ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

ANÁLISIS Y OPTIMIZACIÓN DE LA INFRAESTRUCTURA DE UN PROVEEDOR DE SERVICIOS DE INTERNET INALÁMBRICO, QUE UTILIZA LA TECNOLOGÍA WLAN PARA CLIENTES CORPORATIVOS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

HENRY NELSON ROA MARÍN

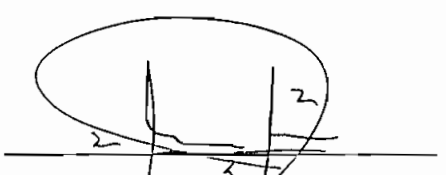
DIRECTOR: MSc. TANIA PÉREZ

Quito, Octubre del 2005

DECLARACIÓN

Yo Henry Nelson Roa Marín, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.



Henry Nelson Roa Marín

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Henry Nelson Roa Marín bajo mi supervisión.

MSc. Tania Pérez
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Deseo expresar mi agradecimiento a todas las personas que me han brindado su ayuda, sus conocimientos y su apoyo incondicional para que este proyecto saliera adelante de la mejor manera. Quiero también hacer extensivo mi agradecimiento a mis compañeros de trabajo quienes de una u otra forma me ayudaron y motivaron día a día para que el presente proyecto culmine.

De manera especial quiero agradecer a mi directora del proyecto de titulación, la MSc. Tania Pérez por toda la confianza depositada desde el inicio de este proyecto, por los consejos constantes y por la dedicación absoluta, tanto personal como profesional, para terminar el proyecto exitosamente.

DEDICATORIA

Este proyecto está dedicado a todas las personas que más quiero en mi vida, a mis hermanos, a Dios y especialmente a mi Madre, quien con su esfuerzo y trabajo me ha dado la oportunidad de llegar a ser lo que soy, apoyando mis objetivos y proyectos de manera incondicional, y sobre todo por todo el amor, cariño y comprensión que me ha brindado.

CONTENIDO

RESUMEN

En el presente proyecto se realiza el análisis y optimización de la infraestructura de un proveedor de servicios de Internet inalámbrico de la ciudad de Quito, que utiliza la tecnología WLAN según el estándar 802.11b para dar acceso a clientes corporativos.

En el capítulo I se hace una revisión de la red de redes Internet y una descripción de los proveedores de servicios de Internet analizando su definición, servicios que presta, clasificación, arquitectura y características principales de éstos. También se describe cada uno de los componentes básicos de un ISP y las funciones que desempeña el mismo.

En el capítulo II se hace un estudio de las redes WLAN, abarcando inicialmente la definición de lo que son este tipo de redes. Se revisa las aplicaciones actuales que tienen las redes WLAN en diferentes áreas. Se hace referencia a los requisitos que debe tener una WLAN. Se analizan las ventajas y desventajas de las redes WLAN sobre las redes fijas. También se revisan las tecnologías de transmisión que utilizan las redes WLAN como son los infrarrojos y espectro expandido. Luego se hace una descripción puntual de las organizaciones actuales que manejan las redes WLAN, y las tecnologías y estándares más importantes en este tipo de redes. Finalmente se hace una revisión del estándar IEEE 802.11b.

En el capítulo III se hace un estudio de la seguridad en redes WLAN, para lo cual se realiza una introducción de lo que significa el término seguridad dentro de las redes. Se revisan los riesgos actuales a los que están sometidas las redes WLAN. Se describen los métodos más utilizados por los *hackers* para detectar la presencia de una red WLAN. Luego, se realiza una clasificación de los ataques que se pueden perpetrar y se describen los ataques más comunes que una red WLAN puede sufrir hoy en día, como son el *eavesdropping, wep cracking*, ataques MAC, entre otros. Finalmente, se describen una serie de mecanismos y estándares actuales que se utilizan para asegurar una red WLAN como es el caso

del algoritmo WEP, el uso de filtros, uso de VPNs, WPA, WPA2 entre otros.

En el capítulo IV se realiza un análisis de la situación actual de un Proveedor de Servicios de Internet, para lo cual se hace una introducción a los diferentes tipos de dispositivos WLAN y las antenas que estos dispositivos utilizan. Se describe en forma global la topología del ISP y en forma detallada cada uno de sus componentes así como las funciones que tienen dentro del ISP. Igualmente se hace una descripción de la infraestructura del *backbone* analizando los dispositivos de cada uno de los nodos, los enlaces principales y los enlaces de última milla. Finalmente se describen las políticas de seguridad que el ISP maneja actualmente en lo que concierne al uso de la tecnología WLAN según la especificación 802.11b en los enlaces inalámbricos de última milla y enlaces principales.

En el capítulo V se describen las ventajas y desventajas que tiene el uso de las redes WLAN como enlaces de última milla y de *backbone* dentro del ISP. Se realiza un análisis de los principales problemas tanto actuales como a futuro debido al uso de este tipo de redes como son la falla en los enlaces de *backbone*, saturación de la red a causa del *broadcast* y la imposibilidad para limitar la velocidad de transmisión a nuevos clientes. Luego se analizan los cambios óptimos que se deben realizar a la infraestructura del ISP para solventar los problemas encontrados, describiendo en que consiste cada uno de estos cambios y cual es la mejor forma de implementarlos para reducir complicaciones operativas y económicas. Finalmente se analizan las políticas que se pueden y deben tomarse para garantizar la seguridad en las redes WLAN utilizadas para entregar accesos de última milla.

PRESENTACIÓN

Actualmente las redes WLAN están siendo utilizadas en muchas aplicaciones, que salen del fin mismo para las que fueron establecidas, sin embargo este tipo de aplicaciones han permitido solucionar muchos problemas de acceso, costos y rapidez en la implementación de la solución.

El análisis que se realiza en el presente proyecto a un proveedor de servicios de Internet de la ciudad de Quito, permitirá abrir los horizontes actuales en lo referente a redes de acceso, ya que el manejo de la tecnología WLAN ha permitido dar el servicio de Internet a sitios donde el acceso mediante redes cableadas es casi imposible, a costos y rapidez de instalación muy por debajo de lo que implica dar un servicio mediante la contratación de los servicios de una empresa portadora.

Ñ

La solución mediante redes WLAN en los accesos de última milla dentro del ISP, es muy beneficiosa pero lamentablemente esta solución está presentando problemas con el progresivo crecimiento del número de clientes del ISP, de ahí la necesidad de optimizar el mismo y permitir que éste siga utilizando la tecnología WLAN para dar servicio a futuros clientes. De esta forma se evitará la necesidad de utilizar otros tipos de accesos de última milla, los cuales pueden incrementar los costos de operación del proveedor de servicios de Internet y por ende los costos del servicio a sus clientes finales.

La solución dada en el desarrollo del presente proyecto está basada principalmente en cambios y nuevas adiciones a la infraestructura actual del proveedor. De esta forma se permitirá que este proveedor pueda solucionar los problemas actuales y seguir entregando el servicio a nuevos clientes mediante redes WLAN, sin que esto repercuta de ninguna manera en los clientes actuales.

CAPÍTULO I

1 ESTRUCTURA Y COMPONENTES BÁSICOS DE UN PROVEEDOR DE SERVICIOS DE INTERNET LOCAL

1.1 EL INTERNET

El Internet es un recurso muy valioso hoy en día, es por esto que la conexión al mismo es esencial tanto para los negocios, la industria y la educación. Se puede decir que es la red de datos más grande del mundo y está constituida por un conjunto de redes independientes (Redes LAN y WAN), que se encuentran interconectadas entre sí mediante dispositivos de interconexión (puentes, conmutadores o ruteadores), permitiendo el intercambio de datos y constituyendo por lo tanto una red mundial que resulta el medio idóneo para la distribución de datos de todo tipo e interacción con otras personas.

1.1.1 RESEÑA HISTÓRICA DEL INTERNET [1], [2]

El Internet nació como un proyecto del Departamento de Defensa Estadounidense que pretendía obtener una red de comunicaciones segura que se pudiese mantener aunque fallase alguno de sus nodos. Así nació ARPA, una red informática que conectaba computadores localizados en sitios dispersos y que operaban sobre distintos sistemas operativos, de tal manera que cada computador se podía conectar a todos los demás. Los protocolos que permitían tal interconexión fueron desarrollados en 1973 por el informático estadounidense Vinton Cerf y el ingeniero estadounidense Robert Kahn, y son los conocidos Protocolo de Internet (IP) y Protocolo de Control de Transmisión (TCP). Fuera ya del ámbito estrictamente militar, esta Internet incipiente (llamada Arpanet) tuvo un gran desarrollo en Estados Unidos, conectando gran cantidad de universidades y centros de investigación. A la red se unieron nodos de Europa y del resto del mundo, formando lo que se conoce como la gran telaraña mundial (*World Wide*

Web). En el año de 1990 Arpanet dejó de existir.

Además de la utilización académica e institucional que tuvo en sus orígenes, hoy se emplea Internet con fines comerciales. Las distintas empresas no sólo la utilizan como escaparate en el que se dan a conocer ellas mismas y sus productos, sino que, a través de Internet, se realizan ya múltiples operaciones comerciales.

1.1.2 FUNCIONAMIENTO DE INTERNET

El Internet es una red global en la cual, cada computador actúa como un cliente y un servidor; un cliente cuando accede a un servicio del Internet y un servidor cuando es accedido por otro computador desde el Internet. El Internet consta de varios componentes interconectados entre sí:

- ✓ *Backbones*: Son líneas de comunicación de alta velocidad y ancho de banda que unen computadores o redes.
- ✓ Redes: Son grupos de computadores y dispositivos asociados que permiten a los usuarios transferencia electrónica de información.
- ✓ Proveedores del Servicio de Internet (ISPs): Son empresas que tienen acceso al Internet.
- ✓ Computadores: Son los dispositivos cliente/servidor; no sólo pueden ser computadores personales, computadores portátiles sino también PDAs, teléfonos celulares, etc.

La manera en que Internet permite a los computadores conectarse es similar a como trabaja una red de área local (LAN). En una red simple, se tienen dos computadores y una conexión de datos. Los computadores se comunican entre sí enviando un paquete a través de la conexión. Un paquete es una unidad de datos que viaja entre computadores de una red específica, cuyo encabezado tiene información de las direcciones lógicas tanto de origen como de destino de dichos computadores.

Los dos protocolos de Internet conocidos como TCP/IP que trabajan en conjunto para la transmisión de datos son:

Transmission Control Protocol (TCP)
Internet Protocol (IP)

Los computadores también pueden comunicarse con otros fuera de la LAN. Al conjunto de LANs se conoce como redes de área amplia (WAN). Los ruteadores proveen las conexiones entre diferentes LANs. Cuando un ruteador recibe un paquete, el ruteador utiliza la información de la dirección lógica para determinar la localización del destinatario de los datos, luego el ruteador encapsula el paquete en un formato adecuado para enviarlo hacia la siguiente conexión. Los datos pueden cruzar varias LANs antes de llegar a su destino.

La Internet es considerada una red de área amplia, independiente de la topología. Esta independencia de las diversas topologías de LAN la realiza el protocolo estándar IP. El encabezado del paquete IP (IPv4) contiene una dirección de cuatro octetos que identifican a cada uno de los equipos. Cuando un computador envía un paquete hacia otro computador, primeramente determina si el paquete es local o remoto (dentro o fuera de la LAN). Si el paquete es local, él mismo lo transmite; si es remoto lo envía hacia un ruteador, el cual determina la dirección destino. La información de la dirección destino también determina cómo será enrutado el paquete a través de Internet. Normalmente el ruteador utiliza la dirección destino para determinar la mejor ruta para enviar el paquete.

Si alguna red intermedia llegara a estar demasiado ocupada o no disponible, el ruteador dinámicamente selecciona una ruta alterna. Una vez que el paquete es enviado, cada red que reciba el paquete, repite el proceso redirigiéndolo cuando sea necesario. Este proceso se repite hasta que el paquete llega a su destino. Diferentes paquetes pueden tomar diferentes rutas, aún cuando contengan información del mismo archivo o mensaje. Los paquetes son reensamblados en el destinatario.

1.2 DEFINICIÓN DE ISP [1], [3], [4]

Un Proveedor de Servicios de Internet (*Internet Service Provider*), es una empresa que permite el acceso de otras empresas o personas al Internet, ofreciendo servicios de Internet y conectividad. Dentro de los servicios que entrega figuran el correo electrónico (*e-mail*), construcción y hospedaje de sitios Web así como su mantenimiento (*Web Hosting*), servicios de resolución de nombres (DNS), servicios de noticias USENET, servicios de transferencia de archivos (FTP) entre otros.

El centro de un ISP está conformado por servidores que se encargan de las funciones necesarias para proveer el servicio a sus clientes. Los servidores son los dispositivos más importantes de Internet, pues son los que contienen la información con la que cuenta la red. Estos equipos normalmente están disponibles las 24 horas del día durante los 365 días del año.

Los ISPs generalmente proveen acceso *dial-up* a través de un módem y conexión *Point to Point Protocol* (PPP), pero pueden ofrecer también acceso a Internet con otros dispositivos, tales como cable módems o conexiones inalámbricas.

El mercado de los ISPs está evolucionando muy rápidamente. La definición de ISP no es tan clara como suele parecer; por ejemplo: nuevos métodos de acceso han sido implementados (DSL; *Digital Subscriber Line*) y nuevos tipos de dispositivos (teléfonos celulares) tienen acceso a Internet. Continuamente se puede apreciar un cambio en el número de servicios básicos que son la razón misma del comercio ISP. Esto se debe a la feroz competencia, nuevas tecnologías y mejor acceso a mayor ancho de banda. Incluso, se puede apreciar que el ambiente comercial está cambiando con la liberalización de las compañías de Telecomunicaciones (TELCO).

1.2.1 FUNCIONES BÁSICAS DE UN ISP [5]

Un ISP tiene la infraestructura necesaria para constituirse un punto de acceso

hacia Internet y así poder prestar sus servicios. Los grandes ISPs poseen enlaces de comunicaciones propios, lo que les permite ser más independientes de otros proveedores de telecomunicaciones, permitiéndoles de esta manera brindar mejores servicios a sus clientes.

Las funciones básicas de un ISP se pueden dar desde dos puntos de vista distintos:

1.2.2 VISIÓN DEL CLIENTE

Desde el punto de vista del cliente, un ISP tiene dos funciones básicas:

1. Conectividad al Internet: El ISP es la puerta a la gran nube de Internet, permitiéndole así utilizar todos los servicios que esta red de redes ofrece.
2. Servicios de Internet: Luego de establecida la conexión con el ISP, éste debe garantizar a sus clientes los servicios que van a ser utilizados por los mismos, se hace un especial hincapié en dos servicios que son masivamente empleados por los usuarios, estos son correo electrónico y WWW. Un tercer servicio de uso masivo es el de transferencia de archivos.

Estas funciones desde el punto de vista del cliente, se las puede apreciar en la figura 1.1.

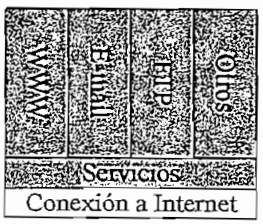


Figura 1.1. Visión del Cliente

1.2.3 VISIÓN DEL PROVEEDOR

El punto de vista del proveedor es mucho más complejo, ya que es éste el

encargado de brindar la conectividad a sus clientes. Cabe recalcar, que un ISP pequeño puede ser cliente de otro ISP mayor, delegando parte del problema de la conexión a Internet en el ISP mayor, tal es el caso del ISP que se analiza en el capítulo IV.

La función de un ISP es la de permitir la interconexión de los computadores de los usuarios a través de él, hacia el Internet. Esto es posible gracias a que el ISP, posee los permisos necesarios para interactuar con otros elementos de la red, tales como módems, ruteadores o *switches*, que son los dispositivos que permiten el acceso a los clientes.

De acuerdo a lo anterior, un ISP debe cumplir con las siguientes funciones:

- ✓ Conservar una alta disponibilidad de conectividad con el Internet y sus clientes
- ✓ Mantener una alta disponibilidad en la prestación de los servicios básicos del ISP
- ✓ Mantener una adecuada calidad de servicio

Para cumplir con lo anterior un ISP básico necesita contar con los elementos siguientes:

- ✓ Canal de acceso Cliente – ISP
- ✓ Canal de acceso ISP – Internet
- ✓ Servicios básicos (resolución de nombres)
- ✓ Mecanismos de seguridad

1.3 SERVICIOS DE UN ISP [1], [3], [4]

Los servicios que presta un ISP no son los mismos para un consumidor corporativo y un consumidor residencial. Los requerimientos para consumidores corporativos son muchos mas dificultosos de reunir en términos de desempeño, disponibilidad y lo más importante seguridad. Las diferencias se ilustran en la

figura 1.2.

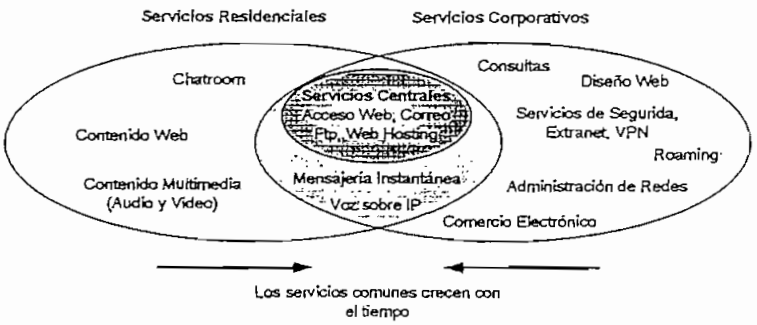


Figura 1.2. Servicios Centrales y de Valor Agregado

Con el tiempo se produce un cambio de asignación de estos servicios, los servicios comunes y servicios centrales tienden a crecer con éste. Los requerimientos de los usuarios corporativos están liderando la escalada en la tecnología. Después de algún tiempo, esta tecnología puede encontrarse adelante en el mercado del consumidor residencial. Este avance inevitablemente beneficiará a los consumidores residenciales con nuevos servicios innovadores y calidad de servicio a su disposición.

Los servicios centrales más importantes que un ISP debe ofrecer como correo electrónico, Servicio Web, FTP, DNS, etc. se describen a continuación:

1.3.1 SERVICIO DE CORREO ELECTRÓNICO

El correo electrónico es uno de los servicios de mayor uso a través de Internet. Permite enviar mensajes de un usuario a otro en la red, con la posibilidad de adjuntar archivos, lo que aumenta enormemente sus potencialidades.

El sistema de correo electrónico se basa en los protocolos SMTP (*Simple Mail Transfer Protocol;* Protocolo Simple de Transferencia de Correo) y POP3 (*Post Office Protocol* version 3) o IMAP4 (*Internet Message Access Protocol version 4;* Protocolo de Acceso de Mensajes de Internet). De estos tres protocolos el primero se encarga del envío y recepción del correo y los otros dos permiten a los

usuarios el acceso a los buzones de correo.

Los mensajes de correo electrónico no se envían directamente a los computadores personales de cada usuario, pues puede ocurrir que esté apagado o que no esté ejecutando la aplicación de correo electrónico sino que se envían al servidor que se encarga de almacenar los mensajes recibidos, el cual actúa como servidor de correo electrónico permanente. Los mensajes permanecerán en el servidor hasta que el usuario los transfiera a su propio computador para leerlos.

1.3.2 SERVICIO WEB

El Servicio WWW (*World Wide Web*), es un mecanismo proveedor de información electrónica para usuarios conectados a Internet. El acceso a cada sitio Web se canaliza a través del URL o identificador único de cada página de contenidos.

Este sistema permite a los usuarios el acceso a una gran cantidad de información: leer publicaciones periódicas, buscar referencias en bibliotecas, realizar paseos virtuales por pinacotecas, compras electrónicas o audiciones de conciertos, buscar trabajo y otras muchas funciones. Gracias a la forma en que está organizada la *World Wide Web* (WWW), los usuarios pueden saltar de un recurso a otro con facilidad. Las conexiones entre los servidores que contienen la información se hacen de forma automática y transparente para el usuario, pues el medio admite las funciones de hipertexto e hipermedia.

Los usuarios visualizan estos datos mediante una aplicación, denominada explorador o *browser* (como *Navigator*, de Netscape, o *Internet Explorer*, de Microsoft). El explorador muestra en la pantalla una página con el texto, las imágenes, los sonidos y las animaciones relativas al tema que previamente ha sido seleccionado. El usuario puede entonces interactuar con el sistema señalando con el *mouse* (ratón) aquellos elementos que desea estudiar en profundidad, pues, si la página lo permite, dichos objetos estarán vinculados a otras páginas Web de ese servidor u otros que aportan información relacionada. Cada vez más compañías implantan redes corporativas, conocidas con el nombre

de intranets, que están basadas en esta tecnología pero a menor escala.

Las páginas Web están escritas en HTML (*Hypertext Markup Language*), DHTML o XML (*Extended Markup Language*), lenguajes de marcado de hipertexto. El protocolo HTTP (*Hypertext Transfer Protocol*) es el encargado de hacer llegar las diferentes páginas desde los servidores remotos al equipo del usuario que las solicita.

La *World Wide Web* fue desarrollada en 1989 por un científico inglés, Timothy Berners-Lee. El propósito original del sistema era permitir que los equipos de investigadores de física de alta energía del CERN de Ginebra, Suiza, pudieran intercambiar información. Con el paso del tiempo la WWW se convirtió en una plataforma de desarrollo de programas relacionados con este entomo. El número de equipos conectados creció rápidamente, sirviendo de soporte a muchos proyectos, como por ejemplo un mercado a gran escala. El MIT (Instituto de Tecnología de Massachusetts), a través del consorcio WWW, intenta coordinar el desarrollo futuro de este sistema, aunque el éxito de los últimos años hace difícil planificar la expansión del mismo.

1.3.3 SERVICIO FTP

El Servicio FTP (*File Transfer Protocol*; Protocolo de Transferencia de Archivos) es un servicio que se utiliza en Internet y otras redes para transmitir archivos entre servidores o entre un usuario y un servidor. El protocolo asegura que el archivo se transmite sin errores, para lo que dispone de un sistema de corrección de errores basado en un control de redundancia de datos y en su caso, de la capacidad de retomar la descarga en el punto en que falló la conexión o el envío o la recepción de datos.

El sistema que almacena archivos que se pueden solicitar por FTP se denomina servidor de FTP. El servicio FTP forma parte del conjunto de protocolos TCP/IP, que permite la comunicación en Internet entre distintos tipos de computadores y redes.

Los programas que son capaces de acceder a servidores FTP y descargar archivos de ellos y, en su caso, enviar otros al servidor, se denominan clientes FTP. Habitualmente precisan de claves de acceso (usuario y contraseña); los denominados servidores de FTP anónimo (*Anonymous FTP Server*) permiten el acceso libre, sin más que indicar datos como la dirección de correo electrónico del usuario que accede a ello como contraseña. Lo más común es que los servidores anónimos sólo permitan descargar archivos del servidor FTP, pero no enviar otros nuevos.

1.3.4 SERVICIO DE NOTICIAS USENET

El servicio de noticias *Usenet News* es el servicio más apropiado para intercambiar artículos a nivel mundial acerca de un determinado tema y de esta manera entablar foros de discusión. Consiste de un grupo de noticias (*news groups*), que son clasificados dentro de jerarquías de similar interés en su contenido, y a su vez estas se dividen en sub-jerarquías.

Existen cerca de 500 jerarquías oficiales, pero las 8 más grandes son: *Usenet Computer, Usenet discussions about humanities, Usenet miscellaneous, Usenet news, Usenet recreational, Usenet science, Usenet social issues y Usenet talk newsgroups.*

Un usuario de este servicio debe suscribirse a uno o varios de estos grupos de noticias para poder participar en los foros de discusión. Los *browsers como Netscape Navigator* o *Internet Explorer* proveen soporte para *Usenet* y pueden acceder a cualquier grupo de noticias que se escoja. Los artículos o mensajes que se envían a los grupos de noticias se hacen públicos y cualquier persona puede leerlos y enviar una contestación. En algunos casos estos foros de discusión tienen un moderador que filtra, edita y envía los mensajes.

Cada servidor de noticias, mantiene una copia del grupo de noticias y envía una copia de cada uno a los servidores de noticias vecinos, de ésta manera se propagan las noticias. NNTP (*Network News Transfer Protocol;* Protocolo de

Transferencia de Noticias de Red), es el encargado de enviar, distribuir y recuperar mensajes de un servidor de noticias *Usenet*.

1.3.5 SERVICIO TELNET

Este servicio está basado en el protocolo *Telnet*, que es un protocolo de comunicaciones que permite al usuario de un computador con conexión a Internet establecer una sesión como terminal remoto de otro sistema de la Red. Si el usuario no dispone de una cuenta en el computador o computador remoto, puede conectarse como usuario *anonymous* y acceder a los ficheros de libre distribución. Muchas computadores ofrecen servicios de búsqueda en bases de datos usando este protocolo. En la actualidad se puede acceder a través de *World Wide Web* (WWW) a numerosos recursos que antes sólo estaban disponibles usando *Telnet*.

1.3.6 SERVICIO WEB HOSTING

El servicio de *Web Hosting* consiste en proveer al cliente un espacio para albergar sus páginas Web en un servidor denominado *Web Host* para su posterior publicación en la WWW. El servicio puede ser gratuito o contratado y la diferencia en el servicio radica en la cantidad de espacio que se le puede asignar al cliente; en el servicio gratuito se puede conseguir hasta 5 MB (típicamente), mientras que en un contratado se puede conseguir 25 MB, 100 MB o más.

1.3.7 SERVICIO DNS [6]

El servicio DNS (*Domain Name Service*; Servicio de Nombre de Dominio) es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y viceversa. Aunque Internet sólo funciona en base a direcciones IP, el DNS permite que los usuarios usen nombres de dominio que son bastante más simples de recordar en lugar de las complicadas direcciones IP.

El sistema de nombres de dominios en Internet es un sistema distribuido, jerárquico, replicado y tolerante a fallas. Aunque parece muy difícil lograr todos

esos objetivos, la solución no es tan compleja en realidad. El punto central se basa en un árbol que define la jerarquía entre los dominios y los sub-dominios. En un nombre de dominio, la jerarquía se lee de derecha a izquierda. Por ejemplo, en *www.google.com*, el dominio más alto es *com*. Para que exista una raíz del árbol, se puede ver como si existiera un punto al final del nombre: *www.google.com.*, y todos los dominios están bajo esa raíz (también llamada "punto").

Cada componente del dominio (y también la raíz) tiene un servidor primario y varios servidores secundarios. Todos estos servidores tienen la misma autoridad para responder por ese dominio, pero el primario es el único con derecho para hacer modificaciones en él. Por ello, el primario tiene la copia maestra y los secundarios copian la información desde él.

1.3.8 SERVICIO PROXY-CACHÉ

Siempre que un cliente solicita una página Web o archivo vía FTP, el servidor Proxy-Caché actúa de intermediario y solicita dicha página o archivo al destino final y se la reenvía al cliente. Este servidor mantiene una copia local y temporal en su memoria de todas las páginas y archivos que han sido solicitados. Cuando estas páginas o archivos son solicitados, el servidor Proxy-Caché envía lo que tiene en la memoria.

Este tipo de servicio beneficia al cliente ya que mejora los tiempos de respuesta, incrementándose la velocidad en la entrega del servicio Web debido a que el caché está generalmente más cerca del cliente de lo que está la fuente original de la página Web solicitada.

1.3.9 SERVICIO DE CONVERSACIÓN MULTIUSUARIO IRC

El servicio IRC (*Internet Relay Chat*), es un servicio que permite intercambiar mensajes por escrito en tiempo real entre usuarios que estén simultáneamente conectados a la red. El servicio IRC se estructura sobre una red de servidores, cada uno de los cuales acepta conexiones de programas clientes, uno por cada

usuario.

El IRC es un servicio de conversación multiusuario, donde la gente se reúne en canales (lugar virtual, normalmente con un tema de conversación) para hablar en grupo o en privado. Cada canal trata sobre un tema o debate en particular por lo que lo primero que hay que hacer es elegir el canal al que se desea acceder o en su defecto crear uno nuevo.

Este servicio trabaja en una arquitectura cliente-servidor. El cliente corre un programa cliente llamado "IRC", el cual se conecta vía red con otro programa servidor. La misión del servidor es pasar los mensajes de usuario a usuario a través de la red IRC.

1.3.10 SERVICIO DE VOZ E IMÁGENES

Este tipo de servicio permite establecer una conexión con voz, imágenes o las dos combinadas (comúnmente denominada videoconferencia) entre dos personas conectadas a Internet desde cualquier parte del mundo sin tener que pagar el costo de una llamada internacional.

1.4 CLASIFICACIÓN DE LOS ISPs [1], [3]

En la actualidad no se puede decir que existe un solo tipo de Proveedores de Servicios de Internet, el continuo incremento de nuevos usuarios, nuevas aplicaciones, nuevos servicios y una mejor calidad de servicio, han obligado a que éstos varíen ampliamente en tamaño y cobertura.

De acuerdo a los objetivos y políticas de empresa que tenga cada ISP, éstos estarán en la capacidad de proveer únicamente servicios básicos o servicios avanzados, pero se debe destacar que todos estos están obligados a tener la suficiente escalabilidad, para soportar el incremento de nuevos usuarios.

Tomando en cuenta lo dicho anteriormente, se puede decir que los ISPs se

pueden clasificar de acuerdo a dos características principales:

1. Número de usuarios
2. Cobertura geográfica

1.4.1 ISPs DE ACUERDO AL NÚMERO DE USUARIOS

Según el número de usuarios que tengan los ISPs, se los puede clasificar en tres categorías:

1.4.1.1 ISPs pequeños

Estos ISPs tienen aproximadamente hasta unos 10000 suscriptores.

1.4.1.2 ISPs medianos

Estos ISPs tienen aproximadamente entre 10000 y 100000 suscriptores.

1.4.1.3 ISPs grandes

Estos ISPs tienen aproximadamente más de 100000 suscriptores.

Hay que reconocer que esta clasificación que se realiza es un poco ambigua, y se aplica más a ISPs de regiones extensas; por ejemplo en el Ecuador un ISP de unos 10000 suscriptores ya se considera como un proveedor grande y de cobertura nacional.

1.4.2 ISPs DE ACUERDO A LA COBERTURA GEOGRÁFICA

Según la cobertura geográfica que tengan los ISPs, éstos se pueden clasificar en:

- ✓ ISPs Locales
- ✓ ISPs Regionales

- ✓ ISPs Nacionales e Internacionales

1.4.2.1 ISPs Locales

Los ISPs locales, son ISPs pequeños que no pueden cubrir un área más allá de una determinada ciudad o parte de ella. A los ISPs locales se lo puede ver como un PoP (Punto de Presencia) de un ISP de nivel superior.

Para poder acceder al *backbone* de Internet y proveer de acceso a sus clientes, los ISPs locales se encuentran conectados a un ISP regional, nacional o internacional. Generalmente proveen sus servicios al sector residencial y pequeñas empresas mediante acceso *dial-up*.

Dependiendo del tamaño, los ISPs locales están conformados por una oficina central y en algunos casos por una o varias oficinas locales. En la figura 1.3 se puede observar la estructura de un ISP local.

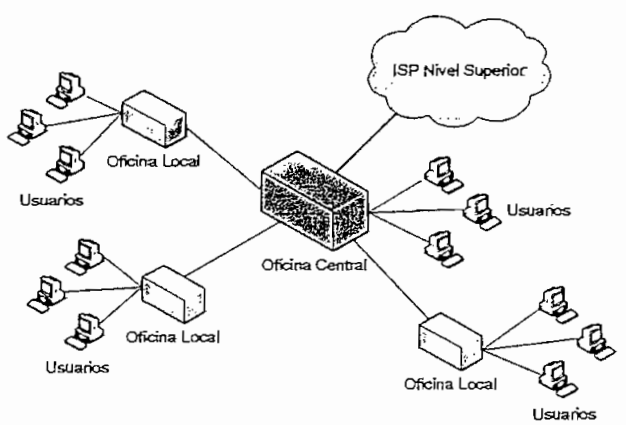


Figura 1.3. Estructura de un ISP Local

1.4.2.1.1 Oficina Central

La oficina central opera como un centro de servicio y administración para el cliente de la red, encontrándose en ésta todos los servidores y ruteadores que conforman la estructura central del ISP.

En la oficina central se encuentra el ruteador principal que se encarga de proveer conectividad externa y servidores de acceso a la red (NAS) para los clientes *dial-up*, también se encuentra en ésta, el ruteador de acceso a las oficinas locales, encargado de terminar los circuitos provenientes de las oficinas locales y proveer enrutamiento del tráfico entre ellas.

Los servicios que se ofrecen en este tipo de ISPs son básicamente: servicios de correo electrónico, DNS, Proxy-Caché, Web, *Web Hosting* para páginas de los clientes y un servicio de *browser* USENET. Estos servicios pueden encontrarse operativos a través de distintos servidores o en el caso de ISPs locales muy pequeños, éstos utilizan un único servidor para albergar todos los servicios.

1.4.2.1.2 Oficinas Locales

Las oficinas locales también denominadas PoPs se encargan de dos funciones principales: terminación de llamadas *dial-up* entrantes de los clientes y terminación del circuito proveniente de la oficina central.

1.4.2.2 ISPs Regionales

Los ISPs regionales tienen sus PoPs distribuidos en determinadas zonas geográficas, no sólo proveen acceso *dial-up*, sino, tienen la capacidad de ofrecer acceso permanente a sus clientes, esto demanda velocidades de acceso y calidad de servicios más altas. Por lo general se encuentran conectados a un ISP Nacional o Internacional, pero pueden estar conectados directamente a una compañía de telecomunicaciones que le brinde acceso directo al *backbone* de Internet.

Un ISP regional está conformado por varias oficinas centrales, una o varias regionales y varias locales, tal como se aprecia en la figura 1.4.

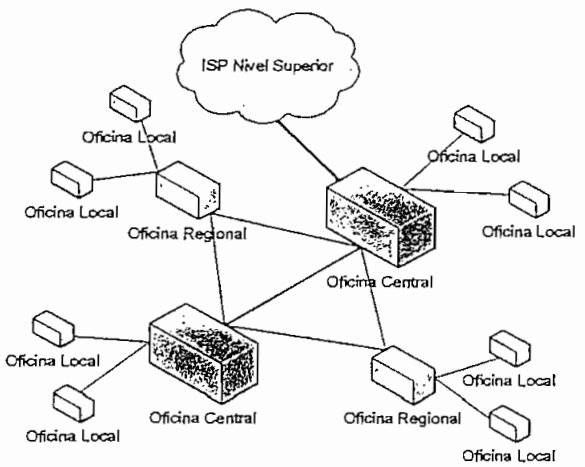


Figura 1.4. Estructura de un ISP Regional

1.4.2.2.1 Oficinas Centrales

Las funciones de las oficinas centrales se encuentran distribuidas entre ellas, para disminuir la carga y obtener un respaldo mutuo. Estas se encuentran interconectadas mediante circuitos primarios y adicionalmente poseen algunos caminos de respaldo, todo esto para mejorar la disponibilidad del servicio.

En las oficinas centrales se encuentran todos los servicios que ofrece el ISP a sus clientes, generalmente utilizan plataformas de servicio (servidores) individuales para cada servicio y no un único servidor como alternativa.

1.4.2.2.2 Oficinas Regionales y Locales

Los circuitos de las oficinas locales terminan en las oficinas regionales dentro de un ruteador el cual enruta este tráfico hacia las oficinas centrales. Las oficinas regionales están compuestas de ruteadores, unidades de acceso a la red, y un conjunto básico de servidores locales, los cuales a su vez están enlazados hacia los servidores principales de la oficina central. En la oficina regional no necesariamente se deben encontrar todos los servidores, se puede tener acceso a éstos a través de la oficina central.

La oficina local provee el servicio de conexión a Internet mediante un acceso *dial-up* o un acceso permanente. El acceso permanente de los clientes se lo realiza mediante el ruteador de acceso, este servicio de acceso puede ser de n x 64 Kbps, *Frame Relay* y otros servicios de portadora.

1.4.2.3 ISPs Nacionales e Internacionales

Los ISPs Nacionales tienen sus PoPs distribuidos en varias regiones a lo largo de un país, mientras que los ISPs Internacionales se encuentran presentes en varios países llegando inclusive a constituirse en ISPs de alcance mundial.

Los ISPs Internacionales son empresas a gran escala que pueden ser clasificadas como se indica a continuación:

1.4.2.3.1 ISPs Integrados

Los ISPs Integrados son aquellos que surgen del crecimiento de los ISPs Regionales para constituirse en una red de alta velocidad conectando a un grupo de oficinas centrales. Estas oficinas centrales alimentan a un determinado número de oficinas regionales y a su vez éstas alimentan a varias oficinas locales. La figura 1.5 muestra la estructura de un ISP integrado.

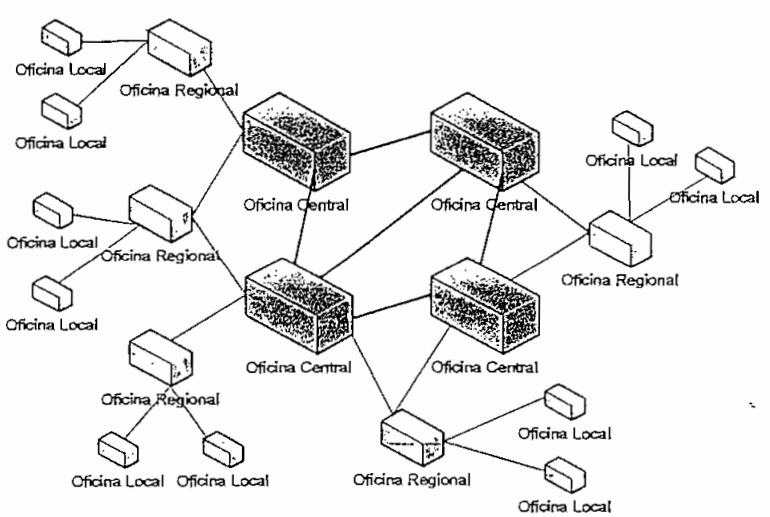


Figura 1.5. Estructura de un ISP Integrado

1.4.2.3.2 ISPs de Acceso Outsourced

El *outsourcing* o tercerización consiste en transferir a terceros proveedores aquellas actividades que no están como actividades básicas del negocio. Básicamente, ésta es una modalidad mediante la cual determinadas organizaciones, grupos o personas ajenas a una compañía son contratados para hacerse cargo de "una parte del negocio" o un determinado servicio con el fin de agilizarlo, optimizar su calidad y/o reducir sus costos.

Dentro del contexto ISP, un proveedor de acceso a gran escala del tipo *outsourced* utiliza un grupo de proveedores locales rentados para brindar servicios de acceso local a los clientes y entonces transportar el tráfico a través de la red de los proveedores locales rentados. Este método permite al ISP extenderse hacia más áreas marginales de pequeña penetración en el mercado mediante la compartición de infraestructura de acceso. En este tipo de proveedor el ISP de acceso *outsourced* opera la oficina central y el *backbone* de la red, pero no el acceso mediante las oficinas locales y regionales lo cual lo hace el proveedor de acceso contratado.

1.4.2.3.3 ISPs Multimodo

Los ISPs multimodo son empresas telefónicas que proveen servicios de mayor amplitud, ofreciendo paquetes completos de servicios de acceso a Internet utilizando su propia infraestructura como medio de transporte de la información, de ésta manera ofrecen un amplio rango de servicios de acceso y cobertura a gran escala.

1.5 ARQUITECTURA DE UN ISP [3]

El análisis de la arquitectura que se realiza a continuación, se refiere al de un ISP básico tipo local e incluye la descripción de cada uno de sus componentes. Para facilitar su estudio se puede dividir su arquitectura en tres áreas:

1. Acceso a Internet
2. Red del ISP
3. Red de Acceso al Cliente

Estas tres áreas se pueden observar en la figura 1.6:

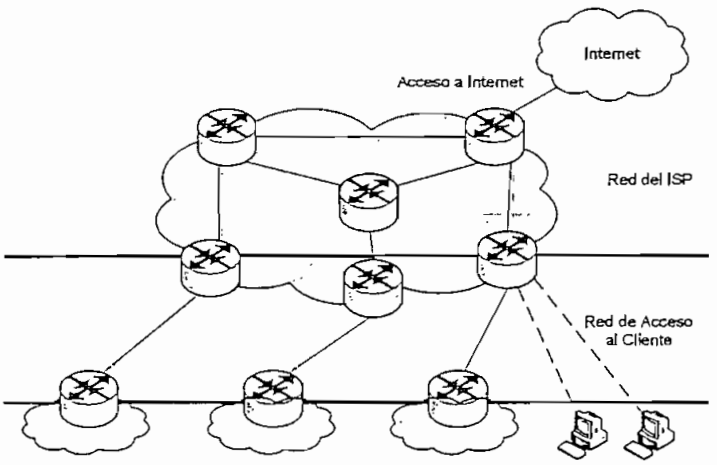


Figura 1.6. Arquitectura de un ISP

1.5.1 ACCESO A INTERNET

La conexión de la red del ISP a Internet se la realiza a través de uno o más enlaces WAN a ISPs de niveles superiores, estos proveedores son usualmente llamados proveedores de *backbone* o proveedores *upstream*. En el caso de ISPs más grandes, éstos pueden estar directamente conectados al *backbone* de Internet mediante enlaces dedicados arrendados.

Cuando un ISP pequeño inicia lo hace con un único proveedor de *backbone* y un solo enlace WAN, pero debido al continuo crecimiento del número de usuarios, se presenta la necesidad de enlaces y proveedores de respaldo.

El enlace WAN es una conexión permanente, generalmente T1/E1 con PPP (*Point to Point Protocol*), circuitos X.25, *Frame Relay*, ISDN (*Integrated Services Digital Network*), ATM (*Asynchronous Transfer Mode*), etc., o enlaces satelitales.

1.5.2 RED DEL ISP

Para entender la estructura de la red de un ISP, se analizan las posibles topologías existentes, los elementos de la oficina central y los PoPs.

1.5.2.1 Topologías de Red de un ISP

En un ISP se pueden dar las siguientes Topologías de Red:

1.5.2.1.1 Topología en Estrella

La topología en estrella o jerárquica, tiene un punto central que actúa como el núcleo de la red y circuitos radiales que conectan distintos puntos de la red al punto central, esto se puede apreciar en la figura 1.7.

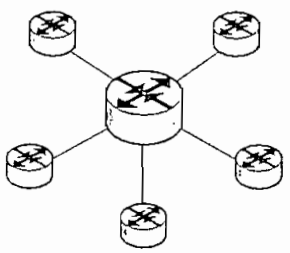


Figura 1.7. Topología en Estrella

Una mejora a este tipo de topología es la topología de estrella en cascada, en la cual un *backbone* con topología en estrella alimenta una concentración de puntos que son a su vez parte de la topología en estrella más pequeña, un ejemplo se muestra en la figura 1.8.

Estas topologías pueden presentar algunos problemas ya que si el punto central falla, entonces la red entera falla, pero presenta una solución eficiente al transporte de datos a un costo mínimo.

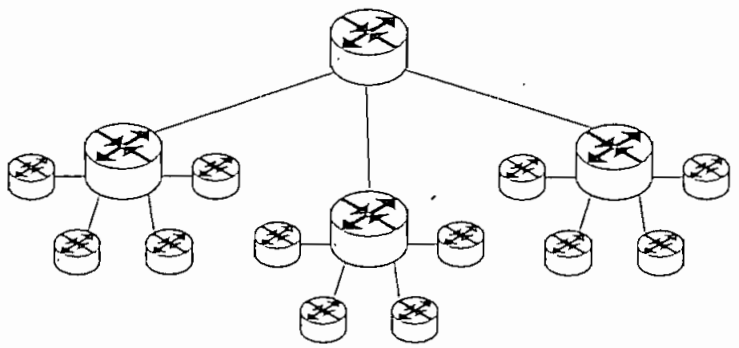


Figura 1.8. Topología Estrella en Cascada

1.5.2.1.2 Topología en Lazo

La topología en lazo es una solución a los problemas que presenta la topología en estrella, en este esquema el *backbone* del ISP tiene una configuración en lazo, en el cual cada punto de la red se conecta con otros dos puntos, resultando una conectividad en forma de anillo. La ventaja de esta topología, es la de ser más flexible ante las fallas de un único enlace ya que el algoritmo de enrutamiento de estado de enlace utilizado por esta configuración reestablecerá la conectividad, sin embargo los costos son elevados debido a los circuitos de acceso de alta capacidad para administrar la carga que transita por el *backbone*. En la figura 1.9 se puede apreciar un ejemplo de topología en lazo.

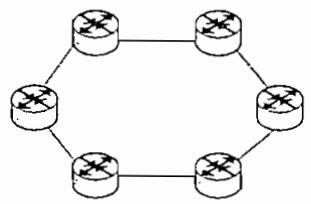


Figura 1.9. Topología en Lazo

1.5.2.1.3 Topología en Malla

La topología en malla enlaza cada punto de la red con dos o más puntos remotos distintos, de esta forma si un enlace de la red falla, la conectividad con dicho punto no se pierde ya que existen caminos alternativos; y si una localización

entera de la red falla y es necesario aislar este punto, ninguna otra localización es aislada como efecto secundario; esto se puede apreciar en la figura 1.10. Las topologías malladas son más costosas que las topologías jerárquicas pero pueden soportar mayores flujos de tráfico que una topología de lazo.

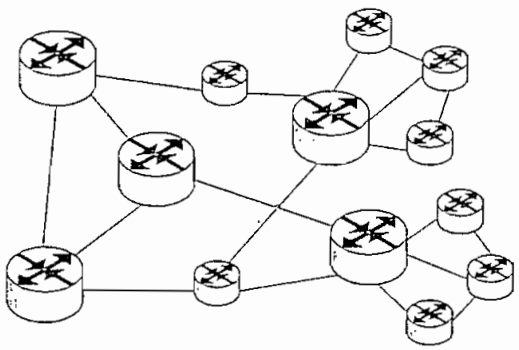


Figura 1.10. Topología en Malla

1.5.2.1.4 Dial Backup

La topología *Dial Backup* es una topología diversa complementada con un circuito de respaldo *dial* o *dial backup.* Cuando un enlace falla, los ruteadores pueden ser configurados para establecer dinámicamente un circuito temporal que actuará como un puente sobre el punto de falla. Esta configuración puede ser posible usando servicios X.25, ISDN, circuitos virtuales conmutados dentro de *Frame Relay*, ATM o circuitos de módems establecidos a través de la PSTN.

1.5.2.2 Elementos de la Oficina Central de un ISP [7]

La red de la oficina central de un ISP se puede separar en tres redes locales que separan las funciones de servicio y las funciones administrativas, tal como lo muestra la figura 1.11.

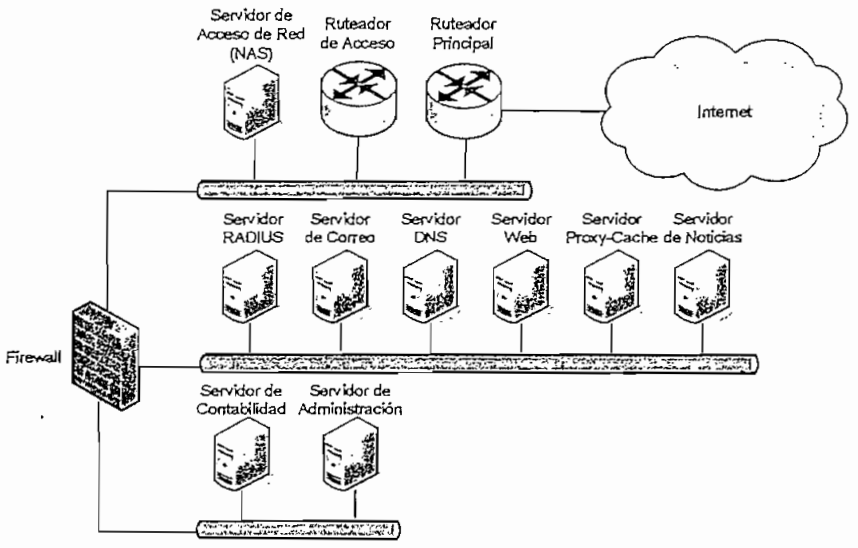


Figura 1.11. Elementos de un ISP

La red de servidores de aplicación básicamente está conformada por:

- ✓ Servidor RADIUS
- ✓ Servidor de Correo
- ✓ Servidor DNS
- ✓ Servidor Web
- ✓ Servidor Proxy-*Caché*
- ✓ Servidor de Noticias

La red de servidores de administración puede estar conformada por:

- ✓ Servidor de Contabilidad
- ✓ Servidor de Administración

En los dispositivos de acceso se pueden encontrar:

- ✓ Ruteador Principal
- ✓ Ruteador de Acceso
- ✓ Servidor de Acceso de Red (NAS)

La función que desempeñan algunos de estos elementos en la red del ISP, se describe brevemente a continuación. El resto de elementos son descritos más adelante.

1.5.2.2.1 Servidor RADIUS [8]

El servidor RADIUS (*Remote Authentication Dial-In User Service*) es un servidor que proporciona los servicios de autenticación y servicios de contabilidad del tiempo de conexión a la red para facturación. Cuando un usuario trata de conectarse al ISP, éste debe ingresar su *username* y *password,* esta información es pasada al Servidor RADIUS, el cual chequea que la información sea correcta y autoriza el acceso al ISP.

1.5.2.2.2 Servidor de Correo

El servidor de correo se encarga de almacenar los buzones de correo de los usuarios, además de realizar las funciones de envío de correo. Utiliza los protocolos estándares de Internet como SMTP, POP3 e IMAP4.

1.5.2.2.3 Servidor DNS

El servidor DNS (*Domain Name Service;* Servicio de Nombres de Dominio) se encarga de convertir los nombres de dominio como por ejemplo *http://www.google.com* en direcciones IP y viceversa.

1.5.2.2.4 Servidor Proxy-Caché

El servidor proxy-caché acepta las peticiones realizadas por un cliente y las dirige al servidor que contiene la información solicitada, espera el resultado del servidor y lo envía al cliente. Un servidor Proxy-Caché también almacena los objetos solicitados en su memoria local (caché) economizando así el ancho de banda de la red y el tiempo de respuesta cuando el mismo usuario u otro accedan al mismo objeto.

1.5.2.2.5 Servidor Web

El servidor Web almacena sitios Web inicialmente páginas de Hipertexto en formato HTML, hoy en día también almacenan información multimedia como imágenes, música (sonidos) e incluso archivos ejecutables, bases de datos, etc.

1.5.2.2.6 Servidor de Noticias

Los servidores de Noticias almacenan los cientos de miles (millones) de mensajes hacia y desde decenas de miles de grupos de noticias que existe en la red. Este tipo de servidores son mantenidos por compañías o usuarios individuales y pueden albergar miles de grupos de noticias diferentes.

1.5.2.2.7 Servidor de Contabilidad [9]

El servidor de contabilidad se encarga de almacenar las actividades que un usuario ha realizado mientras estuvo accediendo a los recursos de la red, incluso el tiempo gastado en la red, los servicios accedidos y la cantidad de datos que trasfirió durante la sesión. Este tipo de servidores son utilizados para análisis de tendencia, planificación de la capacidad, facturación, análisis y asignación de costos.

1.5.2.2.8 Servidor de Administración [10]

El servidor de administración de la red ayuda a los administradores del sistema a monitorear y administrar la red en áreas como:

- ✓ Seguridad: Asegurándose que la red esté protegida de usuarios no autorizados.
- ✓ Desempeño: Eliminando cuellos de botella en la red.
- ✓ Confiabilidad: Asegurándose que la red esté siempre disponible a los usuarios y respondiendo ante cualquier mal funcionamiento de hardware y software.

1.5.2.2.9 Ruteador Principal

Es el elemento central más importante del *backbone* de un ISP ya que permite la conexión hacia un ISP de mayor jerarquía o a un NAP (*Network Access Point;* Punto de Acceso a la Red), sus interfaces deben soportar medios de transmisión de alta velocidad.

1.5.2.2.10 Firewall

El *firewall* es un componente o conjunto de componentes que restringen el acceso entre una red interna (intranet) protegida y cualquier otra red, comúnmente Internet. Puede estar basado en hardware, software o una combinación de ambos y su objetivo principal es implementar una política de seguridad determinada.

1.5.2.3 Puntos de Presencia (PoPs)

Los puntos de presencia o PoPs son la misma red de la oficina central de un ISP que se ha extendido debido a la demanda de usuarios. Estos puntos de presencia permiten a los ISPs estar presentes en otras áreas geográficas para proveer servicio a clientes corporativos o servicio *dial-up*.

Normalmente cada uno de los servicios que brinda un PoP usa una plataforma de hardware dedicada, sin embargo estos pueden ser integrados en una única plataforma de hardware minimizando así los costos, pero esto puede crear un punto de falla de la red muy crítico. Algunos de los servidores (como los de autenticación, Web y correo electrónico) no necesariamente deben estar presentes ya que se puede acceder a estos servicios desde el ISP central.

En un PoP existen ruteadores de acceso y ruteadores internos. En los ruteadores internos terminan los enlaces de transmisión internos y en los ruteadores de acceso terminan los circuitos de los clientes. Adicionalmente pueden incluir Servidores de Acceso a la Red (NAS; *Network Access Servers*). La figura 1.12 muestra la estructura de un PoP.

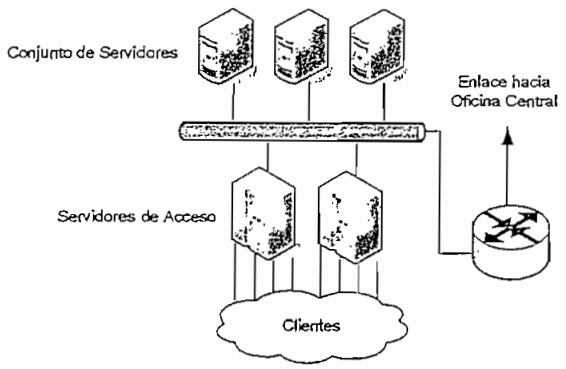


Figura 1.12. Estructura de un PoP

1.5.3 RED DE ACCESO AL CLIENTE

Existen dos tipos de clientes: el cliente corporativo que puede ser una empresa, un campus universitario, una agencia gubernamental, un ISP pequeño o una entidad similar y el cliente *dial-up* que es un sistema único como una PC residencial o una PC de una oficina pequeña con conexión bajo demanda.

1.5.3.1 Cliente Corporativo

La estructura típica de conectividad para las redes del cliente corporativo y del ISP se indica en la figura 1.13 y está compuesta de tres elementos:

- ✓ Ruteador Fronterizo del Cliente
- ✓ Circuito de Transmisión
- ✓ Ruteador de Acceso del ISP (ruteador PoP)

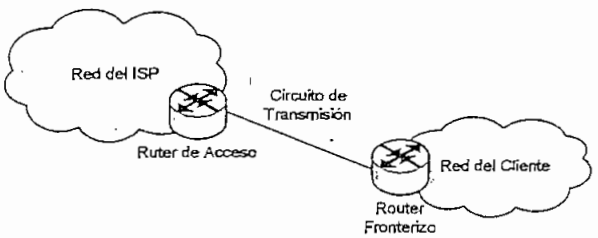


Figura 1.13. Red de Acceso Cliente Corporativo

1.5.3.1.1 Ruteador Fronterizo del Cliente

El ruteador fronterizo del cliente normalmente se encuentra en el lado del cliente e interconecta a la red local del cliente; se encarga de funciones específicas del cliente, incluyendo funciones de *firewall* y filtros de tráfico para permitir algún nivel de seguridad en el lado del cliente.

1.5.3.1.2 Circuito de Transmisión

El circuito de transmisión es un circuito dedicado, éste puede ser arrendado desde el *carrier* o puede ser alguno de los circuitos conmutados, tal como un circuito ISDN, un circuito virtual *Frame Relay* o un circuito virtual ATM.

1.5.3.1.3 Ruteador de Acceso o PoP

El *ruteador* de acceso o PoP típicamente se encarga de las funciones de control de enrutamiento de la red y tiene la responsabilidad de administrar el acceso de la red del cliente. También se encarga del control de tráfico que entra o sale de la red, monitoreo y contabilidad, porque es la frontera lógica del campo de administración del ISP. Los ruteadores de acceso deben soportar acceso ISDN, *Frame Relay*, ATM, o servicios de transmisión punto a punto para los clientes dedicados.

Un cliente corporativo puede conectarse a uno o varios ISPs de acuerdo a tres modelos:

1. Cliente *Single-Homed* si el cliente se conecta exclusivamente a un ISP utilizando un puerto de acceso dedicado.
2. Cliente Multiconectado si el cliente se conecta al mismo ISP usando más de una conexión.
3. Cliente *Multi-Homed* si el cliente se conecta a múltiples ISPs.

1.5.3.2 Cliente Dial-up

El acceso *dial-up* involucra un PC, un módem y el uso de una línea telefónica de la PSTN (*Public Switched Telephone Network*; Red Telefónica Pública Conmutada) para alcanzar el servidor de acceso de red (NAS) del ISP. También se relaciona con este tipo de clientes al acceso *dial* de redes LAN, acceso ISDN, y otros mecanismos de acceso sobre demanda.

Los elementos que intervienen en un ISP para dar acceso *dial-up* se muestran en la figura 1.14 y son:

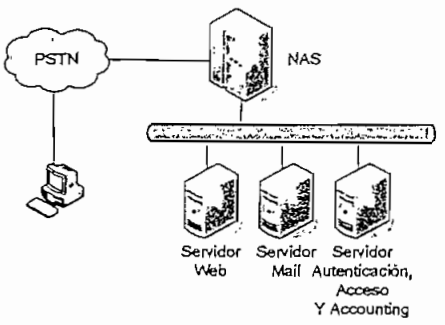


Figura 1.14. Red de Acceso Cliente Dial-up

- ✓ Unidades NAS
- ✓ Sistema de Soporte de Autenticación
- ✓ Sistema de Soporte de Acceso

1.5.3.2.1 Servidor NAS

El NAS (Network Access Server; Servidor de Acceso de Red) es un dispositivo combinado que consiste de un banco de módems y un servidor de acceso y es el encargado de responder las llamadas y proveer conectividad PPP a los clientes *dial-up*, sean éstos a través de PSTN o ISDN.

1.5.3.2.2 Sistema de Soporte de Autenticación

El sistema de soporte de autenticación permite o no el acceso de un usuario remoto a los recursos de la red del ISP, para esto se requiere de una base de datos donde estén registrados los usuarios mediante sus datos personales y recursos a los cuales tiene acceso. Esta base de datos puede ser local en el servidor de acceso o remota mediante un servidor RADIUS.

1.5.3.2.3 Sistema de Soporte de Acceso

El sistema de soporte de acceso entrega servicios de correo, para lo cual el ISP debe operar un *host send-mail* para permitir la recopilación de mensajes del usuario y operar un *host POP/IMAP mail* para permitir descargar mensajes hacia el usuario. Los servicios de soporte de acceso también incluyen servicios de DNS, servicios *Web Hosting* entre otros. Todos estos servicios pueden ser colocados en un único *host* si el ISP es de tamaño pequeño, caso contrario deben ser albergados en múltiples servidores operando en paralelo para dar servicio a los clientes.

1.5.3.3 Tecnologías Recientes para Redes de Acceso

Actualmente para dar el acceso de Internet a clientes, se están utilizando nuevas tecnologías como es el caso de:

- ✓ Redes de acceso HFC
- ✓ Redes xDSL
- ✓ Redes de acceso inalámbrico

1.5.3.3.1 Redes de Acceso HFC [11]

Una red de cable HFC o Híbrida Fibra Óptica-Coaxial, son redes de telecomunicaciones bidireccionales por cable que combina la fibra óptica y el cable coaxial como soportes de transmisión de las señales, constituyéndose en

una plataforma tecnológica de banda ancha que permite el despliegue de todo tipo de servicios de telecomunicaciones, además de la distribución de señales de TV analógica y digital.

La transmisión de datos en redes HFC se realiza a través de un medio de acceso compartido, en el que los usuarios comparten un determinado ancho de banda; por ejemplo un canal de 6 MHz podría tener una capacidad entre 10 y 30 Mbps. Las redes HFC mediante el uso de módems, especialmente diseñados para las comunicaciones digitales en redes de cable, tienen capacidad para ofrecer servicios de acceso a redes de datos como Internet a altas velocidades. En la figura 1.15 se indican los elementos que intervienen para el acceso a Internet, a través de una red HFC.

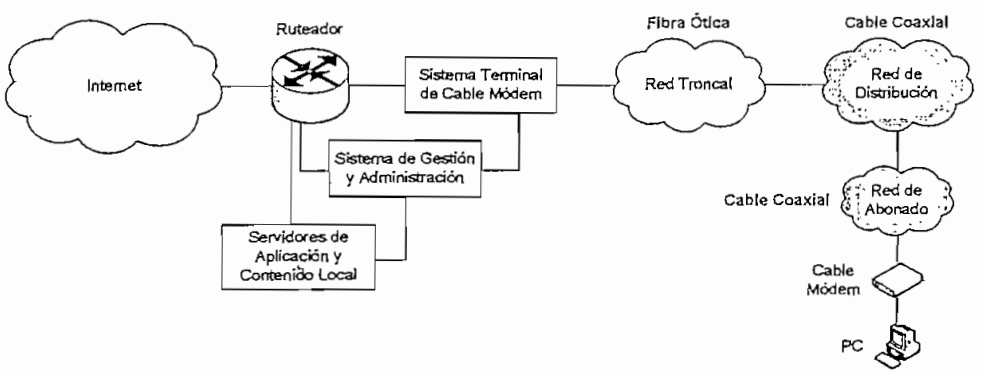


Figura 1.15. Red HFC para Acceso a Internet

1.5.3.3.2 Redes de Acceso xDSL [3], [11]

Bajo el nombre de xDSL (*Digital Subscriber Line*; Línea Digital de Abonado), se definen una serie de tecnologías que permiten el uso de una línea de cobre para transmisión de datos de alta velocidad y, a la vez, para el uso normal como línea telefónica.

Las tecnologías xDSL convierten las líneas analógicas convencionales en digitales de alta velocidad, con las que es posible ofrecer servicios de banda ancha en el domicilio de los abonados, similares a los de las redes de cable o

redes inalámbricas.

xDSL es una tecnología en la que es requerido un dispositivo módem xDSL en cada extremo del circuito de cobre. Estos dispositivos aceptan flujo de datos en formato digital y lo adaptan a una señal analógica de alta frecuencia. Los datos pasan por un dispositivo denominado "spliter", que permite la utilización simultanea del servicio telefónico básico y del servicio xDSL. El spliter se coloca delante de los módems del usuario y de la central, y está formado por dos filtros uno pasa bajos y otros pasa altos. La finalidad de estos dos filtros es la de separar las señales transmitidas por el canal en: señales de alta frecuencia (datos) y señales de baja frecuencia (voz). El dispositivo denominado DSLAM (*Digital Subscriber Line Access Multiplexer*) concentra el tráfico de datos desde múltiples bucles xDSL sobre una sola interfaz. En la figura 1.16 se pueden apreciar los elementos de una red xDSL.

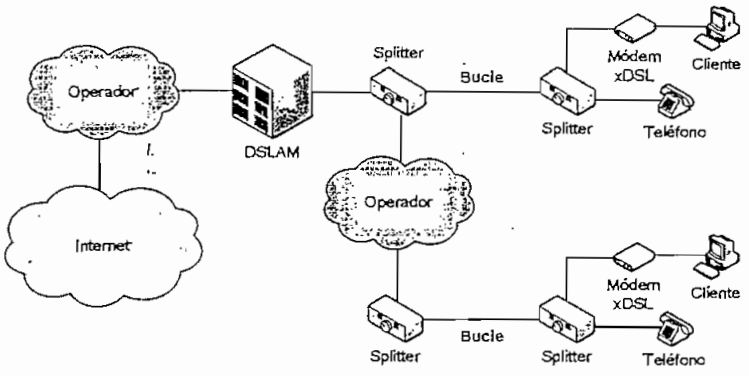


Figura 1.16. Red de Acceso xDSL

En la tabla 1.1 se exponen los tipos más importantes de las tecnologías xDSL.

1.5.3.3.3 Redes de Acceso Inalámbrico [3]

Los sistemas inalámbricos tienen una larga historia. Los enlaces de microonda han sido utilizados para la comunicación de voz y datos desde hace un largo tiempo y nuevos avances en esta tecnología han permitido que se haga uso de frecuencias cada vez más altas. Como resultado, las antenas que se usan

actualmente son más pequeñas, los sistemas son más baratos y más fáciles de implementar. Actualmente las tecnologías inalámbricas más difundidas son LMDS y espectro expandido.

Tipo	Velocidad Upstream	Velocidad Downstream	Tipo de Tráfico	Distancia Máxima
ADSL (*Asymmetric Digital Subscriber Line*)	16 a 640 kbps	1.5 a 8 Mbps	Asimétrico	2 a 3 km
HDSL (*High-bit-rate Digital Subscriber Line*)	1.544 y 2.048 Mbps	1.544 y 2.048 Mbps	Simétrico	3 a 4 km
SDSL (*Symmetric Digital Subscriber Line*)	1.544 y 2.048 Mbps	1.544 y 2.048 Mbps	Simétrico	6 a 5 km
VDSL (*Very High-bit-rate Digital Subscriber Line*)	1.6 a 19.2 Mbps	12.9 Mbps a 55.2 Mbps	Simétrico o Asimétrico	300 m a 1 km

Tabla 1.1. Tecnologías xDSL

LMDS (*Local Multipoint Distribution Service*), es una tecnología inalámbrica de banda ancha punto-a-multipunto que trabaja en la banda de los 28 GHz y en la de los 31 GHz. Basada en una concepción celular, cada celda puede tener un radio de aproximadamente 4 km, pudiendo variar dentro de un intervalo en torno a los 2 y 7 km.

