cada dispositivo deberá estar equipado con un pequeño chip que transmite y recibe información a una velocidad de 1Mbps en la banda de frecuencias de 2.4GHz, que está disponible en todo el mundo, con ciertas particularidades según los diferentes países de aplicación, ya que es empleada con enorme profusión en numerosos dispositivos.

Con una finalidad muy similar, la tecnología homeRF, basada en el protocolo de acceso compartido SWAP *"Shared Wireless Access Protocol"*, encamina sus pasos hacia la conectividad sin cables dentro del hogar. Los principales seguidores de estos sistemas, se agrupan en torno al consorcio que lleva su mismo nombre homeRF, teniendo a Proxim (una filial de Intel) como el miembro que más empeño está poniendo en la implantación de dicho estándar. Además de la sombra de Intel, Compaq es otra de las firmas relevantes que apoya el desarrollo del producto homeRF. El soporte a esta tecnología se materializa en que actualmente ambas significativas firmas poseen cada una de ellas un producto bajo esta novedosa configuración. Al igual que WECA o Bluetooth SIG (*"Bluetooth Special Interest Group"*), el *HomeRF Working Group* (HRFWG) es un grupo de compañías encargadas de proporcionar y establecer un cierto orden en este océano tecnológico, obligando que los productos fabricados por las empresas integrantes de este grupo tengan una buena interoperatividad. Por si toda esta competitividad no fuera suficiente, el Instituto de Estándares de Telecomunicaciones Europeo (ETSI) es otra de las reconocidas organizaciones de estandarización, culpable, entre otros, de haber desarrollado el estándar GSM para la telefonía celular digital. También son responsables de haber llevado a cabo durante los años 1991 y 1996 el proyecto HyperLAN, en el cual su objetivo primordial era conseguir una tasa de transferencia mayor que la ofrecida por la especificación IEEE 802.11. Según los estudios realizados, HyperLAN incluía cuatro estándares diferentes, de los cuales el denominado Tipo 1, es el que verdaderamente se ajusta a las necesidades futuras de las WLAN, estimándose una velocidad de transmisión de 23.5 Mbps, notablemente superior a los 1 ó 2 Mbps de la normativa IEEE 802.11b. Actualmente, el ETSI

dispone de la especificación LANHiper2 que mejora notablemente las características de sus antecesoras, ofreciendo una mayor velocidad de transmisión en la capa física de 54Mbps para lo cual emplea el método de modulación OFDM (*Orthogonal Frequency Digital Multiplexing*) y ofrece soporte QoS. Bajo esta especificación se ha formado un grupo de reconocidas firmas el *HiperLAN2 Global Forum* (H2GF), con la intención de sacar al mercado productos basados en ese competitivo estándar.

La tabla 2.1 muestra un cuadro resumen de las nuevas especificaciones relacionadas con el IEEE 802.11:

Especificaciones IEEE802.11

Estándar	Espectro	Tasa Física Máxima	Tasa de Datos Nivel 3	Método de Transmisión	Compatibilidad
802.11	2.4 Ghz	2 Mbps	1.2 Mbps	FHSS/DSSS	No
802.11a	5.0 Ghz	54Mbps	32 Mbps	OFDM	No
802.11b	2.4 Ghz	11Mbps	6-7 Mbps	DSSS	802.11
802.11g	2.4 Ghz	54Mbps	32 Mbps	OFDM	802.11/ 802.11b

Tabla 2.1

El medio cambiante y las condiciones en las que operan las redes inalámbricas hacen que aún sean consideradas como medio alternativo para ofrecer servicios. La inseguridad inherente en este tipo de redes debido a la facilidad de acceso al medio de transmisión las hace muy vulnerables a ataques frecuentes. Son dos de las principales desventajas de las redes inalámbricas. Campos en los que se está investigando profundamente con el fin de superarlas y convertirlas en un medio importante de transmisión de datos. La calidad en la transmisión de los datos requiere de una adaptación particular de este tipo de redes a este medio cambiante.

En forma simple, la calidad en el servicio en redes inalámbricas se puede ofrecer ya sea a través de la reservación de recursos en la red o a través de la adaptación de la aplicación que se ejecuta sobre la red. Este trabajo pretende establecer el mayor ancho de banda que otorgaría una comunicación WAN inalámbrica entre las sedes del Instituto Norbert Wiener que la red actual.

2.2. Topologías de redes LAN inalámbricas

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. La primera conocida como INFRAESTRUCTURA, una topología administrable o alojada y la segunda conocida llamada AD HOC, topología no administrable o par a par. A continuación se describe las dos topologías o modos de funcionamiento.

2.2.1. Modo infraestructura

En el modo de infraestructura se utiliza puntos de acceso (AP). Estos dispositivos realizan una importante labor para el mantenimiento de la red simplificándolo en gran medida. Los puntos de acceso deberán proveer soporte de asociación y autentificación para que los dispositivos puedan conectarse con él, permitir *roaming* para dispositivos procedentes de otros APs de la misma red. Además deberán aportar mecanismos de sincronización, control de energía y funciones de calidad de servicio.

La configuración en el modo infraestructura, consiste en un punto de acceso, que permite cubrir una célula y dar cobertura a toda una zona, conociendo a ésta zona, como BSS (*Basic Service Set*) o conjunto de servicios básicos. Además los APs podrían estar interconectados, o conectados a una red cableada, esto permite extender el alcance de la red, ya que donde no llegue el alcance de un AP llegará otro, para ello se hace necesario funciones de roaming entre celdas.

Estando conectado a una red fija, o una LAN, permitirá a los dispositivos móviles acceder a servicios de los LANs tradicionales, como intranets o recursos fijos.

Varios APs conectados forman un ESS (*Extended Service Set*)o conjunto de servicios extendidos, que consiste en dos o más BSSs formando una subred; conociendo a la red que los conecta, como sistema de distribución. Este sistema de distribución podría estar montado sobre cualquier sistema, no siendo limitado a variantes de IEEE802.3.

El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura (Figura 2.1), puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

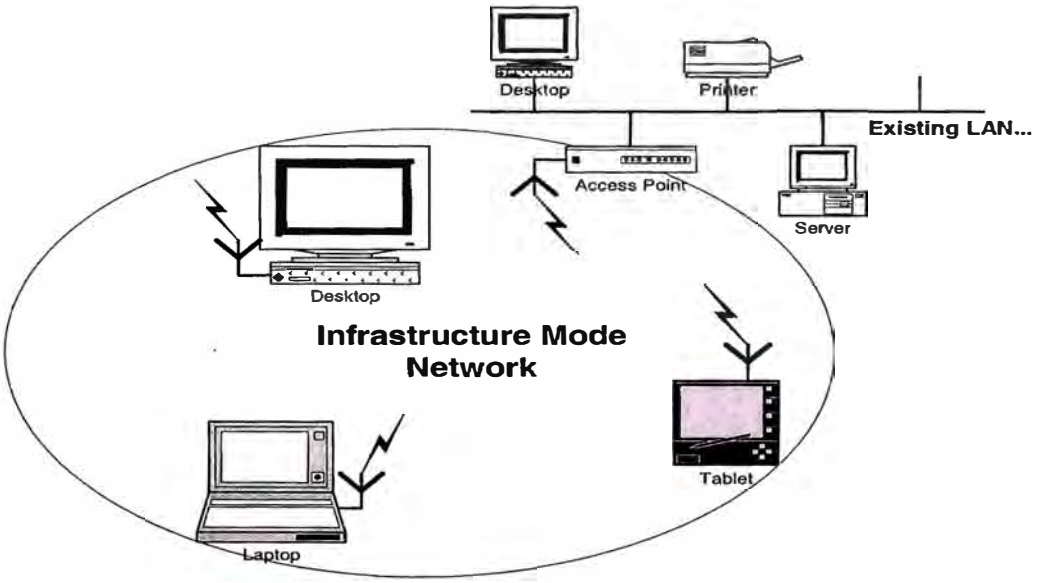


Figura 2.1: Red de la modalidad de infraestructura

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

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

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

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

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de

una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones. Observe que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

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

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

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria

por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

El punto de acceso (*access point*), controla el tráfico ya que dirige los datos de la red. y aumenta el alcance de la red inalámbrica puesto que ahora la distancia máxima no es entre estaciones sino entre cada estación y punto de acceso.

Para dar cobertura a una zona hay que instalar varios puntos de acceso de forma que las áreas que abarquen (llamadas celdas) se solapen parcialmente para que el usuario se pueda mover con libertad sin perder la conexión. Pueden utilizarse hasta tres coberturas superpuestas simultáneamente y sin interferencia, pero hay que tener en cuenta que deben tener frecuencias distintas, es decir, deben utilizar distintos canales. Debe existir una separación de 25MHz (5 canales) entre celdas con superposición de señales.

Se produce **diafonía** cuando los puntos de acceso detectan las señales de otros puntos adyacentes. En ese caso, el tráfico de la información proveniente de los distintos ordenadores colisiona en los puntos de acceso y ocurre una mezcla de información. Como los puntos de acceso necesitan un tiempo para clasificar la información combinada, hay una reducción considerable del rendimiento.

El número de usuarios en una WLAN es prácticamente ilimitado y puede ampliarse añadiendo más puntos de acceso. El ancho de banda es compartido por los usuarios como en las redes alámbricas, por lo que cuantos más usuarios hayan para el *access point*, más lento irá el tráfico.

Para que un cliente y un *access point* puedan comunicarse, requieren tener el mismo *SSID*, que es el nombre de la red compartida por las computadoras. Este nombre debe ponerse en un campo que aparece cuando se ejecuta el software de configuración.

El cliente localiza el punto de acceso con la señal más intensa, se asocia a él y configura el canal correspondiente a ese punto de acceso.

Este modo es aplicable en empresas en que usuarios móviles requieren acceso a Bases de Datos centralizadas o Aplicaciones cliente-servidor.

En el modo infraestructura, la red wireless consiste por lo menos en un punto de acceso conectado a un conjunto de estaciones wireless, que se pueden conectar a una red cableada. Dado que la mayoría de WLANs requieren un acceso a los servicios de la LAN cableada (servidor de ficheros, impresoras, Internet), operarán en modo infraestructura.

Las redes de infraestructura combinan diferentes elementos como puntos de acceso (*access point*) y puentes (*bridge*) para constituir redes de acceso y radioenlaces entre edificios o al interior de ellos. Los clientes acceden a la red por medio de sus tarjetas inalámbricas.

En la figura 2.2, se ilustra la utilización del *access point*, para el acceso de una computadora portátil en forma inalámbrica.

Figura2.2: Acceso inalámbrico de una PC portátil

En la figura 2.3 se ilustra la utilización del Bridge (unidad central) y antenas para la conexión de Redes LAN, ubicados en edificios distantes algunos kilómetros.

Figura 2.3: Conexión de 2 edificios (Redes LAN)

2.2.2. Modo ad hoc

El modo ad hoc (también llamado modo peer-to-peer) o IBSS, "*Independent Basic Service Set*" es simplemente un conjunto de estaciones 802.11 wireless que se comunican directamente con otra sin necesidad de un punto de acceso o cualquier conexión a una red cableada. Este modo es muy eficaz para montar una red wireless rápidamente en cualquier parte sin una infraestructura wireless, como en una habitación de un hotel, en un centro de convenciones, aeropuertos, o donde el acceso a la red cableada está bloqueado (como por ejemplo para consultores en la casa del cliente).

En una topología ad hoc (Figura 2.4), los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

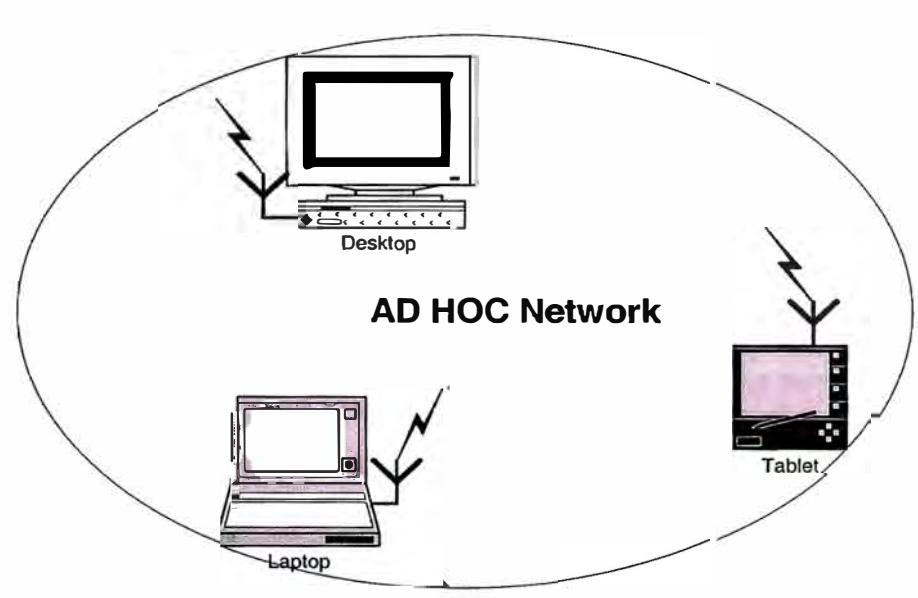


Figura 2.4: Red ad hoc

Por ejemplo, cuando se combinan con la nueva generación de software y soluciones par a par inteligentes actuales, estas redes inalámbricas ad hoc pueden permitir a los

usuarios móviles colaborar, participar en juegos de equipo, transferir archivos o comunicarse de algún otro modo mediante sus PCs o dispositivos inteligentes sin cables.

Es posible constituir redes Ad-hoc donde los portátiles o PC's móviles, se interconectan entre sí a través de sus tarjetas inalámbricas. Uno de ellos puede compartir su acceso al resto de la red.

2.3. Modelo OSI en redes inalámbricas

Considerando el modelo de referencia OSI, las redes Wireless se diferencian de las convencionales redes cableadas en las dos primeras capas, es decir, la capa física y la capa de enlace de datos, las cuales serán analizadas en los párrafos siguientes. La capa física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos (denominada MAC), se encarga de describir como se empacan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, ruteadores o compuertas para conectarse.

2.3.1. Nivel físico: tecnologías de transmisión

Existen diferentes tecnologías de transmisión utilizadas en redes inalámbricas, como por ejemplo la transmisión por ondas de luz (utilizadas para conectar dos LANs que están en edificios distintos), los infrarrojos y los basados en radio frecuencia. Estas dos últimas son las tecnologías que tienen su aplicación más directa en Wireless.

a) Infrarrojos

Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las estaciones se encuentran en un solo cuarto o piso, ya que no son capaces de atravesar paredes u objetos. Esta tecnología es la utilizada en los controles remotos de televisores o aparatos eléctricos que se usan en el hogar.

El mismo principio se usa para la comunicación de Redes, se utiliza un "*transreceptor*" que envía un haz de luz infrarroja, hacia otro que la recibe. La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente. Uno de los pioneros en esta área es Richard Allen, que fundó Photonics Corp., en 1985 y desarrolló un "Transreceptor Infrarrojo". Los primeros transreceptores dirigían el haz infrarrojo de luz a una superficie pasiva, generalmente el techo, donde otro transreceptor recibía la señal. Se pueden instalar varias estaciones en una sola habitación utilizando un área pasiva para cada transreceptor. El grupo de trabajo de Red Inalámbrica IEEE 802.11 está trabajando en una capa estándar MAC para redes infrarrojas.

Esta tecnología no es práctica para usuarios móviles ya que cualquier objeto que se interpusiera impediría la transmisión y siendo aplicadas en conexiones locales punto a punto y para las multipunto dentro de áreas limitadas (por ejemplo una habitación). La cobertura de esta tecnología está limitada a LAN o campus si se utilizan repetidores inalámbricos o puentes.

Pueden utilizarse tanto directamente (en línea de vista) como indirectamente (tecnología difundida/reflectiva). Esta última está limitada a cuartos individuales en zonas cercanas.

b) Ondas de radio

Para la utilización de esta tecnología en redes inalámbricas de radiofrecuencia , la FCC (*Federal Communication Comision*) permitió la operación sin licencia de dispositivos que utilizan 1Watt de energía o menos, en tres bandas de frecuencia : 902 a 928MHz, 2.400 a 2.4835GHz y 5.725 a 5.850GHz. Estas bandas de frecuencia, llamadas bandas ISM (*Industrial Scientific Medical*), estaban anteriormente limitadas a instrumentos científicos, médicos e industriales. Es una banda abierta.

Son fáciles de generar, pueden viajar distancias muy largas, penetrar edificios sin problemas y se utilizan tanto en interiores como en exteriores.

El transmisor y el receptor no tienen la necesidad de alinearse físicamente debido a que las ondas de radio son omnidireccionales, es decir que viajan en todas direcciones desde la fuente. Aún así, hay dos tipos de acuerdo a su direccionalidad.

b.1) Direccional

Estos sistemas también son llamados de Banda Angosta (*Narrow Band*). La antena de transmisión emite la energía electromagnética en un haz por lo que transmisor y receptor deben estar alineados.

A mayor frecuencia, más factible es concentrar la energía en un haz direccional por lo que la frecuencia de la transmisión debe ser mucho mayor que la utilizada en transmisiones omnidireccionales.

Se transmite y recibe la información en una radiofrecuencia determinada. El receptor filtra aquellas frecuencias que no son para él.

El cruce entre canales es evitado al situar diferentes usuarios en diferentes canales de frecuencia, por lo que si se tienen muchos usuarios no es viable.

En un sistema de radio, cuanto más separadas están las frecuencias unas de otras, mayor privacidad y ausencia de interferencia se logra.

b.2) Omnidireccional

Son los llamados sistemas de espectro extendido (*Spread Spectrum)* o de espectro amplio, es la técnica más utilizada en redes inalámbricas inicialmente desarrollada con el propósito de combatir las interferencias en las comunicaciones militares.

Consiste en dividir las señales informativas en distintas frecuencias que están en la banda reservada para aplicaciones generales industriales, científicas y médicas llamada banda ISM(*Industrial-Scientifc and Medical radiofrequency*) la cual ocupa la parte del espectro que va de 902 - 928MHz , 2.4 - 2.484GHz y 5.725 – 5.850GHz, frecuencias también utilizadas por hornos microondas y controles de puertas eléctricas entre otros (para estas frecuencias no es necesario licencia).

Si el receptor no está sincronizado a la frecuencia correcta, una señal de espectro extendido se tomaría como ruido de fondo. Además, con esta técnica se reduce la interferencia con otras señales no deseadas.

A continuación pasamos a comentar los tipos de espectro extendido que existen:

- **FHSS (*Frequency Hopping Spread Spectrum*) 2Mbps**

El espectro disperso por salto de frecuencia fue la primera implementación de espectro extendido y consiste en lo siguiente:

Los datos son divididos en paquetes enviados a frecuencias distintas de forma que sólo el que conoce el patrón de frecuencias (*Hopping Pattern*) a la que son enviados, pueda recibir la información. Para ello el receptor debe cambiar de frecuencia de forma síncrona con el transmisor de modo que se establecerá un canal lógico. Las reglas del FCC exigen usar 75 o más frecuencias por canal de transmisión con un tiempo máximo de permanencia de un salto en la misma frecuencia de 400ms.

Esta técnica reduce la interferencia porque una señal de un sistema de banda estrecha sólo afectará al espectro extendido si ambos están transmitiendo a la misma frecuencia al mismo tiempo, por tanto hace posible la transmisión de varios transmisores y receptores en la misma banda de frecuencia sin interferir entre ellos. Para un usuario externo la recepción de una señal FHSS es como ruido de corta duración.

FHSS se utiliza en distancias cortas, normalmente en aplicaciones punto a multipunto, donde se tienen una cantidad de receptores repartidos en un área relativamente cercana al punto de acceso. El estándar 802.11 lo utiliza, pero

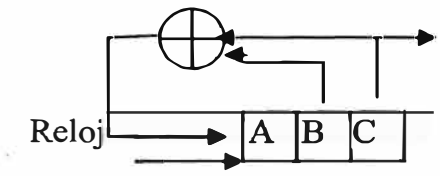
sobretodo es utilizado en la tecnología bluetooth (capaz de transmitir a velocidades de hasta 1Mbps).

- **DSSS (*Direct Sequence Spread Spectrum*) 11Mbps**

A diferencia de FHSS, esta técnica no requiere cambiar de frecuencia sino que cada transmisor modifica los datos con bits adicionales (un mínimo de 10) y sólo el que conoce el algoritmo de estos bits adicionales puede descifrar los datos

Se basa en una secuencia pseudoaleatoria llamada secuencia de dispersión donde a cada bit de la secuencia se le llama "chip", la tasa de bits de transmisión se denomina "tasa de chips" y el número de bits de la secuencia son el factor de dispersión.

La generación de la secuencia binaria pseudoaleatoria se puede realizar mediante registros de desplazamiento y puertas OR exclusivas. Con el siguiente ejemplo se pretende dar la idea de cómo se haría con un registro de desplazamiento y una OR exclusiva.



