Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

"Gestión de una Red Lan Inalámbrica usando herramienta propietaria basada en SNMP"

Proyecto de Graduación

Previo a la obtención del título de:

Ingeniero en Electricidad

Especialización – Electrónica

Presentado por:

Ingrid García Ríos
Marjorie Montalvo Morán
Xavier Zavala Mendoza

Guayaquil – Ecuador
Año 2003

Agradecimiento

Al Ing. Edgar Leyton

Director de Tópico, por su valiosa ayuda y colaboración para la realización de este trabajo.

Dedicatoria

A Dios por guiarme y darme la fortaleza y sabiduría para culminar con mi carrera profesional
A la memoria de mi Padre(+), a mi Madre por darme su apoyo incondicional en todo momento, a mis hermanos y todas las personas que hicieron posible lograr una de mis metas.

Ingrid García Ríos

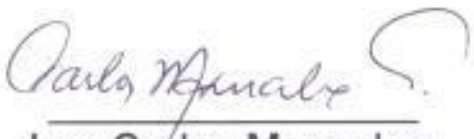
A Dios por darme la fuerza necesaria para poder5 terminar este proyecto, a mis padres y en especial a mi hermano mayor por toda la ayuda brindada a lo largo de mis estudios universitarios.

Xavier Zavala M.

A Dios por darme la fortaleza necesaria para culminar esta parte importante de mi vida, mi carrera. A mis padres, hermanos y abuelos por darme siempre su apoyo, dedicación, consejos y una luz para seguir adelante en todas la metas que he emprendido y en las que restan por venir, sin nunca dejarme vencer. Quiero dar un agradecimiento en especial a mi abuelo Panchito que en paz descanse, por sus enseñanzas de bondad y humildad, elementos importantes para emprender la lucha por ser mejores y seguir siempre adelante.

Marjorie Montalvo Morán.

Tribunal



Ing. Carlos Monsalve
Presidente del Tribunal

Ing. Edgar Leyton
Director de Tópico

Ing. Juan Carlos Aviles
Miembro Principal

Ing. César Yépez
Miembro Principal

Declaración Expresa

La responsabilidad por los hechos, ideas y doctrinas expuesto en este proyecto, nos corresponden exclusivamente; y, el Patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

(Reglamento de Exámenes y Títulos Profesionales de la ESPOL).-

Ingrid García Ríos

Marjorie Montalvo Morán

Xavier Zavala Mendoza

RESUMEN

Las redes inalámbricas proveen a los usuarios de una LAN, acceso a la información en tiempo real en cualquier lugar dentro de la empresa. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red cableada. La instalación de una red inalámbrica puede ser tan rápida y fácil, y además que puede eliminar la posibilidad de pasar cable a través de paredes y techos. Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN cableada, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los sistemas WLAN's pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

El presente proyecto tiene como objetivo, entregar una solución inalámbrica de alta velocidad para establecer una red LAN de uso intra – Building, gestionada por un software propietario basado en SNMP (Simple Network Management Protocol), que cuenta con herramientas de diagnóstico que simplifiquen la tarea de resolución de problemas y de esta manera obtener una continua disponibilidad, y un óptimo desempeño de la misma.

En el capítulo 1, se describen conceptos básicos de lo que son las redes de área local inalámbricas comúnmente llamadas WLAN, se empieza explicando la historia de estas redes, el estándar que las define, sus aplicaciones, tecnologías, configuraciones y por último se analiza sus ventajas con relación a las redes cableadas.

El capítulo 2, se refiere al estudio del protocolo de gestión de redes SNMP (aplicado en redes TCP/IP), que es el protocolo de gestión mediante el cual se podrá administrar la red a diseñar (WLAN).

En el capítulo 3, se explica en base a que infraestructura se realizará el diseño y gestión de la WLAN, se tomó como referencia la red LAN de la compañía SATLINK, por tanto se describe el equipamiento inicial con que cuenta este ISP.

En el capítulo 4, se describen los equipos y programas que se usan para el diseño y gestión de la red, que son de la marca Lucent Technologies y su línea inalámbrica **Orinoco.**

En el capítulo 5, se explica el diseño de toda la red WLAN; considerando la tecnología que se utiliza, la infraestructura diseñada, se trata también el tipo de configuración que se aplica a la red, la selección de la estación de red que se usa

para la gestión de la misma, el esquema de direccionamiento IP que se utiliza, y por último se muestran los costos que implicarían implementar este diseño.

En el capítulo 6, se describe como sería la instalación de las herramientas y equipos necesarios para el diseño y gestión de la red. En lo que respecta a hardware, se explica como se instalan las tarjetas PC, los adaptadores USB, los puntos de acceso y la antena extensora de rango y en lo que es software, se explica la instalación del **Administrador OR** y el **Administrador del cliente**.

En el capítulo 7, se explica la gestión de toda la red inalámbrica, usando el software Orinoco con sus herramientas; el administrador OR y el administrador del cliente. Estas herramientas permiten manejar los siguientes tipos de gestión:

- Gestión de la configuración.
- Gestión del rendimiento.
- Gestión de seguridad.

INDICE GENERAL

CAPITULO 3

INFRAESTRUCTURA DE LA RED ACTUAL.

CAPITULO 4

DESCRIPCIÓN GENERAL DEL EQUIPAMIENTO Y SOFTWARE A UTILIZAR PARA EL DISEÑO Y GESTIÓN DE LA RED.

INDICE DE FIGURAS

CAPITULO 1

CAPITULO 2

CAPITULO 3

CAPITULO 4

CAPITULO 5

CAPITULO 6

CAPITULO 7

INDICE DE TABLAS

Introducción

En los últimos años, las redes inalámbricas (WLAN, Wireless Local Area Network) han ganado muchos adeptos y popularidad en mercados verticales tales como hospitales, fabricas, bodegas, tiendas de autoservicio, tiendas departamentales, pequeños negocios y áreas académicas. Las redes inalámbricas permiten a los usuarios accesar información y recursos en tiempo real sin necesidad de estar fisicamente en un sólo lugar.

Con WLAN's, la red por sí misma es móvil y elimina la necesidad de usar cables, y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las actividades diarias de la empresa. Un usuario dentro de una red inalámbrica puede transmitir y recibir voz, datos y video dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de hasta 11 Mbps.

El momento decisivo para la consolidación de estos sistemas, fue la conclusión del estándar IEEE 802.11 el mes de junio de 1997. En este estándar, se encuentran las especificaciones tanto fisicas como a nivel MAC que hay que tener en cuenta a la hora de implementar una red de área local inalámbrica.

Muchos de los fabricantes de computadoras y equipos de comunicaciones como PDAs (Personal Digital Assistants), módems, microprocesadores inalámbricos,

lectores de punto de venta y otros dispositivos, están introduciendo aplicaciones en soporte a las comunicaciones inalámbricas. Las nuevas posibilidades que ofrecen las WLAN's, son permitir una fácil incorporación de nuevos usuarios a la red, ofrecen una alternativa de bajo costo a los sistemas cableados, además de la posibilidad ubicua para accesar cualquier base de datos o cualquier aplicación localizada dentro de la red.

Este proyecto, tiene como finalidad el **Diseño y Gestión** de una red LAN inalámbrica (WLAN) según el estándar IEEE 802.11, específicamente 802.11b definido para trabajar a velocidades de hasta 11 Mbps. La gestión de la red se basa en el protocolo de administración SNMP. Para este diseño, se ha tomado como referencia la red LAN de la empresa SATLINK, que es un proveedor de servicio de Internet (ISP) y basándose en su equipamiento (computadoras, switches, etc) y arquitectura del edificio, se ha efectuado el diseño de la WLAN. Mediante ésta red los usuarios podrán compartir recursos (archivos, discos duros, diskettes, impresoras, etc..), incluso acceso a Internet proporcionado por el mismo ISP.

El equipamiento inalámbrico que se utilizará para el diseño de la red, es de la marca Lucent Technologies y su línea inalámbrica ORINOCO, estos equipos incluyen herramientas de gestión (software) basadas en SNMP, que es el protocolo de administración que se utilizará para la gestión de la WLAN.

A continuación, se da a conocer el presente trabajo esperando que en él, se encuentre una guía para la implementación de nuevas redes que se adapten a las necesidades de los usuarios.

CAPITULO 1
GENERALIDADES SOBRE LAS WLAN (WIRELESS LAN)

En este capítulo se describen conceptos básicos de lo que son las redes de área local inalámbricas, comúnmente llamadas **WLAN** (Wireless LAN); se empieza explicando la historia de estas redes, el estándar que las define (IEEE 802.11) con todas sus aplicaciones, tecnologías, configuraciones y ventajas en relación con las redes cableadas.

1.1 Breve Reseña Histórica

Las redes de área local inalámbricas funcionan desde hace más de quince años en entornos industriales y de investigación.

Este tipo de redes se implementó por primera vez en el año 1979. La casa IBM Suiza utilizó enlaces infrarrojos creando una red de área local en una fábrica. Posteriormente, se utilizaron implementaciones basadas en tecnologías de microondas según los esquemas de transmisión de espectro ensanchado.

En marzo de 1985 la Comisión Federal de Comunicaciones FCC, organismo encargado de la regulación de las telecomunicaciones en Estados Unidos, asignó a los sistemas **WLAN** las bandas frecuenciales (902-928 MHz), (2.400-

2.4835 GHz) y (5.725-5.850 GHz) también conocidas estas tres bandas como ISM (Industrial, Cientifica y Médica), que pueden utilizarse bajo licencia administrativa. Esta asignación de una localización frecuencial fija, propició una mayor actividad industrial.

En este punto, las redes de área local inalámbrica dejaron de ser meramente experimentales para empezar a introducirse en el mercado. Entre los años 1985 y 1990 se trabajó en el desarrollo de productos **WLAN** y finalmente en mayo de 1991 se publicaron algunos trabajos que hablaban sobre redes inalámbricas que superaban la velocidad de transferencia de 1 Mbps, velocidad mínima a partir de la cual el comité IEEE considera que una red es de área local.

Hasta ese momento, las **WLAN** habían tenido una aceptación marginal en el mercado por dos razones fundamentales: falta de un estándar y precios elevados de la solución inalámbrica. En estos últimos años se ha producido un crecimiento en el mercado de hasta un 100 % anual. Este hecho es atribuible a dos razones principales:

- El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles, que han producido que los usuarios puedan estar en continuo movimiento manteniendo comunicación constante con otros terminales y elementos de la red. En este sentido, las

comunicaciones inalámbricas ofrecen una prestación no disponible en las redes cableadas: movilidad y acceso simultáneo a los recursos de la red.

- La conclusión de la definición de la norma IEEE 802.11 para redes de área local inalámbricas en junio de 1997, que ha establecido un punto de referencia y ha mejorado muchos de los aspectos de estas redes.

1.2 El Estándar IEEE 802.11 para Redes Inalámbricas.

La norma 802 fue desarrollada por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), y versa sobre la arquitectura de redes de datos LAN (Local Area Network). Esta norma establece un estándar de tecnología en el mercado mundial, garantizando que los productos compatibles con la norma 802 sean también compatibles entre sí.

La norma posee muchos apartados, que describen y especifican las distintas funciones que se implementan en una comunicación de datos de red. Ejemplos de estos apartados pueden ser: 802.1, describe las funciones de Bridging; 802.2, controla el enlace lógico; 802.4, método de control de tráfico Token-Passing; 802.5, Método de control de tráfico Token-Ring; 802.10, seguridad en comunicaciones de datos, etc. El apartado 802.11, es el que describe y especifica una interface inalámbrica para comunicaciones de datos compatibles con la Norma IEEE 802.

La norma 802.11 ha sufrido diferentes extensiones para obtener modificaciones y mejoras. De esta manera tenemos las siguientes especificaciones:

- 802.11: Especificación para 1-2 Mbps en la banda de los 2.4 GHz, usando técnica de salto de frecuencias (FHSS) o secuencia directa (DSSS).
- 802.11 b: Extensión del 802.11 en la banda de 2.4 Ghz, con velocidades de comunicación de datos de hasta 11 Mbps usando DSSS, también conocido como Wi-Fi (Wireless Fidelity).
- 802.11 a: Extensión del 802.11 en la banda de 5.8 Ghz, con velocidades de comunicación de datos 54 Mbps usando modulación OFDM.
- 802.11 g: Extensión de 802.11 para proporcionar velocidades de 20-54 Mbps, usando DSSS y OFDM. Es compatible con el 802.11b. Tiene mayor alcance y menor consumo de potencia que el 802.11a.

Como se ve en las especificaciones arriba mencionadas, existe también otra subdivisión dentro de la norma 802.11. Es la referida al método de modulación de los datos. La norma describe los métodos DSSS (Direct Sequence Spread Spectrum), FHSS (Frequency Hoping Spread Spectrum), Infrared (Infrarrojo) y OFDM (Orthogonal Frecuency Division Multiplexing).

Cabe mencionar que la banda de frecuencia 2.4 Ghz, utilizada por la tecnología 802.11b, es una banda **No Licenciada** lo que significa que su uso es libre.

La norma 802.11b, es la que actualmente se comercializa en forma masiva a través de una gran variedad de productos y aplicaciones. La norma 802.11a está evolucionando, y se supone que en un futuro cercano también ofrecerá soluciones económicas al mercado de datos inalámbricos al igual que el 802.11g.

Resumiendo los conceptos más relevantes de la norma 802.11b:

- Es un estándar internacional en Comunicaciones de Datos.
- Tecnología probada por muchos años a nivel Mundial.
- Existe gran variedad de productos orientados a distintas aplicaciones.
- Opera en una banda No Licenciada

1.3 Definición de Red de Área Local Inalámbrica.

Una red de área local inalámbrica puede definirse, como a una red de alcance local que tiene como medio de transmisión el aire; también llamada Wireless LAN (**WLAN**), es un sistema flexible de comunicaciones que puede implementarse como una extensión o directamente como una alternativa a una red cableada.

Este tipo de redes utiliza tecnología de radiofrecuencia, minimizando así la necesidad de conexiones cableadas. Este hecho proporciona al usuario una gran movilidad sin perder conectividad. El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado.

Aún así, debido a que sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 11 Mbps, frente a los 10 y hasta los 100 Mbps ofrecidos por una red convencional, las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite, y en general las **WLAN** se utilizarán como un complemento de las redes fijas.

1.4 Aplicaciones de los Sistemas WLAN.

Las aplicaciones más típicas de las redes de área local que podemos encontrar actualmente son las siguientes:

- Implementación de redes de área local en edificios históricos de difícil acceso, y en general en entornos donde la solución cableada es inviable.
- Posibilidad de reconfiguración de la topología de la red, sin añadir costos adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.

- Redes locales para situaciones de emergencia o congestión de la red cableada.
- Acceso a la información mientras el usuario se encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes.
- Generación de grupos de trabajo eventuales y reuniones Ad-Hoc (tipo de configuración inalámbrica explicada mas adelante). En estos casos, no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo.
- En ambientes industriales con severas condiciones ambientales, este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.
- Interconexión de redes de área local que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red de área local inalámbrica para interconectar dos o más redes de área local cableadas situadas en dos edificios distintos.

1.5 Tecnologías utilizadas en las Redes Inalámbricas.

En esta sección se describirán dos tipos de tecnologías inalámbricas existentes definidas en el estándar 802.11:

- Espectro ensanchado
- Infrarrojos

1.5.1 Tecnologías de Espectro Ensanchado.

Un sistema de espectro ensanchado, es aquel en el cual la señal transmitida es propagada en una banda de frecuencia amplia, mucho más de hecho que el mínimo ancho de banda requerido para transmitir la información que será enviada. Las comunicaciones de **espectro ensanchado** no puede decirse que sean una manera eficiente de utilizar el ancho de banda. Sin embargo, son de utilidad cuando se combinan con los sistemas existentes que ocupan la frecuencia. La señal de **espectro ensanchado,** que es propagada en un ancho de banda grande, puede coexistir con señales de banda estrecha añadiendo únicamente un ligero incremento en el ruido de fondo que los receptores de banda estrecha pueden ver. El receptor de espectro ensanchado no ve las señales de banda estrecha, pues está escuchando en un ancho de banda mucho más amplio.

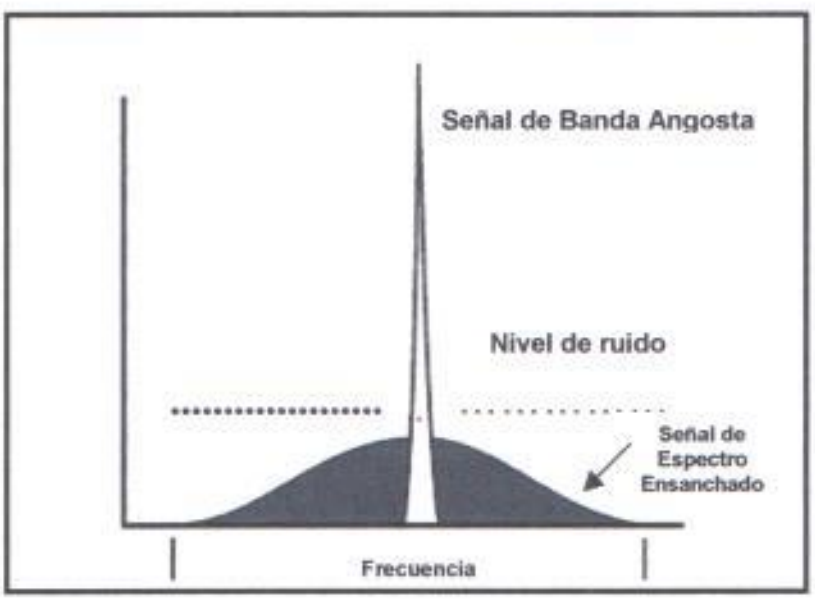


Fig 1.1: Comparación de una señal de banda angosta con una señal de espectro ensanchado

Existen dos tipos de tecnologías de espectro ensanchado:

- Espectro Ensanchado por Secuencia Directa (DSSS).
- Espectro Ensanchado por Salto en Frecuencia (FHSS).

1.5.1.1 Tecnología de Espectro Ensanchado por Secuencia Directa (DSSS).

Esta técnica, opera en un canal determinado y consiste en representar cada bit de la señal original por múltiples bits en la señal transmitida. Cada bit trasmitido se modula con una secuencia de 11 bits aleatorios (Código de Barker), esta secuencia tiene propiedades matemáticas que lo hacen ideal para modular radiofrecuencias. Un ejemplo de la secuencia de Barker podría ser:

+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

En la figura 1.2, se muestra el aspecto de una señal de dos bits a la cual se le ha aplicado la secuencia de Barrer descrita arriba.

DSSS tiene definidos dos tipos de modulaciones a aplicar a la señal resultante (señal de información luego de aplicarle la Secuencia de Barker), tal y como especifica el estándar IEEE 802.11: la modulación DBPSK (Differential Binary Phase Shift Keying), y la modulación

DQPSK (Differential Quadrature Phase Shift Keying), proporcionando unas velocidades de transferencia de 1 y 2 Mbps respectivamente.

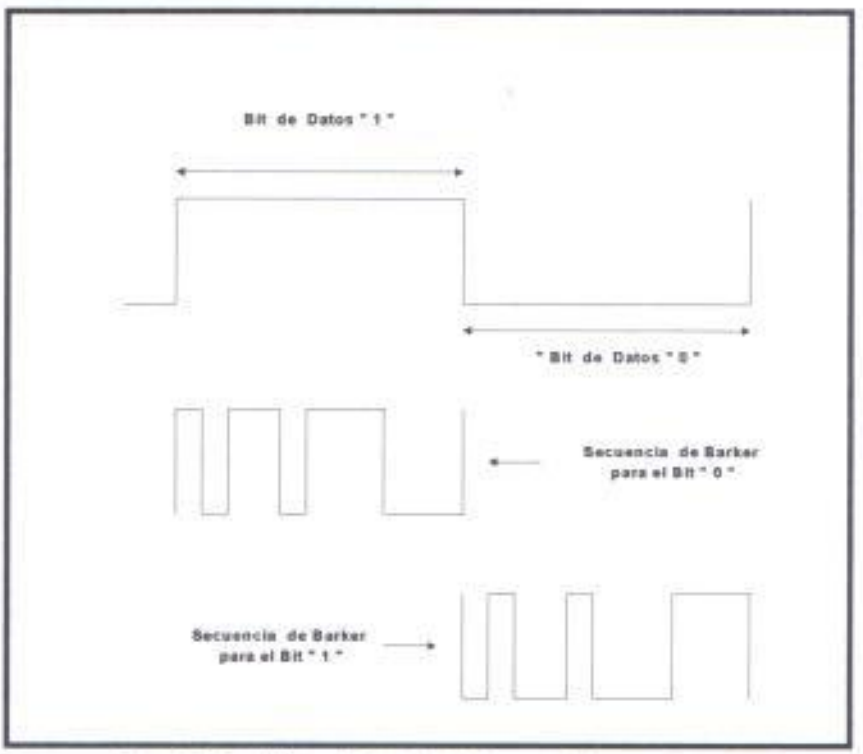


Fig 1.2: Codificación de la información mediante la secuencia de Barker

Para lograr velocidades de 5.5 y 11 Mbps, la codificación que se usa es CCK (Complementary Code Keying); en vez de usar el código de Barker, se usan series de secuencias complementarias que cuentan con 64 únicas palabras que pueden usarse. En contraposición al Código de Barker, por CCK se pueden representar 6 bits de datos en una sola palabra y no 1 bit de datos por palabra como el Código Barker.

En recepción, es necesario de realizar el proceso inverso para obtener la señal de información original.

En el caso de Estados Unidos y de Europa, la tecnología de espectro ensanchado por secuencia directa (DSSS), opera en el rango que va desde los 2.4 GHz hasta los 2.4835 GHz, es decir, con un ancho de banda total disponible de 83.5 MHz. Este ancho de banda total se divide en 14 canales con un ancho de banda por canal de 5 MHz, de los cuales cada país utiliza un subconjunto de los mismos según las normas reguladoras para cada caso particular. En el caso de Ecuador, se utilizan 11 canales que van desde los 2.412 GHz (canal 1) hasta los 2.462 GHz (canal 11).

En topologías de red que contengan varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias en el sistema; si la separación entre las frecuencias centrales es como mínimo de 25 MHz. Esto significa que de los 83.5 MHz de ancho de banda total disponible, podemos obtener 3 canales independientes, que pueden operar simultáneamente en una determinada zona geográfica sin que aparezca interferencia en un canal procedente del otro, (figura 1.3).

Esta independencia entre canales, permite aumentar la capacidad del sistema de forma lineal con el número de puntos de acceso, operando en un canal que no se esté utilizando y hasta un máximo de tres canales, como ya se mencionó.

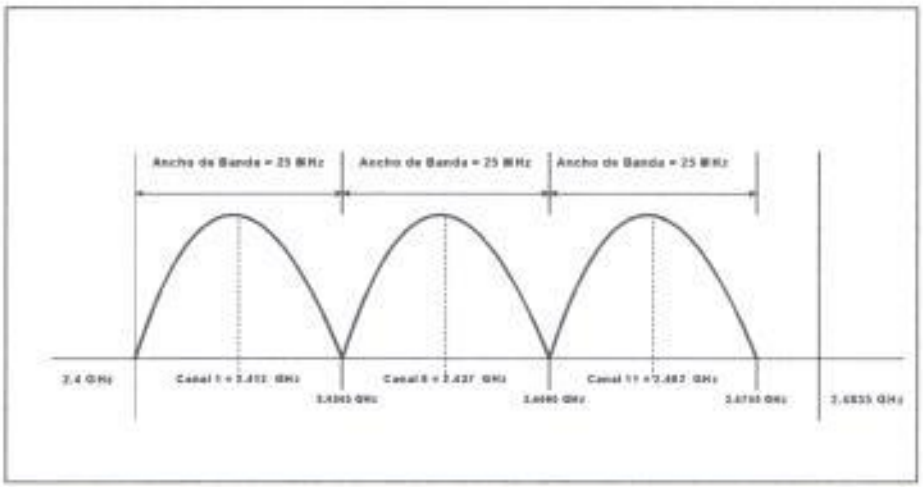


Fig 1.3: Operación de 3 canales independientes DSSS

1.5.1.2 Tecnología de Espectro Ensanchado por Salto en Frecuencia (FHSS).

La tecnología de espectro ensanchado por salto en frecuencia, consiste en transmitir una parte de la información en una determinada frecuencia, durante un intervalo de tiempo llamada *dwell time* e inferior a 400 ms. Pasado este tiempo, se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera, cada tramo de

información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo (figura 1.4).

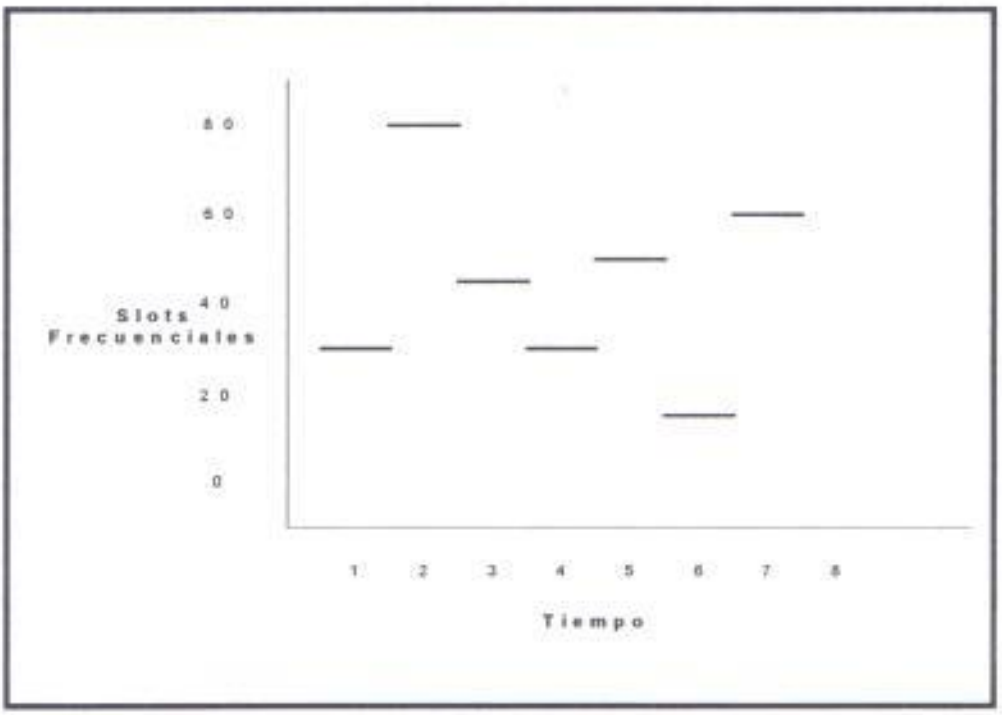


Fig 1.4: Modo de trabajo de la técnica FHSS

Cada una de las transmisiones a una frecuencia concreta, se realizan utilizando una portadora de banda estrecha que va cambiando (saltando) a lo largo del tiempo. Este procedimiento equivale a realizar una partición de la información en el dominio temporal. El orden en los saltos en frecuencia que el emisor debe realizar viene determinado según una secuencia pseudoaleatoria, que se encuentra definida en unas tablas que tanto el emisor como el receptor deben conocer.

La ventaja de estos sistemas frente a los sistemas DSSS, es que con esta tecnología podemos tener más de un punto de acceso en la misma zona geográfica sin que existan interferencias, si se cumple que dos comunicaciones distintas no utilizan la misma frecuencia portadora en un mismo instante de tiempo.

Si se mantiene una correcta sincronización de estos saltos entre los dos extremos de la comunicación, el efecto global es que, aunque vamos cambiando de canal físico, con el tiempo se mantiene un único canal lógico a través del cual se desarrolla la comunicación.

Para un usuario externo a la comunicación, la recepción de una señal FHSS equivale a la recepción de ruido impulsivo de corta duración. El estándar IEEE 802.11 describe esta tecnología mediante la modulación en frecuencia FSK (Frequency Shift Keying), y con una velocidad de transferencia de 1Mbps ampliable a 2Mbps, bajo condiciones de operación óptimas.

1.5.2 Tecnología de Infrarrojos.

Una tercera tecnología definida también en el estándar 802.11 y de momento no demasiado utilizada en el ámbito comercial para implementar WLAN's, es la de infrarrojos. Los sistemas de infrarrojos se sitúan en altas

frecuencias, justo por debajo del rango de frecuencias de la luz visible. Las propiedades de los infrarrojos son, por tanto, las mismas que tiene la luz visible. De esta forma los infrarrojos no pueden pasar a través de objetos opacos, pero se pueden reflejar en determinadas superficies.

Las longitudes de onda de operación se sitúan alrededor de los 850-950 nm, es decir, a unas frecuencias de emisión que se sitúan entre los $3,15x10e^{14}$ Hz y los $3,52x10e^{14}$ Hz. Los sistemas que funcionan mediante infrarrojos, se clasifican según el ángulo de apertura con el que se emite la información en el emisor en:

- Sistemas de corta apertura, de haz dirigido o de visibilidad directa, que funcionan de manera similar a los mandos a distancia de los aparatos de televisión. Esto supone que el emisor y el receptor tienen que estar orientados adecuadamente antes de empezar a transmitirse información.
- Sistemas de gran apertura, reflejados o de difusión, que radian tal y como lo haría un foco; permitiendo el intercambio de información en un rango más amplio.

La figura 1.5 muestra un transreceptor, que es el que envía el 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. El sistema tiene un rango de 200 mts.

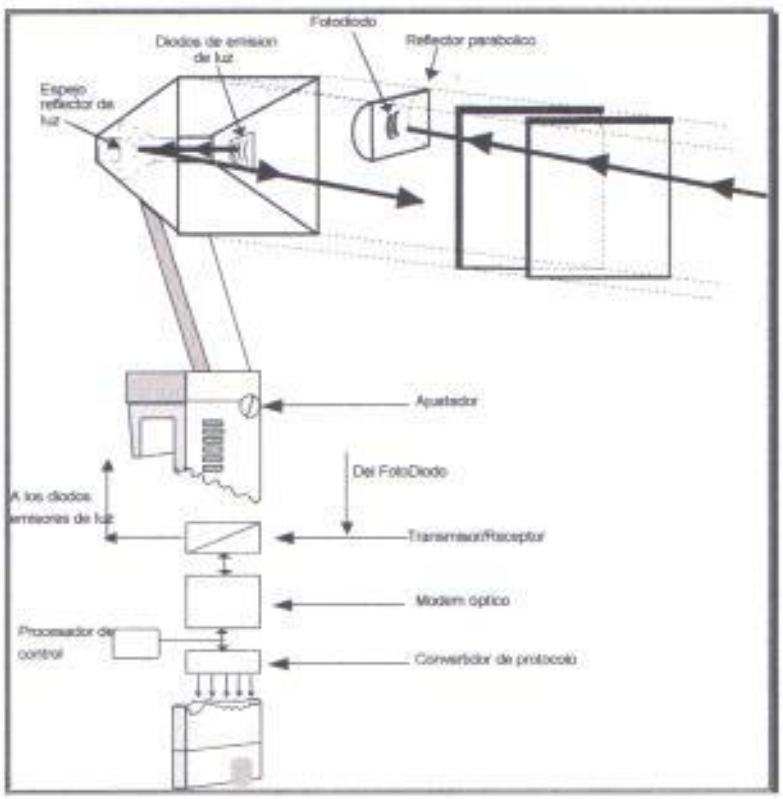


Fig 1.5: Transreceptor infrarrojo

La norma IEEE 802.11, especifica dos modulaciones para esta tecnología: la modulación 16 ppm y la modulación 4 ppm, proporcionando unas velocidades de transmisión de 1 y 2 Mbps respectivamente.

Esta tecnología, se aplica típicamente en entornos de interior para implementar enlaces punto a punto de corto alcance, o redes locales en

entornos muy localizados como puede ser un aula concreta o un laboratorio, (figura 1.6).