Las tecnologías inalámbricas de espectro expandido trabajan en la bandas de uso libre de 2.4 y 5 GHz, y permiten obtener velocidades de transmisión en enlaces punto-a-punto y punto-a-multipunto de hasta 54 Mbps. Este tipo de tecnología es una de las más difundidas dentro de nuestro medio, no sólo por su bajo costo y el uso de bandas libres para su operación, sino también por ser de fácil diseño e implementación.

BIBLIOGRAFÍA CAPÍTULO I

[1] TOSCANO JIMÉNEZ, Miguel Ángel / GUIJARRO CÓRDOVA, René Fernando. Estudio y diseño de un ISP para la EPN y de la conectividad entre la EPN y un nodo principal del backbone de Internet. Escuela Politécnica Nacional. 2004.

[2] http://www.carsoft.com.ar/arquitectura_de_internet.htm: Arquitectura de Internet.

[3] CAICEDO JARAMILLO, María Soledad / YÁNEZ ANDAGANA, Fernando Isaías. Planificación de un Proveedor de Servicios de Internet y diseño de su sistema de seguridad. Escuela Politécnica Nacional. 2002.

[4] http://www.redbooks.ibm.com/redbooks/pdfs/sg246025.pdf: Integrating an ISP into a RS/6000 SP.

[5] http://www.dcc.uchile.cl/~raparede/papers/2000memorialSP.pdf: Diseño e Implementación de Experiencias Docentes para un Sitio Proveedor de Servicios Internet.

[6] http://www.dcc.uchile.cl/~jpiquer/Internet/DNS/node2.html: El DNS.

[7] PROAÑO AYABACA, Hugo Iván. Sistemas autónomos para Proveedores de Servicio de Internet. Escuela Politécnica Nacional. 2001.

[8] http://www.webopedia.com/TERM/R/RADIUS.html: What is RADIUS.

[9] http://www.webopedia.com/TERM/a/accounting.html: What is accounting.

[10] http://www.webopedia.com/TERM/n/network_management.html: What is network management.

[11] CANDO SANTO, Washington Oswaldo / CAZARES GUERRERO, Félix Federman. Estudio de un sistema MMDS bidireccional para la distribución de Internet de banda ancha. Escuela Politécnica Nacional. 2002.

CAPÍTULO II

2 REDES WLAN SEGÚN EL ESTÁNDAR IEEE 802.11b

2.1 DEFINICIÓN DE WLAN [1], [2]

Como su nombre lo indica, una WLAN (*Wireless Area Local Network*; Red Inalámbrica de Área Local), es una red con todas las características y beneficios de las LAN tradicionales pero sin las limitaciones de los cables.

Una WLAN, al igual que una LAN, requiere de un medio físico a través del cual transmitir las señales. En lugar de usar cable UTP o fibra óptica, las WLANs utilizan luz infrarroja o radio frecuencias. De estos dos medios físicos el más popular es el uso de radio frecuencias por su mayor alcance, mayor ancho de banda y mayor cobertura. En radio frecuencia las WLAN utilizan las bandas de frecuencias de 2.4 GHz y 5 GHz, las cuales pueden ser utilizadas sin la necesidad de licencias en algunos países.

La importancia de las WLANs, no se debe únicamente a la ausencia de cables, sino que las WLANs han dado inicio a una nueva definición de lo que es una infraestructura de red. Una infraestructura ya no necesita ser sólida y fija, difícil de movilizar y costosa de cambiar. Por el contrario, puede moverse con el usuario y cambiar tan rápido como la organización lo haga.

2.2 APLICACIONES DE LAS DE LAS REDES WLAN [2], [3]

Hoy en día las redes WLAN se han hecho muy populares y han tenido una gran aceptación, no sólo en los grandes países industrializados sino también en nuestro medio debido a las muchas ventajas que ofrecen para una variedad de situaciones. En esta sección se describen algunos de los usos más comunes y apropiados de las redes WLAN.

2.2.1 ROLES PRINCIPALES DE LAS REDES WLAN

Las redes WLAN según el estándar IEEE 802.11 usualmente se las utiliza como redes de acceso, en donde las estaciones móviles se comunican entre sí a través de un punto de acceso fijo, y a través de otros puntos de acceso se comunican con otras redes. Las tecnologías de enlace de datos comúnmente utilizadas en un rol similar son *Ethernet, DSL, Dial-Up y Cable modem.*

Algunas redes WLAN son usadas como redes de distribución. Los *bridges* inalámbricos pueden ser usados para transportar el tráfico de las redes conectadas a sus puertos *Ethernet*, mediante una conectividad *building to building* como se indica más adelante. Las tecnologías comúnmente usadas en el rol de la distribución son *Ethernet, Frame Relay y* ATM.

Debido a las bajas velocidades de transmisión y a su baja resistencia en ambientes de alto tráfico, las redes inalámbricas normalmente no se implementan en redes de *core*. Cabe recalcar que en redes pequeñas, no existe mucha diferencia entre redes de *core*, redes de distribución y redes de acceso.

2.2.2 ACCESO A DATOS CORPORATIVOS Y MOVILIDAD DE USUARIOS FINALES

Un uso común de las redes WLAN es proveer acceso a recursos corporativos en áreas donde la conectividad cableada suele ser cara e inconveniente. En este rol, las redes WLAN simplemente son herramientas que permiten proveer el acceso a los recursos corporativos.

Las redes WLAN ofrecen una solución específica a un gran problema que es la movilidad. Sin duda, las redes WLAN resuelven este candente problema de empresas y usuarios caseros, pero cabe hacer notar que todos estos problemas descienden de la necesidad de librarse de los molestosos cables de conexión de datos que impiden la movilidad. La tecnología celular ha estado disponible desde hace algún tiempo, permitiendo a los usuarios hacer *roaming* de un área a otra,

pero a velocidades muy bajas y a costos muy altos. Las redes WLAN son razonablemente más rápidas y menos costosas, y pueden ser ubicadas casi en cualquier sitio.

En la figura 2.1 se puede apreciar varios usuarios móviles obteniendo acceso a través de un dispositivo de conexión (Punto de Acceso).

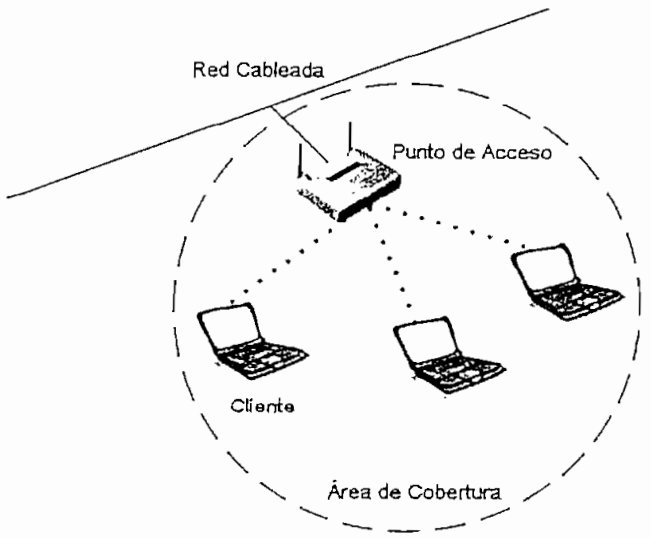


Figura 2.1. WLAN como Red de Acceso

2.2.3 USO EDUCATIVO EN AULAS DE CLASE

Las redes WLAN son particularmente apropiadas para aulas de clase. Aunque los estudiantes normalmente no se están moviendo durante una clase (ya que permanecen sentados en sus asientos), una red WLAN permite a los estudiantes acceder a recursos desde cualquier sitio dentro del aula, a través de sus computadores portátiles. Esto les facilita cambiarse de una clase a otra sin ningún inconveniente evitando así las molestias que conlleva el uso de una estación fija y cableada.

2.2.4 USO EN APLICACIONES MÉDICAS

Los hospitales y consultorios médicos son otro ejemplo de aplicaciones de

movilidad y acceso a datos corporativos. Los consultorios médicos usan redes WLAN en la misma forma que lo hacen las oficinas convencionales, pero el cuidado médico exige demandas adicionales. Las salas de emergencia por ejemplo, son extremadamente móviles y necesitan un rápido acceso a bases de datos médicas y registros de pacientes donde quiera que el doctor se encuentre.

Cabe recalcar que en este tipo de aplicaciones, los hospitales proporcionan un desafío único a las redes WLAN, ya que a menudo los hospitales suelen utilizar tecnología inalámbrica propietaria tanto para sus comunicaciones como para su equipo médico, la cual podría interferir con los equipos WLAN o viceversa.

2.2.5 EXTENSIONES DE RED A ÁREAS REMOTAS

Las redes WLAN pueden servir como una extensión de una red cableada. Esto no solo debido a que la instalación de un nuevo cableado puede significar altos costos, sino que por ejemplo en edificaciones muy extensas, las distancias pueden ser demasiado grandes para el uso de cobre y si se utiliza fibra óptica los costos de migración de la red igualmente serían muy altos.

Las redes WLAN pueden ser instaladas fácilmente para proveer una conectividad directa entre una edificación y un área remota, esto se puede apreciar en la figura 2.2.

2.2.6 MANUFACTURA Y ALMACENAJE INDUSTRIAL

Las aplicaciones de redes WLAN dentro de industrias tales como la manufactura y almacenaje son un ejemplo común de aplicaciones de extensiones de red. Estas instalaciones con frecuencia no tienen cableado *Ethernet*, por lo que agregar cableado sería muy difícil. Una red inalámbrica puede ser utilizada para extender la cobertura a toda el área en cuestión, con una única desventaja, que es la interferencia que se podría producir en las comunicaciones debido a las estructuras metálicas e interferencia de radio frecuencia que existen en este tipo de entornos.

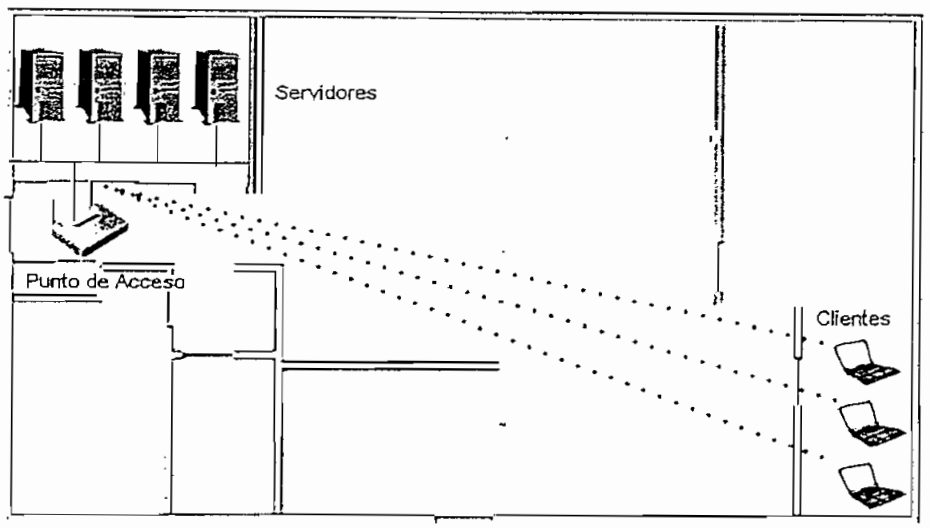


Figura 2.2. WLAN como una Extensión de Red

2.2.7 BRIDGING O CONECTIVIDAD BUILDING-TO-BUILDING

En un ambiente de campus o un ambiente con algunas edificaciones aledañas, puede existir la necesidad de que los usuarios de red de cada una de las diferentes edificaciones necesiten acceso directo a la misma red del campus. Algunos años atrás, este tipo de acceso y conectividad solía ser llevada a cabo colocando cables bajo tierra de una edificación a la otra o alquilando costosas líneas arrendadas (líneas para la transferencia rápida de datos), en una compañía portadora o *carrier*.

Usando la tecnología WLAN, los equipos pueden ser instalados fácil y rápidamente para permitir que dos o más edificaciones sean parte de la misma red sin necesidad de utilizar otras tecnologías costosas. Con el apropiado uso de antenas, un gran número de edificaciones puede ser enlazado en forma simultánea en la misma red.

Existen dos tipos diferentes de Conectividad *Building-to-Building*. La primera es denominada *Point-to-Point* (PTP; Punto-a-Punto), y la segunda *Point-to-Multipoint* (PTMP; Punto-a-Multipunto). Los enlaces punto a punto son conexiones inalámbricas, sólo entre dos edificaciones como se muestra en la figura 2.3 y casi siempre utilizan antenas semi-direccionales o antenas direccionales al final de

cada enlace.

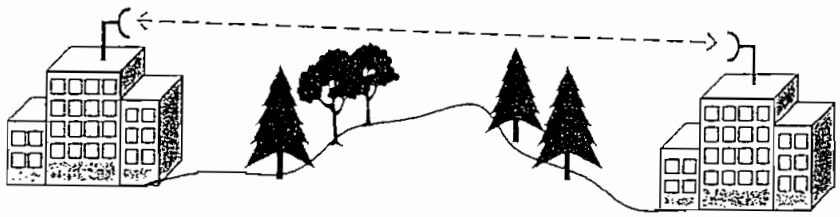


Figura 2.3. Enlace Punto-a-Punto

Los enlaces punto a multipunto son conexiones inalámbricas entre tres o más edificaciones, típicamente implementadas en una topología tipo estrella, donde una edificación es el punto central de la red. Esta edificación central es la que tendría la red de *core*, la conectividad hacia Internet y la granja de servidores. Los enlaces punto a multipunto típicamente utilizan antenas omni-direccionales en la edificación central y antenas semi-direccionales en cada una de las edificaciones remotas.

2.2.8 SERVICIOS DE ÚLTIMA MILLA

Los WISPs (*Wireless Internet Service Providers*; Proveedores de Servicio de Internet Inalámbrico), están tomando ventaja de los recientes avances en la tecnología inalámbrica para ofrecer el servicio de entrega de datos en la última milla a sus clientes. La última milla se refiere a la infraestructura de comunicación (cableada o inalámbrica) que existe entre la oficina central de la compañía de telecomunicaciones (TELCO) o compañía de cable y el usuario final. Los TELCOs y compañías de cable normalmente tienen su propia infraestructura de última milla, pero por las grandes ventajas de la tecnología inalámbrica los WISPs están ahora entregando su propio servicio de última milla inalámbrico, esto se puede observar en la figura 2.4.

Si un cliente vive en un área rural y desea acceder a una conexión de banda ancha, es mucho más rentable para un WISP ofrecer su propio acceso inalámbrico a este sitio remoto, que incurrir en gastos de instalación de una última

milla mediante una compañía de cable o una TELCO. Ciertamente los WISPs no pueden entregar una solución a prueba de fallas, pero tienen la capacidad de ofrecer acceso de banda ancha a usuarios, donde las otras tecnologías convencionales no llegan.

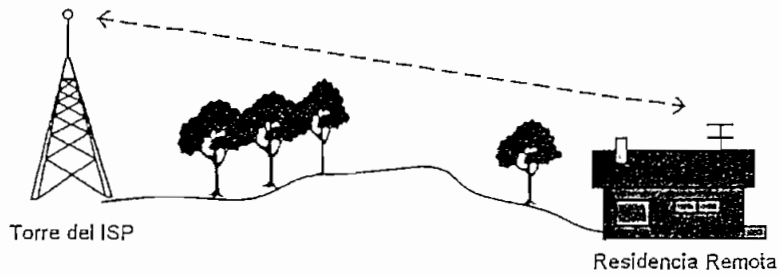


Figura 2.4. Servicio de Última Milla

2.2.9 MOVILIDAD

Como solución de redes de acceso, las redes WLAN no pueden reemplazar a las redes LAN cableadas en términos de velocidad de transmisión, ya que éstas alcanzan como máximo los 54 Mbps en comparación por ejemplo a 1 Gbps que ofrece *Gigabit Ethernet* o 10 Gbps que ofrece *10 Gigabit Ethernet*. Los ambientes inalámbricos hacen uso de conexiones intermitentes y tienen altos índices de error sobre lo que es generalmente un ancho de banda angosto. Como resultado, las aplicaciones y protocolos diseñados para el mundo cableado operan deficientemente en un ambiente inalámbrico. Sin embargo lo que ofrecen las redes WLAN es el incremento de la movilidad, a cambio de velocidad y calidad de servicio; esto se aprecia en la figura 2.5.

Algunas de las nuevas tecnologías inalámbricas permiten a los usuarios realizar *Roaming*, que es moverse físicamente de un área de cobertura inalámbrica a otra sin que se produzca una pérdida de la conectividad, igual que un usuario de telefonía móvil, el cual es capaz de hacer *Roaming* en diferentes áreas de cobertura celular. En grandes organizaciones, donde la cobertura inalámbrica abarca grandes áreas, la capacidad de *Roaming* ha significado un incremento de la productividad de estas organizaciones, simplemente porque los usuarios

permanecen conectados a la red a pesar de que se encuentran lejos de su principal área de trabajo.

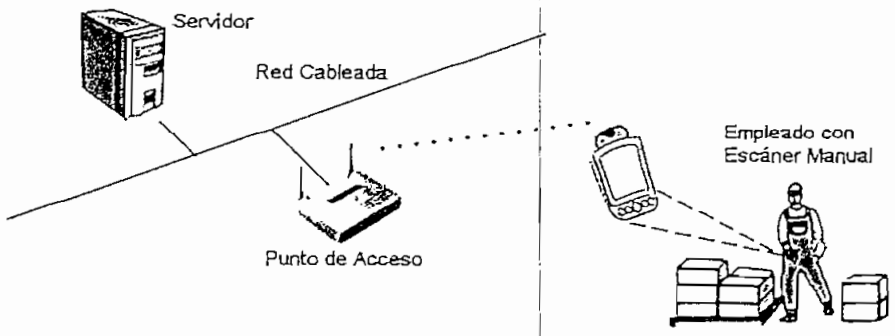


Figura 2.5. Movilidad en una WLAN

2.2.10 SMALL OFFICE-HOME OFFICE (SOHO)

En muchos hogares, incluso empresas o negocios que tienen pocos empleados, es común encontrar más de un computador, los cuales probablemente necesitan compartir archivos, una impresora o una conexión de Internet para mayor eficiencia y mayor productividad.

Para este tipo de aplicaciones denominadas *Small Office-Home Office* o simplemente SOHO, una red WLAN es una solución muy simple y efectiva, evitando así las molestas y complicadas instalaciones de cableado de red. La figura 2.6 muestra una solución típica para una SOHO mediante el uso de una red WLAN.

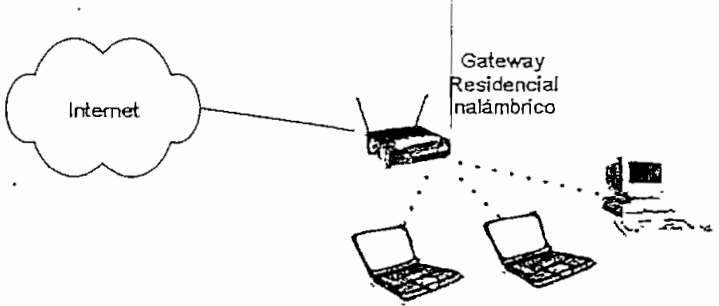


Figura 2.6. SOHO Wireless LAN

2.2.11 HOTSPOTS PÚBLICOS [2]

Un *hotspot* es una localidad geográfica específica en la cual un punto de acceso provee servicios de red inalámbrica de banda ancha (como por ejemplo el Internet), en forma pública a visitantes móviles a través de redes WLAN. Los *hotspots* con frecuencia se sitúan en lugares altamente concurridos como aeropuertos, estaciones de tren, librerías, puertos, centros de convención y hoteles.

Generalmente los *hotspots* tienen un rango de acceso corto y algunos pueden ser de uso gratuito mientras que otros no.

2.3 REQUISITOS DE UNA WLAN [4]

Una red WLAN no sólo debe cumplir con los mismos requisitos de una red LAN como son alta capacidad, cobertura pequeña, conectividad total de estaciones, capacidad de difusión, etc., sino que además, por desarrollarse en un medio inalámbrico, deben cumplir con un conjunto de necesidades específicas. Entre las más importantes se pueden citar:

- ✓ Las redes WLAN deben utilizar de forma eficiente el medio de transmisión inalámbrico para así maximizar la capacidad de transmisión.
- ✓ Una red WLAN en caso de estar conformada por una gran cantidad de nodos, debe hacer uso de varias celdas para poder dar soporte a todos los clientes. Una celda se encuentra conformada únicamente por un dispositivo concentrador inalámbrico, el cual no solo controla el tráfico entre los nodos de la WLAN, sino también el tráfico entre la WLAN y la LAN cableada en caso de que este dispositivo se encuentre conectado a la misma.
- ✓ En la mayoría de los casos es necesaria la interconexión de la WLAN con estaciones situadas en una LAN cableada. Esto se realiza como se indicó anteriormente, mediante el uso de un dispositivo concentrador inalámbrico.
- ✓ Una red WLAN debe prestar un área de cobertura cuyo diámetro típico esté entre los 100 y 300 metros, y así permitir el acceso a todos los nodos que

estén dentro de una organización.

- ✓ En caso de que los usuarios sean móviles y estos utilicen adaptadores inalámbricos sin cables de alimentación, la tecnología en la que se fundamente la WLAN debe ser tal que permita un bajo consumo de energía para así incrementar el tiempo de vida de las baterías.
- ✓ Toda red WLAN debe permitir transmisiones fiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas por parte de usuarios no deseados.
- ✓ Las redes WLAN deben tener la posibilidad de trabajar sobre bandas de frecuencias que no requieran el uso de una licencia para su utilización.
- ✓ Una WLAN debe permitir a las estaciones móviles desplazarse de una celda a otra sin ningún inconveniente.
- ✓ La inserción, eliminación y traslado dinámicos y automáticos de estaciones debe ser transparente para otros usuarios de tal forma que no les afecte.

2.4 VENTAJAS DE LAS WLANs SOBRE LAS REDES FIJAS [5], [6]

Las redes WLAN presentan muchas ventajas sobre las redes fijas, entre las más evidentes se puede indicar las siguientes:

- ✓ Movilidad
- ✓ Confiabilidad
- ✓ Facilidad en la instalación
- ✓ Accesibilidad económica
- ✓ Escalabilidad

2.4.1 MOVILIDAD

Las redes WLAN permiten a los usuarios acceso en tiempo real a la información desde cualquier sitio dentro de su organización, sin tener que buscar un lugar para conectarse a la red mediante un cable, lo que incrementa enormemente la productividad.

2.4.2 CONFIABILIDAD

Las redes WLAN son muy confiables en el sentido de fallas a nivel físico, pues el uso de menos cables y menos conectores implica menos problemas para los usuarios y administradores de red.

2.4.3 FACILIDAD EN LA INSTALACIÓN

Las redes WLAN no requieren de costosas, largas y dificultosas instalaciones de cable, y se usan principalmente en áreas de difícil acceso para las redes cableadas donde no está permitido perforar ni pasar cables a través de paredes y techos.

2.4.4 ACCESIBILIDAD ECONÓMICA

La instalación de una red WLAN y los costos de vida de los productos pueden ser significativamente más bajos que los incurridos con redes cableadas, especialmente en ambientes que requieren cambios y traslados frecuentes.

2.4.5 ESCALABILIDAD

Los sistemas de WLAN 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 resulta muy fácil la incorporación de nuevos usuarios a la red.

2.5 TECNOLOGÍAS DE TRANSMISIÓN EN LAS REDES WLAN

Una red WLAN puede ser clasificada generalmente de acuerdo a la técnica de transmisión usada. Actualmente existen tres tipos de tecnología de transmisión que utilizan las redes WLAN:

- ✓ Infrarrojos (IR)

- ✓ Microondas de Banda Estrecha
- ✓ Espectro Expandido

2.5.1 INFRARROJOS (IR) [7]

Los sistemas basados en infrarrojos son los más simples y menos costosos en las redes WLAN. Estos sistemas trabajan mucho mejor cuando operan con línea de vista (es decir cuando los *transceivers* se pueden ver el uno al otro sin ninguna obstrucción física).

Los infrarrojos no restringen su ancho de banda ya que la señal no se dispersa, algunos dispositivos que utilicen infrarrojos pueden usar todo el ancho de banda del infrarrojo, cuando se estén comunicando con otro sin provocar ningún tipo de interferencia con algún otro dispositivo.

Estos dispositivos pueden alcanzar altas velocidad a un relativo bajo costo comparado con otros tipos de sistemas. Otro beneficio de usar un sistema basado en infrarrojos es que éste no requiere ningún tipo de licencia por el uso del espectro. La radiación infrarroja cae en el segmento visible del espectro electromagnético el cual no es regulado por ninguna entidad.

Una red de infrarrojos correctamente apuntada puede lograr un largo alcance, hasta varios kilómetros, lo cual puede ser muy beneficioso. Sin embargo, cuando se necesita conectividad omni-direccional el desempeño de estos sistemas es limitado.

Los sistemas infrarrojos sufren interferencias de la luz solar y luz artificial. Inicialmente, los sistemas infrarrojos fueron muy populares, pero su falta de confiabilidad debida a la fácil obstrucción de las señales han hecho que estas redes tengan un uso limitado.

2.5.2 MICROONDAS DE BANDA ESTRECHA [4]

Estas WLANs operan en el rango de las microondas pero no hacen uso del espectro expandido. Algunos de estos productos operan a frecuencias para las que es necesario licencia para su uso, mientras que otras lo hacen en alguna de las bandas ISM (Industria, Científica y Médica), para las cuales no es necesario tener licencia.

La gran ventaja de este tipo de redes es su alta velocidad de transmisión, alcanzando velocidades que van de 10 a 20 Mbps en un rango de 40 a 15 metros respectivamente, normalmente son usadas en escenarios comerciales.

2.5.3 SPREAD SPECTRUM [3], [7]

El *Spread Spectrum* o Espectro Expandido es una técnica de comunicación que se caracteriza por utilizar un gran ancho de banda para reducir la probabilidad de que los datos sean corrompidos y una baja potencia de transmisión. Las comunicaciones de Espectro Expandido utilizan varias técnicas de modulación en las redes WLAN y posee muchas ventajas sobre su precursora, la comunicación de Banda Estrecha. Las señales de Espectro Expandido son similares al ruido, difíciles de detectar, y aún más difícilmente de interceptar o demodular sin el equipo apropiado. La figura 2.7 muestra la diferencia entre Espectro Expandido y Banda Estrecha.

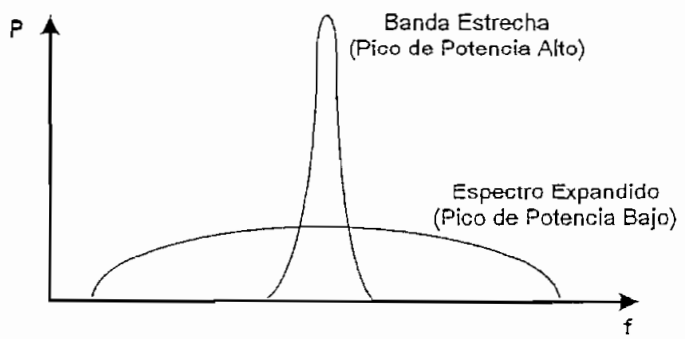


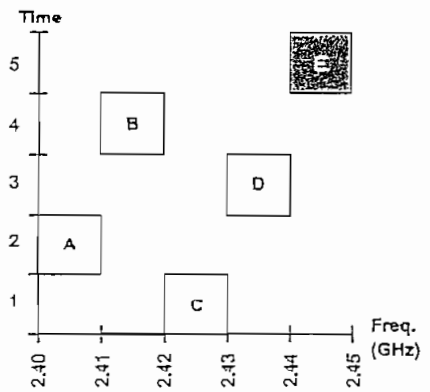
Figura 2.7. Espectro Expandido v.s. Banda Estrecha en el Dominio de Frecuencia

Actualmente existen dos tipos de tecnología de Espectro Expandido: FHSS y DSSS. Estas dos tecnologías se las describirá brevemente en las siguientes secciones.

2.5.3.1 Frequency Hopping Spread Spectrum (FHSS) [3], [8]

La técnica de Espectro Expandido por Salto de Frecuencia o FHSS es una técnica de Espectro Expandido que utiliza saltos de frecuencia para expandir los datos sobre un ancho de banda superior a los 83 MHz. El salto de frecuencia se refiere a la habilidad que tienen los transmisores para cambiar la frecuencia de transmisión abruptamente dentro de la banda de frecuencia disponible.

En los sistemas de salto de frecuencia, la portadora cambia de frecuencia, o salta de frecuencia, de acuerdo a una secuencia pseudoaleatoria. La secuencia pseudoaleatoria es una lista de varias frecuencias a las cuales la portadora saltará en un intervalo de tiempo específico. El transmisor utiliza estos saltos de frecuencia para determinar la frecuencia de transmisión. La portadora se quedará en una cierta frecuencia por un tiempo específico (conocido como *dwell time*), y luego usará una pequeña porción de tiempo para saltar a la siguiente frecuencia (*hop time*). Cuando la lista de frecuencias se haya terminado, el transmisor repetirá la secuencia.



Time	Freq. (GHz)
1	2.42
2	2.40
3	2.43
4	2.41
5	2.44

Figura 2.8. Sistema Simple de Salto de Frecuencia

La figura 2.8 muestra un sistema de salto de frecuencia que utiliza una secuencia

de salto de cinco frecuencias representadas como C-A-D-B-E. Una vez que el radio ha transmitido la información en la portadora de los 2.44 GHz, el radio repetirá la secuencia de salto, empezando nuevamente en los 2.42 GHz. El proceso de repetición de la secuencia continuará hasta que la información sea recibida completamente.

La estación receptora deberá tener el mismo patrón de saltos para poder identificar la secuencia de frecuencias en la cual llegan los paquetes. Con esto también se logra establecer un cierto nivel de seguridad, ya que si la información se enviase en una sola frecuencia, sería fácilmente interceptable; con este patrón de saltos únicamente el receptor que tenga la misma secuencia pseudoaleatoria podrá recibir correctamente la información.

2.5.3.2 Direct Sequence Spread Spectrum (DSSS) [3], [8]

La técnica del Espectro Expandido por Secuencia Directa o DSSS es una técnica de Espectro Expandido muy conocida, debiendo la mayoría de su popularidad a su facilidad de aplicación y su alta velocidad de transmisión. Hoy en día la mayoría de los equipos existentes en el mercado para redes WLAN utilizan tecnología DSSS. DSSS es un método de envío de datos, en el cual tanto el sistema de transmisión como el de recepción trabajan en un conjunto de canales de frecuencia de 22 MHz cada uno. Este gran ancho de banda de los canales permite que los dispositivos transmitan mucha más información a más altas velocidades que los sistemas FHSS.

La técnica DSSS combina la señal de datos que se desea enviar con una secuencia de bits de alta velocidad, esta secuencia de bits o (chips) se la conoce como *chipping code* o proceso de ganancia. El *chipping code* o proceso de ganancia incrementa la resistencia de la señal a la interferencia. La mínima longitud del *chipping code* que la FCC (*Federal Communications Commission*; Comisión Federal de Comunicaciones) permite es 10, y la mayoría de los productos comerciales que utilizan DSSS operan bajo una longitud de 20.

El proceso de Secuencia Directa comienza con la modulación de una portadora mediante el *chipping code*. El número de chips en el *chipping code* determinará la magnitud de la dispersión o extensión, y el número de chips por cada bit de datos y la velocidad del *chipping code* (en chips por segundo) determinará la velocidad de transmisión.

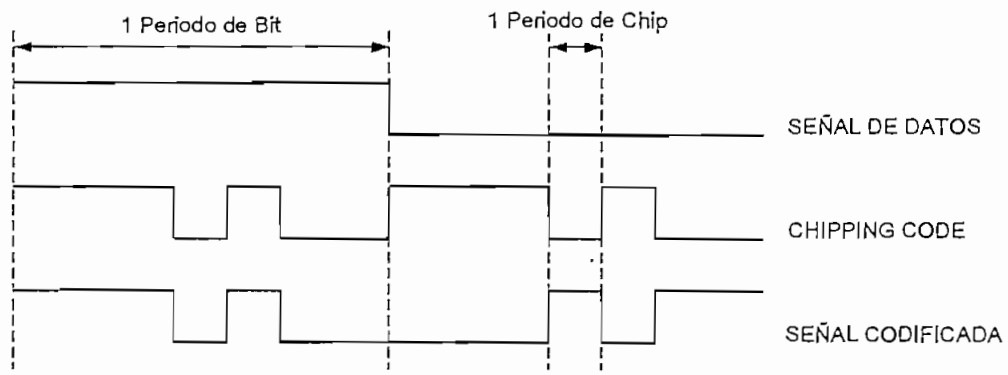


Figura 2.9. Procesamiento de la Señal en DSSS

2.5.3.3 Orthogonal Frequency Division Multiplexing (OFDM) [7]

La técnica OFDM distribuye los datos a ser transmitidos en pequeños paquetes, los cuales son transmitidos simultáneamente sobre múltiples canales de frecuencia espaciados entre sí. Este espaciado provee la ortogonalidad, la cual impide que los demoduladores vean frecuencias distintas a las que demodula.

Cuando se transmiten datos usando OFDM los datos primeramente son divididos dentro de tramas y se les aplica un algoritmo matemático conocido como la Transformación Rápida de Fourier (*Fast Fourier Transformation*; FTT), luego se le agregan los parámetros OFDM a cada trama. Las tramas resultantes luego se transmiten sobre las frecuencias designadas.

Un receptor realiza la operación inversa, se aplica una Transformación Inversa Rápida de Fourier (*Inverse Fast Fourier Transformation*; IFFT) a las tramas, para conseguir los datos transmitidos.

Los beneficios de OFDM son aprovechamiento eficiente del espectro, resistencia a la interferencia de radio frecuencias y baja distorsión por multitrayectora.

2.6 ORGANIZACIONES DE REDES WLAN [2], [3], [5]

La gran demanda de redes WLAN ha propiciado que surjan muchas organizaciones y organismos de normalización en la industria de las WLANs a nivel mundial, entre las más importantes se tiene:

- ✓ FCC
- ✓ IEEE
- ✓ Alianza Wi-Fi
- ✓ ETSI
- ✓ WLANA

2.6.1.1 Federal Communications Commission (FCC)

La FCC es una agencia gubernamental independiente de los Estados Unidos que se encarga de regular las comunicaciones vía radio, televisión, medios de cobre, satélite y cable, tanto entre los estados de este país como internacionalmente.

Esta entidad establece reglas tanto para el uso de frecuencias como para la potencia de transmisión en los dispositivos WLAN. La FCC ha establecido que las WLAN pueden usar las bandas ISM (Industria, Científica y Médica), las cuales son libres de licencias en algunos países, incluido el nuestro. Las bandas ISM están localizadas en las siguientes bandas de frecuencias:

- ✓ La banda de 902 a 908 MHz
- ✓ La banda de 2.4 GHz a 2.5 GHz
- ✓ La banda de 5.8 GHz a 5.9 GHz

Como suplemento a las bandas ISM, la FCC especifica tres bandas UNII (*Unlicensed National Information Infrastructure*). Estas bandas se encuentran

dentro del rango de los 5 GHz y tienen un ancho de banda de 100 MHz cada una, como se indica a continuación:

- ✓ La banda baja está entre los 5.15 y 5.25 GHz
- ✓ La banda media está entre los 5.25 y 5.35 GHz
- ✓ La banda alta está entre los 5.725 y 5.825 GHz, que no es la misma banda ISM de los 5.8 GHz

2.6.1.2 Institute of Electrical and Electronics Engineers (IEEE)

El IEEE es el fabricante de estándares más importante en los Estados Unidos para el área de las Tecnologías de la Información. Parte de la misión del IEEE es desarrollar estándares para la operación de las WLANs dentro del marco de ley y regulaciones de la FCC. Los cuatro estándares principales del IEEE para las redes WLAN son:

1. 802.11
2. 802.11b
3. 802.11a
4. 802.11g

2.6.1.3 La Alianza Wi-Fi

La Alianza Wi-Fi (*Wireless Fidelity*) originalmente llamada WECA (*Wireless Ethernet Compatibility Alliance*), es una asociación internacional sin fines de lucro formada en el año de 1999. Wi-Fi fue creada para certificar la interoperatividad de los productos WLAN basados en la especificación IEEE 802.11.

2.6.1.4 European Telecommunications Standards Institute (ETSI)

La ETSI es una organización sin fines de lucro cuya misión es producir los Estándares de Telecomunicaciones que serán usados por toda Europa. La ETSI representa administraciones, operadores de red, fabricantes, proveedores de

servicio, cuerpos de investigación y usuarios. Las actividades de la ETSI son determinadas por las necesidades del mercado las cuales son expresadas por sus miembros.

2.6.1.5 Wireless LAN Association (WLANA)

La WLANA es una asociación de comercio educativa sin fines de lucro conformada por los líderes e innovadores de la industria de la tecnología WLAN. La misión de la WLANA es educar y mejorar el conocimiento del usuario con respecto al uso y disponibilidad de las WLANs así como también promover la industria de las WLANs en general.

2.7 TECNOLOGÍAS Y ESTÁNDARES WLAN ACTUALES [3], [7]

Actualmente existen muchas tecnologías y estándares para redes WLAN, la popularidad o no de cada una de éstas depende de la región donde sean utilizadas y las bondades que cada una presente ante sus posibles aplicaciones. A continuación se da una breve descripción de las tecnologías y estándares más populares.

2.7.1 IEEE 802.11

El estándar 802.11 describe la operación de las redes WLAN que proveen velocidades de transmisión de hasta 2 Mbps, utilizando la tecnología FHSS o DSSS en la banda ISM de los 2.4 GHz e infrarrojos. Este estándar define la Capa Física (PHY), la subcapa MAC, las primitivas de seguridad y los modos de operación básicos.

2.7.2 IEEE 802.11b

El estándar 802.11b es una extensión del estándar 802.11 para operar a 1, 2, 5.5 y 11 Mbps en la banda de los 2.4 GHz utilizando únicamente DSSS. Este estándar también es conocido como el estándar 802.11 de alta velocidad o Wi-Fi

(*Wireless Fidelity*).

2.7.3 IEEE 802.11a

El estándar 802.11a es una extensión del estándar 802.11, el cual opera a velocidades de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps en la tres bandas UNII *(Unlicensed National Information Infrastructure)* utilizando un esquema de codificación OFDM (*Orthogonal Frequency Division Multiplexing*) al igual que la tecnología de Espectro Expandido.

2.7.4 IEEE 802.11g

El estándar 802.11g opera a velocidades de 1, 2, 5.5, 11, 18, 24, 36, 48 y 54 Mbps y es compatible con los dispositivos 802.11b. Este estándar al igual que el 802.11b especifica su operación en la banda ISM de los 2.4 GHz con la única diferencia de que no utiliza DSSS sino que hace uso de la modulación OFDM para poder operar a velocidades superiores a los 20 Mbps.

2.7.5 HOMERF

HomeRF opera en la banda ISM de los 2.4 GHz utilizando tecnología de Salto de Frecuencia. La nueva versión de HomeRF, HomeRF 2.0 usa el Salto de Frecuencias de Banda Ancha aprobado recientemente por la FCC y un protocolo de acceso llamado SWAP *(Shared Wireless Access Protocol)*, lo que le permite operar a 0.8, 1.6, 5 y 10 Mbps.

2.7.6 BLUETOOTH

Bluetooth es otra tecnología de salto de frecuencia que opera en la banda ISM de los 2.4 GHz. No está diseñada para altas tasas de transmisión más bien lo está para redes WPAN (*Wireless Personal Area Network;* Red Inalámbrica de Área Personal). Una red WPAN está definida como una red inalámbrica con un alcance de aproximadamente 3 metros, fundamentalmente alrededor del espacio personal

de una persona. Las aplicaciones incluyen la sincronización de datos de dispositivos portátiles como audífonos, agendas electrónicas, etc.

2.7.7 OPENAIR

El estándar *OpenAir* fue creado por el desaparecido WLIF (*Wireless LAN Interoperatibility Forum*), mediante el cual muchos sistemas WLAN fueron creados para complementarse como una alternativa al estándar 802.11. *OpenAir* utiliza la tecnología de espectro expandido mediante salto de frecuencia en la banda ISM de los 2.4 GHz y opera a velocidades de 800 kbps y 1.6 Mbps.

2.7.8 HIPERLAN/1 E HIPERLAN/2

Los estándares *HiperLAN* fueron establecidos por la ETSI. El estándar *HiperLAN/1* soporta rangos de velocidad de hasta 24 Mbps haciendo uso de la tecnología DSSS tanto en la banda baja UNII como la banda media UNII. El nuevo estándar *HiperLAN/2* soporta rangos de velocidad de hasta 54 Mbps utilizando la tecnología OFDM y el uso de todas las tres bandas UNII.

2.8 EL ESTÁNDAR IEEE 802.11

Actualmente el término 802.11 se refiere a toda una familia de protocolos dentro del cual se tienen el 802.11, 802.11b, 802.11a, 802.11g y otros. El IEEE 802.11 es un estándar inalámbrico el cual especifica conectividad para estaciones fijas, estaciones portátiles y estaciones móviles dentro de un área local y su propósito es proveer conectividad inalámbrica a equipos o estaciones que requieran implementaciones rápidas.

El estándar 802.11 es oficialmente designado como "*IEEE Standard for WLAN MAC and PHY Specifications*" y se encarga de definir los protocolos necesarios para soportar redes inalámbricas en un área local.

2.8.1 COMPONENTES DE LA ARQUITECTURA IEEE 802.11 [2], [9]

Las redes WLAN según el estándar IEEE 802.11 se encuentran basadas en una arquitectura celular, donde el sistema está dividido en celdas; a cada celda se la conoce con el nombre de BSS (*Basic Service Set*; Conjunto de Servicio Básico), el cual está formado por dos o mas estaciones y es controlado por una estación base, conocido como AP (*Access Point*; Punto de Acceso).

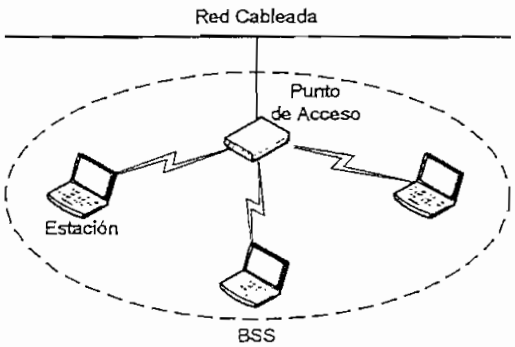


Figura 2.10. Conjunto de Servicio Básico (BSS)

Cuando dos o más estaciones se comunican directamente entre sí, sin la necesidad de un punto de acceso, forman lo que se denomina un IBSS (*Independent Basic Service Set*; Conjunto de Servicio Básico Independiente).

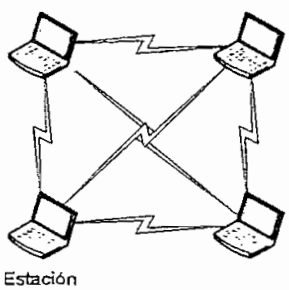


Figura 2.11. Conjunto de Servicio Básico Independiente (IBSS)

Aunque una WLAN puede formarse por una sola celda y un solo punto de acceso, muchas instalaciones requieren más de un punto de acceso para lograr la cobertura deseada; estos puntos de acceso se unen entre sí a través de un

backbone que puede ser cableado o inalámbrico y se denomina DS (*Distribution System*; Sistema de Distribución).

Al conjunto de BSSs interconectadas entre sí, se les denomina ESS (*Extended Service Set*; Conjunto de Servicio Extendido). El estándar también define el concepto de portal; un portal es un dispositivo que interconecta una red WLAN con una LAN cableada. Este dispositivo es similar a un *bridge* o puente y por lo general suele estar incluido en las funcionalidades del punto de acceso, aunque el estándar no lo especifica. La figura 2.12 permite apreciar el arreglo de estos componentes.

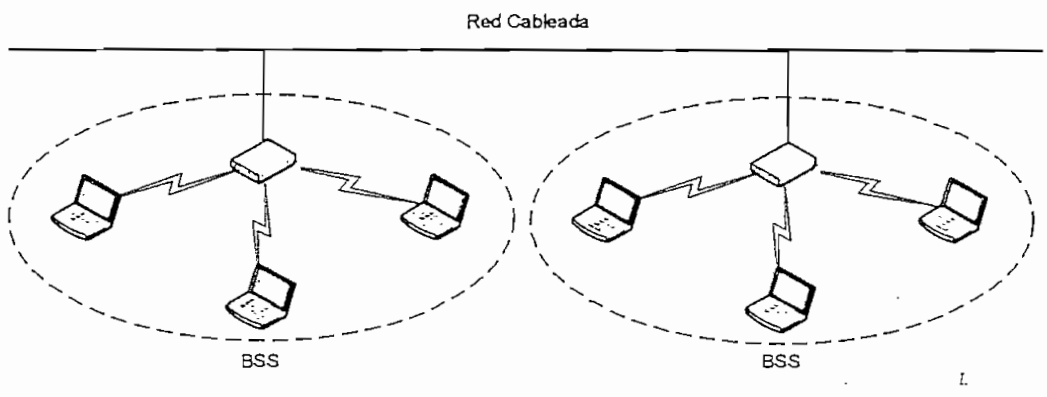


Figura 2.12. Conjunto de Servicio Extendido (ESS) y el Sistema de Distribución (DS)

2.8.2 MODOS DE OPERACIÓN O TOPOLOGÍAS DEL IEEE 802.11 [9]

Dentro de las redes inalámbricas, cuando se describe topologías no se hace referencia a las disposiciones estáticas de los dispositivos en ubicaciones específicas, sino a las reglas básicas que utilizan para comunicarse, es ésta la razón de que el término más común es configuraciones y no topologías.

El Estándar IEEE 802.11 define dos modos de operación:

1. Redes *Ad-Hoc* o IBSS
2. Redes de Infraestructura

2.8.2.1 Redes Ad-Hoc o IBSS

Una red *Ad-Hoc* es una red compuesta únicamente por estaciones donde cada estación se encuentra dentro del límite de comunicación del resto a través del medio inalámbrico, generalmente se originan de forma espontánea y son de naturaleza temporal. El término *Ad-Hoc* es con frecuencia usado para referirse a un IBSS (*Independent Basic Service Set*; Conjunto de Servicio Básico Independiente). En la figura 2.13 se puede apreciar una red *Ad-Hoc* o IBSS.

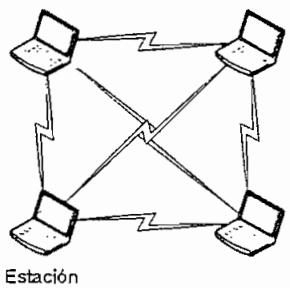


Figura 2.13. Red Ad Hoc o IBSS

2.8.2.2 Redes de Infraestructura

Una red de infraestructura es una red que se encuentra conformada por un Conjunto de Servicio Básico (BSSs) o por un Conjunto de Servicio Extendido (ESS), un Sistema de Distribución (DS) y de uno o más portales; en otras palabras la red se encuentra formada de al menos un punto de acceso conectado a la infraestructura de la red cableada y un conjunto de estaciones inalámbricas.

2.8.3 MODELO DE REFERENCIA [8], [9]

El modelo de referencia utilizado en el estándar IEEE 802.11 es el OSI (*Open System Interconnection*; Sistema de Interconexión Abierto). Para las redes LAN, el modelo OSI tiene dividida la Capa de Enlace en dos subcapas: la LLC (*Logical Link Control*; Control de Enlace Lógico) y la MAC (*Media Access Control*; Control de Acceso al Medio).

La definición de la subcapa LLC es responsabilidad del estándar IEEE 802.2, por lo cual no se hará referencia al mismo, mientras que el estándar IEEE 802.11 se responsabiliza de la subcapa MAC y la capa física. En la figura 2.14 se puede apreciar el modelo OSI con la capa de enlace dividida.

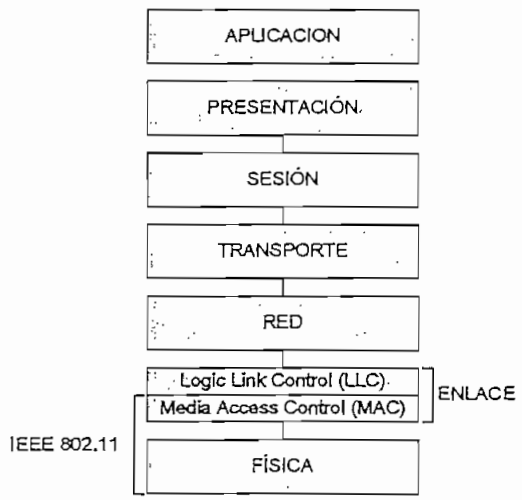


Figura 2.14. Modelo de Referencia OSI

2.8.4 LA SUBCAPA MAC [2], [9], [10]

La subcapa MAC determina la forma en que se asigna el canal, es decir, a quien lo toca transmitir a continuación. Puesto que el protocolo de la subcapa MAC para el estándar 802.11 es muy diferente al de *Ethernet* (debido a la complejidad que presenta el entorno inalámbrico en comparación con el de un sistema cableado), el estándar 802.11 no utiliza CSMA/CD (*Carrier Sense Multiple Access with Collision Detection;* Acceso Múltiple por Detección de Portadora con Detección de Colisiones), sino que hace uso de DCF (*Distributed Coordination Function*; Función de Coordinación Distribuida) y PCF (*Point Coordination Function*; Función de Coordinación Puntual), como se explica en una de las secciones más adelante.

2.8.4.1 Servicios MAC

La Subcapa MAC en el estándar IEEE 802.11 proporciona tres tipos de servicios:

1. Servicio de datos asincrónicos
2. Servicios de seguridad
3. Ordenamiento MSDU (*MAC Service Data Unit*)

2.8.4.1.1 Servicio de Datos Asincrónicos

Este servicio permite a la subcapas LLC local y remota, intercambiar MSDUs (*MAC Service Data Unit*; Unidad de Datos de Servicio MAC), utilizando los servicios proporcionados por la capa física para transportarlos a otras entidades pares MAC. El transporte de MSDUs es no orientado a conexión y utiliza el concepto del mejor esfuerzo, es decir que hará todo lo posible por entregar los paquetes pero no se garantiza que éstos lleguen a su destino exitosamente. Esta capa soporta tramas del tipo *broadcast* y *multicast* pero debido a las características propias del medio inalámbrico, puede que sufran de una menor calidad de servicio en comparación con la proporcionada a tramas *unicast*.

2.8.4.1.2 Servicios de Seguridad

Los servicios de seguridad en IEEE 802.11 son proporcionados por los servicios de autentificación y el mecanismo WEP (*Wired Equivalent Privacy*; Privacidad Equivalente a una Cableada), y están limitados al intercambio de datos de una estación a otra estación.

Estos servicios de seguridad proporcionados por el mecanismo WEP cumplen con las siguientes metas: Confidencialidad, Integridad de Datos y Control de Acceso; y lo realiza mediante la encriptación de las MSDUs lo cual es transparente a la subcapa LLC y las otras capas por encima de la subcapa MAC.

2.8.4.1.3 Servicios de Ordenamiento MSDU

Los servicios proporcionados por la subcapa MAC permiten y pueden requerir el reordenamiento de las MSDUs. Si fuera necesario, la subcapa MAC puede reordenar las MSDUs para mejorar la probabilidad de entrega acertada, esto

basándose en el modo operacional actual de la estación o estaciones receptoras señaladas. El único efecto de este reordenamiento es un cambio en el orden de entrega de las MSDUs de *broadcast* y *multicast*. Las MSDUs *unicast* tienen mayor prioridad que las de *multicast* y *broadcast*.

2.8.4.2 Formato de la trama MAC [4]

Como se puede aprecia en la figura 2.15 una trama MAC consta de tres partes principales:

1. Una cabecera MAC que está conformada por los campos de control, duración, dirección y control de secuencia.
2. Un cuerpo de longitud variable que contiene información específica del tipo de trama.
3. Y un FCS (*Frame Check Sequence*; Secuencia de Chequeo de Trama) que contiene un CRC (*Cyclic Redundancy Check*; Control de Redundancia Cíclica) de 32 bits.

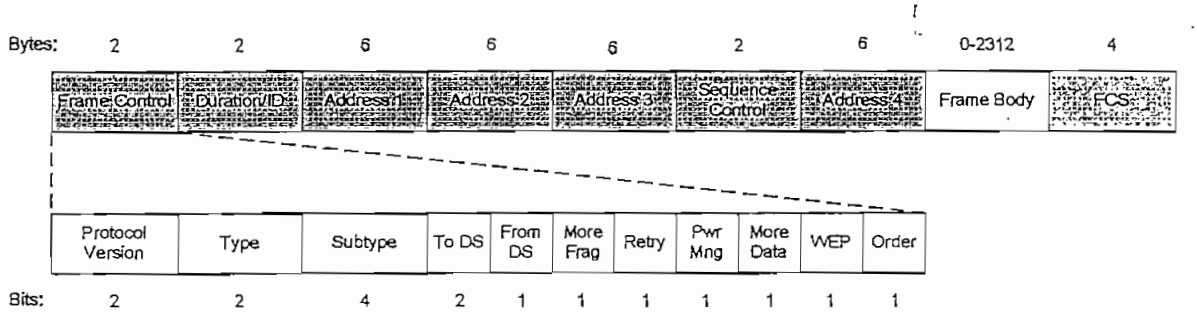


Figura 2.15. Formato de la Trama MAC

El campo *Frame Control* está conformado de 11 subcampos. El primero es el *Protocol Version*, que identifica la versión del Estándar IEEE 802.11. Luego se tiene el campo *Type* para especificar si la trama es de datos, control o de administración; y el campo de *Subtype* para indicar por ejemplo si es un RTS o CTS. Los bits *To DS* y *From DS* indican que la trama va hacia o viene del sistema de distribución entre celdas. El bit *More Frag* indica que siguen más fragmentos. El bit *Retry* marca una retransmisión de una trama que se envió anteriormente. El

bit de *Pwr Mng* es utilizado por la estación base para poner al receptor en estado de hibernación o sacarlo de tal estado. El bit *More Data* indica que el emisor tiene tramas adicionales para el receptor. El bit *WEP* especifica que el cuerpo de la trama se ha codificado utilizando el algoritmo WEP. Por último, el bit *Order* indica al receptor que una secuencia de tramas que tenga este bit encendido debe procesarse en orden estricto.

El segundo campo de la trama es el *Duration/ID*. En tramas de control del tipo *Power Save* para dispositivos con limitaciones de potencia, contiene el identificador o AID (*Association Identity*) de estación. En tramas de datos indica cuánto tiempo ocuparán el canal, la trama y su confirmación de recepción.

El encabezado de trama contiene cuatro direcciones. Dos son para el origen y destino, y las otras dos direcciones son para los puntos de acceso de origen y destino para el tráfico entre celdas.

El campo de *Sequence Control* permite que se numeren los fragmentos. De los 16 bits disponibles, 12 identifican la trama y 4 el fragmento.

2.8.4.3 Tipos de Tramas

Los tres principales tipos de tramas usados en la subcapa MAC son:

1. Tramas de Datos
2. Tramas de Control
3. Tramas de Administración

Las tramas de datos son usadas exclusivamente para la transmisión de datos. Las tramas de control, tal como la RTS (*Request to Send*), CTS (*Clear to Send*) y ACK (*Acknowledgment*), controlan el acceso al medio. Las tramas de administración, son transmitidas de la misma forma que las tramas de datos para intercambiar información de administración, pero no son enviadas a las capas superiores.

2.8.4.4 Arquitectura de la Subcapa MAC

Antes de transmitir una trama, una estación debe obtener acceso al medio usando cualquiera de los dos métodos siguientes:

1. El método fundamental de acceso de la subcapa MAC en el estándar IEEE 802.11, es el CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance;* Acceso Múltiple por Detección de Portadora con Evasión de Colisiones), denominado como DCF (*Distributed Coordination Function*; Función de Coordinación Distribuida) dentro de este estándar. La DCF es implementada en todas las estaciones, para el uso dentro de la configuración *Ad-Hoc* y de Infraestructura.
2. La subcapa MAC del IEEE 802.11 puede también implementar un método de acceso opcional, denominado PCF (*Point Coordination Function*; Función de Coordinación Puntual), la cual crea acceso libre de contención CF (*Contention Free*). El PCF sólo puede ser usado en la configuración de infraestructura.

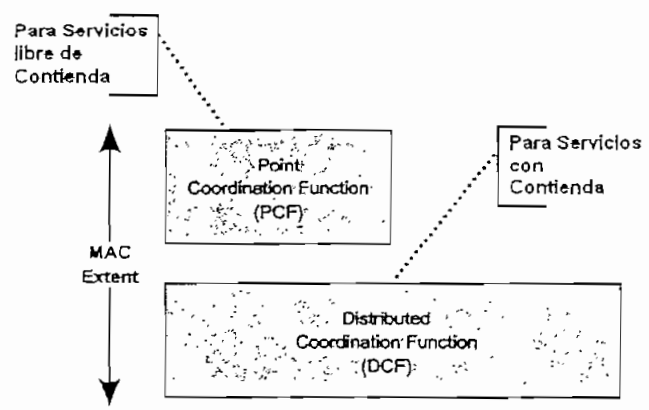


Figura 2.16. Arquitectura de la Subcapa MAC

2.8.4.4.1 Protocolo CSMA/CA y MACA

El propósito del CSMA/CA es controlar la compartición del medio y reducir la probabilidad de colisiones entre múltiples estaciones que mayoritariamente se producen inmediatamente después de que el medio se desocupa, esto se realiza

"escuchando" el medio con el fin de determinar si alguna estación está efectuando una transmisión. Si el medio está libre es posible empezar la transmisión, caso contrario antes de hacerlo, la estación deberá esperar un intervalo de tiempo determinado por el Algoritmo de *Backoff*, aún así la estación deberá asegurarse de que el medio esté libre antes de intentar transmitir otra vez. Si el medio continúa ocupado la estación deberá esperar hasta que se termine la transmisión que se está efectuando y además esperar un tiempo de duración aleatoria.

El Algoritmo de *Backoff* es el método utilizado para resolver la contención entre diferentes estaciones que quieren acceder al medio. Una característica de este algoritmo es que hace que el intervalo de espera crezca en forma exponencial a medida que aumenta el número de colisiones. La especificación IEEE 802.11 define que el algoritmo debe ejecutarse en los siguientes casos:

- ✓ Cuando la estación censa el medio antes de empezar a transmitir y el medio se encuentra ocupado o colisiona.
- ✓ Después de cada retransmisión.
- ✓ Después de una transmisión exitosa.

El único caso que el mecanismo no es utilizado, es cuando la estación decide transmitir un nuevo paquete y el medio se halla libre por un tiempo mayor al de un DIFS (Espaciado entre Tramas DCF).

Sin embargo, CSMA/CA en un entorno inalámbrico y celular presenta una serie de problemas, los dos principales son:

1. Nodos ocultos: una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no lo puede escuchar.
2. Nodos expuestos: una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

La solución que propone 802.11 es MACA (*Multi Access Collision Avoidance;*

Acceso Múltiple con Evasión de Colisiones). Según este protocolo, antes de transmitir el emisor envía una trama RTS (*Request to Send*), indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS (*Clear to Send*), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos. La solución final de 802.11 es utilizar MACA con CSMA/CA para enviar los RTS y CTS.

El tráfico que se transmite bajo DCF es de carácter asincrónico ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles, los cuales no son tolerados por los servicios sincrónicos.

2.8.4.5 Operación de la Subcapa MAC

La Función de Coordinación Distribuida DCF y la Función de Coordinación Puntual PCF pueden operar al mismo tiempo dentro de la misma BSS. Cuando éste es el caso, los dos métodos de acceso se alternan, esto con un período libre de contención CF seguido por un período de contención. Además, todas las transmisiones de tramas bajo el PCF pueden usar un IFS (*Interframe Space;* Espaciado entre Tramas) que es más pequeño que el usado por las tramas transmitidas por el método del DCF. El uso de un IFS más pequeño implica que el tráfico coordinado puntualmente tendrá prioridad en el acceso al medio sobre las estaciones operando en el modo DCF.

2.8.4.6 Mecanismo de Detección de Portadora

Para determinar el estado del medio se utilizan dos mecanismos de detección de portadora, el mecanismo físico y el mecanismo virtual. Cuando cualquiera de los dos mecanismos indica un medio ocupado, el medio es considerado ocupado. Si el medio no esta ocupado se lo considerará desocupado. Uno de los mecanismos de detección de portadora es proporcionado por la Capa Física y el otro por la subcapa MAC.

La subcapa MAC provee el mecanismo virtual de detección de portadora. El

mecanismo hace referencia al NAV (*Network Allocation Vector*; Vector de Asignación de la Red). El NAV mantiene una predicción del futuro tráfico en el medio basado en la información dentro del campo de duración de las tramas *unicast*. La información de duración también está disponible en las cabeceras MAC de todas las tramas enviadas durante el periodo de contención CP (*Contention Period*).

2.8.4.7 Acuses de Recibo a Nivel MAC

La recepción de algunas tramas requiere que la estación receptora responda con un acuse de recibo, generalmente una trama ACK, si el FCS de la trama es correcto. Esta técnica es conocida como acuse de recibo positivo. Esto se muestra en la figura 2.17.

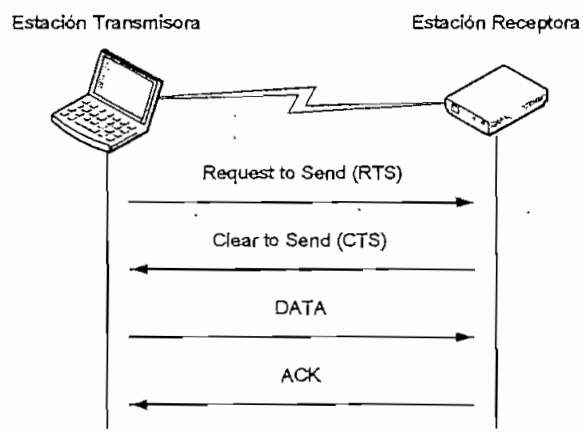


Figura 2.17. Acuses de Recibo a Nivel MAC

La no recepción de una esperada trama ACK, indica a la estación transmisora que un error ha ocurrido. Es posible que la estación receptora haya recibido la trama correctamente y que el error haya ocurrido en la entrega de la trama ACK. Para la estación que inicia el intercambio de tramas, estas dos condiciones son indistinguibles.

2.8.4.8 Espaciado entre Tramas IFS

El intervalo de tiempo entre las tramas se denomina IFS (*Interframe Space*; Espaciado entre Tramas). Durante este período mínimo, una estación estará "escuchando" el medio antes de transmitir. Cada intervalo IFS es definido como el tiempo entre el último bit de la trama anterior y el primer bit del preámbulo de la trama siguiente. Como se puede apreciar en la figura 2.18, se definen cuatro diferentes IFS para proveer niveles de prioridad para el acceso al medio inalámbrico.

2.8.4.8.1 SIFS (Espaciado Corto entre Tramas)

SIFS es el intervalo más corto, se utiliza para permitir que las distintas partes de un diálogo transmitan primero. Esto incluye dejar que el receptor envíe un CTS para responder a una RTS, dejar que el receptor envíe un ACK para un fragmento o una trama con todos los datos y dejar que el emisor de una ráfaga de fragmentos transmita el siguiente fragmento sin tener que enviar un RTS nuevamente.

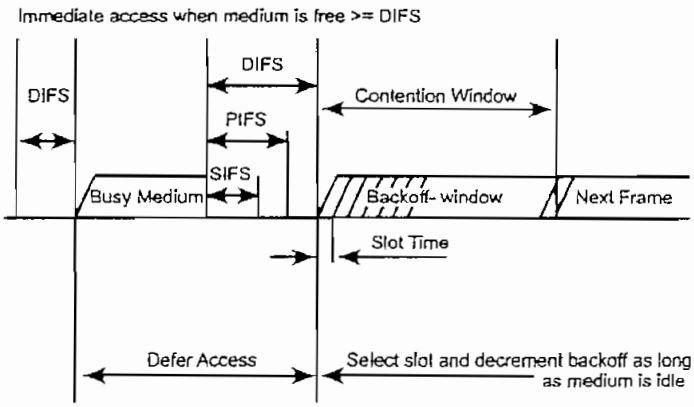


Figura 2.18. Espaciado entre tramas IFS

2.8.4.8.2 PIFS (Espaciado entre Tramas PCF)

El intervalo PIFS es utilizado únicamente para que estaciones que están operando como PCF ganen prioridad en el acceso al medio, al inicio de un

período libre de colisiones y puedan transmitir inmediatamente después de que han detectado que el medio está libre.

2.8.4.8.3 DIFS (Espaciado entre Tramas DCF)

Es utilizado por estaciones que estén actuando como DCF para la transmisión de tramas de datos y de administración, luego de que hayan detectado mediante su mecanismo de portadora que el medio está libre.

2.8.4.8.4 EIFS (Espaciado entre Tramas Extendido)

Es utilizado por una estación que ha detectado la recepción incorrecta o incompleta de una trama por medio del FCS, este intervalo de tiempo empieza luego de que se detecta la trama incorrecta, el objetivo de este espaciado entre tramas es prevenir las colisiones de tramas pertenecientes a la misma comunicación.

2.8.5 LA CAPA FÍSICA [2], [11], [12]

En las secciones anteriores se ha hecho una revisión de la subcapa MAC en la especificación IEEE 802.11 ya que es la misma para el resto de especificaciones como es el caso de la especificación IEEE 802.11b, que es la razón principal de este estudio. En las siguientes secciones se seguirá revisando la especificación IEEE 802.11 ya que tiene mucha similitud con la especificación motivo de este estudio, sin embargo donde sea necesario se remitirá únicamente a la especificación IEEE 802.11b.