Secuencia binaria Pseudoaleatoria

Reloj	A	B	C
0	1	1	1
1	0	1	1
2	0	0	1
3	1	0	0
4	0	1	0
5	1	0	1
6	1	1	0

Se observa que no está, el estado 000 porque sino el registro de desplazamiento no cambiaría después de cada pulso de reloj. Hay un máximo de $2^n - 1$ estados para un registro de n bits y si la realimentación produce todos estos estados, se le llama

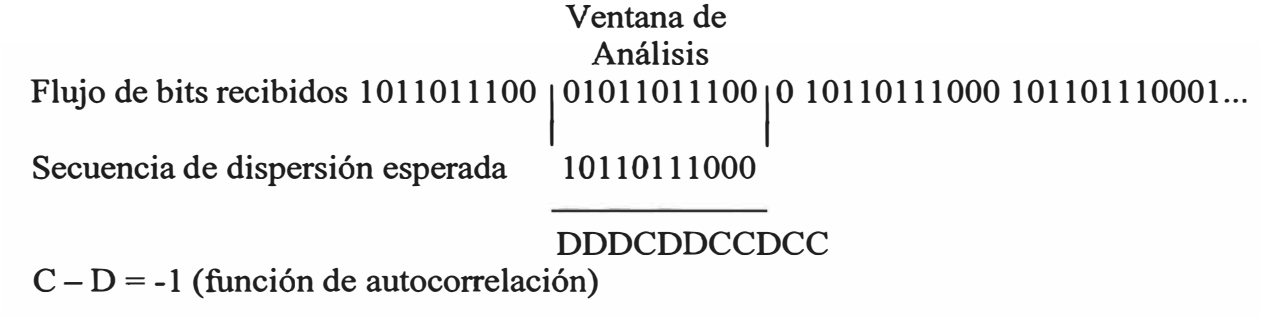
registro de desplazamiento de longitud máxima. La salida del bit más significativo del registro (en este caso C) será el que se utilizará como patrón, es decir como secuencia de dispersión. La secuencia para un 0 binario será la inversa que para un 1 binario.

La trama va precedida de un preámbulo que sirve para la sincronización. En este caso, la **sincronización** se realiza del modo siguiente:

El preámbulo (que tiene todos los bits a 1) se pasa por un registro de desplazamiento de n bits (donde n es el número de bits de la secuencia de dispersión) y se compara chip por chip con la secuencia conocida. Si los dos bits de una posición de chip son iguales, se dice que hay concordancia (C), sino hay una discordancia (D). Cuando todos los bits del registro de desplazamiento concuerden con los de la secuencia, es decir, cuando C – D = n, entonces la ventana de análisis está en la posición de la secuencia de dispersión y por tanto están sincronizados.

Ejemplo:

Supongamos la secuencia de dispersión 10110111000 (secuencia de Baker). La ventana de análisis (registro de desplazamiento) irá corriéndose una posición a la derecha examinando cada vez todos los bits del registro. Recordemos que la C indica concordancia, obsérvese el siguiente diagrama.



10110111000 |10110111000| 10110111000...

Secuencia de dispersión esperada 10110111000

CCCCCCCCCCC

C – D = +11 (función de autocorrelación)

Cuanto más grande sea esta secuencia, más grande es la probabilidad de que los datos iniciales puedan ser recuperados (aunque se requerirá más ancho de banda) y no hay necesidad de retransmisión en caso de bits dañados, gracias a unas técnicas estadísticas que existen en el radio transmisor que hace posible la recuperación de la señal original. Además, como cada transmisor emplea una secuencia distinta, es posible que varios transmisores operen en la misma área sin interferirse.

Debido al efecto de los chips, el DSSS está actualmente limitado a 2Mbps en la banda de 902MHz y a 10Mbps en la banda de 2.4GHz.

En E.E.U.U. y Europa, DSSS opera en el rango 2.4GHz hasta 2.4835GHz, esto implica un total de 83.5MHz que se dividen en 14 canales cada uno con 5MHz de ancho de banda. Cada país utiliza unos determinados canales (en el caso de España son los canales 10 y 11 que corresponden a 2.457 y 2.462GHz respectivamente).

En topologías de red en las que haya varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias si la separación entre frecuencias centrales es como mínimo 30MHz. Esto quiere decir

que de los 83.5MHz podemos obtener 3 canales independientes que pueden operar simultáneamente en una determinada zona geográfica con ausencia de interferencias.

DSSS cubre una distancia de 150 metros y se utiliza normalmente en aplicaciones punto a punto.

- **OFDM (*Wideband Orthogonal Frequency Division Multiplexing*)**

Esta es la técnica utilizada por el estándar 802.11a. Codifica la información en múltiples radiofrecuencias simultáneamente, es decir, parte una señal (portadora) de alta velocidad en decenas o centenas de señales de menor velocidad que son transmitidas en paralelo (subportadoras).

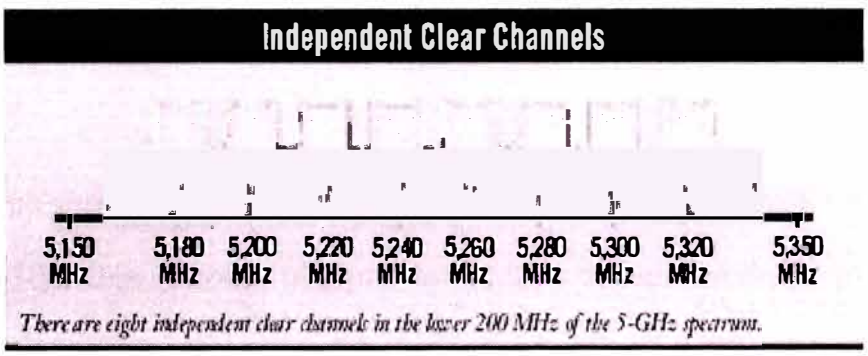


Figura 2.5: Tecnología OFDM

Cada portadora tiene un ancho de banda de 20MHz y es dividido en 52 subcanales siendo cada uno de 300KHz aproximadamente de ancho (ver figura 2.5). De estos canales, el COFDM (código OFDM) usa 48 para datos y los 4 restantes se usan para la corrección de errores.

En cuanto a los tipos de modulación se emplean:

BPSK (*Binary Phase-Shift Keying*), es usado para codificar 125Kbps de datos por canal, es decir, una tasa de datos de 6Mbps.

QPSK (*Quadrature Phase-Shift Keying*), dobla la cantidad de datos codificados produciendo una tasa de datos de 12Mbps.

16-QAM (16 *Level Quadrature Amplitude Modulation*), se logra una tasa de datos de 24 Mbps (codificando 4 bits por Hertz).

64-QAM permite obtener una tasa de datos de 54Mbps (produce 8 bits por ciclo o 10 bits por ciclo).

Hay que tener en cuenta que cuantos más bits por ciclo (Hertz) son codificados, más susceptible será la señal a la interferencia y a desvanecerse, de donde se puede deducir que con una tasa de datos de 54Mbps será más susceptible a la señal y a desvanecerse.

Se ofrece un modo propietario que combina dos portadoras para una tasa de datos teórica de 108Mbps y como mínimo de 72Mbps usando modo propietario de doble canal.

OFDM es tolerante al ruido y la señal que se transmite es difícil de descifrar.

Los equipos con tecnología OFDM son una buena solución en distancias moderadas para redes de información punto a punto, multipunto, acceso de alta velocidad a Internet, videoconferencia, telefonía, etc.

2.3.2. Nivel de enlace de datos: Protocolo CSMA/CA

La capa de enlace del 802.11 consiste en dos subcapas: *Logical Link Control* (LLC) y *Media Access Control* (MAC).

El estándar 802.11 utiliza el mismo LLC(control de enlace lógico) que el 802.2, pero el nivel MAC(Control de Acceso al Medio) es diferente.

En las redes inalámbricas podemos diferenciar 3 tipos de tramas:

Tramas de administración: tramas para transmitir información de administración.

Tramas de datos: usadas para transmitir datos.

Tramas de control: tramas que se usan para controlar el acceso al medio(RTS, CTS y ACK).

El 802.11 usa un protocolo un poco modificado del CSMA/CD(protocolo que regula como las estaciones Ethernet establecen el acceso al medio y como detectan y tratan las colisiones) que es conocido como CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), o el DCF (*Distributed Coordination Function*). CSMA/CA intenta evitar las colisiones usando ACK explícitos, es decir que la estación que recibe los datos envía un paquete ACK si ha recibido los datos correctamente; como se explica al hacer el análisis del protocolo CSMA/CA cuyo funcionamiento es el siguiente:

Una estación que desee transmitir mira si el medio esta ocupado(en este caso es el aire), si el canal esta libre, la estación esta autorizada a transmitir y entonces

transmite al medio sí este continua libre (después de haberse esperado 10ms para asegurar que las tramas van separadas al menos ese tiempo). Si por el contrario el canal esta ocupado, la estación dejará la transmisión para más tarde, esperando un tiempo aleatorio (periodo de contención) después de la transmisión de cada nodo, permitiendo cada nodo un acceso equitativo al medio.

Si el paquete transmitido se recibe correctamente (se comprueba el CRC), la estación receptora envía un ACK.

Si la estación emisora recibe el ACK se completa el proceso. Si el ACK no es detectado por la estación emisora, porque el paquete original no ha sido recibido correctamente ó porque el ACK se ha perdido, se asume que se ha producido una perdida y el paquete de datos se retransmite de nuevo después de esperar otro tiempo aleatorio.

Si no se utilizaran ACKs explícitos cabría la posibilidad de que varias estaciones estuvieran sondeando el canal y al detectar que esta libre simultáneamente intentara transmitir al mismo tiempo, provocando colisión.

Para mejorar la eficiencia posee reconocimiento positivo, retransmisión a nivel MAC (*Media Access Control*)y fragmentación.

Reconocimiento positivo:

El receptor envía el ACK para indicar que ha recibido el paquete satisfactoriamente. Si no es recibido o tiene errores, no responderá, es decir, no existe NACK. ACK se

envía transcurridos 5ms desde que recibió el dato, durante ese tiempo se comprueba el CRC de la trama recibida.

Retransmisión a nivel MAC:

Si el ACK no es recibido en un tiempo determinado, el emisor volverá a enviar el paquete.

Fragmentación:

Se da la posibilidad de dividir los paquetes en fragmentos que el receptor reunirá. Así se consigue reducir la probabilidad de error porque cuanto más grandes son, más probabilidad de error hay. También se consigue reducir el tiempo de retransmisión porque por cada fragmento correcto, el receptor enviará ACK y por tanto, si el emisor debe retransmitir, solo tendrá que volver a enviar el fragmento del que no recibió la correspondiente confirmación.

Pero surge un problema debido a que las redes con cable pueden escuchar a cualquier estación que transmita gracias al cable, pero en las redes inalámbricas, como el medio de transmisión es el aire, solo pueden abarcar una determinada área por lo que aparece el "Problema de la estación oculta o ruido oculto", que consiste en que dos estaciones en lados opuestos del punto de acceso pueden escuchar actividad del punto de acceso pero no de ellas, debido principalmente a la distancia o alguna obstrucción, lo que provocaría colisión. Para resolver este problema, 802.11 especifica un protocolo RTS/CTS (*Request To Send*, Petición de envío y *Clear To*

Send, permiso para enviar) opcional en la capa MAC. Este mecanismo funciona de la siguiente manera:

Una estación esperando para transmitir envía un paquete de control RTS(que contiene el ACK) y espera que el punto de acceso le conteste con un CTS sí el medio esta libre. Como todas las estaciones de la red pueden escuchar al AP, el CTS retrasa cualquier intento de transmisión.

Para entender mejor el problema de la estación oculta, veamos el siguiente ejemplo:

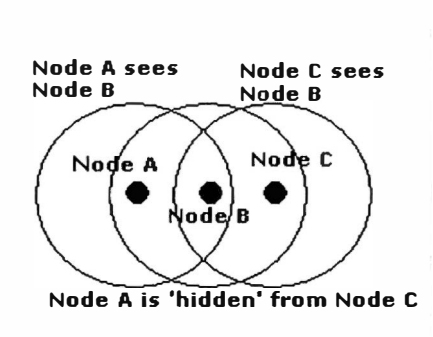


Figura 2.6: Problema de la estación oculta

Como podemos observar en la figura 2.6, A no se enteraría si C transmite y viceversa. Este problema se soluciona usando el **protocolo RTS/CTS** previo a la transmisión del paquete. Los pasos a realizar serían:

El nodo A envía un RTS (*Request To Send*), indicando el tamaño del paquete a enviar, que es oído por B (pero no por C).

B envía un CTS (*Clear To Send*), en el que se indica el tamaño del paquete a transmitir, que es oído por A y por C. Por tanto, C sabrá que no debe transmitir durante el tiempo equivalente a esos bytes.

Si todas las estaciones se escuchan entre sí, el uso de RTS/CTS perjudica porque se estarían haciendo transmisiones inútilmente.

Dependiendo del modelo que se utilice, este dispositivo implementa diferentes funciones, pero su misión elemental es adaptar la información transmitida en un medio inalámbrico a otro cableado, garantizando la calidad y seguridad de la transmisión.

Para servicios con límite de tiempo, por ejemplo vídeo y voz, existe una funcionalidad opcional llamada Función de Punto de Coordinación (PCF), que utiliza un acceso de mayor prioridad, así el AP controla el acceso al medio y emite peticiones de sondeo a las estaciones para transmitir datos. El punto de acceso sondeará cada estación en busca de datos, y después de un tiempo cambia a la siguiente estación. Ninguna estación puede transmitir hasta que sea elegida, y las estaciones reciben datos del punto de acceso solamente cuando sean elegidas. Por lo que el PCF da a cada estación un turno para transmitir en un momento predeterminado, garantizando un retraso o latencia máxima. El hecho de un AP tenga el control de acceso al medio y sondee las estaciones hace que no sea eficaz para redes grandes.

Si el modo de operación es el modo infraestructura con el PCF habilitado el tiempo se divide y el sistema puede estar en modo PCF y en el que está en el modo DCF.

El mecanismo de fragmentación de paquetes permite hacer control de congestión. El tamaño de los paquetes es importante en una LAN inalámbrica ya que la probabilidad de que un paquete se deteriore aumenta con su tamaño, si se deteriora

su retransmisión cuesta menos y en un sistema con salto de frecuencia, el medio se interrumpe por el salto por lo que los paquetes pequeños tienen menos posibilidad de que la retransmisión se posponga. Esta fragmentación reduce la necesidad de retransmisión en muchos casos y así mejora el funcionamiento radio de la red completa.

La capa MAC es la responsable de reconstruir los fragmentos recibidos, siendo el proceso transparente a los protocolos de nivel superior.

2.4. Seguridad en redes inalámbricas

Las redes inalámbricas por el uso de radiofrecuencia para la comunicación de datos, son muy vulnerables en lo referente a la seguridad de los mismos, debido a que cualquier computador con acceso inalámbrico que se encuentre a menos de 100 metros de un punto de acceso, podría tener acceso a una red que no le corresponde, inclusive se tienen técnicas para la ubicación de redes inalámbricas como warchalking y wardriving.

El *warchalking,* consiste en caminar por la calle con un computador portátil dotado de una tarjeta Wireless, buscando la señal de puntos de acceso. Cuando se encuentra uno, se hace una marca especial, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red.

El *wardriving*, localiza puntos de acceso inalámbrico desde un automóvil. Para éste fin se necesita de un computador portátil con una tarjeta Wireless, una antena

adecuada, un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas, que se consigue libremente en la Internet.

Es común encontrar redes inalámbricas protegidas adecuadamente con un firewall para su acceso a Internet, pero al interior de la red existen puntos de acceso inalámbrico desprotegidos e irradiando señal hacia el exterior del edificio. Una red inalámbrica segura, debería cumplir con los siguientes requisitos:

• Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.

• Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta y a la red, constatar que el cliente está autorizado para acceder a ella.

• Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Existen varios modelos de seguridad para redes inalámbricas, cada uno de ellos basados en protocolos de encriptación y autenticación, con sus propias ventajas y desventajas, logrando un nivel diferente de seguridad. A continuación, se hace una presentación de cada uno de ellos.

2.4.1. Modelos de seguridad

Los modelos utilizados en la implementación de seguridad para redes Wireless, son:

- ✓ WLAN LAN EXTENSIONS 802.1X/EAP
- ✓ WLAN LAN EXTENSIONS IPSec
- ✓ WLAN STATIC WEP Keys.

Estos modelos se desarrollan en base a las siguientes consideraciones: seguridad, aplicación, perfomance y usuario.

a) Modelo: WLAN LAN extensions 802.1x/EAP

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local cableadas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.

El protocolo 802.1x involucra tres elementos:

- Equipo del cliente, que desea conectarse con la red.
- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (*Remote Authentication Dial-In User Service*), cuya especificación se puede consultar en la RFC 2058.
- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto) que recibe la conexión del cliente. El autenticador actúa como intermediario entre el cliente y el servidor de autenticación, y solamente permite el acceso del cliente a la red cuando el servidor de autenticación así lo autoriza.

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. A continuación se explica cada una de las consideraciones para éste modelo

Seguridad

Una implementación 802.1x/EAP WLAN LAN opera en la capa de enlace (capa 2) para proveer autenticación, autorización, cuenta y encriptación, cuyo esquema se muestra en la figura 2.7:

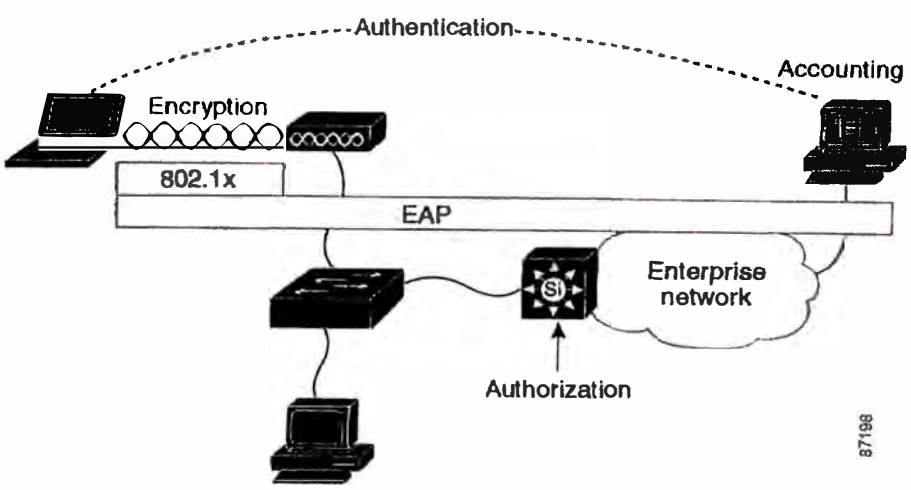


Figura 2.7: Esquema modelo 802.1x/EAP

- La autenticación ocurre entre el cliente y el servidor de autenticación. Diferentes tipos de EAP (EAP-CISCO, EAP-TLS, EAP-TTLS) son soportados y permiten elegir el tipo de autenticación.

- La encriptación está en la capa de enlace entre el cliente WLAN y el AP. Los mecanismos de encriptación Standard utilizados son *Wired Equivalent Privacy* (WEP), WEP plus TKIP, MIC. Se están desarrollando para uso futuro *Wi-Fi Protected Access* (WPA) y *Encriptación Estándar Avanzada* (AES).

- La autorización es controlada por los miembros VLAN en conjunto con los controles de acceso aplicado en el router de acceso.

- Las cuentas son provistas por el RADIUS de cuenta comunicada por el AP al RADIUS.

Aplicacion

Las WLAN se conectan en la capa de acceso. Una vez que el tráfico del cliente WLAN abandona el AP, representa el mismo tráfico que una Red cableada sujeta a los mismos controles de acceso, colas y ruteos. La no ejecución de algunas aplicaciones podrían deberse a políticas o limitaciones propias de las WLAN y no a la arquitectura 802.1x/EAP.

Perfomance

Las redes WLAN tienen un menor ratio de bits comparadas con las redes cableadas, diferencia que se puede disminuir usando herramientas de QoS disponibles en WLAN y la AP.

Usuario

Los diferentes tipos de EAP en 802.1x/EAP permiten a las empresas elegir el mecanismo de autenticación de acuerdo a los requerimientos de seguridad, permitiendo la integración a este mecanismo de usuarios ya existentes.

b) Modelo: WLAN LAN EXTENSIONS IPSec

La arquitectura de IPSec proporciona varios servicios de seguridad para el tráfico en la capa IP, en los entornos IPv4 e IPv6. Las RFCs describe los objetivos de los sistemas, sus componentes y cómo ellos encajan entre si y en el entorno de la capa IP. También describe los servicios de seguridad ofrecidos por los protocolos de IPSec, y cómo estos servicios pueden emplearse en el entorno IP. Las RFCs definen:

- Protocolos de seguridad
- Asociaciones de seguridad
- Manejo de claves
- Algoritmos de autentificación y cifrado

La gama de servicios de seguridad ofrecidos incluye control de acceso, fiabilidad de la conexión, autentificación del origen de los datos, protección contra réplicas y confidencialidad dentro de un flujo de tráfico limitado. Estos servicios son proporcionados a la capa IP, ofreciendo protección para IP y los protocolos de capas superiores.