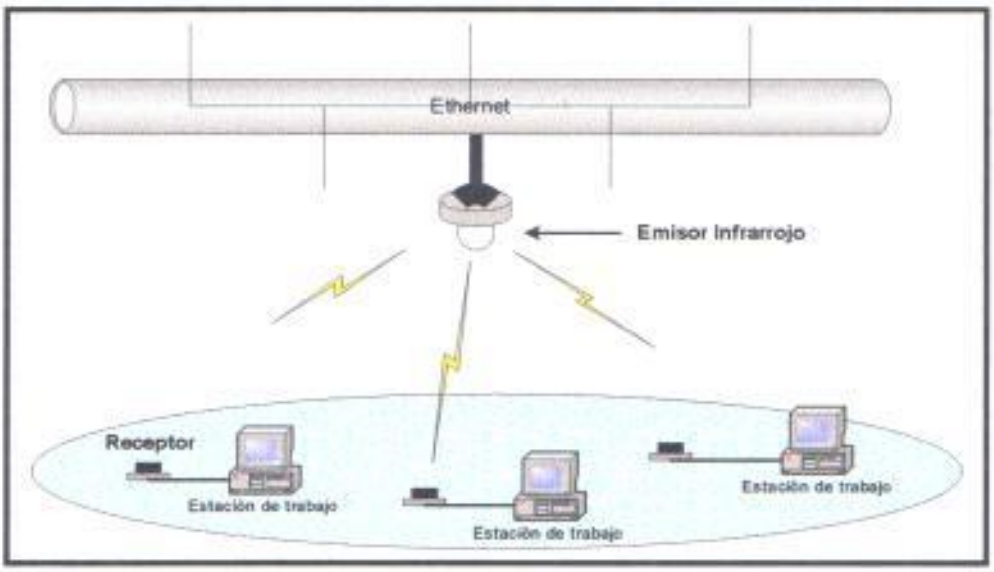


Fig 1.6: Red LAN con una célula Infrarroja

1.6 Configuraciones WLAN

El grado de complejidad de una red de área local inalámbrica es variable, dependiendo de las necesidades a cubrir y en función de los requerimientos del sistema que se quiera implementar, se pueden utilizar diversas configuraciones de red tales como:

- Punto a Punto.
- Extensión en celdas básicas.
- Enlaces entre varias LAN.

1.6.1 Punto a Punto.

La configuración más básica es la llamada *punto a punto* o *ad – hoc*, consiste en una red de dos o más terminales móviles equipados con la correspondiente tarjeta adaptadora para comunicaciones inalámbricas; en la figura 1.7 se muestra un ejemplo. Para que la comunicación entre estas estaciones sea posible, hace falta que se vean mutuamente de manera directa, es decir, que cada una de ellas esté en el rango de cobertura radioeléctrica de la otra. Las redes de tipo *ad-hoc* son muy sencillas de implementar y no requieren ningún tipo de gestión administrativa.

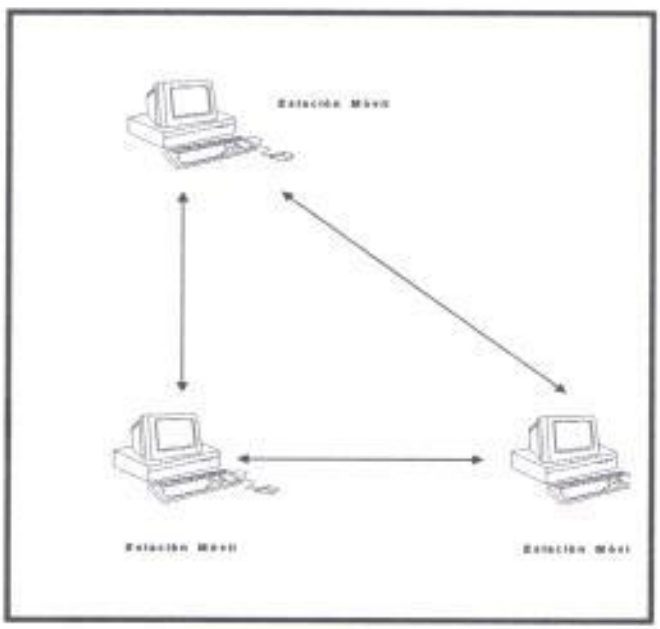


Fig 1.7: Conexiones punto a punto entre estaciones móviles

1.6.2 Extensión de las celdas básicas.

Para aumentar el alcance de una red del tipo anterior, hace falta la instalación de un ***Punto de Acceso (Access Point, AP)***. Con este nuevo elemento se dobla el alcance de la red inalámbrica (ahora la distancia máxima permitida no es entre estaciones, sino entre cada estación y el punto de acceso), en la figura 1.8 se muestra un ejemplo. Además, los *puntos de acceso* se pueden conectar a otras redes, y en particular a una red fija, con lo cual un usuario puede tener acceso desde su terminal móvil a otros recursos.

Fig 1.8: Alcance de un punto de acceso

Para dar cobertura en una zona determinada, habrá que instalar varios puntos de acceso, de tal manera que podamos cubrir la superficie necesaria

con las celdas de cobertura que proporciona cada punto de acceso, y ligeramente solapadas para permitir el paso de una celda a otra sin perder la comunicación (**roaming**).

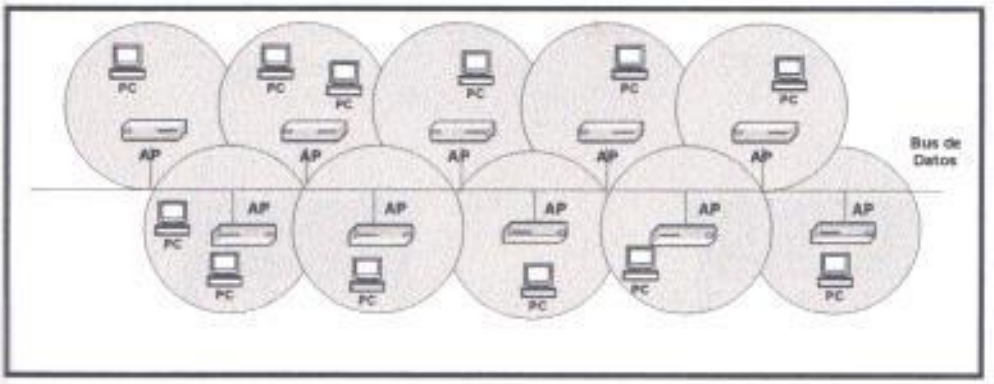


Fig 1.9: Extensión de una celda por cobertura con AP´s

1.6.3 Enlace entre varias LAN.

Para finalizar, otra de las configuraciones de red posibles es la que incluye el uso de antenas direccionales. El objetivo de estas antenas direccionales, es el de enlazar redes que se encuentran situadas geográficamente en sitios distintos tal y como se muestra en la figura 1.10. Un ejemplo de esta configuración, se tiene en el caso en que se tenga una red local en un edificio y se la quiera extender a otro edificio.

Una posible solución a este problema, consiste en instalar una antena direccional en cada edificio apuntándose mutuamente. A la vez, cada una de

estas antenas está conectada a la red local de su edificio mediante un punto de acceso. De esta manera podemos interconectar las dos redes locales.

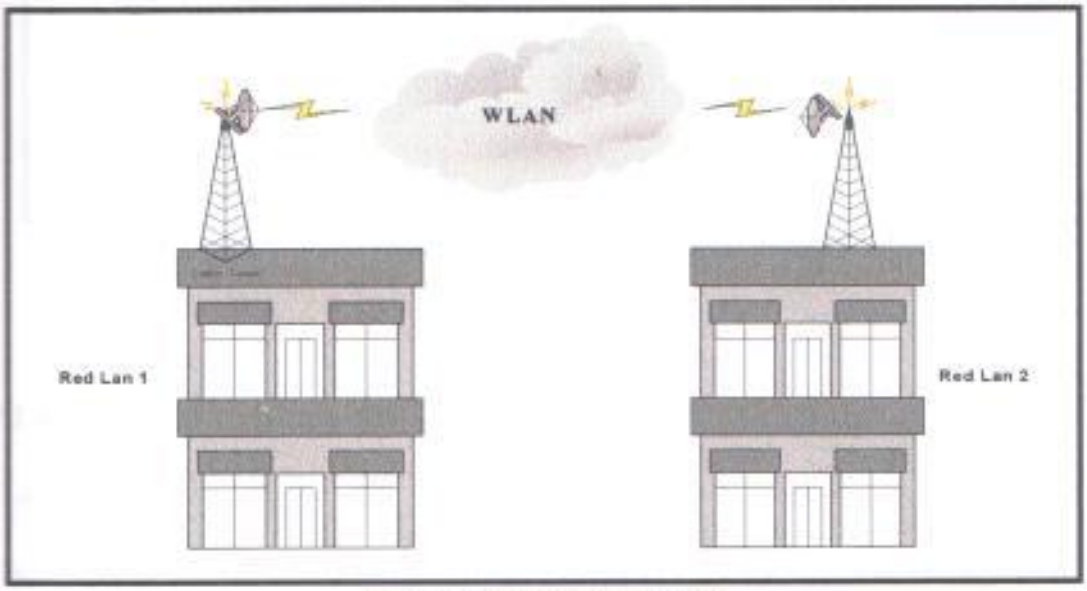


Fig 1.10: Enlace entre LAN´s

1.7 Algoritmo de Acceso Mac.

El comité IEEE ha definido un conjunto de estándares para el acceso a las redes de área local. Los diferentes métodos de acceso de la familia IEEE 802 están diseñados según el modelo de referencia OSI y se encuentran ubicados en el nivel físico y en la parte inferior del nivel de enlace o subnivel MAC, (figura 1.11).

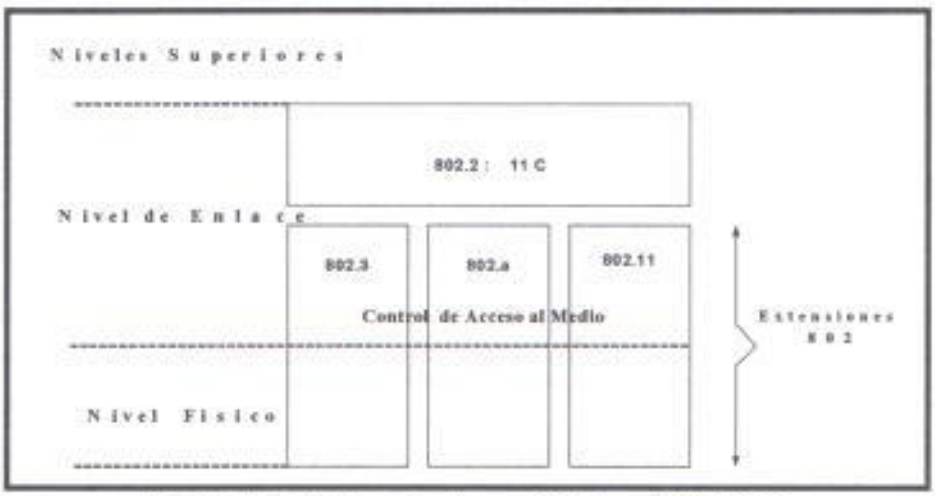


Fig 1.11: Relación entre los estándares IEEE 802.X

1.7.1 Arquitectura del Subnivel MAC.

La arquitectura MAC del estándar 802.11 se compone de dos funcionalidades básicas: la Función de Coordinación Puntual (PCF) y la Función de Coordinación Distribuida (DCF), figura 1.12

Se define *función de coordinación*, como la funcionalidad que determina, dentro de un conjunto básico de servicios (BSS), cuando una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico.

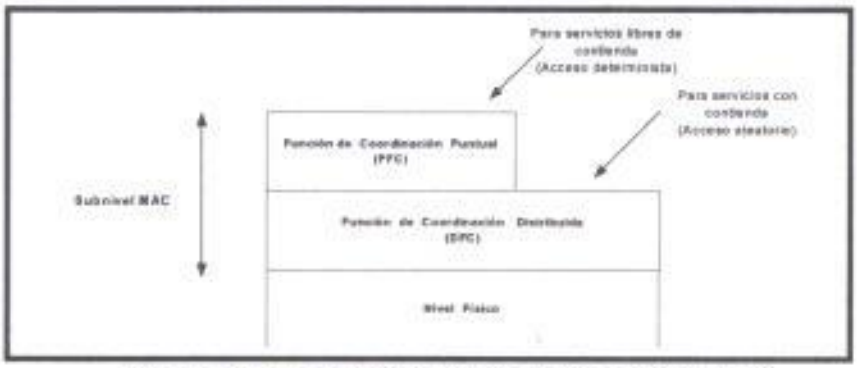


Fig 1.12: Arquitectura IEEE 802.11 de niveles 1 y 2

Función de Coordinación Distribuida.- En el nivel inferior del subnivel MAC, se encuentra la función de coordinación distribuida y su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio. El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono, ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles no tolerados por los servicios síncronos. El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 y es el llamado CSMA/CA (Carrier Sense Multiple Access / Collision Advoidance). El funcionamiento de este algoritmo se lo puede ver en la figura 1.13 y se lo describe a continuación:

1. Antes de transmitir información una estación debe testear el medio, o canal inalámbrico, para determinar su estado (libre / ocupado).
2. Si el medio está libre, la estación ejecuta una espera llamada *espaciado entre tramas* (IFS).

3. Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción, si de lo contrario el medio permanece libre durante el intervalo IFS la estación iniciará el proceso de transmisión una vez que finalice el mismo.
4. Una vez finaliza esta espera debida a la ocupación del medio, la estación ejecuta el llamado algoritmo de Backoff, según el cual se determina una espera adicional y aleatoria. El algoritmo de Backoff da un tiempo aleatorio y su función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.
5. Mientras se ejecuta la espera marcada por el algoritmo de Backoff, se continúa escuchando el medio, de tal manera que si el medio se determina libre, la estación espera el tiempo restante y luego de esto transmite. En cambio, si el medio no permanece libre el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición.

En la figura 1.13, en lugar de iniciar la transmisión de una trama inmediatamente después que el canal queda inactivo, el nodo espera un intervalo de tiempo aleatorio adicional corto (espera determinada por el algoritmo de Backoff), y sólo si después de este intervalo el canal sigue

libre, comienza a transmitir. De esta manera si hay otros nodos en espera, el nodo que calcula el tiempo mas corto obtendrá el acceso primero

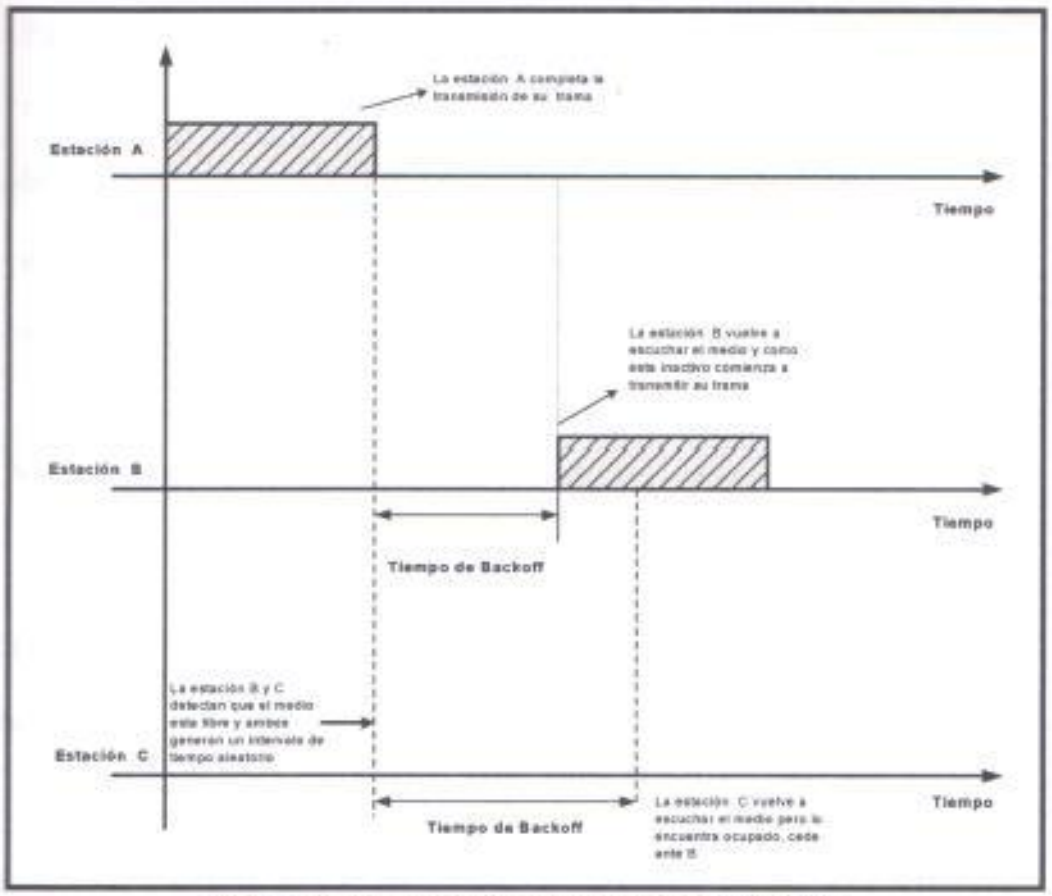


Fig 1.13: Funcionamiento del protocolo CSMA/CA

En resumen, no se puede escuchar a la vez que se trasmite, es decir no se pueden detectar colisiones. La técnica que se aplica entonces es intentar evitarlas, que es a lo que se refiere el método CSMA with Collision Avoidance, descrito anteriormente y que se puede puntualizar en:

- Si el canal está ocupado se espera a que esté libre.
- Si está libre, se espera un tiempo aleatorio, y si sigue libre se transmite.

Función de Coordinación Puntual.- Por encima de la funcionalidad DCF se sitúa la función de coordinación puntual PCF, asociada a las transmisiones libres de contienda (en el que se puede transmitir), que utilizan técnicas de acceso deterministas. Esta funcionalidad está pensada para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio.

1.8 Ventajas de una red LAN Inalámbrica sobre una LAN con cable.

En está sección se resumen algunas ventajas que presentan las WLAN con relación a las redes LAN cableadas:

Movilidad: Las redes inalámbricas pueden proveer a los usuarios de una LAN, acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red cableada.

Simplicidad y rapidez en la instalación: La instalación de una red inalámbrica puede ser tan rápida y fácil, además que puede eliminar la posibilidad de pasar cable a través de paredes y techos.

Flexibilidad en la instalación: La tecnología inalámbrica permite a la red llegar donde la cableada no puede ir.

Costo de propiedad reducido: Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en *hardware* de una LAN cableada, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

Escalabilidad: Los sistemas de WLAN's pueden ser configurados en una variedad de topologías, para satisfacer las necesidades de las instalaciones y aplicaciones especificas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

CAPITULO 2

PROTOCOLO SIMPLE DE GESTIÓN DE REDES SNMP.

Este capítulo se refiere al estudio del protocolo de gestión de redes TCP/IP más conocido y usado (SNMP), que es el protocolo de gestión mediante el cual se podrá administrar la red (WLAN) a diseñar.

2.1 Áreas Funcionales de Gestión de Red.

ISO divide la administración de la red en cinco partes que se definen dentro del Modelo de Referencia para Interconexión de Sistemas Abiertos (Open Systems Interconnection Reference Model, OSI-RM).

- Gestión de Fallos y Recuperación.
- Gestión de la Configuración.
- Gestión del Rendimiento.
- Gestión de la Contabilidad.
- Gestión de Seguridad.

Estas funciones de gestión, proporcionan todas las funcionalidades genéricas y especializadas necesarias para gestionar todas las actividades de

telecomunicaciones, como por ejemplo: la prueba de circuitos, la vigilancia de alarmas, la gestión y análisis de tráfico, etc; aplicables a diferentes dominios de telecomunicaciones como el mantenimiento de centrales, supervisión de redes de telecomunicaciones, gestión de redes de área local, etc.

A continuación se describirá cada una de estas cinco áreas funcionales de gestión de redes.

- **Gestión de Fallos y Recuperación:** Detecta, aisla y corrige las fallas, incluyendo el mantenimiento de un registro y un diagnóstico de los errores.Esta función en general comprende el conjunto de actividades orientadas a detectar, diagnosticar, anular, reparar e informar sobre los fallos de los equipos que componen las redes o los servicios de telecomunicación utilizados.

- **Gestión de la Configuración:** Administra la configuración real de la red, es decir proporciona las funciones para controlar, identificar, recoger datos de la red y suministrar datos a los diferentes elementos de la red de telecomunicaciones, con el objetivo de preparar, inicializar, gestionar y terminar los servicios.

- **Gestión del Rendimiento:** Esta área comprende, el conjunto de funciones destinada a evaluar el comportamiento de equipos de

telecomunicaciones e informar al respecto midiendo las prestaciones de los diferentes elementos de hardware, software y medios de comunicación. Mediante la medida y gestión del rendimiento, se puede asegurar que la capacidad y prestaciones de la red corresponden a las necesidades de los usuarios.

- **Gestión de la Contabilidad:** Permite analizar la utilización de cada recurso de la red por parte de un usuario o grupo de usuarios, y poder así identificar los costos de utilización de los recursos, para en función de los mismos poder establecer los cargos por consumo a los usuarios.

- **Gestión de la Seguridad:** Es el proceso para controlar el acceso a la información de la red que puede encontrarse en los elementos conectados a ella, y protege la red contra fallos intencionados o accidentales, acceso no autorizados, etc.

2.2 Normas para la Gestión de Red.

El Comité Asesor de Internet (Internet Advisory Board, IAB), ha elaborado o adoptado varias normas para la gestión de la red. En su mayoría, éstas se han diseñado específicamente para ajustarse a los requerimientos del TCP/IP, aunque, cuando es posible, cumplen con la arquitectura OSI. Un grupo de trabajo Internet, responsable de las normas para la gestión de la red, adoptó un enfoque de dos pasos para cubrir las necesidades actuales y futuras.

El primer paso comprende el uso del Protocolo Simple para la gestión de redes (Simple Network Management Protocol, SNMP), el cual fue diseñado y aplicado por el grupo de trabajo. SNMP se utiliza actualmente en muchas redes Internet, y está integrado dentro de muchos de los productos comerciales que están disponibles. Conforme se ha mejorado la tecnologia, SNMP ha evolucionado y se ha vuelto más completo.

El segundo paso comprende, las normas OSI para administración de la red, llamados Servicios Comunes de Información sobre la Administración (Common Management Information Services, CMIS), y al Protocolo Común de Información sobre la Administración (Common Management Information Protocol, CMIP), los cuales se utilizarán en las futuras aplicaciones de TCP/IP. IAB ha publicado Common Management Information Services and protocol over TCP/IP (CMOT), como una norma para TCP/IP y para la gestión OSI.

Tanto SNMP como CMOT utilizan el concepto de los administradores de red que intercambian información con los procesos que se encuentran dentro de los dispositivos de la red, como las estaciones de trabajo, los puentes, los ruteadores y los multiplexores. La estación de gestión primaria se comunica con los diferentes procesos de gestión, construyendo la información sobre el estado de la red.

La arquitectura tanto de SNMP como de CMOT es tal, que la información recopilada se almacena de una forma que permita a otros protocolos leerla.

2.3 Arquitectura SNMP

El Protocolo simple de gestión de redes (SNMP), fue diseñado originalmente para proporcionar un medio para manejar los ruteadores de una red. SNMP, aunque es parte de la familia de protocolos TCP/IP, no depende del IP.

SNMP fue diseñado para ser independiente del protocolo (de manera que pueda correr igual de fácil bajo IPX de SPX/IPX de Novell, por ejemplo), aunque la mayor parte de las instalaciones SNMP utilicen IP en redes TCP/IP.

2.3.1 Elementos del Sistema de Gestión.

El modelo de gestión de red utilizado para la gestión de redes TCP/IP contiene los siguientes elementos clave (figura 2.1):

- Estación de Gestión.
- Agente de Gestión.
- Base de Gestión de Información (MIB).
- Protocolo de Gestión de Redes (SNMP).

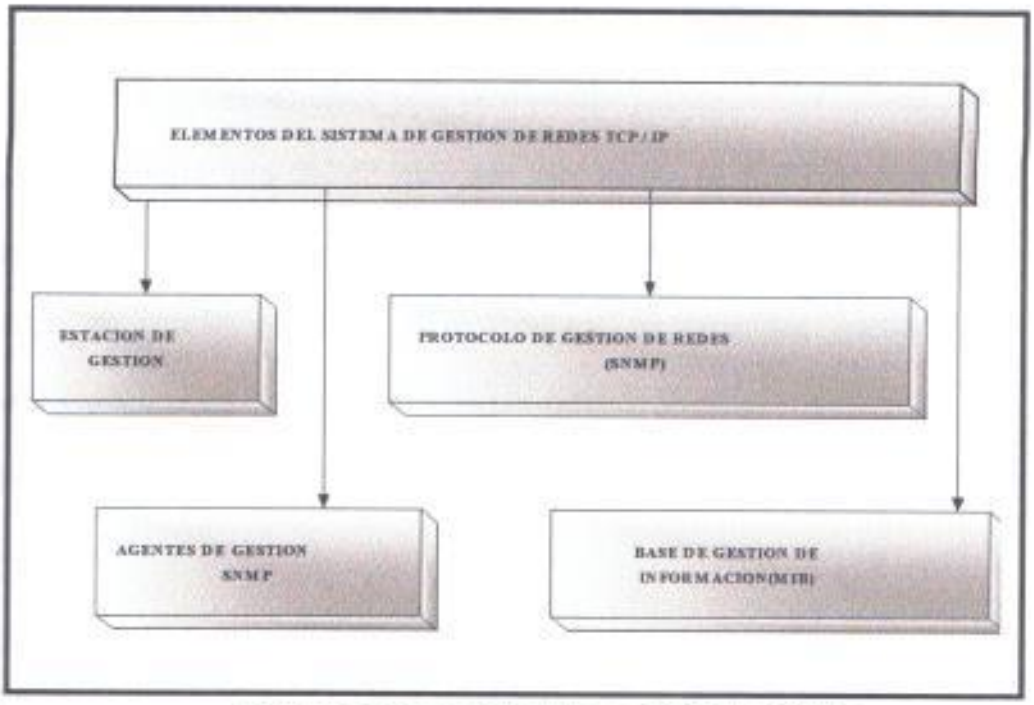


Fig 2.1: Elementos del sistema de Gestión SNMP

Estación de gestión.- Es tipicamente, un dispositivo dedicado a las tareas de gestión, aunque también puede dedicarse a otras tareas. En cualquier caso, la estación de gestión sirve como interface entre el gestor de redes (humano) y el sistema de gestión de red.

En la estación de gestión reside un software denominado SNMP manager; se trata de una entidad que puede preguntar a los agentes utilizando operaciones SNMP. Además proporciona una interface generalmente gráfica, que permite a los usuarios pedir datos o visualizar alarmas, además almacena los datos permitiendo analizar tendencias.

Agente de gestión.- Es el otro elemento activo en el sistema de gestión de redes. Las plataformas clave tales como hosts, puentes, routers y hubs, se pueden equipar con SNMP para ser gestionadas desde la estación de gestión. El agente de gestión, es un software que proporciona acceso a los datos de gestión de un dispositivo de red en particular, responde a peticiones de información y acciones por parte de la estación de gestión; y puede enviar a ella cierta información importante no solicitada de un modo asíncrono.

Los dispositivos situados en la red son gestionados mediante transacciones entre el gestor y el agente SNMP. SNMP proporciona dos clases de transacciones de gestión:

- Petición por parte del gestor SNMP y respuesta por parte del agente SNMP (sondeo).
- Notificaciones no solicitadas (Traps) desde el agente al gestor.

Base de Gestión de la Información (MIB).- Para poder gestionar los recursos, estos son representados como objetos. Cada objeto es, esencialmente, una variable que representa un aspecto del agente gestionado. Al conjunto de objetos se le denomina MIB; la MIB funciona como un conjunto de puntos de acceso al agente desde la estación de gestión. Una estación de gestión realiza la función de monitorización,

leyendo el valor de los objetos de la MIB (en la sección 2.3.2.1 se explica en detalle las entradas y tipos de MIB que existen)

Protocolo de Gestión de redes (SNMP).- Es utilizado, para la comunicación entre la estación de gestión y los agentes (este elemento se analiza detalladamente en la sección 2.3.2.3)

2.3.2 Familia de Protocolos SNMP.

SNMP no es un solo protocolo, sino tres protocolos que juntos forman una familia; todos diseñados para trabajar en pro de las metas de la gestión. Los protocolos que conforman la familia SNMP y sus papeles se detallan a continuación:

- **Base de Gestión de Información (MIB):** Una base de datos que contiene información sobre los elementos a gestionar.
- **Estructura e Identificación de la Información sobre la Gestión (SMI):** Describe cómo están definidos los objetos gestionados en la MIB.
- **Protocolo Simple de Gestión de Redes (SNMP):** Define el protocolo usado para gestionar estos objetos.

2.3.2.1 MIB, Base de Gestión de la Información.

El estándar especifica los elementos de los datos que un equipo debe conservar y las operaciones permitidas en cada uno.

Cada dispositivo gestionado por SNMP, mantiene una base de datos que contiene estadísticas y otro tipo de información. Estas bases de datos se llaman Base de Gestión de Información, o MIB

Entradas de la MIB

Las entradas de la MIB tienen cuatro datos:

- Un tipo de objeto.
- Una sintaxis.
- Un campo de acceso.
- Un campo de estado.

Las entradas MIB generalmente las estandarizan protocolos y siguen reglas estrictas para el formateo, definidas por la Notación para Sintaxis Abstracta Uno (Abstract Syntax Notation One, ASN. I).

Para explicar las cuatro entradas que tiene la MIB se muestra la siguiente definición de objeto:

```
TcpRtoAlgorithm OBJECT-TYPE
        SYNTAX INTEGER {
                Other(1), -- none of the following
                constant(2), --a constant rto
                rsre(3), --MILSTD-1778, Appendix B
                vanj(4) – Van Jacobson's algorithrn [10]
        ACCESS read-only
        STATUS mandatory
        DESCRIPTION
                "The algorithm used to determine the timeout
                value used for retransmitting unacknowiedged
                octects"
        ::= {tcp 1}
```

En el ejemplo anterior, se define un objeto gestionable. Los siguientes puntos explican las entradas:

TcpRtoAlgorithm.- Es **el tipo de objeto,** que define el nombre de la entrada especifica, generalmente a manera de un simple nombre. Todos los objetos SNMP se definen utilizando la macro OBJET-TYPE, que realiza una asignación de valor para definir el OBJECT-IDENTIFIER del objeto, y también captura la semántica del objeto.

La sintaxis (SINTAX).- Especifica el tipo de objeto, que en este caso es INTEGER. Realmente se trata de un "enumered INTEGER". El valor de un "entero numerado" esta restringido a uno de los valores listados explícitamente, que en este ejemplo es 1,2,3 y 4. El nombre asociado a cada valor facilita la comprensión para las personas.

El campo de acceso (ACCESS).- Especifica el acceso máximo al objeto. Los derechos de acceso pueden ser menores dependiendo del comunity string utilizado y la implementación particular de la MIB. Los valores posible son:

- read-Only
- read-write
- write-only
- not-accesible

El campo de estado (STATUS).- Proporciona información sobre el estado del objeto. Los valores posibles son:

- Mandatory: Indica que el objeto debe ser implementado.
- Optional: Nunca se usa, pues por convenio en SNMP, si se implementa un objeto dentro de un grupo, el resto de objetos del mismo grupo deberían ser implementados. Un grupo, es un conjunto de objetos que cuelgan de un nodo común. En el ejemplo "tcp" es un grupo.
- Obsolete: Indica que el objeto ya no soporta.
- Deprecated: Indica que el objeto se está desfasando y dentro de un tiempo pasará a ser obsoleto.