2.8.5.1 Funciones de la Capa Física

La subcapa MAC es sólo una parte de la operación total del 802.11. La capa física (PHY) es la otra mitad. En el estándar IEEE 802.11 la capa física tiene tres funciones principales:

1. Procedimiento de Convergencia de la Capa Física PLCP
2. Sistema Dependiente del Medio Físico PMD
3. Capa Física de Gestión

2.8.5.1.1 Procedimiento de Convergencia de la Capa Física

El Procedimiento de Convergencia de la Capa Física PLCP (*Physical Layer Convergence Procedure*) define un método de convergencia que transforma las MPDUs (*MAC Sublayer Protocol Data Units;* Unidades de Datos del Protocolo de la Subcapa MAC), en un formato de trama adecuado para el envío y recepción entre dos o más estaciones a través de uno de los medio físicos definidos por el IEEE 802.11. El PLCP también entrega tramas que provienen del medio inalámbrico a la subcapa MAC.

Los servicios de la capa física son entregados a la entidad MAC en una estación a través de un Punto de Acceso de Servicio SAP (*Service Access Point*), denominado el PHY-SAP, como se muestra en la figura 2.19.

2.8.5.1.2 Sistema Dependiente del Medio Físico

El sistema PMD define las características y los métodos de transmisión y recepción de datos a través del sistema inalámbrico entre dos o más estaciones.

Un conjunto de primitivas son definidas para describir la interfaz entre la subcapa PLCP y la PMD. Esta interfaz se denomina la PMD-SAP y se muestra también en la figura 2.19.

La subcapa PMD acepta las primitivas de servicio de la subcapa PLCP y proporciona el método mediante el cual los datos se trasmiten o reciben del medio.

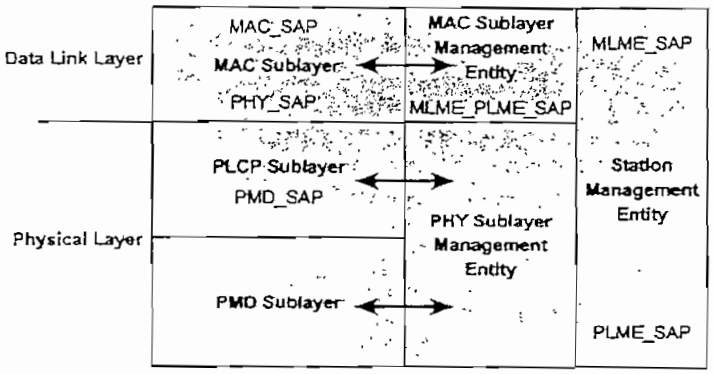


Figura 2.19. Funciones de la Capa Física

2.8.5.1.3 Capa Física de Gestión

En la capa Física de Gestión se puede distinguir la estructura MIB (*Management Information Base*; Base de Información para la Administración), que contienen por definición las variables de gestión, los atributos, las acciones y las notificaciones requeridas para gestionar una estación. Consiste de un conjunto de variables donde se especifica o almacena el estado y la configuración de las comunicaciones de una estación.

2.8.5.2 La especificación IEEE 802.11b (High-Rate)

La especificación 802.11b permite transmitir a dos nuevas velocidades, 5.5 y 11 Mbps utilizando únicamente la técnica DSSS. Esta especificación por lo tanto es compatible y puede interoperar con dispositivos que estén bajo el estándar original que operen a 1 y 2 Mbps usando DSSS.

2.8.5.2.1 Modulación y Velocidad de Transmisión

El estándar original especifica una secuencia de 11 chips denominada *Barker Sequence* para codificar los datos. Cada secuencia de 11 bits representa un único bit de datos (0 o 1) el cual se modula en una portadora convirtiéndose en una forma de onda denominada símbolo para luego ser enviado a través del medio inalámbrico. Los datos son transmitidos a 1 Mbps usando la técnica DBPSK

(*Differential Binary Phase Shift Keying*) y a 2 Mbps usando DQPSK (*Differential Quadrature Phase Shift Keying*).

Para incrementar la velocidad de transmisión, el estándar 802.11b hace uso de técnicas de codificación más avanzadas y no de la secuencia de 11 chips como en el estándar original; 802.11b hace uso de CCK (*Complementary Code Keying*), que consiste de un conjunto de palabras código de 64 Bytes con ciertas características matemáticas que les permite distinguirse una de otra en un receptor a pesar del ruido y la interferencia. En la velocidad de 5.5 Mbps se utiliza CCK codificando 4 bits en una portadora, mientras que en la de 11 Mbps se codifica 8 bits por portadora. Ambas velocidades utilizan modulación DQPSK. La tabla 2.1 muestra las diferentes técnicas de modulación y los rangos de velocidad utilizados en el estándar 802.11b.

Velocidad de Tx	Longitud del Código	Tipo de Modulación
1 Mbps	11 (Barker Sequence)	DBPSK
2 Mbps	11 (Barker Sequence)	DQPSK
5.5 Mbps	8 (CCK)	DQPSK
11 Mbps	8 (CCK)	DQPSK

Tabla 2.1. Técnicas de Modulación y Velocidades de Transmisión

Para soportar varios ambientes de ruido y mayor alcance, 802.11b utiliza un rango dinámico de velocidades de transmisión, permitiendo que la velocidad se ajuste automáticamente dependiendo de la interferencia y ruido que se presente.

2.8.5.2.2 Número de Canales en Operación

Las frecuencias centrales y los números de CHNL_ID de los canales asignados al estándar IEEE 802.11b se muestran en la figura 2.20. Como se puede observar en esta figura, en algunas regiones no se utilizan todos los canales, por ejemplo en EE.UU. que está regulado por la FCC únicamente se utilizan 11 canales, mientras que en Japón que está regulado por la MKK sólo se utiliza un canal para esta aplicación.

		Regulatory domains					
CHNL_ID	Frequency (MHz)	X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32' France	X'40' MKK
1	2412	X	X	X	—	—	—
2	2417	X	X	X	—	—	—
3	2422	X	X	X	—	—	—
4	2427	X	X	X	—	—	—
5	2432	X	X	X	—	—	—
6	2437	X	X	X	—	—	—
7	2442	X	X	X	—	—	—
8	2447	X	X	X	—	—	—
9	2452	X	X	X	—	—	—
10	2457	X	X	X	X	X	—
11	2462	X	X	X	X	X	—
12	2467	—	—	X	—	X	—
13	2472	—	—	X	—	X	—
14	2484	—	—	—	—	—	X

Figura 2.20. Canales de Frecuencia para el Estándar 802.11b

Los canales operativos no solapados y solapados así como sus frecuencias centrales para Norte América se muestran en la figura 2.21.

Set	Number of channels	HR/DSSS channel numbers
1	3	1, 6, 11
2	6	1, 3, 5, 7, 9, 11

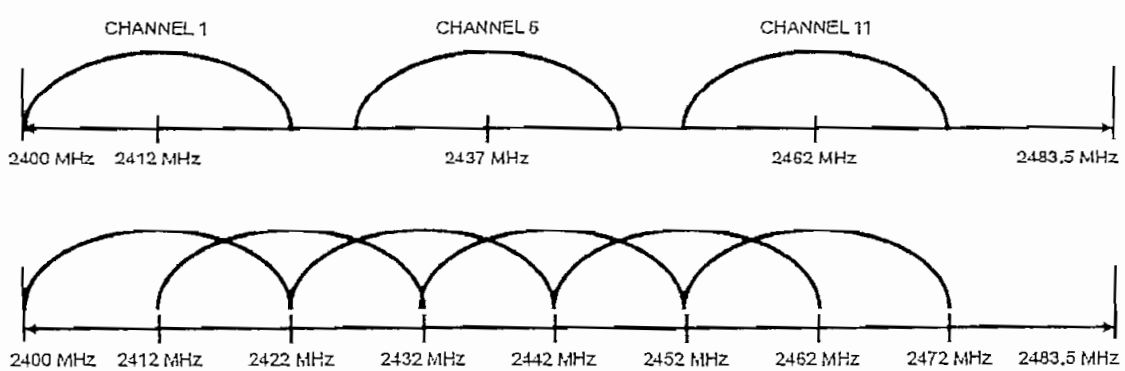


Figura 2.21. Canales Operativos Norte América

2.8.6 MECANISMOS DE SEGURIDAD [2], [4], [11]

El estándar 802.11 así como su extensión 802.11b proveen dos mecanismos de seguridad; un mecanismo de control de acceso a nivel de subcapa MAC y un mecanismo de encriptación conocido generalmente como WEP (*Wired Equivalent Privacy;* Privacidad Equivalente a una Cableada). Además de esto, el estándar 802.11 complementa su seguridad mediante el uso de dos mecanismos de autenticación de estaciones clientes. A continuación se explicara brevemente cada uno de estos mecanismos.

2.8.6.1 Control de Acceso

Para el control de acceso utiliza el SSID (*Service Set Identifier;* Identificador de Conjunto de Servicio), que es un conjunto de 1 a 32 caracteres ASCII, el cual se programa dentro de cada punto de acceso y debe ser conocido por el usuario para poderse asociar con un punto de acceso.

La mayoría de puntos de acceso tienen las opciones de realizar "*broadcast* del SSID" y "permitir cualquier SSID". Usando la opción de "permitir cualquier SSID", el punto de acceso permite el acceso a cualquier cliente con un SSID en blanco. La opción "*broadcast* del SSID", hace que el punto de acceso envíe paquetes de aviso, los cuales anuncian el SSID.

Aunque en el estándar IEEE 802.11 no está especificado, muchos fabricantes hacen uso de una tabla de direcciones MAC, la cual se incluye igualmente dentro del punto de acceso, restringiendo el acceso sólo a clientes cuyas direcciones MAC se encuentren dentro de la lista.

2.8.6.2 Encriptación WEP

Para la encriptación de datos, el estándar 802.11 hace uso de un algoritmo de clave compartida de 40 bits conocido como WEP (*Wired Equivalent Privacy;* Privacidad Equivalente a una Cableada), basado en el Algoritmo RC4. Este

algoritmo fue diseñado por Ronald Rivest y se mantuvo en secreto hasta que fue filtrado y se publicó en Internet en 1994. Todos los datos enviados y recibidos mientras una estación está asociada con un punto de acceso, son encriptados mediante la clave. Cuando la encriptación está siendo utilizada, el punto de acceso emitirá un paquete encriptado a cualquier estación que intente asociarse con el. La estación debe utilizar su clave para encriptar la respuesta con el fin de autentificarse y poder ganar acceso a la red.

2.8.6.3 Autenticación y Asociación

La Autenticación Abierta y Autenticación de Clave Compartida son dos métodos que el estándar IEEE 802.11 define en las estaciones clientes para conectarse a un punto de acceso. A continuación se explica estos dos métodos y los pasos que la estación experimenta durante el proceso.

2.8.6.3.1 Autenticación Abierta

La Autenticación Abierta básicamente es un método de autenticación nula, lo que significa que no hay verificación del usuario. Usando este método de autenticación, una estación puede asociarse con cualquier punto de acceso que utilice este método basado solamente en tener el SSID correcto. Los SSIDs deben coincidir tanto en el punto de acceso como en el cliente antes de que al cliente le sea permitido completar el proceso de autenticación.

Como se puede apreciar en la figura 2.22, el proceso de Autenticación Abierta ocurre de la siguiente manera:

1. El cliente inalámbrico hace una petición para asociarse con el punto de acceso.
2. El punto de acceso confirma la autenticación y registra al cliente.
3. El cliente envía una petición de asociación.
4. El punto de acceso confirma la asociación y registra el cliente.

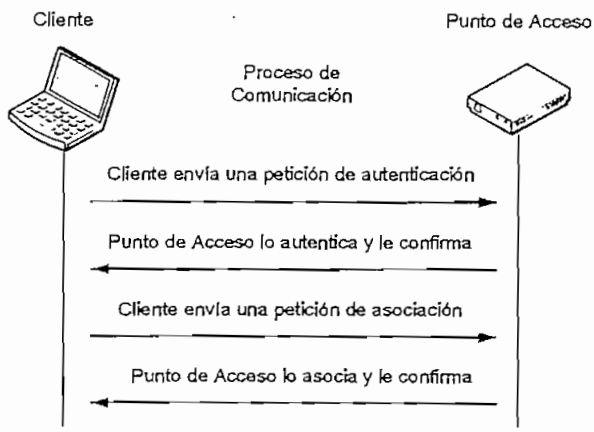


Figura 2.22. Proceso de Autenticación Abierta

Normalmente este tipo de autenticación no se encuentra ligada a una clave WEP. Un cliente podría asociarse con una clave WEP incorrecta e incluso sin una clave WEP al punto de acceso ya que en la Autenticación Abierta no existe verificación de la clave WEP. Sin embargo un cliente con una clave WEP equivocada es incapaz de enviar o recibir datos ya que la carga útil de la trama es encriptada. Hay que tomar en cuenta que la cabecera no es encriptada por el algoritmo WEP, únicamente se encriptan los datos.

2.8.6.3.2 Autenticación de Clave Compartida

La Autenticación de Clave Compartida es un método de autenticación que requiere el uso de la encriptación WEP. La encriptación WEP utiliza claves que son ingresadas normalmente por el administrador de la red dentro del punto de acceso y del cliente. Estas claves deben ser iguales en ambos lados para que WEP trabaje apropiadamente.

Como se puede apreciar en la figura 2.23, el proceso de Autenticación de Clave Compartida ocurre como sigue:

1. Un cliente solicita asociarse a un punto de acceso, paso similar al de la autenticación abierta.
2. El punto de acceso emite un mensaje de desafío al cliente, el cual es un

texto sin cifrar generado en forma aleatoria y que se trasmite sin ninguna protección.

3. El cliente responde al mensaje de desafío encriptandolo mediante el uso de su clave WEP y enviándolo de regreso al punto de acceso.
4. El punto de acceso responde a la respuesta del cliente desencriptando el mensaje que le envió de regreso para verificar que el mensaje fue encriptado utilizando la clave WEP apropiada. A través de este proceso, el punto de acceso determina si el cliente tiene la clave WEP correcta o no. Si la clave WEP es correcta, el punto de acceso responderá positivamente y autentificará al cliente caso contrario, el punto de acceso responderá negativamente y no autentificará al cliente.

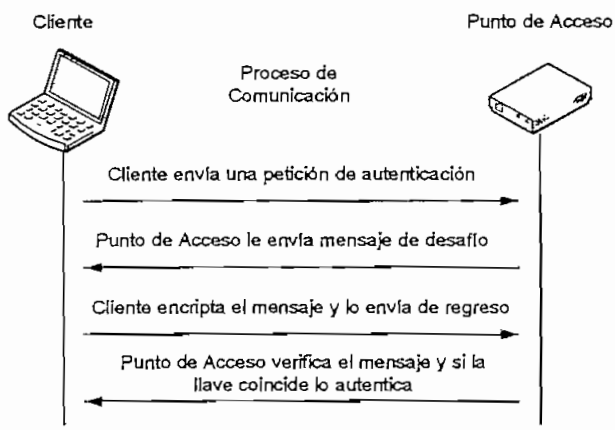


Figura 2.23. Proceso de Autenticación de Clave Compartida

La Autenticación de Clave Compartida es menos segura que la Autenticación Abierta porque en la Autenticación de Clave Compartida, el punto de acceso trasmite el mensaje de desafío y recibe el mismo mensaje pero encriptado con la clave WEP, permitiendo que los *hackers* obtengan estos dos mensajes y descifren la clave WEP para luego poder acceder al tráfico encriptado.

BIBLIOGRAFÍA CAPÍTULO II

[1] http://www.aed.com.ve/pdf/AK-WiFi-05-03-04.pdf: Redes de Área Local Inalámbricas.

[2] CISCO NETWORKING ACADEMY PROGRAM. Fundamentals of Wireless LANs v1.0.

[3] CERTIFIED WIRELESS NETWORK ADMINISTRADOR. Official Study Guide. MacGraw-Hill. Second Edition. 2003.

[4] STALLINGS, Williams. Data and Computer Communications. Prentice Hall. Sixth Edition. 2000.

[5] 05b_El_auge_de_las_redes.pdf: El Auge de las Redes Inalámbricas (WLANs).

[6] http://home.intermec.com/eprise/main/Intermec/Content/About/getArticle?section=about&ArticleID=260.htm: Wireless LAN Basics.

[7] Wiley - Building Secure Wireless Networks with 802.11.pdf: Building Secure Wireless Networks with 802.11.

[8] CHAMORRO ARIAS, Julio Cesar. Diseño de una Red de Área Local (LAN) Inalámbrica para la Ex-Facultad de Ingeniería Eléctrica. Escuela Politécnica Nacional. 2001.

[9] 802.11-1999.pdf: ANSI/IEEE Std 802.11, 1999 Edition.

[10] 08-802.11-Francisco-Lopez-Ortiz-res.pdf: El estándar IEEE 802.11 Wireless LAN.

[11] IEEE 802_11b Wireless LAN White Paper.pdf: IEEE 802.11b Wireless LANs.

[12] 802.11b-1999.pdf: IEEE Std 802.11b-1999 (Supplement to ANSI/IEEE Std 802.11, 1999 Edition).

CAPÍTULO III

3 SEGURIDAD EN REDES WLAN

3.1 INTRODUCCIÓN A SEGURIDAD DE REDES [1]

Seguridad en Redes es un proceso mediante el cual, los recursos de información son protegidos. La meta de la seguridad es mantener la integridad, preservar la confidencialidad y garantizar la accesibilidad.

El principal propósito de la seguridad es mantener a los intrusos fuera. Para las redes cableadas esto significa construir establecimientos pequeños con paredes fuertes y puertas bien resguardadas para así proveer acceso seguro a un selecto grupo de personas. Sin embargo, esta estrategia no funciona para las redes WLAN. El ascenso del comercio móvil y las redes inalámbricas hace que el viejo modelo de seguridad sea inadecuado. Debido a esto en la actualidad las soluciones de seguridad deben ser transparentes, flexibles, manejables e integradas discretamente.

El concepto de Seguridad no implica sólo asegurar que los usuarios puedan ejecutar tareas y obtener información a la que ellos están autorizados. Seguridad también significa que los usuarios no puedan causar daños a los datos, aplicaciones o al ambiente operativo de un sistema. La palabra Seguridad implica además, protección contra ataques maliciosos y control de los efectos por errores y fallas de equipos en la red.

3.2 RIESGOS DE LAS REDES WLAN [2], [3]

Las redes WLAN se han vuelto muy populares debido a que permiten el acceso a los usuarios sin la necesidad de cables sino mediante el uso del aire como medio de transmisión. La propagación de las ondas de radio fuera del sitio donde está

ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible a una empresa y a la seguridad informática de la misma.

Muchos son los riesgos que se derivan del factor anterior. Como se describen posteriormente, se pueden perpetrar un sinnúmero de ataques a una red WLAN con el fin de tener el acceso a la red, obtener información valiosa o simplemente deshabilitar la red WLAN.

Por ejemplo, cuando una red WLAN se encuentra configurada en una topología Ad-Hoc, el hecho de que no se pase por un punto de acceso puede permitir que se ataque directamente a una de las estaciones cliente, generando problemas si dicha estación ofrece servicios TCP/IP o comparte archivos. También existe la posibilidad de duplicar las direcciones IP o MAC de estaciones clientes legítimas, permitiendo a cualquier *hacker* tener acceso a la red.

Los puntos de acceso en la mayoría de los casos están expuestos a Ataques por Fuerza Bruta para descifrar y averiguar los *passwords*, por lo que una configuración incorrecta de los mismos facilitaría la infiltración de intrusos en la red WLAN.

Igualmente, como se indica en las siguientes secciones, a pesar de los riesgos que una red WLAN pueda tener, existen varias soluciones y mecanismos de seguridad que impiden de una u otra manera que usuarios maliciosos puedan introducirse en la red.

3.3 MÉTODOS DE DETECCIÓN DE REDES WLAN [3], [4]

Como ya se indicó en las secciones anteriores, con frecuencia la señal de las redes WLAN no se queda entre las cuatro paredes de una oficina o entre la línea de vista de un enlace sino que puede ser detectada, utilizada y/o explotada por aquellos atacantes conocidos como *hackers* de señales inalámbricas (*War Chalkers*) y *hackers* de redes inalámbricas (*War Drivers*). Con la ayuda de un

equipo sencillo y un software "rastreador" de puntos de acceso inalámbricos, estos individuos recorren ciudades enteras en busca de puntos de acceso inalámbrico inseguros. Actualmente existen dos métodos de detección de redes WLAN:

1. El *Warchalking*
2. El *Wardriving*

3.3.1 EL WARCHALKING

El *Warchalking* consiste en caminar por la calle con un computador portátil dotado de una tarjeta de red inalámbrica, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta un símbolo especial en un objeto cercano como una acera, un muro o un poste, indicando la presencia del punto de acceso y si tiene o no configurado algún tipo de seguridad. De este modo otras personas o *hackers* pueden conocer la localización de la red. En la figura 3.1 se puede observar la simbología que se utiliza en este método de detección.

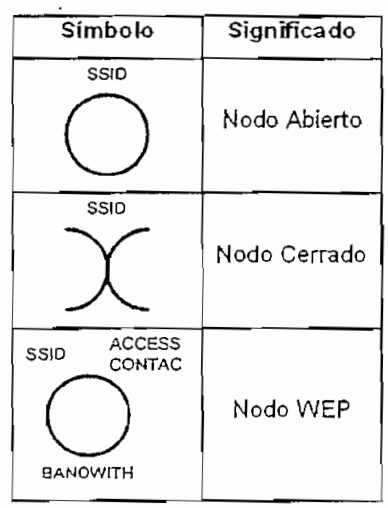


Figura 3.1. Simbología Warchalking

Algunos *hackers* hacen uso de palabras para la señalización. Por ejemplo, la palabra *bellum* indica la presencia de un nodo abierto. Si el nodo es protegido luego por algún tipo de encriptación, o si el nodo es temporal, la palabra *bellum*

suele ser cruzada o reemplazada por la palabra *pax*. Estas palabras son la traducción al latín de guerra y paz respectivamente.

3.3.2 EL WARDRIVING

El *Wardriving* es un método muy similar al anterior con la diferencia de que la localización de puntos de acceso se lo realiza desde un automóvil y con un equipo más sofisticado. Para este fin se hace uso de un computador portátil con una tarjeta de red inalámbrica, una antena adecuada, un GPS para obtener las coordenadas exactas (longitud y latitud), y un software para detección de redes inalámbricas, todo esto con fines de mapeo.

3.4 TIPOS DE ATAQUES A REDES WLAN [5], [6]

Las redes WLAN al trabajar a través del aire sin una conexión física palpable hacen que cada vez sean más susceptibles a ataques por parte de *hackers* maliciosos, los cuales pueden pretender deshabilitar o intentar ganar acceso a la red WLAN. Los diferentes tipos de ataques existentes según el objetivo que tengan, pueden ser agrupados dentro de dos grupos:

1. Ataques Pasivos
2. Ataques Activos

3.4.1 ATAQUES PASIVOS

Los ataques pasivos tienen como objetivos la intercepción de datos y el análisis de tráfico sin la alteración de la comunicación. Es decir, el atacante únicamente "escucha" o monitorea los datos para descifrarlos y poder obtener la información que se ha transmitido.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

3.4.2 ATAQUES ACTIVOS

Los ataques activos realizan una variedad de procesos en el paso de los mensajes por el segmento inalámbrico, lo cual puede modificar el flujo de datos transmitidos o crear un falso flujo de datos. Este tipo de ataques se los puede dividir dentro de cuatro categorías:

1. Modificación de Mensajes, que consiste en realizar modificaciones directamente sobre el contenido del mensaje (borrar, insertar, modificar).
2. Denegar entrega de mensajes, que consiste en no permitir que el mensaje sea entregado a su destino a través de bloqueos o retenciones.
3. Retardar entrega de mensajes, que consiste en hacer que un mensaje no llegue a su destino en el tiempo normal, de manera deliberada.
4. Enmascarar, que consiste en utilizar una falsa identidad para que un mensaje sea aceptado.

Los ataques activos permiten a los *hackers* desempeñar algún tipo de función dentro de la red. Un ataque activo puede ser usado para ganar acceso a un servidor y así poder obtener datos valiosos, usar el acceso a Internet de la organización para propósitos maliciosos e incluso cambiar la configuración de la infraestructura de la red.

3.5 ATAQUES MÁS COMUNES EN REDES WLAN [7]

Actualmente existen un sinnúmero de métodos que permiten ganar acceso no autorizado a las redes WLAN, ésto se debe principalmente a una serie de falencias que tienen este tipo de redes, entre los métodos de ataque más comunes se tiene:

- ✓ *Eavesdropping*
- ✓ WEP *Cracking*
- ✓ Ataques MAC
- ✓ Ataques *Man-In-The-Middle*

- ✓ Ataques de Diccionario y por Fuerza Bruta
- ✓ Ataques de *Jamming*

3.5.1 EAVESDROPPING

El *Eavesdropping* (escucha a escondidas) es unos de los ataques pasivos más simples y efectivos en redes WLAN. Este tipo de ataques no deja rastro de la presencia del *hacker* ya que éste no tiene que conectarse realmente al punto de acceso para "escuchar" los paquetes que atraviesan el segmento inalámbrico. Lo que hace el *hacker* en realidad es situarse en los alrededores de las instalaciones y mediante el uso de una antena direccional y de un software adecuado "escucha" y recolecta los paquetes que atraviesan el segmento inalámbrico.

Existen aplicaciones habituales como los analizadores de protocolos WLAN que son capaces de recolectar *passwords* de sitios HTTP, correo electrónico, mensajería instantánea, sesiones FTP, y sesiones Telnet, los cuales son enviados sin cifrar. Otras aplicaciones pueden descifrar las claves WEP de la red WLAN, permitiendo a los *hackers* tener acceso total a la red inalámbrica.

3.5.2 WEP CRACKING

Como se indica en una de las secciones más adelante, el algoritmo WEP es muy vulnerable porque la encriptación de claves permanece estática y las claves son muy cortas. Las claves de encriptación utilizadas por WEP, nunca cambian, a no ser que éstas sean cambiadas en forma periódica y manual por el administrador de la red en todos los dispositivos inalámbricos, algo que es muy molesto y raramente ejecutado.

Un *hacker* mediante el uso de un *sniffer* para recolectar paquetes inalámbricos, luego de reunir una cantidad suficiente de estos, puede correr fácilmente herramientas de software, las cuales pueden determinar las claves de encriptación en pocos minutos, permitiendo al *hacker* descifrar los paquetes y poder acceder a toda la información que pasa por el segmento inalámbrico.

3.5.3 ATAQUES MAC (SPOOFING)

Un ataque MAC o *Spoofing* es la capacidad que tiene un *hacker* para engañar a un equipo de red y hacerle pensar que la conexión que está viendo es de una estación valida y permitida de su red. Los agresores pueden lograr esto de diversa formas, la más fácil es simplemente redefinir la dirección MAC de una tarjeta de red inalámbrica.

Las direcciones MAC pueden ser atacadas muchas veces de la misma forma que las claves WEP. Una vez que las claves de encriptación son descifradas, todos los paquetes de datos, incluyendo la dirección MAC están expuestos. Más aún, si no se utiliza encriptación, la dirección MAC puede ser extraída de una forma extremadamente fácil.

Luego de que una dirección MAC válida ha sido obtenida, los *hackers* pueden cambiar la dirección MAC de una tarjeta inalámbrica de una PC intrusa para igualar a una tarjeta de alguna PC de la WLAN, e instantáneamente ganar acceso a toda la red WLAN. Algunas tarjetas inalámbricas permiten el cambio de sus direcciones MAC a través de software o cambios en la configuración del sistema operativo de la PC.

Puesto que dos estaciones con las mismas direcciones MAC, no pueden coexistir en una misma LAN, el *hacker* debe encontrar la dirección MAC de una estación móvil la cual sea removida de los alrededores de la WLAN en una hora particular del día. Sólo durante este tiempo, en que la estación móvil no está presente, el *hacker* puede ganar acceso dentro de la red sin ningún problema.

3.5.4 ATAQUES MAN-IN-THE-MIDDLE [5]

Un ataque *man-in-the-middle* es una situación en la cual un individuo malicioso usa un punto de acceso para secuestrar nodos móviles mediante el envío de una señal más fuerte que la enviada por el punto de acceso legítimo, a estos nodos. Los nodos móviles que se asocian con el punto de acceso intruso, envían sus

datos a las manos equivocadas sin darse cuenta. La figura 3.2 muestra un ataque *man-in-the-middle*, secuestrando clientes WLAN.

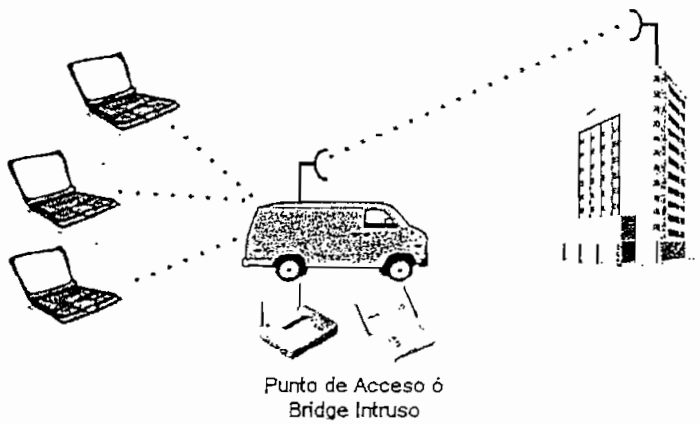


Figura 3.2. Ataque Man-In-The-Middle

A fin de permitir que los clientes se reasocien con el punto de acceso intruso, la potencia de transmisión del punto de acceso intruso debe ser mucho más alta que el de los otros puntos de acceso en el área. La perdida de conectividad con un punto de acceso legítimo sucede de forma discreta como parte del proceso de *roaming* de tal forma que algunos clientes se conectan al punto de acceso intruso accidentalmente.

La persona que esté perpetrando un ataque de este tipo primeramente debe conocer el SSID (*Service Set Identifier;* Identificador de Conjunto de Servicio) que los clientes inalámbricos están utilizando, esta información es fácilmente obtenible. EL *hacker* también debe conocer las claves WEP de la red en el caso de que la encriptación WEP esté siendo utilizada en la misma.

Muchas veces los ataques *man-in-the-middle* son provocados mediante el uso de un simple PC portátil con dos tarjetas inalámbricas incluidas y algún software que emule un punto de acceso. Una de las tarjetas de la PC es usada como punto de acceso y la otra tarjeta es usada para conectar la PC al punto de acceso legítimo más cercano. Esta configuración hace a la PC un *"man-in-the-middle"*, operando entre clientes y el punto de acceso legítimo, de esta forma un *hacker* puede

obtener información valiosa corriendo un analizador de protocolos en la PC sobre este escenario.

Un particular problema con el ataque *man-in-the-middle* es que es indetectable para los usuarios. Siendo este el caso, la cantidad de información que un *hacker* puede obtener en esta situación es limitada sólo por la cantidad de tiempo que éste pueda permanecer en el lugar antes de ser atrapado. La seguridad física de los alrededores es la mejor recomendación para los *ataques man-in-the-middle.*

3.5.5 ATAQUES DE DICCIONARIO Y POR FUERZA BRUTA [6]

Los ataques de diccionario consisten en probar nombres y contraseñas de usuarios hasta acertar con un usuario y contraseña valido. Este método de prueba y ensayo se realiza de forma automática mediante el uso de software diseñado con este fin, el cual toma como fuente diccionarios basados en centenares de millares de palabras, de nombres y de frases. Este tipo de ataques son posibles debido a que muchos usuarios utilizan palabras comunes como nombres y contraseñas en una conexión.

El ataque por fuerza bruta es muy similar al ataque de diccionario, con la diferencia de que en vez de utilizar un listado delimitado emplea todas las combinaciones de caracteres posibles.

Una vez que se ha descifrado un nombre y una contraseña de una conexión válida mediante cualquiera de los dos métodos descritos anteriormente, un *hacker* puede tener acceso libre a la red WLAN con todos los privilegios con que cuente el usuario al que se está atacando.

3.5.6 ATAQUES DE JAMMING [5]

Mientras un *hacker* puede usar un ataque pasivo o activo para obtener información valiosa o ganar acceso a la red, un ataque de *jamming* (introducir a la fuerza), es una técnica usada simplemente para detener la red inalámbrica. Las

redes WLAN pueden ser detenidas mediante el uso de una fuerte señal de radio frecuencia, la cual puede ser intencional, no intencional, removible o no removible.

Cuando un *hacker* perpetúa un ataque intencional de *jamming*, el *hacker* puede usar equipos WLAN, pero lo más probable es que use un generador de señales de radio frecuencia de alto poder o un generador de barrido. La figura 3.3 muestra un ejemplo de ataque de *jamming* en una red WLAN.

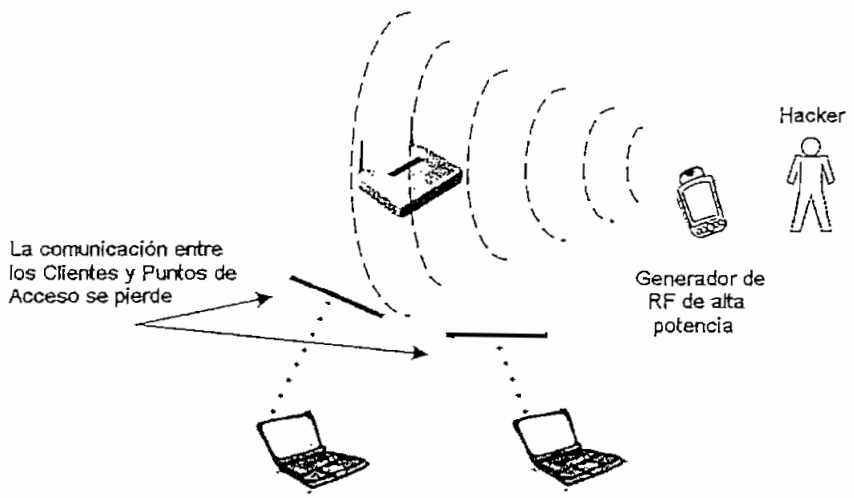


Figura 3.3. Ataque de Jamming en una WLAN

Para remover este tipo de ataques de la red WLAN, primero se requiere localizar la fuente de la señal de RF. La localización de la fuente de la señal de RF se puede realizar mediante el uso de un analizador de espectros. Existen muchos analizadores de espectros en el mercado, pero tener uno que sea portátil y operado por batería es muy útil.

Cuando el *jamming* es causado por una fuente no movible, no maliciosa como una torre de comunicaciones u otro sistema legítimo, el administrador de la red WLAN deberá considerar el hecho de utilizar un nuevo sistema WLAN que utilice un diferente conjunto de frecuencias.

El *jamming* no intencionado ocurre regularmente debido a que muchos dispositivos de diferentes clases y de diferentes industrias comparten la banda

ISM de los 2.4 GHz con las redes WLAN. El *jamming* malicioso no es una amenaza común porque no es muy popular entre los *hackers*, la razón de esto se debe a que es bastante caro montar un ataque (considerando el costo de los equipos que se requieren), y la única victoria que el *hacker* conseguiría es temporalmente deshabilitar a la red.

3.6 SOLUCIONES Y MECANISMOS DE SEGURIDAD PARA REDES WLAN [7]

Actualmente, existen varios tipos de tecnologías que permiten dar seguridad a las redes WLAN. Por ejemplo, se tiene la encriptación que codifica los datos usando técnicas de criptografía y la autenticación que identifica a los usuarios y computadores que tratan de acceder a una red. Como se indica en las siguientes secciones existen varios estándares, métodos y protocolos para cada una de estas tecnologías, los cuales varían el grado de protección e interoperabilidad de la red; entre los más conocidos se tiene:

- ✓ Encriptación WEP
- ✓ Filtros
- ✓ VPNs
- ✓ Estándar 802.11x-EAP
- ✓ Protocolo TKIP
- ✓ Especificación WPA
- ✓ Protocolo AES
- ✓ Estándar IEEE 802.11i
- ✓ Especificación WPA2

3.6.1 ENCRIPTACIÓN WEP [3], [5], [8]

WEP (*Wired Equivalent Privacy;* Privacidad Equivalente a una Cableada), es un algoritmo de encriptación que utiliza un proceso de clave compartida diseñado con el fin de autentificar a los usuarios y proteger los datos que se transmiten sobre un segmento inalámbrico.

WEP es parte del estándar IEEE 802.11, opera a nivel 2 del modelo OSI y es un algoritmo que utiliza PRNG (*Pseudo Random Number Generator*; Generador de Números Seudo Aleatorios) y cifrado de secuencia RC4. Por muchos años el algoritmo RC4 fue considerado un secreto de la industria y sus detalles no estuvieron disponibles, pero en Septiembre de 1994 alguien lo descifró y lo publicó en la red de Internet. Actualmente, el código está disponible y es marca registrada de RSADSI. El cifrado de secuencia RC4 es muy rápido de cifrar y descifrar, lo cual ahorra muchos ciclos del CPU, y es además, bastante simple de implementar en software para la mayoría de desarrolladores.

3.6.1.1 Proceso de Cifrado WEP

Como se puede apreciar en la figura 3.4, el proceso de cifrado WEP en el lado del transmisor se da de la siguiente forma:

- ✓ A la trama sin cifrar se le calcula un código de integridad ICV (*Integrity Check Value*) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.
- ✓ Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede tener 40 o 104 bits (64 o 128 bits tomando en cuenta el vector de inicialización IV).
- ✓ Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas sin cifrar iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización IV (*Initialization Vector*) de 24 bits. El IV cambia con cada trama.
- ✓ La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo-aleatorios denominado WEP PRNG. El generador RC4 puede generar una secuencia seudo-aleatoria tan larga como se desee a partir de la semilla.
- ✓ El WEP PRNG genera una clave de secuencia, del mismo tamaño de la trama a cifrar más 32 bits para cubrir la longitud de la trama y el ICV.

- ✓ Se realiza una operación XOR bit a bit entre la concatenación de la trama y el ICV, con la clave de secuencia; como resultado se obtiene la trama cifrada.
- ✓ En el último paso, la trama cifrada se adiciona al vector de inicialización IV; luego se transmite la información.

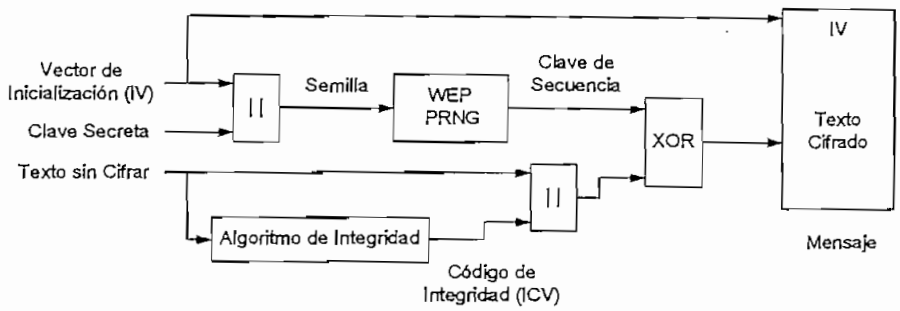


Figura 3.4. Proceso de Cifrado WEP

3.6.1.2 Proceso de Descifrado WEP

Como se puede apreciar en la figura 3.5, el proceso de descifrado WEP en el lado del receptor se da de la siguiente forma:

- ✓ Con el vector de inicialización IV recibido y la clave secreta compartida se genera la semilla que se utilizó en el transmisor.
- ✓ Un generador WEP PRNG produce la clave de secuencia a partir de la semilla (concatenación de la clave secreta y el vector de inicialización IV). Si la semilla coincide con la empleada en la transmisión, la clave de secuencia también será idéntica a la usada en la transmisión.
- ✓ Se efectúa una operación XOR bit a bit de la trama cifrada con la clave de secuencia, obteniéndose de esta forma la trama sin cifrar y el código de integridad ICV.
- ✓ A la trama sin cifrar se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido. Si los dos códigos de integridad ICVs son iguales, la trama se acepta; en caso contrario se rechaza.

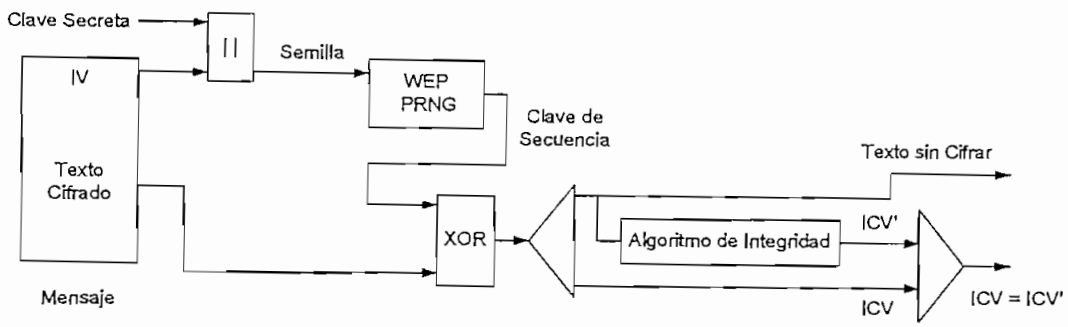


Figura 3.5. Proceso de Descifrado WEP

3.6.1.3 Vulnerabilidades del Algoritmo WEP [3]

El algoritmo WEP resuelve aparentemente el problema de la encriptación de datos entre el transmisor y el receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera como es empleado en la mayoría de aplicaciones:

1. La mayoría de redes instaladas hacen uso de WEP con claves de cifrado estáticas. Es decir, se configura una clave en el punto de acceso y no se la cambia nunca o muy de vez en cuando. Esto hace posible que un atacante acumule grandes cantidades de tramas cifradas con la misma clave y pueda intentar un ataque por fuerza bruta.
2. El vector de inicialización IV que se utiliza es de longitud insuficiente, pues tiene únicamente 24 bits. Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio 2^{24} vectores de inicialización (IVs) distintos. Esto no es problema en una red casera con bajo tráfico, pero en una red que posee alto tráfico se puede agotar el espacio de los IV en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos sin cifrar de ambas tramas. Con el texto sin cifrar de una trama y su respectivo texto cifrado se puede obtener la clave de secuencia y conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

Además de las dos situaciones anteriores, el algoritmo WEP no ofrece el servicio de autenticación, por lo que un cliente no puede autentificarse en la red ni al contrario; basta con que un cliente móvil y el punto de acceso compartan la misma clave WEP para que la comunicación pueda llevarse a cabo.

3.6.2 FILTRADO [5]

El filtrado es un mecanismo básico de seguridad que puede ser usado en adición a WEP. Filtrar significa literalmente mantener fuera a quienes no son deseados y permitir el acceso a quienes si lo son. Existen dos tipos básicos de filtrado que pueden ser implementados en una red WLAN:

1. Filtrado SSID
2. Filtrado de direcciones MAC

3.6.2.1 Filtrado SSID

El Filtrado SSID es un método básico de filtrado, y debería ser usado únicamente para los controles de acceso más básicos. El SSID es utilizado como un nombre de la red y puede tener entre 0 y 32 bytes de longitud. Para que un cliente se autentique y se asocie al conjunto de servicios de una red WLAN, el SSID de una estación debe coincidir con el SSID del punto de Acceso (modo de infraestructura) o de las otras estaciones (modo Ad-Hoc).

El SSID puede ser descubierto muy fácilmente mediante el uso de un *sniffer,* puesto que el SSID se incluye en todos los paquetes de aviso que se envían a través de un punto de acceso o las estaciones de una red WLAN. Por este motivo muchos fabricantes han implementado la opción de quitar el SSID de las tramas de aviso. Cuando éste es el caso, se dice que el sistema está configurado como un "sistema cerrado" y el cliente debe tener igual SSID para asociarse al punto de acceso. El filtrado SSID no es considerado un método confiable para mantener a los usuarios no autorizados fuera de la red WLAN.

Algunos errores comunes que los usuarios de redes WLAN cometen en la administración de SSIDs son:

- ✓ Usan el SSID que viene predeterminado de fábrica en los equipos WLAN.
- ✓ Usan SSIDs que se relacionan con terminología de la empresa o la región.
- ✓ Usan el SSID como un método de seguridad en la WLAN, debiéndose ser utilizado únicamente como un método de segmentación más no como un método de seguridad.
- ✓ Realizan un *broadcast* innecesario del SSID, activando esta opción en los puntos de acceso.

3.6.2.2 Filtrado de direcciones MAC

Las redes WLAN pueden ser filtradas basándose en las direcciones MAC de las estaciones. Casi la mayoría de puntos de acceso tienen la funcionalidad de filtrar direcciones MAC. El administrador de red puede recopilar, distribuir y mantener una lista de las direcciones MAC permitidas y programarlas dentro de cada punto de acceso. Si una tarjeta de una PC u otro cliente con una dirección MAC que no esté en la lista de filtrado del punto de acceso trata de obtener acceso a la WLAN, la funcionalidad del filtro de direcciones MAC no permitirá que el cliente se asocie con el punto de acceso. En la figura 3.6 se puede apreciar lo indicado anteriormente.

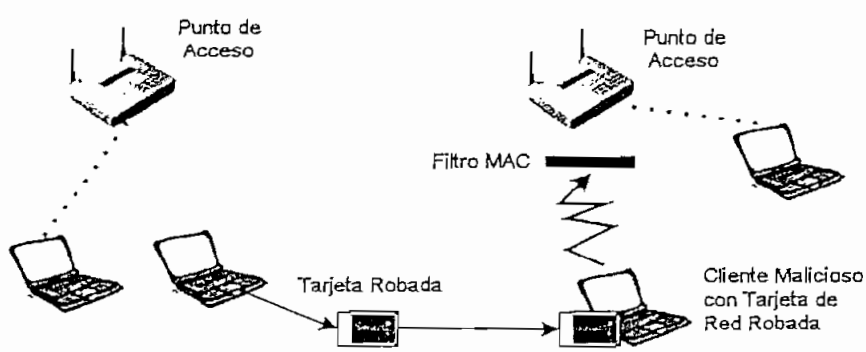


Figura 3.6. Filtrado de Direcciones MAC

A pesar de que los filtros MAC pueden parecer ser un buen método de seguridad

en las redes WLAN, en algunos casos estos filtros todavía son susceptibles a:

- ✓ Robo de una tarjeta de PC que esté en el filtro MAC de un Punto de Acceso.
- ✓ Escucha pasiva de la WLAN para descifrar una dirección MAC para luego emularla mediante software y así acceder a la WLAN fuera de las horas de trabajo. Se puede acceder únicamente fuera de las horas de trabajo, porque las direcciones MAC son únicas y por lo tanto no pueden coexistir dos equipos con direcciones MAC idénticas a la vez.

Los filtros MAC son excelentes para el hogar y redes de pequeñas oficinas donde existe un número pequeño de estaciones y el uso de la red es bajo. La combinación de WEP y filtros MAC provee una adecuada solución de seguridad en estos casos ya que los *hackers* en redes de bajo uso, tendrán que gastar muchas horas para poder romper la encriptación WEP y el filtrado MAC.

3.6.3 VPNs [3], [7]

Una VPN (*Virtual Private Network;* Red Privada Virtual), como su nombre lo indica es una Red Privada Virtual que se crea sobre una red de acceso público para permitir una comunicación privada entre usuarios, oficinas remotas y empresas. Las VPNs otorgan privacidad a través de procedimientos de seguridad que incluyen encriptación, claves de acceso, autenticación y protocolos para la creación de túneles. Estos protocolos verifican usuarios y servidores, cifran y descifran datos, y crean un túnel que no puede ser accedido por datos o usuarios que no estén apropiadamente cifrados o autenticados, respectivamente.

Los protocolos de seguridad que se utilizan en las VPNs son IPSec (*Internet Protocol Security*; Protocolo de Seguridad de Internet), L2TP (*Layer 2 Tunneling Protocol*; Protocolo de creación de Túneles de Capa 2) y PPTP (*Point to Point Tunneling Protocol*; Protocolo de Creación de Túneles Punto a Punto), entre otros. También utilizan protocolos de encriptación tales como Triple DES (3 DES) y AES (*Advanced Encryption Standard*; Estándar de Cifrado Avanzado), los cuales son

mucho más fuertes que los utilizados en el algoritmo de encriptación WEP.

Debido a que las VPNs funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP, éstas resultan especialmente atractivas para proteger las redes inalámbricas. Para configurar una WLAN utilizando VPNs, el segmento de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red mediante el uso de una lista de acceso adecuada en un ruteador o agrupando todos los puertos de acceso inalámbrico en una VLAN (*Virtual Local Area Network;* Red de Área Local Virtual), mediante un *switch*. Esta lista de acceso o VLAN sólo debe permitir el acceso de la estación a los servidores de la VPN. Únicamente en el caso de que la estación sea debidamente autorizada y autenticada, la estación tendrá un acceso completo. En la figura 3.7 se puede apreciar la estructura de una VPN básica.

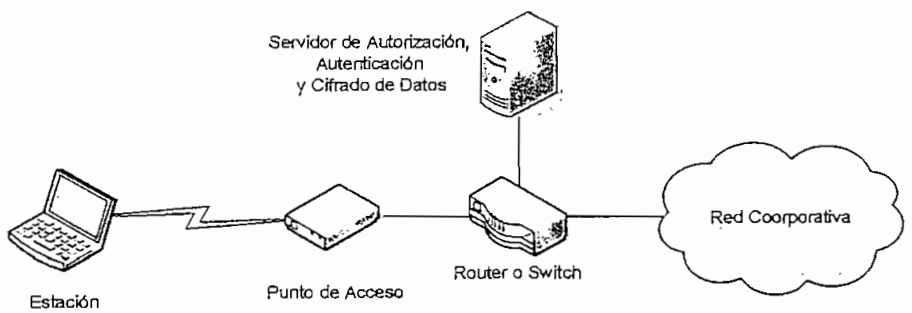


Figura 3.7. Estructura de una VPN para una WLAN

Los servidores de una VPN son servidores de autenticación y encriptación que se encargan de autenticar a las estaciones y cifrar todo el tráfico desde y hacia dichos clientes. Algunos fabricantes de equipos para redes WLAN incluyen el software de servidor VPN en sus puntos de acceso, permitiendo que la tecnología VPN sea implementada sin la necesidad de hardware adicional. Cuando el servidor VPN es implementado dentro del punto de acceso, las estaciones deben utilizar el software dado por el fabricante para primeramente asociarse con el punto de acceso y luego establecer la VPN. Una solución de este tipo se puede apreciar en la figura 3.8.

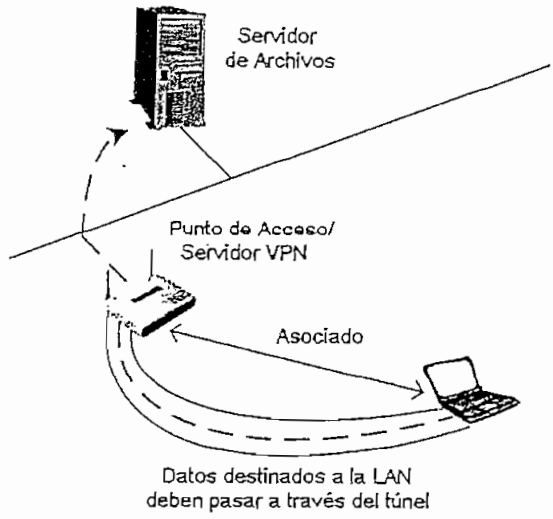


Figura 3.8. VPN con Servidor dentro del Punto de Acceso

3.6.4 EL ESTÁNDAR 802.1x Y EL PROTOCOLO EAP [3], [8], [9], [10]

El Estándar 802.1x fue creado por la IEEE en sus inicios para el uso en redes LAN cableadas, pero actualmente ha sido incorporado por muchos fabricantes dentro de los sistemas WLAN. Este estándar define el control de acceso basándose en puertos, es decir controla el acceso en el punto en el cual el usuario se acopla a la red. Cuando un usuario desea acceder a la red a través de un puerto mediante 802.1x, este puerto pone la conexión del usuario en modo bloqueado en espera de la verificación de la identidad del usuario mediante un sistema de autenticación.

El Estándar 802.1x divide al universo de la red dentro de tres entidades:

1. El Suplicante o Equipo del Cliente, que desea conectarse con la red.
2. El Servidor de Autorización y Autenticación (El Estándar 802.1x fue diseñado para emplear servidores RADIUS), que contiene toda la información necesaria para saber cuales equipos y/o usuarios están autorizados para acceder a la red.
3. El Autenticador, que es el equipo de red (como un *switch*, un ruteador, un punto de acceso), el cual actúa como intermediario entre el suplicante y el servidor de autenticación recibiendo la conexión del suplicante.

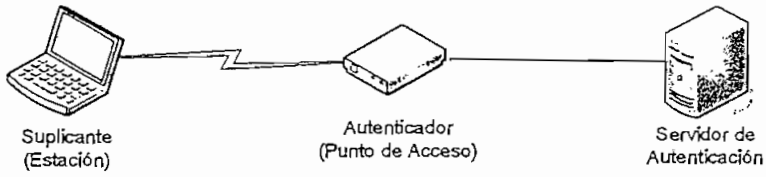


Figura 3.9. Arquitectura de un Sistema de Autenticación 802.1x

Cuando el Estándar 802.1x se combina con el protocolo EAP (*Extensible Authentication Protocol;* Protocolo de Autenticación Extensible) puede proveer un ambiente muy seguro y flexible basado en muchos escenarios de autenticación que se usan hoy en día.

El protocolo EAP definido inicialmente como parte del protocolo PPP (*Point to Point Protocol;* Protocolo Punto a Punto), es un protocolo para autenticación que soporta múltiples métodos de autenticación como MD5, Kerberos, *One Time Password*, certificados, autenticación de claves públicas y tarjetas inteligentes.

3.6.4.1 Proceso de Autenticación 802.1x-EAP

Como se puede apreciar en la figura 3.10, la autenticación del cliente se lleva a cabo mediante el protocolo EAP y el servidor RADIUS de la siguiente forma:

- ✓ El proceso inicia cuando la estación de trabajo se enciende y logra asociarse con un punto de acceso. En ese momento, el punto de acceso bloquea el paso de tráfico normal y lo único que admite es tráfico EAPOL (*EAP over LAN*), que es el requerido para efectuar la autenticación.
- ✓ La estación envía un mensaje *EAPOL-Start* al punto de acceso, indicando que desea iniciar el proceso de autenticación.
- ✓ El punto de acceso contesta a la estación solicitando que se identifique mediante un mensaje *EAP-Request-Identity.*
- ✓ La estación se identifica enviando un mensaje *EAP-Response-Identity* al punto de acceso.
- ✓ Una vez recibida la información de identidad, el punto de acceso envía un mensaje *RADIUS-Access-Request* al servidor de autenticación y le pasa

los datos básicos de identificación del cliente.

- ✓ El servidor de autenticación responde con un mensaje *RADIUS-Access-Challenge*, en el cual envía un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje *EAP-Request.*
- ✓ El cliente da respuesta al desafío mediante un mensaje *EAP-Response (Credentials)* dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje *RADIUS-Access-Response.*
- ✓ Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje *RADIUS-Access-Accept*, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además envía un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre le cliente y el punto de acceso. El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente, para evitar el problema de descubrimiento de clave que tiene WEP.
- ✓ El autenticador envía un mensaje *EAP-Success* al cliente y abre el puerto para que el cliente puede acceder a la red.

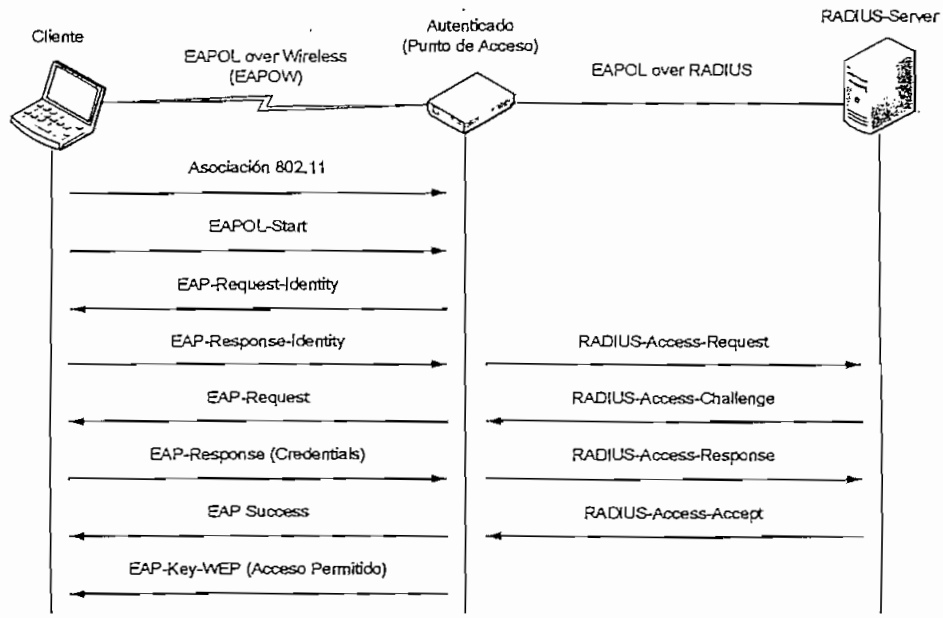


Figura 3.10. Proceso de Autenticación 802.1x-EAP

3.6.5 PROTOCOLO TKIP [5]

El protocolo TKIP (*Temporal Key Integrity Protocol;* Protocolo de Integridad de Clave Temporal), es un protocolo diseñado para mejorar las deficiencias del algoritmo WEP especialmente el reuso de las claves de encriptación. TKIP provee un vector de inicialización segmentado en varias partes y el uso de claves dinámicas para evitar los ataques pasivos. También provee un MIC (*Message Integrity Check;* Chequeo de Integridad en el Mensaje) para ayudar a determinar si un usuario no autorizado ha modificado los paquetes luego de la transmisión.

TKIP puede ser implementado a través de mejoras en el *firmware* y software de puntos de acceso, *bridges*, y dispositivos inalámbricos de los clientes. El uso de TKIP produce un desempeño bajo de la red, pero este decremento del desempeño puede ser recompensado si se considera la seguridad que se obtiene en la red.

El proceso TKIP comienza con una clave temporal de 128 bits que es compartida entre todos los clientes y puntos de acceso. Esta clave temporal es luego combinada con la dirección MAC del cliente y agregada al vector de inicialización (IV), que en este caso es de 16 Bytes (a diferencia de los 24 bits que utiliza WEP), para generar la clave de encriptación actual. Mediante el uso de este proceso, TKIP asegura que cada estación use diferentes claves de secuencia para la encriptación de datos. Para realizar la encriptación de datos TKIP hace uso del algoritmo RC4 al igual que WEP, de este modo TKIP es en cierta forma compatible con la encriptación WEP. TKIP para mejorar aún más la seguridad en la red, cambia cada diez mil (10000) paquetes la clave temporal de 128 bits en un período corto de tiempo el cual puede ser menos de una hora en muchos casos.

La mayoría de hardware existente en el mercado (no todos) puede ser actualizado para el uso de TKIP a través de una actualización del *firmware*. Sin embargo, los puntos de acceso que manejen TKIP, todavía pueden dar servicios a clientes WEP, pero esto no es recomendado porque introduciría un desperfecto de seguridad dentro de la red.

3.6.6 ESPECIFICACIÓN WPA [11], [12]

WPA (*Wi-Fi Protected Access;* Acceso Protegido para Wi-Fi) es una especificación propuesta por los miembros de la Alianza Wi-Fi en colaboración con la IEEE para incrementar los niveles de protección de datos y control de acceso de las actuales y futuras redes Wi-Fi, eliminando las conocidas debilidades de WEP que es el mecanismo de seguridad original del Estándar IEEE 802.11. Esta especificación fue lanzada oficialmente en el mes de octubre del 2003.

Wi-Fi Protected Access está diseñado para ser compatible con todas las versiones de dispositivos 802.11, incluyendo 802.11b. 802.11a y 802.11g mediante una actualización de su software y con los nuevos dispositivos que se rijan según el estándar IEEE 802.11i (El Estándar IEEE 802.11i es una corrección al estándar 802.11, que especifica mecanismos de seguridad para redes inalámbricas). *Wi-Fi Protected Access* es compatible con el estándar IEEE 802.11i debido a que surgió como un subconjunto del *draft* (anteproyecto) 802.11i, tomando ciertas partes de éste, como es el caso de la implementación de 802.1x y TKIP.

Para solucionar el problema de cifrado de datos, *Wi-Fi Protected Access* propone como nuevo protocolo de cifrado, el protocolo TKIP (*Temporary Key Integrity Protocol*), y un mecanismo de autenticación que emplea 802.1x y EAP, los cuales ya fueron descritos en las secciones anteriores.

Según la complejidad de la red, *Wi-Fi Protected Access* puede funcionar en dos modos:

1. Modo Empresarial
2. Modo Personal

3.6.6.1 Modo Empresarial

La especificación WPA trata con mayor eficiencia los requerimientos de seguridad para las redes empresariales, proveyendo una encriptación más fuerte y un mecanismo de autenticación en forma previa a la ratificación del estándar IEEE 802.11i. En una red empresarial, WPA debe ser usado conjuntamente con un servidor de autenticación, como es el caso de un servidor RADIUS para un control de acceso y administración centralizada. De esta forma el punto de acceso emplea 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

3.6.6.2 Modo Personal [13]

El modo personal o PSK (*Pre-Shared Key*) está diseñado para usuarios del hogar y *Small Office/Home Office* (SOHO), en donde no se dispone de un servidor de autenticación en la red. En esta modalidad se requiere introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles en forma manual. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), puesto que se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

3.6.7 PROTOCOLO AES [5], [14], [15]

AES (*Advanced Encryption Standard;* Estándar de Encriptación Avanzada), también conocido como *Rijndael*, es un cifrado de bloque adoptado como un estándar de encriptación por el gobierno de los Estados Unidos. Este estándar fue adoptado por la NITS (*National Institute of Standards and Technology;* Instituto nacional de Estándares y Tecnología) en Noviembre del 2001 después de un proceso de estandarización de 5 años.

El cifrado fue implementado por dos Criptógrafos Belgas, Joan Daemen y Vincent Rijmen, y sometido al proceso de selección de AES bajo el nombre de *Rijndael.* AES es muy fácil de implementar tanto en hardware como en software y requiere de un bajo uso de memoria.

AES utiliza claves de tamaño fijo de 128 bits, 192 bits y 256 bits, y opera en un arreglo de 4 x 4 bytes llamado estado. El proceso de encriptación de cada ronda, excepto la última, explicado en una forma breve es el siguiente:

1. Sustitución de Bytes, donde cada byte del estado es reemplazado con otro de acuerdo a una tabla dada.

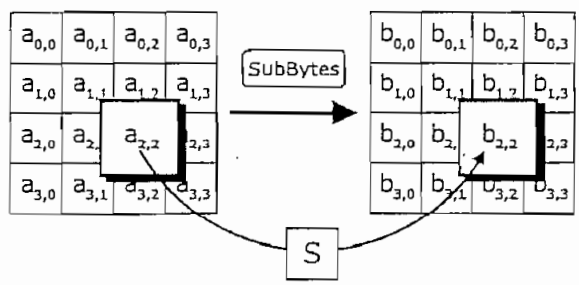


Figura 3.11. Substitución de Bytes

2. Desplazamiento de Filas, donde cada fila del estado es desplazada cíclicamente hacia la izquierda. El número de veces que cada byte es desplazado es diferente para cada fila.

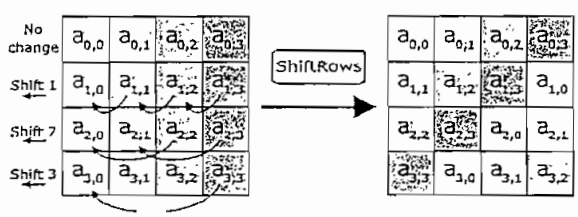


Figura 3.12. Desplazamiento de Filas

3. Mezcla de columnas, donde cada columna del estado es multiplicada por un polinomio constante.

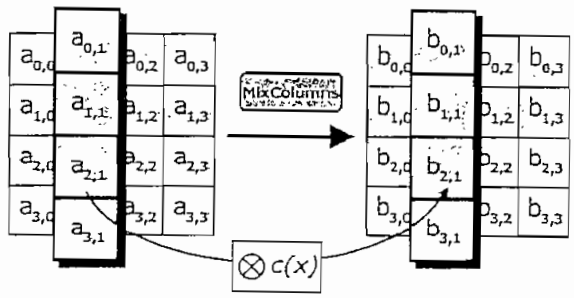


Figura 3.13. Mezcla de Columnas

4. Agregación de una clave a la ronda, donde cada byte del estado es combinado con un byte de una subclave mediante una operación XOR. La subclave que es del mismo tamaño que el estado, se deriva de la clave principal mediante un cronograma de claves.

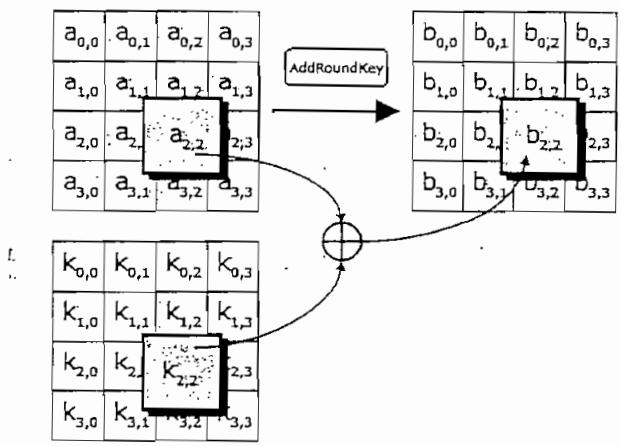


Figura 3.14. Agregación de una Clave a la Ronda

3.6.8 EL ESTÁNDAR IEEE 802.11i [8] [16] [17]

El estándar *IEEE* 802.11i es el estándar más reciente de la IEEE para proporcionar seguridad en redes WLAN, el cual fue aprobado en Junio del 2004. Este estándar especifica una encriptación más fuerte, dos métodos de autenticación y además agrega estrategias de administración de claves. Entre estos nuevos componentes se tiene:

- ✓ Hace uso del protocolo TKIP (*Temporal Key Integrity Protocol*) y el

protocolo AES (*Advanced Encryption Standard*) en conjunto con CCMP (*Counter-Model/CBC-MAC Protocol*), para el proceso de autenticación.