Una de las ventajas de este modelo es su mecanismo de encriptación. IPSec incluye soporte de *Triple Data Encryption Standard* (3DES) y encriptaciones AES, mientras que 802.1x/EAP trabaja con WEP. La implementación de este modelo se considera más complicada, pues se basa en concentradores VPN.

Seguridad

Las características de este modelo son equivalentes a las soluciones 802.1x/EAP WLAN LAN referente a la autenticación, autorización, cuenta y encriptación, cuyo esquema se muestra en la figura 2.8

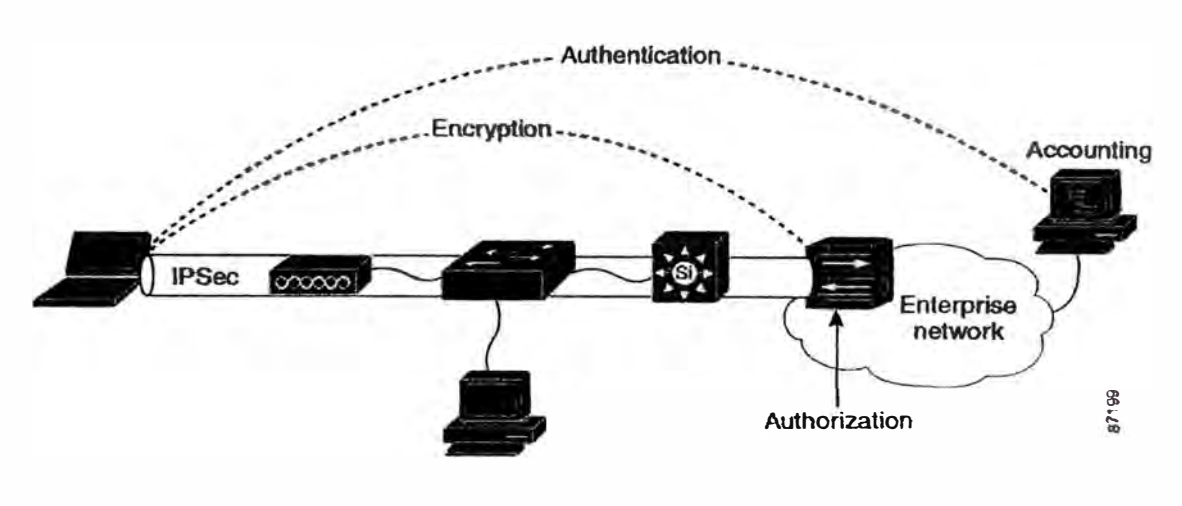


Figura 2.8: Esquema modelo IPSec

- La autenticación ocurre entre el cliente y el concentrador VPN. Múltiples tipos de autenticaciones son soportados con el IPSec framework.
- La encriptación está en la capa de red usando 3DES o AES y es negociado entre el cliente WLAN y el concentrador VPN.

- La autorización es controlada por el concentrador VPN y es determinada en el tiempo de autenticación. Se proveen políticas de Seguridad para el servidor de autenticación.
- Las cuentas son provistas por el RADIUS de cuenta o por el concentrador VPN en conjunto con el Servidor de autenticación.

Aplicación

El tráfico WLAN es transportado sobre el túnel IPSec al concentrador VPN, con las siguientes limitaciones:

Limitaciones de Protocolos: Solo el protocolo IP es soportado, no es multiprotocolo.

Traslado de direcciones: El cliente IPSec opera una forma de traslado de direcciones entre su dirección IP local y el ubicado por el concentrador VPN, lo que puede impactar en la operación de algunas aplicaciones.

No multicast: La conexión al concentrador VPN es punto a punto, por lo que aplicaciones multicast no son soportadas.

Perfomance

El uso del túnel IPSec VPN introduce algunas consideraciones:

Tamaño MTU: Puede ser ajustado para incorporar sobre cabeceras IPSec.

Proceso de sobre cabeceras: Los clientes incurren en procesamiento de sobre cabeceras que podrían ser no notificables en algunas plataformas.

Clasificación del Tráfico y consideraciones QoS: Los valores de tipos de servicios (*Type of Service*-ToS) y *Differenciated Services Code Point* (DSCP) son proyectados desde el paquete del cliente al paquete del IPSec, lo que permite establecer QoS.

Esquemas de Tráfico: Toda cola al concentrador VPN es administrable.

Usuario

Presenta las siguientes características:

Auto iniciación: El cliente VPN puede ser configurado automáticamente desde un rango particular de direcciones.

Integración OS: El cliente VPN captura la información, el nombre de usuario y password en el login.

c) Modelo: WLAN static wep keys.

La implementación de este modelo no es recomendada para propósitos generales de WLAN por la poca difusión de algoritmos de encriptación WEP y la dificultad de configuración y mantenimiento de claves estáticas.

Seguridad

El esquema de éste modelo, se muestra en la figura 2.9

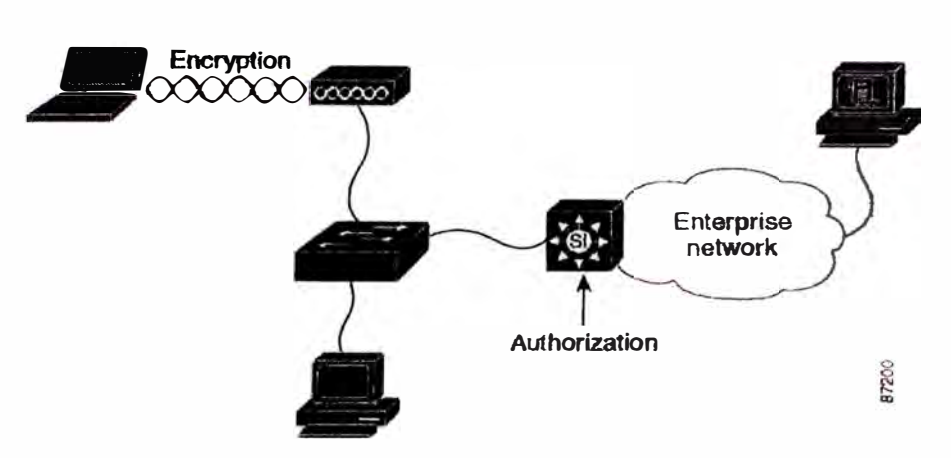


Figura 2.9: Esquema del modelo Static WEP Keys

- Autenticación débil, autentifica a un grupo de dispositivos y no a usuarios individuales.
- Encriptación limitada, está en la capa de enlace, entre el cliente WLAN y el AP. Los mecanismos de encriptación utilizables son WEP y WEP plus TKIP y MIC.

- Autorización limitada, es controlada por el concentrador VPN y es determinado en el tiempo de autenticación. Se proveen políticas de Seguridad para el servidor de autenticación.
- Cuenta no utilizable.

Aplicación

Las WLAN se conectan en la capa de acceso. Una vez que el tráfico del cliente WLAN abandona el AP representa el mismo tráfico que una red cableada sujeta a los mismos controles de acceso, colas y ruteos. La ejecución de aplicaciones están limitadas a los clientes con soporte *Static WEP*, las otras son bloqueadas.

Perfomance

Las redes WLAN tienen un menor ratio de bits comparadas con las redes cableadas, diferencia que se puede disminuir usando herramientas de QoS disponibles en WLAN y el AP.

Usuario

Static WEP no requiere autenticación.

2.4.2. Encriptación y autenticación

El modelo de seguridad más utilizado es el WLAN LAN extensión 802.1x/EAP cuyo proceso de encriptación esta basado en el algoritmo WEP y el Servidor de autenticación RADIUS.

a) Algoritmo de encriptación WEP – *Wired Equivalent Privacy*

WEP está basado en proteger los datos transmitidos por el medio de radiofrecuencia usando una clave de 40bits, un vector de inicialización de 24bits y un algoritmo de encriptación RC4. Cuando se habilita WEP, sólo se protege los datos del paquete y no las cabeceras, para que otras estaciones puedan escuchar a los datos de control necesarios para mantener la red. Sin embargo, las demás estaciones serán incapaces de desencriptar los datos de usuario.

Estos mecanismos ayudarán a evitar acceso a la red por usuarios no deseados, ya que con ellos se prueba que la estación que quiera unirse a la red conoce la clave actual, de forma similar a como se hace en una red cableada.

Una red cableada está dotada de una seguridad inherente en cuanto a que un posible intruso obtenga acceso a la red a través de una conexión por cable, lo que normalmente significa el acceso físico a la red de cables. Sobre este acceso físico se pueden superponer otros mecanismos de seguridad.

En una red inalámbrica, la libertad que obtienen los usuarios también se hace extensiva al riesgo de intrusos. Ahora, la red puede estar disponible en vestíbulos, salas de espera insegura, e incluso fuera del edificio. En un entorno doméstico, la red podría extenderse hasta los hogares vecinos si el dispositivo de red no adopta o no utiliza correctamente los mecanismos de seguridad ya que los datos viajan por el aire a través de ondas de radio.

Desde sus comienzos, 802.11 ha proporcionado algunos mecanismos de seguridad básicos para impedir que esta libertad mejorada sea una posible amenaza. Por ejemplo, los puntos de acceso (o conjuntos de puntos de acceso) 802.11 se pueden configurar con un identificador del conjunto de servicios (SSID). La tarjeta NIC también debe conocer este SSID para asociarlo al AP y así proceder a la transmisión y recepción de datos en la red. Esta seguridad, si se llegase a considerar como tal, es muy débil debido a estas razones:

- Todas las tarjetas NIC y todos los AP conocen perfectamente el SSID
- El SSID se envía por ondas de manera transparente (incluso es señalizado por el AP)
- La tarjeta NIC o el controlador pueden controlar localmente si se permite la asociación en caso de que el SSID no se conozca.
- No se proporciona ningún tipo de cifrado a través de este esquema.

Las especificaciones 802.11 proporcionan seguridad adicional mediante el algoritmo WEP (*Wired Equivalent Privacy*). WEP proporciona a 802.11 servicios de autenticación y cifrado. El algoritmo WEP define el uso de una clave secreta de 40 bits para la autenticación y el cifrado, muchas implementaciones de IEEE 802.11 también permiten claves secretas de 104 bits. Este algoritmo proporciona la mayor parte de la protección contra la escucha y atributos de seguridad física que son comparables a una red con cable.

Una limitación importante de este mecanismo de seguridad es que el estándar no define un protocolo de administración de claves para la distribución de las mismas. Esto supone que las claves secretas compartidas se entregan a la estación inalámbrica IEEE 802.11 a través de un canal seguro independiente del IEEE 802.11. El reto aumenta cuando están implicadas un gran número de estaciones, como es el caso de un campus corporativo.

Para proporcionar un mecanismo mejor para el control de acceso y la seguridad, es necesario incluir un protocolo de administración de claves en la especificación.

En la actualidad se está desarrollando el estándar 802.11i que trata de unificar todos los requisitos de seguridad del mercado.

La especificación 802.11i consta de tres elementos organizados en 2 capas. En la capa más baja, se ha mejorado los algoritmos de encriptación con el protocolo de integridad de clave temporal (TKIP) y el protocolo CBC-MAC (CCMP). Ambos protocolos de encriptación proporcionan mejora en la integridad de los datos sobre el protocolo WEP.

Sobre TKIP Y CCMP se sitúa el 802.11x, un estándar para el control de acceso basado en puertos. De la misma forma que el 802.11i, el 802.1x proporciona un marco de trabajo para la distribución de claves para la autentificación y encriptado robusto del usuario, ambas características ausentes del estándar original del 802.11.

Cuando observamos el 802.11i, es importante comprender que estos tres elementos trabajan juntos para formar un sistema seguro.

El 802.1x es un estándar basado en el control de acceso a red para el puerto. El estándar se puede aplicar tanto para redes cableadas como inalámbricas y proporciona un entorno de trabajo para la autentificación del usuario y distribución de la clave de encriptado. Se puede emplear para restringir el acceso a una red hasta que el usuario haya sido autentificado por ésta. Además, el 802.1x se usa en unión con algún protocolo de capa superior para realizar la verificación de credenciales y generación de las claves de encriptación.

b) Servidor de autenticación RADIUS

Para ofrecer una mayor seguridad de la proporcionada por WEP, se establece el control de acceso a redes basado en puerto que se utiliza para proporcionar acceso a red autenticado para las redes Ethernet. Este control de acceso a red basado en puerto utiliza las características físicas de la infraestructura LAN conmutada para autenticar los dispositivos conectados a un puerto LAN. Si el proceso de autenticación no se realiza correctamente, se puede impedir el acceso al puerto. Aunque este estándar se ha diseñado para redes Ethernet con cable, se puede aplicar a las redes LAN inalámbricas 802.11.

Para las conexiones inalámbricas, el punto de acceso actúa como autenticador para el acceso a la red y utiliza un servidor del Servicio de usuario de acceso telefónico de

autenticación remota (RADIUS) para autenticar las credenciales del cliente. La comunicación es posible a través de un "puerto no controlado" lógico o canal en el punto de acceso con el fin de validar las credenciales y obtener claves para obtener acceso a la red a través de un "puerto controlado" lógico. Las claves de que dispone el punto de acceso y el cliente como resultado de este intercambio permiten cifrar los datos del cliente y que el punto de acceso lo identifique. De este modo, se ha agregado un protocolo de administración de claves a la seguridad de 802.11.

Los pasos siguientes describen el planteamiento genérico que se utilizaría para autenticar el equipo de un usuario de modo que obtenga acceso inalámbrico a la red.

- Sin una clave de autenticación válida, el punto de acceso prohíbe el paso de todo el flujo de tráfico. Cuando una estación inalámbrica entra en el alcance del punto de acceso, éste envía un desafío a la estación.
- Cuando la estación recibe el desafío, responde con su identidad. El punto de acceso reenvía la identidad de la estación a un servidor RADIUS que realiza los servicios de autenticación.
- Posteriormente, el servidor RADIUS solicita las credenciales de la estación, especificando el tipo de credenciales necesarias para confirmar su identidad. La estación envía sus credenciales al servidor RADIUS (a través del "puerto no controlado" del punto de acceso).
- El servidor RADIUS valida las credenciales de la estación (da por hecho su validez) y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que sólo el punto de acceso pueda interpretarla.
- El punto de acceso utiliza la clave de autenticación para transmitir de manera

segura las claves correctas a la estación, incluida una clave de sesión de unidifusión para esa sesión y una clave de sesión global para las multidifusiones.

- Para mantener un nivel de seguridad, se puede pedir a la estación que vuelva a autenticarse periódicamente.
- Este planteamiento de 802.1x saca partido del uso extendido y creciente de RADIUS para la autenticación. Un servidor RADIUS puede realizar consultas en una base de datos de autenticación local si ello es adecuado para el escenario. O bien, la solicitud puede transmitirse a otro servidor para su validación. Cuando RADIUS decide que se puede autorizar el equipo en esta red, vuelve a enviar el mensaje al punto de acceso y éste permite que el tráfico de datos fluya hacia la misma. Un ejemplo real podría ser similar al siguiente:
  - Un usuario enciende su equipo portátil, con tarjeta 802.11, en un aeropuerto.
  - El equipo detecta que existen redes inalámbricas disponibles, elige la óptima y se asocia a ella.
  - El equipo envía las credenciales de usuario al punto de acceso para verificar que tiene permiso en esta red.
  - El usuario es, por ejemplo, HrY@bigco.com. BigCo ha adquirido acceso inalámbrico para todos sus usuarios en todos los aeropuertos del mundo.
  - El servidor RADIUS, que recibe la solicitud desde el punto de acceso, comprueba el paquete y descubre que procede de un usuario de BigCo.
  - A continuación, el servidor RADIUS pide a un servidor de BigCo que determine si esta persona es un usuario real y si le conceden acceso.

- Si el servidor de BigCo responde afirmativamente, se indica al punto de acceso que permita el flujo del tráfico del usuario.

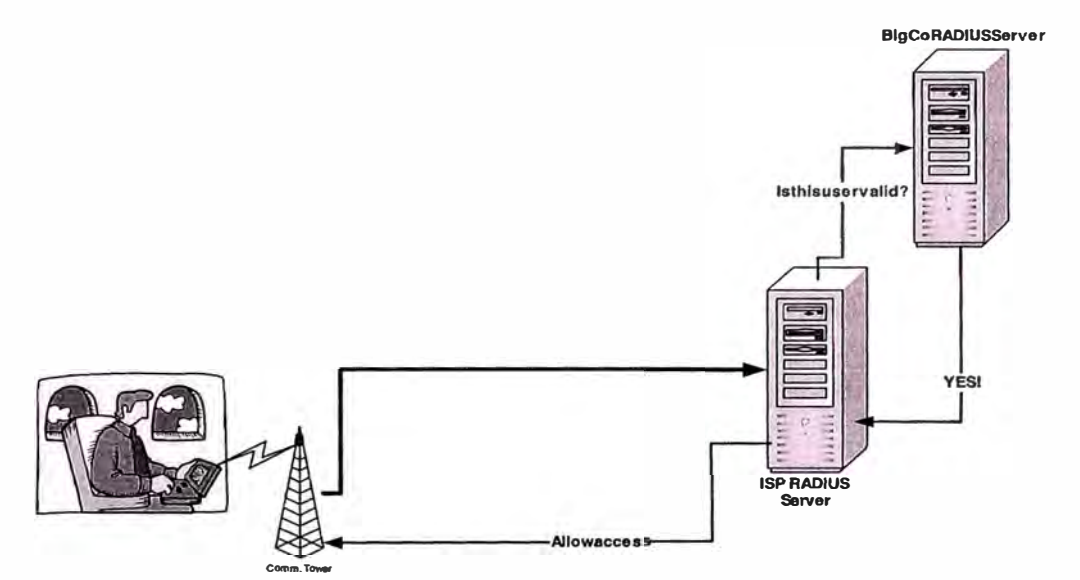


Figura 2.10: Ejemplo de escenario de acceso público

En la actualidad para Windows XP, Microsoft incluye una implementación del cliente 802.1X que mejora el servidor RADIUS de Windows y el servidor de autenticación de Internet (IAS), para admitir la autenticación de dispositivos inalámbricos.

c) Redes privadas virtuales (virtual private network VPN)

Una red privada virtual (*Virtual Private Network*, VPN) proporciona, mediante procesos de encapsulación y de cifrado, una red de datos privada sobre infraestructuras de telecomunicaciones públicas, como Internet. Las VPNs logran esto al permitir que se realice un túnel seguro a través de una red pública de tal forma que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que sólo están disponibles en las redes privadas.

Una vez establecido un túnel seguro, los datos pueden ser transmitidos con confianza y seguridad entre los dispositivos.

Las VPNs permiten a los usuarios conectarse en una forma segura a un servidor remoto utilizando la infraestructura de enrutamiento que proporciona una red pública (como Internet) y son recomendadas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

Desde la perspectiva del usuario, la VPN es una conexión punto a punto entre la computadora del usuario y un servidor corporativo. La naturaleza de la red intermedia es irrelevante, debido a que parece que los datos se estuvieran enviando sobre un enlace privado dedicado.

Existen tres tipos básicos de conexiones VPN:

Conexión Host a Red: Crea un túnel de transmisión entre una computadora y una red, desde cualquier lugar en Internet y es ideal para dispositivos móviles.

Conexión Red a Red: Crea un túnel de transmisión seguro entre dos redes, como dos oficinas de una misma compañía que se encuentran en ciudades diferentes.

Conexión Host a Host: Crea un túnel de transmisión seguro entre dos computadoras cualesquiera.

La implementación de una solución de red privada virtual, debe facilitar un acceso controlado a los recursos y a la información, es decir, debe permitir que los clientes

remotos autorizados se conecten fácilmente a los recursos corporativos dentro de una red y también que las oficinas remotas se conecten entre sí para compartir recursos e información, garantizando la privacidad e integridad de los datos que viajan por el Internet u otra red pública. Una solución de VPN debe proporcionar lo siguiente:

Autenticación: Verificar la identidad y restringir el acceso a la VPN. Proporcionando además registros de auditoria y contables.

Administración de dirección: Asignar una dirección al cliente en la red privada y deberá asegurarse que las direcciones privadas se mantengan así.

Cifrado de datos: Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

El cifrado se basa en dos componentes: un algoritmo y una llave. Un algoritmo criptográfico es una función matemática que combina texto plano u otra información inteligible con un cadena de dígitos llamados llave, para, producir el texto cifrado. La llave y el algoritmo usados son cruciales para el cifrado.

Cifrado de Claves Simétricas (una clave)

Este cifrado utiliza una clave única para el remitente y el destinatario. La clave es utilizada tanto para el cifrado como para el descifrado, también es llamada clave de sesión. Existen muchos algoritmos para el cifrado de claves simétricas; pero el objetivo siempre es el mismo: la transformación reversible de texto (sin cifrar) en

texto cifrado. La seguridad está basada en el tamaño de la clave. Cuanto mayor sea el tamaño de la clave, más claves habrá que probar para encontrar la clave correcta que descifre los datos, siendo por tanto, más difícil romper el algoritmo. La limitación de este método es la necesidad de distribuir la clave entre los participantes de una manera segura.