Tipos de MIB.

Existen dos tipos de MIB, llamados MIB-1 y MIB-2. Las estructuras son diferentes. MIB-1 se utilizó a principios de 1988 y tiene 114 entradas en la tabla, las cuales están divididas en grupos. Para que un dispositivo administrado pueda ser compatible con MIB-1, debe manejar grupos que son aplicables a ésta. Por ejemplo, una impresora administrada no tiene que aplicar todas las entradas que traten con el Protocolo para Gateway Exterior (Exterior Gateway Protocol EGP), el cual generalmente lo aplican solamente los ruteadores y los dispositivos similares.

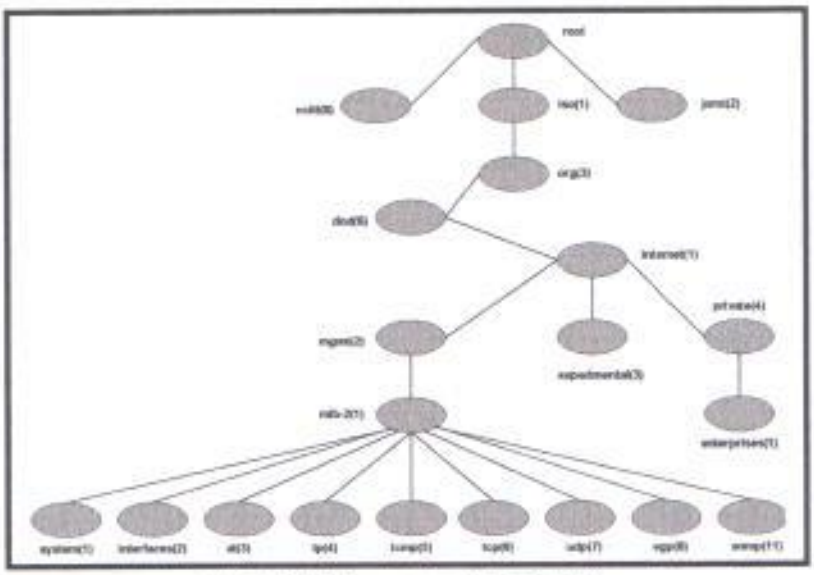


Fig 2.2: Vista general del la MIB

MIB-2, es una ampliación a MIB-1 hecha en 1990, está conformada por 171 entradas que están divididas en nueve grupos (figura 2.2). Las adiciones amplían algunas de las entradas de los grupos básicos de MIB-1 y agregan tres nuevos grupos. Al igual que con MIB-1, un dispositivo SNMP que pretenda ser compatible con MIB-2 debe adaptar todos esos grupos que son aplicables a ese tipo de dispositivo. Se encontrarán muchos dispositivos que son compatibles con MIB-1 pero que no lo son con MIB-2.

La MIB para TCP/IP, divide la información de la administración en 9 categorías así como muestra la tabla I.

Categoria MIB	Incluye información sobre
System	Descripción del Sistema
Interfaces	Descripción de las Interfaces del sistema
Addr.trans.	Mapping entre direcciones físicas e IP
Ip	Estadísticas del Protocolo de Internet
Icmp	Estadísticas del Protocolo de Mensajes de Control de Internet
Tcp	Estadísticas del Protocolo de Transmisión de Internet
Udp	Estadísticas del Protocolo de Datagrama de Usuario
egp	Estadísticas de Protocolo de Compuerta Exterior
SNMP	Estadísticas del propio protocolo SNMP

Tabla I: Grupos de la MIB II

2.3.2.2 SMI, Estructura de la Información de Administración (*Structure of Management Information)*

La estructura de la información de gestión, define el marco de trabajo general dentro del cual una MIB puede ser definida y construida. SMI identifica los tipos de datos que pueden ser usados en la MIB y como se representan y nombran a los recursos dentro de la misma.

SMI establece restricciones a los tipos de variables permitidas en MIB, especifica las reglas para nombrar tales variables y crea reglas para definir tipos de variables. Por ejemplo, el estándar SMI incluye definiciones de términos como *IpAddress* (definiéndolo como una cadena de cuatro octetos) y *Counter* (definida como un entero en el rango de 0 a 2^{32}-1), y especifica que son los términos utilizados para definir variables MIB.

Algo muy importante, las reglas en SMI describen cómo se refiere MIB a las tablas de valores (por ejemplo, la tabla de ruteo IP).

2.3.2.3 SNMP, Protocolo Simple de Gestión de Redes (Simple Network Management Protocol, SNMP).

Por lo general, SNMP se utiliza como una aplicación cliente/servidor asincrónica, lo que significa que tanto el dispositivo gestionado como el

software servidor SNMP pueden generar un mensaje para el otro y esperar una respuesta, en caso de que haya que esperar una; ambos lo empaquetan y manejan el software para la red (como el IP), como lo haría cualquier otro paquete.

SNMP utiliza UDP (User Datagram Protocol), como un protocolo de transporte de mensajes. El puerto 161 de UDP se utiliza para todos los mensajes, excepto para los traps, que llegan el puerto 162 de UDP. Los agentes reciben sus mensajes del administrador a través del puerto UDP 161 del agente.

Comandos utilizados en SNMP.

Conceptualmente, el SNMP contiene sólo dos comandos que permiten a un administrador buscar y obtener un valor desde un elemento de datos (GET), o almacenar un valor en un elemento de datos (SET). Todas las otras operaciones, se definen como consecuencia de estas dos operaciones.

El SNMP es especialmente estable ya que sus definiciones se mantienen fijas, aún cuando nuevos elementos de datos se añadan a la MIB y se definan nuevas operaciones como efectos del almacenamiento de esos elementos.

Desde el punto de vista de los administradores, por supuesto, el SNMP se mantiene oculto. Un usuario de una interfaz para software de administración de red puede expresar operaciones como comandos imperativos (por ejemplo, arrancar).

Así pues, hay una pequeña diferencia visible entre la forma en que un administrador utiliza SNMP y otros protocolos de administración de red.

El SNMP ofrece más que las dos operaciones que se han descrito:

- **Get Request:** Comando para la obtención del valor de la variable de la MIB de un dispositivo de red.
- **GetNextRequest:** Comando para la obtención del valor siguiente (en orden lexicográfico) al solicitado en la anterior primitiva GetRequest.
- **SetRequest:** Comando para la modificación de variables en la MIB del agente SNMP.
- **GetResponse:** Comando empleado por el agente SNMP para devolver al gestor los datos solicitados.
- **Trap:** Este es un comando especial que los agentes pueden enviar asincronicamente a un gestor para notificar determinadas condiciones e estados, previamente definidos.

Versiones de SNMP.

SNMP ha pasado por varias iteraciones. La versión más utilizada se llama SNMP v1.

SNMP v2, añade algunas nuevas posibilidades a la versión anterior de SNMP, de las cuales, la más útil para los servidores es la operación *get-bulk*. Esta permite que se envien un gran número de entradas MIB en un solo mensaje, en vez de requerir múltiples consultas *get-next* para SNMP v1.

Para corregir las deficiencias de seguridad que hasta ahora venian arrastrando SNMPv1/SNMPv2 fueron presentadas una serie de recomendaciones en Enero de 1998. Estas recomendaciones están orientadas a definir una arquitectura y nuevas capacidades en cuanto a seguridad.

SNMPv3, es un protocolo de manejo de red interoperable, que proporciona seguridad de acceso a los dispositivos por medio de una combinación de autenticación y encripción de paquetes que trafican por la red. Las capacidades de seguridad que SNMPv3 proporcionan son:

- Integridad del Mensaje: Asegura que el paquete no haya sido violado durante la transmisión.
- Autenticación: Determina que el mensaje proviene de una fuente válida.
- Encripción: Encripta el contenido de un paquete como forma de prevención.

Es importante resaltar que SNMPv3, no es un reemplazo de SNMPv1 ó SNMPv2. SNMPv3 define una serie de nuevas capacidades a ser utilizadas en conjunto con SNMPv2 (preferiblemente) y SNMPv1.

Seguridad en SNMP.

El sistema de seguridad de SNMP, está basado en el concepto de **community** (comunidad); una comunidad es una relación entre un agente SNMP y un conjunto de estaciones de gestión SNMP, que define unas características de autentificación y control de acceso. El agente establece una comunidad para cada combinación deseada de autentificación y control de acceso, y a cada comunidad se le da un nombre (community name), que es único dentro del agente.

Las estaciones de gestión pertenecientes a una comunidad, deberán emplear ese nombre de comunidad en todas las operaciones get y set. El agente puede establecer cualquier número de comunidades, pudiendo pertenecer una misma estación de gestión a varias comunidades.

Puesto que las comunidades se definen localmente para un agente, se puede emplear el mismo nombre para varios agentes. Una estación de gestión deberá almacenar los nombres de comunidad asociados con cada uno de los agentes a los que desea acceder.

Cuando un agente define una comunidad, está limitando el acceso a su MIB a un cierto conjunto de estaciones de gestión. Si utiliza más de una comunidad, el agente puede proporcionar diferentes categorías de acceso a las estaciones de gestión. Este **control de acceso** tiene dos vertientes:

- Vista de la MIB SNMP: Es un subconjunto de los objetos de una MIB. Se pueden definir diferentes vistas de la MIB para las distintas comunidades. Estos objetos no necesitan pertenecer a la misma rama del árbol.
- Modo de acceso SNMP: Este podrá ser READ-ONLY o READ-WRITE .Para cada comunidad se definirá un método de acceso.

A la combinación de una vista de la MIB y de un modo de acceso se le denomina SNMP community profile (perfil de comunidad SNMP). El modo de acceso se aplicará uniformemente a todos los objetos de la vista de la MIB.

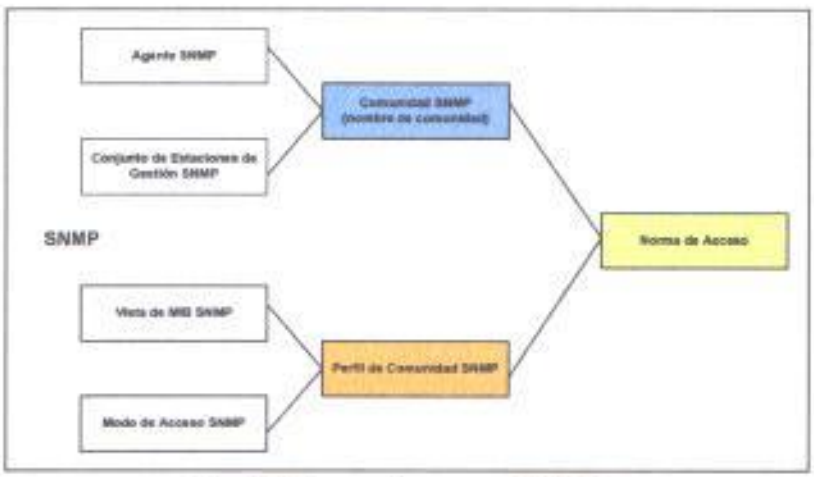


Fig 2.3 Norma de acceso SNMP

A cada comunidad se le asocia un perfil de comunidad, denominándose a esta asociación access policy (norma de acceso SNMP), figura 2.3

Tal y como podemos deducir, SNMP utiliza un sistema de seguridad muy limitado. Cada PDU (Protocol Data Unit) contiene el nombre de comunidad, que es equivalente a una contraseña. Al configurar un dispositivo gestionable SNMP, se puede configurar un community

name que permita el acceso de lectura y escritura a ciertos objetos del dispositivo, y otro community name que limita el acceso a solo lectura.

La petición realizada por la estación de gestión únicamente es atendida si el community name es correcto. En caso de ser incorrecto, el agente SNMP no envía ninguna respuesta. Si no se especifica el community name, por defecto suele ser "public", permitiendo cualquier acceso.

A pesar de su extenso uso, SNMP tiene algunas desventajas. La más importante es que se apoya en UDP (User Datagram Protocol). Puesto que UDP no tiene conexiones, no existe contabilidad inherente al enviar los mensajes entre el servidor y el agente.

Otro problema es que SNMP proporciona un solo protocolo para mensajes, por lo que no pueden realizarse los mensajes de filtrado. Esto incrementa la carga del software receptor. Finalmente, SNMP casi siempre utiliza el sondeo en cierto grado, lo que ocupa una considerable cantidad de ancho de banda.

2.4 Funcionamiento SNMP.

SNMP fue diseñado para ser un protocolo de nivel de aplicación formando parte de la familia de protocolos TCP/IP. Opera por encima de UDP. La figura 2.4 sugiere la típica configuración de protocolos para SNMP. En una estación de gestión dedicada, hay un proceso gestor que controla el acceso a la MIB central en la estación de gestión y proporciona una interface al gestor de red.

El proceso gestor realiza la gestión de red usando SNMP, el cual está por encima de UDP, IP, y los protocolos relevantes dependientes de la red (ej: Ethernet, FDDI, X25).

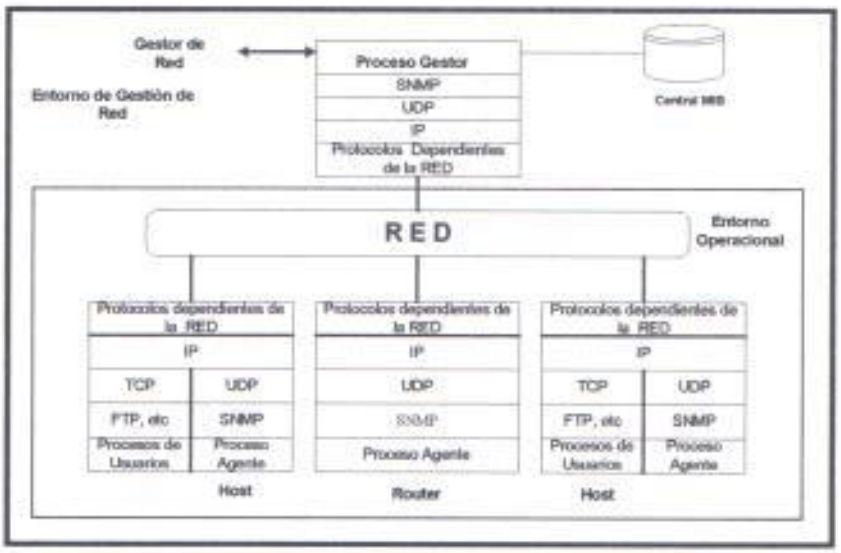


Fig 2.4: Enclave de SNMP dentro de los protocolos TCP/IP

Cada agente también debe implementar SNMP, UDP e IP. Además, hay un proceso agente que interpreta los mensajes SNMP y controla la MIB del

agente. Para un dispositivo agente que soporta otras aplicaciones, como FTP o TELNET, se requiere TCP además de UDP.

La figura 2.5 proporciona una panorámica mas detallada del contexto del protocolo de SNMP. Desde una estación de gestión se pueden enviar tres tipos de mensajes a saber: GetRequest, GetNextRequest y SetRequest. Los dos primeros son variaciones de Get. Los tres mensajes son reconocidos por el agente mediante un mensaje GetResponse, el cual es pasado a la aplicación de gestión. Además un agente puede emitir un mensaje Trap en respuesta a un evento que afecte a la MIB y a los recursos gestionados.

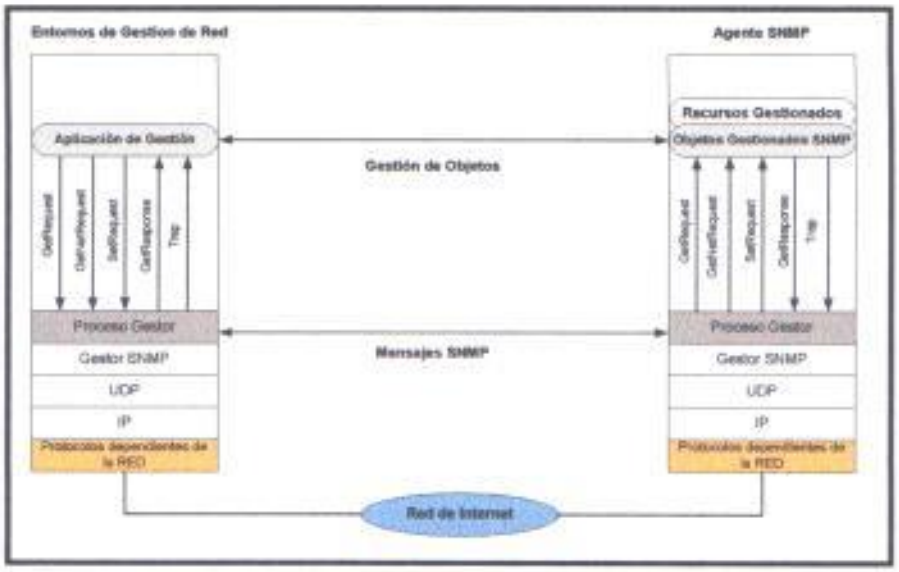


Fig 2.5: Enclave del agente y Administrador SNMP

SNMP es un protocolo no orientado a conexión, pues utiliza UDP, por lo que no se mantienen las conexiones entre la estación de gestión y sus agentes. Por

lo tanto, cada intercambio es una transacción separada entre la estación de gestión y un agente. El mensaje GetNextRequest es similar al GetRequest, pero permite al gestor extraer datos de una tabla. Por otro lado, si el gestor pide cambiar el valor de ciertas variables utilizando un PDU del tipo SetRequest, el agente los deberá cambiar todos, es decir el agente cambiará o todos los valores o ninguno.

Para cada PDU de "petición", hay exactamente un PDU de "respuesta". Es el caso de un Getrequest o un GetNextRequest, el PDU de respuesta traerá un estatus de error en el caso de que falle el set, o bien la respuesta será idéntica a la petición (y todas las variables utilizadas).

El agente puede incluir los nombres y valores de ciertos objetos en el PDU del trap para proporcionar al administrador información adicional sobre el evento. Es importante resaltar la falta de confirmación del gestor para indicar que se ha recibido el trap.

Los periféricos que tienen integradas las capacidades para SNMP corren un paquete de software agente para gestión, cargado como parte de un ciclo de arranque o incrustado en la memoria fija (firmware) del dispositivo. Estos dispositivos que tienen agentes SNMP se dice que se tratan de dispositivos gestionados.

Los dispositivos gestionados por SNMP se comunican con el software servidor SNMP, que está localizado en cualquier parte de la red. El dispositivo habla con el servidor de dos formas como ya se había mencionado: por sondeo o por interrupciones (traps).

Un dispositivo sondeado hace que el servidor se comunique con el dispositivo, preguntándole sobre su condición o sobre sus estadísticas actuales. El sondeo en ocasiones se hace en intervalos regulares, teniendo al servidor conectado a todos los dispositivos gestionados de la red. El problema con el sondeo es que la información no siempre es actual, el tráfico de la red se incrementa con el número de dispositivos administrados y la frecuencia del sondeo.

Un sistema SNMP basado en la interrupción (traps), hace que el dispositivo gestionado envie mensajes al servidor cuando algunas condiciones lo garanticen. De esta forma, el servidor conoce inmediatamente cualquier problema (a menos que el dispositivo falle, en cuyo caso la notificación debe hacerse desde otro dispositivo que haya tratado de comunicarse con el dispositivo que falló).

Los dispositivos basados en traps tienen sus propios problemas; en primer lugar entre los problemas está la necesidad de ensamblar un mensaje para el servidor, lo que puede requerir de una gran cantidad de ciclos del CPU, todos los cuales se toman de la tarea normal del dispositivo. Esto puede provocar cuellos de botella y otros problemas en el dispositivo. Si el mensaje que va a enviarse es extenso, como sucede cuando contiene una gran cantidad de estadísticas, la red puede padecer de una notable degradación mientras el mensaje se ensambla y transmite.

Si existe una falla mayor en cualquier parte de la red, como cuando falla la corriente eléctrica y se activan las fuentes de energía, cada dispositivo administrado por SNMP tratará de enviar al mismo tiempo, mensajes controlados por interrupción hacia el servidor, para reportar el problema. Esto puede congestionar la red y producir una información errónea en el servidor.

A menudo se utiliza una combinación de sondeo y de interrupción para sobreponerse a todos estos problemas. La combinación se llama sondeo dirigido por traps, e implica que el servidor haga un sondeo de las estadísticas a intervalos regulares, o cada vez que lo ordene el administrador de sistema. Además, cada dispositivo gestionado por SNMP puede generar un mensaje de interrupción cuando se presenten ciertas condiciones, pero estos mensajes

tienden a estar más rigurosamente definidos que en el simple sistema controlado por interrupción. Por ejemplo, si utiliza SNMP sólo mediante traps, un ruteador puede reportar un incremento de la carga cada 10 por ciento. Si utiliza un sondeo dirigido por traps, se conoce la carga del sondeo regular y se puede dar instrucciones al ruteador, para enviar una sola interrupción cuando se experimente un incremento significativo en la carga.

Después de recibir un mensaje con sondeo dirigido por traps, el servidor puede seguir sondeando al dispositivo para mayores detalles, en caso de ser necesario.

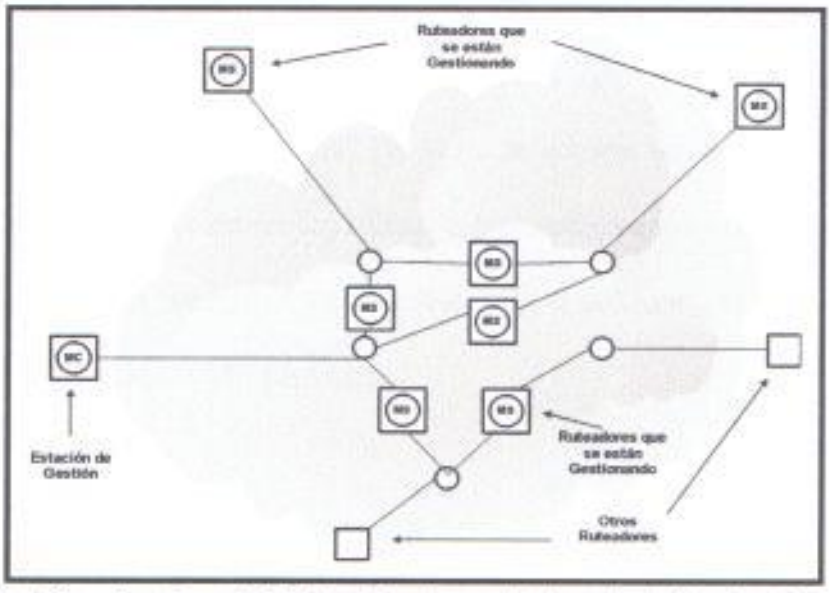


Fig 2.6: Ejemplo de administración de red. Un administrador invoca al software de gestión del cliente (MC) que conecta al software servidor de gestión (MS) en los ruteadores, a través de la red.

La computadora del administrador no necesita conectarse directamente hacia todas las redes físicas que contiene entidades gestionadas. Un paquete de software servidor SNMP puede comunicarse con los agentes SNMP y transferir o solicitar diferentes tipos de información.

Generalmente, el servidor solicita las estadísticas del agente incluyendo el número de paquetes que se manejan, el estado del dispositivo, las condiciones especiales que están asociadas con el tipo de dispositivo (como las indicaciones de que se terminó el papel o la pérdida de la conexión en un módem), y la carga del procesador.

El servidor también puede enviar instrucciones al agente para modificar las entradas de su base de datos MIB (la Base de gestión de Información). El servidor también puede enviar los límites o las condiciones bajo las cuales el agente SNMP debe generar un mensaje trap para el servidor, como cuando la carga del CPU alcanza el 90 por ciento.

Las comunicaciones entre el servidor y el agente se llevan a cabo de una forma un tanto sencilla, aunque tienden a utilizar una notación abstracta para el contenido de sus mensajes. Por ejemplo, el servidor puede enviar un mensaje *what is your current load* y recibir un mensaje del 75%. El agente nunca envía

datos hacia el servidor, a menos que se genere un trap o se haga una solicitud de sondeo. Esto significa que pueden existir algunos problemas constantes sin que el servidor SNMP sepa de ellos, simplemente porque no se realizó un sondeo ni se generó interrupción.

CAPITULO 3

INFRAESTRUCTURA DE LA RED ACTUAL.

3.1 Introducción

Para poder diseñar y gestionar la WLAN se tomó como base y referencia la red LAN del ISP Satlink S.A., que es un proveedor de Internet nuevo el cual funciona en un edificio de 4 plantas.

3.2 Distribución de la Infraestructura Interna de la Compañía Satlink S.A.

A continuación, se detalla la distribución de cada departamento en el edificio para que se tenga una idea de cómo esta estructurada la empresa y en el momento especifico del diseño de la WLAN, guiarse en la ubicación de él o los puntos de acceso necesarios para la red:

Planta Baja, Recepción, Contabilidad y Cobranzas

Primer piso, Presidencia y Servicio al Cliente.

Segundo piso, Gerencia General y Comercialización.

Tercer Piso, Departamento Técnico y Bodega.

El Backbone de la red de Satlink, se concentra en el tercer piso en el área técnica; en un rac de comunicaciones donde se encuentra todo su equipamiento (figura 3.5)

3.3 Descripción Básica de la Red actual.

Como ya se había mencionado, Satlink es un proveedor de servicios de internet por lo tanto cuenta con un equipamiento especial dedicado a brindar este acceso a clientes.

A continuación, se presenta de manera general un diagrama que corresponde a la red del ISP Satlink:

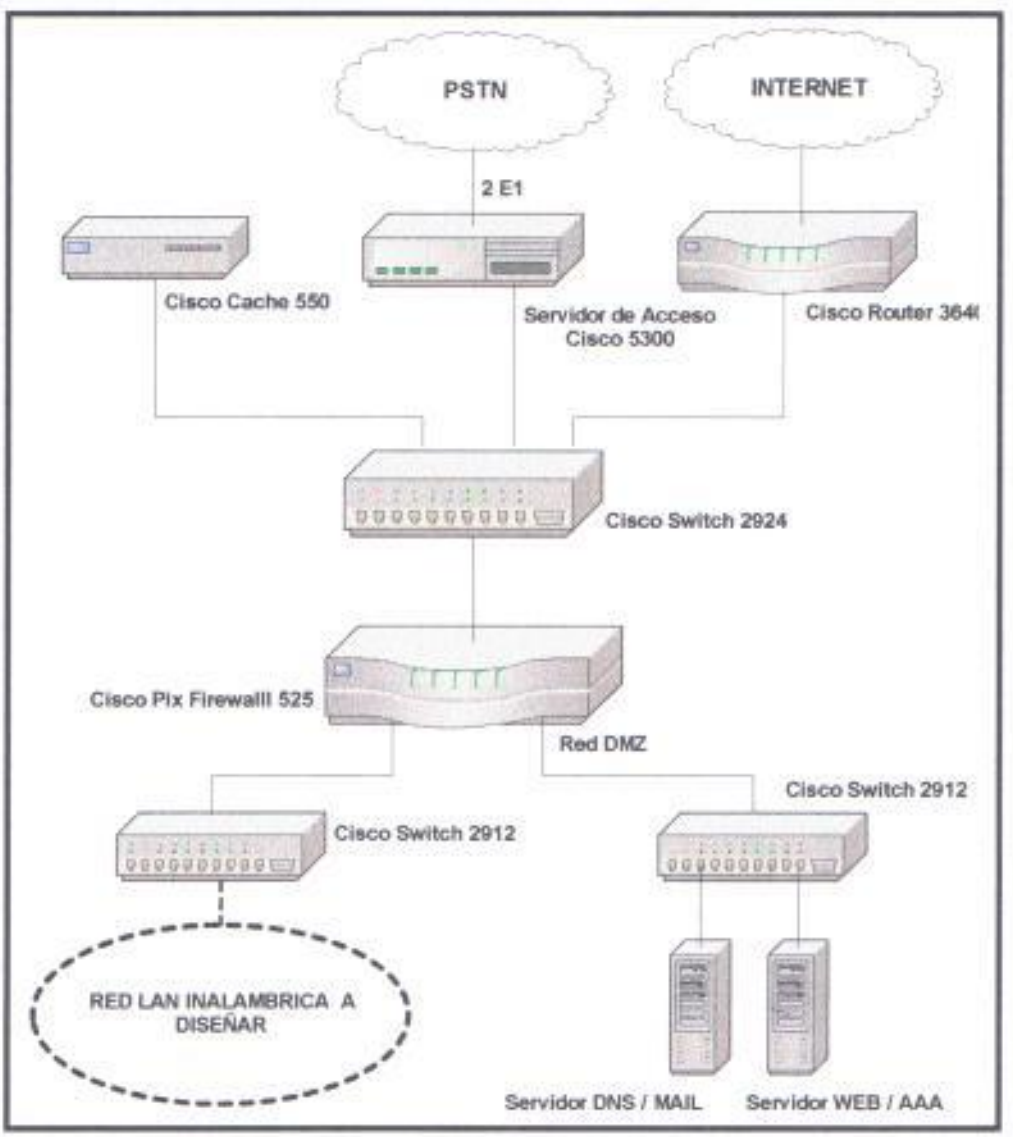


Fig 3.1: Red del ISP SATLINK S.A.

Esta red consta de los siguientes equipos:

Ruteador Cisco 3640.

Es el que brinda la salida a Internet a través de un enlace satelital, el uso de este equipo garantiza la posibilidad de escalar la red y también de que se pueda disponer de la tecnologia mas adecuada para nuevos servicios que surjan, como pueden ser: Servicios Multimedia, Voip, Redes Privadas Virtuales, etc.

Servidor de Acceso Cisco 5300.

Este equipo, permite el acceso de los usuarios dial up a través de los 2 canales E1 (60 lineas digitales).

Servidor Web Cache Cisco 550.

Este equipo permite el almacenamiento de páginas web visitadas por los usuarios, para optimizar el enlace de salida a Internet; cuando un nuevo usuario trate de navegar en páginas ya registradas en el cache de este equipo.

Switch Cisco Catalyst 2924.

Este switch es el nodo principal donde se conectan el ruteador, servidor de acceso, servidor cache y Firewall.

Firewall Cisco Pix 525.

Es el equipo que brinda la seguridad a la red, segmenta lógica y físicamente la misma; además controla el flujo de información de entrada y salida a la red privada de SATLINK. Este equipo maneja la asignación de la traducción de las direcciones de la red privada a direcciones públicas (NAT), para los paquetes que salen a Internet.

El Firewall tiene dos salidas ethernet, de las cuales una está siendo usada para la conexión de un switch Cisco 2912 en donde se concentra la red DMZ (zona desmilitarizada). En la segunda salida ethernet del firewall se conecta el otro switch Cisco 2912, que es donde se concentrará la WLAN.

Switch Cisco Catalyst 2912.

En la red aparecen dos switchs de este modelo, por un lado uno de ellos sirve para la conexión de los servidores (WEB, AAA, DNS, MAIL), mientras que el otro switch sirve para la conexión de la red inalámbrica a diseñar (figura 3.1), en el capítulo 5 se explica detalladamente este diseño. Esta red (WLAN) permitirá a los usuarios compartir recursos tales como archivos, impresoras, diskettes, etc, y hasta el acceso a internet proporcionado por el ruteador mencionado anteriormente.

3.4 Distribución de las PC´s en cada departamento.

Satlink cuenta con 11 PC´s, las cuales se encuentran distribuidas de la siguiente manera en el edificio.

Recepción, contabilidad y cobranzas, cuentan con 3 PC´s de escritorio, una para cada lugar de trabajo, (figura 3.2).