- ✓ Hace uso de un sistema de distribución de claves mediante IEEE 802.1x-EAP, para el control de acceso a la red.
- ✓ Un proceso de negociación para seleccionar correctamente tanto el protocolo de confidencialidad como los sistemas de claves, para cada tipo de tráfico (*unicast* y *broadcast*).
- ✓ Almacenamiento de claves, que permite a los clientes realizar *roaming* de un lado a otro entre diferentes puntos de acceso (a los cuales ya se han asociado previamente), sin la necesidad de iniciar de nuevo todo el proceso de autenticación. Con esto, el tiempo para lograr conectarse a la red, se reduce.
- ✓ Pre-autenticación, que permite a los clientes que ya se hayan asociado a la red, realizar *roaming* a través de puntos de acceso (a los cuales aún no se han asociado), sin la necesidad de iniciar nuevamente todo el proceso de autenticación.

El CCMP (*Counter-Mode/CBC-MAC Protocol*), es un protocolo de confidencialidad de datos que maneja autenticación de paquetes y cifrado. Para la confidencialidad, CCMP utiliza el estándar AES *(Advanced Encryption Standard)* en modo inverso con una clave de 128 bits y para la autenticación e integridad, hace uso de un método llamado CBC-MAC (*Cipher Block Chaining Message Authentication Code*).

3.6.9 ESPECIFICACIÓN WPA2 [18], [19], [20], [21]

El estándar *Wifi-Protected Access 2* (WPA2), fue lanzado oficialmente en Septiembre del 2004 y es la última generación en estándares de seguridad de la Alianza Wi-Fi. WPA2 combina las técnicas actuales más poderosas de autenticación y encriptación para proteger las redes inalámbricas de usuarios no autorizados. Basado en el estándar IEEE 802.11i que fue recientemente ratificado en Junio del 2004, WPA2 agrega AES (*Advanced Encryption Standard*), a la especificación original *Wifi-Protected Access* (WPA) para entregar el más alto

nivel de seguridad disponible.

Wifi-Protected Access 2 (WPA2), está diseñado para ser compatible con el estándar original WPA. Ambos estándares utilizan las técnicas de autenticación IEEE 802.1x y EAP, pero WPA2 suplanta a la encriptación original de WPA, el *Temporal Key Integrity Protocol* (TKIP) con una herramienta de encriptación más poderosa, el *Advanced Encryption Standard* (AES).

Todos los productos Wi-Fi certificados con WPA2 pueden interoperar con los productos certificados con WPA. Algunos productos WPA tienen la capacidad de ser actualizados a WPA2 mediante una actualización de software. Sin embargo muchos otros requieren necesariamente un cambio de hardware, para poder ejecutar los algoritmos de encriptación que exige AES.

El hecho de que WPA2 sea el estándar más reciente y sea parte del estándar IEEE 802.11i, hace que WPA2 probablemente sea adoptado por la mayoría de usuarios de redes WLAN. Sin embargo, WPA continuará jugando un papel muy valioso dentro de las necesidades de seguridad para muchos usuarios Wi-Fi.

Al igual que en WPA, *Wi-Fi Protected Access 2* puede funcionar en dos modos:

- ✓ Modo Empresarial
- ✓ Modo Personal

3.6.9.1 Modo Empresarial

En una red empresarial, WPA2 debe ser usado conjuntamente con un servidor de autenticación, como es el caso de un servidor RADIUS para un control de acceso y administración centralizada. De esta forma el punto de acceso emplea 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

3.6.9.2 Modo Personal

WPA2 también opera en modo personal o PSK (*Pre-Shared Key*), para redes caseras y redes SOHO en las cuales no se dispone de un servidor de autenticación. Para esto se requiere introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles en forma manual. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, AES (*Advanced Encryption Standard*) entra en funcionamiento para garantizar la seguridad del acceso.

BIBLIOGRAFÍA CAPÍTULO III

[1] CISCO NETWORKING ACADEMY PROGRAM. Fundamentals of Wireless LANs. V1.0.

[2] SeguridadWireless.pdf: Seguridad en Redes Inalámbricas.

[3] Jamdrid-seguridad_redes_inalambricas.pdf: Seguridad en Redes Inalámbricas.

[4] http://en.wikipedia.org/wiki/Warchalking: Warchalking.

[5] CERTIFIED WIRELESS NETWORK ADMINISTRATOR. Official Study Guide. MacGraw-Hill. Second Edition. 2003.

[6] http://www.canal-ayuda.org/Seguridad/tipos_ataques.htm: Clasificación y Tipos de Ataques Contra Sistemas de Información.

[7] WLAN_Security_Concepts.pdf: Wireless LAN Security.

[8] Addison Wesley - Real 802.11 Security Wi-Fi Protected Access And 802.11I Sharereactor.pdf: Real 802.11 Security: Wi-Fi Protected Access and 802.11i.

[9] http://www.faqs.org/rfcs/rfc2284.html: RFC 2284 - PPP Extensible Authentication Protocol.

[10] http://www.iec.org/online/tutorials/acrobat/eap_methods.pdf: EAP Methods for 802.11 Wireless LAN Security.

[11] http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf: Wi-Fi Protected Access.

[12] http://www.weca.net/opensection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf: Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks.

[13] http://www.stargeek.com/item/20270.html: WPA's Little Secret.

[14] http://www.criptored.upm.es/descarga/Laredo_jgg2.zip. Las Redes Substitución - Permutación y el AES (Advanced Encryption Standard).

[15] http://www.kriptopolis.com/rijndael.pdf: Algoritmo Criptográfico Rijndael.

[16] http://standards.ieee.org/getieee802/download/802.11i-2004.pdf: IEEE Std 802.11i-2004.

[17] http://www.embedded.com/showArticle.jhtml?articleID=34400002: IEEE 802.11i and wireless security.

[18] http://www.wi-

fi.org/OpenSection/ReleaseDisplay.asp?TID=4&ItemID=181&StrYear=2004&st rmonth=9: Wi-Fi Alliance Introduces Next Generation of Wi-Fi Security.

[19] http://www.weca.net/opensection/pdf/memberprs/sep04/pr_bw_wpa2_pr_fin al.pdf: Broadcom Wireless LAN Solutions Wi-Fi CERTIFIED for WPA2.

[20] http://www.weca.net/opensection/pdf/wpa2_q_a.pdf: Questions and Answers.

[21] http://www.weca.net/opensection/pdf/WFA_02_27_05_WPA_WPA2_White _Paper.pdf: Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise.

CAPÍTULO IV

4 SITUACIÓN ACTUAL DEL PROVEEDOR DE SERVICIOS DE INTERNET INALÁMBRICO

4.1 INTRODUCCIÓN

El ISP (*Internet Service Provider*; Proveedor de Servicios de Internet) que se ha tomado como caso de estudio en el presente proyecto se trata de una pequeña empresa proveedora de servicios de Internet que cuenta con una oficina central y dos oficinas locales. La oficina principal se encuentra en la ciudad de Quito y las dos sucursales en la ciudad de Guayaquil y Cayambe respectivamente. En los actuales momentos este ISP presta el servicio de Internet Corporativo en las localidades de Quito y Cayambe, y el servicio de Transmisión de Datos exclusivamente a una entidad financiera, e Internet dedicado en la ciudad de Guayaquil.

Para estos dos tipos de servicios que el ISP está prestando, en la mayoría de sus accesos de última milla se utilizan enlaces inalámbricos mediante redes WLANs según el estándar IEEE 802.11b, incluso los enlaces principales o de *backbone* están utilizando esta tecnología como se describe más adelante.

La razón de la decisión del uso de la tecnología WLAN IEEE 802.11b en los enlaces inalámbricos se debe exclusivamente a los bajos costos que demandan los dispositivos que manejan esta tecnología, ya que estos enlaces trabajan en frecuencias que no necesitan licencias para su uso, sino únicamente tener registrado cada uno de los enlaces que trabajen en estas frecuencias ante el ente regulador.

Por razones de seguridad, políticas de la empresa y principalmente debido a que la mayoría de problemas que se presentan y se pueden presentar a futuro están

en la red de la ciudad de Quito, se toma como caso de estudio únicamente a esta red. Cabe destacar además que existe total independencia entre las tres sucursales del ISP: Quito, Guayaquil y Cayambe, por lo que el estudio de la red de Quito no se verá afectado por las otras dos sucursales.

En sus inicios el ISP, nació como una empresa para prestar únicamente servicios locales en al área urbana de la ciudad de Quito, sin embargo debido a la constante demanda del servicio, éste se ha ido expandiendo. Como no ha existido una planificación previa para solventar todos los problemas de crecimiento, se ha tenido que resolver cada uno de estos de una manera no coordinada ni planificada menos aún proyectada hacia el futuro.

Toda esta falta de planificación ha llevado a la empresa actualmente a un riesgo muy grave, debido a que el servicio se encuentra muy afectado por fallas en la infraestructura de la red, lo que repercute inmediatamente en el cliente debido a una baja calidad de servicio que se le presta.

El objetivo principal de este trabajo es describir los cambios óptimos que se deben realizar a la infraestructura para resolver los problemas actuales y así poder entregar un servicio de calidad y además que permita que los nuevos clientes en el futuro vayan accediendo al servicio sin ningún inconveniente.

En las siguientes secciones se describe la infraestructura actual del ISP y la función de sus componentes, para lo cual primeramente se realiza una breve introducción de los dispositivos más importantes que se utilizan en las redes WLAN.

4.2 ANTENAS DE RADIO FRECUENCIA PARA DISPOSITIVOS WLAN [1]

Una antena de RF es un dispositivo usado para convertir señales de alta frecuencia que viajan sobre líneas de transmisión (cables o guías de onda) a ondas electromagnéticas que se propagan a través del aire y viceversa.

El campo electromagnético emitido por las antenas se determina por su lóbulo de radiación. Según cómo las antenas irradian la energía, estos elementos se pueden clasificar dentro de tres categorías genéricas:

1. Antenas omni-direccionales
2. Antenas semi-direccionales
3. Antenas altamente-direccionales

Como se indica más adelante, dentro de estas tres categorías existen múltiples tipos de antenas, cada una de las cuales tienen diferentes características de RF y usos apropiados.

4.2.1 ANTENAS OMNI-DIRECCIONALES (DIPOLOS)

Las antenas omni-direccionales o dipolos son unas de las antenas más comunes en los dispositivos WLAN. Este tipo de antenas se denominan omni-direccionales porque irradian energía de igual forma en todas las direcciones alrededor de su eje. La figura 4.1 muestra ejemplos de diferentes tipos de antenas omni-direccionales.

Figura 4.1. Antenas Omni-direccionales

Las antenas omni-direccionales de alta ganancia ofrecen una mayor área de cobertura horizontal, pero la cobertura vertical es reducida. Esto se puede apreciar en la figura 4.2.

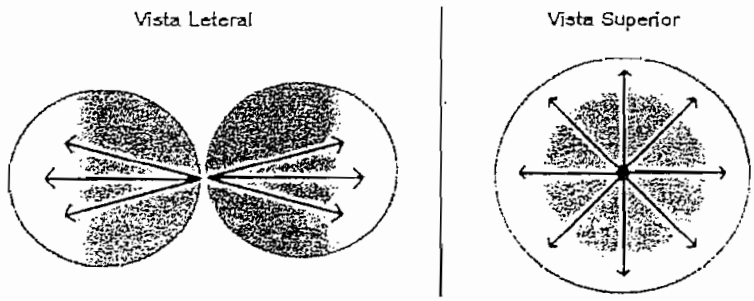


Figura 4.2. Radiación Antenas Omni-direccionales

Las antenas omni-direccionales son usadas cuando se necesita cobertura en todas las direcciones alrededor del eje de la antena. En ambientes internos se las utiliza para proveer cobertura en salones abiertos y en ambientes externos se las utiliza para entregar enlaces punto a multipunto con topología tipo estrella.

4.2.2 ANTENAS SEMI-DIRECCIONALES

Las antenas semi-direccionales dirigen la energía del transmisor en una dirección en particular más significativamente, antes que en forma uniforme. El patrón de radiación de este tipo de antenas se puede apreciar en la figura 4.3.

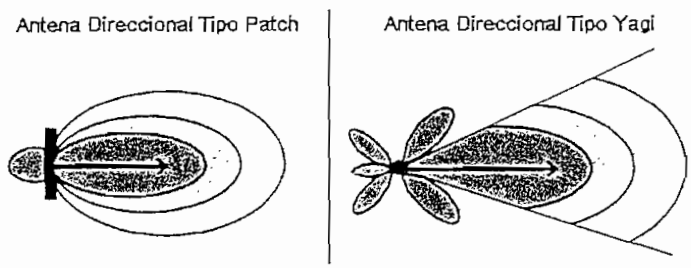
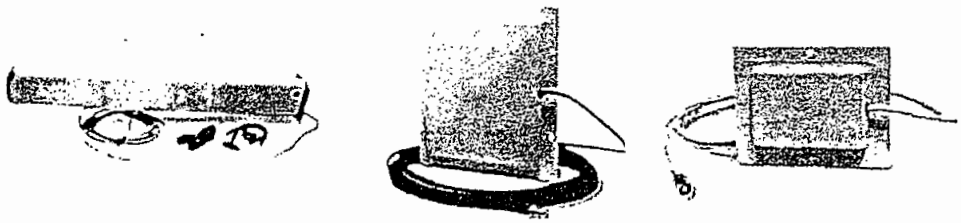


Figura 4.3. Patrón Radiación Antenas Semi-direccionales

Las antenas semi-direccionales vienen en diferentes estilos y formas. Algunos de los tipos de antenas semi-direccionales frecuentemente usados con dispositivos WLAN son antenas tipo *patch*, tipo *panel* y tipo *yagi*, cada una de las cuales tienen sus propias características de cobertura. Todas estas antenas son generalmente planas y están diseñadas para ser montadas sobre paredes. La figura 4.4 muestra algunos ejemplos de antenas semi-direccionales.



Antena Tipo Yagi Antena Tipo Patch Antena Tipo Panel

Figura 4.4. Antenas Semi-direccionales

Las antenas semi-direccionales, en ambientes externos son utilizadas generalmente para *bridging* de corto y mediano alcance como por ejemplo para enlazar dos edificios no muy distantes. En ambientes internos grandes, si el transmisor se coloca en la esquina del sitio o en un corredor, la antena semi-direccional puede proveer una excelente cobertura.

Las antenas tipo *yagi* son por lo general utilizadas para proveer enlaces punto a punto de hasta 3.3 km. Las antenas tipo *patch* y tipo *panel* son usadas más típicamente en enlaces punto a punto de corto alcance y enlaces direccionales dentro de edificaciones.

4.2.3 ANTENAS ALTAMENTE DIRECCIONALES

Como su nombre lo indica, las antenas altamente-direccionales emiten la señal en un haz muy estrecho y se caracterizan por tener una alta ganancia, que va desde unos discretos 15 dBi, llegando en los modelos superiores hasta los 24 dBi. Cuanta más alta es la ganancia de este tipo de antenas, más alta es su direccionalidad, ya que se reduce muchísimo el ángulo en el que irradian la señal, llegando a ser tan estrechos como 8 grados de apertura. Las antenas altamente direccionales son formadas por platos cóncavos (parabólicos), como se puede apreciar en la figura 4.5.

Las antenas altamente direccionales no tienen un área de cobertura adecuada para que los dispositivos clientes la puedan utilizar. Estas antenas son exclusivamente utilizadas para enlaces punto a punto, los cuales pueden

transmitir a distancias de hasta 42 km.

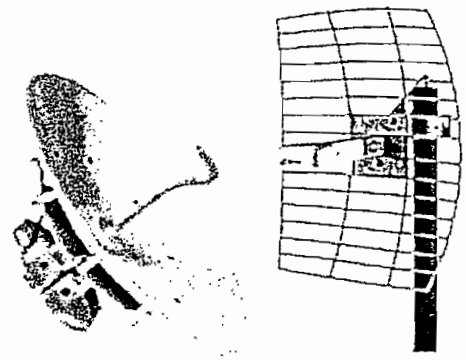


Figura 4.5. Antenas Altamente-direccionales

4.2.4 CABLE PIGTAIL

El *pigtail* no es más que un pequeño cable, que sirve de adaptación entre la tarjeta de red inalámbrica, un punto de acceso o un bridge y la antena o el cable que va hacia la antena. Este *pigtail* tiene 2 conectores: el propietario de cada tarjeta en un extremo, y por el otro un conector tipo N estándar en la mayoría de los casos. Estas características se pueden apreciar en la figura 4.6.

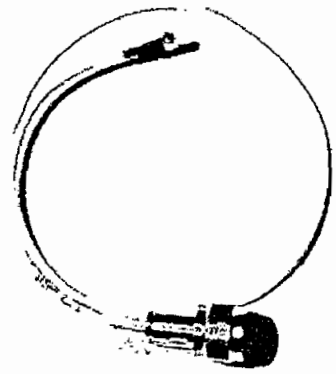


Figura 4.6. Cable Pigtail

El *pigtail* depende del fabricante de la tarjeta por lo que no es un elemento estándar. El uso de este cable es imprescindible para conectar una antena a la tarjeta, salvo en algunos modelos de antenas diseñadas expresamente para

usarse en interiores en los cuales el conector ya viene incluido desde fábrica.

4.3 DISPOSITIVOS ACTIVOS EN REDES WLAN [1]

En esta sección se revisan algunos de los tipos de equipos más importantes para la consolidación de una infraestructura de red WLAN. Entre los equipos WLAN más comunes e importantes dentro de una red WLAN, se tiene:

- ✓ Puntos de acceso
- ✓ *Bridges* inalámbricos
- ✓ *Workgroup bridges* inalámbricos
- ✓ Dispositivos clientes
- ✓ *Gateways* inalámbricos

4.3.1 PUNTOS DE ACCESO

Un punto de acceso es un dispositivo *half duplex* con una capacidad equivalente a la de un sofisticado switch *Ethernet*, el cual permite la comunicación de varios dispositivos inalámbricos entre sí y/o con una red cableada. Estos puntos de acceso son los dispositivos más comunes luego de las tarjetas de red inalámbricas de los clientes dentro de una red WLAN. En la figura 4.7 se pueden apreciar algunos puntos de acceso de distintos fabricantes

Figura 4.7. Puntos de Acceso

4.3.1.1 Modos de Configuración de un Punto de Acceso

La mayoría de puntos de acceso de diferentes fabricantes (no todos), pueden comunicarse con clientes inalámbricos, con la red cableada y con otros puntos de acceso mediante tres modos de configuración:

1. Modo raíz
2. Modo puente
3. Modo repetidor

4.3.1.1.1 Modo Raíz

El modo raíz se configura cuando un punto de acceso se conecta a la red cableada a través de su interfaz *Ethernet*. La mayoría de puntos de acceso que soportan otros modos de configuración, vienen configurados en este modo por defecto.

Este modo de configuración también se utiliza cuando varios puntos de acceso se conectan a un mismo sistema de distribución cableado para permitir *roaming* entre los clientes inalámbricos. En la figura 4.8 se puede apreciar dos puntos de acceso funcionando en modo raíz.

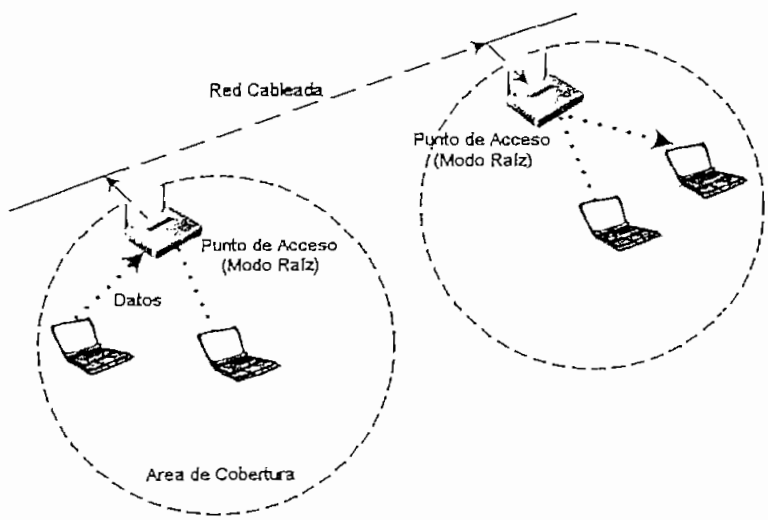


Figura 4.8. Puntos de Acceso en Modo Raíz

4.3.1.1.2 Modo Puente

En el modo puente los puntos de acceso actúan exactamente como *bridges* inalámbricos, los cuales se discuten en una de las secciones más adelante. Solamente algunos puntos de acceso permiten este modo de configuración en el cual no permiten que se asocien clientes inalámbricos, sino más bien son usados para enlazar entre si, dos o más segmentos de red en forma inalámbrica. En la figura 4.9 se puede apreciar dos puntos de acceso operando en este modo.

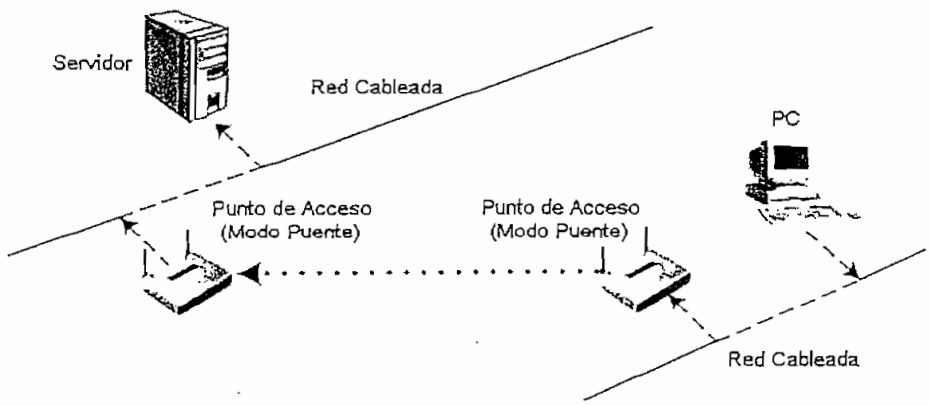


Figura 4.9. Puntos de Acceso en Modo Puente

4.3.1.1.3 Modo Repetidor

En el modo repetidor, los puntos de acceso lo que hacen es expandir el segmento inalámbrico para llegar a sitios más alejados. Este modo de operación no es muy recomendado, ya que la cobertura de los dos puntos de acceso se traslapa en un mínimo del 50% reduciendo su capacidad, además la velocidad de transmisión disminuye y la latencia aumenta en el segmento inalámbrico. En la figura 4.10 se puede apreciar un punto de acceso funcionando en este modo.

4.3.1.2 Características Comunes

Los puntos de acceso existentes en el mercado poseen muchas características tanto en hardware como en software, entre las características más comunes se tiene:

- ✓ Antenas fijas o desmontables
- ✓ Capacidades de filtrado avanzado
- ✓ Tarjetas de radio removibles
- ✓ Potencia de salida variable

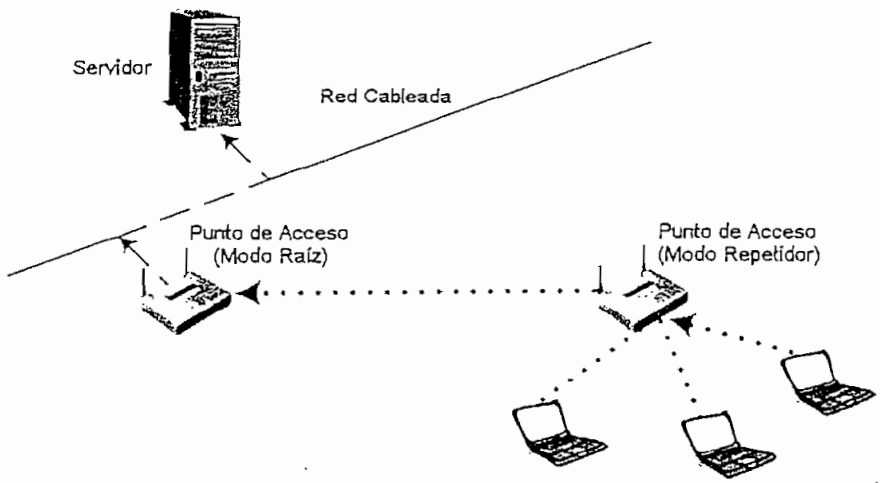


Figura 4.10. Punto de Acceso en Modo Repetidor

4.3.1.2.1 Antenas Fijas o Desmontables

Los puntos de acceso tienen antenas fijas o antenas desmontables. Los puntos de acceso con antenas desmontables permiten que se les adapten antenas diferentes usando para esto cualquier longitud requerida de cable.

También los puntos de acceso pueden venir con o sin diversidad de antenas. La diversidad de antenas permite el uso de múltiples antenas con múltiples entradas en un simple receptor para muestrear de mejor manera las señales que llegan al punto de acceso.

4.3.1.2.2 Capacidades Avanzadas de Filtrado

Algunos fabricantes incorporan filtros MAC y filtros de protocolos dentro de los puntos de acceso. Los filtros MAC, son un método básico de seguridad que permite discriminar y mantener fuera de la red WLAN a usuarios no deseados.

Los filtros de protocolos permiten a los administradores discernir y controlar el tráfico que pasa a través del enlace inalámbrico en función del tipo de protocolos que generan este tráfico.

4.3.1.2.3 Tarjetas de Radio Removibles

Algunos fabricantes permiten agregar y remover radios de ranuras PCMCIA (*Personal Computer Memory Card International Association;* Asociación Internacional de Tarjetas de Memoria para Computadores Personales), incorporadas en los puntos de acceso. Ciertos puntos de acceso pueden tener hasta dos ranuras de radio, permitiendo de esta forma que una tarjeta de radio actúe como punto de acceso mientras que la otra actué como bridge.

Otro uso que se da, es utilizar a cada tarjeta de radio como un punto de acceso diferente, para lo cual se debe configurar cada tarjeta en canales no solapados, normalmente en el canal 1 y 11 respectivamente.

4.3.1.2.4 Potencia de Salida Variable

Esta opción de los puntos de acceso permite a los administradores controlar la potencia que el punto de acceso utiliza para transmitir los datos. Esto puede ser necesario en algunas situaciones donde los dispositivos distantes no pueden localizar al punto de acceso. También esta opción puede ser útil para disminuir el área de cobertura del punto de acceso al disminuir su potencia, como un mecanismo de seguridad.

4.3.2 BRIDGES INALÁMBRICOS

Un bridge inalámbrico al igual que los puntos de acceso son dispositivos *half duplex* los cuales proveen conectividad inalámbrica entre dos segmentos de red cableada. Generalmente son utilizados en configuraciones punto a punto y punto a multipunto. En la figura 4.11 se puede apreciar dos *bridges* inalámbricos de distintos fabricantes.

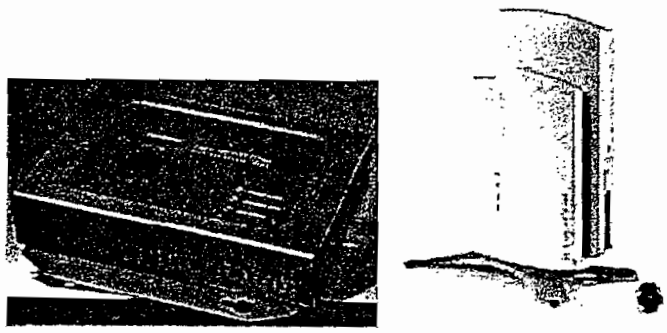


Figura 4.11. Bridges Inalámbricos

4.3.2.1 Modos de Configuración de un Bridge Inalámbrico

Los bridges inalámbricos pueden comunicarse con otros bridges inalámbricos a través de cuatro modos:

1. Modo raíz
2. Modo no raíz
3. Modo punto de acceso
4. Modo repetidor

4.3.2.1.1 Modo Raíz

Un bridge inalámbrico debe ser configurado en modo raíz, dentro de un grupo de bridges inalámbricos. Un bridge inalámbrico en modo raíz solo puede comunicarse con bridges inalámbricos configurados en modo no raíz y otros dispositivos inalámbricos clientes, y no se puede asociar con otro bridge en modo raíz. En la figura 4.12 se puede apreciar un bridge en modo raíz comunicándose con bridges en modo no raíz.

4.3.2.1.2 Modo No Raíz

Los bridges inalámbricos en modo no raíz, se conectan en forma inalámbrica a los bridges inalámbricos configurados en modo raíz. En la figura 4.12 se puede apreciar dos bridges configurados en este modo.

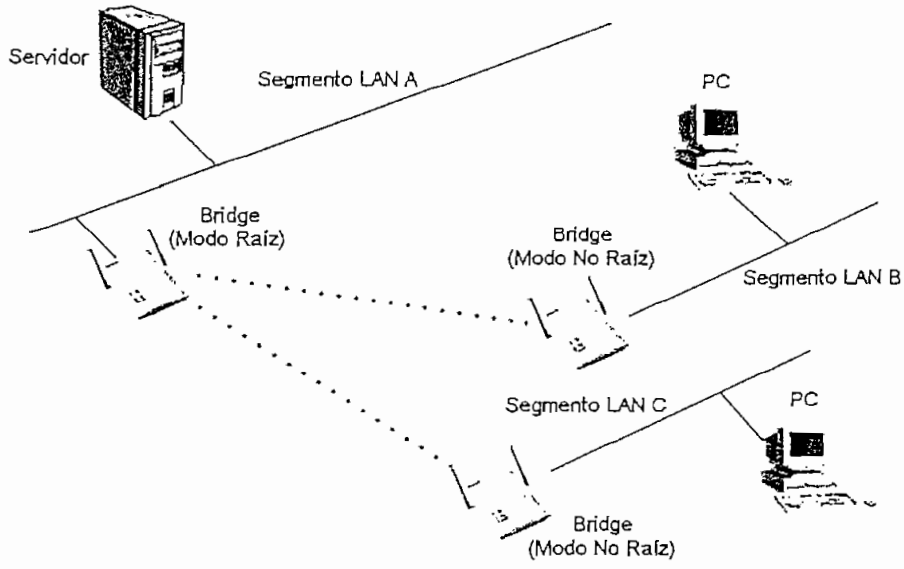


Figura 4.12. Bridges Inalámbricos en Modo Raíz y en Modo No Raíz

4.3.2.1.3 Modo Punto de Acceso

Algunos fabricantes de *bridges* incorporan una opción que permite a los administradores la habilidad de tener clientes conectados a los *bridges*, dándole de esta forma la funcionalidad de punto de acceso. Algunos *bridges* permiten este modo dentro de su configuración lo que los puede convertir en un punto de acceso completamente.

4.3.2.1.4 Modo Repetidor

Los *bridges* inalámbricos también pueden ser configurados en el modo repetidor, esto se puede apreciar en la figura 4.13. En el modo repetidor, un bridge será colocado entre otros dos bridges con el propósito de extender la longitud del segmento inalámbrico.

Cuando se usa un bridge inalámbrico en esta configuración se tiene la ventaja de extender el enlace, pero al mismo tiempo se tiene la desventaja de una baja velocidad de transmisión al tener un solo radio *half duplex* para repetir las tramas.

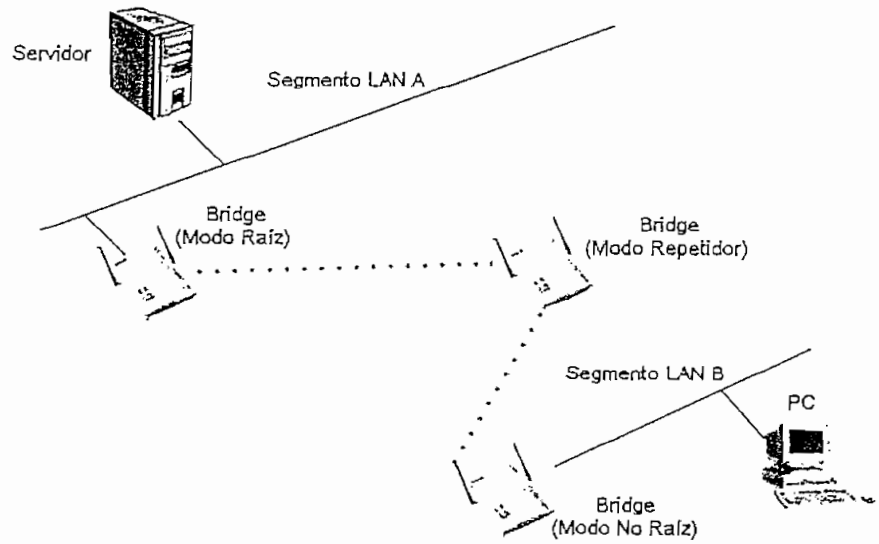


Figura 4.13. Bridge Inalámbrico en Modo Repetidor

4.3.2.2 Características Comunes

Las características de hardware y software de un bridge inalámbrico, son similares a los de un punto de acceso, entre estas características más comunes se tiene:

- ✓ Antenas fijas o desmontables
- ✓ Capacidades avanzadas de filtrado
- ✓ Tarjetas de radio removibles
- ✓ Potencia de salida variable

4.3.3 WORKGROUP BRIDGES INALÁMBRICOS

Los *workgroup bridges* son dispositivos muy similares a los *bridges* descritos en la sección anterior. La gran diferencia entre estos dos dispositivos es que los *workgroup bridges* son dispositivos clientes que permiten agregar varios dispositivos clientes de una LAN cableada dentro de un solo cliente inalámbrico. La figura 4.14 muestra dos *workgroup bridges* de diferentes fabricantes.

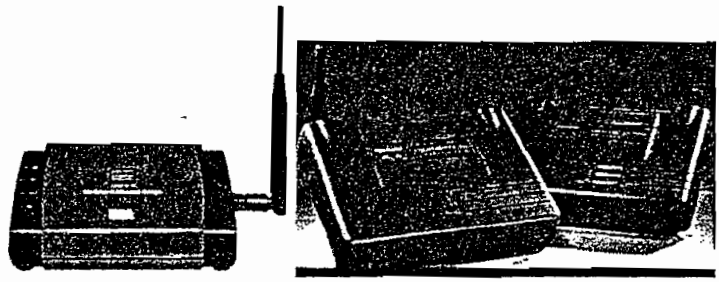


Figura 4.14. Workgroup Bridges Inalámbricos

Al ser un dispositivo cliente, un *workgroup bridge* aparecerá como un simple dispositivo cliente en la tabla de asociación de un punto de acceso. Las direcciones MAC de los dispositivos detrás de *workgroup bridge* no serán vistas por el punto de acceso. La figura 4.15 muestra un *workgroup bridge* instalado en una red mixta.

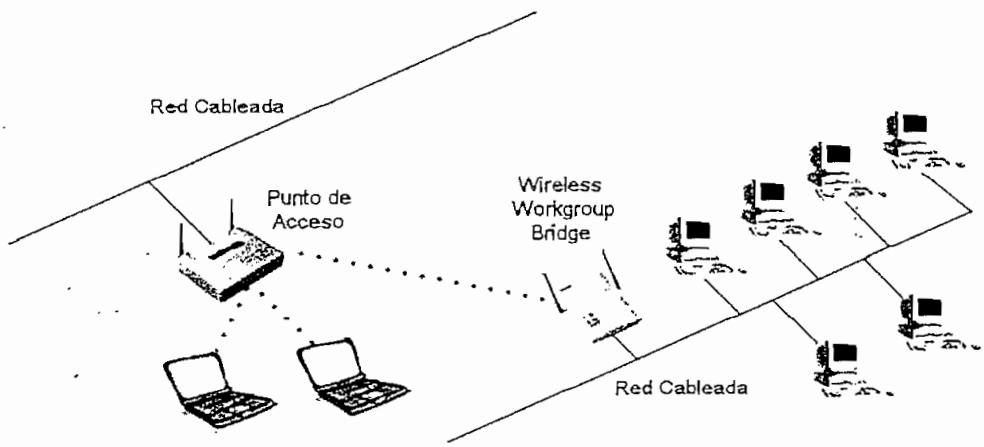


Figura 4.15. Workgroup Bridge Inalámbrico en una Red WLAN

4.3.4 DISPOSITIVOS CLIENTES WLAN

El término "dispositivos clientes" cubre varios tipos de dispositivos WLAN que un punto de acceso puede reconocer como un cliente en una red. Entre los dispositivos cliente más comunes se tiene:

- ✓ Tarjetas PCMCIA
- ✓ Convertidores *Ethernet*

- ✓ Adaptadores USB
- ✓ Adaptadores PCI

Los dispositivos clientes inalámbricos listados anteriormente proveen conectividad a los clientes WLAN. Los clientes WLAN son los equipos de los usuarios finales como por ejemplo, PCs, *laptops*, PDAs, etc., los cuales necesitan conectividad inalámbrica dentro de la infraestructura de la red WLAN.

4.3.4.1 Tarjetas PCMCIA

El componente más común en una red inalámbrica son las tarjetas PCMCIA (*Personal Computer Memory Card International Association;* Asociación Internacional de Tarjetas de Memoria para Computadores Personales). También conocidas como "PC *cards*", estos dispositivos son utilizados en *laptops* y PDAs. Los PC *cards* son los componentes que proveen la conexión inalámbrica entre un equipo cliente y la red WLAN. También son utilizados como módulos de radio en puntos de acceso, *bridges, workgroup bridges*, adaptadores USB entre otros.

Las antenas de las PC *cards* varían con cada fabricante. Algunas PC *cards* tienen antenas pequeñas y planas, otras en cambio tienen antenas desmontables para mediante el uso de accesorios poder soportar otros tipos de antenas.

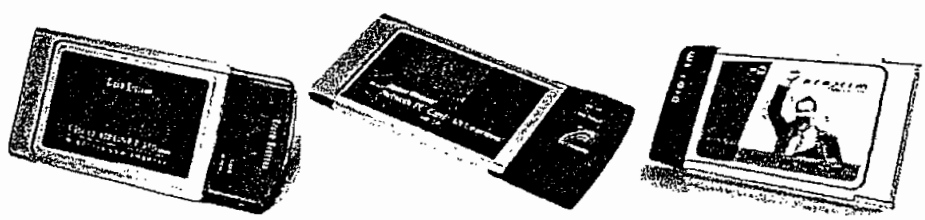


Figura 4.16. Tarjetas PCMCIA

4.3.4.2 Convertidores Ethernet y Seriales

Los convertidores *Ethernet* y seriales son usados con dispositivos que tengan puertos Ethernet y puertos seriales respectivamente con el propósito de convertir

estos puertos, en puertos para acceso inalámbrico.

Cuando se usa un convertidor *Ethernet* inalámbrico o un serial, lo que se hace es conectar externamente un radio WLAN a dicho dispositivo mediante un cable UTP o un cable serial dependiendo del puerto. Un uso común de estos convertidores es la conexión de servidores para impresión a la red WLAN.

Normalmente este tipo de convertidores no incluyen el radio PC *card*. De hecho, esta PC *card* debe ser adquirida separadamente e instalada en la ranura PCMCIA. En la figura 4.17 se puede apreciar un convertidor *Ethernet* & Serial el cual tiene una ranura PCMCIA en su costado derecho para la inserción de una PC *card*.

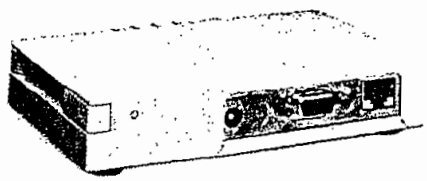


Figura 4.17. Convertidor Ethernet

4.3.4.3 Adaptadores USB

Los adaptadores USB (*Universal Serial Bus;* Bus Serial Universal), son usados en dispositivos que cuenten con puertos USB para conectarlos en una red WLAN. Este tipo de adaptadores son dispositivos *plug and play* y no requieren de fuentes de alimentación externa sino únicamente la que entrega el puerto USB del PC. Algunos de estos adaptadores ya incluyen el radio como las PC *cards* otros no. En la figura 4.18 se puede apreciar dos modelos diferentes de adaptadores USB de un mismo fabricante.

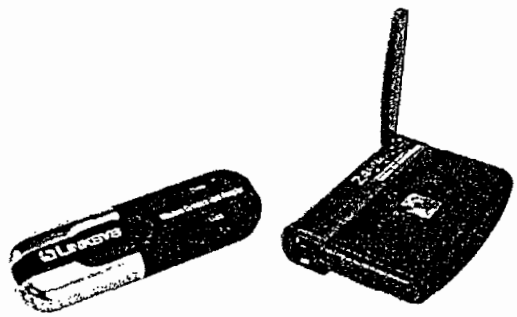


Figura 4.18. Adaptadores USB

4.3.4.4 Adaptadores PCI

Los adaptadores PCI (*Peripheral Component Interconnect;* Conector de Componentes Periféricos), son tarjetas que incluyen un módulo de radio, las cuales pueden ser insertadas dentro de cualquier computador personal o servidores que tengan una ranura de expansión PCI libre. Normalmente este tipo de adaptadores vienen con una antena que se adapta a un conector externo, la cual puede ser removida para adherir otro tipo de antenas. En la figura 4.19 se puede apreciar dos adaptadores PCI de fabricantes diferentes.

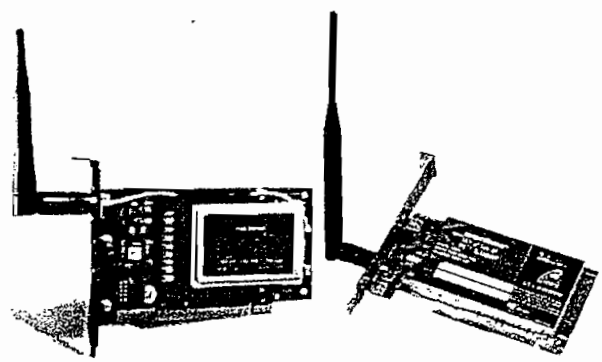


Figura 4.19. Adaptadores PCI

4.3.5 GATEWAYS INALÁMBRICOS

Un *gateway* inalámbrico es un dispositivo diseñado para conectar un número pequeño de nodos inalámbricos a otro dispositivo para conectividad de capa 2 o de capa 3 hacia el Internet u otra red. Es muy común encontrar estas

características dentro de los puntos de acceso ya que los fabricantes han empezado a combinar los roles de los puntos de acceso y de los *gateways* inalámbricos dentro de un único dispositivo. En la figura 4.20 se puede apreciar un punto *gateway* inalámbrico.

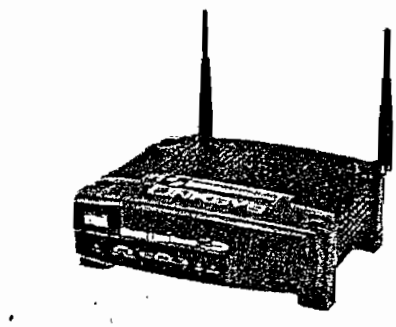


Figura 4.20. Gateway Inalámbrico

El puerto WAN (*Wide Area Network*; Red de Área Extendida), en un *gateway* inalámbrico es un puerto *Ethernet*, el cual puede ser conectado al Internet u otra red a través de:

- ✓ Un módem de cable
- ✓ Un módem xDSL
- ✓ Un módem analógico
- ✓ Un módem satelital

La figura 4.21 muestra un *gateway* inalámbrico usado en una red WLAN para el acceso a Internet mediante un módem.

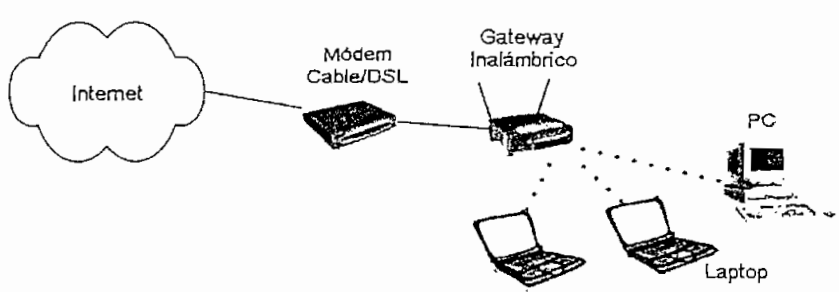


Figura 4.21. Gateway Inalámbrico en una Red WLAN

4.3.5.1 Características Comunes

La popularidad de los *gateways* inalámbricos se ha ido incrementado dentro de usuarios caseros y pequeños negocios, por lo que los fabricantes cada vez han ido agregando nuevas características a estos dispositivos. Entre las características más comunes se tiene:

- ✓ Soportan PPP (*Point to Point Protocol;* Protocolo Punto a Punto) sobre *Ethernet*
- ✓ Permiten configuración de NAT (*Network Address Translation;* Traducción de la Dirección de Red)
- ✓ Soportan VPNs (*Virtual Private Networks;* Redes Privadas Virtuales)
- ✓ Poseen servicios de impresión
- ✓ Poseen características de *Firewall*
- ✓ Poseen Servicios DHCP (*Dynamic Host Configuration Protocol;* Protocolo de Configuración Dinámica de Host)

Este arreglo de diversas funcionalidades permite a los usuarios de redes caseras y redes SOHO (*Small Office-Home Office*) disponer de una solución simple ante muchos problemas, mediante el uso de un solo dispositivo el cual por lo general es muy fácil de configurar.

4.4 TOPOLOGÍA GLOBAL DEL ISP

En forma global la red del ISP en la ciudad de Quito está conformada de una oficina central, y tres nodos. Tanto los nodos como los clientes se interconectan mediante una topología estrella en cascada, tal como se muestra en la figura 4.22.

En la oficina central ingresan varios clientes directamente y el tráfico de dos enlaces principales, uno del nodo 1 y el otro del nodo 2. En el nodo 1 y en el nodo 2 también se concentran clientes, además el nodo 1 se enlaza con el nodo 3 a través de un enlace principal. Los enlaces inalámbricos que existen actualmente

en la red utilizan tecnología WLAN IEEE 802.11b como se indica más adelante.

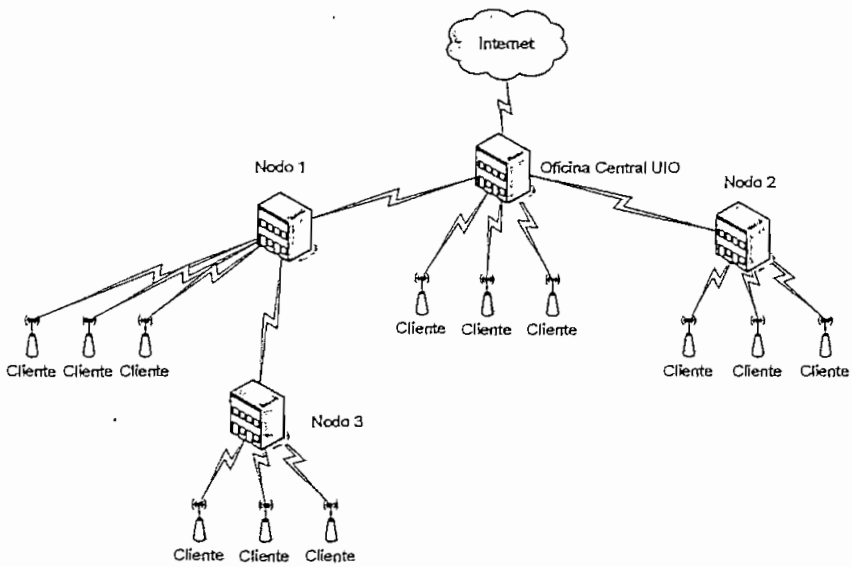


Figura 4.22. Topología de Red del ISP

4.5 INFRAESTRUCTURA DE LA OFICINA CENTRAL

Para una mayor comprensión de la infraestructura actual, se la divide en cuatro secciones jerárquicas que diferencian claramente las funciones de los diferentes dispositivos de hardware que conforman la red. Esto se puede apreciar en la figura 4.23:

- ✓ Red de *core*
- ✓ Red de distribución
- ✓ Red de acceso
- ✓ Red de gestión

4.5.1 RED DE CORE

La red de *core* o red central permite la interconexión del ISP con el Internet, para esto el ISP utiliza un enlace satelital que interconecta éste con un ISP de mayor jerarquía y un enlace de *backup* que interconecta la red del ISP de la ciudad de

Quito con la de red del ISP de Cayambe. El ISP de Cayambe cuenta con su propio enlace satelital.

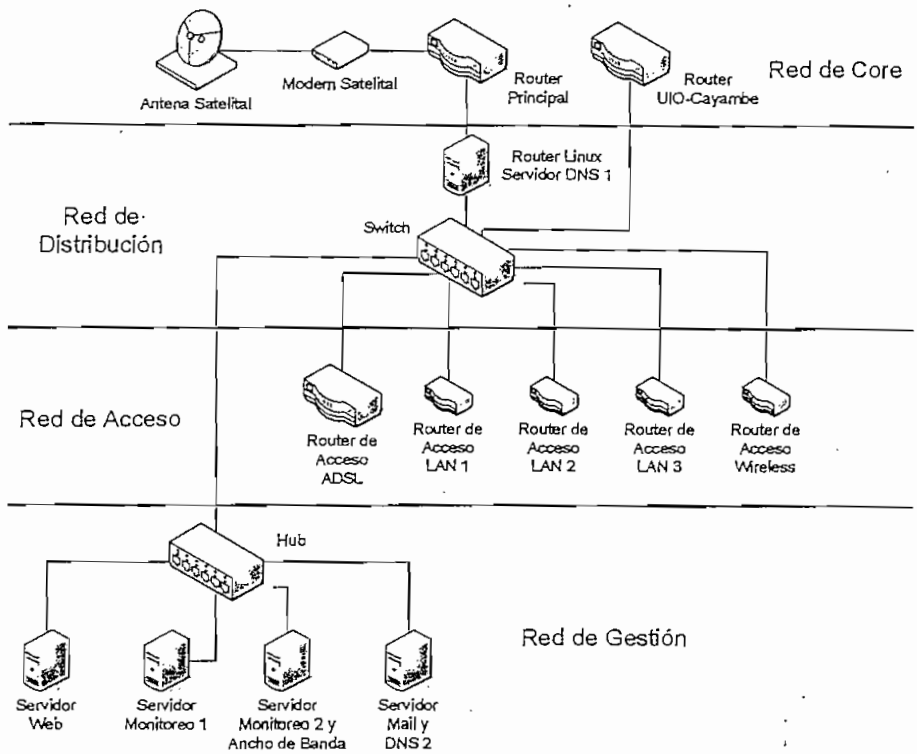


Figura 4.23. Estructura Interna Actual de la Oficina Central

El ancho de banda del enlace satelital mediante el cual accede a Internet es: 640 kbps para el enlace de subida o *up-link* y 1024 kbps para el enlace de bajada o *down-link*, esto se puede apreciar en la figura 4.24.

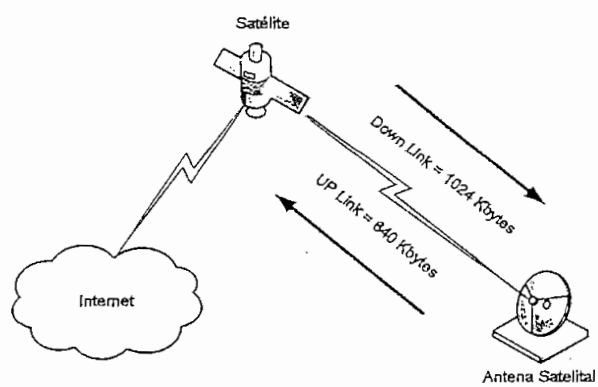


Figura 4.24. Enlace Satelital

En la figura 4.25 se puede apreciar el comportamiento actual del tráfico de entrada que está en color verde y el tráfico de salida que está en color rojo a través del enlace satelital del ISP. En el eje *x* tenemos el tiempo y en el eje *y* la cantidad de bits por segundo.

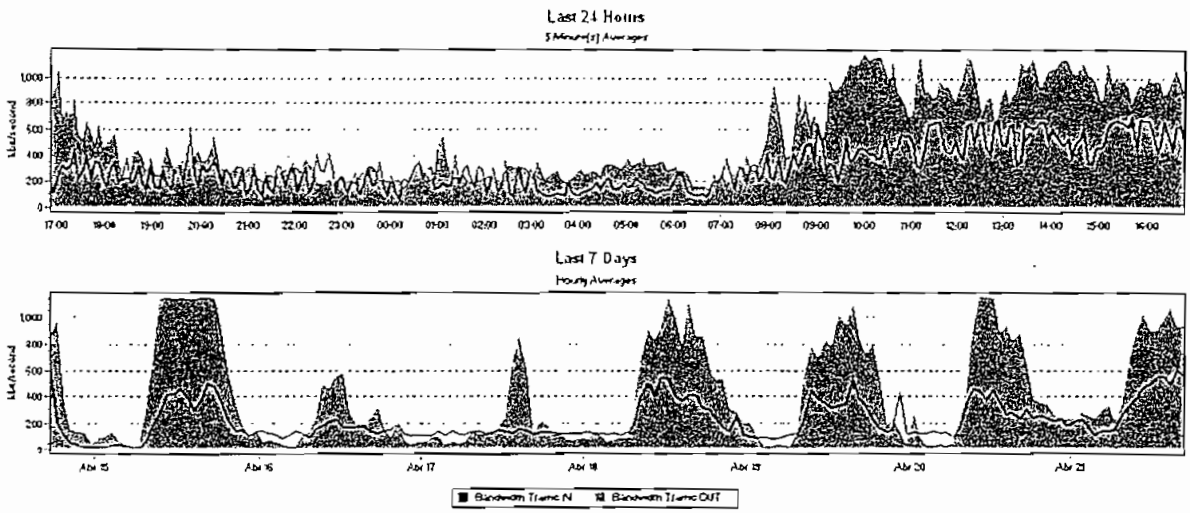


Figura 4.25. Tráfico de Entrada y Salida en Enlace Satelital

Como se puede apreciar en la figura 4.23, la red de *core* se encuentra conformada por varios dispositivos:

- ✓ Antena satelital
- ✓ Módem satelital
- ✓ Ruteador principal
- ✓ Ruteador UIO-Cayambe

4.5.1.1 Antena Satelital

La antena satelital y los dispositivos que permiten la comunicación satelital son proporcionados por el proveedor del servicio, razón por la cual sale del motivo de este estudio.

4.5.1.2 Módem Satelital [2]

El módem satelital que se encuentra instalado para el enlace satelital, es un módem marca Comtech SDM-300, el cual permite velocidades de transmisión variables de hasta 5 Mbps.

Para mayor información acerca de las características de este equipo, remitirse al *datasheet* que se encuentra en el Anexo 1.

4.5.1.3 Ruteador Principal

El ruteador principal o ruteador de *core* es un ruteador Cisco de la Serie 2600, específicamente un Cisco 2620. Este ruteador es el encargado de establecer el enrutamiento óptimo entre nodos de diferentes redes, enviando paquetes a gran velocidad entre el ISP y el ISP de jerarquía superior. Este ruteador posee las siguientes características:

- ✓ Ruteador Cisco modelo 2620
- ✓ *Release* IOS 12.0(7)T
- ✓ Procesador MPC 860
- ✓ Memoria *Flash* de 8 MBytes
- ✓ Memoria de Sistema DRAM de 26 MBytes
- ✓ Una interfaz *Fast Ethernet*
- ✓ Dos interfaces seriales

Para mayor información acerca de este equipo, remitirse a las características y configuraciones de este ruteador en el Anexo 1.

4.5.1.4 Ruteador UIO-Cayambe

La función de este ruteador es la de interconectar la red de Quito y la de Cayambe mediante un enlace de respaldo a través de un enlace de cobre. La finalidad de la interconexión entre estas dos redes es la de ofrecer un servicio de

backup mutuo en caso de que sus enlaces internacionales hacia Internet fallen en cualquiera de estas dos redes.

La red de Cayambe cuenta con su propio enlace internacional independiente del enlace que existe en Quito. En caso de una falla de cualquiera de los dos enlaces internacionales, el administrador de la red que falla lo que hace es enrutar a los clientes más importantes a través de este enlace de *backup* para que salga a través de la otra red. Esto no se hace en forma automática sino manualmente, lo que conlleva a que los clientes se queden sin servicio por varios minutos en caso de un incidente.

Las características de este ruteador son:

- ✓ Ruteador Cisco modelo 805
- ✓ *Release* IOS 12.2(8)T5
- ✓ Procesador MPC 850
- ✓ Memoria Flash de 4 MBytes
- ✓ Memoria de Sistema DRAM por defecto 8 MBytes
- ✓ Una interfaz *Ethernet*
- ✓ Una interfaz serial

Para mayor información acerca de este equipo, remitirse a las características y configuraciones de este ruteador en el Anexo 1.

4.5.2 RED DE DISTRIBUCIÓN

La red de distribución que se encuentra situada entre la red de *core* y la red de acceso, es la encargada de segmentar la red en diferentes dominios de colisión. También se encarga de concentrar el tráfico de las diferentes redes de acceso hacia la red core. En la red de distribución se encuentran:

- ✓ Servidor Linux
- ✓ *Switch*

4.5.2.1 Servidor Linux

El servidor Linux es un servidor que tiene incorporado dos tarjetas de red e instalado el Sistema Operativo Linux. Mediante esto y la ejecución de varios servicios, el servidor Linux cumple con dos funciones específicas:

1. Función de Ruteador
2. Función Servidor DNS 1

El Servidor como ruteador se encarga del enrutamiento de todos los paquetes que llegan a cualquiera de sus dos interfaces de red, tanto por el lado WAN como EL lado LAN. El fin de este servidor como ruteador es un tanto redundante e ineficiente, ya que se está realizando un salto innecesario en el enrutamiento de paquetes. La justificación para que este se haya instalado, era la de disminuir el procesamiento en el ruteador principal ya que en sus inicios se tenía la idea de hacerle funcionar con protocolos de enrutamiento dinámico y no estático como ahora, de esta forma el ruteador Linux se encarga de discernir que paquetes tienen que salir hacia el Internet y que paquetes tienen que quedarse dentro de las subredes del ISP.

El servidor DNS1 tiene la función de DNS primario para la resolución de nombres de domino a dirección IP y viceversa para todos los usuarios del ISP.

4.5.2.2 Switch [3]

El switch instalado es un 3COM *Baseline Switch 2016*. Este *switch* que tiene la capacidad de dividir en diferentes dominios de colisión por ser de capa 2, permite la interconexión de la red de gestión, la red de acceso y la red de distribución.
Las características de este *switch* son las siguientes:

- ✓ Switch de Capa 2 según el modelo ISO/OSI, no administrable
- ✓ Puertos: 16 puertos 10Base-T/100Base-TX con auto-detección y auto-configuración MDI/MDIX

- ✓ Interfaces para medios: RJ-45
- ✓ Funciones de *switching Ethernet*: conmutación *Store & Forward*, auto-negociación y control de flujo *full duplex* y *semi duplex*
- ✓ Direcciones MAC que se soportan: 4000

Para mayor información acerca de las características de este equipo, remitirse al *datasheet* que se encuentra en el Anexo 1.

4.5.3 RED DE ACCESO

La red de acceso es el punto de entrada de los diferentes grupos de trabajo o redes de usuarios a la red del ISP. Esta red se encuentra conformada por los siguientes dispositivos:

- ✓ Ruteador de acceso ADSL
- ✓ Ruteadores de acceso LAN
- ✓ Ruteador de acceso Wireless

4.5.3.1 Ruteador de Acceso ADSL [4]

Las líneas ADSL (*Asymmetric Digital Subscriber Line*; Línea Digital Asimétrica de Abonado), permiten a los clientes disponer de forma simultanea y permanente, voz y acceso de banda ancha sobre una línea telefónica convencional. El usuario es provisto de un equipo cliente que incluye un módem ADSL. Este equipo se conecta al punto de terminación telefónica en el domicilio o sitio de trabajo del cliente. En el otro extremo del par de cobre se localiza el DSLAM (*Digital Subscriber Line Access Multiplexer*), encargado de terminar las conexiones ADSL de nivel físico de múltiples usuarios y conmutar las celdas ATM transportándolas hacia la red de acceso del ISP. El ISP se conecta mediante un enlace ATM al PAI (Punto de acceso indirecto) del operador de acceso, que establece una PVC (*Permanent Virtual Connection*; Conexión Permanente Virtual) entre el cliente y el PAI.

Este servicio de última milla es provisto por un *carrier*, que para el caso del ISP en estudio, es la empresa Andinadatos la cual se encarga de proporcionar la infraestructura necesaria para la interconexión de los clientes mediante líneas ADSL hacia el ISP. La figura 4.26 muestra un esquema de esta interconexión.

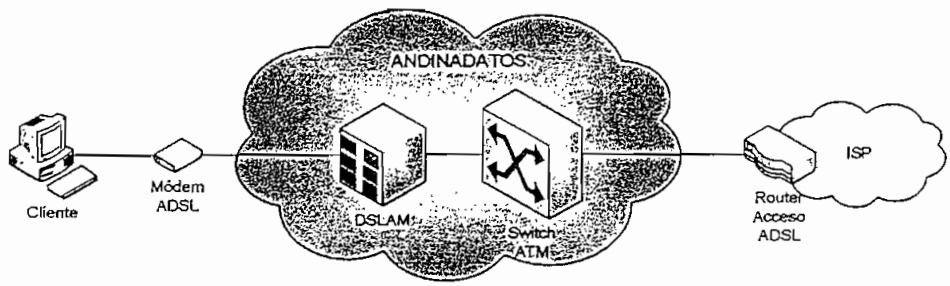


Figura 4.26. Acceso ADSL

La función del ruteador de acceso ADSL es la de terminar este enlace ATM proveniente del *carrier*, el cual multiplexa varias conexiones ADSL en diferentes PVCs y la de establecer las rutas para conmutar el tráfico de estos PVC de los clientes con la red del ISP y viceversa.

El ruteador de concentración ADSL es un ruteador Cisco de la serie 820, específicamente es un Cisco 827 con las siguientes características:

- ✓ Ruteador Cisco modelo 827
- ✓ Release IOS 12.2(8)T4
- ✓ Procesador MPC 855 T
- ✓ Memoria *Flash* de 8 MBytes
- ✓ Memoria de Sistema DRAM de 15 MBytes
- ✓ Una interfaz *Ethernet*
- ✓ Una interfaz ATM

Para mayor información acerca de este equipo, remitirse a las características y configuraciones de este ruteador en el Anexo 1.

4.5.3.2 Ruteadores de Acceso LAN [5]

Los ruteadores de acceso LAN 1, LAN 2 y LAN 3 permiten que varios clientes que se encuentran en localidades cercanas a la oficina central del ISP (que no sobrepasen los 100 m de cableado), puedan acceder a Internet mediante conexiones directas a las interfaces LAN. Cuando un cliente se encuentra a una distancia muy extensa que sobrepase los 100 m, entonces se le entrega un acceso ADSL o un acceso Wireless.

Estos ruteadores se encargan de concentrar el tráfico de las diferentes redes de los clientes y establecer las rutas para conmutar paquetes en forma bidireccional entre estas redes y la red del ISP. Los ruteadores que se emplean para este fin son equipos Linksys con un *switch* de cuatro puertos incluido, estos equipos tienen las siguientes características:

- ✓ Switch incorporado con 4 puertos para LAN 10Base-T/100Base-TX
- ✓ Un puerto para WAN 10Base-T/100Base-TX
- ✓ Administración y actualización remota a través de *Web Browser*
- ✓ Se puede configurar como Servidor DHCP (*Dynamic Host Configuration Protocol*)
- ✓ Soporta VPNs usando conexiones IPSec (*Internet Protocol Security*; Seguridad en el Protocolo de Internet) y PPTP (*Point-to-Point Tunneling Protocol*; Protocolo de Creación de Túneles Punto a Punto)
- ✓ Funciones avanzadas de Administración para Filtrado de Puertos, Filtrado de MAC *Address* y DMZ *Hosting* (*Demilitarized Zone*; Zona Desmilitarizada)
- ✓ Detección automática de cable directo o cable cruzado

Para mayor información acerca de las características de este equipo, referirse al *datasheet* que se encuentra en el Anexo 1.

4.5.3.3 Ruteadores de Acceso Wireless [6]

El ruteador de acceso wireless permite que los diferentes clientes que utilizan la tecnología WLAN IEEE 802.11b puedan acceder al Internet. La función de este ruteador al igual que la de los ruteadores anteriores es la de concentrar el tráfico de los diferentes clientes y establecer las rutas para conmutarlo en forma bidireccional con la red del ISP.

Este ruteador es un Linksys con un *switch* de ocho puertos incluido, con las siguientes características:

- ✓ *Switch* incorporado con 8 puertos LAN 10Base-T/100Base-TX Half-Duplex y Full-Duplex
- ✓ Un puerto para WAN 10Base-T Half-Duplex
- ✓ Provee seguridad en sus puertos, filtrado de paquetes y filtros para acceso a usuarios internos
- ✓ Capacidad de QoS basada en Priorización de Datos en los Puertos y Servicios de Internet
- ✓ Se puede configurar como servidor DHCP (*Dynamic Host Configuration Protocol*)
- ✓ Soporta VPNs usando conexiones IPSec (*Internet Protocol Security*) y PPTP (*Poin-to-Point Tunneling Protocol*)
- ✓ Configuración local o remota a través del *Web Browser*
- ✓ Funciones avanzadas de Administración para Filtrado de Puertos, Filtrado de direcciones MAC y DMZ (*Demilitarized Zone*) *Hosting*

4.5.4 RED DE GESTIÓN

Actualmente la red de gestión está conformada por varios servidores integrados mediante un Hub 3COM:

- ✓ Servidor Web
- ✓ Servidor de Mail Cliente

- ✓ Servidor de Monitoreo 1
- ✓ Servidor de Monitoreo 2 y Ancho de Banda
- ✓ Servidor de Mail y DNS 2

4.5.4.1 Servidor Web [7]

El servidor *Web* es un servidor que esta basado en el sistema operativo *Windows 2003 Server*, el mismo que tiene instalado los servicios del *Internet Information Server* para brindar *Web Hosting* a los clientes que lo requieran.