Cifrado de Claves Públicas (dos claves)

En el cifrado de claves públicas se usan dos claves: una pública y otra privada, que están relacionadas matemáticamente. En el cifrado de claves públicas, la clave pública puede intercambiarse libremente entre las partes o publicarse en un depósito público. Sin embargo, la clave privada sigue siendo privada. Los datos cifrados con la clave pública sólo pueden descifrarse con la clave privada. Los datos cifrados con la clave privada sólo pueden descifrarse con la clave pública. El cifrado de claves públicas proporciona un método eficiente para enviar a otra persona la clave simétrica que se usará cuando se realice una operación de cifrado simétrico sobre una gran cantidad de datos.

Administración de llaves: Consiste en generar y renovar las llaves de cifrado para el cliente y para el servidor. Los certificados digitales son "elementos" que permiten identificar las partes involucradas en una transacción telemática.

Soporte múltiple de protocolos: La solución deberá poder manejar protocolos comunes utilizados en las redes públicas. Estos incluyen Protocolo de Internet (IP), Central de paquete de Internet (IPX), etc.

La configuración de una red inalámbrica utilizando las VPN, debe considerar parte de la red que maneja el acceso inalámbrico aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

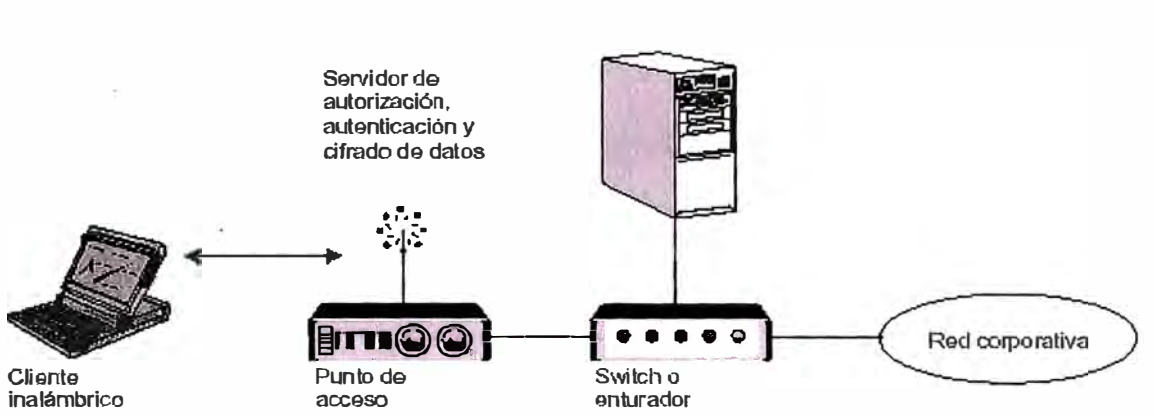


Figura 2.11: Estructura de una VPN para acceso inalámbrico seguro.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

2.5. Calidad de servicio WLAN - QoS

Calidad de Servicio (*Quality of Services* - QoS), significa la capacidad de una red de proveer un mejor servicio para seleccionar el tráfico de red sobre varias tecnologías.

Las tecnologías para QoS proveen un conjunto de bloques para negocios multimedia y aplicaciones de voz usadas en WANs y proveedores de servicios de red. La QoS permite a los administradores de red el nivel de servicio adecuado a los usuarios, a través de un SLA (*Service Level Agreement*). Habilita los recursos de red para ser compartidos eficientemente y maneja mejor las aplicaciones de misión crítica. Administra el tráfico en aplicaciones multimedia y voz, para asegurar que este tráfico recibe alta prioridad, mayor ancho de banda, menor retardo.

Las características para establecer un servicio de calidad son:

- Soportar ancho de banda para aplicaciones y usuarios críticos.
- Controlar los valores de Latencia y Jitter (requerido para tráfico en tiempo real).
- Administración y minimización de la congestión de la red.
- Configurar la prioridad del tráfico en la red.

2.5.1. Esquema QoS en Wireless

Hoy en día, las redes WLAN trabajan sobre ambientes empresariales y son usadas para transportar altos anchos de banda, aplicaciones multimedia y aplicaciones de datos sensibles en el tiempo, lo que conlleva a la necesidad de QoS Wireless.

Los dispositivos de calidad de servicio están soportadas por el protocolo IEEE 802.11e *Enhaced Distributed Coordination Function* - EDCF

Un esquema de calidad de servicio para aplicaciones de voz se muestra en la figura 2.12

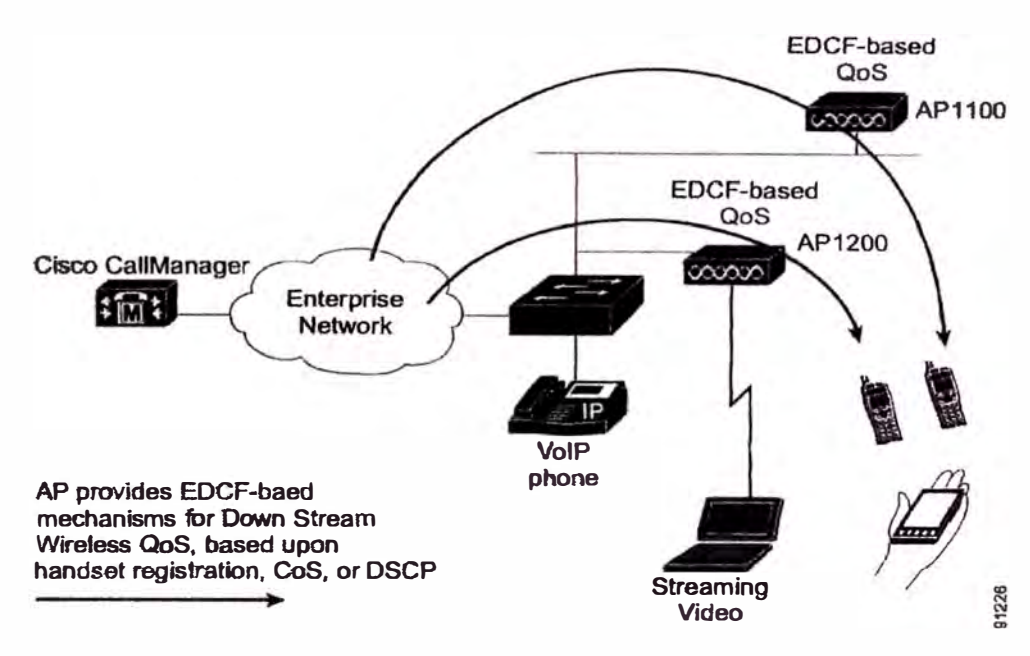


Figura 2.12: Esquema de QoS Wireless basado en EDCF

En la figura el AP provee EDCF, para que los diversos dispositivos utilicen el ancho de banda que les permita un óptimo funcionamiento.

2.5.2. Parámetros de QoS

La QoS está definida como la medida de la performance para un sistema de transmisión que refleja su calidad de transmisión y calificación de servicio. La calificación del servicio es un elemento crucial de la QoS. Para la implementación de QoS la infraestructura debe ser altamente calificada, la calidad de la transmisión es determinada por los siguientes factores:

- Latencia
- Jitter
- Loss

Latencia o retardo

Es la cantidad de tiempo que tiene un paquete para alcanzar el punto de recepción después que es transmitido desde el punto de envió, este periodo de tiempo es llamado retardo de fin a fin y puede ser dividido en dos áreas: Retardo fijo de red y retardo variable de red.

- **Retardo fijo de red.-** Incluye el tiempo de codificación y descodificación (para voz y video) como el mínimo tiempo requerido para que los pulsos eléctricos u ópticos puedan atravesar el medio hacia su destino.
- **Retardo Variables de Red.-** Se refiere generalmente a las condiciones de red, tal como congestión, que puede afectar el tiempo requerido para el transito.

Jitter

Jitter o variación del retardo, es la diferencia en los puntos finales de latencia de cada paquete. Por ejemplo si un paquete requiere 125ms para atravesar la red desde el punto origen al punto destino y el siguiente paquete requiere 150ms, para hacer el mismo viaje, entonces el jitter es calculado en 25ms

Loss

Loss o paquetes perdidos es una medida comparativa de los paquetes realmente recibidos del total que fueron transmitidos. Loss es expresado como el porcentaje de paquetes que fueron extraviados.

2.6. Equipos y dispositivos Wireless

2.6.1. Estación Wireless

Una Estación Wireless es un equipo (PC, PDA, Impresora, etc.) o recurso de red con capacidad para conectarse a través de ondas al punto de acceso central de la red. Normalmente poseerá una tarjeta con la tecnología inalámbrica.

2.6.2. Tarjeta de red (NIC network interface card)

Tarjetas de red o "TR", generalmente integrada a nuestro ordenador o conectada mediante un conector *Personal Computer Memory Card International Association* - PCMCIA o Universal Serial Bus – USB, si estamos en una computadora portátil o en un *slot Peripheral Component Integrated* - PCI si estamos en una computadora de

escritorio. Substituyen a las tarjetas de red *Ethernet o Token Ring* utilizadas en las redes convencionales. Recibirán y enviarán la información hacia su destino desde el ordenador en el que estemos trabajando. La velocidad de transmisión / recepción de los mismos es variable dependiendo del fabricante y de los estándares que cumpla.

Permiten conectar una gran variedad de dispositivos Wireless, algunas están basadas en la tecnología DSSS (*Direct Sequence Spread Spectrum*) y operan en la banda de 2.4GHz de acuerdo al estándar IEEE 802.11b asegurando total compatibilidad. Se tienen dos tipos de tarjetas de red:

- PCMCIA para PCs portátiles y PDA. Este es un producto estándar PCMCIA con antena atachada.
- PCI para PCs de escritorio, tienen generalmente un conector RP-TNC el cual puede ser conectado a antenas externas.

Otras operan a 5GHz ó 54Mbps bajo el estándar IEEE 802.11a y operan en las bandas UNII-1 y UNII-2. Algunos fabricantes como CISCO incluyen un software utilitario que permiten la configuración, monitoreo y administración de la tarjeta, los usuarios pueden configurar el canal, conjunto de servicios de identificación (SSID), clave WEP y el método de autenticación. Proveyéndose driver para los sistemas operativos mas populares como Windows 98, Windows 2000, Windows ME, Windows CE, Mac OS 9.x, Mac OS X y Linux.

2.6.3. *Access point* - AP

Un a*ccess point* o punto de acceso, es un dispositivo que posibilita la conexión de una estación *wireless* con una red de área local (LAN). Con un punto de acceso, cualquier estación *wireless* puede ser rápidamente integrada en una red cableada ya existente. El AP (actúa similarmente a un Hub), es el punto central de red para que se vean todos los equipos de la red inalámbrica WLAN.

Características:

- Potencia de transmisión 100 mW para 802.11b (1, 5, 20, 30, 50, 100 mW).
- Potencia de transmisión 40 mW para 802.11a (40, 30, 20, 20, 10, 5 mW).
- Configuración de la velocidad de datos
- Incorporación de antena

2.6.4. Workgroup bridges

Los *workgroup bridges* proveen conectividad a redes cableadas convencionales a un sitio central a través de una conexión inalámbrica. Algunos *workgroup bridge* soportan hasta una gama de dispositivos tales como PCs, impresoras y computadoras portátiles, a través de un HUB Ethernet o Switch conectados al puerto Ethernet. A continuación se ilustran dos aplicaciones de los *workgroup bridges*.

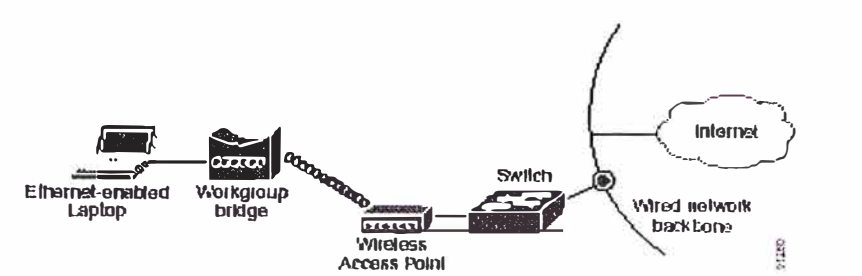


Figura 2.13: Aplicación 1 - Usuario de Ethernet móvil

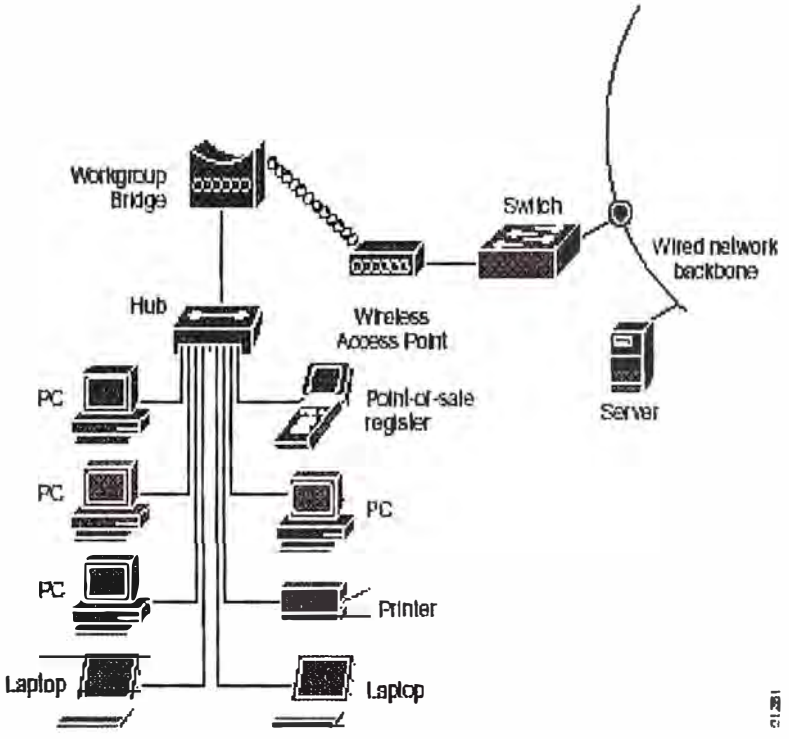


Figura 2.14: Aplicación 2 - Workgroup Remoto

2.6.5. Wireless bridges

Los *wireless bridges* o simplemente *bridges* son usados para conectar en forma inalámbrica dos redes ubicadas en dos edificios diferentes. Cómo se aprecia en la figura 2.15 con una apropiada selección de antenas y una línea de vista limpia, el rango se puede extender hasta 25 millas a 11Mbps. Se puede observar que solo los

bridges tienen la capacidad de extender el rango. Operando de acuerdo a las especificaciones del estándar IEEE 802.11 y con una correcta selección de la potencia de transmisión, cable y antena. El alcance de un AP operando en el estándar 802.11b está limitado a una milla.

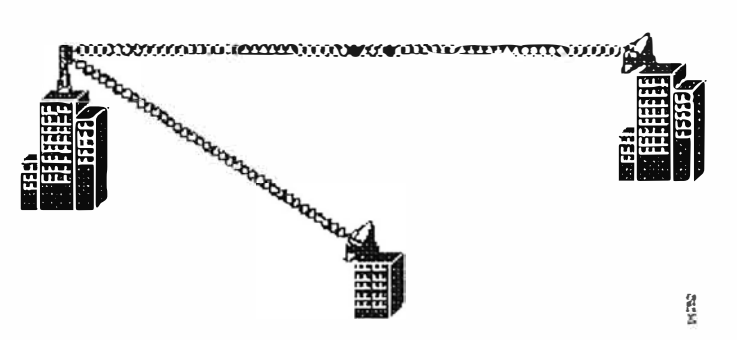


Figura 2.15: Aplicación típica de un Bridge, conexión de redes (edificios) en un área Metropolitana o Campus

Nota: Los APs no pueden ser usados para conectar dos redes cableadas.

2.6.6. Antenas

Son dispositivos que nos permiten dar un mayor alcance a una señal de radio. Se dividen en dos tipos: direccionales y omnidireccionales.

a) Antenas direccionales

Envían la información a una cierta zona de cobertura, a un ángulo determinado, es decir, orientan la señal en una dirección determinada, 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. Se utilizan para unir dos puntos a largas distancias, ya que ilumina un área concreta pero con un haz más intenso. En la figura 2.16 se muestra la antena direccional HG2424G y en la tabla 2.2 sus características.

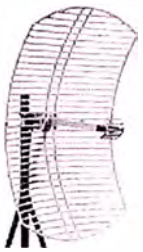


Figura 2.16: Antena HG2424G

Características Antena HG2424G

Tipo	**Direccional**	
Apta para interiores	No	
Apta para exteriores	Si	
Herrajes incluidos	Si	
Ganancia	24	dBi
Cobertura vertical	8	Grados
Cobertura horizontal	8	Grados
Alcance	10000	metros *
Dimensiones : Alto	100	Cm
Dimensiones : Ancho	60	Cm
Dimensiones : Profundo	12	Cm
Conectores y cables	incluidos	

Tabla 2.2

La antena tiene un cable de 0.50 metros terminado en un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable *Pigtail*.

b) Antenas omnidireccionales

Envían la información teóricamente a los 360 grados, es decir, en todas las direcciones, 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. En la figura 2.17 se muestra una antena omnidireccional y en la tabla 2.3 sus características.

Figura 2.17: HGV2409U HyperG Omnidireccional 8.5dBi Exterior

Características antena HGV2409U HyperG

Tipo	**OmniDireccional**	
Apta para interiores	No	
Apta para exteriores	Si	
Herrajes incluidos	Si	
Ganancia	8.5	dBi
Cobertura vertical	15	grados
Cobertura horizontal	360	grados
Alcance	900	metros *

Dimensiones : Alto	50	cm
Dimensiones : Ancho	2	Cm
Dimensiones : Profundo	2	Cm
Conectores y cables	Incluidos	

Tabla 2.3

La antena tiene directamente un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable *Pigtail.*

CAPÍTULO III

MODELO WIRELESS PROPUESTO

En el presente capitulo se hará la descripción de 2 propuestas de modelos de red inalámbricas, uno de los cuales será tomado en un futuro para su implementación. El primer modelo, es trabajado con productos del fabricante NetKrom Technologies cuyos dispositivos son de costo relativamente bajo, modelo donde se interconectan 8 puntos por medio de 7 enlaces, quedando 4 puntos para ser conectados vía línea dedicada, por lo cual no se toma la propuesta en el análisis de factibilidad, que se hace en el capitulo IV. El segundo modelo se hace en función al fabricante Cisco Technologies líder mundial en soluciones de redes, cuyos productos son menos económicos, pero tienen la garantía de la marca y de contar con un staff de profesionales a nivel mundial para el soporte técnico respectivo.

El modelo 2 propuesto en función a productos Cisco como el *bridge* Cisco Aironet 1300, es el tomado en cuenta para hacer el análisis de factibilidad y en el que se interconectan las 12 sedes, alquilándose adicionalmente los aires de 3 edificaciones que son usados como *Backbone* para la interconexión de las 4 sedes no conectadas en el modelo 1, como se describe en las siguientes secciones.

3.1. Consideraciones para la determinación del modelo

Para la determinación del modelo se ha considerado la evaluación de los siguientes parámetros: velocidad de operación, distancia entre las sedes y las líneas de vista entre cada uno de los locales adyacentes.

3.1.1. Parametros o variables consideradas

En el diseño de una red inalámbrica, se deben tener en cuenta los siguientes criterios:

- ✓ Es necesaria una relación señal-interferencia, para una comunicación correcta.
- ✓ Se requiere de un margen expresado en estadísticas para generar esta relación, aún en niveles de señal variables.
- ✓ La posición de las antenas que realizan la transmisión, la cual puede ser imitada por las estaciones y perfectamente controlada por puntos de acceso fijos.
- ✓ La función de la distancia para el nivel de la señal, está dada por el valor promedio de la señal, considerando las diferencias en la altura de la antena, de los terminales y los impedimentos naturales en la trayectoria.

a) Factor de distancia.

El promedio de inclinación de curva es reconocido por tener un exponente correspondiente a 35-40 dB/Decena para una extensión lejana y de propagación no óptica. Para distancias cortas el exponente es más cerca al espacio libre o 20 dB/Decena. El aislamiento de estaciones simultáneamente activas con antenas omni-direccionales puede requerir factores de reuso de 49 o más en espacio libre. La

distancia de aislamiento trabaja muy bien con altos porcentajes de atenuación media. Dependiendo de lo disperso del ambiente, la distancia de aislamiento en sistemas pequeños resulta ser en algunos casos la interferencia inesperada y por lo tanto una menor cobertura.

b) Alcance

Para poder implementar nuestra red, sería deseable que fuese igual a nuestras redes cableadas anteriores, tanto en prestaciones como en alcance. El alcance va a ser un elemento fundamental a la hora de elegir una u otra tecnología inalámbrica, ya que mayor alcance puede significar mayor flexibilidad, y menores costes de instalación si podemos cubrir más espacio con menos puntos de acceso.