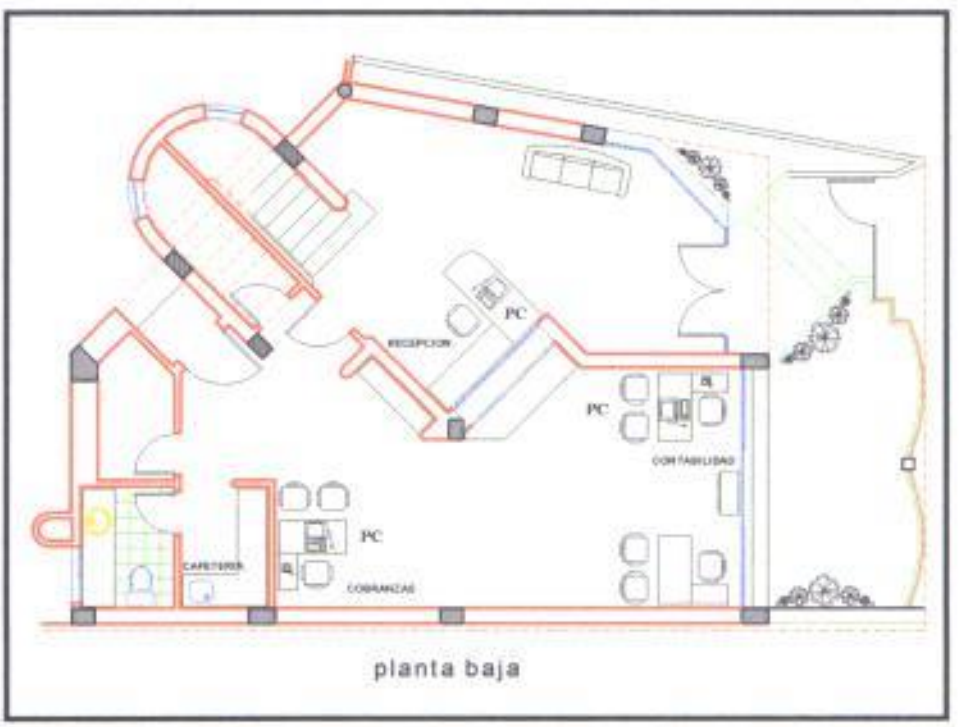


Fig 3.2: Ubicación de las PC´s en Planta Baja

Presidencia, secretaria de presidencia y servicio al cliente cuentan también con 3 PC´s, de las cuales una es portátil (presidencia) y el resto de escritorio (figura 3.3)

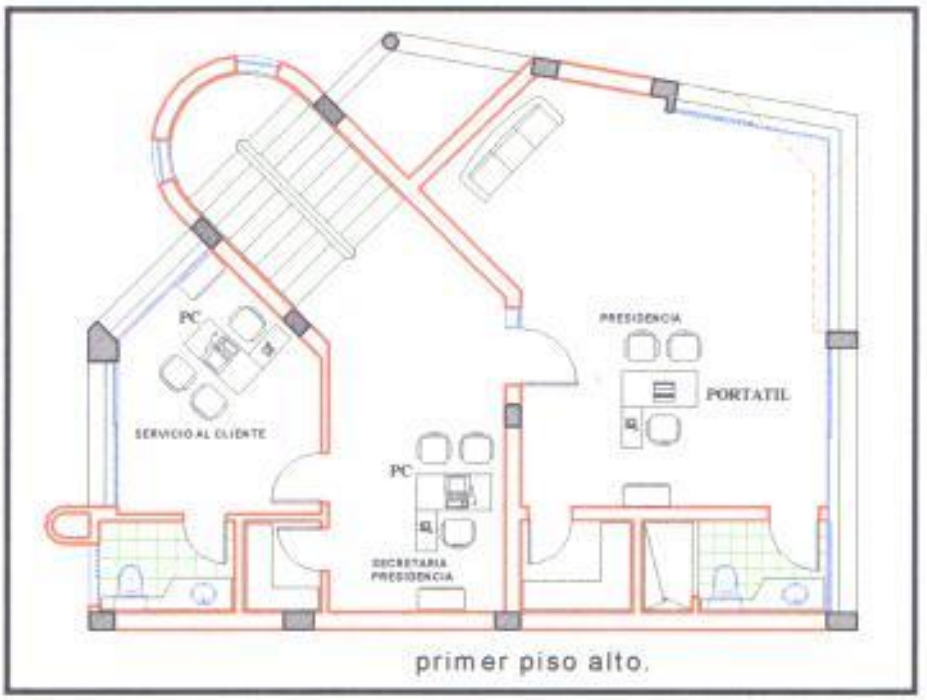


Fig 3.3: Ubicación de las estaciones en el Primer Piso

Gerencia general y gerencia de comercialización tienen 2 PC's portátiles (figura 3.4).

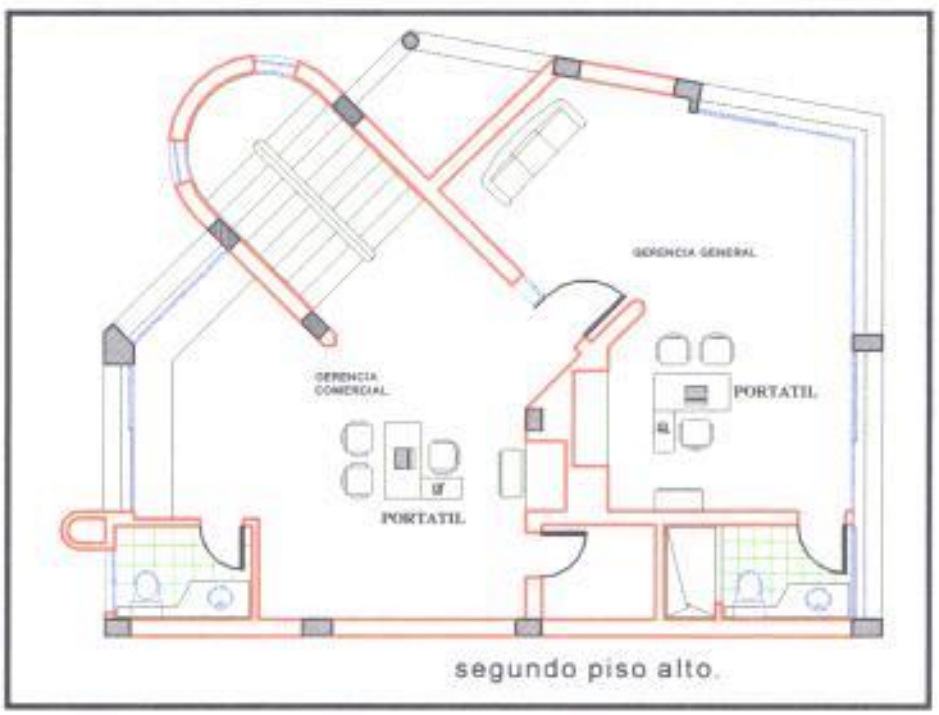


Fig 3.4: Ubicación de las estaciones en el Segundo Piso

Bodega y departamento técnico cuentan con 3 estaciones, de las cuales una es de escritorio y el resto portátiles (departamento técnico), figura 3.5.

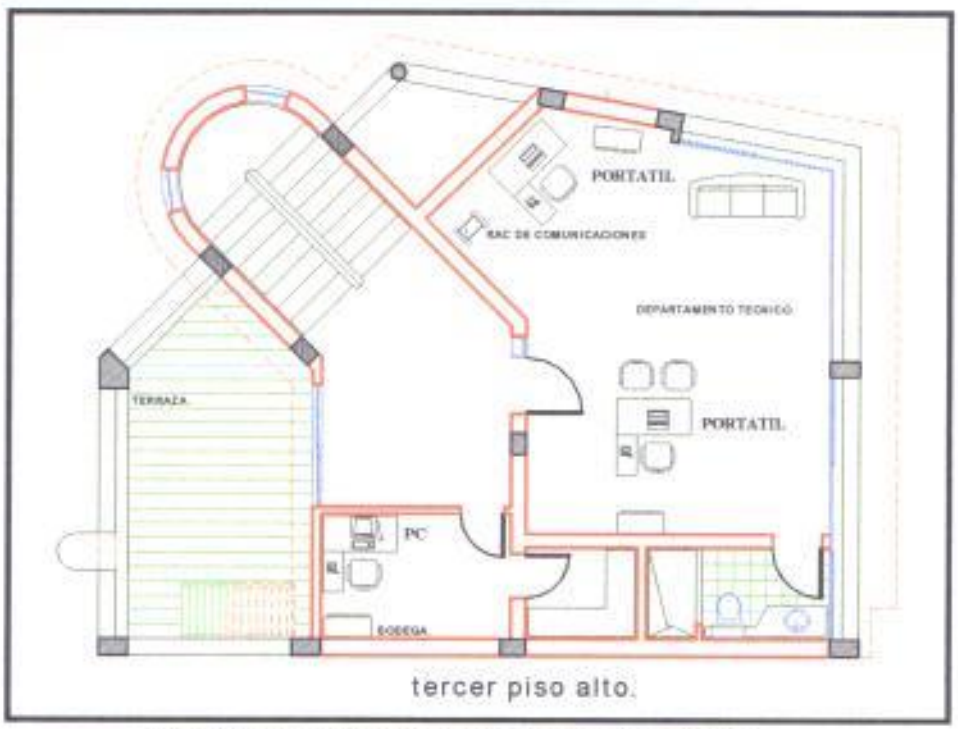


Fig 3.5: Ubicación de las PC´s en el Tercer Piso

La idea es que las 11 PC's existentes en el edificio conformen la red LAN interna de la empresa, conectándose de manera inalámbrica a través de puntos de acceso ubicados estratégicamente.

CAPITULO 4

DESCRIPCIÓN GENERAL DEL EQUIPAMIENTO Y SOFTWARE A UTILIZAR PARA EL DISEÑO Y GESTIÓN DE LA RED.

Para el diseño y gestión de la red se utilizarán equipos marca Lucent Technologies con su línea inalámbrica Orinoco, el cual trae su propio software de gestión que cuenta con algunas herramientas que ayudarán para el diseño de la red.

4.1 Equipamiento Lucent Technologies. Línea Orinoco.

Los productos de la familia Orinoco, son un sistema de equipos de red que permiten la construcción de cualquier tipo de configuración de red, desde una pequeña red inalámbrica hasta una completa y gran infraestructura inalámbrica.

Los productos de la familia Orinoco consisten de:

- Tarjetas de red inalámbricas.
- Adaptadores USB.
- Puntos de Acceso (AP).
- Antenas extensoras de rango.

4.1.1 Tarjetas de Red Inalámbricas ORINOCO.

Son tarjetas utilizadas para computadoras móviles, que permiten la conexión inalámbrica con otra estación o con un punto de acceso AP.

4.1.1.1 Características de la Tarjeta de Red Inalámbrica.

La tarjeta PC (figura 4.1), es una tarjeta de red inalámbrica que es compatible con cualquier slot estándar tipo II (PCMCIA).

Fig 4.1: Tarjeta PC Orinoco

La tarjeta PC cuenta con dos leds indicadores y con dos antenas integradas (figura 4.2). Opcionalmente se puede usar la tarjeta PC en combinación con una antena externa, que es el caso de este diseño.

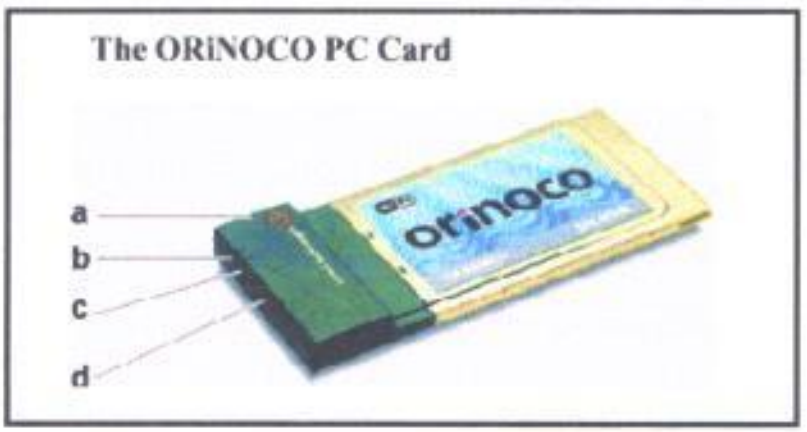


Fig 4.2: Descripción de la tarjeta de red inalámbrica.

A continuación se describe la figura mostrada:

a. Antenas integradas.

b. LED Transmisión / Recepción.

- Apagado; sin actividad inalámbrica.
- Parpadeando; Sensando/Transmitiendo datos inalámbricos.

c. LED de Poder Encendido/Apagado

- Verde; Modo de Operación Estándar.
- Verde parpadeando; Modo de administración de poder.

d. Conector para una antena externa opcional.

4.1.1.2 Tipos de Tarjetas de Red Inalámbrica.

La tarjeta PC Orinoco, es una tarjeta de red inalámbrica que cumple con el estándar de redes inalámbricas LAN IEEE 802.11. Esta tarjeta soporta velocidades de hasta 11 Mbps y está disponible en dos variantes:

1) Orinoco Silver.
2) Orinoco Gold.

Ambos tipos de tarjetas PC son:

- Wi-Fi (Fidelidad inalámbrica), certificado por la Alianza de compatibilidad del ethernet inalámbrico (WECA). Esto significa que el hardware Orinoco se comunicará también con otros vendedores de productos LAN inalámbricos IEEE 802.11.

- Totalmente compatible con cualquier sistema inalámbrico basado en la tecnología de radio de Espectro ensanchado por secuencia directa (DSSS), que cumpla con el estándar IEEE 802.11 de redes LANs inalámbricas.
- También compatible con cualquier otro modelo previamente lanzado por los productos de la familia WAVELAN/IEEE.

1) Tarjeta PC Silver.

La tarjeta PC Silver Orinoco soporta las siguientes características inalámbricas LAN.

- Tasas de transmisión seleccionables en el rango de 1, 2, 5.5 y 11Mbps.
- 11 canales de frecuencia seleccionables (Banda 2.4 GHz).
- **Roaming** sobre múltiples canales.
- Administración del poder de la tarjeta.
- Encriptación de los datos (WEP, Wired Equivalent Privacy), basado en 64 bits del algoritmo de encriptación RC4, como se define en el estándar IEEE 802.11 de redes inalámbricas LANs.

Nota: Este tipo de tarjetas son las usadas para este proyecto.

2) **Tarjeta PC Gold.**

Las tarjetas PC Golds soportan las mismas funcionalidades que la tarjeta Silver. La tarjeta Gold, sin embargo provee una reforzada encriptación de los datos (WEP) basado en 128 bits de acuerdo al algoritmo RC4.

4.1.2 Adaptadores USB Orinoco.

Es utilizado para brindar conexión inalámbrica a computadoras de escritorio que tengan puertos USB (Universal Serial Bus).

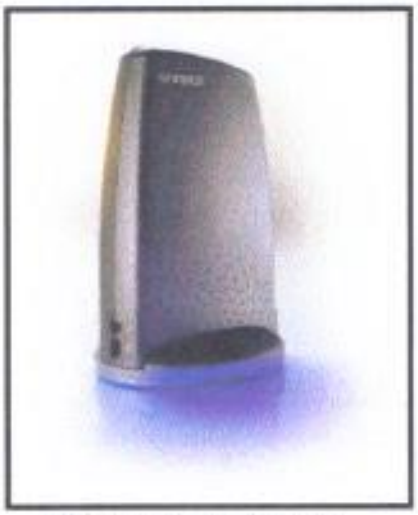


Fig 4.3: Adaptador USB

4.1.2.1 Características del Adaptador USB.

El adaptador USB es un dispositivo de red inalámbrico, que está conectado a través de un cable USB a cualquier conector estándar USB del computador.

A continuación se detallan las partes de este adaptador, (figura 4.4):

a. LED de poder de encendido/apagado

b. LED de Radio.

- Apagado, sin actividad inalámbrica.
- Parpadeando, sensando / transmitiendo datos inalámbricos.
- Verde, modo de Operación estándar.

c. Conector USB.

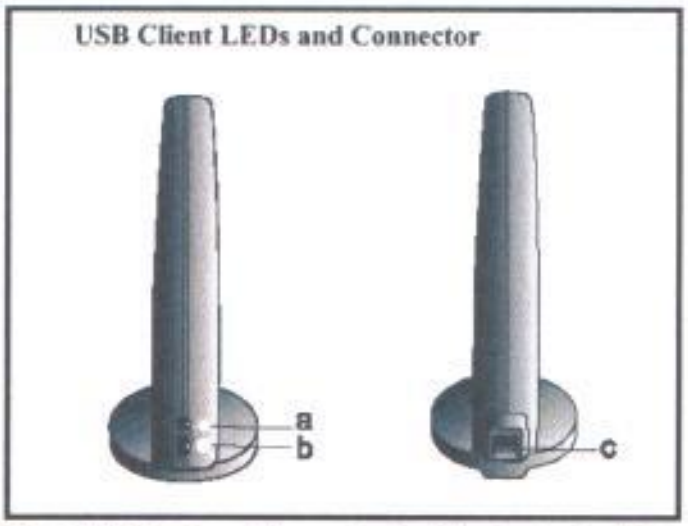


Fig 4.4: Vista Frontal y posterior del adaptador USB

El adaptador. USB es:

- Wi-Fi (Fidelidad inalámbrica), certificado por la Alianza de compatibilidad del ethernet inalámbrico (WECA). Esto significa que el hardware Orinoco se comunicará también con otros vendedores de productos LAN inalámbricos IEEE 802.11.

- Totalmente compatible con cualquier sistema inalámbrico basado en la tecnología de radio de Espectro ensanchado por secuencia directa (DSSS), que cumpla con el estándar IEEE 802.11 de redes LANs inalámbricas.
- Compatible con el bus serial universal.

El adaptador USB soporta las siguientes características de redes inalámbricas:

- Tasas de transmisión seleccionables en el rango de 1, 2, 5.5 y 11 Mbps.
- 11 Canales de frecuencia seleccionables (Banda 2.4 GHz).
- Administración de poder.

Nota: Es importante recalcar que un adaptador USB equivaldría a una tarjeta PC inalámbrica, la diferencia está en la interface de conexión al computador, ya que la tarjeta PC se la coloca insertándola directamente en el slot PCMCIA, mientras que el adaptador USB se lo conecta a través del puerto USB del computador.

4.1.3 Puntos de Acceso (Acces Point) ORINOCO.

Permiten conectar inalámbricamente estaciones con la infraestructura LAN ethernet existente.

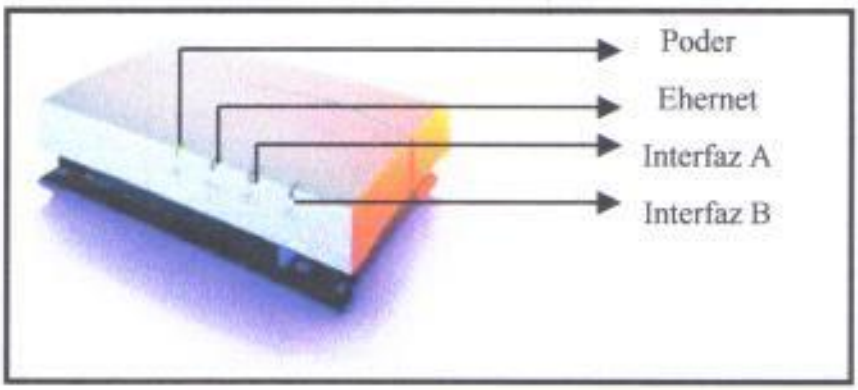


Fig 4.5: Punto de Acceso (AP), Modelo AP-1000

Los puntos de acceso que se utilizarán en el diseño de la red son el modelo AP-1000 (figura 4.5), que es un dispositivo que trabaja como un puente transparente equipado con dos slots para tarjetas PC. Las interfaces de red inalámbricas A y B son correspondientes a los slots A y B del AP-1000, en los cuales las tarjetas PC pueden ser insertadas.

A continuación se muestra una tabla con la actividad de los leds en el equipo.

LED	Definición	Actividad	Descripción
	Poder	Verde	Poder habilitado
	Ethernet	Verde parpadeando	Actividad Ethernet Lan
	Interface inalámbrica A	Verde parpadeando	Actividad inalámbrica Lan
	Interface inalámbrica B	Verde parpadeando	Actividad inalámbrica Lan

Tabla II: Actividad de los leds en el AP

La actividad de los leds, solo ocurrirá cuando hay actividad en la red en la correspondiente interface del punto de acceso. Cuando no hay actividad, el led está apagado.

La interface de red Orinoco no es muy diferente que la interfaz de red LAN común, incluso el sistema operativo no notará la diferencia.

La interfaz de red Orinoco es compatible con todos los protocolos que son soportados por los estándares de adaptadores de tarjetas ethernet. Igual que las interfaces de red LAN cableadas, la interface de red Orinoco es instalada con un controlador Orinoco dedicado, pero a diferencia de la interface de

red cableada, las interfaces Orinoco no necesitan de un cable para conectarse a la red. Con las tarjetas de red Orinoco se podrá agregar sitios de trabajo sin necesidad de cablear o hacer algún cambio en las conexiones al switch.

4.1.4 Antena Extensora de Rango para las Tarjetas de Red Inalámbricas.

La antena extensora de rango es una antena interior que habilita o provee un aumento del rendimiento de la red que se va a diseñar y gestionar. Esta antena se la puede usar en combinación con las tarjetas PC, cuando la misma está instalada dentro de un punto de acceso.

Fig 4.6: Antena extensora de rango

Esta antena es usada cuando las antenas integradas de la tarjeta PC están ocultas o por ejemplo:

- Cuando el dispositivo Orinoco (AP) está dentro de un lugar, como un closet o gabinete, o montado por dentro de un escritorio.
- Cuando la señal de radio de la tarjeta Orinoco es obstruida por objetos como repisas gruesas de libros, armarios de archivos u otro equipo de oficina.

4.2 Herramientas de Gestión (Software Orinoco).

El software Orinoco consiste de un sistema de herramientas de gestión que permiten:

- Mostrar y modificar la configuración (remota) de los componentes de la red.
- Configurar los componentes de red, tal como los puntos de acceso.
- Diagnosticar el funcionamiento de la red y, si es necesario, identificar y resolver errores en la misma.
- Administrar y optimizar el funcionamiento de la red.
- Implementar mecanismos de protección que permitan tener una red mucho más confiable y segura.

El software Orinoco consiste de las siguientes herramientas:

- Administrador del cliente Orinoco (Client Manager).
- Administrador OR Orinoco (OR Manager).
- Administrador PRO Orinoco.

- Administrador AP Orinoco.

Estas herramientas pueden ser instaladas en estaciones que corran Microsoft Windows 95, 98, NT 4.0, o 2000.

Nota: En este proyecto se utilizarán como herramientas de gestión el Administrador del Cliente y el Administrador OR.

4.2.1 Administrador del Cliente Orinoco.

El administrador del cliente Orinoco es una herramienta de diagnóstico que monitorea la comunicación de radio entre una estación inalámbrica y un punto de acceso Orinoco, o monitorea el enlace entre dos estaciones inalámbricas en una red independiente (este programa es instalado en las estaciones de trabajo).

Además, este software cuenta con una herramienta muy importante llamada **Site Monitor,** que sirve para demostrar la cobertura del punto de acceso Orinoco instalado en cierta área (esta herramienta es la que se utiliza para diseñar la red).

4.2.2 Administrador OR Orinoco.

El Administrador OR Orinoco es una herramienta para los administradores de LAN o los Supervisores de Sistemas, en este proyecto esta sería la herramienta principal que se utilizará para realizar la gestión de la red (este programa es instalado en la estación de gestión). El Administrador OR es un programa que sirve para:

- Configurar **ruteadores** y **puntos de acceso** Orinoco.
- Mostrar y modificar la configuración de los puntos de acceso y/o ruteadores.
- Diagnosticar el comportamiento de la red, y si es necesario identificar y resolver errores en la misma.
- Administrar y Optimizar el desempeño de la red.

4.2.3 Administrador PRO Orinoco

El Administrador Pro Orinoco es una herramienta especialmente diseñada por sistemas HP Open View. Esta herramienta permite configurar puntos de acceso Orinoco, monitorear el desempeño de la red inalámbrica, y analizar el enlace entre dos estaciones inalámbricas. Este programa deberá ser instalado en la estación de gestión.

4.2.4 Administrador AP Orinoco

El Orinoco Administrador del AP es una herramienta para los administradores de LAN o los Supervisores de Sistemas. El programa administrador del AP se usa exclusivamente para configurar puntos de acceso Orinoco y para monitorear el funcionamiento de la red inalámbrica. Este programa puede ser instalado en la estación de gestión o en cualquier estación de trabajo.

CAPITULO 5

DISEÑO DE LA RED LAN INALÁMBRICA A GESTIONAR.

En este capítulo se explica el diseño de toda la red WLAN, considerando la tecnología usada, la infraestructura que se montaría, se trata también el tipo de configuración que se aplicará a la red, se detalla además el procedimiento para escoger cual de las la PC´s de la red se usará para la gestión de la misma, el esquema de direccionamiento IP utilizado y los costos que representarían implementar este diseño.

5.1 Tecnología a utilizar.

La red inalámbrica a **diseñar y gestionar** utiliza tecnología de espectro ensanchado, específicamente por secuencia directa, tecnología ya explicada en el capítulo 1; la frecuencia de trabajo será la banda de 2.4 GHz, tal como lo define el estándar IEEE 802.11b, que permite velocidades de hasta 11 Mbps.

5.2 Infraestructura de la Red.

Para empezar este diseño se necesita primero elegir el lugar de ubicación del o de los puntos de acceso de ser necesario, es decir hay que realizar una inspección general del edificio y ayudarse del software **Administrador del**

Cliente (herramienta ya descrita en el capítulo 4), para deducir la ubicación y cuántos puntos de acceso se requerirá para establecer la WLAN.

Según la inspección hecha a las instalaciones de SATLINK, se pudo determinar que se necesitan dos puntos de acceso (con sus respectivas tarjetas de red) para cubrir óptimamente todo el edificio (se llegó a esta conclusión utilizando la herramienta **Site Monitor,** explicada detalladamente en el capítulo 7 en la sección Administrador del Cliente.). Un punto de acceso será ubicado en el primer piso y el otro en el tercero, así como se describe en las figuras 5.1 y 5.2.

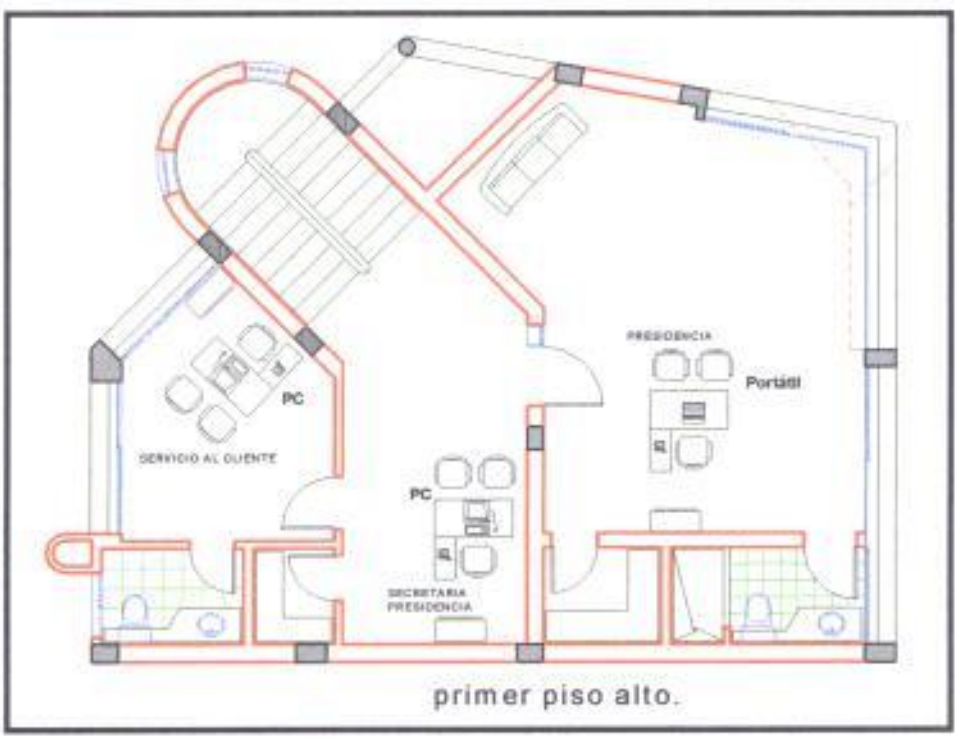


Fig 5.1: Punto Acceso ubicado en el Primer Piso

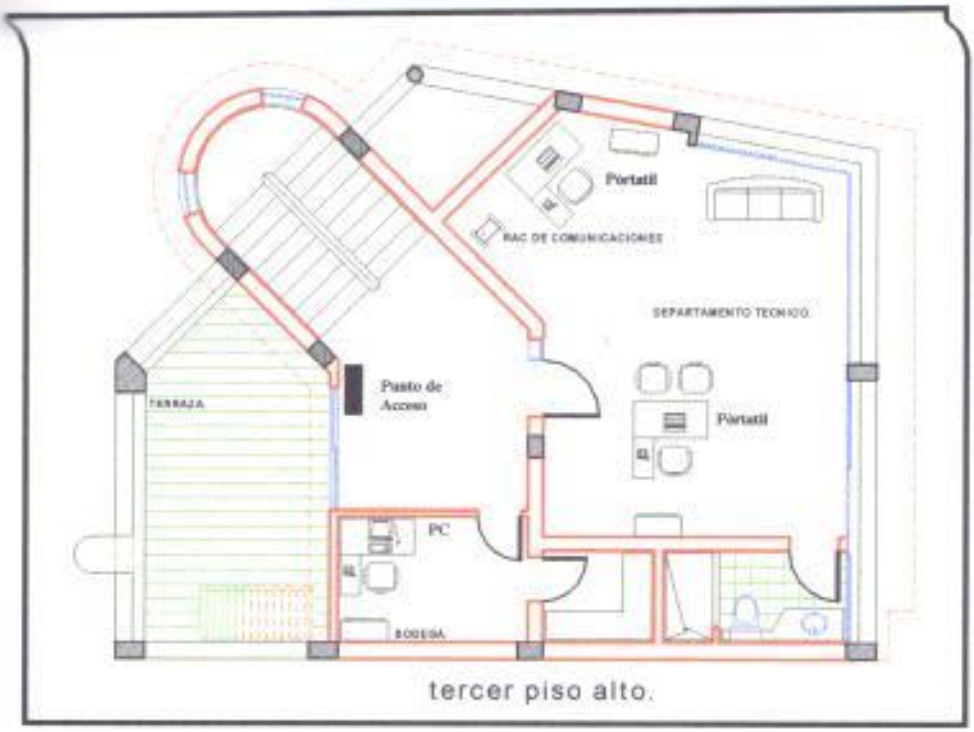


Fig 5.2: Punto de Acceso ubicado en el tercer piso

Cada tarjeta de red correspondiente a cada AP, utilizará una antena extensora de rango de 7.5 dbi de ganancia, lo que dará la seguridad de que todas las áreas del edificio sean cubiertas eficientemente.

La red interna de Satlink cuenta con 11 PC´s, de las cuales 6 son fijas y 5 son portátiles; con estas computadoras se formará la red inalámbrica. Todos los PC´s de esta red trabajan bajo el sistema operativo Windows 98, por lo tanto todos los controladores y software de los equipos que se instalarán correrán bajo este sistema operativo.

Las portátiles serán equipadas con las tarjetas de red inalámbrica (PCMCIA), mientras que las PC´s de escritorio utilizarán los adaptadores USB para poder comunicarse con los puntos de acceso; para esto todas las portátiles cuentan con el respectivo slot PCMCIA al igual que las PC´s de escritorio con su puerto USB. Todas las tarjetas de red utilizadas son del tipo **Silver**.

En la figura 5.3 se presenta como sería el diseño de la red LAN interna de SATLINK.