Los Servicios de *Microsoft Internet Information Server* con *Windows Server 2003* proporcionan capacidades de servidor *Web* integrado, confiable, escalable, seguro y administrable en una intranet, una extranet o en Internet.

4.5.4.2 Servidor de Monitoreo 1

El servidor de monitoreo 1 basado en el sistema operativo Windows 2000, permite sondear los eventos diarios y la conectividad de cada uno de los nodos y clientes pertenecientes a la red del ISP. Para cumplir con este fin, este servidor tiene instalado una herramienta de software muy conocida y sencilla de operar, el *WhatsUp Gold* versión de Software 8.0. En la figura 4.27 se puede apreciar una captura de pantalla de esta herramienta.

4.5.4.2.1 WhatsUp Gold [8]

WhatsUp Gold es un sistema gráfico para el monitoreo de redes, diseñado para diferentes protocolos de red. Este sistema monitorea dispositivos y servicios críticos e inicia alarmas audibles y visuales cuando detecta un problema. Entre las principales características de este sistema se tiene:

- ✓ **Creación de Mapas de Red:** Posee muchas opciones para realizar un descubrimiento automático y así crear un mapa de los dispositivos (por ejemplo: ruteadores, *switches*, servidores, estaciones de trabajo) en una

red. El descubrimiento automático también descubre servicios (por ejemplo: Web, mail o ftp) en cada dispositivo.

- ✓ **Monitoreo de Dispositivos y Servicios:** Usa protocolos estándares como TCP/IP (*Transmission Control Protocol/Internet Protocol*; Protocolo de Control de Transmisión/Protocolo de Internet), SNMP (*Simple Network Management Protocol*; Protocolo Simple de Gestión de Redes), NetBIOS (*Network Basic Input Output System*; Sistema de Red Básico de Entrada y Salida) e IPX (*Internetwork Packet Exchange;* Intercambio de Paquetes en Red Interna), para monitorear los mapas de red. Para esto *WhatsUp Gold* continuamente censa los dispositivos creados en el mapa de red y los servicios en los dispositivos, e inicia alarmas visibles y audibles cuando censa dispositivos y servicios que están caídos.
- ✓ **Notificación de Problemas:** Cuando *WhatsUp Gold* detecta un problema, se puede recibir una notificación por *beeper*, sonido, e-mail, mensajes de voz y otros.
- ✓ **Generación de Reportes:** *WhatsUp Gold* permite generar reportes para ayudar a analizar el *uptime* (tiempo de disponibilidad) de la red y tiempo de respuesta de los dispositivos.
- ✓ **Administración Remota:** *WhatsUp Gold* posee un servidor Web que permite el uso de cualquier *Web Browser* sobre cualquier computador en el Internet para ver el estatus de la red y cambiar parámetros en el *WhatsUp Gold.*

4.5.4.3 Servidor de Monitoreo 2 y Ancho de Banda

Este servidor que tiene como función principal asignar el ancho de banda (velocidad de transmisión), a cada uno de los clientes mediante un paquete de software, también se lo utiliza como un servidor alterno para el monitoreo de la red. Su sistema operativo es el Sistema Operativo Windows 2000 y para su función como servidor de monitoreo tiene instalado el software *WhatsUp Gold* al igual el que el servidor de monitoreo principal.

Como servidor de asignación de ancho de banda (velocidad de transmisión), este

servidor es uno de los más importantes ya que de éste depende que los clientes puedan acceder a Internet. Si este servidor sufre algún inconveniente todos los clientes no tendrán servicio puesto que todo el tráfico pasa por este servidor antes de salir a Internet, debido a que es el *default gateway* de los ruteadores de acceso.

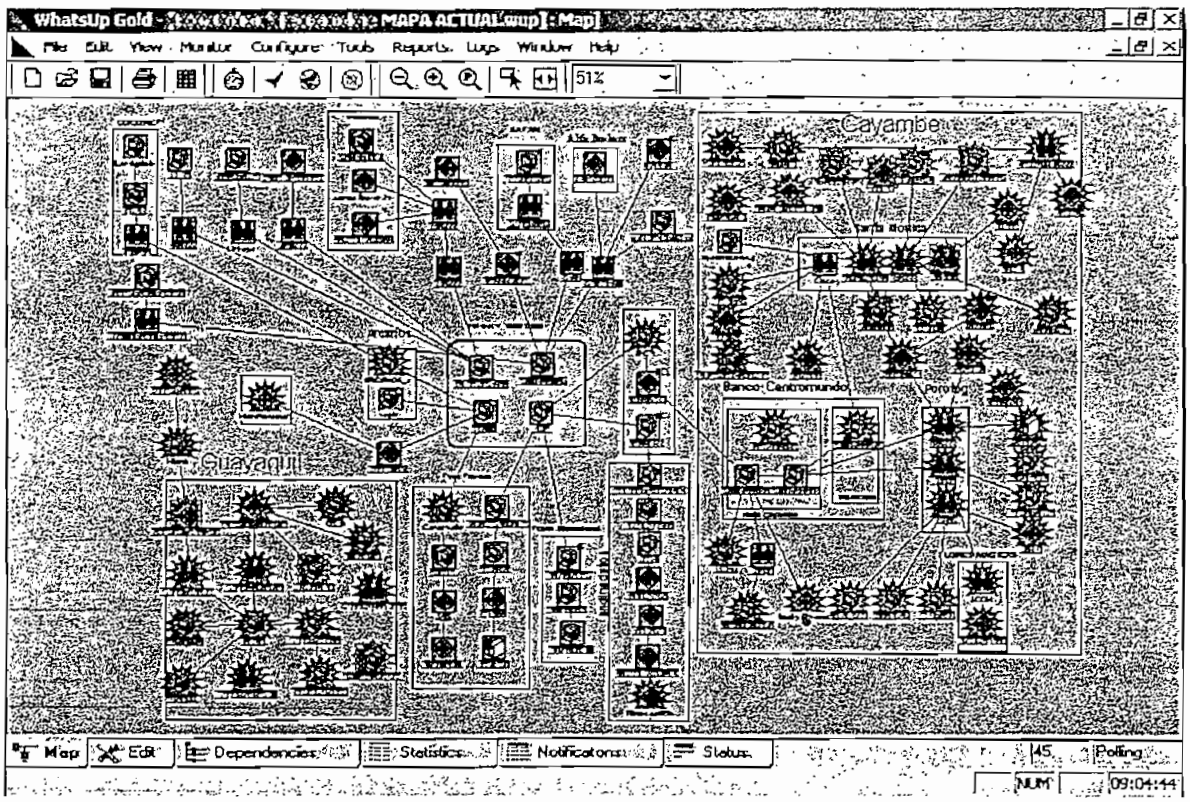


Figura 4.27. Captura de Pantalla de WhatsUp Gold

El sistema instalado en este servidor para poder realizar el control de ancho de banda de la red, es un software muy sencillo de utilizar denominado *Bandwidth Controller.*

4.5.4.3.1 Bandwidth Controller [9]

El sistema *Bandwidth Controller* es útil en un ambiente donde se necesite un control total sobre la utilización de la red. Por ejemplo si se tiene muchos clientes accediendo al Internet a través de un único servidor (como es el caso del ISP en

análisis), se puede limitar el *throughput* de todos los clientes, de tal forma que uno solo no utilice el ancho de banda disponible. Incluso es posible, a través del uso de filtros, controlar un solo computador y dar el acceso sin restricción a todos las demás.

Bandwidth Controller usa filtros para controlar el tráfico en la red. Un filtro es un conjunto de reglas que especifican el tipo de tráfico que será limitado. Cualquier tráfico que iguale los atributos de un filtro será procesado por el filtro, de lo contrario éste atravesará el adaptador de red intacto. Se pueden tener hasta 20 filtros activos a la vez. Entre las principales características de este software se tiene:

- ✓ **Administración Centralizada:** *Bandwidth Controller* realiza el *traffic shaping* (configuración de tráfico) dentro de un único servidor de la red por lo que no es necesario instalar ningún tipo de software en los computadores de los clientes para limitar el ancho de banda. Esta administración centralizada además permite mantener el control asegurado contra ataques de usuarios maliciosos.
- ✓ **Filtrado Individual y Grupal:** *Bandwidth Controller* permite limitar el ancho de banda no sólo de un cliente, sino de un grupo entero de clientes a través de un único filtro.
- ✓ **Control Preciso de la Velocidad de Transmisión:** La velocidad de transmisión puede ser configurada entre 0 y 1 GigaByte por segundo. La unidad básica de medida que utiliza es 1 byte por segundo lo que hace posible limitar el ancho de banda con una alta precisión.
- ✓ **Estadísticas Detalladas:** *Bandwidth Controller* permite observar el uso del ancho de banda en cada filtro, con un gráfico en tiempo real que puede desplegar varias estadísticas, incluyendo la suma de tráfico que ha sido filtrado y el tráfico de uso actual. Esto se puede apreciar en la figura 4.28.
- ✓ **Filtrado de Puertos y Protocolos:** El control de datos también se puede dar en función de los protocolos y puertos que están siendo usados. Esto permite limitar tráfico IP, TCP, UDP, HTTP, FTP y otros tipos de tráfico.
- ✓ **Interfaz de Usuario:** El *Bandwidth Controller Manager* es la interfaz de

usuario la cual permite agregar o remover filtros, observar estadísticas y configurar el software. La figura 4.29 muestra esta interfaz.

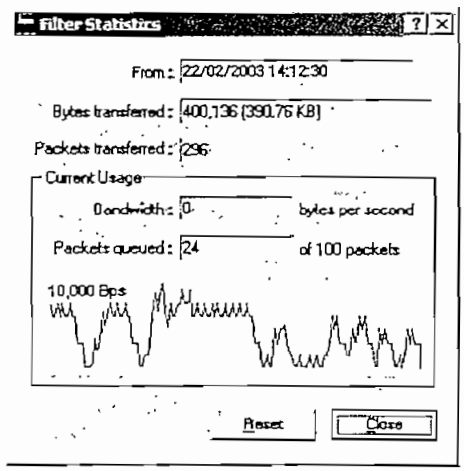


Figura 4.28. Estadísticas de Bandwidth Controller

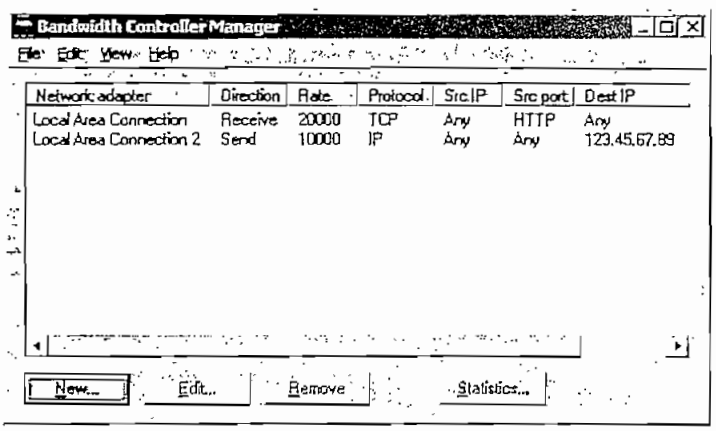


Figura 4.29. Interfaz Bandwidth Controller Manager

4.5.4.4 Servidor de Correo y DNS 2

Este servidor se encuentra basado en el Sistema Operativo Windows Server 2003 y presta dos tipos de servicios:

1. Servicio de Correo
2. Servicio de DNS (*Domain Name System*) Secundario

Para el servicio de correo el servidor tiene instalado el paquete de software *Merak* que es un software que permite montar este servicio y realizar su administración. El servicio de DNS Secundario se ejecuta como un servicio propio de Windows Server 2003, luego de realizar su instalación y configuración ya que no viene como un servicio por defecto.

4.5.4.4.1 Merak Mail Server [10]

El servidor de correo Merak es una solución integral de correo para usuarios de redes LAN o comunicaciones por Internet. Es una herramienta basada en Windows muy fácil de instalar y administrar, posee un alto desempeño y es muy segura. Soporta un número muy grande de usuarios y de dominios, protocolos POP3, SMTP, IMAP4, HTTP, análisis de virus, filtros de *spam*, *Web mail* entre otras cosas. En la figura 4.30 se puede apreciar el panel de administración de esta herramienta.

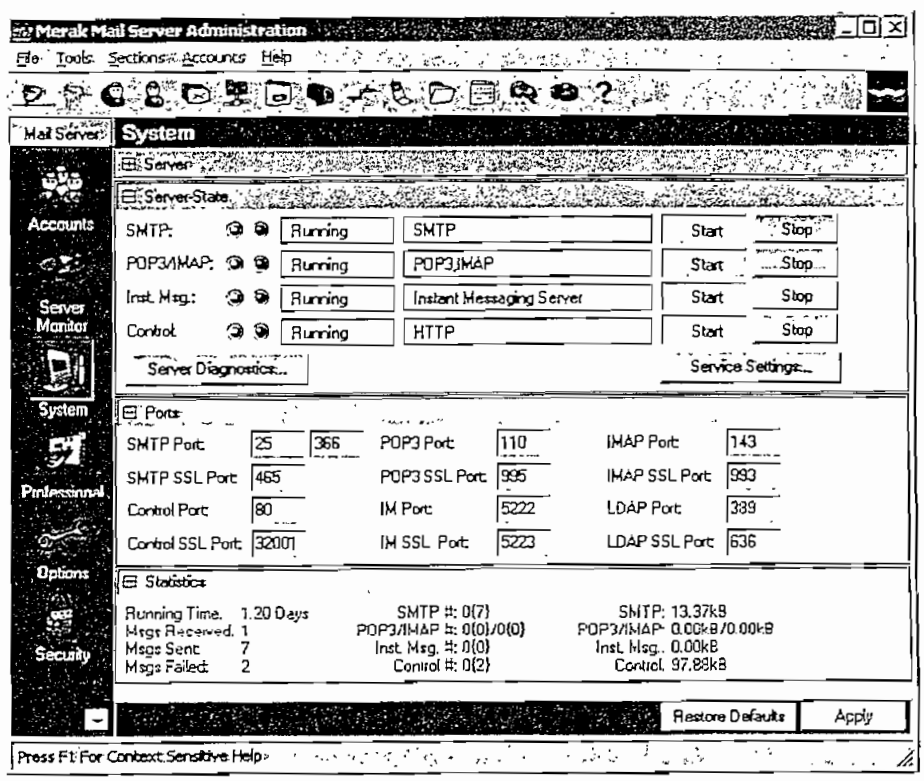


Figura 4.30. Panel de Administración de Merak

4.6 INFRAESTRUCTURA DEL BACKBONE

El *backbone* o red principal del ISP está conformado de un nodo principal y tres nodos secundarios situados estratégicamente sobre la ciudad de Quito para permitir el acceso de todos sus clientes. Estos cuatro nodos se interconectan entre sí mediante una topología estrella en cascada a través de tres enlaces de radio como ya se indicó en la sección 4.5.

4.6.1 NODO PRINCIPAL

El nodo principal se encuentra situado en la oficina central. A este nodo llegan dos radios enlaces principales y varios enlaces de última milla con tecnología WLAN IEEE 802.11b. Como se puede apreciar en la figura 4.31, el nodo principal se encuentra conformado de:

- ✓ Dos ruteadores Linksys
- ✓ Dos puntos de acceso AP-2000
- ✓ Seis puntos de acceso WAP11
- ✓ Un PC Linux-Cisco Aironet

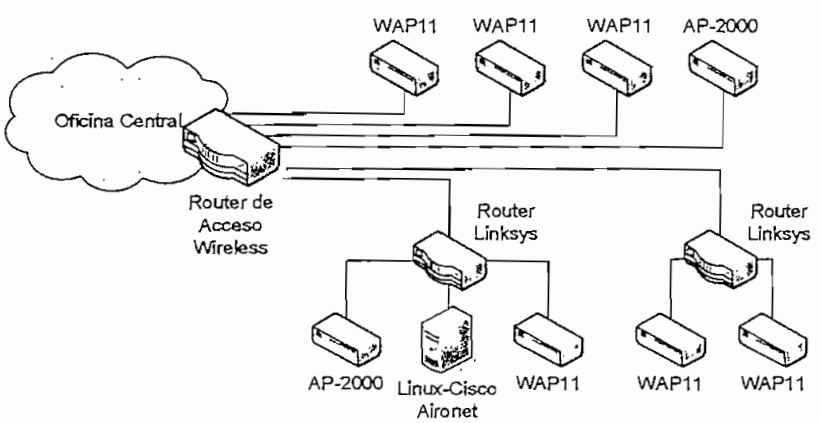


Figura 4.31. Dispositivos del Nodo Principal

4.6.1.1 Ruteadores Linksys

Los ruteadores Linksys se interconectan a través de dos de los 8 puertos del ruteador de acceso wireless para así expandir la capacidad de este ruteador, y segmentar la red. Esta expansión de la capacidad permite que más clientes puedan interconectarse con el ISP, el resto de clientes se conectan directamente a través de los 6 puertos restantes del ruteador de acceso wireless. Las características de estos ruteadores son similares a las del ruteador de acceso wireless.

4.6.1.2 Puntos de Acceso AP-2000 [11]

Los equipos ORiNOCO AP-2000 son puntos de acceso de alta capacidad para redes inalámbricas, muy fáciles de administrar y que soportan varios tipos de seguridades. Entre las principales características de estos puntos de acceso se tiene:

- ✓ Soportan estándares 802.11b, 802.11g y 802.11a
- ✓ Permiten actualización de hardware y software para soportar nuevos estándares
- ✓ Soportan WPA (*Wi-Fi protected Access*) incluyendo 802.1x y encriptación dinámica TKIP (*Temporal Key Integrity Protocol*)
- ✓ Soportan actualizaciones de AES (*Advanced Encryption Standard*) y 802.11i
- ✓ Soportan hasta 16 VLANs por cada interfaz
- ✓ Poseen dos interfaces 10 Base -T/100 Base-TX con conectores RJ-45
- ✓ Poseen dos ranuras PCMCIA para conectar tarjetas de red inalámbricas
- ✓ Poseen una interfaz RS-232 para configuración del equipo
- ✓ Poseen un procesador Intel SA110 de 233 MHz
- ✓ Memoria SDRAM de 16 MBytes
- ✓ Memoria Flash de 8 MBytes

Como se puede apreciar en la figura 4.31, uno de los puntos de acceso *AP-2000*

se conecta directamente al ruteador de acceso wireless, permitiendo establecer un enlace de última milla e interconectar el cliente con el ISP. El otro AP-2000 se interconecta a uno de los ruteadores Linksys, permitiendo establecer uno de los enlaces principales para interconectar el nodo principal con el nodo 1.

4.6.1.3 Puntos de Acceso WAP11 [12]

Los dispositivos WAP11 son puntos de acceso de la marca Linksys. Entre las principales características de estos equipos se tiene:

- ✓ Transferencia de datos de alta velocidad de hasta 11 Mbps
- ✓ Compatibilidad con equipos IEEE 802.11b en la banda de 2.4 GHz
- ✓ Soporta modos de operación de *bridging* inalámbrico y repetidor inalámbrico
- ✓ Filtrado de direcciones MAC
- ✓ Configuración y Administración vía *Web Browser*

Todos los puntos de acceso en este nodo funcionan en el modo punto de acceso y no en el modo puente para establecer los enlaces de última milla hacia los clientes.

4.6.1.4 PC Linux-Cisco Aironet

El PC Linux-Cisco Aironet es un PC que tiene instalado el sistema operativo Linux y montado varios servicios para permitir que mediante la conexión de una tarjeta de red inalámbrica PCI del tipo *Aironet* de Cisco con tecnología WLAN IEEE 802.11b, simule a una estación cliente. Este servidor además de la tarjeta inalámbrica, también tiene instalada una tarjeta de red convencional para interconectarse con uno de los ruteadores Linksys que se encuentran en este nodo.

4.6.2 NODO 1

Como se puede apreciar en la figura 4.32, el nodo 1 se encuentra conformado de tres equipos:

- ✓ Dos puntos de acceso AP-2000
- ✓ Un ruteador Linksys

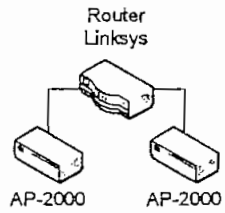


Figura 4.32. Dispositivos del Nodo 1

4.6.2.1 Puntos de Acceso AP-2000

Estos puntos de acceso tienen las mismas características que los puntos de acceso AP-2000 descritos en la sección anterior. Uno de estos puntos de acceso se interconecta con el nodo principal a través de una tarjeta de red inalámbrica PCMCIA insertada en una de las ranuras y a través de otra tarjeta en la otra ranura se interconecta directamente con un cliente, prestando un enlace de última milla. El otro punto de acceso AP-2000 permite la interconexión con el nodo 3 a través de una tarjeta insertada en una de sus ranuras. Esto se describe con más detalle en una de las secciones más adelante.

4.6.2.2 Ruteador Linksys

Las características de este ruteador son similares a las del ruteador de acceso wireless. Su función principal es la de establecer las rutas para alcanzar las redes del nodo 3, la red del cliente que ingresa al nodo y las rutas para el intercambio de tráfico con la oficina central.

4.6.3 NODO 2

Como se puede apreciar en la figura 4.33, el nodo 2 se encuentra conformado de 8 equipos:

- ✓ Siete Puntos de Acceso WAP11
- ✓ Un ruteador Linksys

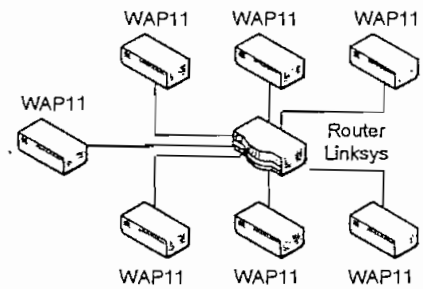


Figura 4.33. Dispositivos del Nodo 2

4.6.3.1 Puntos de Acceso WAP 11

Los puntos de acceso WAP11 de este nodo son de iguales características que los que existen en el nodo principal.

Al igual que en el nodo principal, todos los puntos de acceso en este nodo funcionan en el modo punto de acceso y no en el modo puente para establecer los enlaces de última milla hacia los clientes.

4.6.3.2 Ruteador Linksys

Las características de este ruteador son similares a las del ruteador de acceso wireless. Su función principal es la de enrutar el tráfico entre la red del ISP y las subredes de los clientes que ingresan a este ruteador.

4.6.4 NODO 3

Actualmente, el nodo 3 se encuentra conformado únicamente de un punto de acceso AP-2000. Este punto de acceso mediante la ranura de la interfaz 1 permite la interconexión del nodo 1 con el nodo 3 y mediante la ranura de la interfaz 2 permite entregar el enlace de última milla a uno de los clientes del ISP.

4.6.5 ENLACES INALÁMBRICOS PRINCIPALES

Los nodos del ISP se interconectan entre sí mediante tres enlaces inalámbricos principales que utilizan tecnología 802.11b, para permitir el acceso de todos sus clientes. Estos enlaces se pueden apreciar en la figura 4.34.

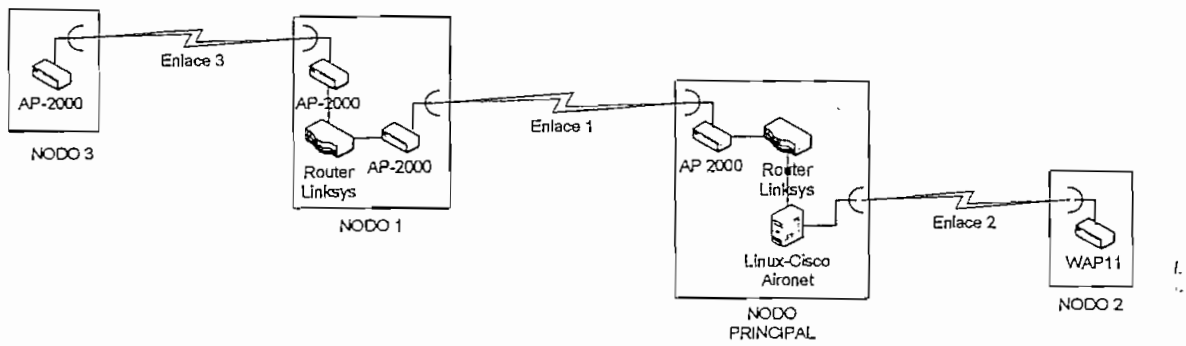


Figura 4.34. Enlaces Inalámbricos Principales

4.6.5.1 Enlace Principal 1

El enlace 1 se lo realiza a través de un punto de acceso AP-2000 del Nodo 1 y un punto de acceso AP-2000 del Nodo principal, estos dos equipos soportan la tecnología WLAN IEEE 802.11b. Para establecer el enlace se encuentra insertada una tarjeta de red inalámbrica PCMCIA del tipo *Orinoco Classic Gold PC Card* (Estas tarjetas de red inalámbricas PCMCIA, son tarjetas que soportan la tecnología de la especificación IEEE 802.11b), en una de las dos ranuras que tienen cada punto de acceso AP-2000. Cada una de estas tarjetas se conecta con una antena altamente direccional tipo grilla mediante un *pigtail*.

Este enlace se establece gracias a que las antenas se encuentran perfectamente alineadas para que tengan línea de vista y a que los puntos de acceso AP-2000 tienen configurada las interfaces que intervienen en este enlace en el modo WDS (*Wireless Distribution System*; Sistema de Distribución Inalámbrico).

Un sistema de distribución inalámbrico (WDS) crea un enlace entre dos unidades AP-2000 a través de sus interfaces de radio. El enlace retransmite el tráfico de un punto de acceso AP-2000 a un segundo AP-2000.

4.6.5.2 Enlace Principal 2

El enlace inalámbrico 2 interconecta el servidor Linux-Cisco Aironet que se encuentra en el Nodo principal y un punto de acceso WAP11 que se encuentra en el Nodo 2; ambos dispositivos manejan la tecnología WLAN IEEE 802.11b.

Este enlace se establece gracias a que el servidor Linux-Cisco Aironet se encuentra configurado como una estación cliente y el punto de acceso WAP11 está configurado en el modo punto de acceso. Además, estos dos equipos utilizan antenas tipo grilla en sus extremos las cuales se encuentran perfectamente alineadas para que tengan línea de vista.

En el PC Linux-Cisco Aironet, la antena se conecta a la tarjeta de red inalámbrica Cisco Aironet mediante un *pigtail* y en el punto de acceso WAP11 la antena se conecta en uno de los dos conectores que este punto de acceso tiene igualmente mediante un *pigtail*.

4.6.5.3 Enlace Principal 3

El enlace 3 se establece entre el Nodo 1 y el Nodo 3 mediante dos puntos de acceso AP-2000, para lo cual cada interfaz que interviene en este enlace se configura en el modo WDS.

Igualmente como en los otros enlaces, a cada interfaz inalámbrica se le conecta

mediante un *pigtail* una antena tipo grilla las cuales se encuentran perfectamente alineadas para que tengan línea de vista.

4.6.6 ENLACES INALÁMBRICOS DE ÚLTIMA MILLA

La última milla de la mayoría de los clientes se la entrega mediante el uso de enlaces inalámbricos con tecnología WLAN IEEE 802.11b, utilizando para este fin equipos de diferentes fabricantes que soportan dicha tecnología.

Esta combinación de diferentes tipos de equipos se debe a que los fabricantes se rigen al estándar 802.11 y sus diferentes especificaciones, para la elaboración de sus equipos, lo que permite que equipos de distintas marcas puedan interactuar entre si.

En la figura 4.35 se puede apreciar los enlaces de última milla existentes hasta el momento del análisis, en la red del ISP. Estos enlaces se encuentran representados de color amarillo y violeta, también se puede apreciar el nodo principal al que ingresan estos enlaces y los enlaces principales que interconectan los nodos.

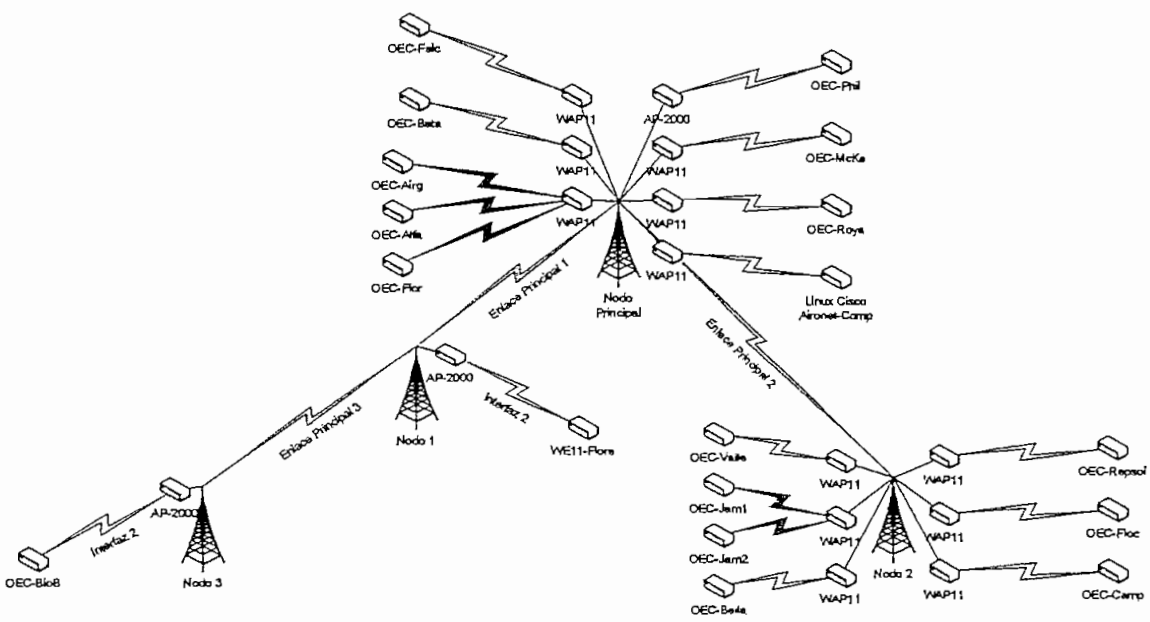


Figura 4.35. Enlaces Inalámbricos Clientes

Como ya se comentó en el Capítulo II, las redes WLAN pueden ser aplicadas de muchas formas como es el caso de los enlaces de última milla y la conectividad *Building-to-Building*. En el ISP que se ha tomado como caso de estudio se puede ver que estas aplicaciones son puestas en práctica para poder dar acceso inalámbrico a los clientes de este ISP. Los enlaces inalámbricos que se pueden encontrar en forma general son de dos tipos:

1. Enlaces punto a punto
2. Enlaces punto a multipunto

4.6.6.1 Enlaces punto a punto

Los enlaces punto a punto son conexiones inalámbricas que se establecen entre el nodo del ISP y el sitio de trabajo del cliente, en la figura 4.35 se pueden apreciar estos enlaces en color amarillo. Para esto, cada enlace debe tener un equipo WLAN tanto en el nodo como en el lado del cliente, específicamente se utilizan puntos de acceso en el nodo y dispositivos clientes en el lado del usuario. Los diferentes tipos de enlaces inalámbricos punto a punto que se pueden encontrar en esta red se pueden dar por la interacción de los siguientes equipos:

- ✓ WAP11 y OEC
- ✓ AP-2000 y OEC
- ✓ WAP11 y WET11
- ✓ WAP11 y Linux-Cisco Aironet

En cada uno de estos enlaces los puntos de acceso se encuentran configurados en modo *raíz* para de esta forma permitir que los dispositivos clientes que se encuentran en el lado del cliente se puedan asociar con el punto de acceso.

Tanto los puntos de acceso situados en los nodos, como los dispositivos clientes en el lado del usuario, se encuentran conectados con sus respectivas antenas tipo grilla mediante *pigtails* para incrementar el alcance y la ganancia; y así poder enlazarse con el equipo remoto. Cabe destacar que estas antenas se encuentran

perfectamente alineadas para que tengan línea de vista.

4.6.6.1.1 Convertidores Ethernet OEC [13]

Como se puede apreciar en la figura 4.35, la gran mayoría de enlaces tienen equipos OEC en el lado del cliente. Estos equipos son convertidores *Ethernet* de Lucent Technologies los cuales poseen una ranura PCMCIA para la inserción de tarjetas de red inalámbrica. En el caso del ISP en análisis las tarjetas inalámbricas son del tipo *Orinoco Classic Gold PC Card* (Estas tarjetas de red inalámbricas PCMCIA, son tarjetas que soportan la tecnología de la especificación IEEE 802.11b), ya que los OEC no soporta tarjetas con especificaciones superiores como la especificación IEEE 802.11a. Entre las características más importantes de éstos equipos se tiene:

- ✓ Poseen una ranura PCMCIA para una interfaz inalámbrica
- ✓ Poseen un puerto 10 Base-T con conector RJ-45
- ✓ Soportan encriptación WEP

Para mayor información acerca de las características de estos equipos, remitirse al *datasheet* que se encuentra en el Anexo 1.

4.6.6.1.2 Punto de Acceso WET11 [14]

En la figura 4.35, también se puede apreciar que en el lado del cliente existe un equipo WET11 que es un *bridge* inalámbrico de la marca Linksys. Entre las principales características de este *bridge* inalámbrico se tiene:

- ✓ Es compatible con equipos con tecnología IEEE 802.11b
- ✓ Realiza cambios automáticos de velocidad para máxima adaptabilidad
- ✓ Soporta encriptación WEP de 64 y 128 bits
- ✓ Posee un puerto 10Base-T con conector RJ-45

Para mayor información acerca de las características de este equipo, remitirse al

datasheet que se encuentra en el Anexo 1.

4.6.6.2 Enlaces punto a multipunto

Los enlaces punto a multipunto son conexiones inalámbricas entre un nodo del ISP y dos o más clientes, en la figura 4.35 se puede apreciar estos enlaces en color violeta. Estos enlaces se forman debido a que los diferentes equipos, se asocian con un único punto de acceso situado en el nodo del ISP.

Cada uno de estos dispositivos clientes y el punto de acceso situado en el nodo se interconectan con antenas parabólicas tipo grilla para incrementar el alcance y la ganancia mediante *pigtails.* Las antenas de los dispositivos clientes se encuentran en perfecta alineación para que tengan línea de vista con la antena situada en el punto de acceso del nodo del ISP. Además, para que los enlaces se puedan establecer las antenas de los dispositivos clientes deben estar dentro del lóbulo de radiación de la antena del punto de acceso.

Cuando se utilizan antenas altamente-direccionales como las tipo grilla, es muy difícil lograr establecer enlaces punto a multipunto debido a que los clientes que se deseen enlazar de esta forma deben estar muy próximos para que puedan ser cubiertos por el lóbulo de radiación de la antena del punto de acceso. Esta es la principal razón por la que los enlaces punto a multipunto no son muy comunes en el ISP.

4.7 POLÍTICAS DE SEGURIDAD DEL ISP

Las políticas de seguridad que actualmente maneja el ISP para lo referente a seguridad en los puntos de acceso, son escasas. Actualmente en todos los enlaces de última milla y en los enlaces principales el único recurso que se tiene para asegurar estos enlaces de posibles ataques tanto activos como pasivos es la configuración de un SSID (*Service Set Identifier*), no común en cada uno de los equipos WLAN.

El uso de la encriptación WEP (*Wired Equivalent Privacy*), se usa únicamente en ciertos enlaces de última milla en los cuales se ha tenido algún indicio de algún tipo de ataque. Esta política se aplica debido a que los administradores de la red tratan de disminuir al máximo el procesamiento en los equipos WLAN (especialmente en los dispositivos clientes), ya que estos son equipos no están diseñados para condiciones extremas de tráfico y de procesamiento como es el caso de un enlace de última milla.

Estas políticas de seguridad como se puede apreciar son muy deficientes, sin embargo debido al uso que tienen las redes WLAN IEEE 802.11b en el ISP en estudio, los ataques por parte de usuarios maliciosos son muy difíciles de lograr tanto en ataques pasivos como ataques activos, ya que estas redes se utilizan como redes de última milla. Por lo general, las antenas que se utilizan para establecer los enlaces se encuentran en sitios muy altos como azoteas y terrazas de edificios siendo muy difícil poder acceder a estos sitios en caso de que un *hacker* desee perpetrar algún tipo de ataque.

BIBLIOGRAFÍA CAPÍTULO IV

[1] CERTIFIED WIRELESS NETWORK ADMINISTRADOR. Official Study Guide. MacGraw-Hill. Second Edition. 2003.

[2] http://206.223.8.10/linksite/manuals/datasheets/ds-sdm300a.pdf:SDM-300A Satellite MODEM.

[3] http://www.3com.com/other/pdfs/products/en_US/400838.pdf: 3Com Baseline Switches.

[4] http://greco.dit.upm.es/~david/TAR/trabajos2002/10-Infraestructura-ISP-Andoni-Perez-res.pdf: Infraestructura de un ISP.

[5] ftp://ftp.linksys.com/datasheet/befsr41v3_ds.pdf: EtherFast Cable/DSL Router with 4-Port Switch.

[6] ftp://ftp.linksys.com/datasheet/befsr81ds.pdf: EtherFast Cable/DSL Router.

[7] http://www.microsoft.com/spain/servidores/windowsserver2003/evaluation/overview/technologies/iis.aspx: Novedades de los Servicios de Internet Information Server 6.0.

[8] ftp://ftp.ipswitch.com/ipswitch/manuals/whatsupg.pdf. WhatsUp Gold - User's Guide.

[9] http://bandwidthcontroller.com/features.html: Bandwidth Controller.

[10] http://www.merakmailserver.com/Products/Merak_Mail_Server/: Merak Mail Server Software.

[11] http://www.proxim.com/learn/library/datasheets/AP-2000_US.pdf: ORiNOCO AP-2000.

[12] ftp://ftp.linksys.com/pdf/wap11_v28_ug.pdf: Wireless-B Access Point.

[13] http://www.proxim.com/support/all/orinoco/manuals/pdf/EC_datasheet.pdf: Datasheet del WAVE LAN.

[14] ftp://ftp.linksys.com/datasheet/wet11_v2_ds.pdf: Wireless-B Ethernet Bridge.

CAPÍTULO V

5 OPTIMIZACIÓN DEL PROVEEDOR DE SERVICIOS DE INTERNET

5.1 USO DE LAS REDES WLANs EN EL ISP

Como se indicó anteriormente, las redes WLAN tienen varios tipos de aplicación que pueden darse tanto en ambientes internos como en ambientes externos. En el caso del ISP en estudio, estas redes WLAN han sido utilizadas en ambientes externos para establecer enlaces de última milla y enlaces de *backbone*. Esto ha permitido resolver varios problemas en lo que se refiere a las redes de acceso al cliente, problemas que serían muy difíciles de solventar con tecnologías de redes cableadas o acarrearía grandes costos si se desease utilizar otro tipo de tecnología inalámbrica.

El uso de este tipo de tecnología al igual que cualquier otra tiene sus ventajas y desventajas. Sin embargo, son mucho más las ventajas que presentan lo que ha provocado que los administradores opten por seguir utilizando esta tecnología y no traten de migrar a otra para continuar entregando el servicio de Internet a los clientes del ISP. A continuación se describen las ventajas y desventajas más importantes del uso de este tipo de redes dentro del ISP.

5.1.1 VENTAJAS DEL USO DE REDES WLAN

El uso de la tecnología WLAN 802.11b para la entrega de enlaces de última milla y enlaces de *backbone* dentro del ISP, presenta muchas ventajas. Entre las más importantes se tienen:

- ✓ Las redes WLAN según el estándar 802.11b utilizan tecnología inalámbrica de espectro ensanchado que trabaja en la banda de frecuencia de los 2.4

GHz. Esta banda de frecuencias es de uso libre por lo que no se necesita de licencias para su utilización.

- ✓ Este tipo de redes por ser inalámbricas permite llegar a clientes donde las redes cableadas que pueden ser de cobre, fibra óptica, etc., no llegan.
- ✓ Un enlace inalámbrico con tecnología WLAN 802.11b se puede montar mucho más rápido en comparación con otras tecnologías cableadas e incluso inalámbricas. Esto principalmente debido a su fácil instalación y la fácil configuración de equipos.
- ✓ Los costos de los equipos son mucho más económicos en comparación con otras tecnologías inalámbricas.
- ✓ Los costos de operación y mantenimiento igualmente son mucho más económicos que cualquier otra tecnología.
- ✓ Existe una extensa gama de productos en el mercado que permiten escoger la solución más adecuada para cada situación. Esto se debe a que estas redes tienen una gran trayectoria y muchos fabricantes han escogido a esta tecnología como una opción más dentro de sus soluciones inalámbricas.

Todas estas ventajas han hecho que los administradores del ISP vean a las redes WLAN 802.11b como una de las mejores opciones en lo referente a accesos de última milla, convirtiéndose de esta forma en uno de los principales métodos de acceso; de ahí el nombre de Proveedor de Servicios de Internet Inalámbrico.

Cabe destacar que actualmente existen otros tipos de tecnologías inalámbricas que podrían ser una mejor opción para redes de acceso, pero se debe tomar muy en cuenta que la tecnología WLAN 802.11b ya está implementada y el hecho de querer adoptar una nueva tecnología haría necesario realizar una inversión muy grande debido a que habría que cambiar gran parte de la infraestructura. Esta solución estaría lejos de volverse realidad ya que el costo-beneficio que traería no sería nada rentable.

5.1.2 DESVENTAJAS DEL USO DE REDES WLAN

En la misma forma que el uso de las redes WLAN presentan una serie de ventajas para el ISP, estas redes también presentan desventajas que a la larga pueden llegar a causar grandes inconvenientes en el funcionamiento del ISP si no se solventan en forma adecuada. Entre las principales desventajas se tienen:

- ✓ Los enlaces con la tecnología WLAN 802.11b hacen uso de la máxima velocidad de transmisión que se pueda establecer en el enlace, la cual depende exclusivamente de la distancia que separan a los dispositivos. Esto impide asignar una velocidad de transmisión específica (ancho de banda) en el enlace entre el ISP y el cliente, lo cual si es posible realizar con el uso de otros tipos de tecnologías de última milla.
- ✓ Este tipo de enlaces debido a las características que tiene la tecnología 802.11b generan una gran cantidad de *broadcast*, el cual puede llegar a ser un grave problema sino se logra segmentar en forma adecuada el dominio de colisión en la red del ISP.
- ✓ Algunos equipos están diseñados para ambientes caseros y de pequeñas empresas, por lo que pueden presentar una serie de inconvenientes en redes de alto tráfico y de uso constante como es el caso de enlaces de *backbone*.

Estas desventajas son un grave problema para el desempeño correcto del ISP, algunas desventajas son tolerables con un bajo número de clientes como el es el caso del *broadcast*, otras se han podido remediar parcialmente como es el caso de la asignación de velocidad de transmisión pero la frecuente inhibición de equipos es algo que no se ha podido solventar.

5.2 PROBLEMAS QUE CONLLEVA EL USO DE LAS REDES WLAN DENTRO DEL ISP

La tecnología WLAN según el estándar 802.11b ha permitido al ISP *dar* el servicio de Internet a sitios donde el acceso mediante redes cableadas es casi imposible,

a costos y rapidez de instalación muy por debajo de lo que implica dar un servicio con otro tipo de tecnología inalámbrica o cableada. Sin embargo, el constante crecimiento del número de enlaces de este tipo puede conllevar a graves problemas e incluso al colapso total de la red del ISP. Los tres principales problemas que pueden presentarse a futuro con el uso de esta tecnología son:

1. Falla en los enlaces de *backbone* a causa de inhibición en los equipos WLAN
2. Saturación de la red a causa del *broadcast* que generan este tipo de enlaces
3. Imposibilidad para limitar la velocidad de transmisión a nuevos clientes

En las siguientes secciones se explicara cada uno de estos problemas más a fondo.

5.2.1 FALLA EN LOS ENLACES DE BACKBONE

Como se indicó en el capítulo anterior, actualmente existen tres enlaces principales que interconectan los cuatro nodos que conforman el ISP, mediante enlaces inalámbricos con tecnología WLAN 802.11b. Estos enlaces son las arterias principales por las que circula el tráfico de muchos clientes, si uno de estos enlaces llega a sufrir algún inconveniente, la pérdida del servicio de Internet se verá reflejada inmediatamente en todos los clientes que ingresan a través del nodo que fue afectado, disminuyendo así el *uptime* y la calidad del servicio.

Los enlaces de *backbone* están experimentando y pueden experimentar fallas principalmente a causa de dos motivos:

1. Los equipos que se utilizan para este fin no soportan grandes cantidades de tráfico, ya que son equipos muy sencillos diseñados para ser usados en redes pequeñas como es el caso de los puntos de acceso AP-2000, los puntos de acceso WAP11 y las tarjetas cliente Cisco Aironet. Con el crecimiento constante del ISP el tráfico que circula por estos enlaces

también va a crecer, esto puede llegar a colapsar los equipos y por ende los enlaces. Este problema ya es un inconveniente frecuente dentro del ISP lo que provoca que los enlaces queden fuera de servicio hasta que se logre resetear manualmente a los equipos involucrados.

2. Los enlaces de *backbone* trabajan en la banda de los 2.4 GHz al igual que los enlaces de última milla por lo que si el número de estos enlaces crece en un nodo, estos enlaces de última milla pueden llegar a causar interferencias en los enlaces de *backbone* convirtiéndolo así en un enlace inestable y no útil.

Cabe recalcar que este tipo de enlaces tienen velocidades de transmisión bajas como es 1, 2 y en el mejor de los casos 5.5 Mbps, esto se debe a las largas distancias que existen entre los dispositivos. Para evitar mayores problemas de inhibición en los equipos, normalmente se configuran con la mínima velocidad de transmisión que es de 1 Mbps.

5.2.2 SATURACIÓN DE LA RED A CAUSA DEL BROADCAST [1]

Para comunicarse con todos los dominios de colisión, los protocolos de la tecnología WLAN utilizan tramas de *broadcast* y *multicast* a nivel de Capa 2 según el modelo OSI. Cuando un dispositivo con esta tecnología necesita comunicarse con todos los *hosts* de la red, envía una trama de *broadcast* con una dirección MAC destino 0xFFFFFFFFFFFF. Esta es una dirección a la cual debe responder la tarjeta de interfaz de red (*Network Interface Card*, NIC) de cada *host*.

Los dispositivos WLAN como cualquier dispositivo de capa 2, deben inundar todo el tráfico de *broadcast* y *multicast* para establecer una comunicación entre sí. La acumulación de tráfico de *broadcast* y *multicast* de cada dispositivo de la red se denomina radiación de *broadcast*. En algunos casos, la circulación de radiación de *broadcast* puede saturar la red, entonces no hay ancho de banda disponible para los datos de las aplicaciones. En este caso, no se pueden establecer las conexiones en la red, y las conexiones existentes pueden descartarse, algo que se conoce como tormenta de *broadcast*. La probabilidad de las tormentas de

broadcast aumenta a medida que crece la red conmutada, es decir cada vez que se agregue un nuevo dispositivo WLAN a la red.

Tomando en cuenta lo indicado anteriormente, si en un nodo del ISP continuamente se agregan nuevos dispositivos WLAN sin segmentar el dominio de *broadcast*, se puede llegar a un punto crítico en el cual el *broadcast* generado por estos dispositivos colapse el ancho de banda de la red. De ahí la necesidad de establecer una solución para poder segmentar el dominio de *broadcast* y no dejar de lado el uso de esta tecnología.

5.2.3 IMPOSIBILIDAD PARA LIMITAR LA VELOCIDAD DE TRANSMISIÓN A NUEVOS CLIENTES

Otro de los problemas latentes que conlleva el uso de la tecnología WLAN 802.11b para enlaces de última milla, es la dificultad que existe para limitar la velocidad de transmisión en este tipo de enlaces. Cuando un cliente corporativo contrata el servicio de Internet a través del ISP, éste lo realiza en función de una velocidad de transmisión específica de acuerdo a sus necesidades. Por lo tanto, si esto no se controla de manera adecuada será imposible establecer calidad de servicio a cada uno de los nuevos clientes que llegue a tener el ISP.

Actualmente el control de velocidad de transmisión se lo realiza a través del uso de un paquete de software, el cual lo limita, mediante el uso de filtros a nivel de capa 3, como ya se explicó en el capítulo anterior. Esta solución actualmente ya está presentando inconvenientes a medida que crece el número de clientes dentro del ISP. Entre los principales problemas que implica el uso de esta solución se tienen:

- ✓ La administración de la velocidad de transmisión es centralizada y se encuentra montada sobre un servidor con plataforma Windows, el cual es muy susceptible a fallas, ataques por parte de *hackers* y virus. En caso de que este servidor falle todos los clientes colapsarían ya que todo el tráfico pasa a través de este servidor antes de su salida hacia Internet.

- ✓ El paquete de software *Bandwith Controller* hace uso de filtros para delimitar la velocidad de transmisión, permitiendo únicamente 20 filtros activos a la vez. Esto quiere decir que solamente se puede delimitar la velocidad a 20 clientes. En caso de necesitar limitar el tráfico a un mayor número de clientes este software ya no sería útil.

Como se puede apreciar, la solución que se ha dado a este problema puede llegar a ser momentánea y no soportar el constante crecimiento del ISP. Es una solución que proporciona una latencia considerable no sólo por el proceso que efectúa el software para delimitar la velocidad sino por el doble recorrido que realiza el tráfico antes de salir al Internet. Además de esto con grandes cantidades de tráfico pueden llegarse a producir cuellos de botella en el punto de entrada del servidor de ancho de banda lo que limitaría notablemente la velocidad de toda la red.

5.3 CAMBIOS PARA OPTIMIZAR LA INFRAESTRUCTURA DEL ISP

Para los problemas indicados en la sección anterior, se pueden dar una serie de cambios a la infraestructura para solventarlos y permitir que el ISP continúe prestando su servicio mediante el uso de redes WLAN 802.11b en la última milla. Los principales cambios que se pueden efectuar son:

- ✓ Mejorar los enlaces de *backbone*
- ✓ Segmentar el dominio de *broadcast*
- ✓ Asignar la velocidad de transmisión en los enlaces de última milla

En las siguientes secciones se indicará en que consiste cada uno de estas soluciones, cual de estos cambios serían los más recomendables y como implementarlos para solventar los futuros problemas que se pueden presentar al seguir utilizando las redes WLAN 802.11b como tecnología de última milla.

5.3.1 REDIMENSIONAMIENTO DE LOS ENLACES PRINCIPALES [2], [3], [4], [5]

Los tres enlaces inalámbricos que interconectan los nodos de la red pueden ser mejorados sustancialmente, para lo cual se podría seguir utilizando la tecnología 802.11b y cambiar únicamente los equipos que establecen estos enlaces, sin embargo tomando en cuenta la posibilidad de que se podrían generar interferencias por parte de los enlaces de última milla es recomendable utilizar equipos con tecnología inalámbrica que trabajen en una banda de frecuencia diferente a la utilizada por los equipos con tecnología 802.11b.

En el mercado local existen varios tipos de equipos que son muy eficientes y que trabajan en la banda libre de los 5.8 GHz, los cuales pueden servir para optimizar el uso de estos enlaces. Entre estos equipos se tienen:

- ✓ *Bridges* inalámbricos Tsunami QuickBridge II 60 de Proxim Wireless Networks, los cuales permiten velocidades de transmisión de 18 a 54 Mbps en distancias de 10 a 5 km respectivamente.
- ✓ *Bridges* inalámbricos Tsunami QuickBridge 20, los cuales permiten velocidades de transmisión de 18 Mbps en enlaces de hasta 10 km.
- ✓ *Bridges* inalámbricos Cisco Aironet 1410, los cuales permiten velocidades de 54 Mbps en distancias de hasta 21 Km y 9 Mbps en distancias de hasta 37 km.
- ✓ Multiplexores Inalámbricos Airmux-104 de Rad Data Comunications, los cuales permiten velocidades de 2.3 Mbps en distancias de hasta 24 km.

En la tabla 5.1 se puede apreciar un cuadro comparativo de las características de estos equipos que puede ayudar a la selección del más adecuado.

Como se indica más adelante, los enlaces principales que interconectan los nodos del ISP en estudio no sobrepasan los 5 km. Tomando en cuenta este factor de alcance, la velocidad de transmisión y el costo, los equipos más adecuados para el caso de estudio son los Tsunami QuickBridge 20. Además de esto, cabe

destacar que estos equipos poseen un desempeño muy bueno incluso en condiciones extremas en comparación con otros equipos (Estos equipos son muy utilizados por empresas locales de últimas millas, las cuales han dado testimonio de la fidelidad de los mismos, tal es el caso de la empresa ISEYCO C.A.), entregando una confiabilidad de hasta el 99.995% en las peores condiciones según el fabricante, lo que los hace ideales para el uso en los enlaces principales. Cabe recalcar que estos equipos trabajan en la banda de los 5.8 GHz lo que los hace mucho más convenientes, ya que se elimina por completo la posibilidad de que se produzcan interferencias en estos enlaces por parte de los enlaces de última milla como ya se indicó anteriormente.

Equipos	Tsunami QuickBridge II 60	Tsunami QuickBridge 20	Cisco Aironet 1410	Multiplexor Airmux-104
Velocidad de Transmisión	54 Mbps	18 Mbps	54 Mbps	2.3 Mbps Full Duplex
Banda de Frecuencias	5.725 - 5.850 GHz	5.725 – 5.850 GHz	5.725 – 5.850 GHz	5.725 – 5.850 GHz
Velocidad Interfaz LAN	10/100 Base-TX	10/100 Base-TX	10/100 Base-TX	10/100 Base-TX
Interfaz de Red	RJ-45	RJ-45	RJ-45	RJ-45
Tipo de Chasis	ODU con antena integrada	ODU con antena integrada	ODU sin antena integrada	ODU con antena integrada y IDU
Potencia de Transmisión	36 dBm	36 dBm	24 dBm	16.7 dBm
Alcance	4 km	9.7 km	21 km	16 km
Costo Aproximado	$ 6999	$ 4499	$ 8882	$ 5130

Tabla 5.1. Características de Equipos para Enlaces de Backbone

Los cuatro nodos del ISP en estudio que ya se describieron en el capítulo anterior, se encuentran situados estratégicamente sobre la ciudad de Quito para poder dar cobertura a los sectores más importantes en los cuales existe una alta demanda del servicio de Internet corporativo. Las coordenadas geográficas, la altura y la ubicación en la que se encuentran estos nodos son:

1. Nodo Principal

   Latitud: 00°10'38.92" S

   Longitud: 78°28'38.92" W

   Altura: 2770 m

Ubicación: Av. República del Salvador y Portugal

2. Nodo 1

   Latitud: 00°12'09.73" S

   Longitud: 78°29'47.03" W

   Altura: 2785 m

   Ubicación: Av. 10 de Agosto y Patria

3. Nodo 2

   Latitud: 00°08'24.32" S

   Longitud: 78°27'09.73" W

   Altura: 2900 m

   Ubicación: Loma de Puengasí

4. Nodo 3

   Latitud: 00°14'35.68" S

   Longitud: 78°29'50.27" W

   Altura: 3078 m

   Ubicación: Barrio Buenos Aires

Como ya se indicó anteriormente se hará uso de los equipos Tsunami QuickBridge 20 de Proxim Wireless Networks en los tres enlaces inalámbricos. Para el cálculo de la confiabilidad de los tres enlaces principales, serán útiles los siguientes datos técnicos entregados por el fabricante:

- ✓ Frecuencias de trabajo:
  - 5.740 GHz, que se utilizará para el enlace principal 1
  - 5.774 GHz, que se utilizará para el enlace principal 2
  - 5.809 GHz, que se utilizará para el enlace principal 3
- ✓ Potencia de transmisión:
  - 15 dBm
- ✓ Ganancia de la antenas:
  - 20 dbi
- ✓ Sensibilidad de los equipos (Umbral de Recepción):
  - -89 dBm

5.3.1.1 Redimensionamiento del Enlace Principal 1

5.3.1.1.1 Levantamiento del Perfil Topográfico

El enlace principal 1, interconecta el nodo principal con el nodo 1. Antes de realizar el redimensionamiento de este enlace, primeramente se debe conocer el perfil topográfico que existe entre estos dos nodos; para esto se hizo uso de cartas topográficas de la ciudad de Quito en la escala de 1:50,000. En la figura 5.1 se puede apreciar la ubicación de los nodos que conforman en enlace principal 1, sobre la carta topográfica.

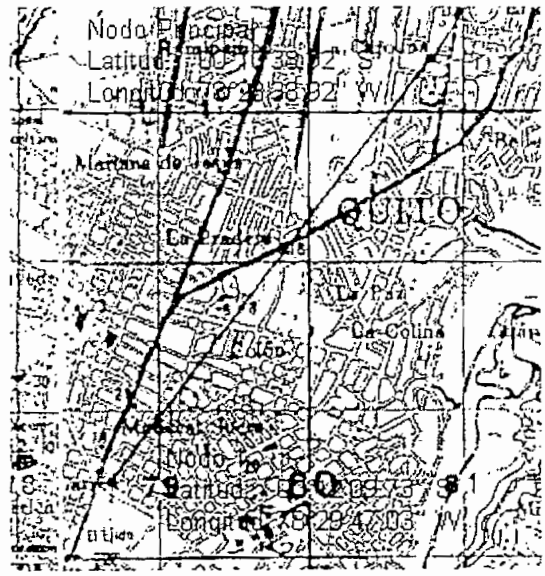


Figura 5.1. Enlace Principal 1

En la tabla 5.2 se puede apreciar los datos obtenidos luego del levantamiento topográfico.

En el nodo principal los equipos de radio serán colocados sobre la misma torre en la que se encuentran montados los puntos de acceso que conforman este enlace actualmente; esta torre tiene una altura de 12 metros y se encuentra instalada sobre la terraza de un edificio de 30 metros ubicado en la Av. República del Salvador y Portugal. En el nodo 1 los equipos de radio también serán colocados sobre la misma torre en la que se encuentran montados los puntos de acceso

actualmente al igual que en el nodo principal; esta torre tiene una altura de 12 metros y se encuentra instalada sobre la torre de un edificio de 30 metros ubicado en la Av. 10 de Agosto y Patria.

Distancia (km)	Altura (m)	Distancia (km)	Altura (m)
Nodo Principal	2770	2	2778
0,2	2770	2,2	2779
0,4	2771	2,4	2780
0,6	2772	2,6	2780
0,8	2773	2,8	2781
1	2774	3	2782
1,2	2775	3,2	2783
1,4	2776	3,4	2784
1,6	2777	Nodo 1	2785
1,8	2777		

Tabla 5.2. Datos Topográficos Enlace Principal 1

La distancia que existe entre estos dos nodos es de 3495.062 m. Estos datos serán útiles más adelante para realizar el cálculo del radio de la primera zona de Fresnel.

5.3.1.1.2 Cálculo de la Primera Zona de Fresnel [6], [7]

El radio de la primera zona de Fresnel permite definir la condición de visibilidad entre antenas, de forma que mientras no exista un obstáculo dentro de la primera zona de Fresnel se considera que la trayectoria no ha sido obstruida. Por el contrario cuando, el obstáculo se encuentra dentro de la primera zona de Fresnel existirá una disminución apreciable en la potencia recibida, por lo que se considera que la trayectoria ha sido obstruida. De forma práctica, al estar la energía concentrada cerca del rayo directo, si el obstáculo no penetra en más de un 40% del radio de la primera zona de Fresnel se suele considerar que dicho obstáculo no contribuye significativamente a la atenuación por difracción.

El radio de la primera zona de Fresnel se debe calcular con la siguiente fórmula:

$$R1 = \sqrt{\lambda \frac{d1d2}{d}}$$

Reemplazando la expresión $\lambda = \frac{c}{f}$ en la ecuación se obtiene:

$$R1 = \sqrt{\frac{c}{f} \frac{d1d2}{d}}$$

En donde:

$R1$ = Radio de la primera zona de Fresnel [m]
$d1$ = Distancia a un extremo del trayecto [m]
$d2$ = Distancia al extremo opuesto del trayecto [m]
d = Longitud total del trayecto [m]
λ = Longitud de Onda [m]
c = Velocidad de la Luz [3×10^8 m/s]
f = Frecuencia [Hz]

El radio máximo de esta zona se da cuando $d1 = d2 = \frac{d}{2}$ obteniéndose:

$$R1 = \frac{1}{2} \sqrt{\frac{c}{f} d}$$

Para el enlace principal 1 la longitud del trayecto es 3495.06 m y la frecuencia es de 5.740 GHz con lo que se obtiene:

$$R1 = \frac{1}{2} \sqrt{\left(\frac{3 \times 10^8 \frac{m}{s}}{5.740\,GHz} \right) (3495.06\,m)}$$

$$R1 = 6.76\,m$$

Con los datos del levantamiento topográfico y el radio de la primera zona de Fresnel se puede trazar el perfil topográfico y la primera zona de Fresnel del enlace principal 1, como se puede apreciar en la figura 5.2.

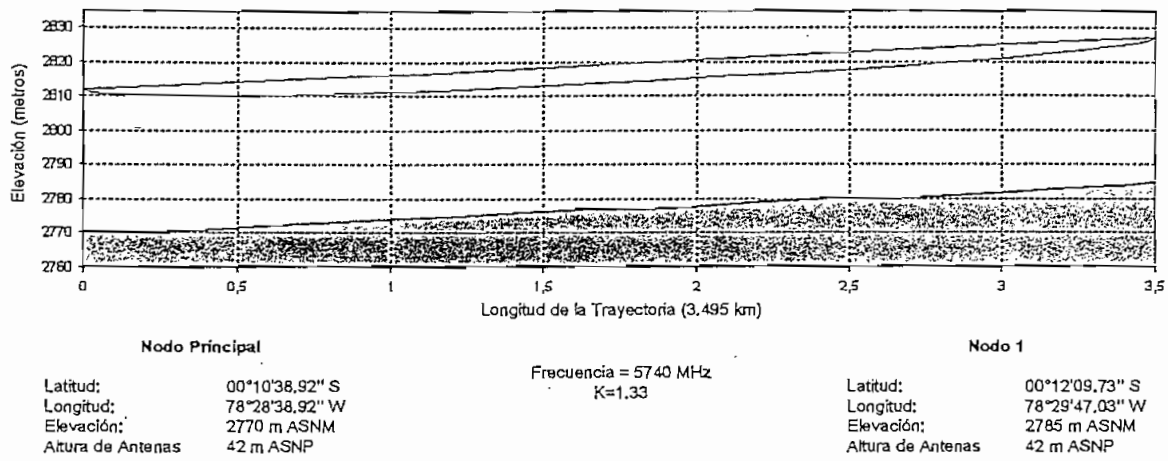


Figura 5.2. Perfil Topográfico y Primera Zona de Fresnel del Enlace Principal 1

5.3.1.1.3 Cálculo de la Potencia Recibida [6], [8], [9]

La potencia de recepción se debe calcular con la expresión:

$$Pr = Pt + Gt + Gr - Lp - Lf - Lb$$

En donde:

Pt = Potencia del transmisor [dB]

Gt = Ganancia de la antena transmisora [dB]

Gr = Ganancia de la antena receptora [dB]

Lp = Pérdida por trayectoria en el espacio libre [dB]

Lf = Pérdida del alimentador de guías de ondas [dB]

Lb = Pérdida total de acoplamiento [dB]

La atenuación de la señal en filtros y acopladores es un dato que normalmente debe facilitar el fabricante, en el caso de los equipos que se utilizarán el fabricante

no lo proporciona de manera que se asume un valor máximo de *Lb* = 2.4 *dB*. Como la antena y el transmisor se encuentra dentro de un mismo dispositivo externo, se asume un valor *Lf* = 0 *dB*.

La pérdida por trayectoria en el espacio libre se debe calcular con la siguiente expresión:

$$Lp = 92.4 + 20\log f + 20\log d$$

En donde:

f = Frecuencia [GHz]

d = Longitud total del trayecto en [km]

Reemplazando los valores correspondientes para este enlace, se tiene:

$$Lp = 92.4 + 20\log(5.740) + 20\log(3.495)$$

$$Lp = 118.447dB$$

Con este valor se calcula la potencia en la recepción:

$$\Pr = Pt + Gt + Gr - Lp - Lf - Lb$$

$$\Pr = 15dBm + 20dB + 20dB - 118.447dB - 0dB - 2.4dB$$

$$\Pr = -65.847dBm$$

Como la sensibilidad de los equipos o el umbral de recepción *Ur* = -89 *dBm*, se puede afirmar que la señal es recibida de manera adecuada; sin embargo para relacionar el margen de desvanecimiento frente a la confiabilidad del enlace, se aplica la fórmula de *Barnett-Vignant*:

$$FM = 30\log d + 10\log 6(ABf) - 10\log(1-R) - 70$$

En donde:

FM = Margen de desvanecimiento [dB]

$(1-R)=\frac{0.0001d}{400}$ = Objetivo de Confiabilidad

d = Longitud del trayecto [km]

A = Factor de rugosidad

= 4 para terreno plano sobre agua

= 1 para terreno promedio

= 0.25 para terreno rugoso

B = Factor climático

= 0.5 para zonas calientes y húmedas

= 0.25 para zonas intermedias

= 0.125 para áreas montañosas o muy secas

f = Frecuencia [GHz]

El margen de desvanecimiento no es más que un "factor de amortiguamiento" incluido en la ecuación de ganancia del sistema (*Gs = Pt –Pr*), que considera las características no ideales y menos predecibles de la propagación de ondas de radio, como la propagación de múltiples trayectorias (pérdida de múltiples trayectorias) y sensibilidad a superficies rocosas. Estas características causan condiciones atmosféricas anormales temporales que alteran la perdida de la trayectoria de espacio libre y usualmente son perjudiciales para el funcionamiento general del sistema.

Para el cálculo del margen de desvanecimiento de los enlaces del ISP en estudio se asumen: A=1, B=0.25 y un objetivo de confiabilidad (1 - *R*) = 99.99%.