Por definición de los estándares el alcance es comparable a la de un medio cableado para el caso de utilizar IEEE802.11b aproximadamente de 100m con una velocidad de 11Mbps con unas buenas condiciones ambientales. Pero para el caso de ir hacia mayores velocidades hemos de utilizar tecnología basada en 11a u 11g. En el caso del estándar 11a estamos en una tecnología que funciona a mayores frecuencias, y por tanto con necesidad de una mayor potencia de envío para la misma distancia. Además, transmisiones a tan alta frecuencia llevan implícito una alta energía, siendo muy fácil alterar la señal, por cualquier ruido o interferencia. De ahí que podemos sacar importantes conclusiones a la hora de comparar 11b con 11a, este segundo necesariamente tendrá un menor alcance.

De hecho, para mantener 54Mbps es necesario un radio máximo de 10m respecto del AP, minúsculo si comparamos a 11b cuya máxima velocidad se mantiene a los 100m.

La Tabla 3.1 provee una comparación de la velocidad de transmisión del dato y el rango de alcance asociado a los estándares inalámbricos 802.11a y 802.11b wireless. Los valores del rango de alcance son los típicos máximos, pero éste varia normalmente hacia abajo dependiendo sobre todo del medio ambiente, por ejemplo el alcance se reduce si se encuentran obstáculos como edificios con estructura metálica.

Comparación de la velocidad de bit y el rango para 802.11a y 802.11b

Bit Rate (en Mbps)	Rango para 802.11b (in feet)	Rango para 802.11a (in feet)
1	350	
2	250	
3.5	180	
6		170
9		150
11	140	
12		140
18		130
24		120
36		100
48		80
54		60

Tabla 3.1

La Figura 3.1, ilustra el área de cobertura de un AP 802.11b a una velocidad máxima de 11Mbps, sobrepuesto con un AP 802.11a a una velocidad máxima de 54Mbps.

Esta comparación muestra la real diferencia en rango del 802.11b y 802.11a. Se requieren diez AP 802.11a para cubrir un área similar al de un AP 802.11b.

La diferencia del área cubierta, representa a favor del 802.11a una ganancia potencial de aproximadamente 49 veces, es decir, la capacidad de una red 802.11a es significativamente mayor.

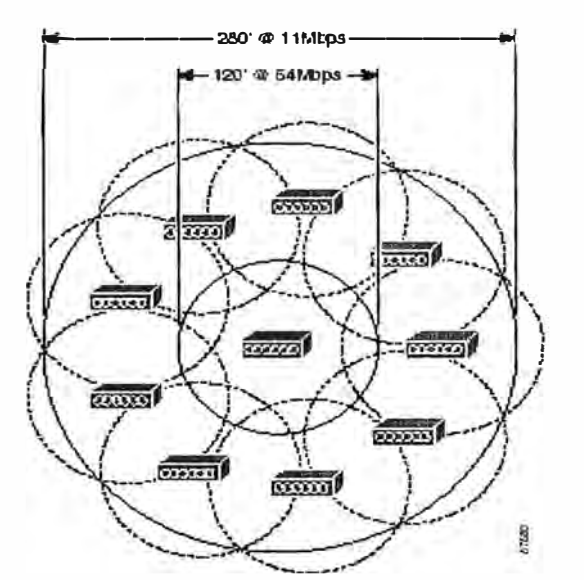


Figura 3.1: Diferencia de Cobertura entre 802.11a y 802.11b

c) Puntos de acceso

La infraestructura de un punto de acceso es simple: "Guardar y Repetir", son dispositivos que validan y retransmiten los mensajes recibidos. Estos dispositivos pueden colocarse en un punto en el cual puedan abarcar toda el área donde se encuentren las estaciones. Las características a considerar son:

1.- La antena del repetidor debe de estar a la altura del techo, esto producirá una mejor cobertura que si la antena estuviera a la altura de la mesa.

2.- La antena receptora debe de ser más compleja que la repetidora, así aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente.

Un punto de acceso compartido es un repetidor, al cual se le agrega la capacidad de seleccionar diferentes puntos de acceso para la retransmisión. (esto no es posible en un sistema de estación-a-estación, en el cual no se aprovecharía el espectro y la eficiencia de un sistema basado en puntos de acceso)

La diferencia entre el techo y la mesa para algunas de las antenas puede ser considerable cuando existe en esta trayectoria un obstáculo o una obstrucción. En dos antenas iguales, el rango de una antena alta es 2x-4x, más que las antenas bajas, pero el nivel de interferencia es igual, por esto es posible proyectar un sistema basado en coberturas de punto de acceso, ignorando estaciones que no tengan rutas de propagación bien definidas entre si.

Los ángulos para que una antena de patrón vertical incremente su poder direccional de 1 a 6 están entre el 0 ° y los 30° bajo el nivel horizontal, y cuando el punto de acceso sea colocado en una esquina, su poder se podrá incrementar de 1 a 4 en su cobertura cuadral. El patrón horizontal se puede incrementar de 1 hasta 24 dependiendo del medio en que se propague la onda. En una estación, con antena no

dirigida, el poder total de dirección no puede ser mucho mayor de 2 a 1 que en la de patrón vertical. Aparte de la distancia y la altura, el punto de acceso tiene una ventaja de hasta 10dB en la recepción de transmisión de una estación sobre otra estación.
Estos 10dB son considerados como una reducción en la transmisión de una estación, al momento de proyectar un sistema de estación-a-estación.

d) Aislamiento en sistemas vecinos.

Con un proyecto basado en puntos de acceso, la cobertura de cada punto de acceso es definible y puede ser instalado para que las paredes sean una ayuda en lugar de un obstáculo. Las estaciones están recibiendo o transmitiendo activamente muy poco tiempo y una fracción de las estaciones asociadas, con un punto de acceso, están al final de una área de servicio; entonces el potencial de interferencia entre estaciones es mínimo comparado con las fallas en otros mecanismos de transmisión de gran escala.

e) Modulación de radio.

El espectro disponible es de 40MHz, según el resultado de APPLE y 802.11. La frecuencia es "desvanecida" cuando en una segunda o tercera trayectoria, es incrementada o decrementada la amplitud de la señal. La distribución de probabilidad de este tipo de "desvanecimientos" se le denomina "*rayleigh*". El desvanecimiento *rayleigh,* es el factor que reduce la eficiencia de uso del espectro con pocos canales de ancho de banda.
Si es usada la señal de espectro expandido, la cual es 1 bit/símbolo, la segunda o tercera trayectoria van a causar un "desvanecimiento" si la diferencia de la

trayectoria es más pequeña que la mitad del intervalo del símbolo. Por ejemplo, una señal a 10Mbs, necesita de 0.1 segundo de tiempo para propagar la señal a 30mts. Diferencias en distancias mayores de 5mts. Causan mayor interferencia entre símbolos que el causado por el "desvanecimiento". Si el símbolo es dividido en 7bits, el mecanismo ahora se aplicará a una séptima parte de 30mts. (4 metros aproximadamente), una distancia en la trayectoria mayor de 4 metros no es causa de "desvanecimiento" o de interferencia entre símbolos.

El promedio de bits debe de ser constante, en el espacio localizado en el espectro y el tipo de modulación seleccionado. El uso de ciertos símbolos codificados, proporcionarán una mejor resolución a la longitud de trayectoria.

Un espectro expandido de 1 símbolo y cada símbolo con una longitud de 7, 11,13, 31 bits, permitirá una velocidad de 10 a 2Mbps promedio. El código ortogonal permite incrementar los bits por símbolo, si son 8 códigos ortogonales en 31 partes y si se incluye la polaridad, entonces es posible enviar 4 partes por símbolo para incrementar la utilización del espacio.

La canalización y señalización son métodos que compiten entre sí por el uso de códigos en el espacio del espectro expandido. Algunos de los códigos de espacio pueden ser usados por la canalización para eliminar problemas de superposición.

El espectro expandido puede proporcionar una reducción del "desvanecimiento" *rayleigh*, y una disminución en la interferencia a la señal para que el mensaje sea transmitido satisfactoriamente, lo cual significa que se reduce el factor de reuso.

Para una comunicación directa entre estaciones de un grupo, cuando no existe la infraestructura, una frecuencia común debe ser alternada para transmisión y recepción. La activación, en la transmisión no controlada, por grupos independientes

dentro de una área con infraestructura definida, puede reducir substancialmente la capacidad de organización del sistema.

f) Eficiencia del tiempo.

El tiempo es importante para poder maximizar el servicio, al momento de diseñar la frecuencia en el espacio. El uso del tiempo está determinado por los protocolos y por los métodos de acceso que regularmente usen los canales de transmisión de la estación.

g) Limite de la longitud del paquete y su tiempo.

Cuando el paquete es más pequeño, la proporción del tiempo usado al accesar el canal, es mayor, aunque la carga pueda ser pequeña para algunas funciones, la transferencia y descarga de archivos son mejor administrados cuando la longitud del paquete es de buen tamaño, para minimizar el tiempo de transferencia.

En paquetes grandes, se incrementa la posibilidad de que el paquete tenga errores en el envío, en sistemas de radio el tamaño aproximado ideal es de 512 octetos o menos, un paquete con una longitud de 100-600 octetos puede permitir la salida oportuna de respuestas y datagramas prioritarios junto con los datagramas normales.

Es necesario proveer formas para dividir los paquetes en segmentos dentro de las redes inalámbricas. Para un protocolo propuesto, el promedio de mensajes transferidos, es mayor para el tráfico originado por el "saludo inicial", que el originado por el punto de acceso. En este promedio se incluyen campos de dirección de red y otras funciones que son agregadas por el protocolo usado y no por el sistema de radio.

El mensaje más largo permitido para superar un retardo de acceso de 1.8 seg. y un factor de reuso de 4, utiliza menos de 600 seg. Un mensaje de 600 octetos utiliza 400 segundos a una velocidad de transmisión de 12Mbps, los 200 segundos que sobran pueden ser usados para solicitar requerimientos pendientes. El tiempo marcado para un grupo de reuso de 4 puede ser de 2,400 seg. Este tiempo total puede ser uniforme, entre grupos comunes y juntos, con 4 puntos de acceso. Sin embargo la repartición del tiempo entre ellos será según la demanda.

Las computadoras necesitan varios anchos de banda dependiendo del servicio a utilizar, transmisiones de datos, de vídeo, de voz, etc. La opción es, si:

- El medio físico puede multiplexar de tal manera que un paquete sea un conjunto de servicios.
- El tiempo y prioridad es reservado para el paquete y los paquetes relacionados con el, la parte alta de la capa MAC es multiplexada.
- La capacidad de compartir el tiempo de estos dos tipos de servicios ha incrementado la ventaja de optimizar la frecuencia en el espacio y los requerimientos para armar un sistema.

Las tres capas físicas originalmente definidas en el 802.11 incluyen dos espectros de radio y una especificación de infrarrojos. Los estándares basados en radio operan dentro de la banda 2.4GHz. Estas bandas de frecuencia son reconocidas por los reguladores internacionales, como FCC (USA), ESTI (Europa), y la MKK (Japón), como operaciones de radio sin licencia, para usos científicos, militares e industriales. Las técnicas de espectro ensanchado, además de satisfacer los requerimientos mínimos, aumentan la seguridad, elevan el *throughput* y permiten que varios

productos inconexos compartan el espectro sin cooperación explícita y con interferencia mínima.

Recordemos que el estándar original 802.11 define velocidades de 1 y 2 Mbps vía ondas de radio usando FHSS (frequency hopping spread spectrum) o DSSS (direct sequence spread spectrum); resaltando además, que FHSS y DSSS son mecanismos de señalización fundamentalmente diferentes y que no pueden interoperar entre ellos.

La principal contribución del 802.11b al estándar de WLANs era estandarizar el soporte de la capa física para dos nuevas velocidades, 5.5Mbps y 11Mbps. Especificando el 802.11b, la modulación *Complementary Code Keying* (CCK), que consiste en un conjunto de 64 palabras código de 8 bits. Como conjunto, estas palabras código tienen propiedades matemáticas únicas que les permiten distinguirse correctamente uno de otra por un receptor incluso en presencia de un ruido importante e interferencia multicamino. La tasa de 5.5Mbps usa el CCK para codificar 4 bits por portadora, mientras que la tasa de 11Mbps codifica 8 bits por portadora. Ambas velocidades usan la técnica de modulación QPSK y señal a 1.375Mbps, obteniéndose así altas tasas de datos.

h) Propagación de señales

Una onda de 5GHz tiene aproximadamente la mitad de longitud que una onda de 2.4Ghz. Las ondas cortas tienen mejor propagación a través del agua. Estando el cuerpo humano constituido en un 95% de agua, en áreas de alta densidad de

personas, los dispositivos Wireless 802.11a que operan a 5GHz son mejores en términos de señal de propagación que dispositivos semejantes de 802.11 que operan a 2.4GHz, pero tienen la desventaja de ser vulnerables a la absorción por materiales de construcción de edificios como el concreto.

i) Consideraciones de antenas

Las opciones de antena son variadas para dispositivos de 2.4GHz y 5GHz. Actualmente las regulaciones disponen que las antenas deben estar integradas a los dispositivos de transmisión a 5Ghz, por tanto, los dispositivos 802.11a no tienen antenas removibles de ellos. Para dispositivos de transmisión a 2.4GHz se pueden tener antenas integradas o conectadas a través de cables, siendo la ubicación de las mismas un parámetro muy importante para la curación de las mismas. La restricción impuesta para 5GHz hace que su configuración sea más complicada, que tenga un menor rango y que su costo de implementación sea muy alto.

Actualmente se tienen productos que pueden operar en UNII-1 y UNII-2 en forma separada o simultáneamente. Cuando la operación es simultanea, las regulaciones de antenas fijadas para UNII-1 se aplican a estos productos.

Asumiendo ambientes equivalentes, con la misma potencia de transmisión, ganancia de antena, 2.4Ghz ofrece el doble del rango que 5GHz. Esto es explicado físicamente por la propagación de ondas de radio que establece que en condiciones

similares, una onda de alta frecuencia tiene un menor rango que una onda de menor rango.

3.1.2. Criterios para la seleccion de tecnologia

En general la tecnología 802.11b a 2.4GHz tiene ventajas sobre 802.11a, básicamente por dispone de un mayor rango de dispositivos, como se observa en la Tablas 3.2, tabla 3.3 y Figura 3.2, teniéndose las siguientes razones para esta diferencia:

- La longitud de onda de 2.4GHz es aproximadamente el doble que la onda de 5GHz.

- Las ondas de 5GHz son más vulnerables a la absorción por materiales de construcción de edificios tales como la piedra de pared y el concreto.

- Las Regulaciones restringen la potencia de transmisión y posibilidades de antena en el rango de 5GHz.

- Con rango reducido, las compañías deben tener un mayor número de APs en 802.11 para cubrir un área designada, lo que conllevaría a altos costos de hardware.

Rango de valores Típicos para 802.11b con Antena Rubber Duck

Data Rates (Mbps)	Indoor Range (Feet)	Outdoor Range (Feet)
1	350	2000
11	150	800

Tabla 3.2

Rango de valores típicos para 802.11a con OmniAntenna

Data Rates (Mbps)	Indoor Range (Feet)	Outdoor Range (Feet)
6.0	170	1000
18.0	130	600
54.0	60	100

Tabla 3.3

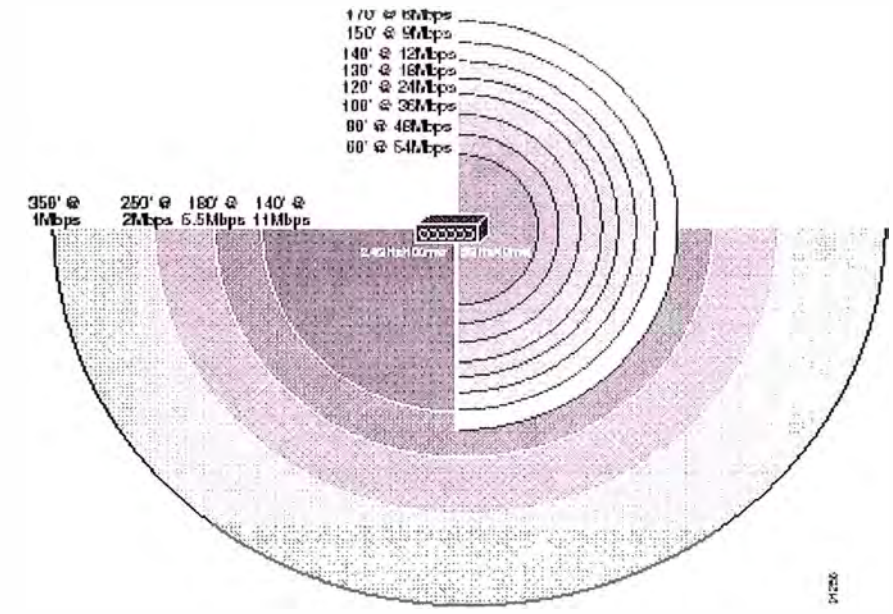


Figure 3.2: Comparación entre 802.11a y 802.11b con AP cisco

El estándar 802.11g usa la misma banda que el 802.11b y está sujeta a las mismas regulaciones del 802.11b con la desventaja de disponer de pocos productos para 802.11g

Las organizaciones desean evaluar la selección de Tecnologías inalámbricas. Por perfomance y capacidad se podría recomendar una implementación con el estándar 802.11a, pero por el rango a cubrir y la facilidad de implementación, se debería seleccionar la tecnología 802.11b. La decisión depende del tipo de actividad, misión y planes futuros. Existen en la actualidad equipos que trabajan con ambas tecnologías.

3.1.3. Locales o puntos de interconexión

Puntos de interconexión de la corporación

PUNTO	SEDE	DIRECCION	UBICACIÓN
PUNTO 1	7801	Calle Grimaldo del Solar N° 701	Miraflores
PUNTO 2	7812	Av. José Pardo N° 650	Miraflores
PUNTO 3	7809	Av. Arequipa N° 1959	Lince
PUNTO 4	7810	Av. Arequipa N° 1593	Lince
PUNTO 5	7805	Av. Arequipa N° 1560	Lince
PUNTO 6	7815	Av. Arequipa N° 1480	Lince
PUNTO 7	7803	Av. Arequipa N° 440	Santa Beatriz
PUNTO 8	7811	Calle Saco Oliveros N° 150	Santa Beatriz
PUNTO 9	7808	Av. Petit Thouars N° 397	Santa Beatriz
PUNTO 10	7807	Av. Paseo Colon N° 203	Lima
PUNTO 11	7802	Av. Wilson N° 1236	Lima
PUNTO 12	7804	Av. Emancipación N° 549	Lima

Tabla 3.4

3.1.4. Parámetros medidos para diseñar el nuevo modelo

Se hizo las mediciones para cada una de las sedes de su altura sobre el nivel del mar y sus respectivas coordenadas, registrándose los siguientes datos:

- **Coordenadas de cada sede**

Coordenadas de cada sede interconectada

PUNTO	ALTURA Snm	ALTURA DE LOCAL	COORDENADAS DE (S)	COORDENADAS DE (W)
1	87m	3m	12°07'8.2"	77°02'7.1"
2	83m	8m	12°02'52.9"	77°02'6.8"
3	121m	8m	12°05'2.8"	77°02'3.9"
4	122m	15m	12°04'48.9"	77°02'6.8"
5	121m	5m	12°04'50.2"	77°02'5.7"
6	121m	18m	12°04'45.3"	77°04'7.4"
7	137m	34m	12°04'7.5"	77°02'13.0"
8	159m	18m	12°04'6.1"	77°02'15.6"
9	127m	45m	12°04'5.0"	77°02'7.8"
10	133m	50m	12°03'336.5"	77°02'18.9"
11	145m	70m	12°03'17.0"	77°02'18.2"
12	147m	50m	12°02'46.2"	77°02'17.0"

Tabla 3.5

3.2. Diseño del modelo

Para establecer el modelo de comparación a utilizarse en la determinación de factibilidad se ha tomado en cuenta propuesta de equipos de 02 fabricantes Netkrom Technologies y Cisco Technologies, lo que nos lleva a plantear 02 modelos, El análisis de factibilidad se hace con el modelo de cisco por representar la alternativa de mayor costo y técnicamente más completa porque en ella, son interconectados todos las sedes, razón por la cual este modelo es presentado en detalles

3.2.1. Modelo 1 (NETKROM TECHNOLOGIES)

Este modelo considera la interconexión de 8 sedes a través de 7 enlaces dejando 4 sedes para interconectarlas por medio de líneas dedicada estableciéndose una red híbrida

a) Velocidad de operación

La frecuencia de interconexión inalámbrica entre las sedes de la institución es 2.4GHz.

b) Distancia de los enlaces

Distancia entre enlaces

ENLACE	DISTANCIA (Km)	SEDES INTERCONECTADAS
PUNTO 3 – PUNTO 4	0.4	7809 – 7810
PUNTO 4 – PUNTO 5	0.05	7810 – 7805
PUNTO 5 – PUNTO 6	0.11	7805 – 7815
PUNTO 4 – PUNTO 7	1.29	7810 – 7803
PUNTO 7 – PUNTO 9	0.17	7803 – 7808
PUNTO 7 – PUNTO 8	0.06	7803 – 7811
PUNTO 8 – PUNTO 10	0.94	7811 – 7807