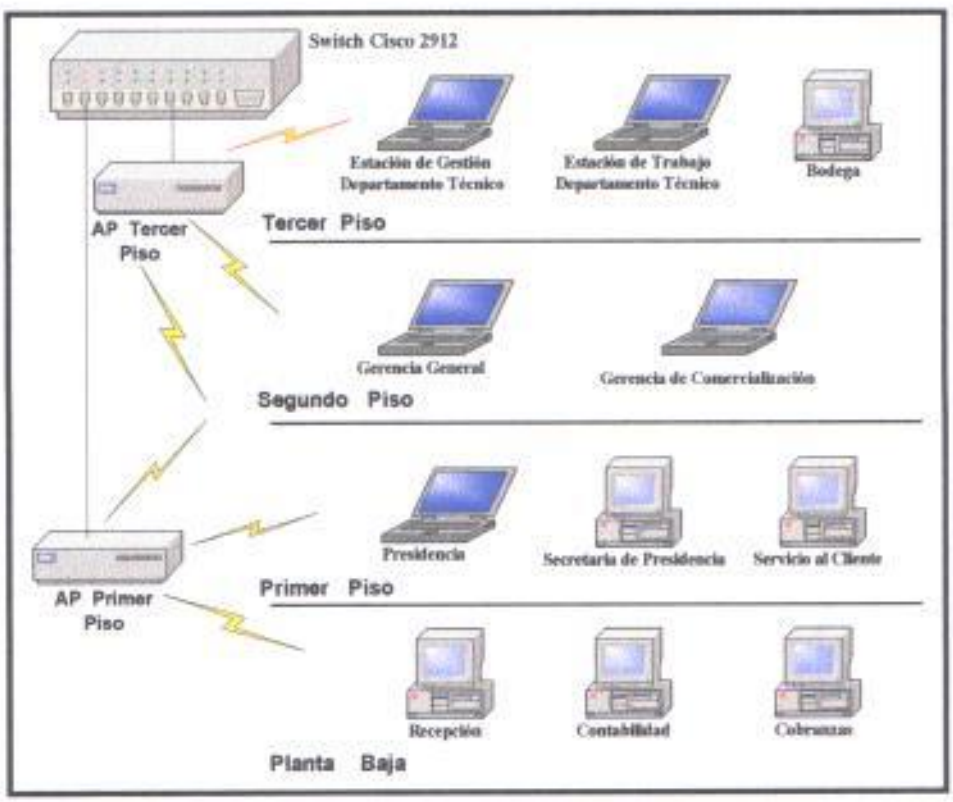


Fig 5.3: Red WLAN SATLINK S.A.

Como se muestra en el gráfico los puntos de acceso a su vez están conectados a la red cableada a través del Switch Cisco 2912, de esta manera las estaciones inalámbricas podrán interactuar con la red fija (compartir recursos, internet, etc..).

Según el esquema mostrado, los usuarios ubicados en planta baja y primer piso se conectaran con el **AP Primer Piso**, mientras que el resto de usuarios ingresarán a la red a través del **AP Tecer Piso**.

En la figura 5.4 se presenta un gráfico que muestra las celdas de cobertura de los AP's. Los usuarios que se muevan de una celda a otra conmutarán automáticamente de frecuencia (roaming) sin perder la conexión de red

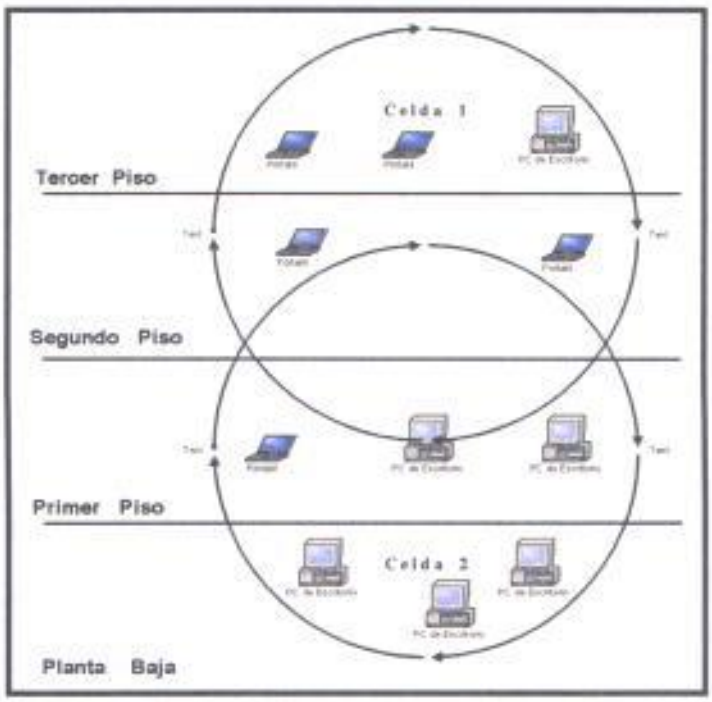


Fig 5.4: Celdas de cobertura de los AP's

Como la red consiste de 2 AP's, se recomienda que se alterne canales de frecuencias, para así proveer más ancho de banda a las estaciones en cada celda. Por lo tanto un AP trabajará en el canal 1 (2.412 Ghz), y el otro en el canal 11 (2.462 Ghz). Esta forma de utilizar la máxima separación de canales en los AP's permite una óptima operación de la red.

5.3 Configuración Inalámbrica.

La configuración usada es la llamada extensión por celdas básicas (ya explicada en el capítulo 1), por lo tanto al switch van conectados vía cable de red los 2 puntos de acceso según el análisis hecho; de esta manera se dará servicio a las 11 PC's de toda la red.

Todas las estaciones inalámbricas que deseen estar en red deben configurarse con el mismo nombre de red (network name, parámetro explicado en el capítulo 7 en la sección gestión de configuración) que los puntos de acceso.

5.4 Selección de la Estación de Gestión.

La estación de gestión LAN es una computadora usada por el administrador de la red para configurar, manejar y monitorear la misma. El servidor de gestión utiliza las herramientas disponibles en el software de Orinoco (OR Manager y/o Client Manager).

5.4.1 Mínimos Requerimientos del Servidor de Gestión.

Para configurar la estación de gestión se puede usar una portátil o una PC de escritorio que tenga los siguientes requerimientos:

- Procesador 80486 o superior.
- Espacio libre en disco de 4 MB.
- 8MB de RAM (16 MB o más, recomendado).
- Microsoft Windows 95, 98, 2000 o NT (v 4.0)

Para utilizar el **Administrador del Cliente** en la estación de gestión se necesitará también:

- Tarjeta PC Orinoco
- Adaptadores USB.
- Protocolo de comunicación TCP/IP.

Para usar el **Administrador OR** en la estación de gestión se necesitará lo siguiente:

- Acceso a la LAN vía tarjeta Ethernet (para configurar los AP's inicialmente).
- Puntos de Acceso Orinoco.
- Protocolo de comunicación TCP / IP.

5.4.2 Administración de la Infraestructura de Red.

La estación de gestión que se elija tendrá instalado el Administrador OR y/o el Administrador del cliente, esta estación permitirá configurar los puntos de acceso y monitorear el tráfico de radio entre los puntos de acceso seleccionados y las estaciones dentro de la red.

En todas las estaciones restantes se instalará el Administrador del cliente, y así monitorear el enlace entre las mismas y los puntos de acceso.

5.4.3 Servidor de Gestión Inalámbrico o Cableado.

La estación de gestión será cableada o inalámbrica dependiendo de las preferencias y habilidades que se tenga para administrar la red.

Por lo tanto se determinará primeramente como se desea administrar la red.

Se podria monitorear y configurar la red desde:

- **En el mismo sitio**, para localizar problemas en la ubicación fisica de la estación, se puede escoger una portátil (estación móvil) como estación de gestión.

  Herramienta: Administrador OR y Administrador del cliente.

- **En una ubicación central**, se puede también escoger como servidor de gestión una estación fija cableada, esto es recomendable para una red grande.

Herramienta: Administrador OR.

- **En una ubicación remota**, se puede tener acceso vía MODEM, llamando a un RAS (Remote Access Server) conectado a la red.

  Herramienta: Administrador OR

En este proyecto se tomará como opción de monitoreo y configuración el primer caso (**en el mismo sitio**), ya que se trata de una red no muy grande; por lo tanto se utilizará como estación de gestión una computadora portátil que cumple con los requerimientos mencionados anteriormente (la estación elegida pertenece al departamento técnico), y que permitirá usar el Administrador del Cliente así como también el Administrador OR.

5.5 Esquema de direccionamiento IP para la red LAN.

En esta parte se mencionan las direcciones de red que se manejarán para la WLAN, así como también las direcciones que ya están establecidas en la red de SATLINK. Esta red utiliza para su funcionamiento los siguientes rangos de direcciones:

216.219.10.64 con máscara **255.255.255.192**.- que es una subred pública usada para el equipamiento en sí del ISP (ruteador, servidor de acceso, servidor cache, firewall, etc...), y para clientes que lo requieran.

10.1.0.0 con máscara **255.255.255.128** - para la red DMZ (intranet) protegida por el firewall, como los servidores DNS/MAIL/WEB/AAA.

10.1.0.128 con máscara **255.255.255.128**, para la red WLAN protegida también por el firewall.

Por lo tanto según este esquema de direccionamiento los puntos de acceso tendrían las siguientes direcciones.

Equipos	**Dirección IP**	**Máscara de red**
Punto de acceso 1	10.1.0.130	255.255.255.128
Punto de acceso 2	10.1.0.131	255.255.255.128
Estación de Gestión	10.1.0.132	255.255.255.128

Las demás estaciones inalámbricas entonces ocuparían desde la dirección 10.1.0.133 en adelante (la dirección de red 10.1.0.129 no es considerada ya que es la que ocupa el firewall).

5.6 Costos de la implementación del diseño.

A continuación se muestran unas tablas que hacen referencia al costo que implicaría implementar la WLAN en la empresa SATLINK.

Cantidad	Nombre del Equipo	Precio unitario	Total
2	AP-1000 (incluye software de Gestión)	$687,75	$1.375,50
7	Tarjetas PC Silver	$122,81	$859,67
6	Adaptadores USB	$132,70	$796,20
2	Pigtail	$50,00	$100,00
2	Antenas Extensoras de Rango 7,5 dbi	$80,00	$160,00
		Subtotal 1	$3.291,37

Tabla III: Costo del equipamiento

Cantidad	Descripción	Precio unitario	Total
45	Cable UTP categoría 5 (metros)	$0,45	$20,25
10	Canaletas (metros)	$1,10	$11,00
10	Conectores RJ-45	$0,50	$5,00
1	Configuración y Puesta en Marcha de la WLAN		$500,00
		Subtotal 2	$536,25

Tabla IV: Costos de la instalación de la WLAN

Por lo tanto el costo total por la implementación de la red sería de $3827,62.

Nota: Estos costos fueron obtenidos de la empresa **SUMISYS TELECOM,** distribuidor autorizado de equipos **Orinoco** en Guayaquil.

CAPITULO 6

ESQUEMA DE INSTALACIÓN DE SOFTWARE Y EQUIPOS NECESARIOS PARA LA GESTIÓN DE LA RED.

En este capítulo, se describe como sería la instalación de las herramientas y equipos necesarios para el diseño y gestión de la red.

En lo que respecta a hardware, se describe como se instalan las tarjetas PC, los adaptadores USB, los puntos de acceso y la antena extensora de rango; y en lo que es software se explica la instalación del **Administrador OR** y del **Administrador del Cliente.**

6.1 Instalación de la Infraestructura (Hardware) de Red.

Para conectar una estación inalámbrica a la red, cada estación debe ser configurada con el mismo **network name** (nombre de red) que el punto de acceso.

Para configurar las estaciones inalámbricas se tiene que tomar en cuenta lo siguiente:

Se tienen portátiles y estaciones fijas en la red, en consecuencia las portátiles usarán las Tarjetas PC y las fijas utilizarán los adaptadores USB como ya se había mencionado, por lo tanto para su instalación se utilizará controladores diferentes, pero el procedimiento de configuración es similar.

6.1.1 Instalación de las Tarjetas de Red Inalámbricas.

Para instalar las Tarjetas PC en las portátiles se procede de la siguiente manera:

- Insertar la tarjeta PC en el slot de la portátil como muestra la figura 6.1.

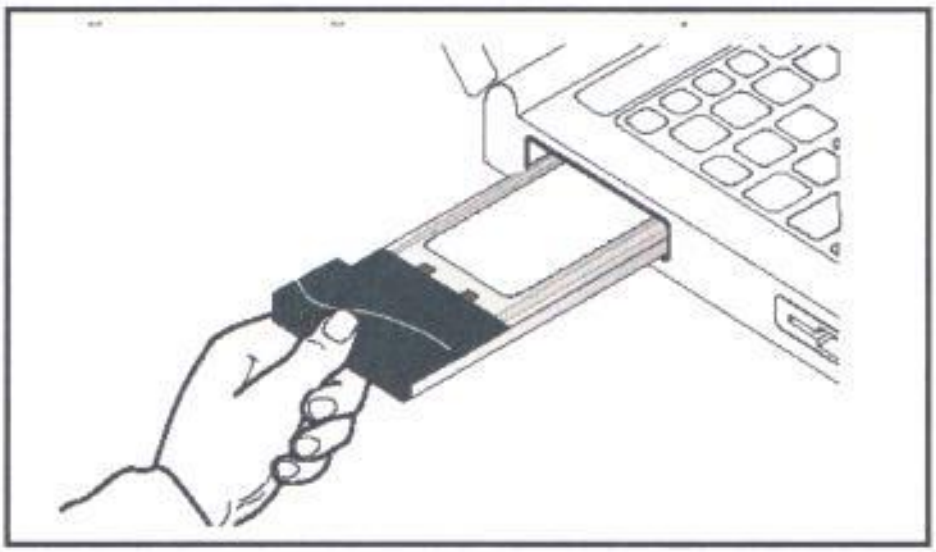


Fig 6.1: Instalando la tarjeta PC en las portátiles

- Cuando Windows detecte el nuevo hardware haga clic en **Siguiente**, el sistema operativo Windows 98 soporta " Plug & Play" para las tarjetas PC, por tanto la tarjeta será reconocida automáticamente y habilitará el controlador Orinoco.

- Introduzca el CD de instalación en la unidad de CD-ROM. Cuando Windows le pida la ubicación del controlador, elija **Buscar el mejor controlador para su dispositivo (se recomienda)** y haga clic en **Siguiente.**
- Elija especificar una ubicación y escoja la ruta donde se encuentra el controlador apropiado (D:\Drivers\Tarjeta PC\Win_98).
- Siga las instrucciones en pantalla. Después de hacer clic en **Finalizar,** tendrá que reiniciar su computadora portátil para completar el proceso de instalación.
- Luego, Windows automáticamente abrirá la ventana de perfil **Add/Edit Configuration Profile**, descrito en el capítulo 7 página 106, correspondiente a la **Gestión de Configuración de las estaciones de trabajo.**

6.1.2 Instalación de los Adaptadores USB.

El procedimiento es exactamente el mismo que el anterior luego que este adaptador ha sido conectado al puerto USB del computador, lo único que cambia es el controlador escogido, es decir ahora se tiene que elegir la ruta D:\Drivers\USB Adapter\Win_98.

6.1.3 Instalación de los Puntos de Acceso (AP´s).

Para instalar los puntos de acceso se deben seguir los siguientes pasos:

1. Verificar los componentes.
2. Colocar la placa de montaje y la fuente de alimentación.
3. Montar el módulo de procesamiento.
4. Conectar las interfaces de red.
5. Prender el equipo.

1. Verificando los componentes

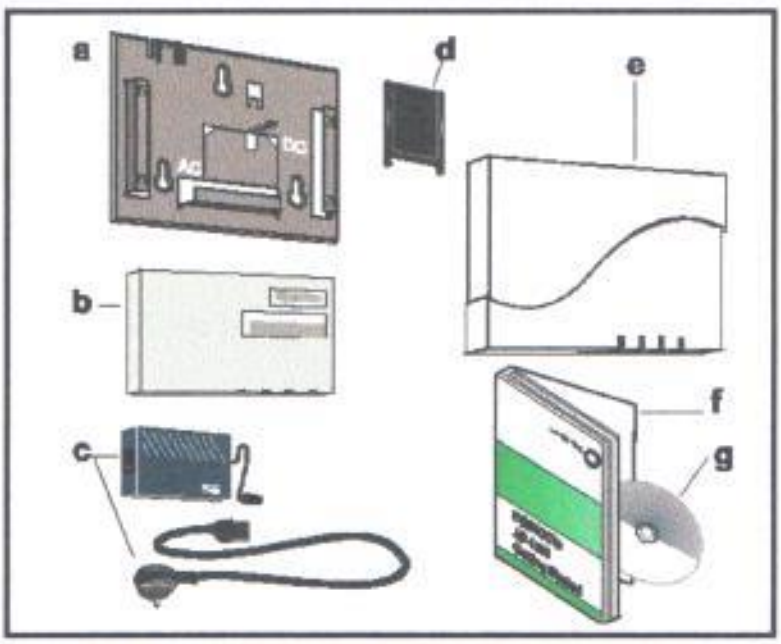


Fig 6.2: Componentes del Punto de acceso

a) Placa de montaje para montar el punto de acceso en una pared.
b) Punto de acceso Orinoco, módulo de Procesamiento.
c) Fuente y cable de poder AC.
d) Protector del slot de la tarjeta.

e) Tapa del punto de acceso.

f) Guía del usuario

g) CD-ROM Orinoco, que contiene el software y controladores **Orinoco**.

2. Colocando la placa de montaje y la fuente de poder.

El punto de acceso se puede ubicar en una superficie vertical como una pared, o en una superficie llana ya sea una mesa o escritorio.

En este caso, los equipos serán ubicados sobre una pared; como ya se mencionó antes según la inspección hecha al edificio de SATLINK.

- Se coloca la placa de montaje del punto de acceso como muestra la figura 6.3, use los tornillos proporcionados.

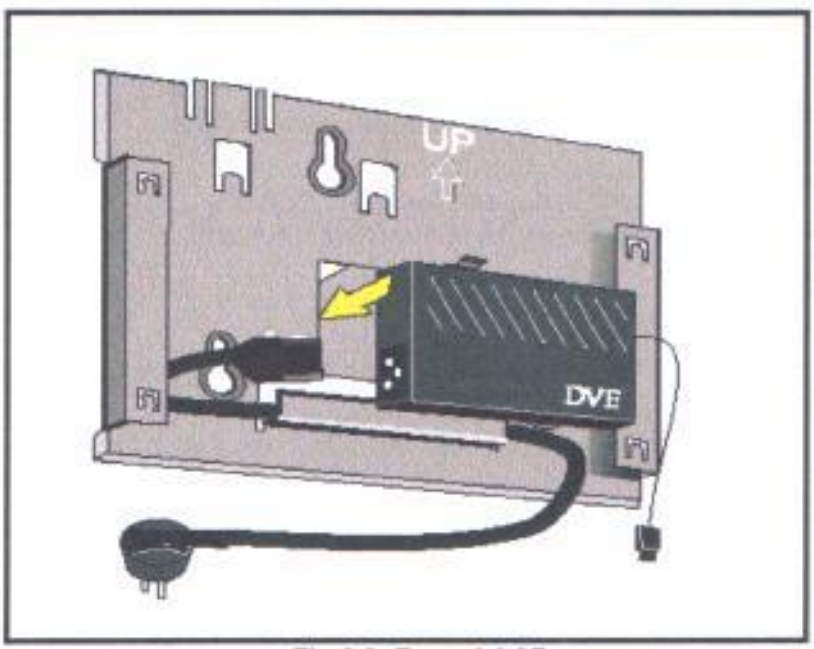


Fig 6.3: Base del AP

- Se conecta el cable de poder a la fuente.
- Hay que asegurarse de que el cable quede dentro de la unidad.

3. Montando el módulo de procesamiento.

- Se conecta el cable de poder DC a la entrada DC del módulo de procesamiento.
- Se coloca el equipo dentro de la base cuidadosamente, asegurándose que quede firme.

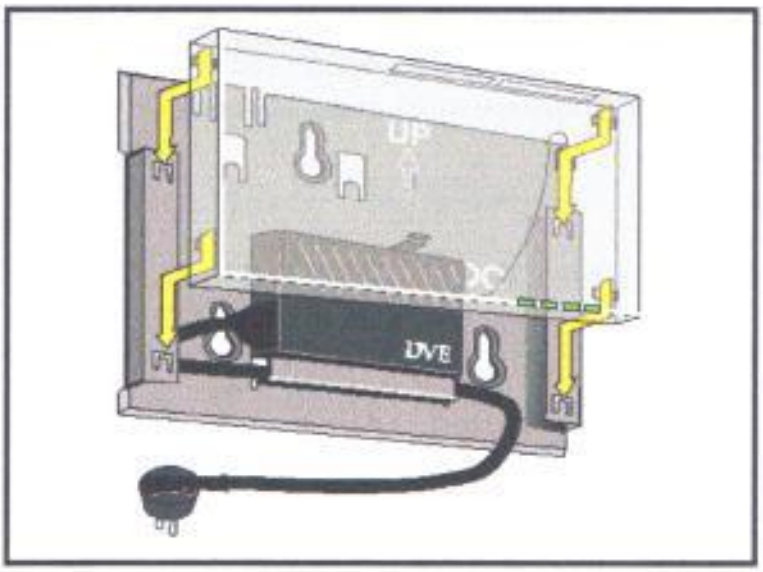


Fig 6.4: Colocando el AP en la base.

4. Conectando las interfaces de red.

Para conectar la tarjeta de red en el AP se procede de la siguiente manera:

- Se inserta la tarjeta PC dentro del módulo de procesamiento. Un slot del equipo esta provisto con un plástico protector, que tiene como propósito proteger al equipo del polvo cuando esta siendo usado con una sola tarjeta PC.

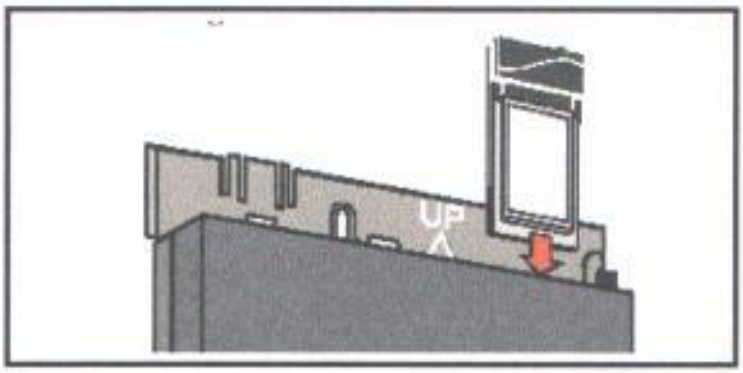


Fig 6.5: Insertando la tarjeta PC en el punto de acceso.

- Se conecta el cable Ethernet (que viene del switch) en la interface que corresponde.
- Se coloca la tapa.

5. Conectando y encendiendo el equipo.

Se conecta el punto de acceso a una toma de corriente, para esto hay que tomar en consideración lo siguiente:

- La toma a la que se conecta el equipo debe estar aterrizada.
- La toma debe estar ubicada de tal manera que el punto de acceso pueda ser desconectado fácilmente.

Cuando el AP ha sido conectado, los leds cambiarán de color en una secuencia ámbar, rojo y verde. Cuando ésto finalice (después de 60 segundos), los leds permanecerán parpadeando según la actividad que realice el equipo.

6.1.4 Instalación de la Antenas Extensoras de Rango.

Para instalar las antenas extensoras de rango se procede de la siguiente manera:

a) Identificar la ubicación óptima de la montura de la antena.

- Permitir que el cable se doble naturalmente, no forzarlo. Se recomienda que se coloque la antena a no más de un metro de la tarjeta PC, para evitar tensión excesiva entre el cable y el conector.

b) Quitar la capa protectora del conector de la antena externa en la tarjeta PC.

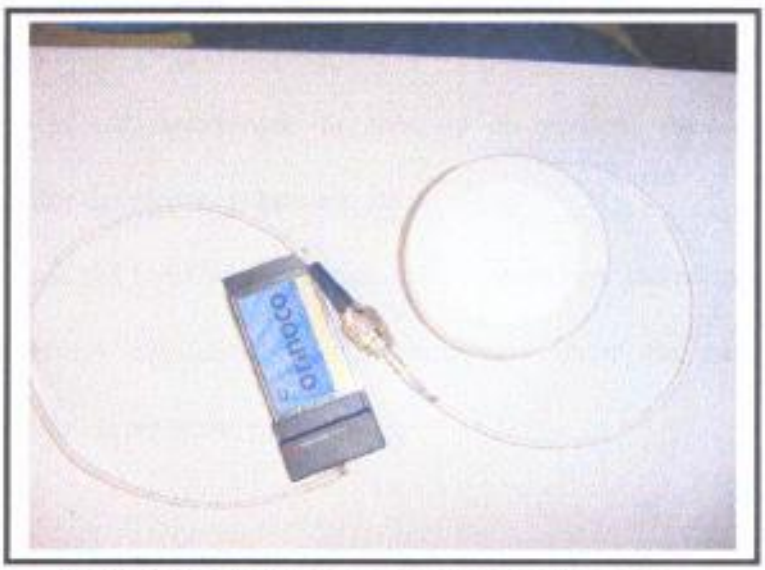


Fig 6.6: Instalando la antena extensora de rango

c) Se inserta el cable en el conector de la antena externa de la tarjeta PC (figura 6.6), se aprieta suavemente hasta que el conector del cable se ubique dentro del lugar. Verificar que se escuche un clic para que este quede en posición, sino hay que maniobrar suavemente hasta que se ubique.

6.2 Instalación del software Orinoco.

En esta sección, se explica la instalación del Administrador del Cliente para todas las estaciones de trabajo y también del Administrador OR que se instalará solo en el servidor de gestión.

6.2.1 Instalación del Administrador del Cliente.

El Administrador del Cliente es una herramienta de diagnóstico que corre sobre estaciones inalámbricas únicamente. Para poder correr este programa, las estaciones deben estar equipadas con la tarjeta PC o el adaptador USB. Por lo tanto, éste programa debe ser instalado en todas las estaciones de trabajo de la red, incluyendo la estación de gestión. Para instalar el Administrador del cliente se procede como sigue:

- Acceda al CD-ROM que contiene los instaladores del programa e ir a la carpeta OR Client, Client Manager y hacer clic en setup, se mostrará la siguiente pantalla.

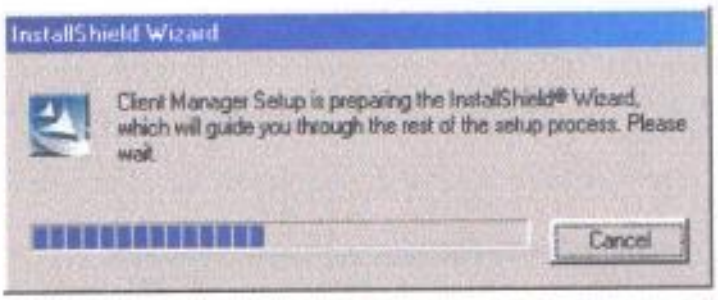


Fig 6.7: Preparando la instalación del Client Manager

- Dar clic en next en la pantalla mostrada.

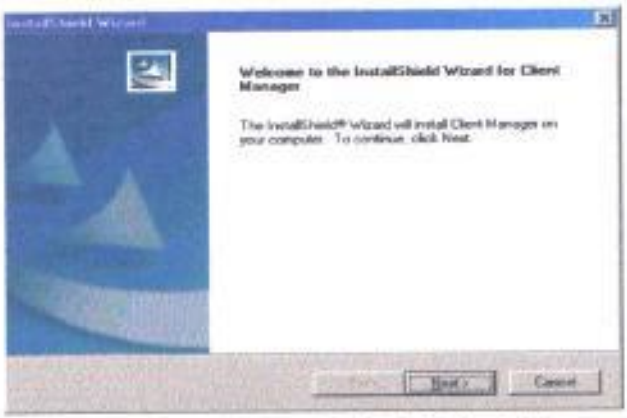


Fig 6.8: Inicio de la instalación del Client Manager

- La siguiente pantalla muestra el directorio donde se instalará el software, si esta de acuerdo hacer en clic en next, o sino en browse y escoger el directorio (figura 6.9).

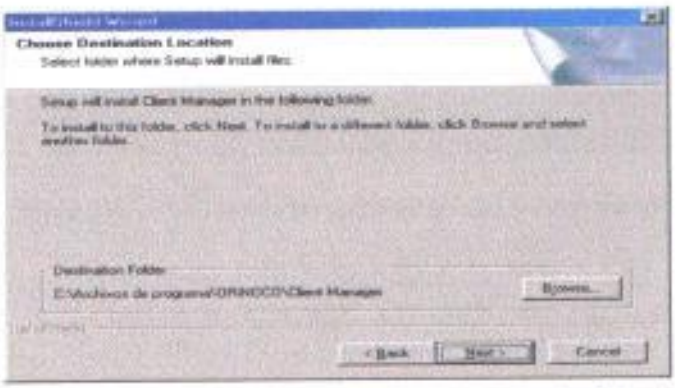


Fig 6.9: Selección del directorio de instalación

- A continuación, el programa se instalará en el directorio especificado (figura 6.10).

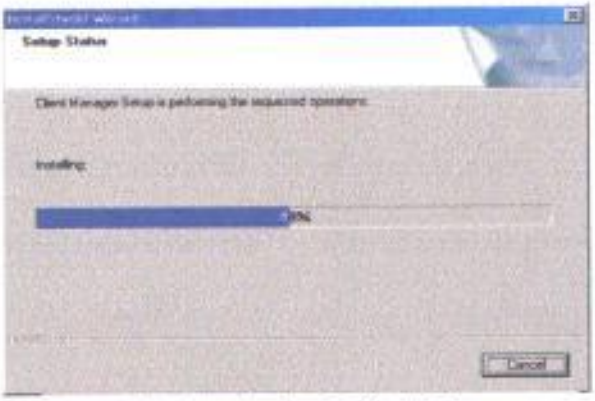


Fig 6.10: Instalando el Client Manager

- Luego de esto, el **Administrador del Cliente** quedará instalado en la estación. Hacer click en Finish, veáse figura 6.11.

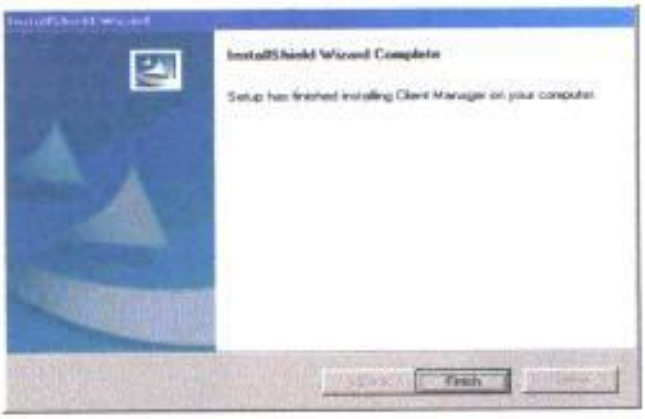


Fig 6.11: Finalizando la instalación del Client Manager

6.2.2 Instalación del Administrador OR.

El Administrador OR estará instalado en una de las dos portátiles que pertenecen al departamento técnico, que es la que se utilizará como la estación de gestión de la WLAN.

Para instalar el programa Administrador OR se procede como sigue:

- Acceda al CD-ROM que contiene los instaladores del programa e ir a la carpeta OR Manager y hacer clic en setup, se mostrará la siguiente pantalla.

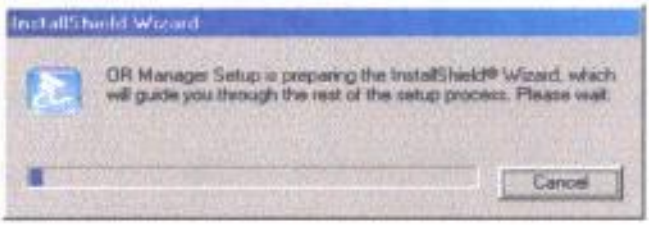


Figura 6.12: Preparando la instalación del OR Manager

- En la pantalla siguiente hacer click en next, figura 6.13.