Con todos los datos anteriores, se determina el margen de desvanecimiento en el enlace principal 1:

$$FM = 30\log(3.495) + 10\log 6(1)(0.25)(5.740) - 10\log\left(\frac{(0.0001)(3.495)}{400}\right) - 70$$

$$FM = 16.24dB$$

Obtenido el margen de desvanecimiento, se determina la potencia recibida incluyendo el objetivo de confiabilidad:

$$\Pr' = \Pr - FM$$
$$\Pr' = -65.847dBm - 16.24dB$$
$$\Pr' = -82.087dBm$$

Como se pude apreciar esta potencia aún está dentro del rango de sensibilidad del equipo por lo que se afirma que el objetivo de confiabilidad si se cumple. Con este objetivo de confiabilidad se determina el tiempo en el que el enlace estará fuera de operación:

$$Tf = (1 - 0.9999)(365\ días)(24\ horas)$$
$$Tf = 0.876\ horas / año$$

El tiempo en el que el enlace se quedaría por fuera, es de 0.876 horas por cada año. Si este tiempo lo distribuimos uniformemente en los 365 días del año se obtiene que el tiempo de pérdida del enlace en un día ordinario es de 8.64 segundos, esto en el peor de los casos.

5.3.1.2 Redimensionamiento del Enlace Principal 2

5.3.1.2.1 Levantamiento del Perfil Topográfico

El enlace principal 2, interconecta el nodo principal con el nodo 2. Para el levantamiento de datos se utilizaron cartas topográficas de la ciudad de Quito en la escala de 1:50,000. En la figura 5.3 se puede apreciar la ubicación de los nodos que conforman en enlace principal 2, sobre la carta topográfica.

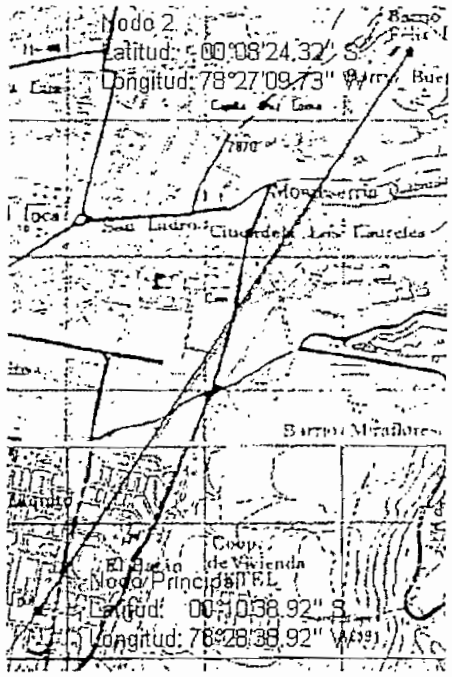


Figura 5.3. Enlace Principal 2

En la tabla 5.3 se puede apreciar los datos obtenidos luego del levantamiento topográfico.

Distancia (km)	Altura (m)	Distancia (km)	Altura (m)
Nodo Principal	2770	2,6	2802
0,2	2770	2,8	2804
0,4	2771	3	2806
0,6	2771	3,2	2808
0,8	2771	3,4	2808
1	2772	3,6	2809
1,2	2772	3,8	2809
1,4	2773	4	2810
1,6	2774	4,2	2820
1,8	2775	4,4	2850
2	2775	4,6	2875
2,2	2790	4,8	2890
2,4	2800	Nodo 2	2900

Tabla 5.3. Datos Topográficos Enlace Principal 2

En el nodo 1 los equipos de radio serán montados sobre la misma torre descrita en la sección anterior. En el nodo 2 los equipos de radio serán montados sobre una torre de 24 metros ubicada en el sector Loma de Puengasí, la cual alberga

los puntos de acceso que conforman este enlace actualmente.

La distancia que existe entre los dos nodos es de 4969.728 m. Estos datos serán útiles más adelante para realizar el cálculo del radio de la primera zona de Fresnel.

5.3.1.2.2 Cálculo de la Primera Zona de Fresnel

Para el cálculo de la primera zona de Fresnel, se hace uso de la expresión:

$$R1 = \frac{1}{2}\sqrt{\frac{c}{f}d}$$

En el enlace principal 2 la longitud del trayecto es de 4969.728 m y la frecuencia que se empleará es de 5.774 GHz, con lo que se obtiene:

$$R1 = \frac{1}{2}\sqrt{\left(\frac{3\times10^{8}\,\frac{m}{s}}{5.774\,GHz}\right)(4969.728\,m)}$$

$$R1 = 8.03\,m$$

Con los datos del levantamiento topográfico y el radio de la primera zona de Fresnel se traza el perfil topográfico y la primera zona de Fresnel del enlace principal 2, respectivamente; como se puede apreciar en la figura 5.4.

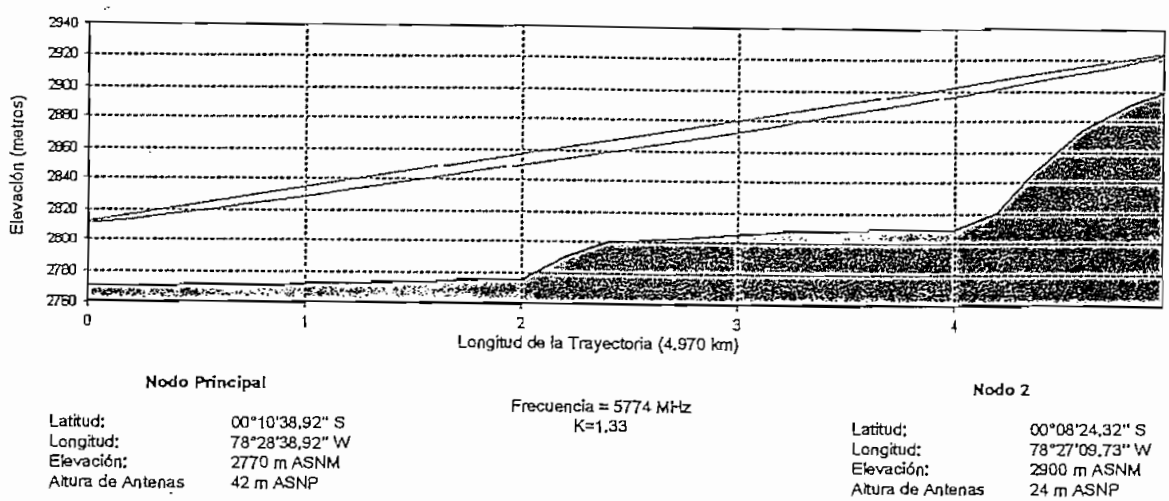


Figura 5.4. Perfil Topográfico y Primera Zona de Fresnel del Enlace Principal 2

5.3.1.2.3 Cálculo de la Potencia Recibida

Para el cálculo de la potencia recibida, primeramente se calcula la pérdida por trayectoria en el espacio libre:

$$Lp = 92.4 + 20\log f + 20\log d$$

$$Lp = 92.4 + 20\log(5.774GHz) + 20\log(4.970km)$$

$$Lp = 121.557dB$$

Con este valor se calcula la potencia en la recepción:

$$\mathrm{Pr} = Pt + Gt + Gr - Lp - Lf - Lb$$

$$\mathrm{Pr} = 15dBm + 20dB + 20dB - 121.557dB - 0dB - 2.4dB$$

$$\mathrm{Pr} = -68.957dBm$$

Luego se calcula el margen de desvanecimiento:

$$FM = 30\log d + 10\log 6(ABf) - 10\log(1-R) - 70$$

$$FM = 30\log(4.970) + 10\log 6(1)(0.25)(5.774) - 10\log\left(\frac{(0.0001)(4.970)}{400}\right) - 70$$

$$FM = 19.323dB$$

Finalmente, se calcula la potencia recibida incluyendo el objetivo de confiabilidad:

$$Pr' = Pr - FM$$
$$Pr' = -68.957dBm - 19.323dB$$
$$Pr' = -88.28dBm$$

Como se puede apreciar esta potencia aún está dentro del rango de sensibilidad del equipo *Ur* = -89 *dBm* por lo que se afirma que el objetivo de confiabilidad si se cumple. Con este objetivo de confiabilidad se determina el tiempo en el que el enlace estará fuera de operación:

$$Tf = (1 - 0.9999)(365días)(24horas)$$
$$Tf = 0.876\ horas / año$$

El tiempo en el que el enlace se quedaría por fuera, es de 0.876 horas por cada año. Si este tiempo lo distribuimos uniformemente en los 365 días del año se obtiene que el tiempo de pérdida del enlace en un día ordinario es de 8.64 segundos, esto en el peor de los casos.

5.3.1.3 Redimensionamiento Enlace Principal 3

5.3.1.3.1 Levantamiento del Perfil Topográfico

El enlace principal 3, interconecta el nodo 1 con el nodo 3. Para el levantamiento de datos se utilizaron cartas topográficas de la ciudad de Quito en la escala de 1:50,000. En la figura 5.5 se puede apreciar la ubicación de los nodos que conforman en enlace principal 3, sobre la carta topográfica.

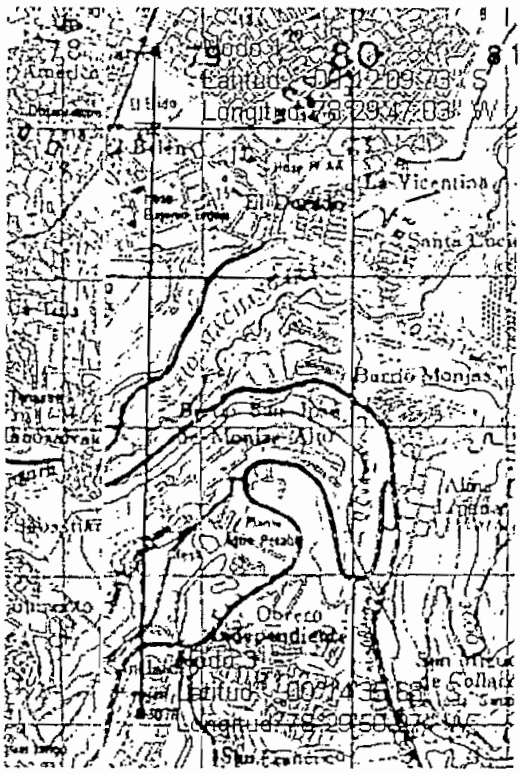


Figura 5.5. Enlace Principal 3

En la tabla 5.4 se puede apreciar los datos obtenidos luego del levantamiento topográfico.

Distancia (km)	Altura (m)	Distancia (km)	Altura (m)
Nodo 1	2785	2,4	2860
0,2	2791	2,6	2868
0,4	2797	2,8	2875
0,6	2803	3	2882
0,8	2809	3,2	2889
1	2815	3,4	2890
1,2	2821	3,6	3012
1,4	2827	3,8	3034
1,6	2833	4	3050
1,8	2839	4,2	3062
2	2846	Nodo 3	3078
2,2	2853		

Tabla 5.4. Datos Topográficos Enlace Principal 3

En el nodo 1 los equipos de radio serán montados sobre la misma torre descrita en las secciones anteriores. En el nodo 3 los equipos de radio serán montados

sobre una torre de 24 metros ubicada en el Barrio Buenos Aires, la cual alberga los puntos de acceso que conforman actualmente este enlace.

La distancia que existe entre los dos nodos es de 4483.985 m. Estos datos serán útiles más adelante para realizar el cálculo del radio de la primera zona de Fresnel.

5.3.1.3.2 Cálculo de la Primera Zona de Fresnel

Para el cálculo de la primera zona de Fresnel, se hace uso de la expresión:

$$R1 = \frac{1}{2}\sqrt{\frac{c}{f}d}$$

En el enlace principal 3 la longitud del trayecto es de 4483.985 m y la frecuencia que se empleará es de 5.809 GHz, con lo que se obtiene:

$$R1 = \frac{1}{2}\sqrt{\left(\frac{3\times10^{8}\,\frac{m}{s}}{5.809\,GHz}\right)(4483.985\,m)}$$

$$R1 = 7.61\,m$$

Con los datos del levantamiento topográfico y el radio de la primera zona de Fresnel se traza el perfil topográfico y la primera zona de Fresnel del enlace principal 2, respectivamente; como se puede apreciar en la figura 5.6.

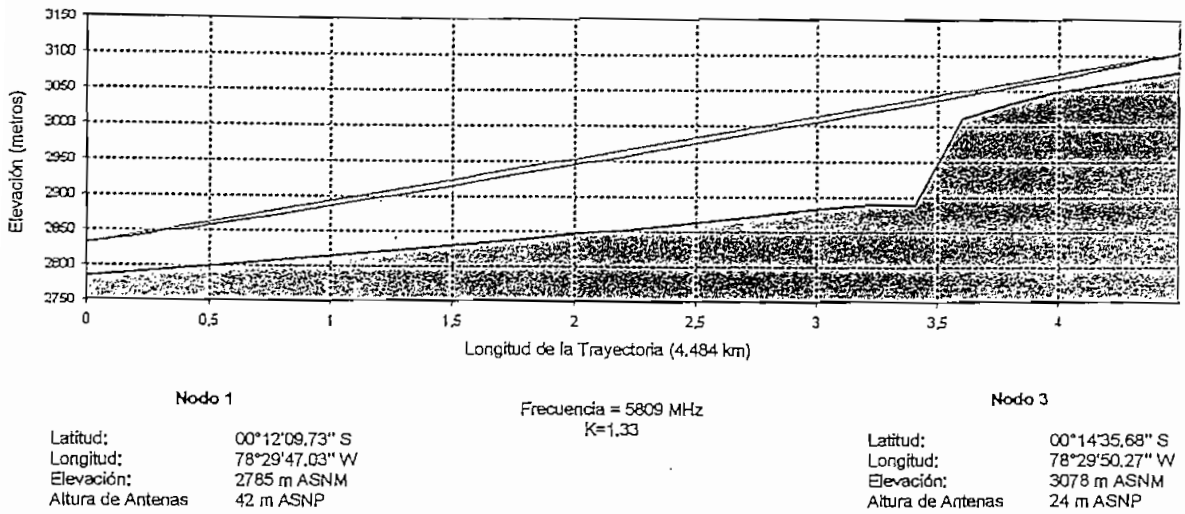


Figura 5.6. Perfil Topográfico y Primera Zona de Fresnel del Enlace Principal 3

5.3.1.3.3 Cálculo de la Potencia Recibida

Para el cálculo de la potencia recibida, primeramente se calcula la pérdida por trayectoria en el espacio libre:

$$Lp = 92.4 + 20\log f + 20\log d$$
$$Lp = 92.4 + 20\log(5.809GHz) + 20\log(4.484km)$$
$$Lp = 120.715dB$$

Con este valor se calcula la potencia en la recepción:

$$\mathrm{Pr} = Pt + Gt + Gr - Lp - Lf - Lb$$
$$\mathrm{Pr} = 15dBm + 20dB + 20dB - 120.715dB - 0dB - 2.4dB$$
$$\mathrm{Pr} = -68.115dBm$$

Luego se calcula el margen de desvanecimiento:

$$FM = 30\log d + 10\log 6(ABf) - 10\log(1-R) - 70$$
$$FM = 30\log(4.484) + 10\log 6(1)(0.25)(5.809GHz) - 10\log\left(\frac{(0.0001)(4.484)}{400}\right) - 70$$

$$FM = 18.456dB$$

Finalmente, se calcula la potencia recibida incluyendo el objetivo de confiabilidad:

$$Pr' = Pr - FM$$
$$Pr' = -68.115dBm - 18.45dB$$
$$Pr' = -86.565dBm$$

Como se puede apreciar esta potencia aún está dentro del rango de sensibilidad del equipo *Ur* = -89 *dBm* por lo que se afirma que el objetivo de confiabilidad si se cumple. Con este objetivo de confiabilidad se determina el tiempo en el que el enlace estará fuera de operación:

$$Tf = (1 - 0.9999)(365días)(24horas)$$
$$Tf = 0.876\ horas/año$$

El tiempo en el que el enlace se quedaría por fuera, es de 0.876 horas por cada año. Si este tiempo lo distribuimos uniformemente en los 365 días del año se obtiene que el tiempo de pérdida del enlace en un día ordinario es de 8.64 segundos, esto en el peor de los casos.

5.3.2 SEGMENTACIÓN DEL DOMINIO DE BROADCAST [1]

La tecnología WLAN genera una cantidad considerable de *broadcast* debido principalmente al control de acceso al medio, es por esto que es muy importante la limitación de los dominios de *broadcast* para evitar así, problemas de saturación de la red. Esta delimitación del dominio de *broadcast* se la puede realizar de dos formas:

1. Mediante una segmentación física
2. Mediante una segmentación lógica

5.3.2.1 Segmentación Física

La segmentación física se logra mediante el uso de dispositivos de capa 3 como los ruteadores o *switches* de capa 3. Los dispositivos de capa 3 dividen a la red en varios dominios de colisión y varios dominios de *broadcast* ya que estos filtran los paquetes basándose en la dirección IP destino. La única forma en la que un ruteador envía un paquete, es cuando la dirección IP destino se encuentra fuera del dominio *broadcast* y si el ruteador tiene una ruta identificada para enviar el paquete.

En la figura 5.7 se puede apreciar una red que se encuentra dividida físicamente entre tres segmentos de red con dominios de *broadcast* diferentes, cada uno de los cuales está conectado al ruteador a través de una interfaz de red. El ruteador establece las rutas para que los diferentes segmentos de red puedan comunicarse entre sí.

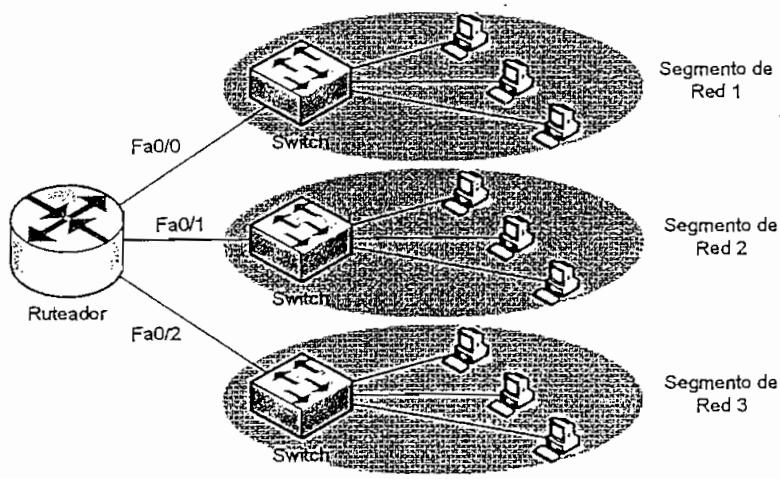


Figura 5.7. Segmentación Física del Dominio de Broadcast

Este tipo de solución no es muy adecuada para el presente caso de estudio ya que para llegar a implementar una solución así, sería necesario adquirir un ruteador que soporte un gran número de interfaces de red; específicamente sería necesario una interfaz de red por cada enlace WLAN que interconecte un cliente con el ISP. Esto implica costos muy altos ya que este tipo de ruteadores tienen un

alto costo, algo que no es óptimo ya que la solución que se debe dar no debe implicar costos exagerados.

5.3.2.2 Segmentación Lógica

Otra forma de poder segmentar una red en diferentes dominios de *broadcast* es mediante el uso de VLANs (*Virtual Local Area Networks*; Redes Virtuales de Área Local). Este tipo de segmentación, es una segmentación lógica en la cual cada VLAN es un dominio de *broadcast* diferente.

Las VLANs se componen de *hosts* o equipos de red conectados mediante un único dominio de puenteo. El dominio de puenteo se admite en diferentes equipos de red. Los *switches* de redes LAN operan protocolos de puenteo con un dominio de puenteo separado para cada VLAN. Los *switches* no puentean ningún tráfico entre VLAN, dado que esto viola la integridad del dominio de broadcast de las VLAN.

Existen dos métodos principales para el etiquetado de tramas en una VLAN: el enlace *Inter-Switch* (ISL) y 802.1Q. ISL es un protocolo propietario de Cisco y antiguamente era el más común, pero está siendo reemplazado por el etiquetado de trama del estándar IEEE 802.1Q.

A medida que los paquetes son recibidos por el *switch* desde cualquier dispositivo conectado a éste, se agrega un identificador único de paquetes dentro de cada encabezado. Esta información de encabezado designa la asociación de VLAN de cada paquete. El paquete se envía entonces a los *switches* o ruteadores correspondientes sobre la base del identificador de VLAN y la dirección MAC. Al alcanzar el nodo destino, el ID de VLAN es eliminado del paquete por el *switch* adyacente y es enviado al dispositivo conectado.

El etiquetado de paquetes brinda un mecanismo para controlar el flujo de *broadcasts* y aplicaciones, sin que se interfiera con la red y las aplicaciones que se desarrollen sobre ésta.

En la figura 5.8 se puede apreciar una red segmentada en tres dominios de *broadcast* diferentes mediante el uso de VLANs establecidas en los puertos del *switch*. La función del ruteador en este caso es la de establecer rutas para el tráfico de las diferentes VLANs entre sí ya que el *switch* no puentea las VLANs.

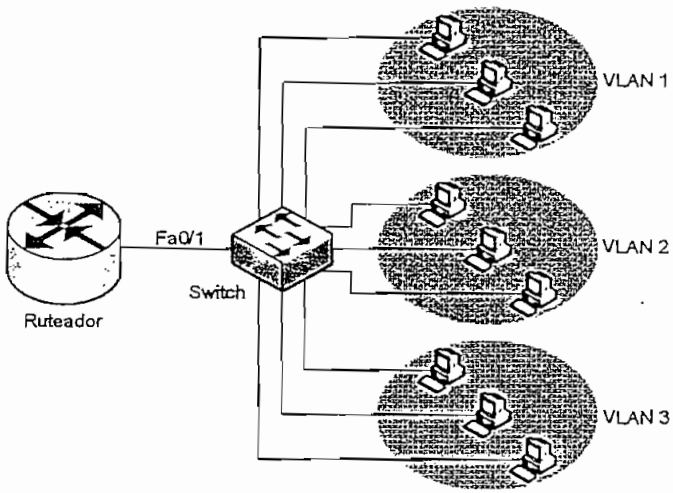


Figura 5.8. Segmentación Lógica del Dominio de Broadcast

Este tipo de solución es la más adecuada ya que no es necesario el uso de un ruteador que soporte un alto número de interfaces sino únicamente el uso de un *switch* para la concentración de los clientes y un ruteador para el enrutamiento de las VLANs que se creen en el *switch*. Esto implica costos mucho menores que realizar una segmentación física.

5.3.2.3 Asignación de VLANs a los Enlaces de Última Milla

Luego de explicar los dos métodos que se pueden utilizar para segmentar el dominio de *broadcast,* se ha decidido realizarlo de forma lógica mediante el uso de *switches* que soporten configuración de VLANs según el estándar 802.1Q. Esto se lo realiza con el fin de minimizar costos ya que una segmentación física incurriría en costos muy elevados como ya se indicó anteriormente. Mediante el uso de *switches,* la capacidad de enlaces de última milla que se podrían anexar a un nodo, dependerá únicamente del número de puertos que posean dichos *switches*.

Para poder segmentar el dominio de *broadcast* con el método señalado, se debe asignar una VLAN a cada uno de los puertos de los *switches*. Cada uno de estos puertos se conectará a un único dispositivo WLAN (para el caso del ISP, serán los puntos de acceso), con lo que se logrará que el *broadcast* que generen estos dispositivos WLAN no se propague más allá del puerto en el que esté conectado.

En la figura 5.9 se puede apreciar lo explicado anteriormente, en donde dos puertos del *switch* el Fa0/2 y el Fa0/3 tienen asignadas diferentes VLANs; la VLAN 10 y la VLAN 20 respectivamente. Cada uno de estos puertos se conecta con un punto de acceso diferente, el cual establece un enlace WLAN con el dispositivo cliente que se encuentra en el lado remoto. De esta forma el *broadcast* generado por estos dispositivos no se propaga a través del resto de puertos del *switch*.

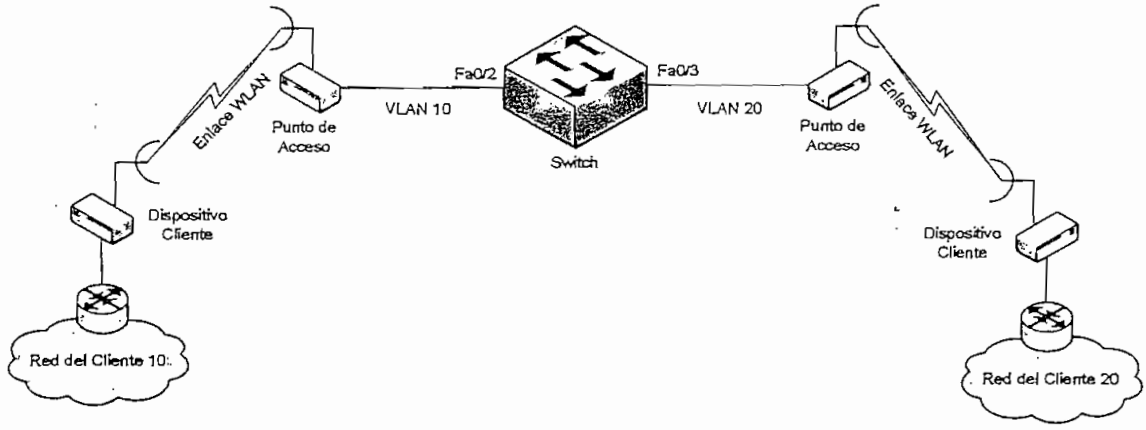


Figura 5.9. Asignación de VLANs

Para el caso del ISP en estudio, se debe colocar un *switch* en cada uno de los cuatro nodos. Con esto se logra concentrar los clientes a los diferentes nodos y a su vez segmentar el dominio de *broadcast*.

5.3.2.3.1 VLANs en el Nodo Principal

En la sección 4.6.6 del capítulo anterior, se puede observar que el número de clientes que ingresan al nodo principal es de nueve. Para esto, el *switch* que se

debe colocar en el nodo principal deberá tener configurado nueve puertos más dos puertos adicionales por los que ingresará el tráfico de dos enlaces principales que interconectan a los nodos 1 y 2 respectivamente. Con esto el número de VLANs que se deben asignar serán de once en total. En la figura 5.10 se puede apreciar lo indicado anteriormente.

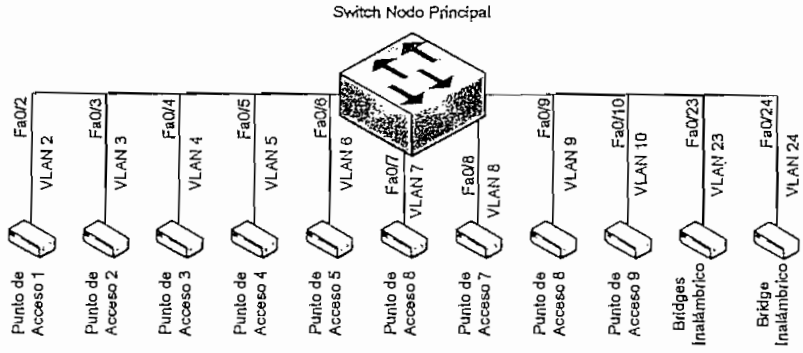


Figura 5.10. VLANs del Nodo Principal

Como el número de VLANs que se va a necesitar es de once, será necesario un *switch* de 24 puertos como mínimo. De esta forma se puede permitir a un futuro que 13 nuevos clientes ingresen a este nodo mediante el uso de un único *switch*. En el caso de que se necesite mayor capacidad de puertos, es factible colocar otro *switch* y configurar un enlace troncal entre estos dos.

En el mercado existen *switches* con variadas características y diferentes marcas que pueden satisfacer los requerimientos anteriores. Entre las marcas más conocidas están 3COM y Cisco Systems. Para el caso del ISP, se ha considerado un *switch* de 24 puertos Catalyst 2950 de Cisco Systems modelo WS-C2950-24, por varias razones:

- ✓ Son muy fáciles de configurar.
- ✓ Son una de las marcas más reconocidas tanto el mercado local como nacional, incluso internacional.
- ✓ Existe cualquier cantidad de información para la configuración de los mismos, en cualquier tipo de aplicación que soporten.

- ✓ Tienen un excelente desempeño tanto en condiciones normales o extremas de tráfico.
- ✓ Soportan protocolos estándar lo que los permite interoperar con otros tipos de equipos y marcas.

Para mayor información acerca de las características de este equipo, remitirse al *datasheet* que se encuentra en el Anexo 2.

5.3.2.3.2 VLANs en el Nodo 1

El número de clientes que existe en el nodo 1 es únicamente de un cliente hasta el momento del análisis. Considerando el caso de que en este nodo haya un incremento del número de clientes, se debe utilizar un *switch* de 24 puertos Catalyst 2950 de Cisco Systems, al igual que en el nodo principal.

En el *switch* que se instale en el nodo 1, se debe configurar un puerto con una VLAN diferente por cada cliente. También se debe configurar un puerto adicional para que ingrese el tráfico de uno de los enlaces principales que conecta el nodo 3 con este nodo.

En la figura 5.11 se puede apreciar la asignación de VLANs en cada puerto del *switch* para cada uno de los enlaces de última milla que se agreguen y el enlace principal hacia el nodo 3.

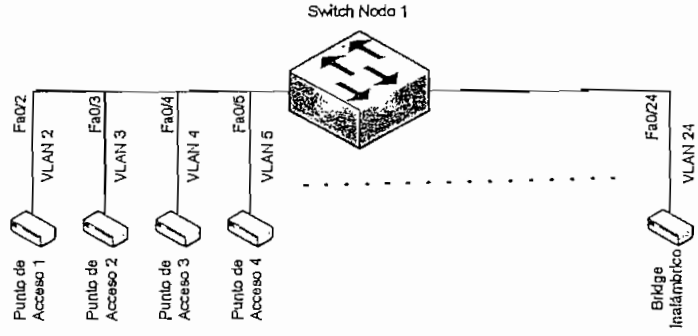


Figura 5.11. VLANs del Nodo 1

5.3.2.3.3 VLANs en el Nodo 2

El número de clientes en el nodo 2 hasta el momento de análisis del ISP es de siete clientes. Para permitir que nuevos clientes ingresen a este nodo se debe utilizar un *switch* de 24 puertos Catalyst 2950 de Cisco Systems, al igual que en los casos anteriores.

En el *switch* que se instale en este nodo al igual que en el resto de nodos, se debe configurar un puerto con una VLAN diferente por cada enlace que se interconecte con este nodo. Para el caso de los siete clientes, se tendrá que configurar siete puertos del *switch* con una VLAN diferente. En la figura 5.12 se puede apreciar lo indicado anteriormente.

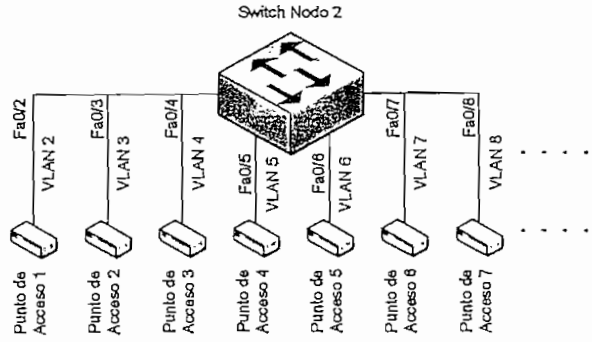


Figura 5.12. VLANs del Nodo 2

5.3.2.3.4 VLANs en el Nodo 3

El número de clientes que existe en el nodo 3 al igual que en el nodo 1 hasta el momento del análisis es únicamente de un cliente. Considerando el caso de que en este nodo se produzca un incremento del número de clientes, se debe utilizar un *switch* de 24 puertos Catalyst 2950 de Cisco Systems para permitir que estos nuevos clientes se interconecten con este nodo.

En el *switch* que se instale en este nodo, se debe configurar igualmente un puerto con una VLAN diferente por cada cliente. En la figura 5.13 se puede apreciar la asignación de VLANs en cada puerto del *switch,* la cual se debe realizar por cada

cliente instalado en el nodo.

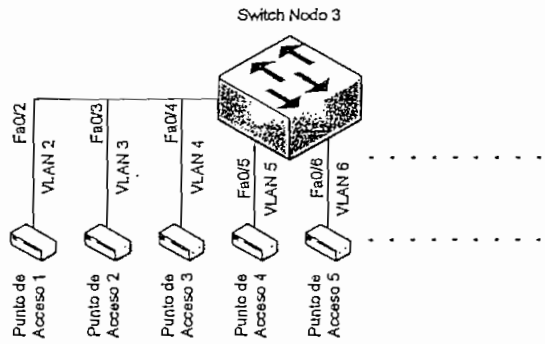


Figura 5.13. VLANs en el Nodo 3

5.3.2.4 Enlaces Troncales

Un enlace troncal es una conexión física y lógica entre dos *switches* o un *switch* y un ruteador a través de la cual viaja el tráfico de la red. El enlace troncal de VLAN permite que se definan varias VLAN en toda la red de una organización, agregando etiquetas especiales a las tramas que identifican la VLAN a la cual pertenecen. Este etiquetado permite que varias VLAN sean transportadas por toda una gran red conmutada a través de un *backbone*, o enlace troncal común. En la figura 5.14 se puede apreciar un enlace troncal entre dos *switches.*

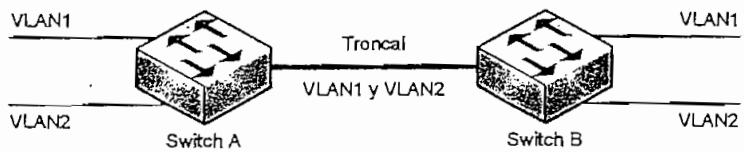


Figura 5.14. Enlace Troncal

La ventaja principal del uso del enlace troncal es la reducción en la cantidad de puertos que se utilizan en el ruteador y en el *switch*. Esto no sólo permite un ahorro de dinero sino también reduce la complejidad de la configuración.

Los dos tipos de mecanismos de enlace troncal estándar que existen son: el etiquetado de tramas y el filtrado de tramas. El que se implementa por lo general

en la actualidad es el etiquetado de tramas según el estándar IEEE 802.1Q. El enlace *Inter-Switch* (ISL) es un protocolo de enlace troncal de filtrado de tramas que es propietario de Cisco por lo que no se lo tomará en cuenta para el presente estudio.

El etiquetado de trama de VLAN se ha desarrollado específicamente para las comunicaciones conmutadas. El etiquetado de trama coloca un identificador único en el encabezado de cada trama a medida que se envía por todo el *backbone* de la red. El identificador es comprendido y examinado por cada *switch* antes de enviar cualquier *broadcast* o transmisión a otros *switches*, ruteadores o estaciones finales. Cuando la trama sale del *backbone* de la red, el *switch* elimina el identificador antes de que la trama se transmita a la estación final objetivo como ya se explicó anteriormente. El etiquetado de trama funciona a nivel de Capa 2 y requiere pocos recursos de red o gastos administrativos.

Para el caso del ISP en estudio, es necesario establecer un enlace troncal en cada uno de los *switches* para que puedan comunicarse con los ruteadores que serán los encargados de regular la velocidad de transmisión, como se explicará más adelante. Si no se establece un enlace troncal en el *switch,* el tráfico de las diferentes VLANs asignadas a cada enlace de última milla, no sería diferenciado por el ruteador con lo cual sería imposible poder delimitar la velocidad de transmisión en los enlaces de última milla.

El enlace troncal en cada uno de los *switches* se debe establecer en el puerto por el cual se interconectan a la interfaz Fast Ethernet de los ruteadores; en el caso del ISP se ha designado al puerto Fa0/1. Para que los ruteadores entiendan que por una de sus interfaces está ingresando tráfico de diferentes VLANs, se deben crear subinterfaces lógicas sobre esta interfaz física y asignarlas a cada una de las VLANs; esto se explica con más detalle en las siguientes secciones.

5.3.2.5 Configuración de los Switches Catalyst 2950

La configuración de cada uno de los *switches* se la debe realizar siguiendo los pasos que se describen a continuación. Como ejemplo de configuración se ha tomado el *switch* del nodo principal. El listado completo de los parámetros que se deben configurar en cada uno de los *switches* se pueden observar en el anexo 3.

5.3.2.5.1 Configuración Básica

Cada uno de los tres *switches* que se coloquen en los nodos del ISP, se deben configurar con los siguientes parámetros básicos:

Nombre del Switch

Para asignar un nombre al *switch* se deben seguir los siguientes pasos:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SwitchNP
SwitchNP(config)#exit
```

Contraseña de Consola

La contraseña de consola se la configura de la siguiente manera:

```
SwitchNP#configure terminal
SwitchNP(config)#line con 0
SwitchNP(config-line)#password ecua2005
SwitchNP(config-line)#login
SwitchNP(config)#exit
```

Contraseñas para las Líneas de Terminal Virtual

Las contraseñas de acceso a través de terminal virtual se las configura mediante los comandos:

```
SwitchNP#configure terminal
SwitchNP(config)#line vty 0 15
SwitchNP(config-line)#password ecua2005
SwitchNP(config-line)#login
SwitchNP(config-line)#exit
```

Contraseña "Enable" para Modo de Comando

La contraseña "*enable*" de modo de comando se configura con los siguientes comandos:

```
SwitchNP(config)#enable password ecua2005
SwitchNP(config-line)#exit
```

Contraseña "Enable Secret" para Modo de Comando

La contraseña "*enable secret*" de modo de comando se configura con los siguientes comandos:

```
SwitchNP(config)#enable secret !ecua*
SwitchNP(config-line)#exit
```

Dirección IP para Administración del Switch

La dirección IP del *switch* con fines de administración se configura con los siguientes comandos:

```
SwitchNP(config)#interface VLAN 1
SwitchNP(config-if)#ip address 192.168.0.2 255.255.255.0
SwitchNP(config-if)#exit
```

Gateway por Defecto del Switch

El *gateway* por defecto para el *switch* y la VLAN de administración se configura con los comandos:

```
SwitchNP(config)#ip default-gateway 192.168.0.1
SwitchNP(config)#exit
```

Verificación de los Parámetros de Administración

Se debe verificar el correcto ingreso de los parámetros anteriores mediante el uso del comando:

```
SwitchNP#show interface VLAN 1
```

Habilitación de la Interfaz Virtual

Luego de verificar el ingreso correcto de los parámetros, se habilita la interfaz virtual mediante los comandos:

```
SwitchNP(config)#interface VLAN1
SwitchNP(config-if)#no shutdown
SwitchNP(config-if)#exit
```

Guardar la configuración

Se realiza una copia de respaldo del archivo de configuración activa en la NVRAM de la siguiente forma:

```
SwitchNP#copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

5.3.2.5.2 Configuración de las VLANs Estáticas

La configuración de las VLANs en cada uno de los *switches* se la debe realizar de la siguiente forma:

Creación de las VLANs

La creación de las diferentes VLANs se lo realiza mediante el uso de los siguientes comandos:

```
SwitchNP#vlan database
SwitchNP(vlan)#vlan 2 name VLAN 2
SwitchNP(vlan)#vlan 3 name VLAN 3
SwitchNP(vlan)#vlan 4 name VLAN 4
SwitchNP(vlan)#vlan 5 name VLAN 5
SwitchNP(vlan)#vlan 6 name VLAN 6
SwitchNP(vlan)#vlan 7 name VLAN 7
SwitchNP(vlan)#vlan 8 name VLAN 8
SwitchNP(vlan)#vlan 9 name VLAN 9
SwitchNP(vlan)#vlan 10 name VLAN 10
SwitchNP(vlan)#vlan 23 name VLAN 23
SwitchNP(vlan)#vlan 24 name VLAN 24
SwitchNP(vlan)#exit
```

Asignación de Puertos a las VLANs

Se debe asignar un puerto diferente a cada una de las VLANs, mediante los

siguientes comandos:

```
SwitchNP#configure terminal
SwitchNP(config)#interface fastethernet 0/2
SwitchNP(config-if)#switchport mode access
SwitchNP(config-if)#switchport access vlan 2

SwitchNP(config)#interface fastethernet 0/3
SwitchNP(config-if)#switchport mode access
SwitchNP(config-if)#switchport access vlan 3

SwitchNP(config-if)#interface fastethernet 0/4
SwitchNP(config-if)#switchport mode access
SwitchNP(config-if)#switchport access vlan 4

SwitchNP(config-if)#interface fastethernet 0/5
SwitchNP(config-if)#switchport mode access
SwitchNP(config-if)#switchport access vlan 5

SwitchNP(config-if)#interface fastethernet 0/6
SwitchNP(config-if)#switchport mode access
SwitchNP(config-if)#switchport access vlan 6

SwitchNP(config-if)#interface fastethernet 0/7
SwitchNP(config-if)#switchport mode access
SwitchNP(config-if)#switchport access vlan 7

SwitchNP(config-if)#interface fastethernet 0/8
SwitchNP(config-if)#switchport mode access
SwitchNP(config-if)#switchport access vlan 8

SwitchNP(config-if)#interface fastethernet 0/9
SwitchNP(config-if)#switchport mode access
```

```
SwitchNP(config-if)#switchport access vlan 9

SwitchNP(config-if)#interface fastethernet 0/10
SwitchNP(config-if)#switchport mode access
SwitchNP(config-if)#switchport access vlan 10

SwitchNP(config-if)#interface fastethernet 0/23
SwitchNP(config-if)#switchport mode access
SwitchNP(config-if)#switchport access vlan 23

SwitchNP(config-if)#interface fastethernet 0/24
SwitchNP(config-if)#switchport mode access
SwitchNP(config-if)#switchport access vlan 24
SwitchNP(config-if)#end
```

Verificación de la Asignación de VLANs:

Con el siguiente comando se puede observar si se realizó una asignación correcta de las VLANs:

```
SwitchNP#show vlan
```

Guardar la Configuración

Se realiza una copia de respaldo del archivo de configuración activa en la NVRAM de la siguiente forma:

```
SwitchNP#copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

5.3.2.5.3 Configuración del Enlace Troncal

El enlace troncal para el caso de estudio se la va a configurar en el puerto Fa0/1 de cada uno de los *switches* como ya se indicó anteriormente. Para realizarlo, se deben seguir los siguientes pasos:

```
SwitchNP(config)#interface fastethernet 0/1
SwitchNP(config-if)#switchport mode trunk
SwitchNP(config-if)#end
```

Guardar la Configuración

Se realiza una copia de respaldo del archivo de configuración activa en la NVRAM de la siguiente forma:

```
SwitchNP#copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...:
[OK]
```

5.3.3 ASIGNACIÓN DE LA VELOCIDAD DE TRANSMISIÓN A CADA ENLACE WLAN

La asignación o limitación de la velocidad de transmisión en los enlaces de última milla es el punto más crítico de todos los problemas que existen actualmente. Normalmente con otro tipo de tecnología en la última milla la velocidad de transmisión es delimitada en la capa física o en la capa de enlace, sin embargo con la tecnología WLAN y los equipos que actualmente maneja el ISP esto no es posible.

Con estos antecedentes, las opciones que se podrían tomar para poder delimitar la velocidad de transmisión en los enlaces inalámbricos de última milla serían:

- ✓ Cambiar por completo la tecnología inalámbrica en la última milla, para lo cual ya no se podría utilizar las redes WLAN 802.11b y sería necesario cambiar toda la infraestructura de la última milla. Esto causaría que los costos del servicio que el ISP presta actualmente se eleven considerablemente, además de que el costo-beneficio de la inversión no sería rentable.
- ✓ Utilizar algún tipo de tecnología WAN en toda la infraestructura del ISP como por ejemplo *Frame Relay*, la cual permite establecer clases de servicio en cada uno de los circuitos que se entreguen a los clientes. Sin embargo, antes de tomarla como una solución, hay que tener en cuenta que el ISP es muy pequeño y no cuenta con el capital suficiente como para tratar de incurrir en una inversión de esta naturaleza.
- ✓ Descentralizar el control de la velocidad de transmisión y delimitarla igualmente a nivel de la capa 3 pero en cada nodo del ISP, mediante el uso de ruteadores con capacidad de segmentación de velocidad en cada una de sus interfaces y subinterfaces.

Lo óptimo, es tomar la última alternativa ya que es la que implica menos cambios e igualmente menos costos. Además, es una solución que va a la par con la segmentación del dominio de *broadcast* explicada en las secciones anteriores. Para esto las series de ruteadores Cisco 1800 y las series superiores tienen una característica que permite controlar la velocidad de transmisión tanto en sus interfaces como subinterfaces.

Los ruteadores que se instalarán en cada uno de los nodos, además de controlar la velocidad de transmisión, también permitirán establecer las rutas para poder alcanzar las diferentes subredes de los clientes que se pegan a cada uno de los nodos.

Estos ruteadores deberán soportar enlaces troncales según el estándar IEEE 802.1Q para que puedan entender el tráfico que provenga de los *switches* y también políticas de calidad de servicio para el control de la velocidad de transmisión. Para el caso del ISP en estudio se han escogido ruteadores Cisco

1841 por cumplir con los requerimientos anteriores y por ser de bajo costo en comparación con las series superiores. Para mayor información acerca de las características de estos equipos, remitirse al *datasheet* en el anexo 2.

Más adelante, se indicará las configuraciones que se deben establecer en los ruteadores para poder realizar el control de la velocidad de transmisión en cada enlace WLAN conectado a los diferentes *switches* Catalyst 2950.

5.3.3.1 Asignación de Subinterfaces del Ruteador a cada VLAN [1], [10]

Como ya se indicó anteriormente el control de la velocidad de transmisión se lo realizará directamente sobre las subinterfaces de los ruteadores, por lo que será necesario asignar una subinterfaz de estos ruteadores a cada una de las VLANs creadas en los diferentes *switches*.

A medida que aumenta la cantidad de VLANs en una red, el enfoque físico de tener una interfaz de un ruteador por cada VLAN se vuelve rápidamente no escalable. Por esta razón las redes con muchas VLANs deben hacer uso de un enlace troncal de VLAN para asignar varias VLANs a una misma interfaz del ruteador, tal es el caso del ISP en estudio.

Una subinterfaz es una interfaz lógica dentro de una interfaz física, como por ejemplo la interfaz Fast Ethernet de un ruteador. Pueden existir varias subinterfaces en una sola interfaz física, cada subinterfaz admite una VLAN a la cual se le debe asignar una dirección IP que debe estar dentro de la misma red o subred de dicha VLAN. En la figura 5.15 se puede apreciar como tres subinterfaces son asignadas a tres VLANs diferentes:

Para el caso del ISP en estudio, se deben configurar y asignar subinterfaces en cada uno de los ruteadores para cada una de las VLANs creadas en los *switches* correspondientes incluyendo a la VLAN 1, que es la VLAN de administración.

Luego de configurar y asignar subinterfaces del ruteador a cada una de las

VLANs, se debe definir en cada subinterfaz que tipo de encapsulamiento se va a utilizar, que en este caso es 802.1Q. Finalmente, se debe asignar a cada subinterfaz una dirección IP que esté dentro de la red o subred en la que se encuentra la VLAN.

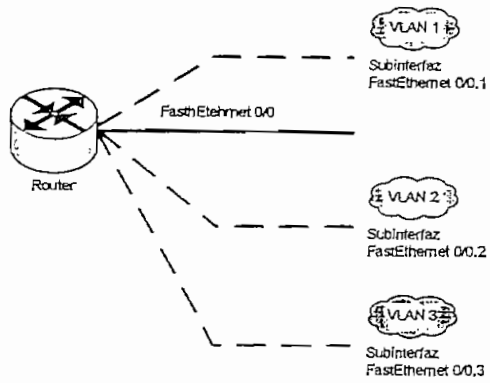


Figura 5.15. Asignación de Subinterfaces a Diferentes VLANs

5.3.3.1.1 Subinterfaces del Ruteador en el Nodo Principal

En el ruteador del nodo principal serán necesarias 12 subinterfaces ya que se encuentran configuradas en el *switch* del nodo principal 12 VLANs (incluyendo la VLAN 1 que es la VLAN de administración). En la figura 5.16 se puede apreciar lo indicado anteriormente, en donde una de las interfaces Fast Ethernet se conecta a la red de la oficina central y la otra interfaz se conecta al *switch* del nodo principal.

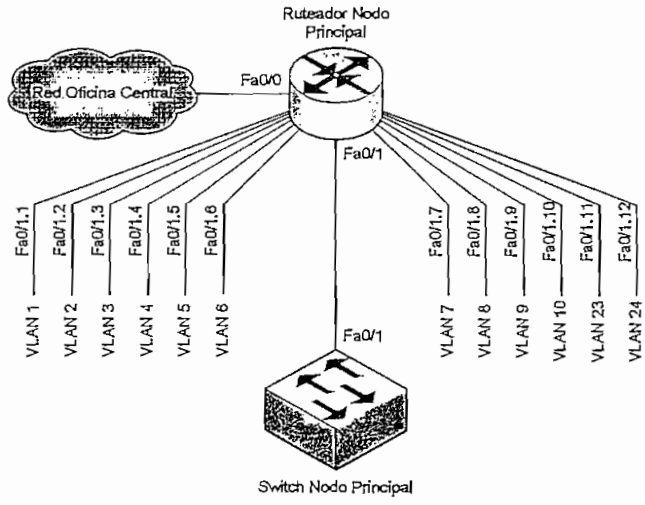


Figura 5.16. Ruteador del Nodo Principal

5.3.3.1.2 Subinterfaces del Ruteador en el Nodo 1

En el ruteador del nodo 1 serán necesarias 6 subinterfaces ya que se encuentran configuradas en el *switch* del nodo principal 6 VLANs (incluyendo la VLAN 1 que es la VLAN de administración). En la figura 5.17 se puede apreciar lo indicado anteriormente, en donde una de las interfaces Fast Ethernet se conecta a un *bridge* inalámbrico y la otra interfaz se conecta al *switch* del nodo 1.

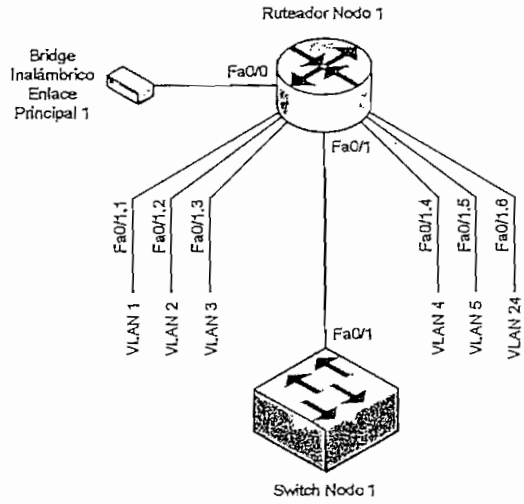


Figura 5.17. Ruteador del Nodo 1

5.3.3.1.3 Subinterfaces del Ruteador en el Nodo 2

En el ruteador del nodo 2 serán necesarias 8 subinterfaces ya que se encuentran configuradas en el *switch* del nodo principal 8 VLANs (incluyendo la VLAN 1 que es la VLAN de administración). En la figura 5.18 se puede apreciar lo indicado anteriormente, en donde una de las interfaces Fast Ethernet se conecta a un *bridge* inalámbrico y la otra interfaz se conecta al *switch* del nodo 2.

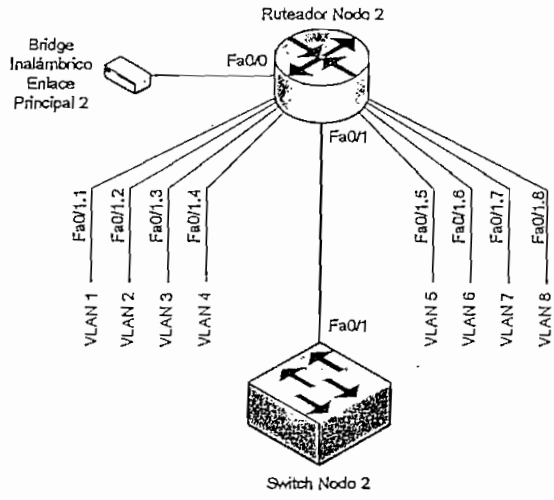


Figura 5.18. Ruteador del Nodo 2

5.3.3.1.4 Subinterfaces del Ruteador en el Nodo 3

En el ruteador del nodo 3 serán necesarias 6 subinterfaces ya que se encuentran configuradas en el *switch* del nodo principal 6 VLANs (incluyendo la VLAN 1 que es la VLAN de administración). En la figura 5.19 se puede apreciar lo indicado anteriormente, en donde una de las interfaces Fast Ethernet se conecta a un *bridge* inalámbrico y la otra interfaz se conecta al *switch* del nodo 2.

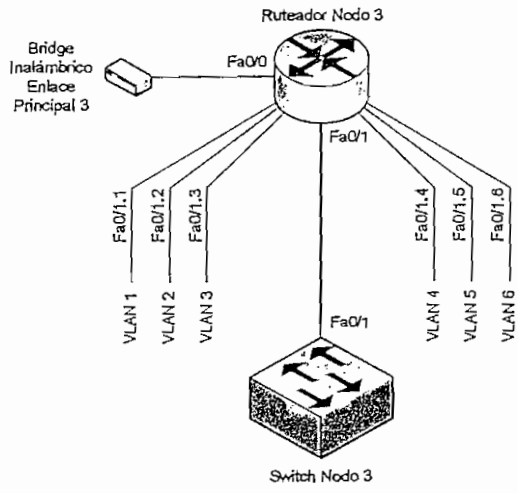


Figura 5.19. Ruteador del Nodo 3

Cabe hacer notar que se van a manejar direcciones privadas para cada una de las VLANs excepto para las VLANs correspondientes a los enlaces principales. Las direcciones públicas serán configuradas en los ruteadores o servidores de los clientes y en los ruteadores de cada uno de los nodos. En el anexo 3 se puede observar la asignación de direcciones IPs y asignación de VLANs a cada una de las subinterfaces de los tres ruteadores que se vayan a instalar.

5.3.3.2 Limitación de la Velocidad de Transmisión [11], [12], [13]

Para la limitación de la velocidad de transmisión se hará uso del CAR (*Committed Access Rate*; Velocidad de Acceso Comprometida) de Cisco Systems, que permite implementar políticas y clases de servicios a través de la limitación de la velocidad. Esta capacidad de CAR permite seccionar a la red dentro de múltiples niveles de prioridad o clases de servicio.

CAR permite clasificar los paquetes mediante el uso de políticas que se basen en puertos físicos, destino de direcciones MAC o IPs, puertos de aplicación, o cualquier otro criterio que se pueda configurar a través de listas de acceso o listas de acceso extendidas. Después de que un paquete ha sido clasificado, una red puede aceptar, anular o reclasificar el paquete de acuerdo a una política específica.

Para el caso del ISP en estudio se hará uso de políticas basadas en puertos, es decir basadas en las subinterfaces que se configuren en cada uno de los ruteadores. Para esto se hará uso del comando *rate-limit.*

El comando *rate-limit* establece una política básica de CAR para cualquier tipo de tráfico IP. Este comando se ejecuta sobre una interfaz o subinterfaz de un ruteador mediante la siguiente sintaxis:

rate limit {**input** | **output**} bps burst-normal burst-max **conform-action** action **exceed-action** action

En donde:

- ✓ **input:** Aplica la política de tráfico CAR a los paquetes recibidos sobre la entrada de la interfaz.
- ✓ **output:** Aplica la política de tráfico CAR a los paquetes enviados sobre la salida de la interfaz.
- ✓ bps: Velocidad promedio, en bits por segundo. El valor debe ser en incrementos de 8 kbps. El valor es un número de 8,000 a 2000,000,000.
- ✓ burst-normal: Tamaño del burst normal, en bytes. El mínimo valor es la velocidad promedio (bps) dividido por 2000. El valor es un número de 1,000 a 512,000,000.
- ✓ burst-max: Tamaño del burst de exceso, en bytes. El valor es un número de 2,000 a 1,024,000,000.
- ✓ **conform-action:** Acción a tomarse en los paquetes que se alinean al límite de velocidad. Para el caso de estudio, se puede especificar una de las siguientes opciones:
  - o **continue:** Evalúa el comando **rate-limit** siguiente.
  - o **drop:** Da de baja al paquete.
  - o **transmit:** transmite el paquete.
- ✓ **exceed-action:** Acción a tomarse en los paquetes que exceden el límite de velocidad especificado. Para el caso de estudio, se puede especificar una de las siguientes opciones:
  - o **continue:** Evalúa el comando **rate-limit** siguiente.
  - o **drop:** Dar de baja al paquete.
  - o **transmit:** transmite el paquete.

Como se puede apreciar en la descripción de cada una de las variables del comando, esta funcionalidad básica de CAR requiere de los siguientes criterios para ser definida:

1. Direccionamiento de paquetes, entrantes o salientes.
2. Una velocidad promedio, a la cual el ruteador siempre está obligado a transmitir en condiciones normales. El tráfico que cae dentro de esta

velocidad siempre será aceptado.

3. Un tamaño del *burst* normal, que es la cantidad de datos que el ruteador se compromete a transmitir durante un intervalo de tiempo
4. Un tamaño de *burst* de exceso, que es la máxima cantidad permitida de datos que pueden exceder el *burst* normal durante el mismo intervalo de tiempo que se mide el *burst* normal.

Cisco recomienda las siguientes expresiones para el cálculo de los valores de los parámetros de *burst* normal y *burst* extendido:

$$burst\ normal = velocidad\ configurada \times \frac{1\ byte}{8\ bits} \times 1.5\ segundos$$

$$burst\ extendido = 2 \times burst\ normal$$

Para el caso del ISP en estudio, los anchos de banda típicos que se entregan a un cliente son:

- ✓ 32 kbps
- ✓ 64 kbps
- ✓ 128 kbps
- ✓ 256 kbps
- ✓ 512 kbps

En la tabla 5.5 se puede apreciar los valores del *burst* normal y el *burst* extendido según la recomendación de Cisco Systems, para los valores de velocidad anteriores.

Velocidad Promedio [Kbps]	Burst Normal [bytes]	Burst Extendido [bytes]
32	6,000	12,000
64	12,000	24,000
128	24,000	48,000
256	48,000	96,000
512	96,000	192,000

Tabla 5.5. Valores del Burst Normal y Burst Extendido

Hay que tomar muy en cuenta que en los enlaces principales que ingresan a algunos de los *switches* que serán instalados, no es necesario y no se debe limitar la velocidad de transmisión, y al contrario deben funcionar a su máxima capacidad para impedir que se formen cuellos de botella, los cuales degradarían la calidad de servicio de los clientes que estén en el nodo remoto.

En la siguiente sección se indica cómo se deben configurar los ruteadores para limitar la velocidad de transmisión en cada una de sus subinterfaces.

5.3.3.3 Configuración de los Ruteadores Cisco 1841

Para la configuración de los ruteadores se ha tomado como ejemplo el ruteador del nodo principal, los parámetros que se deben configurar en el resto de ruteadores se pueden observar en el anexo 3.

5.3.3.3.1 Configuración Básica

En la configuración básica se establece, el nombre del host, contraseñas de consola, contraseñas para líneas de terminal virtual, contraseña "enable" y contraseña "*enable secret*".

Nombre del Host

Para la configuración del nombre del *host*, se deben utilizar los siguientes comandos:

```
Router>enable
Router#configure terminal
RouterP(config)#hostname RouterP
```

Contraseña de Consola

Para la configuración de la contraseña de consola, se deben utilizar los siguientes

comandos:

```
RouterP(config)#line console 0
RouterP(config-line)#password ecua2005
RouterP(config-line)#login
RouterP(config-line)#exit
```

Contraseñas para las Líneas de Terminal Virtual

Para la configuración de las contraseñas para las líneas de terminal virtual, se deben utilizar los siguientes comandos:

```
RouterP(config)#line vty 0 4
RouterP(config-line)#password ecua2005
RouterP(config-line)#login
RouterP(config-line)#exit
```

Contraseña "Enable"

Para la configuración de la contraseña "*enable*", se deben utilizar los siguientes comandos:

```
RouterP(config)#enable password ecua2005
RouterP(config)#exit
```

Contraseña "Enable Secret"

Para la configuración de la contraseña "*enable secret*", se deben utilizar los siguientes comandos:

```
RouterP(config)#enable secret ¡ecua*
RouterP(config)#service password-encryption
RouterP(config)#exit
```

Verificación de la Configuración

La configuración de los parámetros anteriores, se pueden verificar mediante el uso del siguiente comando:

```
RouterP#show running-config
```

Guardar la Configuración

Se realiza una copia de respaldo del archivo de configuración activa en la NVRAM de la siguiente forma:

```
RouterP#copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

5.3.3.3.2 Configuración de las Interfaces y Subinterfaces

En esta configuración primeramente se deben activar las dos interfaces del ruteador y asignar una dirección IP con su máscara de subred respectiva, solamente a la interfaz que no contendrá subinterfaces. Luego se crean las subinterfaces en la interfaz que se conectará con el *switch*, se les asigna el tipo de encapsulamiento y finalmente se les asigna una dirección IP con su máscara de subred respectiva.

Activación de las Interfaces

```
RouterP(config)#interface fastethernet 0/0
RouterP(config-if)#ip address 216.226.233.14 255.255.255.248
RouterP(config-if)#no shutdown

RouterP(config)#interface fastethernet 0/1
RouterP(config-if)#no shutdown
```

Creación y Configuración de las Subinterfaces

```
RouterP(config-if)#interface fastethernet 0/1.1
RouterP(config-subif)#encapsulation dot1q 1
RouterP(config-subif)#ip address 192.168.0.1 255.255.255.0

RouterP(config-subif)#interface fastethernet 0/1.2
RouterP(config-subif)#encapsulation dot1q 2
RouterP(config-subif)#ip address 192.168.1.1 255.255.255.0

RouterP(config-subif)#interface fastethernet 0/1.3
RouterP(config-subif)#encapsulation dot1q 3
RouterP(config-subif)#ip address 192.168.2.1 255.255.255.0

RouterP(config-subif)#interface fastethernet 0/1.4
RouterP(config-subif)#encapsulation dot1q 4
RouterP(config-subif)#ip address 192.168.3.1 255.255.255.0

RouterP(config-subif)#interface fastethernet 0/1.5
RouterP(config-subif)#encapsulation dot1q 5
RouterP(config-subif)#ip address 192.168.4.1 255.255.255.0

RouterP(config-subif)#interface fastethernet 0/1.6
RouterP(config-subif)#encapsulation dot1q 6
```

```
RouterP(config-subif)#ip address 192.168.5.1 255.255.255.0

RouterP(config-subif)#interface fastethernet 0/1.7
RouterP(config-subif)#encapsulation dot1q 7
RouterP(config-subif)#ip address 192.168.6.1 255.255.255.0

RouterP(config-subif)#interface fastethernet 0/1.8
RouterP(config-subif)#encapsulation dot1q 8
RouterP(config-subif)#ip address 192.168.7.1 255.255.255.0

RouterP(config-subif)#interface fastethernet 0/1.9
RouterP(config-subif)#encapsulation dot1q 9
RouterP(config-subif)#ip address 192.168.8.1 255.255.255.0

RouterP(config-subif)#interface fastethernet 0/1.10
RouterP(config-subif)#encapsulation dot1q 10
RouterP(config-subif)#ip address 192.168.9.1 255.255.255.0

RouterP(config-subif)#interface fastethernet 0/1.11
RouterP(config-subif)#encapsulation dot1q 23
RouterP(config-subif)#ip address 216.226.233.81 255.255.255.252

RouterP(config-subif)#interface fastethernet 0/1.12
RouterP(config-subif)#encapsulation dot1q 24
RouterP(config-subif)#ip address 216.226.233.85 255.255.255.252
RouterP(config-subif)#end
```

Guardar la Configuración

Se realiza una copia de respaldo del archivo de configuración activa en la NVRAM de la siguiente forma:

```
RouterP#copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

5.3.3.3.3 Configuración de la Velocidad de Transmisión

En el anexo 3 se puede apreciar las velocidades de transmisión que se deben asignar a cada uno de los enlaces; cabe recalcar que en los enlaces principales no se debe limitar la velocidad de transmisión para evitar cuellos de botella como ya se indicó anteriormente. Como ejemplo de configuración se ha tomado la limitación de la velocidad de transmisión a cada uno de los enlaces en el nodo principal.

Configuración del rate-limit

Para limitar la velocidad de transmisión en los enlaces de última milla, se debe configurar la velocidad tanto en la entrada como en la salida de las subinterfaces:

```
RouterP(config)#interface fastethernet 0/1.1
RouterP(config-subif)#rate-limit input 64000 12000 24000 conform-action
transmit exceed-action drop
RouterP(config-subif)#rate-limit output 64000 12000 24000 conform-action
transmit exceed-action drop

RouterP(config-subif)#interface fastethernet 0/1.2
RouterP(config-subif)#rate-limit input 64000 12000 24000 conform-action
transmit exceed-action drop
RouterP(config-subif)#rate-limit output 64000 12000 24000 conform-action
transmit exceed-action drop

RouterP(config-subif)#interface fastethernet 0/1.3
```

```
RouterP(config-subif)#rate-limit input 128000 24000 48000 conform-action
transmit exceed-action drop
RouterP(config-subif)#rate-limit output 128000 24000 48000 conform-
action transmit exceed-action drop

RouterP(config-subif)#interface fastethernet 0/1.4
RouterP(config-subif)#rate-limit input 64000 12000 24000 conform-action
transmit exceed-action drop
RouterP(config-subif)#rate-limit output 64000 12000 24000 conform-action
transmit exceed-action drop

RouterP(config-subif)#interface fastethernet 0/1.5
RouterP(config-subif)#rate-limit input 128000 24000 48000 conform-action
transmit exceed-action drop
RouterP(config-subif)#rate-limit output 128000 24000 48000 conform-
action transmit exceed-action drop

RouterP(config-subif)#interface fastethernet 0/1.6
RouterP(config-subif)#rate-limit input 64000 12000 24000 conform-action
transmit exceed-action drop
RouterP(config-subif)#rate-limit output 64000 12000 24000 conform-action
transmit exceed-action drop

RouterP(config-subif)#interface fastethernet 0/1.7
RouterP(config-subif)#rate-limit input 64000 12000 24000 conform-action
transmit exceed-action drop
RouterP(config-subif)#rate-limit output 64000 12000 24000 conform-action
transmit exceed-action drop

RouterP(config-subif)#interface fastethernet 0/1.8
RouterP(config-subif)#rate-limit input 256000 48000 96000 conform-action
transmit exceed-action drop
RouterP(config-subif)#rate-limit output 256000 48000 96000 conform-
```

```
action transmit exceed-action drop
RouterP(config-subif)#interface fastethernet 0/1.9
RouterP(config-subif)#rate-limit input 64000 12000 24000 conform-action
transmit exceed-action drop
RouterP(config-subif)#rate-limit output 64000 12000 24000 conform-action
transmit exceed-action drop

RouterP(config-subif)#interface fastethernet 0/1.10
RouterP(config-subif)#rate-limit input 512000 96000 192000 conform-
action transmit exceed-action drop
RouterP(config-subif)#rate-limit output 512000 96000 192000 conform-
action transmit exceed-action drop
RouterP(config-subif)#end
```

Guardar la Configuración

Se realiza una copia de respaldo del archivo de configuración activa en la NVRAM de la siguiente forma:

```
RouterP#copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

5.4 POLÍTICAS DE SEGURIDAD EN LAS REDES WLAN

Como se indicó el capítulo 3, la meta de la seguridad es mantener la integridad, preservar la confidencialidad y garantizar la accesibilidad. En el presente caso de estudio debido al tipo de aplicación que tienen las WLANs dentro del ISP, la meta principal de la seguridad es garantizar la accesibilidad para de esta forma entregar a los clientes una total disponibilidad del servicio de Internet; esto sin dejar de tomar en cuenta las otras dos metas.