Tabla 3.6

c) Diagrama de red WAN Wireless (modelo 1)

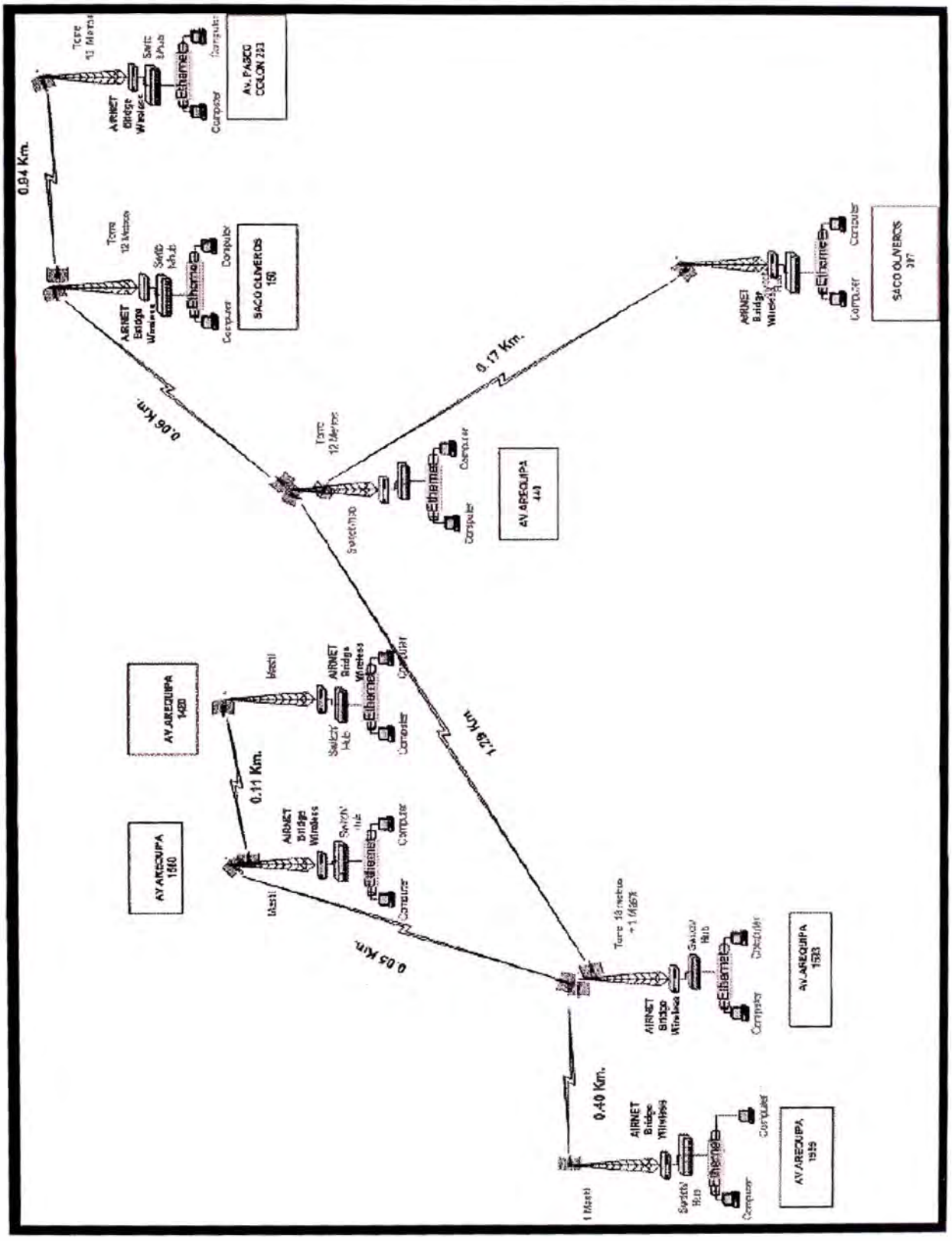


Figura 3.3

En el Diagrama WAN Wireless propuesto para el modelo se interconectan 8 sedes (puntos) que se detallan en la tabla 3.7.

Sedes Interconectadas

PUNTO	SEDE	DIRECCION	UBICACIÓN
PUNTO 3	7809	Av. Arequipa N° 1959	Lince
PUNTO 4	7810	Av. Arequipa N° 1593	Lince
PUNTO 5	7805	Av. Arequipa N° 1560	Lince
PUNTO 6	7815	Av. Arequipa N° 1480	Lince
PUNTO 7	7803	Av. Arequipa N° 440	Santa Beatriz
PUNTO 8	7811	Calle Saco Oliveros N° 150	Santa Beatriz
PUNTO 9	7808	Av. Petit Thouars N° 397	Santa Beatriz
PUNTO 10	7807	Av. Paseo Colon N° 203	Lima

Tabla 3.7

Se tienen 4 sedes no conectadas, las que presentan muchos obstáculos a su alrededor que no permiten realizar un enlace inalámbrico, siguiendo conectadas a través de lineas dedicadas al no establecerse una línea de vista con una sede adyacente. Estas sedes son mostradas en la tabla 3.8.

Sedes no interconectadas

PUNTO	SEDE	DIRECCION	UBICACIÓN
PUNTO 1	7801	Calle Grimaldo del Solar N° 701	Miraflores
PUNTO 2	7812	Av. José Pardo N° 650	Miraflores
PUNTO 11	7802	Av. Wilson N° 1236	Lima
PUNTO 12	7804	Av. Emancipación N° 549	Lima

Tabla 3.8

Para el diagrama propuesto se debe tener en cuenta los siguientes detalles:

- Los enlaces descritos se dan a la frecuencia de 2.4GHz (11Mbps).
- Entre los PUNTO 3 – PUNTO 4 se encuentran edificios demasiados altos por lo que para establecer el enlace, es necesario colocar un mástil en orientación horizontal en cada punto, para encontrar una adecuada línea de vista.
- En el PUNTO 4 se deberá colocar una torre de 18 metros de altura para encontrar línea de vista con el PUNTO 5 y el PUNTO 7, debido a que en la trayectoria de toda la Av. Arequipa se encuentran normalmente árboles de 10 metros de altura.
- El enlace entre PUNTO 5 – PUNTO 6 es prácticamente normal, por lo que para el PUNTO 6 se ha agregado un paso y se ha enlazado éste PUNTO con el PUNTO 7.
- Para el enlace entre el PUNTO 8 – PUNTO 10 se utilizaran torres de 12 metros en ambos locales, ya que el local del PUNTO 10 no tiene demasiada altura

d) Requerimiento de equipos y accesorios

En la tabla 3.9 se muestra el requerimiento de equipos y accesorios por punto de conexión:

Requerimientos de Equipos por Sede Interconectada

PUNTO	EQUIPOS Y ACCESORIOS	CANT
PUNTO 3	AIRNET Bridge 11Mb WATERPPROOF-PoE High Power 100mw.	1
	Antena Grid Semi-Parabólica de 19 dBi 2.4GHz	1
	Mástil de 4 mts. para antenas.	1
PUNTO 4	AIRNET Bridge 11Mb WATERPPROOF-PoE High Power 100mw.	3
	Antena Grid Semi-Parabólica de 19 dBi 2.4GHz	2
	Antena Grid Semi-Parabólica de 24 dBi 2.4GHz	1

	Tramo de torre ventada de 3 metros 25cm de ancho	6
	Mástil de 4 mts. para antenas.	1
PUNTO 5	AIRNET Bridge 11Mb WATERPPROOF-PoE High Power 100mw.	2
	Antena Grid Semi-Parabólica de 19 dBi 2.4GHz	2
	Mástil de 4 mts. para antenas.	1
PUNTO 6	AIRNET Bridge 11Mb WATERPPROOF-PoE High Power 100mw.	1
	Antena Grid Semi-Parabólica de 19 dBi 2.4GHz	1
	Mástil de 4metros para antenas.	1
PUNTO 7	AIRNET Bridge 11Mb WATERPPROOF-PoE High Power 100mw.	3
	Antena Grid Semi-Parabólica de 19 dBi 2.4GHz	2
	Antena Grid Semi-Parabólica de 24 dBi 2.4GHz	1
	Tramo de torre ventada de 3 metros 25cm de ancho	4
PUNTO 8	AIRNET Bridge 11Mb WATERPPROOF-PoE High Power 100mw.	2
	Antena Grid Semi-Parabólica de 19 dBi 2.4GHz	2
	Tramo de torre ventada de 3 metros 25cm de ancho	4
PUNTO 9	AIRNET Bridge 11Mb WATERPPROOF-PoE High Power 100mw.	1
	Antena Grid Semi-Parabólica de 19 dBi 2.4GHz	1
	Tramo de torre ventada de 3 metros 25cm de ancho	2
PUNTO 10	AIRNET Bridge 11Mb WATERPPROOF-PoE High Power 100mw.	1
	Antena Grid Semi-Parabólica de 19 dBi 2.4GHz	1
	Tramo de torre ventada de 3 metros 25cm de ancho	4

Tabla 3.9

En la tabla 3.10, se consolida los requerimientos de equipos y accesorios necesarios para la implementación del diagrama propuesto

Consolidado de equipos y accesorios para la Red Wireless

CODIGO	CANTIDAD	DESCRIPCION
W24-BRO11H	14	AIRNET Bridge 11 Mb WATERPROOF-PoE High Power 100 Mw.
W24-19G	12	Grid Semi-Parabólica de 19dBi 2.4GHz.
W24-24G	2	Grid Semi-Parabólica de 24dBi 2.4GHz
WAC-MA4	4	Mástil de 4 metros para antenas.

W24-TO3M25	16	Tramo de torre ventada de 3 metros 25 cm. de ancho. Requiere Instalación
WCA-CA2	14	Cable Adapter de antena a Radio de 2 m LMR 400/9913 N Hembra a N Macho
AIR-INSTCL	14	Requiere servicio de instalación y configuración por punto.

Tabla 3.10

e) Mapa topográfico

En el anexo 1, se muestra el mapa topográfico de los puntos interconectados.

3.2.2. Modelo 2 (Cisco Technologies)

En este modelo se ha considerado la conexión de todos los puntos, para lo cual hemos agregado tres puntos adicionales, edificios cuyos aires se tiene que alquilar para la instalación de torres, que nos permita tener un backbone al que se conectan los puntos 1, 2, 12 y 4 que en el anterior modelo no fueron considerados debido a la limitación técnica referidas a la falta de línea de vista de estos puntos con algunos de sus adyacentes. Además, para éste modelo, se tiene en cuenta la seguridad, instalándose Firewalls, en cada una de las sedes para asegurar la integridad de los datos.

a) Velocidad de operación

Las frecuencias de interconexión inalámbrica entre las sedes de la institución es 2.4GHz y 5.8GHz, utilizando la frecuencia de 5.8Ghz en el backbone para la interconexión de las 12 sedes.

b) Distancia de los enlaces

Para hacer posible la interconexión de todas las sedes se han considerado 3 puntos adicionales, aires de edificios que se deben alquiler para la instilación de antenas (repetidores, edificios que actuaran como puntos centrales y cuya ubicación, se dan en la tabla 3.11.

Puntos adicionales para interconexión

EDIFICIO	DIRECCION	UBICACIÓN
EDIFICIO 1	C/Líneas de vista a Sedes 1 y 12.	Miraflores
EDIFICIO 2	Av. Arequipa cuadra 24	Lince
EDIFICIO 3	Entre Av. Colmena y Tacna	Lima

Tabla 3.11

Considerando estos puntos adicionales se establecen 14 enlaces, cuyas distancias entre ellas se dan en la tabla 3.12.

Distancia entre enlaces

ENLACE	DISTANCIA (Km)	SEDES INTERCCONECTADAS
PUNTO 1 – EDIFICIO 1	1.0	7801 – EDIFICIO 1
PUNTO 2 – EDIFICIO 1	0.50	7812 – EDIFICIO 1
EDIFICIO 1–EDIFICIO2	3.0	EDIFICIO 1 – EDIFICIO 2
PUNTO 3 – PUNTO 5	0.40	7809 – 7805
PUNTO 5 – PUNTO 4	0.05	7805 – 7810
PUNTO 6 – PUNTO 4	0.10	7815 – 7805
PUNTO 4 – PUNTO 7	1.0	7810 – 7803
EDIFICIO 2 – PUNTO 7	1.8	EDIFICIO 2 – 7803
PUNTO 8 – PUNTO 7	0.06	7811 – 7803
PUNTO 9 – PUNTO 7	0.17	7808 – 7803
PUNTO 10 – PUNTO 7	0.85	7807 – 7803

PUNTO 11 – EDIFICIO3	1.3	7802 – EDIFICIO 3
PUNTO 12 – EDIFICIO3	0.2	7804 – EDIFICIO 3
EDIFICIO 3 – PUNTO 7	2.4	EDIFICIO 3 – 7803

Tabla 3.12

c) Diagrama de red WAN Wireless (modelo 2)

El diagrama Wireless, propuesto para éste modelo, se muestra en la figura 3.4.

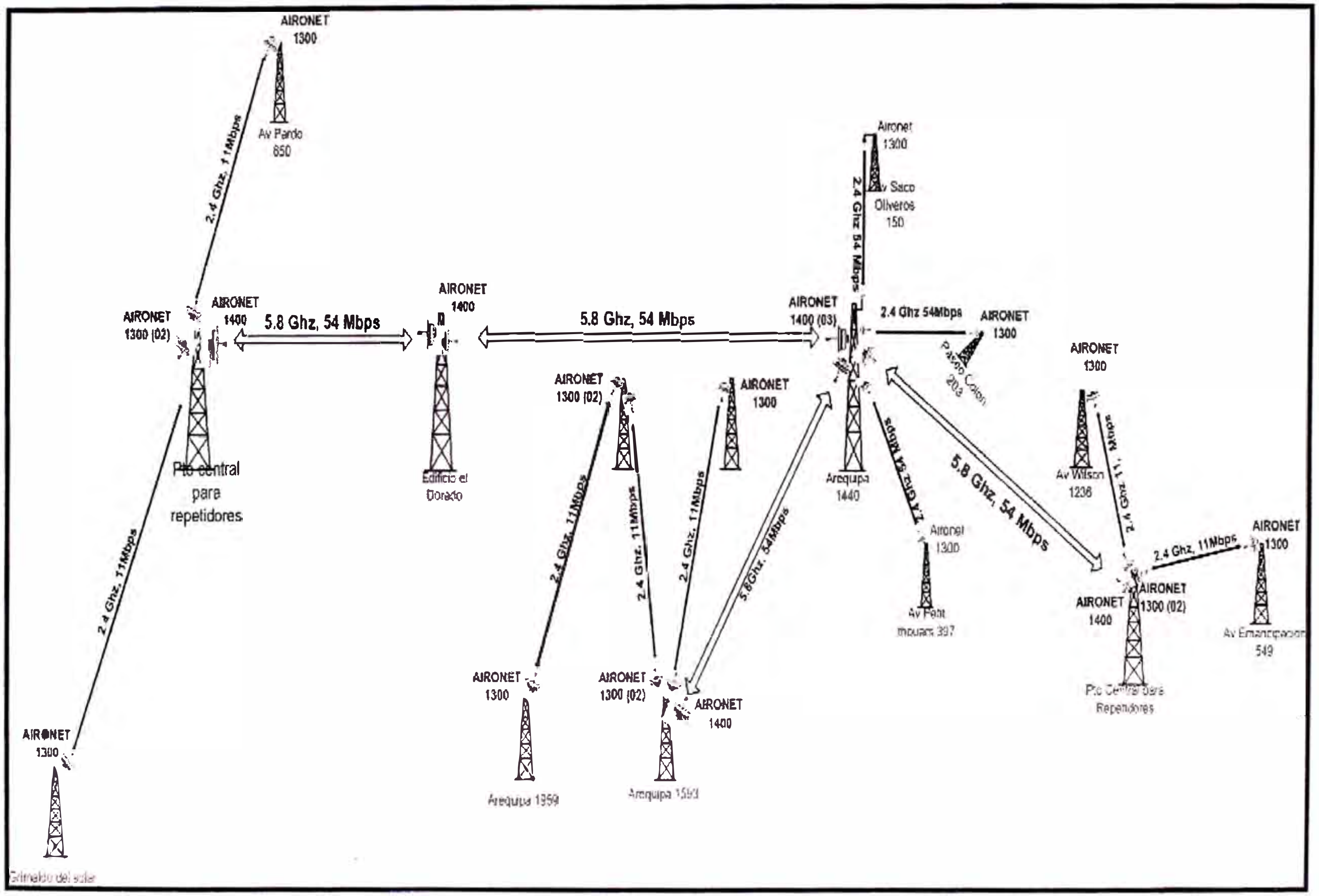

AIRONET 1300
Av Pardo 850
2.4 Ghz, 11Mbps
AIRONET 1300 (02)
AIRONET 1400
5.8 Ghz, 54 Mbps
Pto central para repetidores
AIRONET 1400
Edificio el Dorado
5.8 Ghz, 54 Mbps
Aironet 1300
Av Saco Oliveros 150
2.4 Ghz 54 Mbps
AIRONET 1400 (03)
2.4 Ghz 54Mbps
AIRONET 1300
Paseo Colon 203
Arequipa 1440
AIRONET 1300 (02)
AIRONET 1300
2.4 Ghz, 11Mbps
5.8Ghz, 54Mbps
5.8 Ghz, 54 Mbps
AIRONET 1300
Av Wilson 1236
2.4 Ghz, 11Mbps
Aironet 1300
Av Petit thouars 397
AIRONET 1300
2.4 Ghz, 11Mbps
AIRONET 1400
AIRONET 1300 (02)
Av Emancipacion 549
AIRONET 1300
AIRONET 1300 (02)
AIRONET 1400
Arequipa 1959
Arequipa 1593
AIRONET 1300
Grimaldo del solar

Figura 3.4

En el Diagrama WAN Wireless propuesto, se interconectan todas las sedes (puntos) para los cuales, se debe tener en cuenta los siguientes detalles:

- Los enlaces de los puntos 3 al 10 se dan a la frecuencia de 2.4GHz.
- Para establecer el enlace de los puntos 1 y 2, se debe de alquilar los aires de 2 edificios (uno de ellos podría ser EL DORADO en Lince y el otro se ha considerado ubicado en Miraflores, pero puede estar también ubicado en Surquillo o Magdalena), que permitan tener línea de vista con las sedes 7801 y 7812.
- Para los enlaces de los puntos 1 y 2 se ha creado una troncal desde el edificio 1 al edificio 2 y de allí al local principal a la frecuencia de 5.8Ghz, por encontrarse ambos puntos en una ZONA de mucho "ruido" que pueda afectar la transmisión de datos.
- De forma similar se debe crear otra troncal del Local principal al edificio 3 en el Centro de Lima, para la conexión de los puntos 11 y 12. Ambos ubicados en Lima, cuyo enlace requieren alquilar los aires de un Edificio (recomendable el que se encuentra entre la Av. Tacna y Colmena) para tener línea de vista y se enlace a su vez con el punto 7.
- Por razones técnicas (interferencias) en el local central, no pueden haber más de 4 enlaces a la misma frecuencia, motivo por el cual el enlace con el Punto 5 se debe establecer a 5.8Ghz, también para dar calidad de servicio a la sede 7809 donde se tienen más de 180 PCs.
- El enlace para los puntos 4, 5 y 6 no requiere de consideraciones especiales.

d) Requerimiento de equipos y accesorios

En la tabla 3.13 se muestra el requerimiento de equipos y accesorios por punto de conexión:

Requerimientos de equipos por sede interconectada

PTO	EQUIPOS Y ACCESORIOS	CANT
1	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	1
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	1
	Cisco RP-TNC Male Connector for 9913 Cable	1
	Belden Cable coaxial RG-6 75 ohmios	100
	Amphenol Conector Coaxial F para cable RG-6 exteriores	4
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
2	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	1
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	1
	Cisco RP-TNC Male Connector for 9913 Cable	1
	Belden Cable coaxial RG-6 75 ohmios	100
	Amphenol Conector Coaxial F para cable RG-6 exteriores	4
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
3	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	1
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	1
	Cisco RP-TNC Male Connector for 9913 Cable	1
	Belden Cable coaxial RG-6 75 ohmios	100
	Amphenol Conector Coaxial F para cable RG-6 exteriores	4
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
4	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	2
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	2
	Cisco Aironet 1400 Wireless Bridge with 22.5dBi Antenna, FCC Config.	1
	Hyperlink - Antena 5.8GHz Direccional Grid Mini-reflector	1
	Cisco RP-TNC Male Connector for 9913 Cable	2