Fig 6.13: Inicio de la instalación del OR Manager

- La siguiente pantalla muestra el directorio donde se instalará el software, si esta de acuerdo hacer en clic en next sino en browse, y escoger el directorio (figura 6.14).

Fig 6.14: Selección del directorio de instalación

- A continuación, el programa se instalará en el directorio especificado.

Fig 6.15: Instalando el OR Manager

- Luego de esto, el Administrador OR quedará instalado en la estación de gestión. Hacer click en Finish, veáse figura 6.16.

Fig 6.16: Finalizando la instalación del Or Manager

6.2.3 Verificando la Configuración TCP/IP.

El programa de **Administración OR y del Cliente,** requieren el protocolo de red TCP/IP para comunicarse con los puntos de acceso. Antes de que se configuren los puntos de acceso por primera vez, se necesita verificar la configuración TCP/IP de la estación LAN de administración y del resto de estaciones que conforman la WLAN.

Para verificar si el protocolo TCP/IP está correctamente instalado se debe:

1. En la barra de tareas de Windows hacer click en **Inicio**.
2. Entrar a **Configuración** y hacer click en **Panel de control**.
3. En la ventana del panel de control, hacer doble click en el icono de red.
4. Verifique que la lista de componentes de red incluya el protocolo **TCP/IP** para la interface de red que se usará, para acceder a los puntos de acceso (interface ethernet o adaptador inalámbrico).

- Si es **SI,** proceder con la configuración IP de esta estación.
- Si es **NO,** procedemos con lo siguiente.
  - ✓ Hacer click en el botón agregar.
  - ✓ De la lista de tipos de componentes, seleccionar Protocolo y hacer click en Agregar.
  - ✓ Seleccionar protocolo TCP/IP de la lista mostrada con su respectivo sistema operativo.

5. Habilitar la opción especificar una dirección IP. Esto deshabilitaría el mecanismo DHCP de asignamiento automático de IP, en caso que la red lo tuviere.
6. Ingresar en el campo dirección IP la dirección asignada para la estación (desde la 10.1.0.132 en adelante). En el campo de máscara de red ingresar el valor de 255.255.255.128 y en el campo de puerta de enlace ingresar la dirección 10.1.0.129 que corresponde al Firewall, de esta manera la estación tendrá salida a internet.
7. Dar click en Ok para confirmar y siga las instrucciones que se muestran en la pantalla.
8. Cuando se pregunte por reiniciar el PC, se escoje SI.

Solo si el computador ha reiniciado, se estará listo para configurar los puntos de acceso y/o estaciones de red.

Nota: Esta configuración IP debe verificarse en todas las estaciones que conformarán la WLAN. Cabe recalcar que la dirección de la puerta de enlace debe ser la 10.1.0.129 para todas las estaciones de la red.

CAPITULO 7

GESTIÓN DE LA RED LAN INALÁMBRICA.

En este capítulo, se trata la gestión de toda la red inalámbrica, como ya se había mencionado el software de gestión de la red trabaja sobre SNMP, el cual divide la gestión en cinco módulos:

- Gestión de la Configuración.
- Gestión del Rendimiento.
- Gestión de Seguridad.
- Gestión de Fallas y Recuperación.
- Gestión de la Contabilidad.

De estos cinco tipos de gestión, las que maneja el software de administración Orinoco son los tres primeros. A continuación se explica como se realiza esta gestión sobre la red inalámbrica.

7.1 Gestión de la Configuración.

En esta sección, se analiza la configuración de las estaciones de trabajo utilizando las tarjetas PC y los adaptadores USB, así como también la configuración de los puntos de acceso.

7.1.1 Configuración de las Estaciones de Trabajo usando Tarjetas PC.

Después de haber instalado los controladores de la tarjeta PC (como se explicó en el capítulo 6), Windows automáticamente abrirá la ventana de perfil de configuración **Add/Edit Configutation Profile** de la tarjeta PC Orinoco, como se muestra en la figura 7.1.

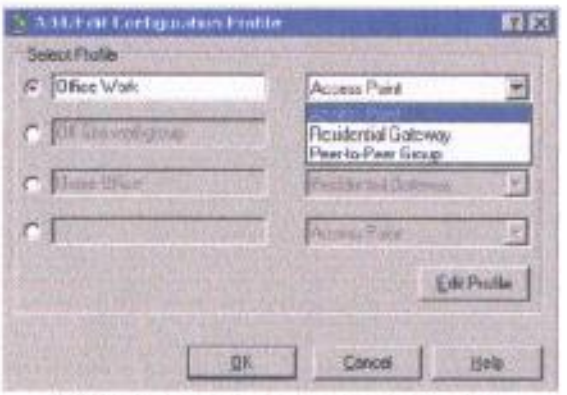


Fig 7.1: Configurando la tarjeta PC

En esta ventana, se habilitan uno o más perfiles de conexión de red. Por ejemplo se pueden configurar los siguientes perfiles:

- **Office Work,** para conectarse a una red empresarial vía punto de acceso.
- **Workgroup Computing,** para compartir archivos entre usuarios de una pequeña red punto a punto sin AP's (redes ad-hoc).
- **Home,** para conectarse a un Residencial Gateway, que es otro equipo de la familia Orinoco utilizado para proveer acceso a internet.

En este diseño se tendrá que escoger la conexión **Oficce Work,** por lo tanto:

- Se selecciona la opción Access Point.
- Luego se selecciona un nombre para la red (network name), veáse figura 7.2.

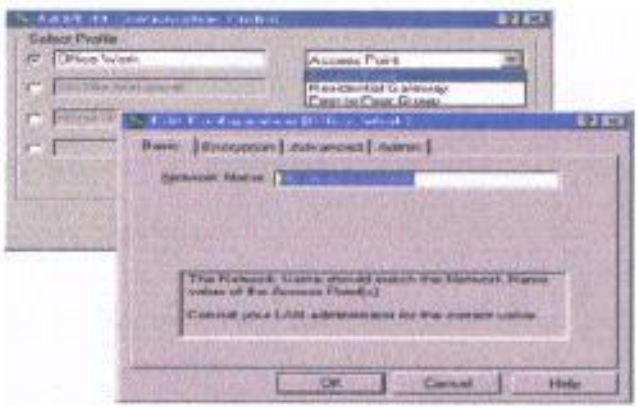


Fig 7.2: Seteando el nombre de red

- En el campo network name, se ingresa los caracteres que definan el nombre de la red inalámbrica con la cuál se va a trabajar; en este diseño se ha usado como netwok name MACAZA.

Con esta configuración básica, la estación de trabajo estará lista para comunicarse con los AP's.

Para verificar si la instalación y configuración de la tarjeta fue completada exitosamente:

1) Se chequea si el icono de la tarjeta PC sobre la barra de tareas de Windows es visible, tal como se muestra en la figura 7.3.

Fig 7.3: Icono de la Tarjeta PC.

2) Revise los leds en la tarjeta PC, lo siguiente deberá ser visible:

- Un led estará en color verde y se mantendrá fijo, indicando que la tarjeta PC está activa.
- El otro led (transmisión y recepción), deberá parpadear en verde indicando actividad inalámbrica mientras transmite los datos (esto ocurrirá en el momento que el AP esté también configurado y activo).

Esta misma configuración debe aplicarse al resto de estaciones de trabajo.

7.1.2 Configuración de las Estaciones de Trabajo usando Adaptadores USB.

El procedimiento de configuración de una estación de trabajo que utiliza un adaptador USB, es exactamente el mismo que como si se utilizara una tarjeta PC; luego que este adaptador ha sido conectado al puerto USB del computador.

7.1.3 Configuración de los Puntos de Acceso.

Para configurar los puntos de acceso por primera vez se procede de la siguiente manera:

1) Conectar la estación de gestión vía cable de red al mismo switch donde están conectados los puntos de acceso, como indica la figura 7.4.

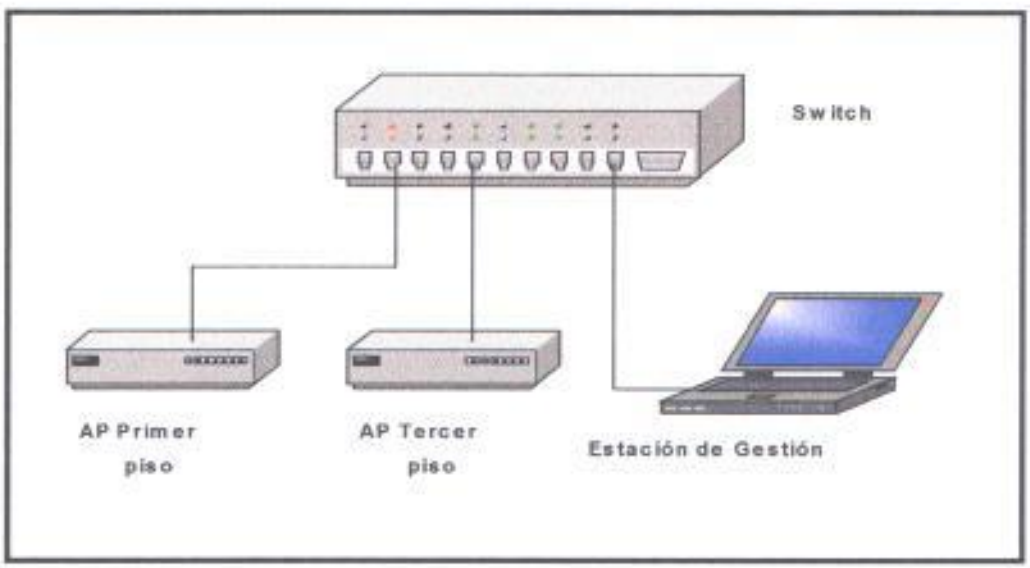


Fig 7.4: Conexión de la estación de gestión al switch

2) Abrir el software Orinoco de administración OR y escoger del menú **File** la opción **Open Remote Config** (figura 7.5).

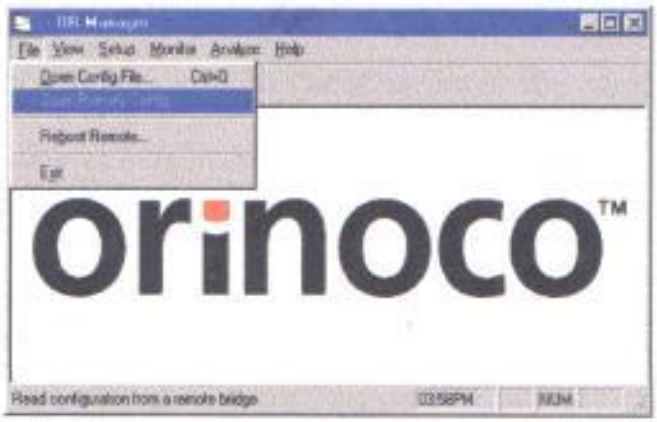


Fig 7.5: Preparando búsqueda de equipos

3) A continuación escoger la opción Scan, así como muestra la figura 7.6.

Fig 7.6: Buscando los AP´s en la red

4) Luego se mostrará una pantalla con la descripción de los dos puntos de acceso conectados al switch (figura 7.7).

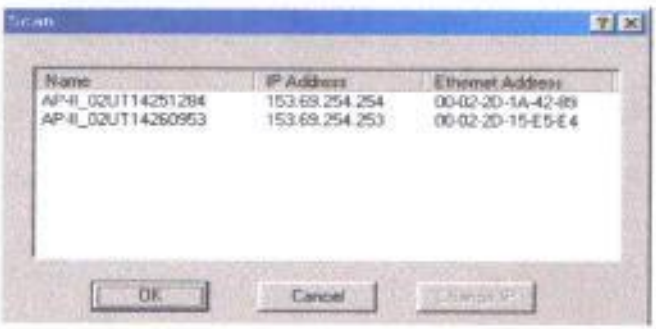


Fig 7.7: Equipos encontrados en la red.

5) Seleccionar uno de los 2 equipos y hacer click en Ok para entrar al AP (figura 7.8), y proceder a configurar los parámetros de network name (nombre de red), y frecuencia.

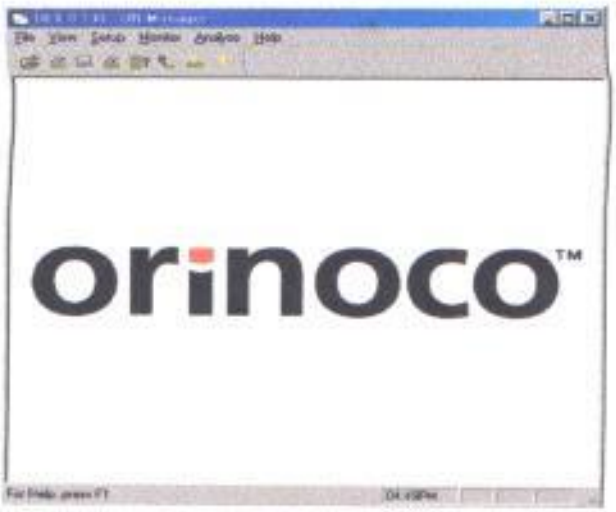


Fig 7.8: Ventana principal del Administrador OR

6) Para configurar el **network name** (nombre de red), entrar al menú **Setup** y escoger la opción **Interface Setup / Setup 2;** y escribir el nombre de red (este nombre de red debe ser el mismo que se configuró en todas las estaciones de trabajo, es decir MACAZA), figura 7.9. La interface 2 corresponde al slot A del AP (access point), donde está insertada la tarjeta PC. El nombre de red puede ser una cadena alfanumérica de 1 a 32 caracteres en el rango de "a hasta z", "A hasta Z", y "0 al 9".

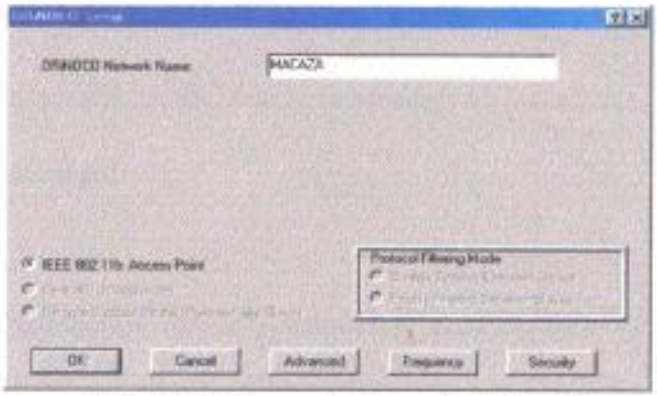


Fig 7.9: Configurando el nombre de red.

7) Luego, ingresar en la opción **Frecuency** y seleccionar el canal deseado, esta opción de configuración brinda la facilidad de seleccionar la frecuencia de operación del rango de canales de la banda 2.4 Ghz. El número de canales seleccionables son 11 (figura. 7.10).

Fig 7.10: Configurando la frecuencia.

Como ya se mencionó en el capítulo 5, para un mejor desempeño de la red cada AP trabajará en una frecuencia diferente, así de esta manera las estaciones de trabajo podrán usar el máximo ancho de banda disponible. Para este AP el canal seleccionado será el 11.

Las estaciones de trabajo que se muevan por todo el edificio, podrán cambiar dinámicamente de frecuencia (**roaming**) al conectarse con el AP que tiene diferente canal.

Estos mismos parámetros deben configurarse para el otro AP, la única diferencia es que la frecuencia en que trabajará este AP es la 1, por lo explicado anteriormente.

Con esta simple configuración los AP´s, deberán entrar en red junto con las estaciones de trabajo.

Nota: De acuerdo a lo explicado, el parámetro de la frecuencia solo se configura en el AP y no en la estación de trabajo. Esto se debe a que las estaciones utilizan el siguiente mecanismo para conectarse a los AP´s:

- Las estaciones comparan su nombre de red con el de los AP´s.
- Una vez que detectan esto, hacen un escaneo de todas las frecuencias hasta encontrar la que esta usando el AP mas cercano y se enganchan a la misma. Por esta razón en las estaciones no se especifica ninguna frecuencia de trabajo.

7.1.3.1 Configuraciones Avanzadas.

En esta sección, se trata las configuraciones adicionales más relevantes que se pueden hacer en los AP's.

Los parámetros adicionales que se pueden manejar en la configuración son los siguientes:

1) Reservación del Medio RTS/CTS.
2) Grado de Interferencia.
3) Distancias entre Ap's.
4) Tasa de Transferencia.
5) Parámetros Bridge.
6) Parámetros IP del AP.
7) Parámetros SNMP.
8) Interface Ethernet

A continuación se explican cada uno de los parámetros:

1) Reservación del Medio RTS/CTS.

El parámetro RTS/CTS (Reservación del Medio), proveerá una solución para las redes donde:

- El número de estaciones ORINOCO y AP (Acces Points) son muy bajas.

- El desempeño de la red sea pobre debido a las excesivas colisiones en los AP's.

Este parámetro es muy importante y se lo explica más detalladamente en la sección correspondiente a la **Gestión de Rendimiento,** en la página 161.

2) Grado de Interferencia

La Robustez de la Interferencia puede ser activada en casos excepcionales cuando el desempeño de la red sea bajo, esto puede ser debido a la interferencia causada por hornos microondas. La interferencia usualmente se presenta con un nivel pobre en la relación señal a ruido (SNR), se basa en un buen nivel de señal y un alto nivel de ruido. Este comportamiento a menudo es percibido cuando:

- Las estaciones o el AP están cerca de una fuente de interferencia.
- La fuente de interferencia está localizada en la trayectoria de la señal entre la estación que tiene problemas y el AP.

3) Distancia entre los AP's

En redes LAN donde se tiene un gran tráfico de datos o muchos usuarios en una área pequeña, se deberá considerar aumentar el

número de AP´s en la red (haciendo que la distancia entre los AP´s sea la mínima), y luego ajustar los parámetros de distancia entre los mismos para optimizar el balanceo de la carga del número de estaciones inalámbricas por AP.

Para cambiar los parámetros de distancia entre AP´s, se ingresa al menú **Setup / Interface Setup / Setup 2 / Advanced**, en el campo de distancia entre AP´s escoger una de las tres opciones, como muestra la figura. 7.11.

- Large (valor por defecto)
- Médium
- Small

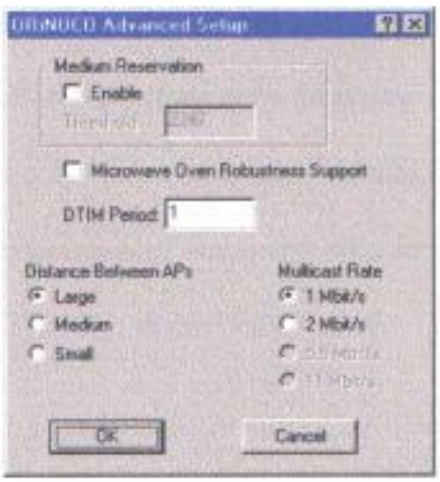


Fig 7.11: Opciones avanzadas de configuración

Large.- Esta opción es la que viene por defecto configurada y provee una máxima cobertura inalámbrica con un mínimo número de puntos de acceso. Esta opción la cual es típicamente usada por redes con una sola celda también provee una eficiente y efectiva solución para la mayoría de redes con múltiples celdas inalámbricas.

Médium.- Esta opción puede seleccionarse en ambientes donde las estaciones experimenten tiempos de respuestas altos, aunque la calidad del enlace de radio esté excelente. Los tiempos de respuestas altos pueden presentarse en áreas donde:

- Un alto número de estaciones inalámbricas se encuentren ubicadas entre sí muy cerca causando de esta manera interferencia en la transmisión de los datos.
- Algunas estaciones estén generando tráfico muy pesado en la red y causen un bajo desempeño en el resto de PC´s.
- El parámetro **Large** cree un solapamiento de las celdas la cual hace que estaciones en una celda difieran sus transmisiones a estaciones ubicadas en una celda vecina.

Small.- Esta opción se debería seleccionar solo cuando se diseñe una infraestructura inalámbrica que incluya un alto número de puntos de

acceso, que no es el caso de este diseño; por lo tanto el parámetro por defecto **Large** es el que se aconseja usar.

Precaución: El parámetro de distancia entre AP's debe ser el mismo para todas la interfaces inalámbricas de la red (es decir en los 2 AP's). Un error en la configuración de este parámetro puede causar resultados imprevisibles en el desempeño de las estaciones de la red.

4) Tasa de Transferencia

Este parámetro indica la velocidad de transmisión con que trabajará el punto de acceso (figura 7.11, Multicast Rate).

5) Parámetros Bridge

Una de las maneras de mejorar el desempeño de la red, es prevenir el tráfico redundante y que éste se transmita sobre la red inalámbrica. El tráfico redundante puede incluir:

- Protocolos específicos de red intercambiados entre dispositivos tales como servidores, que no tienen nada que ver con las estaciones inalámbricas
- Mensajes de broadcast y multicast intercambiados por equipos de red tales como servidores, que no son específicamente dirigidos hacia las estaciones inalámbricas.

- Tráfico basura, generado por ejemplo por mensajes de error causado por el mal funcionamiento de algún equipo o como resultado de una configuración de red incorrecta que podría haber sido evitada.

Filtrando el tráfico redundante se ahorrará ancho de banda para las estaciones inalámbricas, mejorando el desempeño de estas.

El mejoramiento del desempeño inalámbrico usando los **Parámetros Bridge** se logrará de las siguientes maneras:

a) Filtrando protocolos, es decir denegando protocolos específicos de red.
b) Filtrando el tráfico intercambiado entre dos estaciones, que son identificadas por su dirección MAC.

Precuación: Los parámetros bridge deben configurarse igual en todos los puntos de acceso.

Fig 7.12: Parámetros Bridge

a) Filtrando protocolos.

Los protocolos filtrados se listan en la sección BRIDGE, el valor por defecto del punto de acceso es <All protocols bridged>, (figura 7.12), lo cual permitirá que todos los protocolos sean transmitidos sobre el medio inalámbrico. Esta configuración es recomendada cuando no se requiera el filtrado de ningún protocolo en específico, como es el caso de este diseño.

Para filtrar protocolos específicos se procede como sigue:

- Determine los protocolos a filtrarse.
- Hacer click en el botón de EDIT para mostrar todos los protocolos ethernet, como se muestra en la figura 7.13.

Fig 7.13: Filtro por protocolos

- Marque los protocolos que no necesitan que sean transmitidos sobre el medio inalámbrico.
- Si desea agregar un protocolo que no este mostrado en la lista hacer click en el botón **CUSTOM,** para ingresar el protocolo manualmente.

b) Filtro por direcciones MAC estáticas.

Esta opción filtra el tráfico por las direcciones MAC de las estaciones. El valor por defecto es **<All Adreess Pair Permit>** que es utilizado para la mayoría de las configuraciones inalámbricas.

Este parámetro ayuda a mejorar el desempeño e incrementar la seguridad de la WLAN. Se puede permitir o denegar el acceso hacia estaciones individuales especificando sus direcciones MAC.

Todo el tráfico que aparezca listado en el Ethernet pair list, será permitido o denegado según su selección, en la figura 7.14 se muestra un ejemplo.

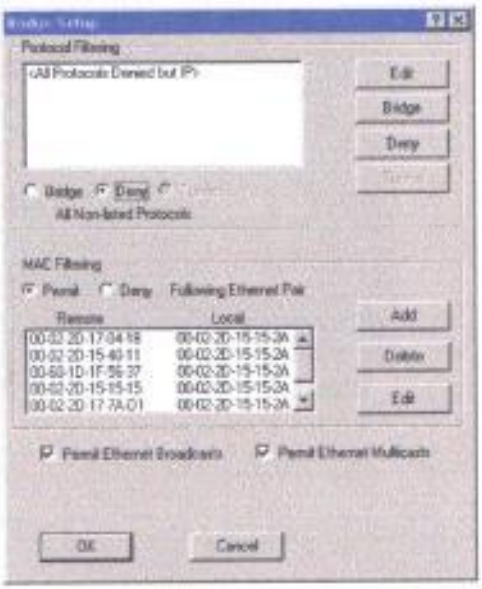


Fig 7.14: Filtro por direcciones MAC

6) Parámetros IP del AP.

Esta opción permite verificar los parámetros IP del punto de acceso así como también modificarlos.

En la figura 7.15, se muestra la configuración IP para el caso de este diseño; cabe mencionar que en el campo **Default Router IP** la dirección ingresada corresponde a la dirección IP del Firewall, que es el equipo que está haciendo NAT y permitirá la salida a internet de la WLAN.

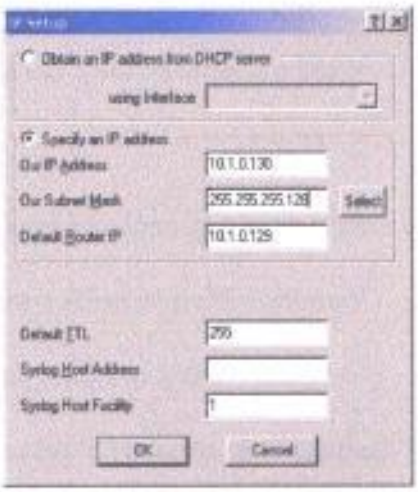


Fig 7.15: Parámetros IP del AP

7) Parámetros SNMP.

Los parámetros usados para este diseño se muestran en figura 7.16. La mayoría de los parámetros SNMP (excepto System Location y System Name), son parámetros comunes y deberían ser los mismos para los 2 AP's de la red.

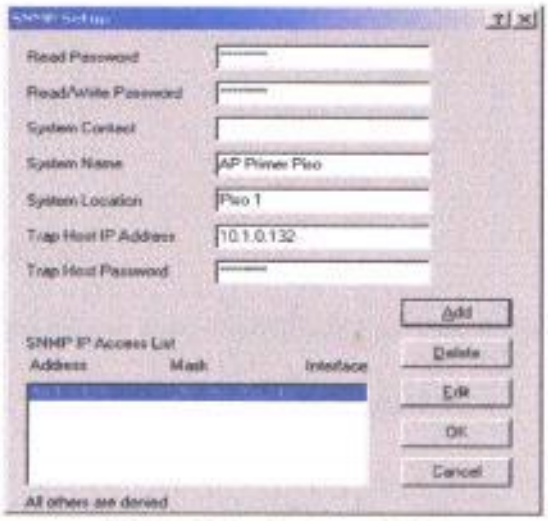


Fig 7.16: Parámetros SNMP

A continuación se explican los siguientes parámetros SNMP:

a) System Contact (Contacto del Sistema)

b) System Name (Nombre del Sistema)

c) System Location (Ubicación del Sistema)

a) System Contact.

Este campo se usa para ingresar un nombre genérico del supervisor de la red o departamento.

b) System Name.

Este campo se utiliza para ingresar el nombre con que se identificará el punto de acceso, para este diseño se ha usado los siguientes nombres para los AP´s:

- AP Primer Piso.
- AP Tercer Piso.

c) System Location.

Este campo se usa para especificar una ubicación física del punto de acceso, por ejemplo Piso 1, ver figura 7.16.

El resto de parámetros SNMP brindan seguridad por lo tanto, son explicados detalladamente en la sección 7.3 en la página 165, correspondiente a la **Gestión de Seguridad**.

Para setear los parámetros SNMP se procede como sigue:

- Asegúrese de que este dentro de un AP y escoja la opción **Setup / SNMP Setup,** como muestra la figura 7.16.
- Verifique y/o modifique los parámetros que desee

8) Interface Ethernet.

Esta opción permite seleccionar la manera que al AP se conectará con la red cableada. Para ingresar a esta opción hacer clic en **Setup / Interface Setup / Ethernet.** La opción mostrada en la figura 7.17 es la que viene por defecto.

Fig 7.17: Configuración de la interfase ethernet

7.2 Gestión del Rendimiento.

Fundamentalmente la gestión del rendimiento consta de dos categorías funcionales: **Monitorización** y **Control.** La monitorización realiza el seguimiento de las actividades de la red. La función de control permite realizar ajustes necesarios para mejorar el rendimiento.

A continuación, se explica la gestión de la WLAN basándose en estas dos categorías.

7.2.1 Monitorización.

Una vez que la red ha sido configurada e instalada, se podrá usar las herramientas del software Orinoco para:

- Monitorear el rendimiento de la red.

- Verificar la ubicación óptima de los AP's y de las estaciones inalámbricas que se quiere controlar.

Se aconseja verificar el desempeño de la red frecuentemente, ya que el rendimiento puede cambiar cuando estaciones inalámbricas se reubiquen, o cuando en las oficinas se realizan cambios fisicos (nuevas paredes, o escritorios), o en el caso de que algún equipo nuevo sea instalado, y posiblemente cause interferencia con la comunicación inalámbrica.

7.2.1.1 Herramientas de Monitoreo.

El software de gestión ofrece 2 herramientas que habilitan el monitoreo de la red:

1) Administrador del Cliente (Client Manager).
2) Administrador del AP (OR Manager).

1) Administrador del Cliente (Client Manager).

El administrador del Cliente ha sido diseñado para monitorear el desempeño de la red en algún lugar de la misma. Se puede usar este programa para:

- Diagnosticar la radio comunicación con los AP's que se encuentran dentro del área de cobertura de la estación.

- Visualizar detalladamente resultados de las mediciones de la prueba de enlace (link test), con el AP más cercano a la estación inalámbrica.

La siguiente pantalla muestra la ventana principal del Administrador del Cliente.

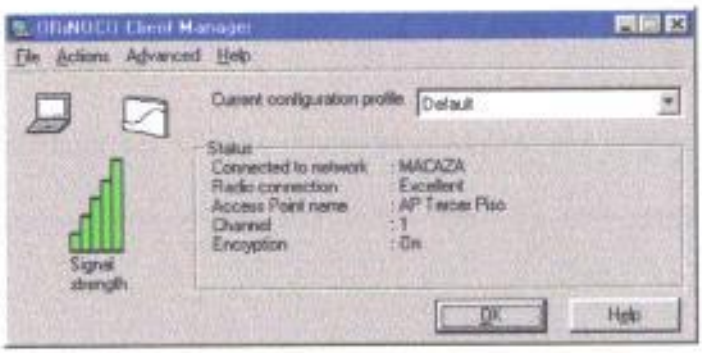


Fig 7.18: Administrador del cliente

Esta ventana muestra información importante de la conexión de red actual, la cual se describe a continuación:

- El nombre de red (MACAZA), a la cual la estación está conectada.
- La calidad de la conexión de radio, que puede ser Excelente, Buena, Marginal, Pobre o Fuera de rango.
- La calidad de conexión de radio es también visualizada en un icono de color:
  - Verde, excelente o buena conexión.

- Amarillo, Conexión Marginal.

- Rojo, Conexión Pobre.

- Rojo con señales de error, no conexión.

- El nombre del AP al cual la estación está conectada en ese momento.
- El canal usado para la conexión.
- Encriptación: Apagado/ Encendido

El Administrador del Cliente en su menú **Advanced** (figura 7.18), ofrece algunos métodos de monitoreo, entre los más importantes tenemos:

a) Link Test (Prueba de enlace).
b) Site Monitor (Monitor del lugar)
c) Card Diagnostics (Diagnóstico de las tarjetas de red inalámbricas).

Métodos de Monitoreo del Administrador del Cliente.

a) Método de monitoreo Link Test (Prueba de Enlace).

Este método es usado para obtener un diagnóstico detallado de la calidad del enlace de radio, entre una estación y un equipo de prueba específico. Este equipo podría ser:

- Un punto de acceso, AP
- Otra estación (en el caso que la configuración usada sea punto a punto)

Para iniciar la prueba de enlace, se selecciona el método de monitoreo **Link Test** en el menú **Advanced** de la ventana principal del **Administrador del Cliente** (figura 7.19).