Las redes WLAN al ser utilizadas como enlaces de última milla, también pueden ser susceptibles tanto a ataques activos como pasivos. Mediante los ataques pasivos los *hackers* maliciosos podrían descifrar información valiosa de los clientes que esté circulando a través de los enlaces WLAN y mediante ataques activos estos *hackers* incluso podrían ganar acceso a servidores de los clientes o simplemente hacer uso del servicio de Internet dejando sin servicio o deteriorando la calidad de servicio a los clientes del ISP.

Para solucionar este tipo de inconvenientes, actualmente existen varios métodos para evitar cualquier tipo de ataques o intromisiones como ya se explicó con anterioridad, pero se debe tomar muy en cuenta que la implementación de alguno de estos métodos puede implicar costos muy elevados, debido a que la mayoría de los dispositivos WLANs que el ISP maneja actualmente no soportan la migración a nuevos protocolos de seguridad.

A pesar de que existen limitaciones en estos dispositivos para establecer nuevos y más eficientes protocolos de seguridad, es factible establecer algunas políticas de seguridad que aprovechen los protocolos que estos dispositivos soportan actualmente.

Las políticas de seguridad que se deben tomar en cuenta al utilizar puntos de acceso y dispositivos clientes WLAN para establecer enlaces de última milla son:

- ✓ Actualizar el *firmware* en todos los puntos de acceso y dispositivos clientes WLAN.
- ✓ Hacer uso de la encriptación WEP con claves de encriptación tan largas como los dispositivos soporten.
- ✓ Cambiar el SSID (Server Set ID) que viene por defecto de fábrica en los dispositivos.
- ✓ No utilizar como SSID, nombres que se relacionen con la terminología de la empresa o la región.
- ✓ Desactivar o inhabilitar la emisión *broadcast* del SSID en todos los dispositivos.

- ✓ Hacer uso de filtros MAC en caso de que los puntos de acceso lo soporten.

Estas reglas aunque son muy básicas y no están a la par con los estándares de seguridad actuales, son muy útiles en este tipo de aplicaciones de las redes WLAN. Esto se debe principalmente a que al ser utilizadas como enlaces de última milla, los *hackers* no pueden acceder de forma sencilla a los alrededores del enlace de última milla, ya que por lo general los puntos de acceso y los dispositivos clientes WLAN son instalados en sitios de difícil acceso e incluso en áreas restringidas como son las torres, terrazas y azoteas. Esto va a complicar mucho su tarea de sabotaje, más aún si se encuentran de por medio con políticas de seguridad como las indicadas anteriormente.

5.5 COSTOS REFERENCIALES DE LA OPTIMIZACIÓN

En esta sección se describen los costos referenciales de los equipos que se van a utilizar para la optimización del ISP en estudio. En la tabla 5.6 se puede apreciar los costos para mejorar cada uno de los enlaces principales y el costo total de los mismos.

Descripción	Equipos	Cantidad	Costo
Enlace Principal 1	Kit Tsunami QuickBridge 20	1	4,499.00
Enlace Principal 2	Kit Tsunami QuickBridge 20	1	4,499.00
Enlace Principal 3	Kit Tsunami QuickBridge 20	1	4,499.00
		Subtotal:	13,497.00

Tabla 5.6. Costos de Equipos para Enlaces Principales

En la tabla 5.7 se puede apreciar los costos de los *switches* y ruteadores que se deben instalar en cada uno de los nodos y el costo total de los equipos por nodo.

En la tabla 5.8 se puede apreciar un resumen de los costos por cada enlace principal y cada nodo, y el costo total de los equipos para la optimización del ISP.

Descripción	Equipos	Cantidad	Costo
Nodo Principal	Ruteador Cisco 1841	1	1,545.00
	Switch WS-C2950-24	1	1,145.00
		Subtotal:	2,690.00

Descripción	Equipos	Cantidad	Costo
Nodo 1	Ruteador Cisco 1841	1	1,545.00
	Switch Cisco WS-C2950-24	1	1,145.00
		Subtotal:	2,690.00

Descripción	Equipos	Cantidad	Costo
Nodo 2	Ruteador Cisco 1841	1	1,545.00
	Switch Cisco WS-C2950-24	1	1,145.00
		Subtotal:	2,690.00

Descripción	Equipos	Cantidad	Costo
Nodo 3	Ruteador Cisco 1841	1	1,545.00
	Switch Cisco WS-C2950-24	1	1,145.00
		Subtotal:	2,690.00

Tabla 5.7. Costo de Equipos en Nodos

Descripción	Costo Unitario	Cantidad	Costo
Equipos por Enlace Principal	4,499.00	3	13,497.00
Equipos por Nodo	2,690.00	4	10,760.00
		Subtotal:	24,257.00
		IVA 12%	2,910.84
		Total:	27,167.84

Tabla 5.8. Resumen de Costos

Como se puede apreciar en la tabla 5.8 el costo referencial total para la optimización de toda la infraestructura del ISP es de $27,167.84. Sin embargo, la implementación se puede realizar por etapas para minimizar el impacto económico en el ISP. En la tabla 5.9 se muestran las etapas en las que se puede realizar la implementación de acuerdo a la urgencia en los cambios, para así solventar los actuales y futuros problemas del ISP.

Descripción	Implementación
Etapa 1	Equipos Nodo Principal
Etapa 2	Equipos Enlace Principal 2
Etapa 3	Equipos Nodo 2
Etapa 4	Equipos Enlace Principal 1
Etapa 5	Equipos Nodo 1
Etapa 6	Equipos Enlace Principal 3
Etapa 7	Equipos Nodo 3

Tabla 5.9. Etapas de Implementación

Como se puede apreciar en la red externa del ISP en la figura 5.20, en la etapa 1 se permitirá el acceso a nuevos clientes a través del nodo principal. En la etapa 2 se evitará problemas de conectividad con el nodo 2 a través de enlace principal 2. En la etapa 3 se permitirá el acceso a nuevos clientes a través del nodo 2. En la etapa 4 se evitará problemas de conectividad hacia el nodo 1. En la etapa 5 se permitirá el acceso a nuevos clientes a través del nodo 1. En la etapa 6 se evitará problemas de conectividad con el nodo 3. Finalmente en la etapa 7 se permitirá el acceso a nuevos clientes a través del nodo 3.

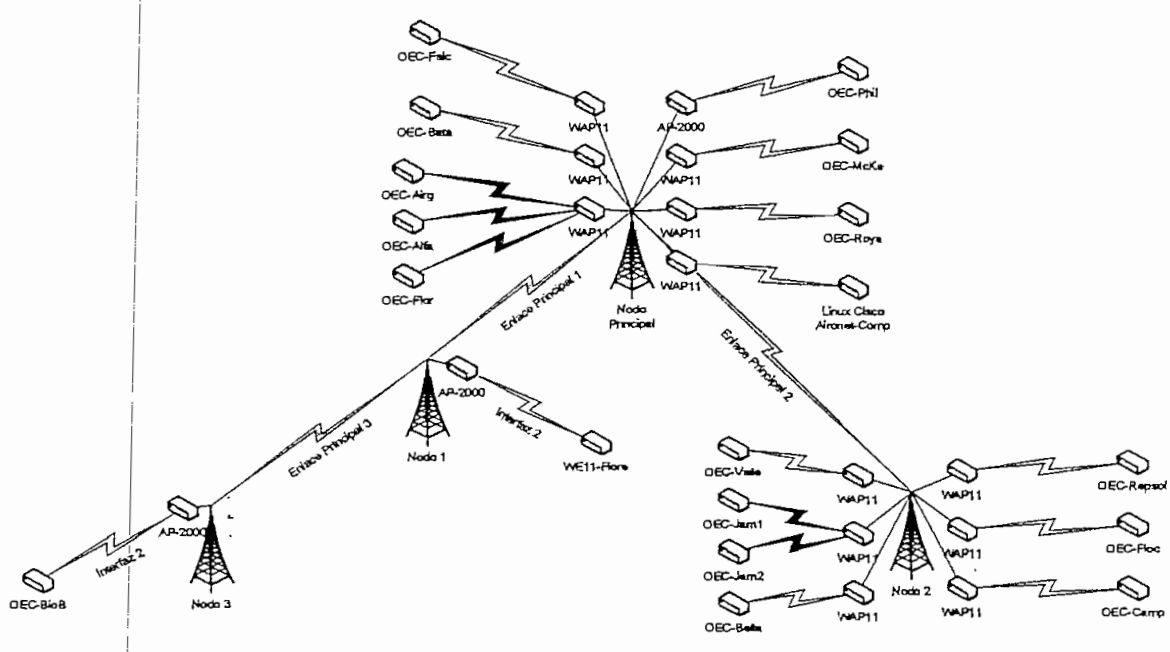


Figura 5.20. Red Externa del ISP

BIBLIOGRAFÍA CAPÍTULO V

[1] CISCO NETWORKING ACADEMY PROGRAM. Cisco Certified Network Associate Study Guide.

[2] http://www.proxim.com/learn/library/datasheets/quickbridge2.pdf: Tsunami QuickBridge II.

[3] http://www.proxim.com/learn/library/datasheets/quickbridge20_US.pdf: Tsunami QuickBridge 20.

[4] http://www.cisco.com/application/pdf/en/us/guest/products/ps5285/c1650/ccmigration_09186a008018495c.pdf: CISCO AIRONET 1400 SERIES WIRELESS BRIDGE.

[5] http://www.rad.com/RADCnt/MediaServer/15258_AirMux_fam.pdf: AirMux Family.

[6] TERÁN MOREANO, Rubén Edison / CASTRO BUNGACHO, Juan Carlos. Estudio y Diseño de Redes Multiacceso para la Entrega de Servicios de Telecomunicaciones Rentables. Escuela Politécnica Nacional. 2003.

[7] PAZMIÑO GÓMEZ, Giovanni René. Diseño de una Red Inalámbrica para Interconectar la Matriz de la Empresa Video Audio Sistemas Sony con sus Sucursales. Escuela Politécnica Nacional. 2002.

[8] GUEVARA ARMIJOS, Jofre Enrique / VILLACÍS NAVAS, Jonathan Mauricio. Diseño de una Red Inalámbrica con Tecnología Spread Spectrum entre Pozos Petroleros y la Central de Operaciones para el Desempeño de un Sistema Móvil de Administración con Terminales PocketPC. Escuela Politécnica Nacional. 2004.

[9] FEHER, Camilo. Digital Communications Microwave Applications. Prentice-Hall. USA. 1981.

[10] http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/8021q.pdf: Cisco IOS IEEE 802.1Q Support.

[11] http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt1/qcfclass.pdf: Classification Overview.

[12] http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt1/qcfcar.pdf: Configuring Committed Access Rate.

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

El presente proyecto de titulación constituye una guía para comprender la estructura y funcionamiento de un proveedor de servicios de Internet o ISP, y cómo se puede utilizar la tecnología WLAN que es de bajo costo, para entregar accesos de última milla.

Un proveedor de servicios de Internet local, básicamente debe estar constituido de tres partes fundamentales para su operación. La primera es la red de acceso a Internet, la cual interconecta el ISP local con un ISP de nivel superior. La segunda es la red interna del ISP, la cual debe tener ciertos servidores con servicios básicos de Internet como son servidor de correo, servidor DNS, servidor *Web*, etc. Y por último la red de acceso al cliente que interconecta cada uno de los clientes mediante tecnologías como HFC, ADSL, *Frame Relay*, ATM, tecnologías Inalámbricas, etc.

Las redes WLAN son redes con todas las características y beneficios de las redes LAN tradicionales pero sin las limitaciones de los cables. Estas redes trabajan en las frecuencias de los 2.4 GHz y 5 GHz, y su rol principal se encuentra en las redes de acceso y redes de distribución. Entre las aplicaciones más comunes en nuestro medio se tienen redes inalámbricas fijas (interconectividad a PCs de escritorio), redes inalámbricas móviles (interconectividad de *laptops* y PDAs) y enlaces punto-a-punto o punto-a-multipunto para accesos de última milla.

Las topologías de las redes WLAN 802.11 indican el verdadero valor de este tipo de redes. Su flexibilidad y versatilidad justifican perfectamente su existencia ya que en circunstancias muy concretas que contemplan las características de

edificios, ubicación de los equipos a interconectar, necesidad de movimiento continuo, etc., las redes WLAN son casi la única solución, permitiendo además una gran variedad de configuraciones, desde la más simple como la red *Ad Hoc* hasta otras más complejas y con más posibilidades como la red de infraestructura.

Las redes WLAN 802.11b utilizan transmisión *half duplex*, por lo cual no pueden trasmitir y recibir información al mismo tiempo en una sola frecuencia. Para solucionar este problema hace uso de CSMA/CA y MACA para el control de acceso al medio. Esto genera una gran cantidad de *broadcast* en todo el segmento de red al que se encuentran conectadas, esto puede originar un gran problema si el número de dispositivos WLAN es considerable.

Las redes WLAN según la especificación 802.11b utilizan la técnica DSSS para la transmisión con velocidades de 1, 2, 5.5 y 11 Mbps lo que las hace compatibles y les permite interoperar con dispositivos WLAN según la especificación original. Esto es muy útil en situaciones en donde se desee bajas tasas de transmisión para lo cual se puede utilizar dispositivos WLAN según la especificación original sin ningún problema.

Las redes WLAN según el estándar 802.11 poseen dos mecanismos de seguridad básicos, un mecanismo de autenticación basado en el SSID y un mecanismo de encriptación que utiliza el algoritmo WEP. Estos mecanismos son poco eficientes a la hora en que un *hacker* malicioso logra tener acceso a los datos que circulan por el segmento inalámbrico, ya que son muy fáciles de descifrar mediante el uso de herramientas de software.

Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del tipo de uso que se vaya a dar a la red, de si es una red ya existente o una nueva, y del presupuesto del que se disponga para implementarla, entre otros factores. En el caso del ISP analizado si se desea dar soluciones utilizando los más recientes avances se puede incurrir en costos muy elevados debido a que es una red ya establecida. Aunque se lograría una

seguridad extrema, ésta puede estar demás por el hecho de que son redes utilizadas como accesos de última milla, las cuales de por si son de difícil acceso.

La restricción de acceso mediante direcciones MAC es insuficiente para cualquier red WLAN, dado el gran número de herramientas disponibles libremente para cambiar la dirección MAC de una tarjeta cualquiera. Sin embargo, hay que tomar en cuenta que estas herramientas son útiles siempre y cuando el atacante logre recolectar una cantidad suficiente de tramas del segmento inalámbrico.

En aplicaciones en ambientes internos de las WLAN, la seguridad mediante el uso de WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso de WEP está formalmente desaconsejado, por la facilidad con la que pueden romper las claves WEP en un entorno de alto tráfico. En aplicaciones en ambientes externos como accesos de última milla esto es mucho más complejo por la dificultad que presenta el recolectar las tramas del segmento inalámbrico.

El uso de las VPNs es una muy buena alternativa en aplicaciones en sitios internos de las WLAN cuando se tiene una red constituida y los dispositivos WLAN no soportan el protocolo 802.1x. Requiere de la instalación de software especializado en los clientes inalámbricos, y de un servidor o una serie de servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso. En ambientes externos esto no es muy aconsejable ya que por lo general el dispositivo cliente no siempre es un PC, sino un ruteador, un switch, etc., los cuales no soportan VPNs.

El uso de nuevas tecnologías para la seguridad inalámbrica como es WPA o WPA2 es una alternativa adecuada, siempre que los equipos de la red inalámbrica soporten actualizaciones ya que en caso de que no sea así, esto no sería adecuado debido a que habría que reemplazar todos los equipos WLAN.

Cualquier mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una

política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza la calidad y confidencialidad de la información presente en los sistemas de una empresa o entidad.

Los dispositivos WLAN pueden ser utilizados para establecer enlaces punto-a-punto y punto-a-multipunto. En el caso de que se utilicen dispositivos WLAN según la especificación 802.11b, se pueden obtener tasas de transmisión de 1, 2, 5.5 y hasta 11 Mbps las cuales van a depender directamente de la distancia de separación entre los puntos a enlazar, a mayor distancia menor tasa de transmisión.

Las antenas altamente direccionales son las antenas más adecuadas para establecer enlaces punto a punto, debido a que se necesita concentrar toda la potencia de transmisión a un sólo punto remoto y no a un área en particular. También son adecuadas, debido a que con este tipo de antenas se reduce el riesgo de que la información transmitida se propague sin control, evitando así posibles ataques por parte de usuarios mal intencionados. Para los enlaces punto-a-multipunto, las antenas más adecuadas son las semi-direccionales y no las omni-direccionales ya que se corre el riesgo de ataques debido a la difusión de la información.

Los enlaces punto-a-punto como los enlaces de última milla, pueden establecerse entre cualquier tipo de dispositivos WLAN; por ejemplo dos puntos de acceso, un punto de acceso y un dispositivo cliente, entre dos bridges inalámbricos, etc. En los enlaces punto-a-multipunto necesariamente se debe hacer uso de un punto de acceso en un extremo para así permitir la asociación de los otros dispositivos que se encuentran en los lados remotos.

El costo de un enlace con tecnología WLAN está muy por debajo que cualquier otra tipo de tecnología inalámbrica. La razón principal de esto es que los radios son mucho más económicos debido a que utilizan transmisión *half duplex* en comparación con los radios de otras tecnologías que utilizan tecnología de

transmisión *full duplex.*

El uso de las VLANs dentro de una red presenta muchas ventajas, pues segmentan de manera lógica la red conmutada facilitando la administración de grupos lógicos de estaciones y servidores, sin importar la ubicación física de los usuarios o las conexiones físicas a la red. Al segmentar de forma lógica la red, cada VLAN se convierte en un dominio de *broadcast* diferente lo que permite segmentar el dominio de *broadcast* de una red en tantos dominios como VLANs se tengan. Esta segmentación del dominio de *broadcast* es muy importante ya que cuando el dominio es muy grande se pueden producir graves problemas de congestión debido a la propagación del *broadcast.*

La asignación de una VLAN diferente a cada uno de los enlaces de última milla, permite que el *broadcast* generado por los dispositivos WLAN que conforman dichos enlaces, no se propague más allá del puerto del switch en el que se encuentra configurada la VLAN, de esta forma se evita cualquier tipo de congestión dentro de la red del ISP por parte de estos dispositivos.

La limitación del ancho de banda a los enlaces de última milla en cada uno de los ruteadores de los diferentes nodos del ISP es muy ventajoso, pues con el uso de CAR de Cisco Systems, se puede establecer la velocidad de transmisión que el cliente necesite, incluso se puede configurar canales asimétricos en el caso de que el cliente necesite mayor tasa de transferencia para su enlace de subida hacia Internet o viceversa.

La limitación del ancho de banda en cada enlace WLAN será factible siempre y cuando dicho enlace se encuentre asociado a una VLAN y esta VLAN a su vez a una subinterfaz del ruteador, al cual se concentre. El CAR de Cisco Systems sólo es posible configurar en la interfaz o subinterfaz de los ruteadores Cisco, es por esto que cada enlace WLAN debe tener su propia subinterfaz asignada.

6.2 RECOMENDACIONES

Para un mejor funcionamiento de la red interna del ISP, se recomienda reemplazar el *hub* de la red de servidores por un *switch*, ya que por este segmento transita mucho tráfico. Al utilizar un *switch* se logra segmentar el dominio de colisión, evitando así saturación en este segmento a causa de las colisiones.

Se recomienda incrementar las políticas de seguridad sobre la red interna del ISP, mediante el uso de un *Firewall*, este puede ser aplicado a nivel de hardware (recomendado) o a nivel de software. El *Firewall* va a impedir que ciertos puertos que no se estén ocupando sean cerrados para evitar visitas inesperadas, por ejemplo el servicio de Telnet sobre el puerto 23.

Se recomienda que el ISP se asocie al NAP local del Ecuador y se interconecte con el mismo. Esto va a ser muy beneficioso para el ISP ya que en muchos de los clientes la mayor parte de tráfico que generan es de carácter Nacional, de este modo se va disminuir notablemente el tráfico internacional, consiguiéndose aprovechar de mejor manera el enlace Internacional.

El Internet en la actualidad tanto en nuestro país como en el mundo entero, se ha convertido en una herramienta indispensable para los negocios, la industria y la educación. Debido a esto, la demanda por el servicio está creciendo día a día e igualmente las empresas que lo proveen, por lo que para tener éxito en el negocio se recomienda que el ISP siga utilizando la tecnología WLAN como accesos de última milla, ya que de esta forma se puede entregar un servicio de calidad y a costos mucho más económicos.

En caso de que una de las redes WLAN sufra algún tipo de ataque, es muy importante documentarlo, abarcando todos los aspectos que se conozcan del mismo, entre los que se deben incluir el daño que ha causado, puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de servicio perdido y los procedimientos para reparar el daño. Dicha documentación

ayudará a modificar las políticas actuales y así evitar ataques fututos o disminuir los daños.

Es recomendable que los equipos WLAN que el ISP adquiera a futuro, soporten los estándares actuales de seguridad pero a su vez deben ser fáciles de instalar, configurar y administrar, y lo más importante deben permitir la interoperatividad con otros dispositivos similares.

REFERENCIAS BIBLIOGRÁFICAS

[1] 05b_El_auge_de_las_redes.pdf: El Auge de las Redes Inalámbricas (WLANs).

[2] 08-802.11-Francisco-Lopez-Ortiz-res.pdf: El estándar IEEE 802.11 Wireless LAN.

[3] 802.11-1999.pdf: ANSI/IEEE Std 802.11, 1999 Edition.

[4] 802.11b-1999.pdf: IEEE Std 802.11b-1999 (Supplement to ANSI/IEEE Std 802.11, 1999 Edition).

[5] Addison Wesley - Real 802.11 Security Wi-Fi Protected Access And 802.11I Sharereactor.pdf: Real 802.11 Security: Wi-Fi Protected Access and 802.11i.

[6] CAICEDO JARAMILLO, María Soledad / YÁNEZ ANDAGANA, Fernando Isaías. Planificación de un Proveedor de Servicios de Internet y diseño de su sistema de seguridad. Escuela Politécnica Nacional. 2002.

[7] CANDO SANTO, Washington Oswaldo / CAZARES GUERRERO, Félix Federman. Estudio de un sistema MMDS bidireccional para la distribución de Internet de banda ancha. Escuela Politécnica Nacional. 2002.

[8] CERTIFIED WIRELESS NETWORK ADMINISTRADOR. Official Study Guide. MacGraw-Hill. Second Edition. 2003.

[9] CHAMORRO ARIAS, Julio Cesar. Diseño de una Red de Área Local (LAN) Inalámbrica para la Ex-Facultad de Ingeniería Eléctrica. Escuela Politécnica Nacional. 2001.

[10] CISCO NETWORKING ACADEMY PROGRAM. Cisco Certified Network Associate Study Guide.

[11] CISCO NETWORKING ACADEMY PROGRAM. Fundamentals of Wireless LANs v1.0.

[12] FEHER, Camilo. Digital Communications Microwave Applications. Prentice-Hall. USA. 1981.

[13] ftp://ftp.ipswitch.com/ipswitch/manuals/whatsupg.pdf. WhatsUp Gold - User's Guide.

[14] ftp://ftp.linksys.com/datasheet/befsr41v3_ds.pdf: EtherFast Cable/DSL Router with 4-Port Switch.

[15] ftp://ftp.linksys.com/datasheet/befsr81ds.pdf: EtherFast Cable/DSL Router.

[16] ftp://ftp.linksys.com/datasheet/wet11_v2_ds.pdf: Wireless-B Ethernet Bridge.

[17] ftp://ftp.linksys.com/pdf/wap11_v28_ug.pdf: Wireless-B Access Point.

[18] GUEVARA ARMIJOS, Jofre Enrique / VILLACÍS NAVAS, Jonathan Mauricio. Diseño de una Red Inalámbrica con Tecnología Spread Spectrum entre Pozos Petroleros y la Central de Operaciones para el Desempeño de un Sistema Móvil de Administración con Terminales PocketPC. Escuela Politécnica Nacional. 2004.

[19] http://206.223.8.10/linksite/manuals/datasheets/ds-sdm300a.pdf:SDM-300A Satellite MODEM.

[20] http://bandwidthcontroller.com/features.html: Bandwidth Controller.

[21] http://en.wikipedia.org/wiki/Warchalking: Warchalking.

[22] http://greco.dit.upm.es/~david/TAR/trabajos2002/10-Infraestructura-ISP-Andoni-Perez-res.pdf: Infraestructura de un ISP.

[23] http://home.intermec.com/eprise/main/Intermec/Content/About/getArticle?section=about&ArticleID=260.htm: Wireless LAN Basics.

[24] http://standards.ieee.org/getieee802/download/802.11i-2004.pdf: IEEE Std 802.11i-2004.

[25] http://www.3com.com/other/pdfs/products/en_US/400838.pdf: 3Com Baseline Switches.

[26] http://www.aed.com.ve/pdf/AK-WiFi-05-03-04.pdf: Redes de Área Local Inalámbricas.

[27] http://www.canal-ayuda.org/Seguridad/tipos_ataques.htm: Clasificación y Tipos de Ataques Contra Sistemas de Información.

[28] http://www.carsoft.com.ar/arquitectura_de_internet.htm: Arquitectura de Internet.

[29] http://www.cisco.com/application/pdf/en/us/guest/products/ps5285/c1650/ccmigration_09186a008018495c.pdf: CISCO AIRONET 1400 SERIES WIRELESS BRIDGE.

[30] http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/8021q.pdf: Cisco IOS IEEE 802.1Q Support.

[31] http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt1/qcfcar.pdf: Configuring Committed Access Rate.

[32] http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt1/qcfclass.pdf: Classification Overview.

[33] http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tqr/qftcmd8.pdf: Rate-Limit.

[34] http://www.criptored.upm.es/descarga/Laredo_jgg2.zip. Las Redes Substitución - Permutación y el AES (Advanced Encryption Standard).

[35] http://www.dcc.uchile.cl/~jpiquer/Internet/DNS/node2.html: El DNS.

[36] http://www.dcc.uchile.cl/~raparede/papers/2000memorialSP.pdf: Diseño e Implementación de Experiencias Docentes para un Sitio Proveedor de Servicios Internet.

[37] http://www.embedded.com/showArticle.jhtml?articleID=34400002: IEEE 802.11i and wireless security.

[38] http://www.faqs.org/rfcs/rfc2284.html: RFC 2284 - PPP Extensible Authentication Protocol.

[39] http://www.iec.org/online/tutorials/acrobat/eap_methods.pdf: EAP Methods for 802.11 Wireless LAN Security.

[40] http://www.kriptopolis.com/rijndael.pdf: Algoritmo Criptográfico Rijndael.

[41] http://www.merakmailserver.com/Products/Merak_Mail_Server/: Merak Mail Server Software.

[42] http://www.microsoft.com/spain/servidores/windowsserver2003/evaluation/overview/technologies/iis.aspx: Novedades de los Servicios de Internet Information Server 6.0.

[43] http://www.proxim.com/learn/library/datasheets/AP-2000_US.pdf: ORiNOCO AP-2000.

[44] http://www.proxim.com/learn/library/datasheets/quickbridge2.pdf: Tsunami QuickBridge II.

[45] http://www.proxim.com/learn/library/datasheets/quickbridge20_US.pdf: Tsunami QuickBridge 20.

[46] http://www.proxim.com/support/all/orinoco/manuals/pdf/EC_datasheet.pdf: Datasheet del WAVE LAN.

[47] http://www.rad.com/RADCnt/MediaServer/15258_AirMux_fam.pdf: AirMux Family.

[48] http://www.redbooks.ibm.com/redbooks/pdfs/sg246025.pdf: Integrating an

ISP into a RS/6000 SP.

[49] http://www.stargeek.com/item/20270.html: WPA's Little Secret.

[50] http://www.webopedia.com/TERM/a/accounting.html: What is accounting.

[51] http://www.webopedia.com/TERM/n/network_management.html: What is network management.

[52] http://www.webopedia.com/TERM/R/RADIUS.html: What is RADIUS.

[53] http://www.weca.net/opensection/pdf/memberprs/sep04/pr_bw_wpa2_pr_final.pdf: Broadcom Wireless LAN Solutions Wi-Fi CERTIFIED for WPA2.

[54] http://www.weca.net/opensection/pdf/WFA_02_27_05_WPA_WPA2_White_Paper.pdf: Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise.

[55] http://www.weca.net/opensection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf: Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks.

[56] http://www.weca.net/opensection/pdf/wpa2_q_a.pdf: Questions and Answers.

[57] http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf: Wi-Fi Protected Access.

[58] http://www.wi-fi.org/OpenSection/ReleaseDisplay.asp?TID=4&ItemID=181&StrYear=2004&strmonth=9: Wi-Fi Alliance Introduces Next Generation of Wi-Fi Security.

[59] IEEE 802_11b Wireless LAN White Paper.pdf: IEEE 802.11b Wireless LANs.

[60] Jamdrid-seguridad_redes_inalambricas.pdf: Seguridad en Redes Inalámbricas.

[61] PAZMIÑO GÓMEZ, Giovanni René. Diseño de una Red Inalámbrica para Interconectar la Matriz de la Empresa Video Audio Sistemas Sony con sus Sucursales. Escuela Politécnica Nacional. 2002.

[62] PROAÑO AYABACA, Hugo Iván. Sistemas autónomos para Proveedores de Servicio de Internet. Escuela Politécnica Nacional. 2001.

[63] SeguridadWireless.pdf: Seguridad en Redes Inalámbricas.

[64] STALLINGS, Williams. Data and Computer Communications. Prentice Hall. Sixth Edition. 2000.

[65] TERÁN MOREANO, Rubén Edison / CASTRO BUNGACHO, Juan Carlos. Estudio y Diseño de Redes Multiacceso para la Entrega de Servicios de Telecomunicaciones Rentables. Escuela Politécnica Nacional. 2003.

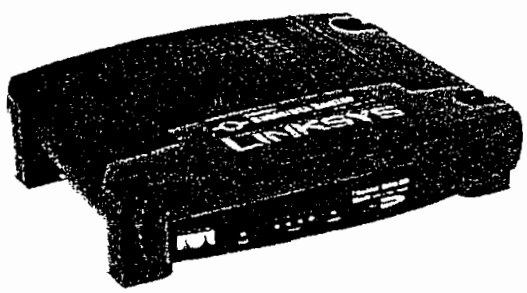
[66] TOSCANO JIMÉNEZ, Miguel Ángel / GUIJARRO CÓRDOVA, René Fernando. Estudio y diseño de un ISP para la EPN y de la conectividad entre la EPN y un nodo principal del backbone de Internet. Escuela Politécnica Nacional. 2004.

[67] Wiley - Building Secure Wireless Networks with 802.11.pdf: Building Secure Wireless Networks with 802.11.

[68] WLAN_Security_Concepts.pdf: Wireless LAN Security.

LINKSYS®
A Division of Cisco Systems, Inc.

Share Your High-Speed Internet Connection Throughout Your Home or Office



Think of the EtherFast Cable/DSL Router with 4-Port Switch as a kind of "splitter" for your Internet connection. Just connect your DSL or Cable Modem to the Router, and all the computers in your household can share the Internet—all at the same time. The built-in 4-port switch lets you attach four local PCs directly, or daisy-chain out to more hubs and switches as your network grows.

Once your computers are connected to the Internet through the Router, they can communicate with each other too, sharing resources and files. All your computers can print on a shared printer connected anywhere in the house. And you can share all kinds of files between computers—music, digital pictures, and other documents. Keep all your digital music on one computer, and listen to it anywhere in the house. Organize all of your family's digital pictures in one place, to simplify finding the ones you want, and ease backup to CD-R. Play head-to-head computer games within the household, or against Internet opponents. Utilize extra free space on one computer when another's hard drive starts to fill up.

It's all easier than you think—the included Setup Wizard takes you through configuring the Router, step by step. The Router can act as a DHCP server for your network, so your PCs are configured automatically. Universal Plug-and-Play (UPnP) lets specialized Internet applications configure the Router so you don't have to. Built-in NAT technology helps you protect your family while the Router helps keep intruders out of your computers.

With the EtherFast Cable/DSL Router with 4-Port Switch at the heart of your home network, you don't need to be a networking genius to share printers, files, and your high-speed Internet connection.

Share your high-speed cable or DSL Internet connection with multiple computers

Built-in switch connects four local PCs directly, and daisy-chain out to more hubs and switches as your network grows

Supports DHCP, Universal Plug-and-Play (UPnP), and includes a user-friendly Setup Wizard for easy configuration

EtherFast®

Cable/DSL Router with 4-Port Switch

Product Data

Model No. **BEFSR41**

CISCO SYSTEMS

herFast®

Cable/DSL Router

with 4-Port Switch

Features

- Supports Universal Plug-and-Play for Easy Configuration
- Supports IPSec and PPTP Pass-through
- Administer and Upgrade the Router Remotely over the Internet
- Configurable as a DHCP Server on Your Network
- Advanced Security Management Function for Port Filtering, MAC Address Filtering, and DMZ Hosting
- Automatically Detects Straight or Cross-over Cable

Specifications

Model Number	BEFSR41
Standards	IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX)
Ports	One 10/100 RJ-45 Port for Broadband Modem Four 10/100 RJ-45 Switched Ports
LED Indicators	Power, Ethernet, Internet
UPnP able/cert	Yes
OS Support	Windows 98SE/Me/2000/XP
Network Protocols	TCP/IP, NetBEUI, IPX/SPX

Environmental

Dimensions (W x D x H)	186 mm x 154 mm x 48 mm (7.32" x 6.06" x 1.89")
Unit Weight	12.28 oz. (0.35 kg)
Power Input	External, 9V AC, 1000 mA
Certifications	FCC, CE
Operating Temp.	32°F to 104°F (0°C to 40°C)
Storage Temp.	-4°F to 158°F (-20°C to 70°C)
Operating Humidity	10% to 85%, Non-Condensing
Storage Humidity	5% to 90%, Non-Condensing

Linksys
17401 Armstrong Ave.
Irvine, CA 92614 USA
E-mail: sales@linksys.com
support@linksys.com
Web: http://www.linksys.com

Linksys products are available in more than 50 countries, supported by 12 Linksys Regional Offices throughout the world. For a complete list of local Linksys Sales and Technical Support contacts, visit our Worldwide Web Site at www.linksys.com.

Minimum Requirements

- Broadband connection and Cable/DSL modem
- TCP/IP Protocol
- CD-ROM Drive
- Internet Explorer 5.0 or Netscape 6 for web-based configuration
- Network adapter
- Network cable

Package Contents

- Phone Cable
- Power Adapter
- Network Cable
- Setup CD-ROM with User Guide
- Fast Start Guide
- Registration Card

BEFSR41 V3-DS-30610NC-UL

Product Data

Model No. **BEFSR41**

LINKSYS®

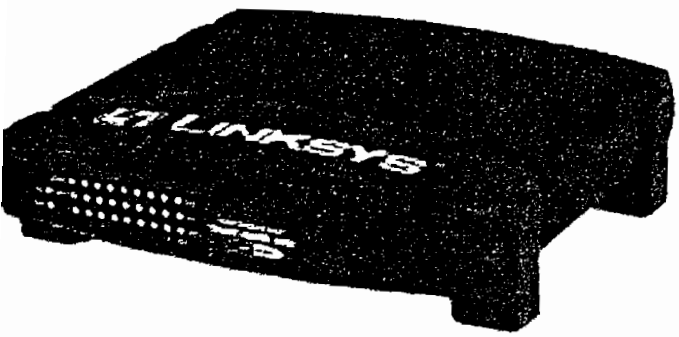
EtherFast® Cable/DSL Router with QoS

With a Built-In 8-Port 10/100 Switch for Sharing High-Speed Internet Access

Do you find Internet sharing software to be nothing but a hassle? Can't find a simple and inexpensive way to share your one Internet IP address over your entire network? If so, then the Linksys Instant Broadband Cable/DSL Router is exactly what you're looking for.

The Instant Broadband EtherFast® Cable/DSL Router from Linksys offers the perfect solution for connecting up to 253 of your PCs to a high-speed broadband Internet connection and a 10/100 Fast Ethernet backbone. Configurable as a DHCP server for your network, the EtherFast® Cable/DSL Router acts as the only externally recognized Internet gateway on your local area network (LAN). The Router can also be configured via SNMP to filter internal users' access to the Internet and serve as a NAT firewall against unwanted outside intruders on the Internet.

The Cable/DSL Router features advanced functions such as dynamic and static port routing, DMZ hosting, filtering and forwarding, and Quality of Service capabilities. All of these functions can be easily configured through your networked PC's web browser.



INSTANT BROADBAND™ CABLE/DSL ROUTER
(BEFSR81)

Benefits

- **Build a Broadband Network in Your Home or Small Office**
- **Provides Port Security, Packet Filtering, and Filters Internal User's Access**
- **QoS Capabilities Reduce the Chance of Data Loss and Allow for Port-Based Prioritization**
- **Access the Internet Over Your Entire Network With Just One IP Address**
- **NAT Firewall Protects Your PCs From Unwanted Outside Intruders on the Internet**
- **Remote Administration Over the Internet**
- **Free Technical Support—24 Hours a Day, 7 Days a Week in North America Only**
- **1-Year Limited Warranty**

Features

- Provides Port Security, Packet Filtering, and Filters Internal User's Access
- Identifies Up to Four Ports for High or Low Port-Based Prioritization
- QoS Capabilities Based on IEEE 802.1p and IP TOS/DS Greatly Reduces the Chance of Data Loss Based on Weighted Round-Robin (WRR)
- Dramatically Speed Up Your Gaming and Multimedia Connections With the Internal Switch
- Full Wirespeed Layer Two Switching on All LAN Ports
- 1K MAC Address Table Means Both Auto Address Learning and Aging
- Configurable Through A Networked PC's Web Browser
- Acts as a DHCP Server For Your Network
- Administrators Can Block Specific Internal Users' Internet Access with Filtering
- Supports WinSock 2.0 and Windows 2000 Smart Applications
- Free Technical Support—24 Hours a Day, 7 Days a Week in North America Only
- 1-Year Limited Warranty

Specifications

Model Number:	BEFSR81
Standards:	IEEE 802.3, IEEE 802.3u, IEEE 802.1p
Protocol:	CSMA/CD
Ports:	LAN: Eight 10/100 RJ-45 Ports WAN: One 10BaseT Port
Cabling Type:	**10BaseT:** UTP Category 3 or Better **100BaseTX:** UTP Category 5 or Better
Topology:	Star
Speed:	LAN: 10Mbps (10BaseT Ethernet) or 100Mbps (100BaseTX Fast Ethernet) WAN: 10Mbps (10BaseT Ethernet)
LEDs:	Power LAN: QoS, Link/Act, Full/Col, 100 WAN: Diag, Act, Link

Environmental

Dimensions:	7.31" x 6.16" x 1.88" (186mm x 154mm x 48mm)
Unit Weight:	17.8 oz. (0.5 Kg)
Power:	External, 5V DC, 3A
Certifications:	FCC Class B, CE Mark Commercial
Operating Temp:	0°C to 40°C (32°F to 104°F)
Storage Temp:	-20°C to 70°C (-4°F to 158°F)
Operating Humidity:	10% to 85% Non-Condensing
Storage Humidity:	5% to 90% Non-Condensing

Package Contents

Instant Broadband
EtherFast® Cable/DSL Router

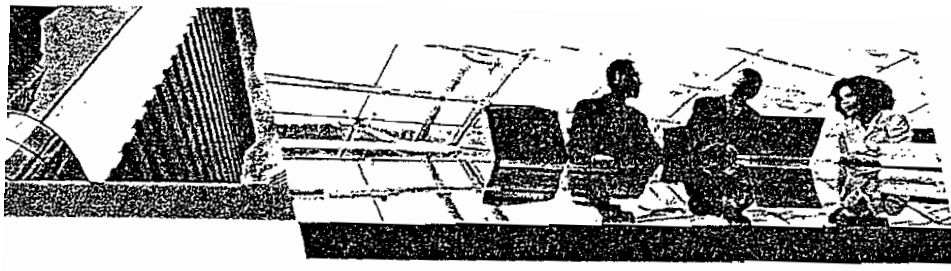
- One Instant Broadband™ Cable/DSL Router
- One AC Adapter and Power Cord
- One User Guide and Registration Card

Model Number: BEFSR81

Linksys
17401 Armstrong Ave.
Irvine, CA 92614 USA

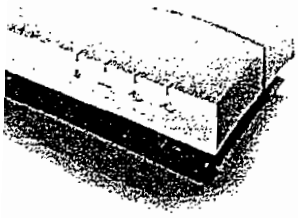
Information	(800) 546-5797
Technical Support	(800) 326-7114
	(949) 261-1288
Fax	(949) 261-8868
World Wide Web	http://www.linksys.com
Email	sales@linksys.com
	support@linksys.com
China	
Tech Support	(10) 6432 1920
Sales	(10) 6432 1923
Fax	(10) 6437 6891
Philippines	
Telephone	(632) 638-6580
Fax	(632) 635-6772
Japan	
Telephone	(03) 5259-5139
Fax	(03) 5259-5117
Singapore	
Telephone	552-8998
Fax	552-1024
Thailand	
Telephone	717-0770
Fax	717-0738
United Kingdom	
Tech Support	0870 7393939
Sales	01245 352403
Fax	0870 7393938

LINKSYS®



proxim
WIRELESS NETWORKS

ORiNOCO AP-2000
Tri-mode Access Point



Applications

Small, medium and large enterprises:
mobile access to improve employee, contractor and customer efficiency

Universities:
flexible, immediate, mobile faculty and student connectivity in dorms, classrooms, libraries and campus quads

Hospitals and medical clinics:
real time information system wide for better patient care and reduced errors

Local, state and federal agencies:
fast access to information to serve constituencies better

Large public hotspots:
robust, secure, Wi-Fi connectivity for airports, convention centers, hotels

Tri-Mode Access Point Delivers High Capacity and Flexibility

The ORiNOCO AP-2000 access point combines enterprise-class security and management features with optional tri-mode (simultaneous 802.11a/b/g) operation for maximum client diversity, and dual radio support for optimal high-density subscriber usage.

- Upgradeable, dual-slot architecture for investment protection and flexibility
- High-speed 54 Mbps support for 802.11b, 802.11g and 802.11a in one platform
- Dual 802.11b or 802.11g radio configuration optimizes for high client density environments

Proactive Security Measures to Protect Your Network

ORiNOCO access points support the latest security standards, such as Wi-Fi Protected Access (WPA), while adding proactive security measures.

- Certified WPA for IEEE 802.1X mutual authentication
- Dynamic per-user, per-session rotating keys
- Rogue access point detection, notification
- Secure management interfaces: SNMPv3 and SSL
- Fully software upgradeable to AES and 802.11i
- Intra-cell blocking to prevent client-to-client snooping

Easy to Deploy and Manage

Ease of deployment and integration with the wired network are critical factors in a successful, profitable wireless LAN rollout. ORiNOCO access points excel with key capabilities that simplify WLAN deployment.

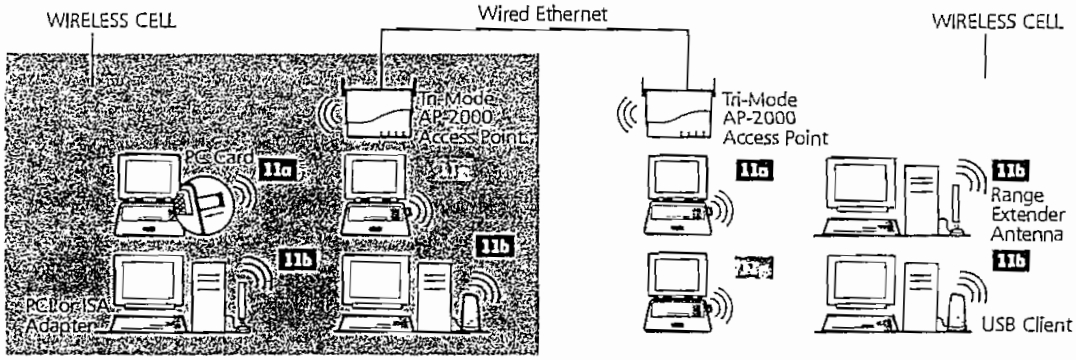
- Tools to speed installation and optimization: automatic channel selection, adjustable transmit power, external antenna connectors
- Wireless repeating functionality in areas without Ethernet wiring
- Remote management via SNMP, HTTP and Telnet
- Extensive RADIUS accounting support
- Powerful group configuration, software updates and automatic alerts via Wavelink Mobile Manager

Reliable by Design

With over 10 years of experience in the design and manufacture of wireless LANs, Proxim understands that service providers and enterprises require the same uptime and reliability in a wireless network as in a wired network. ORiNOCO access points offer:

- Robust features for enterprise, public access – compared to consumer grade APs
- Automatic reconfiguration of security policy in the event of power loss
- Dual firmware image support – for rollback in the event of software or configUration change problems
- IEEE 802.3af Power-over-Ethernet, plenum rating, built-in Kensington lock* and external antenna connectors*

*Not available on all models



Supporting 802.11b, 802.11g and 802.11a clients requires the AP-2000b/g and an AP-2000 11a Kit.

ORiNOCO AP-2000 Specifications

ADDITIONAL FEATURES

Tri-mode 802.11b, 802.11g and 802.11a support	Simultaneous 802.11b, 802.11g and 802.11a support
Field upgradeable	Software and hardware upgradeable to support new standards
Wi-Fi Protected Access (WPA) including 802.1X and dynamic TKIP encryption	Highest authentication and encryption methods including mutual authentication, message integrity check (MIC), per-packet keys initialization vector hashing and broadcast key rotation
Software upgradeable to AES and 802.11i	Investment protection for compatibility with next industry standard security specification[1]
Rogue AP Detection	Detects, alerts and stops unauthorized rogue Access Points[2]
Secure Management Interfaces	SNMPv3 and SSL protect against unauthorized AP changes via the management interface
Multiple VLAN Support	Up to 16 separate VLANs per radio
Auto configuration via DHCP	Ensures new APs automatically receive correct configuration and prevents security vulnerabilities with deliberate resets
Central management and configuration	Allows centralized management of AP settings including group updates of firmware[2]
Dual Image Support	Dual Image Support: Guarantees new AP configuration file is valid before deleting current image
Quality of Service	Allows simultaneous data and Voice over WLAN solutions from Spectralink
Load Balancing	Redirects 802.11b clients to less busy APs based on actual throughput[3]
Transmit Power Control	Supports settable transmit power levels to adjust coverage cell size[1]
Automatic Channel Selection	Simplifies installation by choosing best possible channel upon installation
Designed for Public Access	Extensive RADIUS Accounting support as well as intra-cell blocking to prevent client-to-client snooping
Repeating (Wireless Distribution System)	Allows extension of wireless LAN to areas without Ethernet wiring (parking lots, long corridors, etc) for 802.11b, 802.11g and 802.11a
Advanced Filtering Capabilities	IEEE 802.1d bridging with static MAC address filtering, network protocol filtering, Proxy ARP, multicast/broadcast storm threshold filtering, TCP/UDP port filtering, intra-cell traffic filtering, and Spanning Tree support
Active Ethernet and AC Power	Decreases installation costs up to $1000 per AP when Power over Ethernet is available.
Diversity 2.4 and 5 GHz antennas	Delivers best performance in high multipath environments
External antenna connectors	Allows use of shaped and higher gain antennas to design for most efficient AP placement
Plenum rated	Meets safety and insurance requirements when installed into air spaces
Wi-Fi Certified	Industry certification guarantees interoperability with other Wi-Fi certified clients

INTERFACE

Wired Ethernet	10/100 base-T Ethernet (RJ-45)
Wireless Ethernet	2 CardBus slots for radio NIC
RS-232	Unit configuration

HARDWARE SPECIFICATION

Processor	Intel SA110 – 233MHz
Memory	16 MB SDRAM 8 MB Flash

PHYSICAL SPECIFICATIONS

Dimensions	50 mm x 185 mm x 261 mm (2.0 in. x 7.3 in. x 10.2 in.)
Weight	1.75 kg (3.86 lb.)

ENVIRONMENTAL SPECIFICATIONS

	Temperature	Humidity
Operating	0°C to 40°C	95% (non-condensing)
Storage	-10°C to 50°C	95% (non-condensing)

POWER SUPPLY

Types	• Integrated module • Autosensing 100/240 VAC; 50/60 Hz • IEEE 802.3af Active Ethernet for power over Ethernet (for the AP-2000 AE and the AP-2000b/g)
Voltage	0.2 A

MECHANICAL SPECIFICATION

- Modular design
- Plastic cover
- Metal mounting plate that allows for placement on a wall, ceiling or table

LEDS

4 LEDs:	Power Ethernet LAN Activity Wireless Activity Slot A Wireless Activity Slot B

MANAGEMENT

- SNMPv1, SNMPv2c and secure SNMPv3 management
- Standard & ORiNOCO traps
- ORiNOCO MIB, Etherlike MIB, 802.11 MIB, Bridge MIB, MIB-II
- TFTP support
- Telnet CLI, Serial Port CLI (no proxy required)
- HTTPS (SSL) server for secure web-based management
- WaveLink Mobile Manager for group management (not included)
- Remote link test
- Syslog
- DHCP Server and Client

WARRANTY

1 year (on parts and labor)

PACKAGE CONTENTS

AP-2000:
- AP-2000 unit
- Power supply
- Software and documentation
- Radio must be ordered separately

AP-2000 AE:
- AP-2000 unit
- Support for Active Ethernet (NO power supply)
- Software and documentation
- Radio must be ordered separately

AP-2000b/g:
- AP-2000 unit with b/g radio
- Support for Active Ethernet
- Power supply
- Software and documentation

RELATED PRODUCTS

AP-2000 11b/g Kit, AP-2000 11a Kit, PC Card, Range Extender Antenna

[1] For AP-2000 b/g, AP-2000 with 11g Kit and AP-2000 11a Kit
[2] In conjunction with WaveLink Mobile Manager
[3] For Agere-based 802.11b clients only

ıut Proxim

im Corporation is a
ıal leader in wireless
working equipment for
Fi and broadband wireless
works. The company
vides its enterprise and
ice provider customers
ı wireless solutions for
mobile enterprise, public
spots, security and
veillance, last mile access,
tropolitan area networks
ı voice and data backhaul.

Gear of the Year

CommWeb TESTER'S CHOICE

Wi Fi CERTIFIED

oxim Corporation
35 Stewart Drive
ınnyvale, California 94085
l: 800.229.1630
l: 408.731.2700
x: 408.731.3675
ww.proxim.com

proxim WIRELESS NETWORKS

LINKSYS®

Instant Wireless™ Series

Wireless Access Point

Bridge Your Wired and Wireless Workgroups

Don't be bound by cabling restrictions any longer! The Wireless Access Point from Linksys delivers the freedom to configure your network <u>your</u> way. Utilization of "state-of-the-art" wireless technology gives you the ability to set up workstations in ways you never thought possible; no cables to install means less expense and less hassle.

The Wireless Access Point's high-powered antennas offer a range of operation of up to 300 feet indoors that provide seamless roaming throughout your wireless LAN infrastructure. An advanced user authentication feature ensures a high level of network security. The Wireless Access Point is easy to install (Just plug it in and you're ready to go!) and easy to use--Windows-based diagnostics and statistic tools ensure that you'll always be in control.

When all of these features come together in one compact, lightweight, and power-efficient unit, you have the ultimate in flexible networking--the Linksys Wireless Access Point.

Free Your PC From Cable Restrictions!

WIRELESS ACCESS POINT
(WAP11 VER. 2.2)

Benefits

- **Highly Efficient Antennas Provide Excellent Range of Operation**
- **Provide Wireless Connections to a Wired Network**
- **Easy Setup—Ready to Run Right Out of the Box**

Features

- Provides Wireless Access Point or Bridging
- MAC Filtering, and DHCP Client
- Adjustable Antennas Provide for Easy Physical Configuration
- Long Operating Range up to 1150 feet Outdoors
- Easy to Use Web Browser-Based Configuration
- Up to 256-bit WEP Security
- Free Technical Support—24 Hours a Day, 7 Days a Week, Toll-Free US Calls
- 1-Year Limited Warranty

Specifications

Model Number:	WAP11 ver. 2.2
Standards	IEEE 802.3, IEEE 802.3u, and IEEE 802.11b
Channels	11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
Ports	One 10/100 RJ-45 Port
Cabling Type	10BaseT: UTP Category 3 or better
Operating Range	Indoor: *up to* 300 feet Outdoor: *up to* 1500 feet
Data Rate	Up to 11Mbps
LEDs	Power, Act, Link

Environmental

Dimensions	7.31" x 6.16" x 1.88" (186 mm x 154 mm x 48 mm)
Unit Weight	12 oz.
Power	5V DC, 2A, RF Output 20 dBm
Certifications	CE, FCC Class B, UL Listed, ICS-03, WiFi, MIC
Operating Temp.	0°C to 55°C (32°F to 131°F)
Storage Temp.	0°C to 70°C (32°F to 158°F)
Operating Hum.	0% to 70% Non-Condensing
Storage Hum.	0% to 95% Non-Condensing

Package Contents

Wireless Access Point

- One Wireless Access Point ver. 2.2
- Two Detachable Antennas
- One AC Power Adapter
- One Setup CD with User Guide
- One RJ45 CAT5 UTP Cable
- One Quick Installation
- One Registration Card

Minimum Requirements

- Pentium Class 200MHz or Faster Processor
- 64MB RAM Recommended
- Internet Explorer ver. 4.0 or Netscape Navigator 4.7 or Higher for Web-Based Configuration
- CD-ROM Drive
- Windows 95/98SE/Me/NT/4.0/2000/XP
- 802.11b Wireless Adapter with TCP/IP Protocol Installed per PC

or

- Network Adapter with Ethernet (UTP CAT5) Cabling and TCP/IP Protocol Installed per PC

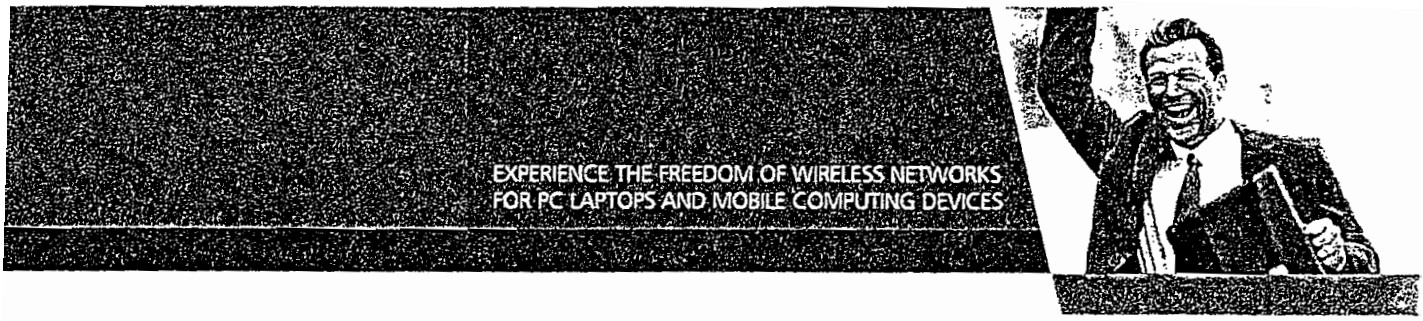
Linksys
17401 Armstrong Ave.
Irvine, CA 92614 USA

World Wide Web*	**http://www.linksys.com**
Email	**sales@linksys.com**
	support@linksys.com
Japan	
Telephone	(03) 5259-5137
Fax	(03) 5259-5117
Philippines	
Telephone	(632) 638 5580
Fax	(632) 635 5772
Singapore	
Telephone	552-8998
Fax	552-1024
Thailand	
Telephone	717-0770
Fax	717-0738
United Kingdom	
Tech Support	0870 7393939
Fax	0870 7393938

* Visit our website for the most current contact information.

LINKSYS®

DS-WAP11 vec2.2-040202B BW



ORiNOCO® 11b Client PC Card

The ORiNOCO 11b Client PC Card connects all your laptop, handheld and portable computing devices to any Wi-Fi 802.11b wireless network. With a smaller antenna and flatter profile, this card is easy to use in tight spaces. The install wizard, global roaming support and superior ORiNOCO performance give you everything you need to work the way you want, anytime and anywhere in the world.

Simple, convenient and secure 802.11b wireless connectivity for Laptop, Handheld and Portable Computing Devices

The ORiNOCO 11b Client PC Card can be used anywhere to connect to 802.11b Wi-Fi networks. The card provides 11 Mbit/s operation in the 2.4 GHz license-free frequency band. With superior radio performance and resilience to radio interference, ORiNOCO has been proven to give the best 802.11b range and throughput in the industry. The card also supports 802.11d global roaming to simplify connecting at facilities world-wide.

Offered in Silver and Gold versions, the card is equipped with a choice of security levels to protect your data: Silver with a 64-bit WEP key, or Gold with user selectable 64- and 128-bit WEP keys. Both versions support ORiNOCO's WEP+ weak key Initialization Vector suppression technology to make the cards more robust against security attacks.

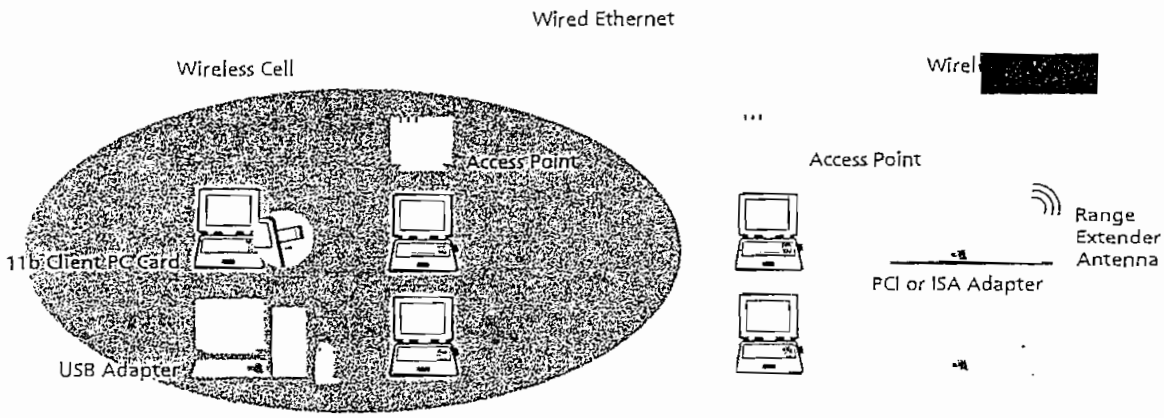
Both Gold and Silver versions of the card are furnished with a streamlined form factor and short antenna which makes it easier to work in crowded spaces. The Gold version antenna includes a built-in connector for an external Range Extender Antenna which improves performance locations where it is difficult to 'see' an Access Point.

APPLICATIONS

- Small/medium business, enterprises: improved productivity with mobile network, Internet, and email inside buildings, around campus
- Universities: flexible, immediate, mobile faculty and student connectivity in dorms, classrooms, offices
- Quick network build-out for new employees
- Hospital-wide transmission of bandwidth-intensive medical data and image files

FEATURES

- Plugs directly into PCMCIA card slot
- Intuitive client manager for easy, fast configuration
- Up to 100 location profiles
- Global roaming per 802.11d standard
- Wide coverage range of up to 1,750ft / 550m
- 802.1x authentication, 64-bit key WEP (Silver), 64/128-bit WEP key (Gold)
- Connector for external Range Extender Antenna (Gold only)



proxim
WIRELESS NETWORKS

ORiNOCO 11b Client PC Card Specifications

INTERFACE	
PCMCIA	

RADIO CHARACTERISTICS	
Frequency	2400 - 2483.5 MHz
Modulation Techniques	Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK)
Spreading	11-chip Barker Sequence
Media Access Protocol	CSMA/CA (Collision Avoidance) with ACK
Bit Error Rate (BER)	Better than 10^{-5}
Nominal Output Power	15 dBm
Power Consumption PC Card	Doze mode – 9 mA Receiver mode – 185 mA Transmit mode – 285 mA

RANGE (METERS/FT)	11 MBIT/S	5.5 MBITS	2 MBIT/S	1 MBIT/S
Open	160m (525 ft)	270m (885 ft)	400m (1300 ft)	550m (1750 ft)
Semi-open	50m (165 ft)	70m (230 ft)	90m (300 ft)	115m (375 ft)
Closed	25m (80 ft)	35m (115 ft)	40m (130 ft)	50m (165 ft)
Receiver Sensitivity dBm	-82	-87	-91	-94
Delay Spread (at FER of <1%)	65ns	225ns	400ns	500ns

PHYSICAL SPECIFICATIONS	
Dimensions	117.8mm X 53.95mm X 8.7mm (PC Card)
Weight	55 gram

ENVIRONMENTAL SPECIFICATIONS		
	Temperature	Humidity
Operating	0-55° C	95% (non condensing)
Storage	-20-75° C	95% (non condensing)

POWER SUPPLY	
Voltage	5VDC from host (±0.2V)

LEDS	
2 LEDs:	Power Network Activity

OPERATING SYSTEMS

Windows 98/2000, Me and XP

MTBF

150,000 hours based on workload, of 2040 hours/year (continuous operation), within operating conditions

WARRANTY

3 years

PACKAGE CONTENTS

- PCMCIA Card
- Getting Started Guide
- Installation Software CD-ROM

ORDERING INFO	
8420	ORiNOCO 11b Client PC Card Gold
8421	ORiNOCO 11b Client PC Card Silver

RELATED PRODUCTS

AP-4000, AP-2500, AP-2000, AP-600, 8G-2000
Range Extender Antenna (2.5 dBi)

ıut Proxim

im Corporation is a global
er in wireless networking
pment for Wi-Fi and
ıdband wireless networks. The
pany provides its enterprise
service provider customers
ı wireless solutions for the
ile enterprise, public hot
:s, security and surveillance,
mile access, metropolitan area
works and voice and data
khaul.

Proxim Corporation
2115 O'Nel Drive
San Jose, CA 95131

tel: 800.229.1630
tel: 408.731.2700
fax: 408.731.3675

proxim WIRELESS NETWORKS

Wi Fi CERTIFIED b

0032-0104

Lucent Technologies
Bell Labs Innovations

ORiNOCO™ EC and EC-S Ethernet® and Serial Converters

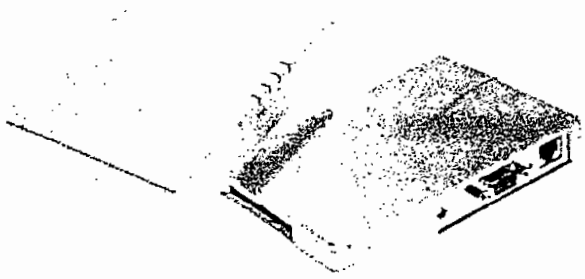
Fast, Reliable Wireless Connectivity for Ethernet Devices

With the ORiNOCO Ethernet Converter (EC) and the ORiNOCO Ethernet and Serial Converter (EC-S) products, you can wirelessly connect your Ethernet devices that are equipped with Ethernet ports and/or serial ports. The EC functions as a direct connection between an Ethernet device, using UTP cabling (10baseT), and the ORiNOCO wireless network. The EC-S adds a serial port, an RS-232 interface to the converter. With the EC-S, you can connect an Ethernet device to the ORiNOCO network while simultaneously using the RS-232 interface. Thus, you can at the same time, run a telnet connection to the network or connect a printer to the same network.

Adaptable for Many Applications

The ORiNOCO Ethernet and Serial Converter products are adaptable for many wireless networking environments such as:

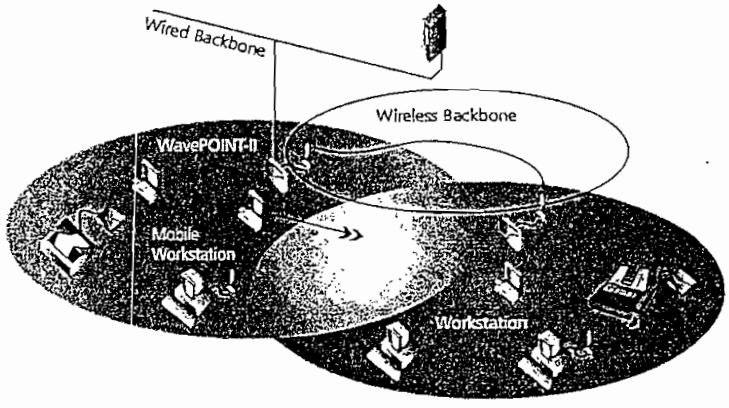
- **Retail environments** – POS terminals and scanners
- **Offices** – printers, copiers, UNIX* machines, or systems with non-standard OS
- **Industrial applications** – data collection



Special ORiNOCO Option

For those client stations that have standard support for Ethernet 10BaseT or a serial port but do not have extension slots available, the ORiNOCO Converters allow connections to the wireless infrastructure. The EC-S unit is easy to install and it is self-configuring. It provides cost-effective, wireless connectivity for Ethernet and/or RS-232 clients. All ORiNOCO EC-S units are equipped with an EC Manager tool, enabling you to customise the unit parameters easily. Clients with RS-232 ports can be serviced with a simple configuration of the ORiNOCO EC-S unit via the EC Manager or via the RS-232 port.