	Belden Cable coaxial RG-6 75 ohmios	300
	Amphenol Conector Coaxial F para cable RG-6 exteriores	12
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
5	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	2
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	2
	Cisco RP-TNC Male Connector for 9913 Cable	2
	Belden Cable coaxial RG-6 75 ohmios	200
	Amphenol Conector Coaxial F para cable RG-6 exteriores	8
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
6	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	1
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	1
	Cisco RP-TNC Male Connector for 9913 Cable	1
	Belden Cable coaxial RG-6 75 ohmios	100
	Amphenol Conector Coaxial F para cable RG-6 exteriores	4
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
7	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	3
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	3
	Cisco Aironet 1400 Wireless Bridge with 22.5dBi Antenna, FCC Config.	3
	Hyperlink - Antena 5.8GHz Direccional Grid Mini-reflector	3
	Cisco RP-TNC Male Connector for 9913 Cable	3
	Belden Cable coaxial RG-6 75 ohmios	600
	Amphenol Conector Coaxial F para cable RG-6 exteriores	24
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
8	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	1
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	1
	Cisco RP-TNC Male Connector for 9913 Cable	1
	Belden Cable coaxial RG-6 75 ohmios	100
	Amphenol Conector Coaxial F para cable RG-6 exteriores	4
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1

9	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	1
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	1
	Cisco RP-TNC Male Connector for 9913 Cable	1
	Belden Cable coaxial RG-6 75 ohmios	100
	Amphenol Conector Coaxial F para cable RG-6 exteriores	4
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
10	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	1
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	1
	Cisco RP-TNC Male Connector for 9913 Cable	1
	Belden Cable coaxial RG-6 75 ohmios	100
	Amphenol Conector Coaxial F para cable RG-6 exteriores	4
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
11	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	1
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	1
	Cisco RP-TNC Male Connector for 9913 Cable	1
	Belden Cable coaxial RG-6 75 ohmios	100
	Amphenol Conector Coaxial F para cable RG-6 exteriores	4
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
12	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	1
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	1
	Cisco RP-TNC Male Connector for 9913 Cable	1
	Belden Cable coaxial RG-6 75 ohmios	100
	Amphenol Conector Coaxial F para cable RG-6 exteriores	4
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
E1	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	2
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	2
	Cisco Aironet 1400 Wireless Bridge with 22.5dBi Antenna, FCC Config.	1
	Hyperlink - Antena 5.8GHz Direccional Grid Mini-reflector	1
	Cisco RP-TNC Male Connector for 9913 Cable	2
	Belden Cable coaxial RG-6 75 ohmios	300

	Amphenol Conector Coaxial F para cable RG-6 exteriores	12
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
E2	Cisco Aironet 1400 Wireless Bridge with 22.5dBi Antenna, FCC Config.	2
	Hyperlink - Antena 5.8GHz Direccional Grid Mini-reflector	2
	Belden Cable coaxial RG-6 75 ohmios	200
	Amphenol Conector Coaxial F para cable RG-6 exteriores	8
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1
E3	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	2
	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	2
	Cisco Aironet 1400 Wireless Bridge with 22.5dBi Antenna, FCC Config.	1
	Hyperlink - Antena 5.8GHz Direccional Grid Mini-reflector	1
	Cisco RP-TNC Male Connector for 9913 Cable	2
	Belden Cable coaxial RG-6 75 ohmios	300
	Amphenol Conector Coaxial F para cable RG-6 exteriores	12
	Grounding BlocK 75 ohmios	1
	Caja Nema 4	1

Tabla 3.13

En la tabla 3.14 se consolida los requerimientos de equipos y accesorios necesarios para la implementación del diagrama propuesto, considerando un equipo Cisco Aironet 1300 con sus equipos y accesorios complementarios de backup.

Consolidado de equipos y accesorios para la red Wireless

CODIGO	CANT	DESCRIPCION
AIR-BR1300G-A-K9	20	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.
HG2424G	20	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz
AIR-BR1400G-A-K9	8	Cisco Aironet 1400 Wireless Bridge w/22.5dBi Antenna, FCC Config.
HG5822G	8	Hyperlink - Antena 5.8GHz Direccional Grid Mini-reflector
AIR-ACC1622	20	Cisco RP-TNC Male Connector for 9913 Cable
1530ª	2100	Belden Cable coaxial RG-6 75 ohmios

F1111M1-001-N-6UU	108	Amphenol Conector Coaxial F para cable RG-6 exteriores
GDB75	16	Grounding BlocK 75 ohmios
CANEMA-04	16	Caja Nema 4
KIT-IMP	1	Kit de torres, cables, canaletas, accesorios para la implementación de la red inalámbrica.

Tabla 3.14

CAPÍTULO IV

EVALUACIÓN TÉCNICO-ECONOMICA DE LOS MODELOS

La comparación entre el modelo actual basado en líneas dedicadas y el modelo propuesto con tecnología inalámbrica, se da en el aspecto técnico donde se ven anchos de banda por sede, más los valores agregados que presenta el nuevo modelo y el aspecto económico sobre la base de la cuota mensual que se paga por líneas dedicadas y el costo de implementación del modelo inalámbrico, datos a partir de los cuales se determinan la factibilidad de la propuesta. Asimismo, debemos indicar que por la necesidad de implementación de laboratorios de cómputo en algunas sedes, se hace necesario el redimensionamiento de los anchos de bandas, por lo cual se tiene una propuesta del proveedor de línea dedicada, propuesta que también se toma en cuenta en el análisis.

4.1. Evaluación técnica

La comparación técnica entre los modelos se realiza en base a los siguientes tres criterios: ancho de banda, el parámetro más importante porque refleja la perfomance de la red, el segundo criterio es la seguridad de la Intranet, por último, se analiza los

valores agregados o servicios diferenciales que nos permitiría el modelo propuesto con respecto al actual.

4.1.1. Comparación por ancho de banda

En la tabla 4.1, se presenta el cuadro comparativo de los modelos en lo referente al ancho de banda que utiliza cada sede interconectada.

Cuadro comparativo por ancho de banda de cada sede

SEDE	PTO	DIRECCION	ANCHO DE BANDA	
			ACTUAL	PROPUESTO
7801	1	Calle Grimaldo del Solar N° 701	64K	11M
7802	11	Av. Wilson N° 1236	64K	11M
7803	7	Av. Arequipa N° 440	2.048M	11M,54M
7804	12	Av. Emancipación N° 549	256K	11M
7805	5	Av. Arequipa N° 1560	256K	11M
7807	10	Av. Paseo Colon N° 203	256K	11M
7808	9	Av. Petit Thouars N° 397	MODEM	11M
7809	3	Av. Arequipa N° 1959	1.024M	11M
7810	4	Av. Arequipa N° 1593	MODEM	11M
7811	8	Calle Saco Oliveros N° 150	MODEM	11M
7812	2	Av. José Pardo N° 650	64K	11M
7815	6	Av. Arequipa N° 1480	128K	11M

Tabla 4.1

De acuerdo a la tabla 2.1, donde se establece que la tasa real bajo el estándar 802.11b a 11Mbps es de 6 a 7Mbps, observamos que el modelo propuesto es superior, en un 300 a 1000% dependiendo de la sede. Además observamos que actualmente, se tienen locales interconectados vía MODEM.

Como mencionamos al inicio, por requerimiento de implementación de laboratorios de cómputo, se hace necesario el aumento de ancho de banda, teniéndose la siguiente propuesta de UP-GRADE de la red privada de comunicaciones de la corporación "Wiener – Carrión".

Esta actualización consiste en colocar 01 Puerto Digital E3 (Igual a 16E1) con una velocidad de 32.768Mbps en la sede principal y en las oficinas remotas (Sede) colocar 01 Puerto Digital con 02 E1 con una velocidad de 4.096Mbps

En la tabla 4.2 se detalla la actualización de anchos de banda y velocidades de la Red Privada.

Actualización de ancho de banda en cada sede

SEDE	DIRECCION	ANCHO DE BANDA	
		ACTUAL	UP GRADE
7801	Calle Grimaldo del Solar N° 701	64K	2E1 = 4.096Mbps
7802	Av. Wilson N° 1236	64K	2E1 = 4.096Mbps
7803	Av. Arequipa N° 440	2.048M	1E3 = 32.768Mbps
7804	Av. Emancipación N° 549	256K	2E1 = 4.096Mbps
7805	Av. Arequipa N° 1560	256K	2E1 = 4.096Mbps
7807	Av. Paseo Colon N° 203	256K	2E1 = 4.096Mbps
7808	Av. Petit Thouars N° 397	MODEM	MODEM
7809	Av. Arequipa N° 1959	1.024M	2E1 = 4.096Mbps
7810	Av. Arequipa N° 1593	MODEM	MODEM
7811	Calle Saco Oliveros N° 150	MODEM	MODEM
7812	Av. José Pardo N° 650	64K	2E1 = 4.096Mbps
7815	Av. Arequipa N° 1480	128K	2E1 = 4.096Mbps

Tabla 4.2

De la observación de la dos tablas, se observa que el modelo inalámbrico propuesto es superior en ambos casos, ya que para la comparación del Puerto E3 de la sede (principal) podemos considerar para el modelo inalámbrico la velocidad de las troncales de 54Mbps (real 32Mbps)

4.1.2. Comparación por seguridad

El control de la seguridad en el modelo actual, está centralizado en el local principal a través de un Firewall, un servidor Proxy y un servidor Proxy reverso, éste ultimo para el control del servidor www.wiener.edu.pe, el cual está ubicado en la sede 7809 y no en la principal, como se observa en la figura 1.3.

La sede 7809 es la que cuenta con el mayor numero de computadoras como se detalla en la tabla 4.3. Además, en su totalidad requiere el acceso a Internet por desarrollarse en ella los cursos de computación e informática, por lo que actualmente la red se congestiona rápidamente, produciéndose caídas de la misma.

Numero de computadoras por sede y estándar de licencia requerida

SEDE	DIRECCIÓN	# DE PC	ESTANDAR
7801	Calle Grimaldo del Solar 701 - Miraflores	3	X15
7802	Av. Wilson 1236 – Lima	1	X15
7803	Av. Arequipa 440 – Lima	180	X1000
7804	Av. Emancipación 549 - Lima	8	X15
7805	Av. Arequipa 1560 – Lince	32	X50
7807	Av. Paseo Colón 203 - Lima	12	X15
7808	Av. Petit Thouars 397 - Lima	10	X15
7809	Av. Arequipa 1959 – Lince	180	X250
7810	Av. Arequipa 1593 – Lince	60	X250
7811	Calle Saco Oliveros 150 – Lima	7	X15
7812	Av. Pardo 650 - Miraflores	40	X50
7815	Av. Arequipa 1480 – Lince	40	X50

Tabla 4.3

En el modelo inalámbrico propuesto, se considera una administración de la seguridad centralizada, pero con control en cada sede, es decir, tener un firewall en cada punto, con licencias de acuerdo al número de computadoras instaladas en la sede mediante la implementación de equipos Firebox. Este equipo extiende un túnel VPN para cada sede, bajo el modelo de seguridad IPSec, así también proporciona una administración antivirus centralizada, el control de intrusos y el control de la navegación de los usuarios.

En la tabla 4.4 se presenta el consolidado de licencias requeridas para la implementación de seguridad en cada sede.

Consolidado de Licencias de seguridad requerida

ITEM	DESCRIPCION	CANTIDAD
1	Firewall licencia x15 c/garantía extendida por 1 año.	6
2	Firewall licencia x50 c/garantía extendida por 1 año.	3
3	Firewall licencia x250 c/garantía extendida por 1 año.	2
4	Firewall licencia x1000 c/garantía extendida por 1 año.	1

Tabla 4.4

4.1.3. Comparación por valores agregados o diferenciales

La posibilidad posterior de implementar telefonía IP, aunque esto se puede realizar en cualquiera de los modelos, el hecho de que el modelo inalámbrico propuesto ofrezca mayor ancho de banda permitiría un mayor perfomance, así como poder ejecutar aplicaciones de video a través de la Intranet.

Un valor diferencial a resaltar, es la posibilidad de que alumnos y docentes a través de equipos portátiles se puedan conectar a las redes LAN Ethernet cableadas ya establecidas.

4.2. Evaluación económica

Para la evaluación económica, se considerará los pagos mensuales que realiza la corporación por el modelo actual utilizado. Asimismo, se toma en cuenta el pago, que se realizaría si se hace la actualización de ancho de banda propuesta por el proveedor de líneas dedicadas, para terminar presentando el costo de implementación del modelo inalámbrico evaluado.

4.2.1. Costos mensuales de la red privada actual

Los costos de operación o pagos mensuales realizados al proveedor de las líneas dedicadas, son presentados en la tabla 4.5, donde se considera las sedes interconectadas y ancho de banda.

Costo mensual de la red privada de comunicaciones

Nº DE PUERTOS	SEDE	ANCHO DE BANDA	RENTA MENSUAL	
			PRECIO UNITARIO US$	PRECIO TOTAL US$
1	7803	2048 Kbps. Puerto Principal	790.00	790.00
1	7803	2048 Kbps. Puerto para Internet	790.00	790.00
1	7803	2048 Kbps. Acceso a Internet	1,800.00	1,800.00
1	7809	1024 Kbps. Puerto Remoto	550.00	550.00
1	7814	128 Kbps. Puerto Remoto	190.00	190.00
3	7805, 7807 y 7804.	256 Kbps. Puertos Remotos	245.00	735.00
3	7812, 7801 y 7802.	64 Kbps. Puertos Remotos	150.00	450.00
4	7808 y 7810.	Comunicación entre locales cercanos MODEM HDSL	100.00	400.00
			SUB TOTAL:	**5,705.00**
			IGV (19%):	1,083.95
			TOTAL	6,788.95

Tabla 4.5

4.2.2. Costos mensuales de la red cableada propuesta

Como mencionamos en la sección anterior, la actualización de la red consiste en colocar 01 Puerto Digital E3 (Igual a 16E1) con una velocidad de 32.768Mbps en la sede principal y en las oficinas remotas, colocar 01 puerto digital con 02 E1 con una velocidad de 4.096Mbps. Teniéndose por parte del proveedor de servicios la siguiente propuesta económica:

En las tablas 4.6 y 4.7, se detallan los pagos por el transporte de señales privadas, tanto el pago por el UP-GRADE como la renta mensual, donde se destaca un descuento por fidelidad y la exoneración del pago mensual de alquiler venta por los equipos como router y dispositivos (tarjetas) que son asumidos en su totalidad por el proveedor de servicios, como se indica posteriormente.

Pagos de up-grade por única vez

CANTIDAD	DESCRIPCION	PRECIO UNITARIO US$	PRECIO TOTAL US$
01	Up Grade de 2048K a DS-3	2,500.00	2,500.00
08	Up Grade a 21 E1 por Sede	500.00	4,000.00
		Sub-Total:	6,500.00
		Descuento x Fidelidad	(-) 2,500.00
		Total US$	4,000.00

Tabla 4.6

Renta Mensual por Transporte de Señales Privadas

CANTIDAD	DESCRIPCION	PRECIO UNITARIO US$	PRECIO TOTAL US$
01	Renta Mensual E-3 = en WAN	5,280.00	5,280.00
08	Renta Mensual por E1 = en WAN	630.00	10,080.00
		Total US$	15,360.00

Tabla 4.7

Los equipos que se utilizarían, en la implementación de la propuesta, serían los siguientes:

En la oficina Principal se requiere 01 router CISCO equipado con un puerto LAN y un puerto WAN, éste ultimo permitiría la interconexión y comunicación desde la oficina principal con las sedes remotas ubicadas en la periferia metropolitana.

En las 8 sedes Remotas, se requiere una Tarjetas E1s que se instalarían en cada router existente en la sede, no requiriéndose la adquisición de nuevos equipos.

En las tabla 4.8, se detalla el costo de instalación y configuración de los equipos, que viene a ser un pago por única vez.

Costo de instalación y configuración - Pagos por Única vez

CANTIDAD	DESCRIPCION	PRECIO UNITARIO US$	PRECIO TOTAL US$
01	Instalación y Configuración ROUTER CISCO equipado con un puerto LAN y WAN.	150.00	150.00
08	Instalación y Configuración por cada ROUTER proporcionado la tarjeta E1	50.00	400.00
		Total US$	550.00

Tabla 4.8

En la tabla 4.9, se consigna la renta mensual que tendría que pagar la Corporación, pero por la actualización del contrato, considerado por el proveedor de servicios, como una acción de fidelidad, éste costo seria cero.

Costo mensual de alquiler – venta de los equipos

CANTIDAD	DESCRIPCION	PRECIO UNITARIO USD	PRECIO TOTAL USD
01	Mensualidad: ROUTER CISCO	2,500.00	2,500.00
08	Mensualidad: Tarjeta E1 ROUTER	30.00	240.00
		Total US$	2,740.00
		Descuento x Fidelidad	(-) 2,740.00
		Total US$	.CERO

Tabla 4.9

En la tabla 4.10, se da un resumen del costo de llevar a cabo esta actualización de ancho de banda.

Resumen de costos de actualización (No incluye IGV)

ITEM	DESCRIPCION	TIPO DE PAGO	TOTAL USD
01	Up grade a puertos E3 y E1	Única vez	4,000.00
02	Instalación y Configuración	Única vez	550.00
03	Renta por Puertos E3 y E1.	Mensual	15,360.00
		Total US$	15,360.00

Tabla 4.10

4.2.3. Costo de implementación del modelo inalámbrico propuesto

El detalle de costos de implementación del modelo inalámbrico, se da en base al consolidado de requerimientos propuesto en el capitulo 3 para los equipos y dispositivos de la red y también se considera, las licencias requeridas para la implementación de seguridad, establecidas en la sección de evaluación técnica.

En la tabla 4.11 se dan los detalles de costos del hardware necesario para la implementación de la red inalámbrica

Costos de Equipos, dispositivos y accesorios Wireless

ITEM	DESCRIPCION	CANT	P.U. US$	P. VENTA US$
1	Cisco Aironet 1300 Outdoor AP/Br w/integrated Antenna, FCC Config.	20	1,295.00	25,900.00
2	Hyperlink - Antena Parrilla 8° 24dB 2.4GHz	20	173.00	3,460.00
3	Cisco Aironet 1400 Wireless Bridge w/22.5dBi Antenna, FCC Config.	8	4,983.00	39,864.00
4	Hyperlink - Antena 5.8GHz Direccional Grid	8	600.00	4,800.00

	Mini-reflector			
5	Cisco RP-TNC Male Connector for 9913 Cable	20	21.00	420.00
6	Belden Cable coaxial RG-6 75 ohmios	2700	0.91	22,457.00
7	Amphenol Conector Coaxial F para cable RG-6 exteriores	108	0.91	98.28
8	Grounding BlocK 75 ohmios	16	26.67	426.76
8	Caja Nema 4	16	106.67	1,706.72
10	Kit de torres, cables, canaletas, accesorios para la implementación de la red inalámbrica.	1	22,500.00	22,500.00
11	Instalación y Configuración de la Red (días)	17	640.00	10,880.00
			SUB-TOTAL (US$)	**112,512.72**
			IGV 19% (US$)	21,377.42
			TOTAL (US$)	133,890.14

Tabla 4.11

En la tabla 4.12 se da el costo de implementación de seguridad para la red inalámbrica, considerando equipos firebox de la marca WatchGuard y una garantía tecnológica de 1 año.

Costos de licencias de seguridad

IT	DESCRIPCIÓN	CANT	P.U. US$	P. TOTAL US$
1	Firebox® X15 hasta 15 usuarios c/1 año	6	964.96	5,789.76
2	Firebox® X50 hasta 50 usuarios c/1 año	3	1,754.49	5,263.47
3	Firebox® X500 hasta 250 usuarios c/1 año	2	3,606.00	7,212.00
4	Firebox® X1000 hasta 1000 usuarios c/1 año	1	5,772.15	5,772.15
5	Instalación y Configuración de los Equipos Firebox.	2	640.00	1,280.00
			SUB-TOTAL (US$)	**25,317.38**
			IGV 19% (US$)	4,810.30
			TOTAL (US$)	30,127.68

Tabla 4.12

En la tabla 4.13 se resumen los costos de implementación de la red inalámbrica, en la cual no se considera los costos de seguridad por no existir en el modelo actual y se adiciona el costo de alquiler del espacio libre de tres edificios, para la implementación de la troncal.

Resumen de costos de implementación de Red Wireless (No incluye IGV)

ITEM	DESCRIPCION	TIPO DE PAGO	TOTAL USD
01	Equipos, dispositivos y accesorios inalámbricos.	Única vez	112,512.72
02	Alquiler de espacio libre de tres edificios por 36 meses.	mensual	32,400.00
		Total US$	144,912.72

Tabla 4.13

4.3. Determinación de la factibilidad

Para determinar la factibilidad, aplicaremos el calculo de anualidades, determinando el numero de meses en que se pagaría el monto de inversión requerido para implementar el modelo inalámbrico, tomado como valor presente, el cual sería financiado a un interés anual, pagando en forma mensual, el monto que se paga por el alquiler de las líneas dedicadas. Este cálculo se hará considerando dos tasas 6% y 12% anual.

Primer caso (6%):

De la tabla 4.13 el valor presente, es:

P = 144,912.72

De la tabla 4.5 la anualidad, es:

A = 5,705.00

Para el cálculo no se considera el IGV, solo el valor venta, tanto para el valor presente, como para la anualidad.