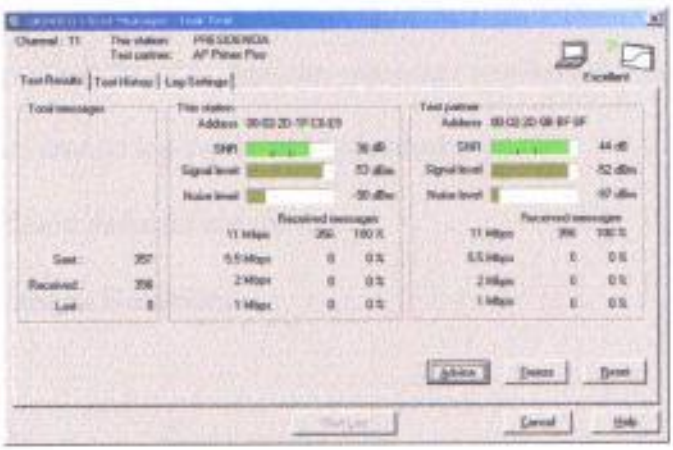


Fig 7.19: Prueba de Enlace

En la parte superior de la ventana Prueba de Enlace, se puede observar:

- El canal de radio sobre el cual ambos dispositivos están comunicándose.
- El nombre de la estación.

- El nombre del AP con quien se está efectuando la prueba del enlace.
- La calidad de la conexión.

La ventana Link Test (figura 7.19) provee algunas opciones para ayudar en el análisis de los datos de la prueba, de los cuales el más importante y utilizado es **Test Results** que se describe a continuación.

La opción **Test Results,** permite visualizar resultados de la prueba del enlace usando los siguientes indicadores:

I. Relación Señal Ruido (SNR)

II. Mensajes Recibidos

I. Relación Señal a Ruido (SNR).

La relación señal a ruido identifica la calidad de la comunicación entre la estación y el AP. Este indicador es actualizado dinámicamente de acuerdo al estatus actual del enlace de radio.

El color del indicador SNR se refiere a la calidad de la comunicación:

- **Verde**- La calidad de la comunicación es excelente o buena, no requiere ninguna intervención.
- **Amarillo**- La calidad de la comunicación es aceptable, no requiere ninguna intervención.
- **Rojo**- La calidad de la comunicación es pobre, requiere intervención inmediata.

Si el nivel de la relación señal a ruido es más bajo que el esperado los indicadores del nivel de señal y del nivel de ruido pueden ayudar a investigar la causa de la siguiente manera:

- Un nivel de señal bajo, indica que la intensidad de la señal de radio es bastante baja. Esto se puede dar debido a que la estación se encuentre fuera de rango con el AP.
- Un nivel de ruido alto, indica que existe interferencia en la trayectoria entre los 2 equipos (la estación y el AP). Comparando los valores de ruido en la estación y en el AP con que se está haciendo la prueba de enlace, ayudará a identificar el lugar donde ocurre la interferencia; y así poder tomar alguna acción para eliminar o resolver esto obteniendo un mejor desempeño.

II. Mensajes Recibidos.

El indicador de mensajes permite determinar la eficiencia del enlace entre la estación y el AP.

Cuando la prueba de enlace está corriendo, la estación intercambia mensajes con el punto de acceso. Este equipo a su vez confirmara que ha recibido el mensaje y enviará una respuesta favorable.

Ambos, la estación y el AP utilizan estos mensajes para:

- Medir la relación señal/ ruido (SNR)
- Comparar el número total de mensajes enviados con el número total de mensajes recibidos de la siguiente manera:
  - Cuando la calidad de la comunicación es considerada como Excelente o Buena, el número total de mensajes perdidos deberá ser cero.
  - Cuando la calidad de comunicación es Aceptable, el número total de mensajes perdidos puede estar en el rango del 1% al 3%.
  - Cuando el número total de mensajes perdidos es > 5%, la red sufrirá algunos problemas en el rendimiento.

En muchas situaciones, se observará que el número de mensajes perdidos incrementará siempre y cuando el nivel de (SNR) disminuya.

b) Método de monitoreo Site Monitor (Monitor del Lugar).

El método Site Monitor permite visualizar la calidad de la comunicación entre la estación de gestión y todos los AP's que estén dentro del área de cobertura de la estación.

El monitor del sitio ha sido diseñado para:

- Determinar la cobertura inalámbrica global de la red.
- Verificar u optimizar la colocación de los AP's, a fin de proveer conectividad a las estaciones móviles.

Cuando se hace **roaming** a través de la red inalámbrica con la estación de gestión, se podrá identificar las áreas que no tienen una cobertura adecuada o que sufren interferencia con otros equipos (inalámbricos), tal como las puertas de seguridad, hornos microondas o fotocopiadoras.

Para iniciar el monitor del sitio, se selecciona la opción **Site Monitor** del menú **Advanced** en la ventana principal del administrador del cliente (figura 7.20).

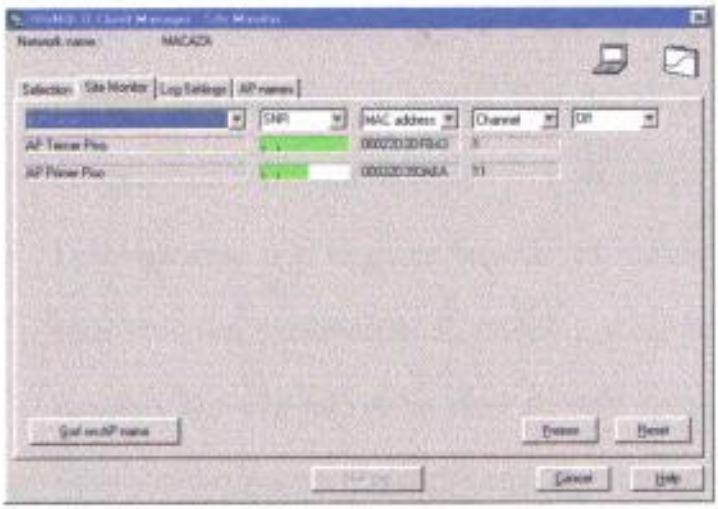


Fig 7.20: Monitor del Lugar

La ventana Site Monitor, cuenta con algunas opciones de las cuales las más relevantes son:

I. Site Monitor, para monitorear el rendimiento de la red.

II. Selection, permite realizar una búsqueda de redes vecinas y seleccionar estas para su monitoreo.

I. Site Monitor.

Esta opción permite realizar un estudio estándar del sitio (lugar donde funciona la WLAN) de la siguiente manera:

- Ingrese a la opción **Site Monitor,** como se describió anteriormente.
- Determinar en que lugares de la red se requiere conexión inalámbrica.
- Utilice una computadora portátil (estación de gestión), que permita moverse a través de todo el área que comprenderá la red inalámbrica.
- Desplazándose a lo largo de toda la red, verifique que cada sitio sea cubierto por lo menos por un punto de acceso y que éste provea un nivel de SNR (relación de señal a ruido) que sea al menos aceptable o mejor.

Nota: Este procedimiento es el que se utilizó en el diseño de la WLAN para determinar el número y ubicación de los AP´s necesarios para la red.

Cuando se abra la ventana **Site Monitor** (figura 7.20), ésta mostrará lo siguiente:

En la parte superior izquierda de la ventana se visualizan los siguientes campos:

Red Actual (Network Name), que identifica el nombre de la red al cual esta conectado actualmente.

Distancia entre AP´s, describe como esta configurado en distancia el AP al cual se está conectado actualmente.

Estos campos permanecen visibles aunque se seleccionen cualquiera de las otras opciones en la ventana del **Site Monitor.**

También se mostrara en esta ventana, los AP´s que estén dentro del rango de cobertura de la estación con las siguientes descripciones:

- Nombre del AP
- SNR.
- Canal.

II. Selection

Esta opción permite seleccionar otras redes en situaciones donde se desee:

- Verificar la presencia de otras redes Orinoco vecinas.
- Determinar si tal red posiblemente interfiera con la red principal.

c) Método de monitoreo Card Diagnostics (Diagnóstico de las tarjetas de red inalámbricas).

Si se sospecha que la tarjeta PC no está funcionando apropiadamente, se puede seleccionar **Diagnostics** en el menú **Advanced** de la ventana principal del Administrador del Cliente, para investigar la funcionalidad del hardware y el software de la tarjeta.

La ventana de diagnóstico de la tarjeta permite chequear el software, información del firmware y de la configuración así como también estadísticas de comunicación.

Para probar la tarjeta hacer click en el botón **Test Card Now** sobre la opción de Chequeo de Tarjeta (figura 7.21)

Nota: En el momento que se está efectuando la prueba, la tarjeta dejará de funcionar normalmente, lo cual podría causar una pérdida en la conexión a la red.

Si la tarjeta PC Orinoco pasa todas las pruebas, el estado de la prueba será **"OK"** en todos los campos y el campo código de error

permanecerá en blanco. Si ocurre un error, hacer click en el botón **"Advice"** para más información en como manejarlo.

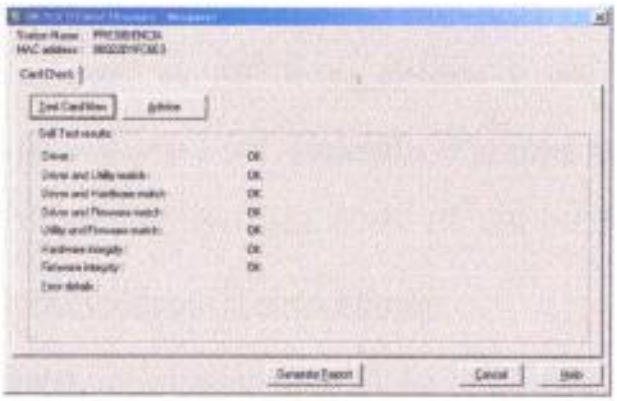


Fig 7.21: Prueba de la tarjeta PC

2) Administrador OR (OR Manager).

El Administrador OR ha sido diseñado para monitorear la red desde una ubicación central, es decir utilizando una estación de gestión LAN.

El programa Administrador OR ofrece una variedad de opciones de diagnóstico, contenidas en el menú **Monitor** y **Analyze** de la ventana principal del software

Entre las opciones de diagnóstico más importante tenemos:

- Visualización de un conjunto estándar de variables SNMP para monitorear el desempeño general del trafico LAN en la red (contenidas en el menú **Monitor**).
- Visualización remota de las mediciones de **Link Test** (prueba de enlace) entre un AP de su elección y una estación inalámbrica conectada a éste (contenidas en el menú **Analyze)**.

Monitoreo de la Red utilizando el menú **Monitor**

Este menú cuenta con las opciones mostradas en la figura 7.22.

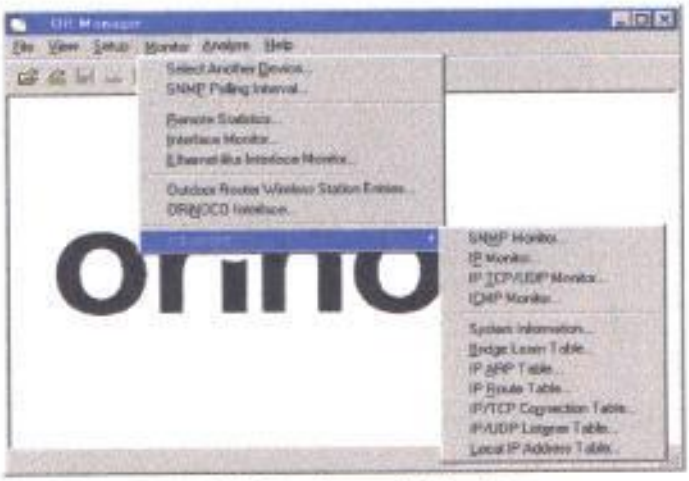


Fig 7.22: Opciones de Monitoreo

A continuación se describen las opciones más importantes de este menú:

a) SNMP Polling Interval (Intervalo de Poleo SNMP).

b) Remote Statistics (Estadísticas Remotas).

c) Interface Monitor (Monito de las interfaces).

d) Orinoco Interface (Interface Orinoco)

e) Advanced (Opciones avanzadas de monitoreo).

a) SNMP Polling Interval (Intervalo de poleo SNMP).

Esta opción permite setear la frecuencia con que el Administrador OR recogerá información SNMP del punto de acceso. Por ejemplo, los datos mostrados en las estadísticas remotas, se actualizan en intervalos regulares que pueden variar de 1 a 5 minutos (figura 7.23).

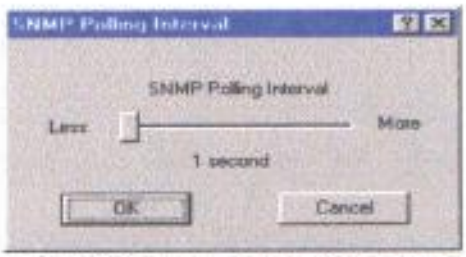


Fig 7.23: Intervalo de poleo SNMP

Se usa un intervalo de tiempo corto (1 minuto) para el monitoreo de las estadísticas remotas, solo si se dispone de un ancho de banda grande. Se usa un intervalo de tiempo largo (5 minutos por ejemplo), solo para información general del estado del enlace o en casos donde se tenga un ancho de banda bajo.

b) Remote Statistics (Estadísticas Remotas).

La opción de Estadísticas Remotas permite monitorear un conjunto de variables SNMP para cada interface del AP (ethernet e inalámbrica).

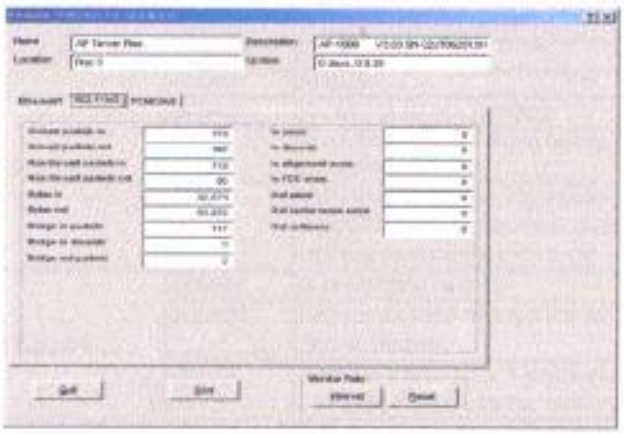


Fig 7.24: Estadísticas Remotas

El rendimiento de cada interface del AP seleccionado, puede ser visualizado escogiendo la interface que se desee (Orinoco o Ethernet como muestra la figura 7.24).

Los indicadores que proveen información relevante sobre el desempeño de las interfaces son llamados **ratio errors to bridge packets**. Hay tres indicadores los cuales tienen un valor en particular:

- "In errors" / "Bridge in packets".
- "Out errors" / "Bridge out packets".
- "Out collisions" / "Bridge out packets"

La siguiente tabla provee una relativa información de diagnostico para cada uno de éstos tres indicadores:

Ratio Errors to Bridge Packets	Conclusión	
0,1 % o menos	Estatus	El desempeño es bueno
	Impacto	Ninguno
	Acción	Ninguno
0,1 % y 1 %	Estatus	El desempeño es aceptable
	Impacto	El rendimiento de la red es normal, pero no es como se espera.
	Acción	Referirse a la sección "Optimizando el Rendimiento" del capítulo 7 para determinar la causa del problema y optimizar el desempeño de la red.
1% o más	Estatus	El desempeño es pobre
	Impacto	Esto puede darse debido a problemas de la red cableado o conectores.
	Acción	Referirse a la sección "Optimizando el Rendimiento" del capítulo 7 para resolver este problema
2% o más	Estatus	El desempeño es muy pobre
	Impacto	Es probable que la red presente serios problemas en su rendimiento
	Acción	Referirse a la sección "Optimizando el Rendimiento" del capítulo 7 para investigar el problema con más detalle

Tabla V: Diagnóstico de la red basado en las Estadísticas Remotas

c) Interface Monitor (Monitor de la Interfaces).

Muestra información genérica sobre las interfaces físicas de los AP's, incluyendo información de configuración y estadísticas de los eventos ocurridos en cada interface (figura 7.25).

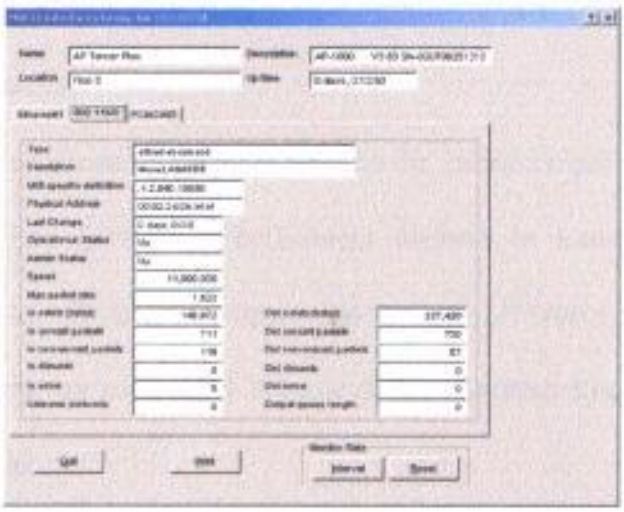


Fig 7.25: Monitoreo de las interfaces del AP

d) Orinoco Interface (Interface Orinoco).

Permite ver la actividad de esta interface en el AP (figura 7.26).

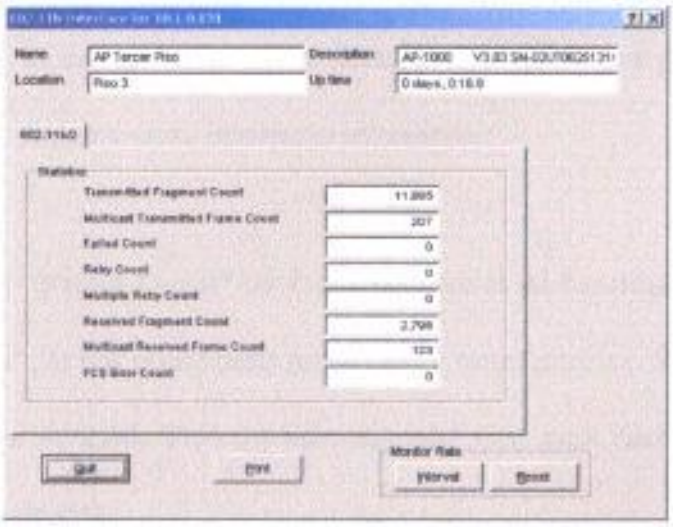


Fig 7.26: Estadísticas de las interfaces inalámbricas del AP

Los tres indicadores a los que se podría prestar particular atención son:

- **Retry count**.- Cuenta el número de paquetes que se han perdido (debido a colisiones) durante la transmisión inicial. Durante la operación normal, el **retry count** podría ser menos del 3% que el **Transmitted Fragment count.**
- **Múltiple retry count.-** Cuenta el número de paquetes que se han perdido después de la transmisión inicial. Durante la operación normal el **"múltiple retry count"** será menos que el 3% del **"retry count"**.
- **Failed Count.-** Cuenta el número de paquetes que han alcanzado el límite de reintentos de envío. Los paquetes fallidos ya no intentarán retransmitir.

Si las **"Failed Count"** es 1% o más que el de **"multiple retry count"**, la red puede estar sufriendo de interferencias. Se usa la opción de **Link Test** del administrador OR, para encontrar la causa de ésta.

e) Advanced (Opciones Avanzadas de Monitoreo).

En ésta sección se muestran estadísticas sobre los grupos pertenecientes a la MIB II de SNMP recogidas por el AP.

Esta opción consta de algunos parámetros, entre los más importantes tenemos:

e1. SNMP Monitor.

e2. IP Monitor.

e3. TCP/UDP Monitor

e4. ICMP (Internet Control Message Protocol) Monitor.

e5. System Information.

e6. Bridge Learn Table.

e7. IP ARP (Address Resolution Protocol) Table.

e1. SNMP Monitor.

Muestra un conjunto de variables recogidas en el agente SNMP que reside en las estaciones, así como muestra la figura 7.27.

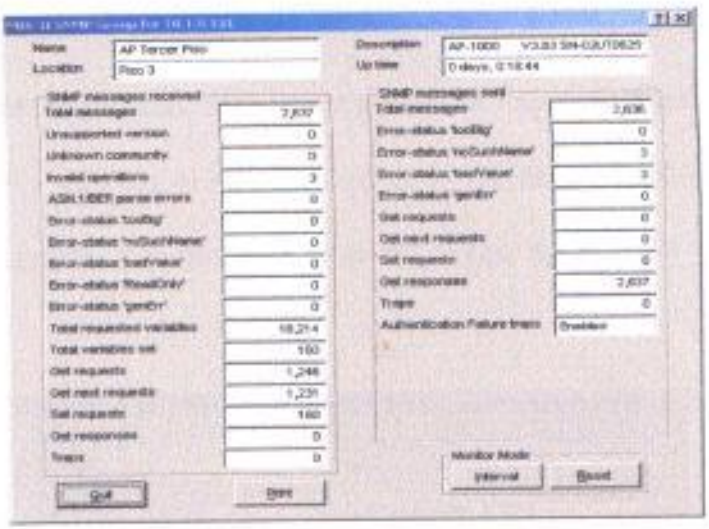


Fig 7.27: Variables SNMP

e2. IP Monitor.

Proporciona información sobre la implementación y ejecución de IP sobre el sistema (figura 7.28).

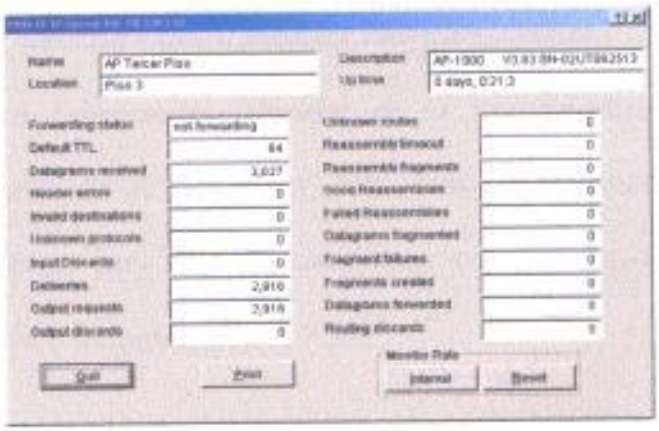


Fig 7.28: Estadisticas del grupo IP de la MIB II

e3. IP-TCP/UDP Monitor.

Muestra información relevante sobre la implementación de TCP y UDP en el AP. Además de la información sobre las datagramas transmitidos y recibidos, (veáse figura 7.29).

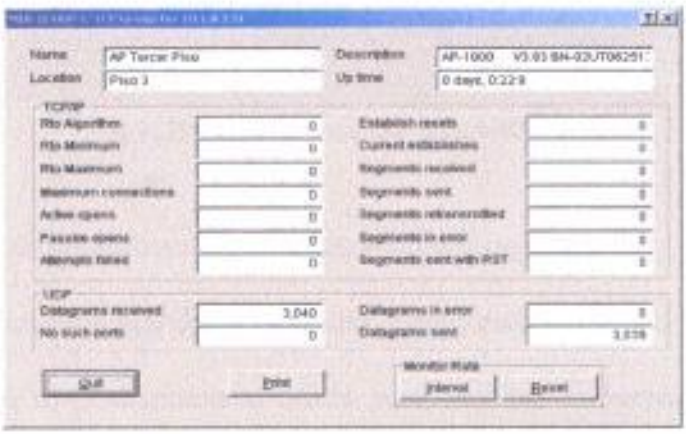


Fig 7.29: Estadísticas del grupo TCP-UDP de la MIB II

e4. ICMP (Internet Control Message Protocol) Monitor.

Muestra información relevante de la implementación y operación de ICMP en el AP. Consta únicamente de contadores, para los diferentes tipos de mensajes ICMP enviados o recibidos, (figura 7.30).

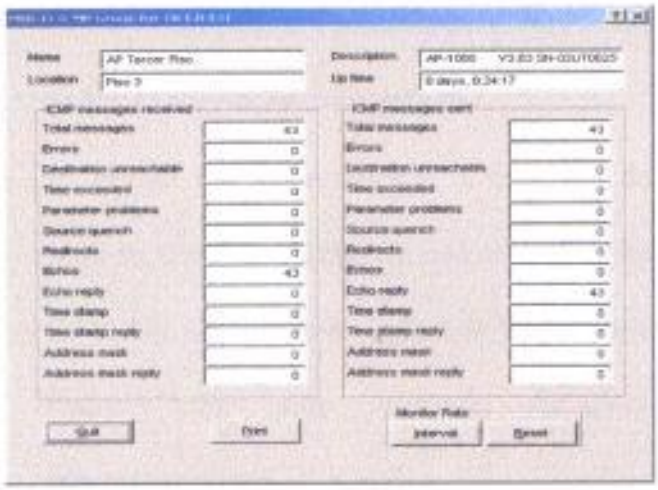


Fig 7.30: Estadísticas del grupo ICMP

e5. System Information (Información del Sistema).

La información del sistema no provee estadísticas en línea, pero es primariamente usada para verificar la versión del software que está cargado en el AP (figura 7.31).

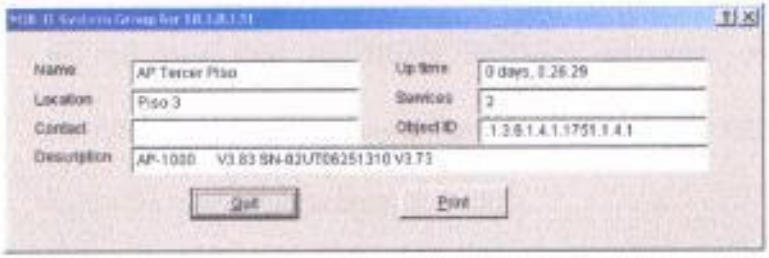


Fig 7.31: Estadísticas del grupo System

A continuación se explican los parámetros más importantes mostrados en la figura.

- Los campos nombre, ubicación y contacto representan los valores que han sido ingresados en los campos

correspondientes a **Parámetros SNMP,** cuando el punto de acceso fue configurado.

- El campo **Up Time** muestra el intervalo de tiempo medido desde la última vez que el AP fue reseteado. Si el **Up time** es más bajo que lo esperado, el AP podría haber sido reseteado manualmente o automáticamente.
- Los campos **Services y Object ID** no muestran información relevante para usuarios finales. Los parámetros mostrados se refieren a variables SNMP explicadas ya en el capítulo 2.
- El campo **Description** es el campo más importante de esta pantalla, le permitirá determinar rápidamente si el AP esta con el último software cargado, o posiblemente requiera una actualización para soportar todas las funcionalidades requeridas.

e6. Bridge Learn Table.

Muestra todas las direcciones MAC de las estaciones conectadas actualmente al AP (figura 7.32). El punto de acceso usa éstos datos para guardar información de

envío/filtro de estaciones, para así determinar como se propaga el paquete recibido.

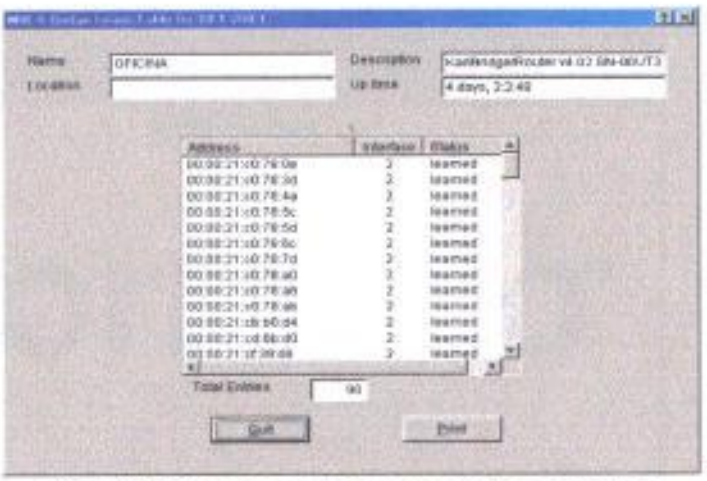


Fig 7.32: Direcciones MAC aprendidas por el AP

e7. IP ARP (Address Resolution Protocol) Table.

Muestra como las direcciones físicas (MAC) son mapeadas a direcciones IP en el punto de acceso, (veáse figura 7.33).

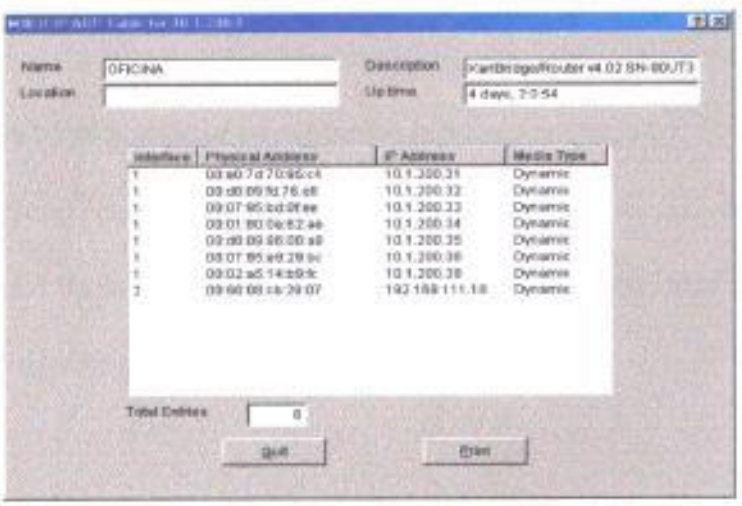


Fig 7.33: Mapeo de direcciones MAC a IP

Monitoreo de la Red utilizando el menú **Analyze**.

Este menú cuenta con las opciones mostradas en la figura 7.34.

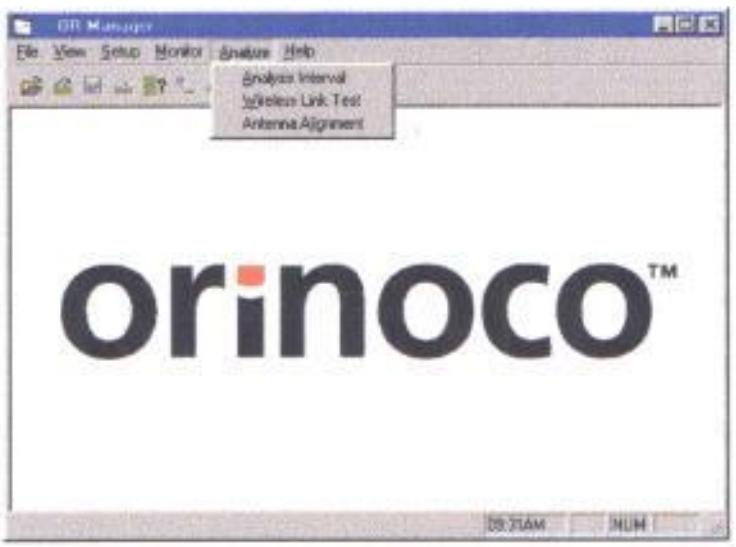


Fig 7.34: Monitoreo usando el menú Analyze

A continuación se describen las más utilizados:

a) Analisys Polling Interval (Análisis del intervalo de poleo).

b) Wireless Link Test (Prueba de enlace inalámbrica).

a) Analisys Polling Interval (Análisis del intervalo de Poleo).

Dependiendo del tipo de conexión, se puede ajustar la tasa de resultados de la prueba de enlace, también llamado análisis del intervalo polling.

Mientras la prueba de enlace remota recoge continuamente resultados de las mediciones, el AP seleccionado transferirá los resultados a la estación de gestión a intervalos regulares que pueden variar de 1 a 15 segundos, (figura 7.35).