Calculo de la tasa mensual:

$i_m = ((1 + i)^{1/12} - 1) * 100$

$i_m = ((1 + 0.06)^{1/12} - 1) * 100$

$i_m = (1.004867 - 1) * 100$

$i_m = 0.004867 * 100$

$i_m = 0.4867\%$

Calculo del número de meses:

$n = (\log A - \log (A - P\ i_m))/\log (1 + i_m)$

$n = (\log 5705 - \log (5705 - 144{,}912.72 * 0.004867))/\log (1 + 0.004867)$

$n = (\log 5705 - \log 4999.70978)/\log (1.004867)$

$n = (3.756256 - 3.6989448)/0.0021086$

$n = 0.0573112 / 0.0021086$

$n = 27.18$ ($n = 28$ meses)

Segundo caso (12%):

De la tabla 4.13 el valor presente, es:

P = 144,912.72

De la tabla 4.5 la anualidad, es:

A = 5,705.00

Para el cálculo no se considera el IGV, solo el valor venta, tanto para el valor presente, como para la anualidad.

Calculo de la tasa mensual:

$i_m = ((1 + i)^{1/12} - 1) * 100$

$i_m = ((1 + 0.12)^{1/12} - 1) * 100$

$i_m = (1.0094888 - 1) * 100$

$i_m = 0.0094888 * 100$

$i_m = 0.94888\%$

Calculo del número de meses:

$n = (\log A - \log (A - P\ i_m))/\log (1 + i_m)$

$n = (\log 5705 - \log (5705 - 144{,}912.72 * 0.0094888))/\log (1 + 0.0094888)$

$n = (\log 5705 - \log 4329.9522)/\log (1.0094888)$

$n = (3.756256 - 3.6364831)/0.0041015$

$n = 0.1197729 / 0.0041015$

$n = 29.17$ ($n = 30$ meses)

Considerando que hemos planteado en la hipótesis un periodo de tiempo para la factibilidad de 3 años (36 meses). Además, efectuado el cálculo en base al pago mensual del modelo actual y no el pago mensual del UP-GRADE propuesto, se determina la **factibilidad del Proyecto**.

CONCLUSIONES

En los siguientes párrafos, se dan las conclusiones obtenidas en el desarrollo del presente trabajo y del análisis de las fuentes bibliográficas, siendo las principales:

1. Las redes inalámbricas son una reciente tecnología que emerge rápidamente debido a las necesidades de movilidad por parte de las empresas para el desarrollo de sus negocios y porque cuenta con numerosas aplicaciones. Las redes inalámbricas no reemplazan a las redes cableadas, sino son un complemento de ellas, ya que tienen como características fundamentales su portabilidad y movilidad, ofreciendo por tanto la posibilidad de compartir información en tiempo real, sin la necesidad de buscar conexión física. Siendo sus campos de aplicación más comunes:
   - ✓ Uso militar: Por la característica de movilidad que requiere una acción militar, las redes inalámbricas son idóneas.
   - ✓ Fácil implementación en construcciones antiguas, ya que Los cimientos inestables de los edificios antiguos pueden dificultar la instalación de redes cableadas o puede que por el hecho de ser edificios históricos estén protegidos

contra la reconstrucción o remodelaciones por lo que la mejor solución son las redes inalámbricas o un caso opuesto de los edificios con paredes de mármol donde también, es más fácil instalar una red inalámbrica.

- ✓ La posibilidad de que profesores y alumnos accedan a la red con sus propios portátiles (o wap, palm, etc.) una vez dentro del campus, como ya ocurre en muchas universidades.
- ✓ Los visitadores médicos, quienes acceden mediante dispositivos móviles a los sistemas de sus empresas.

2. Por su portabilidad las redes inalámbricas constituyen una solución de red en caja, ya que teniéndose los equipos, se puede implementar una red inalámbrica en forma inmediata en cualquier lugar y por tanto, también desmontada cuando no se requiera de la misma. Generando además ahorros entre el 80 y 90 por ciento en costos de reconfiguración. Aplicándose fácilmente en instalaciones con requisitos similares de configuración y siendo sencillo la incorporación de nuevos usuarios a la red.

3. Las tecnologías de transmisión, más utilizadas por las ondas de radio que emplean espectro esparcido, son el DSSS y el OFDM, por operar a velocidades de 2.4GHz y 5GHz. Para la implementación de una red inalámbrica por enlaces de radio, se debe tener autorización de uso por parte del Ministerio de Transporte y Comunicaciones y estas pueden ser en la actualidad a las frecuencias de 2.4GHz y 5.8GHz, teniéndose en cuenta que un determinado espacio, puede estar ya siendo usado por otra empresa que solicitó la autorización con anterioridad

interfiriéndose su señal y generando un reclamo valido. Por lo cual se recomienda adelantarse en el uso de ésta tecnología.

4. El uso de dispositivos *bridge* para establecer la interconexión entre las doce sedes, le da una real perfomance, pero no elimina la natural vulnerabilidad de la redes inalámbricas por utilizar señales de radio, por lo que se recomienda el uso adicional de equipos que realicen un enlace lógico(Túneles VPN) entre las sedes actuando como Firewall.

5. Se debe de considerar una alternativa de contingencia en caso de que un enlace falle (equipo o configuración de los mismos), esto permitiría alta disponibilidad de la información en todos los locales. Para lo cual se tienen dos alternativas: Adquirir un seguro para todos y cada uno de los equipos o adquirir un equipo adicional de respaldo para asegurar una reposición inmediata del servicio, recomendando nosotros la segunda alternativa.

6. El desarrollo de negocios a través del Internet (*e-business*) está basado en la tecnología inalámbrica o *wireless*, ya que permiten realizar operaciones *e-business* desde cualquier lugar y en cualquier momento, es decir, la tecnología inalámbrica abre nuevas oportunidades para la evolución de los modelos y las aplicaciones empresariales, conocidas como *wireless solutions,* que vienen a ser servicios soportados a través de dispositivos móviles inalámbricos.

   Las soluciones wireless incrementan la productividad de las empresas basadas en su movilidad. Estructurándose en tres áreas:

- ✓ Automatización del trabajo de campo
- ✓ Automatización de la fuerza de ventas
- ✓ Oficina móvil para que los empleados dispongan de toda la información de la oficina en cualquier parte, estableciendo una oficina flexible.

7. Para las redes inalámbricas se debe aclarar que su velocidad es limitada, cuando nos referimos a Redes LAN (Wireless LAN), ya que generalmente se compara en este caso con Redes Fast Ethernet, implementada en una topología Bus-Estrella con cable UTP a una velocidad de 100Mbps, pero, si nos referimos a redes WAN, como en el caso del presente estudio, las redes inalámbricas tienen una perfomance superior. Utilizando el estándar 802.11b, es posible transportar todo tipo de aplicaciones, incluidas voz, videoconferencia y televigilancia sobre IP, como se muestra en el anexo 2.

8. Las comunicaciones en la actualidad, son las principales aplicaciones de los sistemas de cómputo y no solamente el procesamiento automático de datos. En este mundo de las telecomunicaciones se han implementado gran número de tecnologías, que permitan la optimización de las comunicaciones elemento base para la globalización basada en elementos móviles e inalámbricos, ofreciendo por tanto un campo de aplicación infinito para las redes inalámbricas.

9. Las redes inalámbricas no están basadas en servicios telefónicos. Los transmisores/receptores inalámbricos se instalan uno por cada edificio, permitiendo una conexión las 24 horas del día con tráfico ininterrumpido. Siendo

una gran ventaja de estas redes inalámbricas, la eliminación de los cortes e interrupciones de servicio que regularmente se sufre con las líneas que las empresas de telefonía y datos venden. Así mismo no se tiene que pagar mensualidades como ocurre con las empresas de telefonía.

10. Las bibliografías destacan la lentitud de las redes inalámbricas con velocidades 1Mbps y 11Mbps que se consideran lentas, si la comparamos con redes cableadas LAN de 100Mbps o 1Gbps. Pero en redes WAN las velocidades de 1Mbps y 11Mbps son velocidades (ancho de banda) muy aceptables en comparación a 256 Kbps o 1Mbps que se tienen trabajando con líneas dedicadas.

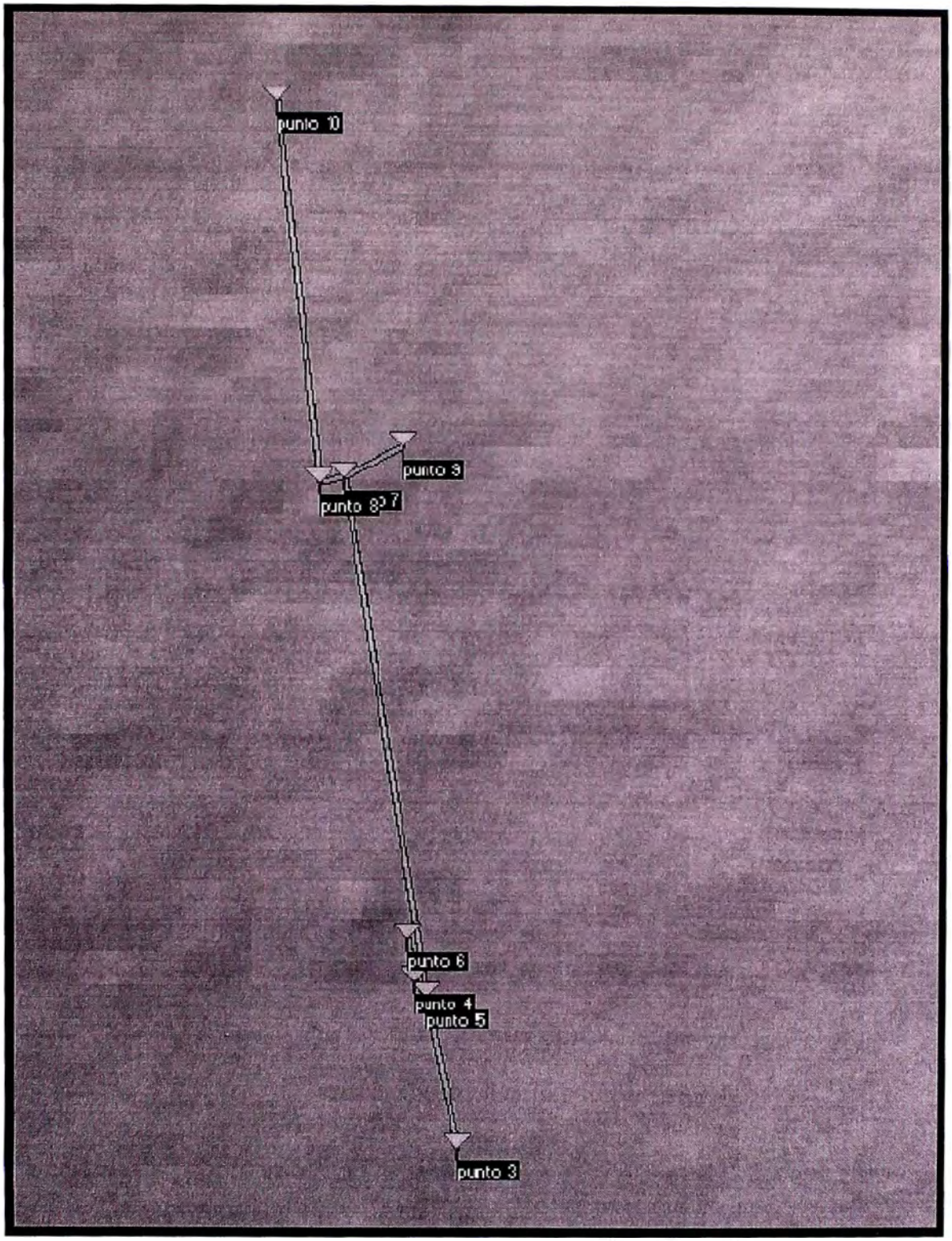
11. Se puede establecer redes de comunicaciones híbridas, es decir, algunos puntos de la red son conectados por medio de ondas de radio y otros con líneas dedicadas.

12. En la actualidad esta tecnología es principalmente utilizada por Empresas privadas, hospitales, escuelas, universidades, y gobiernos locales. Por ser una manera rápida y efectiva de implementar una red inalámbrica de alta velocidad para dar servicios avanzados de telecomunicaciones, enfatizándose que realizar perforaciones en calles y avenidas para instalar cables o fibras ópticas, es muy difícil, además de que sus costos son muy elevados y si por esto fuera poco toma por lo general semanas y hasta a meses su implementación, por el contrario la red inalámbrica toma horas o días.

13. Las redes inalámbricas son redes propietarias, que son controladas por la propia empresa referente al lugar de implementación, configuración deseada y el tipo de servicio que ocupa. Contrariamente a las empresas telefónicas que venden servicios de líneas privadas y realizan un multiplexado de las mismas.

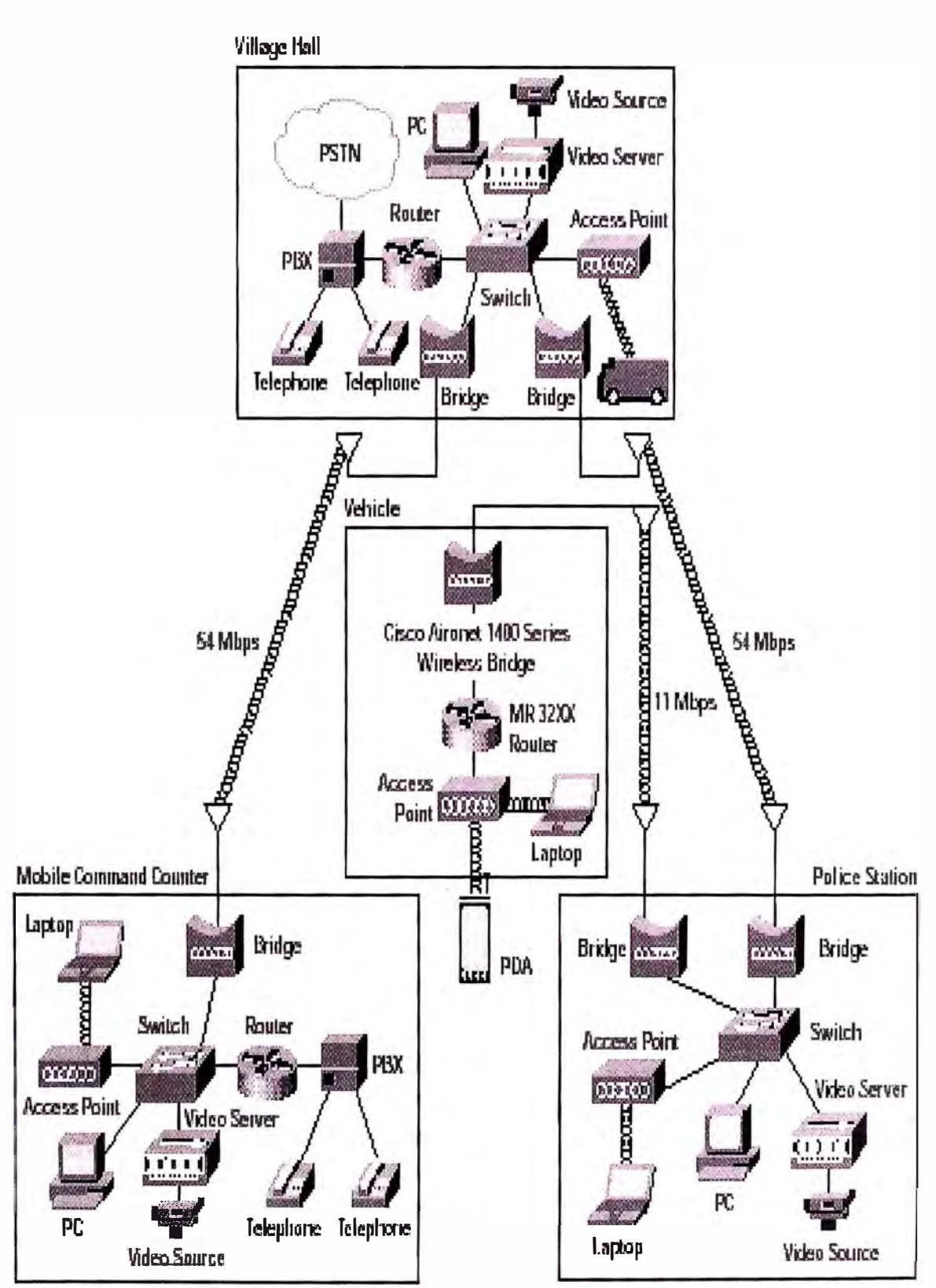
ANEXO 1

MAPA TOPOGRAFICO DE LAS SEDES


punto 10
punto 9
punto 8
punto 7
punto 6
punto 4
punto 5
punto 3

ANEXO 2

APLICACION DE RED INALAMBRICA CON DATA, VOZ Y VIDEO


Village Hall
Video Source
PC
PSTN
Video Server
Router
Access Point
PBX
Switch
Telephone
Telephone
Bridge
Bridge
Vehicle
54 Mbps
Cisco Aironet 1400 Series
Wireless Bridge
11 Mbps
54 Mbps
MR 32XX
Router
Access
Point
Laptop
Mobile Command Counter
Police Station
Laptop
Bridge
PDA
Bridge
Bridge
Switch
Router
Access Point
Switch
PBX
Access Point
Video Server
Video Server
PC
Telephone
Telephone
PC
Laptop
Video Source
Video Source

BIBLIOGRAFÍA

[1] Cisco Systems Inc. "CISCO Avvid Wireless LAN Design", 2003.

[2] Lucent Technologies "WaveACCCESS Technical Training Course", 1999.

[3] Tabenbaum A. "Redes de Computadoras", 4ta edición Pearson Educación, 2003.

[5] Merilee Ford "Tecnologías de Interconectividad de Redes", Prentice Hall, 1998.

[6] http://www.cisco.com/go/wireless

[7] http://www.netkrom.com

[8] http://www.redes-inalambricas.com

[9] http://www.cisco.com/en/US/products/hw/wireless/index.html

[10]http://www.cisco.com/en/US/products/hw/wireless/ps5279/index.html

[11]http://www.cisco.com/en/US/products/hw/wireless/ps5279/products_data_sheet0
91886a008018495c.html

[12]http://www.cisco.com/en/US/products/hw/wireless/ps5279/prod_tecchnical_doc
umentation.html

[13]http://www.cisco.com/en/US/products/ps5861/index.html

[14]http://www.cisco.com/en/US/products/ps5861/products_data_sheets_list.html

[15]http://www.cisco.com/en/US/products/ps5861/prod_technical_documentation.
html

[16]http://www.ietf.org/rfc/rfc2058.txt (rfc2058)

GLOSARIO

3DES	: Triple Data Encryption Standard
AES	: Advanced Encryption Standard
AP	: Access Point
BPSK	: Binary Phase Shift Reging
BSS	: Basic Sercvice Set
CBC - MAC	: Cipher Block Chaining Message Autitentication Cide
CCMP	: Counter CBC – MAC Protocol
DCF	: Distributed Coordination Function
DSCP	: Differenciated Services Code Point
DSSS	: Direct Sequence Spread Spectrum
EAP	: Extensible Authentication Protocol
EDCF	: Enhaced Distributed Coordination Function
ESS	: Extended Service Set
ESTI	: European Telecommunications Standards Institute
FCC	: Federal Comumunications Commision
FHSS	: Frecuency Hopping Spread Spectrum

GPS	: Sistema de Posicionamiento Global.
H2GF	: HiperLAN2 Global Forum
HRFWG	: HomeRF Working Group
IAS	: Internet Authentication Service
IBSS	: Independent Basic Service Set
IEEE	: Institute for Electrical and Electronics Engineers
ISM	: Industrial Scientific Medical
LAN	: Local Area Network
MIC	: Message Integrity Check
MKK	: Norma Japonesa
NIC	: Network Interface Card
OFDM	: Orthogonal Frequency Digital Multliplexing
PCF	: Point Coordination Function
PCMCIA	: Personal Computer Memory Card International Association
PDA	: Asistentes Personales Digitales
PPP	: Point to Point Protocol
QAM	: Quadrature Amplitude Modulation
QoS	: Quality of Service
QPSK	: Quadrature Phase Shift Reging
RADIUS	: Remote Authentication Dial-In User Service
RF	: Radio Frecuency
RTS / CTS	: Request to send / Clear to Send
SIG	: Special Interes Group
SIGU	: Sistema Integrado de Gestión Universitaria

SLA	: Service Level Agreements
SSID	: Service Set Identifier
SWAP	: Shared Wireles Access Protocol
TKIP	: Temporal Key Integrity Protocol
USB	: Universal Serial Bus
VPN	: Virtual Private Network
WAN	: Wide Area Network
WECA	: Wireless Ethernet Compatibility Alliance
WEP	: Wired Equivalent Privacy
WEP	: Wired Equivalent Privacy
WI – FI	: Wireless Fidelity
WLAN	: Wireless Local Area Network
WPA	: Wi – Fi Protected Access