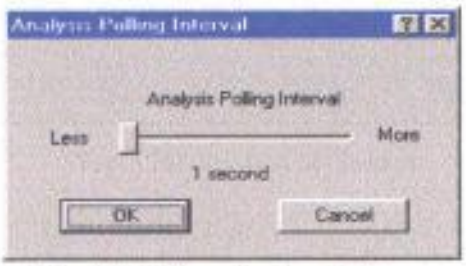


Fig 7.35: Intervalo de Poleo

Se usa un intervalo de tiempo corto (1 segundo por ejemplo) para el monitoreo en línea, esto es recomendable solo si se dispone de un ancho de banda grande. Se usa un intervalo de tiempo largo (15 segundos por ejemplo), solo para información general del estado del enlace o en casos donde la conexión tenga un ancho de banda bajo.

b) Wireless Link Test (Prueba de Enlace inalámbrica).

La Prueba de enlace permite investigar el enlace de radio entre el AP que se seleccione y una estación conectada al mismo (figura 7.36).

Fig 7.36: Prueba de Enlace

Todos los parámetros mostrados en la pantalla ya fueron estudiados en la sección anterior del Administrador del Cliente.

7.2.2 Optimización del Rendimiento, Control

El rendimiento de la red está usualmente determinado por la combinación de diferentes factores. Esta sección presenta un número de consideraciones que pueden ayudar a:

- Determinar si la optimización es realmente necesaria.
- Adaptar la red para optimizar su rendimiento.

Se considera optimizar el rendimiento de la red en situaciones donde:

- Se detecte en la red un problema extraño.
- El rendimiento de la LAN es menos de lo esperado, o

- Chequeos de rutina en intervalos regulares muestren una degradación del rendimiento de la red.

En esta sección, se recomiendan varias soluciones para algunos de los problemas más comunes mencionados. El beneficio de cada una de las soluciones propuestas, dependerá mayormente de la situación real que causó el rendimiento actual.

7.2.2.1 Eliminación del Tráfico Redundante.

Eliminando el tráfico redundante se puede mejorar significantemente el rendimiento de la red. Usando el **Administrador OR** se podrá escoger una o más de las siguientes opciones:

1) Filtrar Protocolos: Para filtrar protocolos que no son concernientes a estaciones inalámbricas.
2) Optimizar conexiones alámbricas: Para eliminar mensajes de errores redundantes debido a conexiones fallidas.
3) Optimizar conexiones Inalámbricas: Para evitar retransmisiones de paquetes perdidos o colisiones.

1) Filtro de Protocolos.

Muchos de los protocolos de red envían grandes volúmenes de broadcast a todas las estaciones. En muchos casos, estos protocolos

pueden no ser requeridos por las estaciones inalámbricas, por lo tanto la opción de filtrar protocolos puede prevenir la transmisión de datos innecesarios, reservando más ancho de banda para la comunicación de datos en la red.

Para verificar si el protocolo de difusión broadcast degrada o no el rendimiento de la red inalámbrica, se puede seleccionar la opción de **Remote Statistics** del menú **Monitor** (figura 7.24), y basándose en los parámetros mostrados en la **interface inalámbrica** establecer el rendimiento de la red, por ejemplo:

a) Compare el número de Out Collisions con el número de Bridge out packets.
   - Cuando el número de out collisions es el 1% menor que los paquetes bridge out, indica que el medio inalámbrico tiene un buen rendimiento.
   - Cuando él número de out colisiones es el 1% mayor que los paquetes bridge out, indica que el medio inalámbrico está muy ocupado.

b) Compare el número de "Unicast out packets" con el número de "Non-unicast packets out".
   - Cuando el número de "Non-unicast packets out" es relativamente alto comparado con él numero de "Unicast

packets out", esto podría indicar que la red genera una gran cantidad de trafico.

Cuando se cree que protocolos de red están afectando adversamente el rendimiento de la misma, se usa el procedimiento ya explicado en la sección **Gestión de la Configuración / Configuraciones avanzadas / Parámetros Bridge**, en la pagina 120; para filtrar protocolos de red innecesarios o no deseados.

2) Optimización de la conexiones alámbricas.

Algunas veces la degradación del rendimiento de la conexión (inalámbrica), es causada por una falla en el sistema de cableado que conecta la red con la infraestructura cableada.

Tales fallas pueden ser causadas por una de las siguientes situaciones:

- Un cable o conector defectuoso en la infraestructura cableada.
- Un segmento LAN ha sido extendido sobre una distancia que es demasiado larga.

Usualmente esto pasará en situaciones en que:

- El sistema no trabaje para nada, o
- El sistema de red generará un número grande de mensajes erróneos, como resultado de conexiones defectuosas. Como

éstos mensajes aumentan el ancho de banda utilizado, el rendimiento de la red puede ser muy lenta.

Un problema en el sistema de cableado puede ser diagnosticado con la opción **Remote Statistics**, seleccionando la opción **ethernet interface**, por ejemplo:

a) Se compara el número de "In errors" con el número de "Bridge in packets".
   - Cuando el número de "in errors" es el 1% o más que el número de "bridge in packets", esto puede indicar un problema de cableado

b) Se compara el número de paquetes "out errors" con el numero de "bridge out packets".
   - Cuando el número de "out Errors" es el 1% o más que el número de "bridge out packets", esto igualmente significa que hay un problema de cableado

c) Se compara el número de "Out carrier sense" errors con el número de "bridge out packets".
   - Cuando el número de "Out carrier sense errors" es el 1% que el número de "bridge out packets", o el valor de "Out carrier sense errors" aumenta demasiado rápido, esto indica

espacio insuficiente en la red debido a una sobrecarga en el backbone, o a un cableado defectuoso.

Usando el procedimiento descrito arriba, se puede determinar el área donde el error de cableado podría ocurrir. Para resolver el problema, chequear cuidadosamente el cableado en esta área verificando si todos los conectores están hechos correctamente a:

- AP's
- Switchs
- Estaciones alámbricas conectadas al sistema de cableado

3) Optimización de las conexiones inalámbricas.

Cuando la calidad del enlace de comunicaciones entre una estación inalámbrica y el AP es pobre, los paquetes entre ésta estación y el AP pueden llegar a perderse. Si no se da una respuesta de confirmación de la estación receptora, la estación que envió el paquete lo retransmitirá.

Al recibir el mismo paquete por segunda vez, la estación receptora puede decidir descartar el paquete recibido, teniendo que recurrir entonces a que la estación transmisora tenga que retransmitir el paquete una vez más.

Note que:

- Muchas retransmisiones pueden afectar la eficiencia de los datos efectivos, que tienen que compartir el ancho de banda inalámbrico con los paquetes retransmitidos.
- Las retransmisiones también degradarían el rendimiento de la red, que puede ser percibido por el usuario final de una estación inalámbrica; por ejemplo guardar un archivo tomaría mucho más tiempo si muchas retransmisiones son requeridas.

Una calidad de enlace pobre puede ser causada por uno o más de los siguientes problemas:

- Una estación está a punto de salir del rango de cobertura del AP.
- Hay una fuente de interferencia en el camino de la señal entre la estación y el punto de acceso.
- Hay una estación que puede ser "oculta" para otra estación dentro de la misma área de cobertura. Una estación oculta es una situación en la cual 2 estaciones inalámbricas están dentro del rango del mismo AP, pero no están dentro del rango de cada una.

Para resolver los dos primeros problemas mencionados anteriormente, se puede hacer uso de las opciones: **Link Test,**

Orinoco Interface, y Remote Statistics, ya detalladas en la sección de **Monitoreo.**

Por otro lado, para resolver el problema de la estación "oculta", se utiliza el algoritmo **RTS/CTS** explicado detalladamente a continuación:

Algoritmo RTS/CTS

EL mecanismo **RTS/CTS** permitirá mejorar el rendimiento inalámbrico en ambientes de red donde el protocolo CSMA/CA (Carrier Sense Multiple Acces / Collsion Avoidance, protocolo que evita que mensajes inalámbricos puedan chocar en situaciones donde 2 o más estaciones deseen comenzar transmisiones al mismo tiempo) habria fallado debido al problema de una estación oculta como se ve en la figura 7.37.

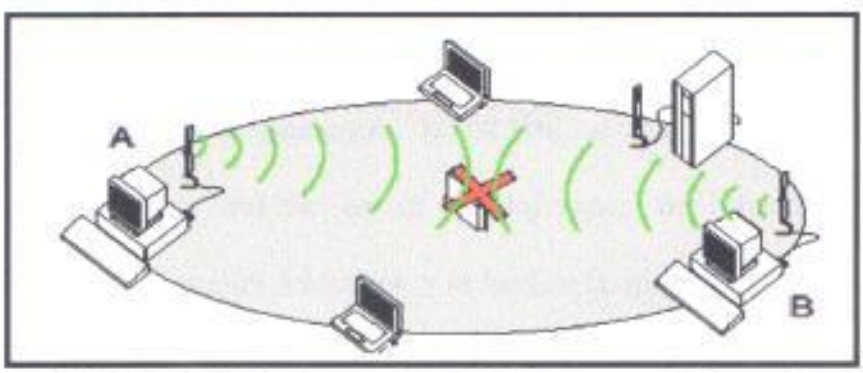


Fig 7.37: Colisión de mensajes debido a una estación oculta

En la figura mostrada, se ilustra un ejemplo del problema de la estación oculta. Ambas estaciones A y estación B están dentro del rango del AP, sin embargo la estación B no puede escuchar a la estación A, por consiguiente la estación A es una estación oculta para la estación B.

Cuando la estación B comienza la comunicación con el AP, ésta no podría recibir la notificación de que la estación A esta usando el medio inalámbrico. Cuando la estación A y la estación B envían mensajes al mismo tiempo, ellos podrían chocar cuando lleguen simultáneamente al AP. La colisión producirá una perdida de mensajes ciertamente para ambas estaciones.

En tales situaciones, el algoritmo **RTS/CTS** puede proveer una solución para prevenir colisiones de mensajes teniendo un control de la transmisión del AP.

Para habilitar el parámetro **RTS/CTS**, se escoge **Add/Edit Configuration Profile** en el administrador del cliente, se selecciona la opción **Advanced** y se habilita la opción **RTS/CTS.**

Cuando se habilita este parámetro en sospecha de una estación oculta, ésta estación y su AP usarán el siguiente método para poder transmitir los datos:

a) La estación enviará un RTS (Request to Send) al AP, que incluirá información acerca de la longitud del paquete que a la estación le gustaría transmitir, (figura 7.38).

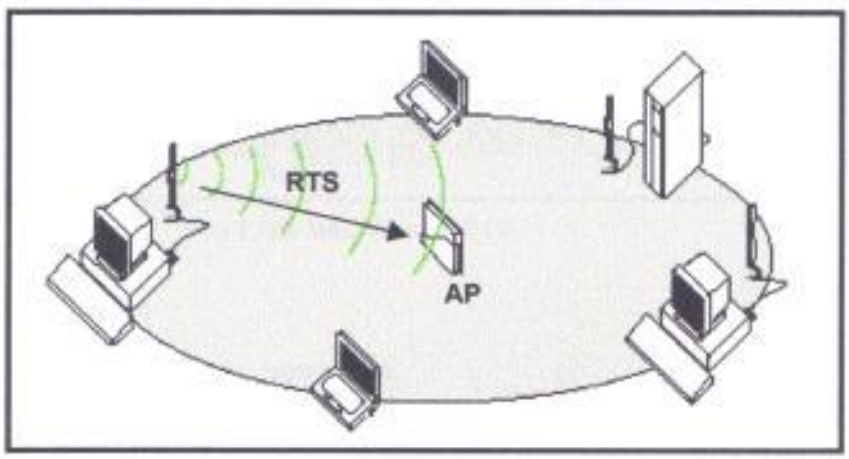


Fig 7.38: Enviando un RTS al AP

b) El punto de acceso responderá con un mensaje CTS (Clear to Send) a todas las estaciones dentro de su rango para:

- Notificar a todas las demás estaciones que difieran las transmisiones por el tiempo requerido, para la transmisión del paquete.
- Confirmar a la estación que desea transmitir, que el AP ha verificado la disponibilidad del medio y lo ha

reservado para el tiempo que dure la transmisión del paquete.

El proceso CTS se muestra en la figura siguiente.

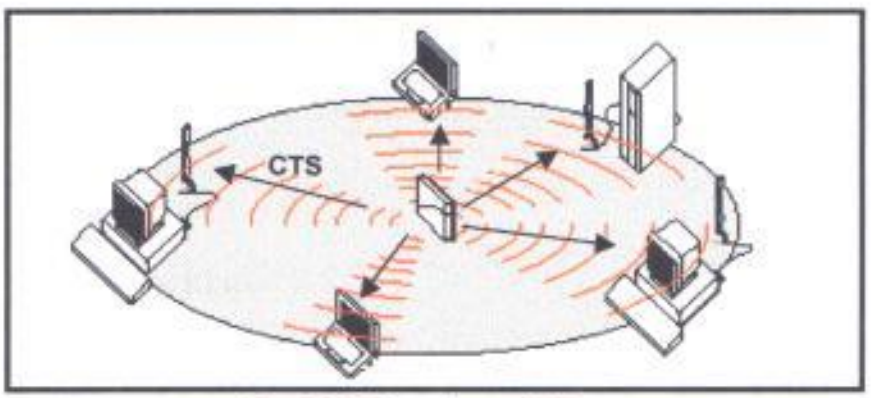


Fig 7.39: Mecanismo CTS

7.2.2.2 Diseño de Redes de alta capacidad.

En esta sección, se menciona de manera general los principios básicos a seguir para diseñar redes donde se tenga una intensa cantidad de usuarios o un gran número de usuarios en una área pequeña. En estas situaciones, el protocolo CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance), puede causar que las estaciones difieran sus transmisiones frecuentemente, lo que afectará directamente en el rendimiento de la red.

Para resolver este problema se debe tomar los siguientes correctivos:

- Agregar más puntos de acceso en la red.

- Configurar cada punto de acceso, para que trabajen en frecuencias de operación diferentes con una máxima separación entre canales.
- Ajustar el parámetro distancia entre AP's, para optimizar el balanceo de carga del número de estaciones por puntos de acceso, (Ver sección Gestión de configuración, configuraciones avanzadas en la página 115).

7.3 Gestión de la Seguridad.

La seguridad que incluye los equipos Orinoco se resumen en:

- Seguridad en el acceso a los datos inalámbricos.
- Encriptación de los Datos inalámbricos.
- Seguridad en la configuración de los puntos de acceso.

7.3.1 Seguridad en el Acceso a los datos inalámbricos.

Para prevenir el acceso no autorizado a los datos que se transmiten sobre la red, los equipos Orinoco cuentan con los siguientes niveles de seguridad:

- Restricción del acceso inalámbrico a la red.
- Encriptación de los datos.

Estas medidas de seguridad, que se aplican a las comunicaciones en la capa fisica, complementan la validación del nombre de usuario y contraseña en la capa de red.

7.3.1.1 Restricción del Acceso Inalámbrico a la Red.

Para excluir a dispositivos de cómputo no autorizados y desconocidos del establecimiento de una conexión inalámbrica a la red, se pueden utilizar las siguientes opciones:

a) Closed Wireless System.- Esta opción cierra la red a todas las estaciones que no han sido configuradas correctamente con el nombre red (network name).

b) Access Control.- Esta opción permite usar tablas de control de acceso, para construir una lista de estaciones autorizadas permitidas y así establecer una conexión inalámbrica a la red.

a) Close Wireless System.

Cerrar la red inalámbrica previene el acceso de usuarios no autorizados a los puntos de acceso. Si un usuario trata de accesar a la red sin configurar su estación con el correcto nombre de red, la estación no será capaz de verse con los AP´s.

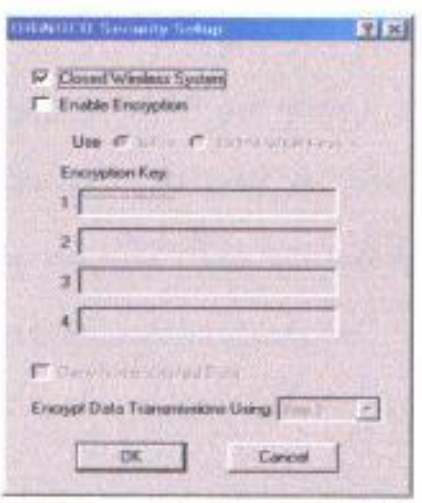


Fig 7.40: Cerrando la red inalámbrica

Hay 2 opciones para este tipo de seguridad de acceso: Abierto y Cerrado.

- Configuración abierta.- Es una de las aplicaciones del estándar IEEE 802.11, modo que permitirá accesar a los AP desde:
  - Todas las estaciones que tengan el correcto nombre de red.
  - Todas las estaciones que tenga como nombre de red **"Any"**.
- Configuración cerrada.- Es el modo propietario que usa Lucent Technologies; que cierra la red para todas las estaciones que no han sido configuradas con el nombre correcto de red. Esta opción denegará el acceso a:
  - Todas las estaciones que tengan configuradas como nombre de red "Any" y
  - Todas las estaciones que no sean Orinoco.

Esta opción de cerrar la red es la que ase aplicó en este proyecto. Para habilitar ésto, se ingresa al AP que desee y se selecciona **Setup / Interface Setup/ Setup 2 / Security**, del Administrador OR (figura 7.40), luego marcar la opción **Close Wireless System**; si esta opción no es marcada la red permanecerá abierta.

b) Access Control.

Otro método para restringir el acceso inalámbrico a los AP's es el uso de las tablas de control de acceso, contenidas en la opción **Setup/Access Control** del Administrador OR (figura 7.41).

Fig 7.41: Control de Acceso por direcciones MAC

Si se decide habilitar la tabla de control de acceso, entonces el AP:

- Solamente permitirá el paso de mensajes, desde/hacia estaciones autorizadas que han sido identificadas en la tabla de control de acceso.
- Ignorará todas las demandas de reenviar los datos desde/hacia estaciones no listadas.

Habilitar el control de acceso es un mecanismo de seguridad más rígido que el de "Cerrar la Red Inalámbrica", ya que requiere que el administrador de la LAN autorize a cada tarjeta PC.

Para autorizar el acceso a la red de las estaciones inalámbricas el administrador de la LAN debe:

- Agregar la dirección MAC de cada tarjeta PC, correspondiente a cada estación en el archivo de la tabla de control de acceso. Y
- Descargar el archivo de la tabla de control de acceso para todos los AP´s en la red.

Nota: En este proyecto esta opción no es habilitada

7.3.2 Encriptación de los Datos Inalámbricos.

Para proveer un nivel más alto de seguridad para la transmisión de los datos, se puede usar la encriptación de datos WEP (Wired Equivalent Privacy).

Se pueden especificar hasta 4 diferentes llaves para desencriptar los datos inalámbricos, y seleccionar una de las llaves para encriptarlos. La opción de usar las cuatro diferentes llaves para desencriptar los datos inalámbricos, permite cambiar sus llaves WEP en intervalos regulares sin afectar el desempeño de la red.

La encriptación de datos WEP (Wired Equivalent Privacy), permite encriptar todos los datos que serán transmitidos por el medio LAN inalámbrico.

Para habilitar la encriptación en el AP, se selecciona la opción **Setup / Setup Interface / Setup 2/ Security** del Administrador OR (figura 7.42).

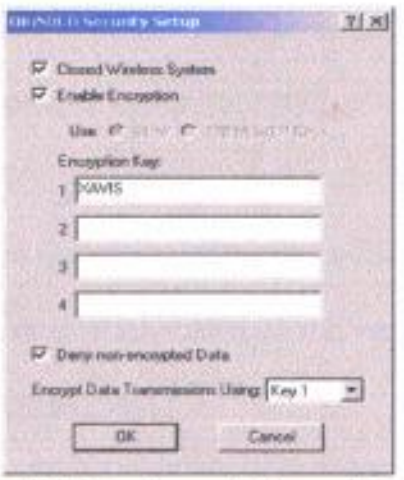


Fig 7.42: Configurando la encriptación

Luego seguir los siguientes pasos:

- Seleccione la opción **Enable Encryption**
- Ingrese 4 diferentes llaves para desencriptar los datos recibidos via la interface inalámbrica.
- Seleccione una de estas claves, para encriptar los datos inalámbricos que están siendo transmitidos via la interface inalámbrica.

Nota: Para este proyecto se ha trabajado con una sola llave de encriptación, ésta misma configuración de encriptación debe ser también cargada en las estaciones.

Para la tarjeta Orinoco Silver los valores validos (llaves para encriptar) son:

- 5 dígitos de valor alfanuméricos en el rango de "a-z" y "0-9" (para este diseño se uso como llave de encriptación la palabra **XAVIS**).
- 10 dígitos de valor hexadecimal, precedido por los caracteres "0x" (zero x), por ejemplo: 0xABCD1234FE

Para la tarjeta Orinoco Gold los valores validos (llaves para encriptar) son:

- 13 dígitos de valor alfanuméricos en el rango de "a-z" y "0-9", por ejemplo: SECURE1234567.
- 26 dígitos de valor hexadecimal, precedidos por los caracteres "0x" (zero x), por ejemplo: 0xABCD1234FE.
- Opcionalmente se pueden también usar los valores de la tarjeta Silver.

Las cadenas hexadecimales que no estén precedidas de "0x" serán interpretadas como una cadena alfanumérica.

Como se muestra en la figura 7.42, existe otra opción **Deny non-Encrypted data**, que siempre deberia estar habilitada, ya que permite que el AP sólo procese mensajes recibidos en la interface inalámbrica cuando éstos han sido encriptados con una de las 4 llaves de identificación. Esto brinda una óptima seguridad contra accesos no autorizados en la red.

Si la opción **Deny non-Encrypted data** no es habilitada, entonces el punto de acceso procesará todos los mensajes recibidos en la interface inalámbrica, indiferentemente si el mensaje ha sido encriptado con una de las llaves de identificación o no.

7.3.3 Seguridad en la Configuración de los Puntos de Acceso.

Medidas de seguridad, como el control de acceso, llegan hacer inefectivas cuando personas no autorizadas pueden ver y modificar la configuración de los puntos de acceso.

Para proteger la configuración de red de modificaciones indeseadas, se recomiendan implementar las siguientes medidas:

- Contraseñas de lectura y lectura/escritura.
- Lista de accesos de direcciones IP SNMP.
- Mecanismo de Alerta de mensajes traps a la estación (opcional).

7.3.3.1 Contraseñas de Lectura y Lectura / Escritura.

Para restringir el acceso a la información de configuración del AP, se pueden crear 2 niveles de autorización de contraseñas:

a) Contraseña de lectura.

b) Contraseña de lectura / escritura.

a) Contraseña de Lectura.

La contraseña de lectura, sólo proveerá acceso a los AP's para monitorear la información de diagnóstico, encontrada en la opción de Monitoreo en la ventana principal del Administrador OR.

Para definir una contraseña de lectura:

1. Se selecciona la opción **Setup / Parámetros SNMP** (figura 7.43).
2. En el campo contraseña de lectura se ingresa la contraseña. El valor por defecto es public (en este diseño se ha cambiado esta contraseña por una personalizada).

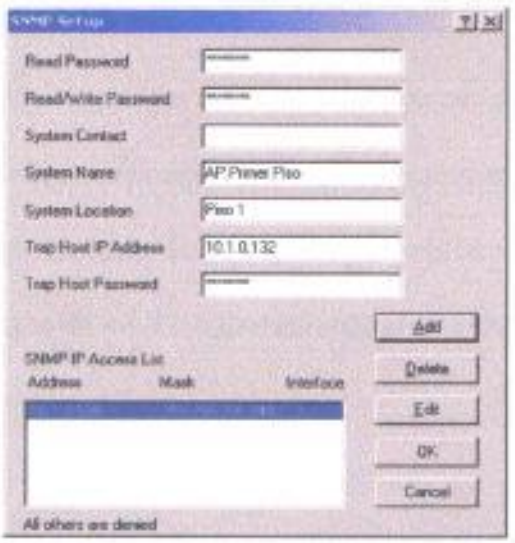


Fig 7.43: Configurando la Seguridad SNMP

b) Contraseña de lectura/ escritura.

La contraseña de lectura / escritura, proveerá de un acceso total para visualizar la información de diagnostico del AP, es decir no solo permitirá monitorear la red, si no también configurar el punto de acceso. Si se ingresa una contraseña errónea resultará un **error fuera de tiempo**, o "**error SNMP**"

Para definir una contraseña de lectura/escritura, se siguen los mismos pasos descritos en el parámetro contraseña de lectura, y se escribe en el campo **read-write password** la contraseña deseada (de igual forma esta contraseña de acceso total ha sido personalizada).

7.3.3.2 Lista de Acceso IP SNMP.

Se puede usar las listas de acceso SNMP para crear un nivel extra de seguridad en adición a las contraseñas de lectura y lectura /escritura. Esto permitirá a un número limitado de estaciones de gestión visualizar y/o modificar los parámetros de los AP´s, basándose en las direcciones IP de estas estaciones.

En el campo de listas de acceso, típicamente deberían incluir todas las direcciones IP de las estaciones de gestión que usarán el administrador OR para configurar y/o monitorear los puntos de acceso.

Para autorizar las estaciones de gestión se debe ingresar:

- La dirección IP de la estación y,
- La interface de red del AP a través de la cual se ingresará al mismo.

  Para indicar la inteface se usa:

  - "1" para la ethernet
  - "2" para la inteface de red inalámbrica A.
  - "3" para la interface de red inalámbrica B.

  Alternativamente se puede usar el valor "X", para permitir el acceso al AP por cualquiera de las interfaces disponibles.

Para permitir que múltiples estaciones de gestión accedan a la configuración y/o monitoreo de los AP´s, se puede asignar también un rango de direcciones IP. Para ésto, se ingresa la máscara de subred que indicarán las estaciones autorizadas para modificar los parámetros.

Cuando la dirección IP o interfaces no concuerde con el listado, en la lista de acceso SNMP IP el solicitante recibirá un error fuera de tiempo.
Para autorizar a una estación administradora, vía lista de acceso SNMP IP, se selecciona la opción **Setup / Parámetros SNMP**, (figura 7.43).

Usar los siguientes botones para modificar la lista de acceso SNMP IP:

- Agregar: Para añadir una dirección IP a la lista
- Borrar: Para quitar la dirección IP de la lista.
- Edit: para cambiar entradas en la lista.

El valor por defecto es <Todos serán permitidos>.

En el caso de este diseño solo se usará una estación de gestión, por tanto se ingresará la dirección IP 10.1.0.132 correspondiente a esta estación con máscara 255.255.255.248, así como muestra la figura 7.43.

7.3.3.3 Mecanismo de Alertas de mensajes Trap hacia la estación.

Se puede usar el mecanismo de traps a la estación de gestión, para informar al administrador de la red cuando alguien resetea el AP, o si hay una autentificación fallida, o cuando un enlace se levanta o se cae; es decir cuando ocurren eventos.

La alerta de traps a la estación, permite al administrador de red verificar si estos eventos fueron originados por usuarios autorizados o no.

Para activar el mecanismo de traps a la estación:

1. Se selecciona la opción **Setup / Parametros SNMP** (figura 7.43).
2. En el campo **Trap Host IP Address**, se ingresa:

- La dirección IP de la estación de gestión, a esta dirección se enviarán los mensajes, por ejemplo si el AP es reseteado.
- (Valor inicial, 0.0.0.0) – Para deshabilitar el agente Trap SNMP.

3. Se ingresa una contraseña en el campo **Trap Host Password**. Se escoge una contraseña que corresponda a la contraseña ingresada en la estación Trap, para filtrar mensajes no solicitados o no autorizados en esta estación.

   La contraseña será incluida en el mensaje trap SNMP enviados por este AP. Si la estación Trap recibe un mensaje sin contraseña o con una contraseña desconocida, el mensaje trap será ignorado.

   - Valores validos: Cualquier valor alfanumérico en el rango de a-z, 0-9 con un mínimo de 2 y un máximo de 31 caracteres.
   - Valor inicial: **public**.

CONCLUSIONES Y RECOMENDACIONES

La WLAN diseñada, permitirá a los usuarios de la red movilidad y acceso a los recursos compartidos al mismo tiempo. Según la topología utilizada en el diseño, se podrá reconfigurar la misma sin que esto implique costos adicionales.

Los equipos utilizados para el diseño de la red son de la marca Lucent Technologies con su línea Orinoco, marca reconocida mundialmente y en nuestro medio comercialmente es la más vendida y utilizada para aplicaciones WLAN. Estos equipos trabajan bajo el estándar IEEE 802.11b, que define la tecnología de espectro ensanchando por secuencia directa permitiendo llegar a velocidades de 11Mbps. Todo lo mencionado garantiza la calidad de servicio de la red, además de la compatibilidad de interactuar con equipos de otras marcas.

El software de gestión utilizado es propietario de Orinoco y consta básicamente de 2 herramientas llamadas: OR Manager y Client Manager. Este software trabaja bajo el protocolo de gestión de redes SNMP, que es el protocolo comúnmente utilizado para redes TCP/IP. La ventaja de este protocolo es que es estable, simple y flexible. Para el administrador de la red, SNMP se mantiene oculto, ya que el software Orinoco presenta una interface gráfica con opciones de gestión muy amigables y fáciles de manejar.

En el diseño de la WLAN, se decidió trabajar con 2 antenas extensoras de rango adicionales a las incorporadas en las tarjetas de red, ya que de esta manera se aumenta el alcance de los puntos de acceso y así las estaciones podrán movilizarse dentro de todo el edificio, asegurando una conexión permanente a la red. Todo esto se ve reflejado en el rendimiento de la WLAN.

El Software de administración Orinoco permite configurar los puntos de acceso y estaciones de trabajo de una manera muy sencilla y rápida, brindado así al administrador de la red una herramienta de trabajo ágil y simple de usar.

El software **Administrador OR** en su opción de Monitoreo, muestra parámetros muy importantes que permiten determinar el estado actual de la red, es decir estos valores indicarán si el desempeño de la red es bueno o no, y de esta manera el administrador de la WLAN podrá tomar correctivos para así obtener una mejora en el rendimiento de la misma. Además, tanto en el **Administrador OR** como en el **Administrador del Cliente** se puede probar la calidad de la conexión, la velocidad máxima alcanzable es de 11Mbps, si la conexión no es muy buena pasará a los 5Mbps, luego a los 2Mbps y finalmente a 1 Mbps.

La seguridad diseñada para la WLAN, de seguro que no es inviolable pero desde luego que debe costar bastante a algún intruso, la red cuenta con algunos mecanismos de seguridad tales como network name, encriptación, contraseñas,

logrando de esta manera restringir el acceso a la WLAN, así como también proteger los datos transmitidos sobre la misma.

En cuanto a **recomendaciones**, se puede mencionar lo siguiente:

La toma de corriente del AP debe estar ubicada de tal manera que el punto de acceso pueda ser desconectado fácilmente, ya que puede darse el caso de que el AP se inhiba debido a excesivo tráfico en la red, por lo tanto se requerirá el reseteo físico del equipo; es decir desconectarlo y volverlo a conectar.

La instalación de las antenas extensoras de rango es algo muy importante, ya que de su buena colocación dependerá el éxito de la WLAN, por lo tanto tomar en cuenta este punto en el momento de su instalación (tratar de ubicar siempre la antena en un lugar alto y libre de obstáculos).

Revisar en períodos regulares el comportamiento de la red, puesto que éste puede cambiar debido a múltiples factores tales como: la reubicación de estaciones, cambios en la infraestructura física del edificio (construcción de nuevas paredes u oficinas), o instalación de otros equipos inalámbricos que pueden interferir con la WLAN.

En casos de que la red presente un tráfico elevado (congestión), lo cual desmejora el desempeño de la WLAN, se puede considerar insertar otra tarjeta PC en el AP; para de esta manera balancear la carga en el AP.

BIBLIOGRAFÍA

- Tutorial de Gestión de Redes y Servicios de Telecomunicaciones por el Ing. Edgar Leyton Q.
- Documentation & Software for Wireless Enterprise & Home Networks, Orinoco.
- http://www.orinocowireless.com
- Wireless Lan Alliance , http://www.wlana.com
- IEEE 802.11, Wireless LANMA Cand Physical Layer Especification. Editors of IEEE, junio 1997.
- http://www.class.udg.mx/~xotchilt/SNMP.html