Basic ORiNOCO EC and EC-S Configuration



YOUR MOBILE BROADBAND CONNECTION

orinoco™ THE NEW WAVELAN

ORiNOCO EC and EC-S Specifications

Device Type	Removable PC Card Type II
Dimensions	14.1 x 9.2 x 3.0 cm (5.6 x 3.6 x 1.2 in)
Interfaces	
Serial interface/EC-S only	RS-232-C DB9 connector
WaveLAN interface	Standard WaveLAN/IEEE PC Card (not included)
Ethernet interface	RJ-45 (10BaseT) UTP
Data Rates	IEEE 802.11 Compliant
LED Indicators (4)	Power (Green) / Error (Red) Ethernet Link (Green) / Activity (Amber) WaveLAN Association (Green) / Activity (Amber) RS-232-C RX (Green) / TX (Amber) (EC-S only)
Input Voltage	5 V DC
Input Current (typical)	
Standby	30 mA
Receive	350 mA
Transmit	400 mA
Power Adapter	5 V DC / 1 Amp (Adapter included)
Operating Conditions	
Temperature	0°C to 55°C
Extended temperature range	–20°C to 70°C with limited range
Humidity	20% to 90% (non-condensing)
Comcodes	
Ethernet Converter	
848 333 415	(US)
848 333 423	(EUR)
848 333 431	(UK)
848 333 449	(AUS)
848 333 456	(JAPAN)
Ethernet & Serial Converter	
848 333 464	(US)
848 333 472	(EUR)
848 333 498	(UK)
848 333 506	(AUS)
848 333 514	(JAPAN)
848 072 633	Range Extender Antenna (5dBi) Option

Acronyms

IEEE	—	Institute of Electrical and Electronics Engineers
LAN	—	Local Area Network
OS	—	Operating System
POS	—	Point of Sale
RF	—	Radio Frequency
RS-232	—	An EIA specified physical interface between data communications equipment and data terminal equipment.
UTP	—	Unshielded Twisted Pair

For additional information, please contact your Lucent Technologies Sales Representative.

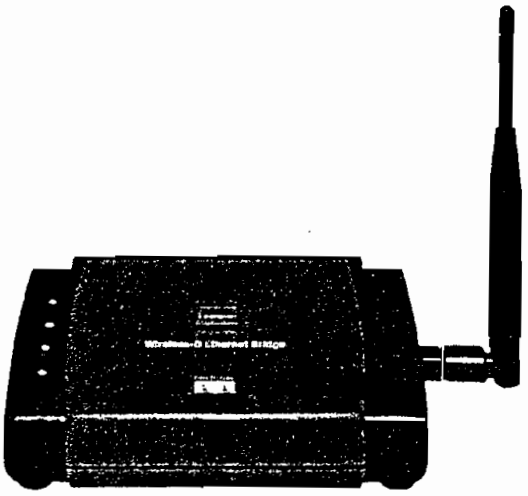
You can also visit our web site at http://www.lucent.com/orinoco or call 1-800-928-3526.

Lucent Technologies Inc.
Marketing Communications
5996 Issue 2 PJE 5/00

Lucent Technologies
Bell Labs Innovations

LINKSYS®
A Division of Cisco Systems, Inc.

Connect any Ethernet-equipped device to a wireless network



The versatile Wireless-B Ethernet Bridge can make any wired Ethernet-equipped device a part of your wireless network. At home, use the Wireless-B Ethernet Bridge to connect game consoles, set-top boxes, or computers into your wireless network to share your high-speed network connection. In the office, convert your Ethernet-wired printer, scanner, camera, notebook or desktop into a wireless networked device.

It's completely driver-free, so it works on any platform and under any operating system! Since there are no drivers to load, setup is a snap—just plug it into your device and configure the network settings through your web browser.

You can also use the Wireless-B Ethernet Bridge as a kind of "cable-less cable" to connect remote areas together. Maybe Shipping is all the way across the warehouse from Receiving. Or maybe you want to set up a home office in your detached garage. With a Wireless-B Ethernet Bridge in the garage, and another one (or a Wireless Access Point) in the house, you're connected—with no cabling hassle.

Converts wired-Ethernet devices to wireless network connectivity	Works without drivers on Macintosh®, Windows®, PlayStation®2, Xbox™, Linux®, network printers—anything with an Ethernet port!	Provides wireless, cable-free bridging between remote workgroups	Easily configurable through your web browser

Wireless-B Ethernet Bridge

Product Data

Model No. WET11

CISCO SYSTEMS

Wireless-B
Ethernet Bridge

Features

- Interoperable with IEEE 802.11b (DSSS) 2.4GHz-Compliant Equipment
- No Additional Drivers Are Needed
- Up to 11 Mbps High-Speed Transfer Rate
- Dynamically Shifts between 11, 5.5, 2, and 1 Mbps for Maximum Adaptability
- Up to 128-bit WEP Encryption
- Easy to Install and Set up
- Free Technical Support—24 Hours a Day, 7 Days a Week, Toll-Free US Calls
- 1-Year Limited Warranty

Wi Fi CERTIFIED

Interoperable with:

2.4 GHz Band	11 Mbps ☑
	54 Mbps ☐
5 GHz Band	54 Mbps ☐
Wi-Fi Protected Access™	☐

www.wi-fi.org

Specifications

Model	WET11
Standards	IEEE 802.11b, IEEE 802.3
Ports	One 10BaseT RJ-45 port, Power port
Buttons	MDI/MDI-X slide switch, Reset
Cabling Type	Category 5 or better
LEDs	Power, LAN, WLAN, Diag
Peak Gain of Antenna	5 dBI
Transmit Power	15 dBm @ Normal Temperature
Receive Sensitivity	-85 dBm
Security	WEP 64/128 bits

Environmental

Dimensions (W x H x D)	4.72" x 1.22" x 3.70" (120 mm x 31mm x 94 mm)
Unit Weight	7.06 oz. (0.2 kg)
Power	External, DC 5 V
Certifications	FCC, CE, IC-03, Wi-Fi
Operating Temp.	0°F to 40°C (32°F to 104°F)
Storage Temp.	-20°F to 70°C (-4°F to 128°F)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Warranty	1-Year Limited Warranty

Linksys
A Division of Cisco Systems, Inc.
18582 Teller Avenue
Irvine, CA 92612 USA

E-mail: sales@linksys.com
support@linksys.com
Web: http://www.linksys.com

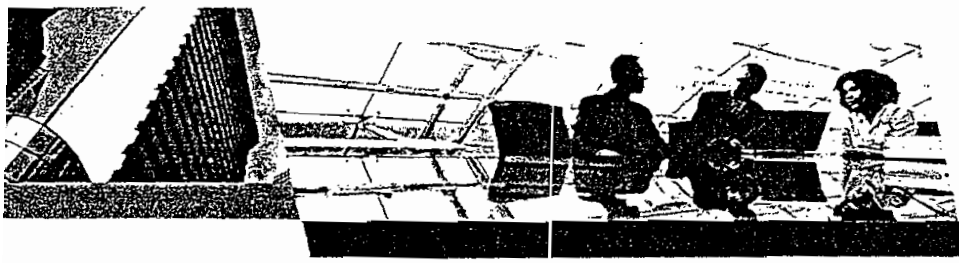
Linksys products are available in more than 50 countries supported by 12 Linksys Regional Offices throughout the world! For a complete list of local Linksys Sales and Technical Support contacts, visit our Worldwide Web Site at www.linksys.com.

Minimum Requirements

- Microsoft Windows 98SE, 2000, Me or XP (for Setup Wizard configuration purposes)
- CD-ROM Drive
- Internet Explorer 4.0 or higher, or Netscape Navigator 4.0 or higher
- Network Adapter with Ethernet (UTP CAT 5) Cabling and TCP/IP Protocol Installed per PC
  or
  802.11g or 802.11b Wireless Adapter with TCP/IP Protocol Installed

Package Contents

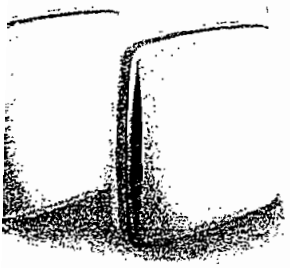
- Wireless-B Ethernet Bridge
- Quick Installation Guide
- Setup CD-ROM
- User's Guide on CD
- Detachable Antenna
- Power Adapter
- Network Cable
- Registration Card



Proxim WIRELESS NETWORKS

Tsunami QuickBridge 20

Wireless Outdoor Bridge



APPLICATIONS

- Enterprise LAN and PBX extension
- Redundant links between locations
- Voice and data backhaul from remote POPs
- Dedicated ISP connections for large subscribers
- Connectivity for long distances
- Affordable alternative to wired networks
- High-performance alternative to indoor 802.11b bridges

Data Connectivity Made Simple

Proxim's Tsunami QuickBridge 20 is a complete, user-installable wireless point-to-point bridging solution designed for reliable building-to-building data connectivity. With 18 Mbps aggregate throughput, this hop-in-a-box is a high-performance, cost-effective alternative to leased lines and indoor Wi-Fi bridges. Eliminating the deployment challenges and recurring fees associated with standard T1 and E1 installations, the Tsunami QuickBridge 20 pays for itself in less than one year.

- Nearly three times the throughput of 802.11b bridges and more than seven times the speed of a T1/E1 leased line
- Voice over IP support enables low-cost voice transmission
- Web-based QuickBridge Manager allows flexible management of local and remote radios

Designed for Complete Ease of Use

Tsunami QuickBridge is the easiest-to-install family of broadband wireless bridges on the market. Requiring no training or wireless experience, they can be set up and installed within hours. Each solution includes everything you need to set up a link right out of the box.

- Hop-in-a-box solution includes two radios with integrated antennas, cables, mounting hardware, power supply and documentation
- Easy to use software enables fast configuration
- Audible tones ensure antennas are properly aligned

Cost-effective Connectivity

The Tsunami QuickBridge family offers the best price-performance for campus networking and backhaul applications. Supporting voice and data transmission, they can easily replace T1/E1 or DS-3 connections with a payback of less than one year.

- Capacity from 6 to 54 Mbps supports enterprise and service provider bandwidth-intensive applications
- Connectivity for buildings located up to 6 miles away
- Synchronous voice channels available for low cost PBX extensions

Flexibly Manage Your Entire QuickBridge Network

Designed for outdoor networks, Tsunami QuickBridge management tools enable network managers to view and proactively maintain all radios located throughout multiple facilities. In contrast to leasing lines, network ownership gives managers complete visibility into local and remote bridges.

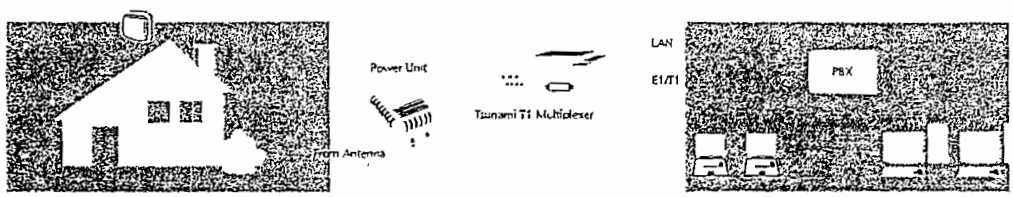
- Built-in SNMP support and web-based QuickBridge Manager simplify remote management and integrate easily into existing network policies
- Proactive alarm notifications enable network managers to maximize network performance

Secure & Reliable

A wireless alternative to a wired network provides greater control over network quality. Backed by more than 20 years of wireless design innovation, Proxim's Tsunami QuickBridge solutions offer the highest security and reliability available in networking today.

- Up to 99.995% RF link availability
- Meets or exceeds wired network security
- Proprietary encryption methods ensure secure data transmission

Installation As Easy As 1-2-3



1 Mount Quickbridge onto outside of each building

2 Using supplied CAT-5 cable, connect Quickbridge unit to indoor power unit, then to Tsunami T1 Multiplexer and power up units

3 Connect directly to exisiting LAN and PBX

Tsunami QuickBridge 20 Specifications

	FREQUENCY BAND	AGGREGATE THROUGHPUT	CHANNEL PLANS	THRESHOLD (BER=1X10⁻⁶)	EIRP OUTPUT POWER	SYSTEM GAIN (INCLUDING ANTENNA)	DISTANCE (MILES/KM)
QuickBridge 20	5.725–5.825 GHz	18 Mbps	7	-89dBm	+36 dBm	145 dB	Up to 6 miles/10 Km

RADIO CHARACTERISTICS	CHANNEL PLAN	FREQUENCY	CHANNEL PLAN	FREQUENCY
Frequency	3A	5740.401 MHz	4A	5743.85 MHz
	3B	5774.984 MHz	4B	5764.60 MHz
	3C	5809.568 MHz	4C	5785.35 MHz
			4D	5806.10 MHz
Transmit Output Power	+16 dBm max; +15 dBm typical			
Antenna	Integrated LHCP; 20dBi, 10° azimuth by 10° elevation			
Maximum Receive Level	-20 dBm error free			
Latency	2.5 msec typical, 5 msec maximum			
Access Method	Time Division Duplex			
Modulation Technique	QPSK with equalization and FEC			
Security Key	16 Character Security ID (Alphanumeric); authentication and PN transmission; scrambling			
Compliance	US: FCC Part 15.247 ISM; Canada: IC RSS 210; Model 40100-25			

DATA INTERFACE	
Ethernet Interface	10/100BaseT via AC power adapter
Connector	RJ-45 female modular plug w/ weather-protected shell
Cable Type	CAT5
Compliance	IEEE 802.3

MANAGEMENT	
Local, Remote Access	QuickBridge Manager (Java-based GUI) for discovery, status, and configuration
Software Upgradeable	Over-the-air reprogramming
Security	2-level password access on Manager

ELECTRICAL SPECIFICATIONS	QUICKBRIDGE
AC Power	Adapter included, 110 VAC or 220 VAC, 450mA; Output: 28V DC, 0.6 A
DC Power (to unit)	+18–+28 VDC
Power Connector	Power over Ethernet CAT5 cable RJ-45

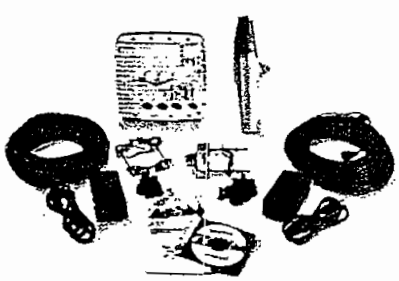
ENVIRONMENTAL SPECIFICATIONS	QUICKBRIDGE
Operational Temperature	-25°–55° C
Storage Temperature	-55°–85° C
Humidity	5–100% condensing
Altitude	Up to 10,000 ft
Wind Loading	115 mph

PHYSICAL SPECIFICATIONS	QUICKBRIDGE
Dimensions	10.5 x 10.5 x 7 in; 26.5 x 26.5 x 14.4 cm
Weight	10 lbs/4.5 kg
Mounting (Installation)	Pole Mount 1.5–2.75 in/3.08–6.98 cm O.D. (hardware included for 1.75 in/4.4 cm O.D.)

PACKAGE CONTENTS

2 QuickBridge Radio Units, 2 sets mounting hardware, 2 power adapters, 2 sets 50 meter Cat5 cable, 2 sets user documentation & utilities on CD-Rom

ORDERING INFORMATION	
301-48001-002	Tsunami QuickBridge 20 Kit – 110/220 VAC



ɔut Proxim

ɨim Corporation is a
ɔal leader in wireless
working equipment for
Fi and broadband wireless
works. The company
vides its enterprise and
vice provider customers
h wireless solutions for
· mobile enterprise, public
: spots, security and
veillance, last mile access,
tropolitan area networks
d voice and data backhaul.

roxim Corporation
35 Stewart Drive
unnyvale, California 94085
l: 800.229.1630
l: 408.731.2700
x: 408.731.3675
ww.proxim.com

proxim WIRELESS NETWORKS

TDG-1004

ISCO SYSTEMS

ATA SHEET

CISCO CATALYST 2950 SERIES SWITCHES WITH STANDARD IMAGE SOFTWARE

'RODUCT OVERVIEW

he Cisco® Catalyst® 2950SX48, 2950T-48, 2950SX-24, 2950-24, and 2950-12 switches, members of the Cisco Catalyst 2950 Series, are tandalone, fixed-configuration, managed 10/100 Mbps switches providing basic workgroup connectivity for small to midsize networks. These wire-peed desktop switches come with Standard Image software features and offer Cisco IOS® Software functions for basic data, voice, and video ervices at the edge of the network.

Embedded in all Cisco Catalyst 2950 Series switches is the Cisco Device Manager software, which allows users to easily configure and monitor the switch using a standard Web browser, eliminating the need for more complex terminal emulation programs and knowledge of the command-line interface (CLI). Customers can easily initialize the switch with web-based Cisco Express Setup, without using the CLI. In addition, with Cisco Network Assistant, a standalone network management software, customers can simultaneously configure and troubleshoot multiple Cisco Catalyst desktop switches. Cisco Device Manager, Cisco Express Setup, and Cisco Network Assistant reduce the cost of deployment by enabling less-skilled personnel to set up switches quickly. Furthermore, Cisco Catalyst 2950 Series switches provide extensive management tools using Simple Network Management Protocol (SNMP) network management platforms such as CiscoWorks.

This product line offers two distinct sets of software features and a range of configurations to allow small, midsize, and enterprise branch offices to select the right combination for the network edge. For networks that require additional security, advanced quality of service (QoS), and high availability, Enhanced Image software delivers intelligent services such as rate limiting and security filtering for deployment at the network edge.

The Cisco Catalyst 2950SX-48, 2950T-48, 2950SX-24, 2950-24 and 2950-12 switches (Figures 1–5) are available only with the Standard Image (SI) software for the Cisco Catalyst 2950 Series. They cannot be upgraded to the Enhanced Image (EI) software.

- **Cisco Catalyst 2950SX 48 Switch**—48 10/100 Mbps ports with two fixed 1000BASE-SX uplinks
- **Cisco Catalyst 2950T 48 Switch**—48 10/100 Mbps ports with two fixed 10/100/1000BASE-T uplinks
- **Cisco Catalyst 2950SX 24 Switch**—24 10/100 Mbps ports with two fixed 1000BASE-SX uplinks
- **Cisco Catalyst 2950 24 Switch**—24 10/100 Mbps ports
- **Cisco Catalyst 2950 12 Switch**—12 10/100 Mbps ports

Figure 1. Cisco Catalyst 2950-12 Switch

igure 2. Cisco Catalyst 2950-24 Switch

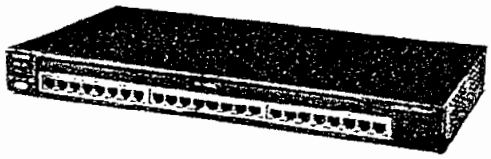


Figure 3. Cisco Catalyst 2950SX-24 Switch

Figure 4. Cisco Catalyst 2950T-48 Switch

Figure 5. Cisco Catalyst 2950SX-48 Switch

These switches provide customers with many connectivity and port-density options. The Cisco Catalyst 2950-12 and Cisco Catalyst 2950-24 switches provide 12 and 24 10/100 Mbps ports, respectively, for edge connectivity. Depending on port-density requirements, customers with gigabit fiber uplink connectivity needs can choose between the Cisco Catalyst 2950SX-24 Switch, which provides 24 10/100 Mbps ports and 2 integrated 1000BASE-SX ports, and the Cisco Catalyst 2950SX-48 Switch, which provides 48 10/100 Mbps ports and 2 integrated 1000BASE-SX ports.

With these integrated ports, customers get an extremely cost-effective solution for delivering gigabit speeds using fiber. These switches are ideal for education and government segments where fiber uplinks are required. For customers that do not need fiber connectivity, the Cisco Catalyst 2950T-48 Switch with 48 10/100 Mbps ports and two integrated 10/100/1000 BASE-T ports is a cost-effective alternative. The 10/100/1000 BASE-T ports can be used for server connectivity or for uplink connectivity to distribution or other switches. Dual ports also provide redundancy and increased availability, as well as provide a cost-effective means for cascading switches and managing them as a cluster. The Cisco Catalyst 2950 Series Intelligent Ethernet switches with Enhanced Image software are fixed-configuration models that bring intelligent services, such as advanced QoS, enhanced security, and high availability to the network edge while maintaining the simplicity of traditional LAN switching. Combining a Cisco Catalyst 2950 Series Intelligent Ethernet Switch with a Cisco Catalyst 3550 Series Switch enables IP routing from the edge to the core of the network. Refer to the Cisco Catalyst 2950 Series Enhanced Image Data Sheet for more information: http://www.cisco.com/en/US/partner/products/hw/switches/ps628/products_data_sheet09186a00801a0c5b.html

ETWORK AVAILABILITY WITH WIRE-SPEED PERFORMANCE IN CONNECTING END STATIONS TO THE LAN

ith a switching fabric of 13.6 Gbps and a maximum forwarding bandwidth of 13.6 Gbps, Cisco Catalyst 2950 Series switches deliver wire-speed rformance on all ports in connecting end stations and users to the company LAN. Cisco Catalyst 2950 Series switches with basic services support rformance-boosting features such as Cisco Fast EtherChannel® to provide high-performance bandwidth between Cisco Catalyst switches, routers, id servers.

ETWORK SECURITY

isco Catalyst 2950 Series switches offer enhanced data security through a wide range of security features. These features allow customers to provide etwork security based on users or MAC addresses. The security enhancements are available free by downloading the latest software for the Cisco 'atalyst 2950 Series switches.

ecure Shell version 2 (SSHv2) protects information from being eavesdropped or being tampered with by encrypting information being passed on he network, thereby guarding administrative information. Private VLAN Edge isolates ports on a switch, ensuring that traffic travels directly from he entry point to the aggregation device through a virtual path and cannot be directed to another port. In addition, for authentication of users with a 'ACACS+ or a RADIUS server, 802.1x provides port-level security. Simple Network Management Protocol Version 3 (SNMPv3) (non-ryptographic) monitors and controls network devices as well as manages configurations, performance, collection of statistics, and security.

For authentication of users with a Terminal Access Controller Access Control System (TACACS+) or RADIUS server, 802.1x provides port-level ecurity. 802.1x, in conjunction with a RADIUS server, allows for dynamic port-based user authentication. 802.1x-based user authentication can be extended to dynamically assign a VLAN based on a specific user, regardless of where they connect on the network. With 802.1x with Guest VLAN, guests are allowed access to the Internet via the Guest VLAN but cannot access the customer's internal network. This intelligent adaptability allows IT departments to offer greater flexibility and mobility to their stratified user populations. By combining access control and user profiles with secure network connectivity, services, and applications, enterprises can more effectively manage user mobility and drastically reduce the overhead associated with granting and managing access to network resources.

With the Cisco Catalyst 2950SX-48, 2950T-48, 2950SX-24, 2950-24, and 2950-12 switches, network managers can make ports and consoles highly ecure. MAC-address-based port-level security prevents unauthorized stations from accessing the switch. Multilevel access security on the switch console and the Web management interface prevents unauthorized users from accessing or altering switch configurations and can be implemented using an internal user database on each switch or a centrally administered TACACS+ or RADIUS server. Using 802.1x in conjunction with a RADIUS server allows dynamic port-based user authentication. In addition, 802.1x can coexist with port security on a per-port basis. Security features can be deployed using Cisco Network Assistant software security wizards, which ease the deployment of security features that restrict user access to a server or portion of the network or restrict the applications used in certain areas of the network.

NETWORK CONTROL

Cisco Catalyst 2950SX-48, 2950T-48, 2950SX-24, 2950-24, and 2950-12 switches deliver LAN-edge QoS, supporting two modes of reclassification. One mode—based on the IEEE 802.1p standard—honors the class-of-service (CoS) value at the ingress point and assigns the packet o the appropriate queue. In the second mode, packets can be reclassified based on a default CoS value assigned to the ingress port by the network dministrator. In the case of frames that arrive without a CoS value (such as untagged frames), these Cisco Catalyst 2950 Series switches support classification based on a default CoS value per port assigned by the network administrator. After the frames have been classified or reclassified using one of the above modes, they are assigned to the appropriate queue at the egress. Cisco Catalyst 2950 Series switches support four egress queues, which allow the network administrator to be more discriminating and granular in assigning priorities for the various applications on the LAN. Strict Priority Scheduling configuration ensures that time-sensitive applications, such as voice, always follow an expedited path through the switch fabric. Weighted Round Robin (WRR) scheduling, another significant enhancement, ensures that lower-priority traffic receives attention without comprising he priority settings administered by a network manager. These features allow network administrators to prioritize mission-critical, time-sensitive

affic, such as voice (IP telephony traffic), enterprise resource planning (Oracle, SAP, etc.), and computer-assisted design and manufacturing, over ss time-sensitive applications such as FTP or e-mail (Simple Mail Transfer Protocol).

ETWORK AVAILABILITY

o provide efficient use of resources for bandwidth-hungry applications like multicasts, Cisco Catalyst 2950 Series switches support Internet Group lanagement Protocol Version 3 (IGMPv3) snooping in hardware. Through the support and configuration of IGMP snooping through the Cisco letwork Assistant software, these Cisco Catalyst 2950 Series switches deliver outstanding performance and ease of use in administering and anaging multicast applications on the LAN.

he IGMPv3 snooping feature allows the switch to "listen in" on the IGMP conversation between hosts and routers. When a switch hears an IGMP oin request from a host for a given multicast group, the switch adds the host's port number to the group destination address list for that group. And vhen the switch hears an IGMP leave request, it removes the host's port from the content-addressable memory (CAM) table entry.

Multicast VLAN Registration (MVR) is designed for applications using wide-scale deployment of multicast traffic across an Ethernet ring-based ervice provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the networkwide multicast VLAN.

Per VLAN Spanning Tree Plus (PVST+) allows users to implement redundant uplinks while also distributing traffic loads across multiple links. This is not possible with standard Spanning Tree Protocol implementations. Cisco UplinkFast technology ensures immediate transfer to the secondary uplink, much better than the traditional 30- to 60-second convergence time. This is yet another enhancement of the Spanning Tree Protocol implementation. An additional feature that enhances performance is voice VLAN. This feature allows network administrators to assign voice traffic to a VLAN dedicated to IP telephony, thereby simplifying phone installations and providing easier network traffic administration and troubleshooting.

NETWORK MANAGEMENT

Customers can configure one switch at a time with the embedded Cisco Device Manager, or configure and troubleshoot multiple switches with Cisco Network Assistant, a free standalone network management software application optimized for LANs of small and medium-sized businesses with up to 250 users. Cisco Device Manager offers a simple and intuitive GUI interface for configuring and monitoring the switch. The software is Web-based and embedded in Cisco Catalyst 3750, 3650, 3550, 2970, 2950, and 2940 Switches. Cisco Express Setup simplifies the switch initialization. Users now have the option to set up the switch through a Web browser, eliminating the need for more complex terminal emulation programs and knowledge of the CLI. Cisco Device Manager and Cisco Express Setup reduce the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches.

With Cisco Network Assistant, customers can configure multiple ports and switches simultaneously, perform software updates across multiple switches at once, and copy configurations to other switches for rapid network deployments. Bandwidth graphs and link reports provide useful diagnostic information, and the topology map gives network administrators a quick view of the network status. Cisco Network Assistant supports a wide range of Cisco Catalyst intelligent switches from Cisco Catalyst 2950 through Cisco Catalyst 4506. Through a user-friendly GUI, users can configure and manage a wide array of switch functions and start the device manager of Cisco routers and Cisco wireless access points

The Cisco Network Assistant Software Guide Mode leads the user step-by-step through the configuration of advanced features and provides enhanced online help for context-sensitive assistance. Cisco AVVID (Architecture for Voice, Video and Integrated Data) Wizards provide automated configuration of the switch to optimally support video streaming or video conferencing, voice over IP (VoIP), and mission-critical applications. In addition, Smartports offers a set of verified feature macros per connection type in an easy-to-apply manner. With these macros, users can consistently and reliably configure essential security, availability, quality of service, and manageability features recommended for Cisco Business Ready Campus solutions with minimal effort and expertise. These Wizards and Smartports can save hours of time for network administrators, eliminate human errors, and ensure that the configuration of the switch is optimized for these applications.

i addition to Cisco Network Assistant, Cisco Catalyst 2950 Series switches provide extensive management tools using SNMP network management latforms such as CiscoWorks. Managed with CiscoWorks, Cisco Catalyst family switches can be configured and managed to deliver end-to-end evice, VLAN, traffic, and policy management. Coupled with CiscoWorks, Cisco Resource Manager Essentials, a Web-based management tool, ffers automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of rror conditions.

RODUCT FEATURES AND BENEFITS

Feature	Benefit
Availability	
Superior Redundancy for Fault Backup	• IEEE 802.1D Spanning Tree Protocol support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • IEEE 802.1w Rapid Spanning- Tree Protocol (RSTP) provides rapid convergence of the spanning tree, independent of spanning-tree timers. • Per VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances. • Support for Cisco Spanning Tree Protocol enhancements such as UplinkFast, BackboneFast, and PortFast technologies ensures quick failover recovery and enhances overall network stability and availability. • Support for Cisco's optional RPS 675, 675-watt redundant AC power system, which provides a backup power source for one of six switches, for improved fault tolerance and network uptime. • Unidirectional link detection (UDLD) and aggressive UDLD detect and disable unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults.
Integrated Cisco IOS Software Features for Bandwidth Optimization	• Bandwidth aggregation through Cisco EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches to routers and individual servers. Port Aggregation Protocol (PagP) is available to simplify configuration. • VLAN1 minimization allows VLAN1 to be disabled on any individual VLAN trunk link. • IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) allows a spanning-tree instance per VLAN, enabling Layer 2 load sharing on redundant links. • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall system performance. • Per VLAN Spanning Tree Plus (PVST+) allows for Layer 2 load sharing on redundant links to efficiently use the extra capacity inherent in a redundant design. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices. Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all ports in the switch. • IGMPv3 snooping provides for fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to the requestors. MVR, IGMP filtering, and fast-join and immediate leave are available as enhancements. IGMP Snooping time can be adjusted to optimize the performance of multicast data flows.
Security	
Networkwide Security Features	• A private VLAN edge provides security and isolation between ports on a switch, ensuring that voice traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port. • Support for the 802.1x standard allows users to be authenticated regardless of which LAN ports they are accessing, and it provides unique benefits to customers who have a large base of mobile (wireless) users accessing the network. – 802.1x with voice VLAN permits an IP phone access to the voice VLAN regardless of the authorized or unauthorized state of the port. – 802.1x with Port Security authenticates the port and manages network access for all MAC addresses, including

Feature	Benefit
	that of the client. – IEEE 802.1x with Guest VLAN allows guests without 802.1x clients to have limited network access on the Guest VLAN. – IEEE 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user regardless of where the user is connected. • SSHv2 provides network security by encrypting administrator traffic during Telnet sessions. SSHv2 requires a special cryptographic software image due to US export restrictions • Port Security secures the access to a port based on the MAC address of a user's device. The aging feature removes the MAC address from the switch after a specific time to allow another device to connect to the same port. • MAC Address Notification allows administrators to be notified of new users added or removed from the network. • Multilevel security on console access prevents unauthorized users from altering the switch configuration. • Trusted Boundary provides the ability to trust the QoS priority settings if an IP phone is present and disable the trust setting in the event that the IP phone is removed, thereby preventing a rogue user from overriding prioritization policies in the network. • TACACS+ and RADIUS authentication enables centralized control of the switch and restricts unauthorized users from altering the configuration. • SPAN support of Intrusion Detection Systems (IDSs) to monitor, repel, and report network security violations • SNMPv3 (non-crypto) monitors and controls network devices, manages configurations, statistics collection, performance, and security. • Cisco Network Assistant software security wizards ease the deployment of security features for restricting user access to a server, a portion of the network, or access to the network.
Quality of Service	
Layer 2 QoS	• Support for reclassifying frames is based either on 802.1p class-of-service (CoS) value or default CoS value per port assigned by network manager. • Four queues per egress port are supported in hardware. • The Weighted Round Robin (WRR) scheduling algorithm ensures that low-priority queues are not starved. • Strict priority queue configuration via Strict Priority Scheduling ensures that time-sensitive applications such as voice always follow an expedited path through the switch fabric.
Management	
Superior Manageability	• SNMP and Telnet interface support delivers comprehensive in-band management, and a CLI management console provides detailed out-of-band management. • An embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis. • A Switched Port Analyzer (SPAN) port can mirror traffic from one or many ports to another port for monitoring all nine RMON groups with an RMON probe or network analyzer. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all switches within the intranet. • Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from the source device to a destination device. • Multifunction LEDs per port for port status, half-duplex/full-duplex, 10BASE-T/100BASE-TX/1000BASE-T indication, as well as switch-level status LEDs for system, redundant power supply, and bandwidth utilization provide a comprehensive and convenient visual management system. • Crash information support enables a switch to generate a crash file for improved troubleshooting.

Feature	Benefit
	• Show-interface-capabilities provide information about the configuration capabilities of any interface. • Response Time Monitoring (RTTMON) MIB allows users to monitor network performance between a Cisco Catalyst switch and a remote device.
Cisco Network Assistant Software	• Cisco Network Assistant Software is a free, standalone network management application software that simplifies the administration of networks of up to 250 users. It supports a wide range of Cisco Catalyst intelligent switches from Cisco Catalyst 2950 through Cisco Catalyst 4506. With Cisco Network Assistant, users can manage Cisco Catalyst switches plus launch the device managers of Cisco integrated services routers (ISRs) and Cisco Aironet WLAN access points by simply clicking on its icon in the topology map. • Cisco AVVID (Architecture for Voice, Video and Integrated Data) wizards use just a few user inputs to automatically configure the switch to optimally handle different types of traffic: voice, video, multicast, and high-priority data. • One-click software upgrades can be performed across the entire cluster simultaneously, and configuration cloning enables rapid deployment of networks. • Cisco Network Assistant Guide Mode helps users configure powerful advanced features by providing step-by-step instructions. • Cisco Network Assistant provides enhanced online help for context-sensitive assistance. • Easy-to-use graphical interface provides both a topology map and front-panel view of the switches. • Multidevice- and multiport-configuration capabilities allow network administrators to save time by configuring features across multiple switches and ports simultaneously. • User-personalized interface allows users to modify polling intervals, table views, and other settings within Cisco Network Assistant and retain these settings the next time they use Cisco Network Assistant. • Alarm notification provides automated e-mail notification of network errors and alarm thresholds.
Support for CiscoWorks	• Manageability is enabled through CiscoWorks network management software on a per-port and per-switch basis, providing a common management interface for Cisco routers, switches, and hubs. • SNMPv1, v2, and v3 (non-cryptographic) and Telnet interface support delivers comprehensive in-band management, and a command-line-interface (CLI) management console provides detailed out-of-band management. • Cisco Discovery Protocol (CDP) versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Support is provided by the CiscoWorks LAN Management Solution.
Ease of Use and Deployment	• Cisco Device Manager is an embedded web-based software that allows the customer to easily configure and troubleshoot the switch, eliminating the need for more complex terminal emulation programs and CLI knowledge, and reducing the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches. • Cisco Express Setup allows the customer to quickly and easily initialize a switch with a web browser • Smartports offers a set of verified feature macros per connection type in an easy-to-apply manner. With these macros, users can consistently and reliably configure essential security, availability, quality of service, and manageability features recommended for Cisco Business Ready Campus solutions with minimal effort and expertise. • Auto-configuration eases deployment of switches in the network by automatically configuring multiple switches across a network using a bootp server. • Autosensing on each port detects the speed of the attached device and automatically configures the port for 10 or 100 Mbps operation, easing the deployment of the switch in mixed-speed environments. • Auto-negotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. This is similar to Cisco EtherChannel and PagP. • Cisco Discovery Protocol versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches.

Feature	Benefit
	• Support for dynamic VLAN assignment through implementation of VLAN Membership Policy Server (VMPS) client functions provides flexibility in assigning ports to VLANs. • Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier network administration and troubleshooting. • The default configuration stored in Flash memory ensures that the switch can be quickly connected to the network and can pass traffic with minimal user intervention.

RODUCT SPECIFICATIONS

Feature	Description
Performance	• 13.6-Gbps switching fabric (Catalyst 2950T-48-SI and 2950SX-48-SI) • 8.8-Gbps switching fabric (Catalyst 2950SX-24, 2950-24, 2950-12) • Cisco Catalyst 2950-12: 2.4 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950-24: 4.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950SX-24: 8.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950T-48: 13.6 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950SX-48: 13.6 Gbps maximum forwarding bandwidth (Forwarding rates based on 64 byte packets) • Cisco Catalyst 2950-12: 1.8 Mpps wire-speed forwarding rate • Cisco Catalyst 2950-24: 3.6 Mpps wire-speed forwarding rate • Cisco Catalyst 2950SX-24: 6.6 Mpps wire-speed forwarding rate • Cisco Catalyst 2950T-48: 10.1 Mpps wire-speed forwarding rate • Cisco Catalyst 2950SX-48: 10.1 Mpps wire-speed forwarding rate • 8 MB packet buffer memory architecture shared by all ports • 16 MB DRAM and 8 MB Flash memory • Configurable up to 8000 MAC addresses

Feature	Description/Part Numbers
Management	• BRIDGE-MIB • CISCO-2900-MIB • CISCO-BULK-FILE-MIB • CISCO-CDP-MIB • CISCO-CLASS-BASED-QOS-MIB • CISCO-CONFIG-COPY-MIB • CISCO-CONFIG-MAN-MIB • CISCO-ENVMON-MIB • CISCO-FLASH-MIB • CISCO-FTP-CLIENT-MIB • CISCO-IMAGE-MIB • CISCO-IPMROUTE-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-MEMORY-POOL-MIB • CISCO-PAGP-MIB • CISCO-PING-MIB

Feature	Description/Part Numbers
	• CISCO-PORT-SECURITY-MIB • CISCO-PROCESS-MIB • CISCO-PRODUCTS-MIB • CISCO-RTTMON-MIB • CISCO-SMI • CISCO-STACKMAKER-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-SYSLOG-MIB • CISCO-TC • CISCO-TCP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • ENTITY-MIB • IANAifType-MIB • IF-MIB (RFC 1573) • OLD-CISCO-CHASSIS-MIB • OLD-CISCO-CPU-MIB • OLD-CISCO-INTERFACES-MIB • OLD-CISCO-IP-MIB • OLD-CISCO-MEMORY-MIB • OLD-CISCO-SYSTEM-MIB • OLD-CISCO-TCP-MIB • OLD-CISCO-TS-MIB • RFC1213-MIB (MIB-II) • RFC1398-MIB (ETHERNET-MIB) • RMON-MIB (RFC 1757) • RS-232-MIB • SNMPv2-MIB • SNMPv2-SMI • SNMPv2-TC • TCP-MIB • UDP-MIB
Standards	• IEEE 802.1x support • IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX ports • IEEE 802.1D Spanning-Tree Protocol • IEEE 802.1p class-of-service (CoS) prioritization • IEEE 802.1Q VLAN • IEEE 802.1s • IEEE 802.1w • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ad

Feature	Description/Part Numbers
Connectors and Cabling	• IEEE 802.3z 1000BASE-X specification • 10BASE-T ports: RJ-45 connectors, two-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling • 100BASE-TX ports: RJ-45 connectors; four-pair Category 5 UTP cabling • 1000BASE-SX ports: MT-RJ connectors, up to 1800 feet (550 meters) cable distance for 50/125 or up to 900 ft (275 m) cable distance for 62.5/125 micron multimode fiber-optic cabling • Management console port: 8-pin RJ-45 connector, RJ-45-to-DB9 adapter cable for PC connections; for terminal connections, use RJ-45-to-DB25 female data-terminal-equipment (DTE) adapter (can be ordered separately, Cisco part number ACS-DSBUASYN=)
MT-RJ Patch Cables for Cisco Catalyst 2950SX 24 Switch	*Type of cable, Cisco part number:* • 1-meter MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-1M • 3-meter MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-3M • 5-meter MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-5M • 1-meter MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-1M • 3-meter MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-3M • 5-meter MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-5M
Power Connectors	Customers can provide power to a switch by using the internal power supply, the Cisco RPS 675 Redundant Power System. The connectors are located at the back of the switch. • Internal power supply connector – The internal power supply is an auto-ranging unit. – The internal power supply supports input voltages between 100 and 240 VAC. – Use the supplied AC power cord to connect the AC power connector to an AC power outlet. • Cisco RPS 675 connector – The connector offers connection for an optional Cisco RPS 675 that uses AC input and supplies DC output to the switch. – The connector offers a 675W redundant power system that supports one of up to six external network devices and provides power to one failed device at a time. – The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. – Attach only the Cisco RPS 675 (Model PWR675-AC-RPS-NI=) to the redundant power supply receptacle with this connector.
Indicators	• Per-port status LEDs: link integrity, disabled, activity, speed, and full-duplex indications • System status LEDs: system, RPS, and bandwidth-utilization indications
Dimensions and Weight (H x W x D)	• 1.72 x 17.5 x 9.52 in. (4.36 x 44.45 x 24.18 cm) (Cisco Catalyst 2950SX-24, 2950-24, 2950-12) • 1.72 x 17.5 x 13 in. (4.36 x 44.45 x 33.02 cm) (Cisco Catalyst 2950SX-48, 2950T-48) • 1 RU high (1.72 in./4.36 cm) • 6.5 lb (3.0 kg) (Cisco Catalyst 2950SX-24, 2950-24, 2950-12) • 10.b lb (4.8 kg) (Cisco Catalyst 2950SX-48, 2950T-48)

Feature	Description/Part Numbers
Environmental Ranges	• Operating temperature: 32 to 113°F (0 to 45°C) • Storage temperature: –13 to 158°F (–25 to 70°C) • Operating relative humidity: 10–85% (non-condensing) • Operating altitude: Up to 10,000 ft (3000 m) • Storage altitude: Up to 15,000 ft (4500 m)
Power Requirements	• Power consumption: 30W (maximum), 102 BTUs per hour (Cisco Catalyst 2950SX-24, 2950-24. 2950-12) • Power consumption: 45W (maximum), 154 BTUs per hour (Cisco Catalyst 2950T-48, 2950SX-48) • AC input voltage: 100 to 127, 200 to 240 VAC (auto-ranging) • AC input frequency: 47 to 63 Hz • DC input voltages for Cisco RPS 675 and Cisco RPS 300: +12V at 4.5A
Acoustic Noise	ISO 7770, bystander position, operating to an ambient temperature of 86°F (30°C): • WS-C2950-24, WS-C2950-12, WS-C2950SX-24: 46 dBa • WS-C2950T-48-SI, WS-C2950SX-48-SI: 48 dBa
Predicted Mean Time Between Failure	• 398,240 hours (Cisco Catalyst 2950-24) • 482,776 hours (Cisco Catalyst 2950-12) • 480,346 hours (Cisco Catalyst 2950SX-24) • 268,876 hours (Cisco Catalyst 2950T-48-SI) • 274,916 hours (Cisco Catalyst 2950SX-48-SI)
Regulatory Agency Approvals	
Safety Certifications	• UL 60950/CSA 22.2 No. 950 • IEC 60950/EN 60950 • AS/NZS 3260, TS001 • CE Marking
Electromagnetic Emissions Certifications	• FCC Part 15 Class A • EN 55022: 1998 (CISPR 22) Class A • EN 55022: 1998 (CISPR 22) • VCCI Class A • AS/NZS 3548 Class A • CE Marking • CNS 13438 Class A • CLEI Code • MIC
Warranty	• Lifetime limited warranty

ERVICE AND SUPPORT

ıe services and support programs described here are available as part of the Cisco Desktop Switching Service and Support solution and are vailable directly from Cisco Systems® and through resellers.

Service and Support	Features	Benefits
Advanced Services		
Total Implementation Solutions (TIS)—Available direct from Cisco Packaged Total Implementation Solutions (Packaged TIS)—Available through resellers	• Project management • Site survey, configuration deployment • Installation, text, and cutover • Training • Major moves, adds, changes • Design review and product staging	• Supplements existing staff • Ensures that functions meet needs • Mitigates risk
Technical Support Services		
Cisco SMARTnet® services and Cisco SMARTnet Onsite services—Available direct from Cisco Packaged Cisco SMARTnet services—Available through resellers	• Around-the-clock access to software updates • Web access to technical repositories • Telephone support through the Technical Assistance Center • Advance replacement of hardware parts	• Enables proactive or expedited issue resolution • Lowers cost of ownership by using Cisco expertise and knowledge • Minimizes network downtime

ORDERING INFORMATION

Model Numbers	Configuration
WS-C2950-12	• 12 10/100 Mbps ports • 1-RU standalone, fixed-configuration, managed 10/100 Mbps switch • Standard Image (SI) Software
WS-C2950-24	• 24 10/100 Mbps ports • 1-RU standalone, fixed-configuration, managed 10/100 Mbps switch • Standard Image (SI) Software
WS-C2950SX-24	• 24 10/100 Mbps ports with two fixed 1000BASE-SX uplinks • 1-RU standalone, fixed-configuration, managed 10/100 Mbps switch • Standard Image (SI) Software
WS-C2950T-48-SI	• 48 10/100 Mbps ports with two fixed 10/100/1000BASE-T uplinks • 1-RU standalone, fixed-configuration, managed 10/100 Mbps switch • Standard Image (SI) Software
WS-C2950SX-48-SI	• 48 10/100 Mbps ports with two fixed 1000BASE-SX uplinks • 1-RU standalone, fixed-configuration, managed 10/100 Mbps switch • Standard Image (SI) Software

OR MORE INFORMATION

or more information about Cisco products, contact:

United States and Canada: 800 553-NETS (6387)
Europe: 32 2 778 4242
Australia: 612 9935 4107
Other: 408 526-7209
World Wide Web: http://www.cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

204108.62_ETMG_MS_12.04

Printed in the USA

Cisco Systems

DATA SHEET

CISCO 1800 SERIES INTEGRATED SERVICES ROUTERS: CISCO 1841 ROUTER (MODULAR)

Cisco Systems® is redefining best-in-class enterprise and small- to-medium-sized business routing with a new line of integrated services routers that are optimized for the secure, wire-speed delivery of concurrent data, voice, and video services. Founded on 20 years of leadership and innovation, the modular Cisco® 1800 Series of integrated services routers (refer to Figure 1) intelligently embed data and security into a single, resilient system for fast, scalable delivery of mission-critical business applications. The best-in-class Cisco 1800 Series architecture has been specifically designed to meet requirements of small–to-medium-sized businesses, small enterprise branch offices, and service provider-managed services applications for delivery of concurrent services at wire-speed performance. The integrated secure systems architecture of the Cisco 1800 Series delivers maximum business agility and investment protection.

PRODUCT OVERVIEW

Cisco 1800 Series integrated services routers are the next evolution of the award-winning Cisco 1700 Series modular access routers. The Cisco 1841 router (Figure 1) is designed for secure data connectivity and provides significant additional value compared to prior generations of Cisco 1700 Series routers by offering more than a fivefold performance increase, integrated hardware-based encryption enabled by an optional Cisco IOS® Software security image, and a dramatic increase in interface card slot performance and density while maintaining support for more than 30 existing WAN interface cards (WICs) and multiflex trunk cards (voice/WICs [VWICs]—for data only on the Cisco 1841 router) of the Cisco 1700 Series.

The Cisco 1841 router features secure, fast, and high-quality delivery of multiple, concurrent services for small-to-medium-sized businesses and small enterprise branch offices. The Cisco 1841 router offers embedded hardware-based encryption enabled by an optional Cisco IOS Software security image; further enhancement of VPN performance with an optional VPN acceleration module; an intrusion prevention system (IPS) and firewall functions; interfaces for a wide range of connectivity requirements, including support for optional integrated switch ports; plus sufficient performance and slot density for future network expansion and advanced applications as well as an integrated real-time clock.

Support of high-density WICs (HWICs) is optional.

Figure 1

Cisco 1800 Series Integrated Services Routers

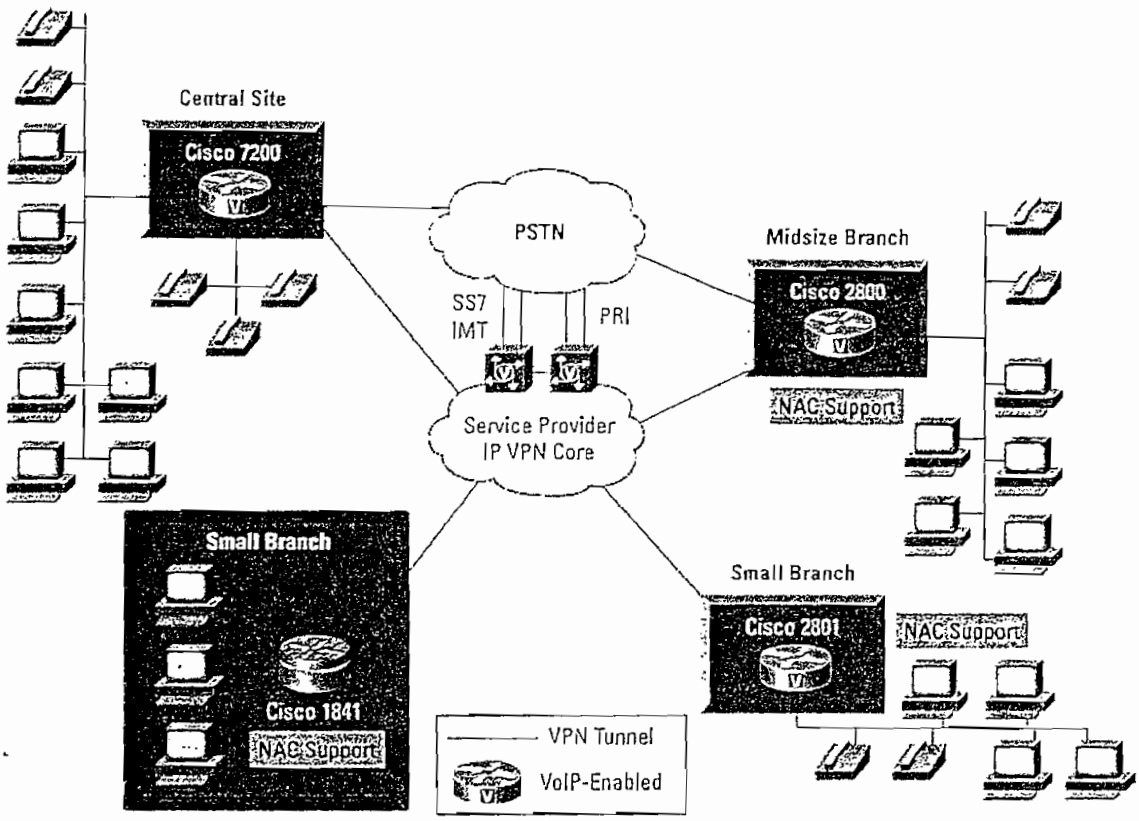
APPLICATIONS

Secure Network Connectivity for Data

Security has become a fundamental building block of any network, and Cisco routers play an important role in embedding security at the customer's access edge. The Cisco IOS Software security feature sets for the Cisco 1841 router that enable the hardware-based encryption on the motherboard provide a robust array of features such as Cisco IOS Firewall, IPS support, IP Security (IPSec) VPNs (Digital Encryption Standard [DES], Triple DES [3DES], and Advanced Encryption Standard [AES]), Dynamic Multipoint VPN (DMVPN), network admissions control (NAC) for antivirus defense, Secure Shell (SSH) Protocol Version 2.0, and Simple Network Management Protocol (SNMP) in one solution set. In addition, the Cisco 1841 router offers bundled network security solutions with a VPN encryption-acceleration module, making it the industry's most robust and adaptable security solution available for small-to-medium-sized businesses and small enterprise branch offices. As Figure 2 demonstrates, the Cisco 1800 Series routers help enable customers to deliver high-performance, concurrent, mission-critical data applications with integrated, end-to-end security.

Figure 2

Secure Network Connectivity with Cisco 1841 Router



Integrated Services

The new, high-performance and secure integrated services architecture of the Cisco 1841 router (as shown in Figure 2) helps enable customers to deploy simultaneous services such as secured data communications with traditional IP routing at wire-speed performance. By offering a hardware-based encryption on the motherboard that can be enabled with an optional Cisco IOS Software security image and the flexibility to integrate a wide array of services, modules, and interface cards, the Cisco 1841 router helps enable businesses to incorporate the functions of a standalone secure data solution.

PRIMARY FEATURES AND BENEFITS

Architecture Features and Benefits

The Cisco 1841 modular architecture has been specifically designed to meet requirements of small-to-medium-sized businesses and small enterprise branch offices as well as service provider-managed applications for concurrent services at wire-speed performance. The Cisco 1841 router, together with other Cisco integrated services routers such as the Cisco 2800 Series, provide the broadest range of secure connectivity options in the industry combined with availability and reliability features. In addition, Cisco IOS Software provides support for a complete suite of transport protocols, quality of service (QoS), and security. Table 1 gives the architecture features and benefits of the Cisco 1841 router.

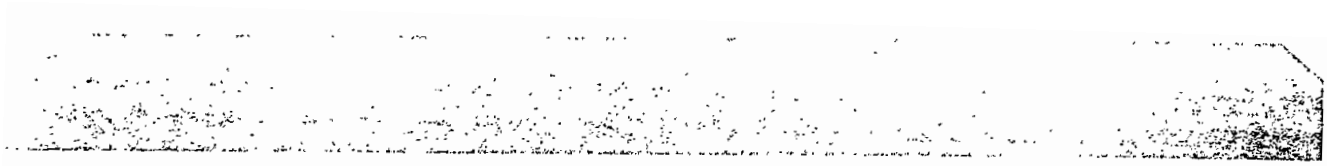


Table 1. Architecture Features and Benefits of Cisco 1841 Router

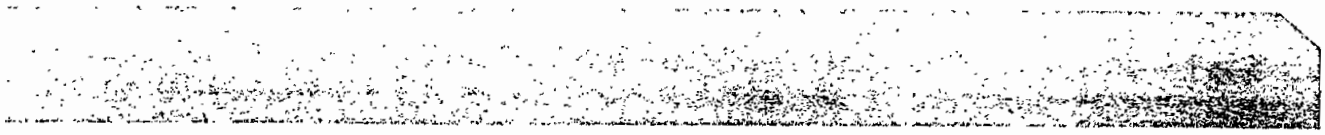
Feature	Benefit
High-performance processor	• Supports concurrent deployment of high-performance, secure data services with headroom for future applications
Modular architecture	• Offers wide variety of LAN and WAN options; network interfaces are field-upgradable to accommodate future technologies
	• Provides many types of slots to add connectivity and services in the future on an "integrate-as-you-grow" basis
	• Supports more than 30 modules and interface cards, including existing WAN (WIC) and multiflex (VWIC) interface cards (for data support only on the Cisco 1841 router) and advanced integration modules (AIMs)
Integrated hardware-based encryption acceleration	• Offers cryptography accelerator as standard integrated hardware that can be enabled with an optional Cisco IOS Software for 3DES and AES encryption support
	• Provides enhanced feature set of security performance through support of optional VPN acceleration card for VPN 3DES or AES encryption
Ample default memory	• Provides 32 MB of Flash and 128 MB of synchronous dynamic RAM (SDRAM) memory to support deployment of concurrent services
Integrated dual high-speed Ethernet LAN ports	• Helps enable connectivity speeds up to 100BASE-T Ethernet technology without the need for cards and modules
	• Allows segmentation of the LAN
Support for Cisco IOS 12.3T feature sets and beyond	• Supports the Cisco 1841 router starting with Cisco IOS Software Release 12.3T
	• Helps enable end-to-end solutions with support for latest Cisco IOS Software-based QoS, bandwidth management, and security features
Integrated standard power supply	• Provides for easier installation and management of the router platform

Modularity Features and Benefits

The Cisco 1841 router provides enhanced modular capabilities while protecting customer investments. The modular architecture has been designed to provide the increased bandwidth and performance required to support concurrent, secure applications. Most existing WICs, multiflex trunk interface cards (for data only), and Advanced Integration Modules (AIMs) are supported in the Cisco 1841. Table 2 lists the modularity features and benefits of the Cisco 1841 router.

Table 2. Modularity Features and Benefits of Cisco 1841 Router

Feature	Benefit
HWIC slots	• The modular architecture on the Cisco 1841 router supports HWIC slots. The newly designed high-speed WAN interface slots significantly increase the data-throughput capability (up to 800-Mbps aggregate). A 4-port High-Speed WAN Interface Card (HWIC-4ESW) is supported on the Cisco 1841.
	• Both slots on the Cisco 1841 router are HWIC slots and provide compatibility with WICs and multiflex trunk (VWICs) interface cards (for data only).
AIM slots (internal)	• The Cisco 1841 router supports hardware-accelerated encryption through an AIM (AIM-VPN/BPII-PLUS).
	• The Cisco 1841 router has one internal AIM slot.



Secure Networking Features and Benefits

The Cisco 1800 Series features a built-in hardware-accelerated encryption on the motherboard that can be enabled with an optional Cisco IOS Software security image. The onboard hardware-based encryption acceleration offloads the encryption processes to provide greater IPSec 3DES and AES throughput. With the integration of optional VPN AIMs, NAC for antivirus defense, and Cisco IOS Software-based firewall and IPS support, Cisco offers the industry's leading robust and adaptable security solution for small to medium-sized businesses and small enterprise branch offices. Table 3 outlines router-integrated security features and benefits.

Table 3. Features and Benefits of Secure Networking

Feature	Benefit
Hardware-based encryption on motherboard	• Support for hardware-based encryption on the Cisco 1841 can be enabled through an optional Cisco IOS Software security image.
AIM-based VPN acceleration	• Support for an optional dedicated VPN AIM can deliver two to three times the performance of embedded encryption capabilities.
NAC	• NAC allows network access only to compliant and trusted endpoint devices for antivirus defense.
IPS support	• Flexible support is provided with Cisco IOS Software. • New intrusion-detection-system (IDS) signatures can be dynamically loaded independent of the Cisco IOS Software release.
Cisco Easy VPN remote and server support	• This feature eases administration and management of point-to-point VPNs by actively pushing new security policies from a single headend to remote sites.
Cisco IOS Firewall, including URL filtering	• URL filtering support is available with optional Cisco IOS Security Software.
Real-time clock support	• Real-time clock support keeps an accurate value of date and time for applications that require an accurate time stamp—such as logging, debugging, and digital certificates.
Cisco Router and Security Device Manager (SDM)	• An intuitive, easy-to-use, Web-based device management tool embedded within the Cisco IOS Software access routers can be accessed remotely for faster and easier deployment of Cisco routers for both WAN access and security features. • Cisco SDM helps resellers and customers to quickly and easily deploy, configure, and monitor a Cisco access router without requiring knowledge of the Cisco IOS Software command-line interface.
USB port (1.1)	• The integrated USB port will be configurable in the future to work with an optional USB token for secure configuration distribution and off-platform storage of VPN credentials.

Cost of Ownership and Ease of Use

The Cisco 1841 router continues the heritage of offering versatility, integration, and power to small-to-medium-sized businesses and small enterprise branch offices. It offers many enhancements to support the deployment of multiple integrated services in the branch office. Key features and benefits that lower the cost of ownership and improve ease of use are outlined in Table 4.

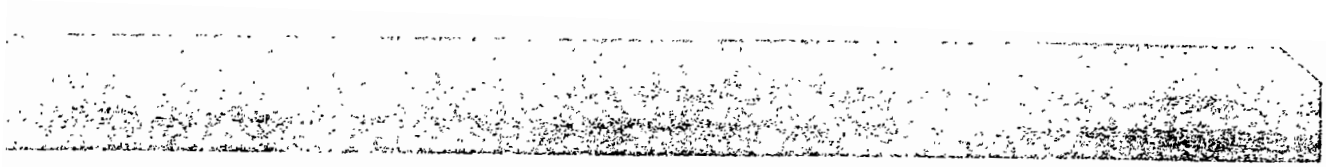


Table 4. Cost of Ownership and Ease of Use—Features and Benefits

Feature	Benefit
Integrated channel service unit (CSU)/data service unit (DSU)	• This feature consolidates typical communications equipment found in branch-office wiring closets into a single, compact unit. This space-saving solution provides better manageability.
USB port (1.1)	• The integrated USB peripheral port is provided to allow future software support for enhanced provisioning and simplified image distribution as well as other functions. These enhancements will aid in reducing support costs and downtime.
Enhanced Setup feature	• An optional setup wizard with context-sensitive questions guides the user through the router configuration process, allowing faster deployment.
CiscoWorks, CiscoWorks VPN/Security Management Solution (VMS) and Cisco IP Solution Center (ISC) support	• Advanced management and configuration capabilities are offered through a Web-based GUI.
Cisco AutoInstall	• This feature configures remote routers automatically across a WAN connection to save the cost of sending technical staff to the remote site.

SUMMARY AND CONCLUSION

As companies increase their security requirements and their need for integrated services, more intelligent office solutions are required. The best-in-class Cisco 1800 Series architecture has been specifically designed to meet these requirements for secure concurrent services at wire-speed performance. The Cisco 1800 Series integrated services routers, consisting of the Cisco 1841 Router, offer the opportunity to consolidate the functions of separate devices into a single, compact solution that can be remotely managed. By providing integrated services, as well as great modular density and high performance, the Cisco 1841 router provides security, versatility, scalability, and flexibility for multiple applications to the small-to-medium-sized office and small enterprise branch office, and the service provider customer edge. The Cisco 1841 router easily accommodates a wide variety of network applications, such as secure branch-office data access including NAC for antivirus defense, VPN access and firewall protection, business-class DSL, IPS support, inter-VLAN routing, and serial device concentration. The Cisco 1841 router provides customers with the industry's most flexible, secure, and adaptable infrastructure to meet both today's and tomorrow's business requirements for maximum investment protection.

SPECIFICATIONS

Table 5 gives product specifications of the Cisco 1841 Router.

Table 5. Product Specifications of Cisco 1841 Router

Cisco 1800 Series	Cisco 1841
Target Applications	Secure data
Chassis	
Form factor	Desktop, 1-rack-unit (1RU) height (4.75 cm high with rubber feet)
Chassis	Metal
Wall-mountable	Yes
Rack-mountable	No
Dimensions (W x D)	13.5 x 10.8 in. (34.3 x 27.4 cm)
	Height without rubber feet: 1.73 in. (4.39 cm)
	Height with rubber feet: 1.87 in. (4.75 cm)

Cisco 1800 Series	Cisco 1841
Weight	Maximum: 6.2 lb (2.8 kg); with interface cards and modules
	Minimum: 6.0 lb (2.7 kg) (no interface cards and modules)
Architecture	
DRAM	Synchronous dual in-line memory module (DIMM) DRAM
DRAM capacity	Default: 128 MB
	Maximum: 384 MB
Flash memory	External compact Flash
Flash memory capacity	Default: 32 MB
	Maximum: 128 MB
Modular slots—total	Two
Modular slots for WAN access	Two
Modular slots for HWICs	Two
Modular slots for voice support	None—The Cisco 1841 does not support voice
Analog and digital voice support	No
VoIP support	Voice-over-IP (VoIP) pass-through only
Onboard Ethernet ports	Two 10/100
Onboard USB ports	One (1.1)
Console port	One–up to 115.2 kbps
Auxiliary port	One–up to 115.2 kbps
Onboard AIM slots	One (internal)
Packet-voice-DSP-module (PVDM) slots on motherboard	None—The Cisco 1841 does not support voice
Integrated hardware-based encryption on motherboard	Yes
Encryption support in software and hardware by default	DES, 3DES, AES 128, AES 192, AES 256
Power Supply Specifications	
Internal power supply	Yes
Redundant power supply	No
DC power support	No
AC input voltage	100 to 240 VAC
Frequency	50 to 60 Hz
AC input current	1.5A maximum
Output power	50W (maximum)
System Power Dissipation	
	153 BTU/hr
Software Support	

Cisco 1800 Series	Cisco 1841
First Cisco IOS Software release	12.3(8)T
Cisco IOS Software default image	IP BASE
Environmental	
Operating temperature	32 to 104°F (0 to 40°C)
Operating humidity	10 to 85% noncondensing operating; 5 to 95% noncondensing, nonoperating
Nonoperating Temperature	-4 to 149°F (-25 to 65°C)
Operating altitude	10,000 feet (3000 meters) @ 77°F (25°C)
Noise level	Normal operating temperature: <78° F/25.6°C : 34 dBA >78°F/25.6°C through <104°F/40°C: 37 dBA >104°F/40°C: 42 dBA
Regulatory Compliance	
Safety	UL60950-1
	CAN/CSA 60950-1
	AS 3260
	EN60950-1
EMI	EN 55022, 1998, class A
	CISPR22, 1997, class A
	CFR47, Part 15, Subpart B, 1995, class A
	EN61000-3-2 Harmonic Current Emission (only for equipment >75W but <16A)
	EN61000-3-3 Voltage Fluctuation and Flicker (only for equipment ≤16A)
Immunity	CISPR24, 1997 ITE-Immunity characteristics, Limits and methods of measurement
	EN 55024,1998 ITE-Immunity characteristics, Limits and methods of measurement
	EN50082-1, 1997 Electromagnetic compatibility—Generic immunity standard, Part 1
	EN 300 386, 1997 Telecommunications network equipment EMC requirements
	The requirements are covered by the following standards:
	IEC 61000-4-2:1995 Immunity to Electrostatic Discharges
	IEC 61000-4-3:1995 Immunity to Radio Frequency Electromagnetic Fields
	IEC 61000-4-4:1995 Immunity to Electrical Fast Transients
	IEC 61000-4-5:1995 Immunity to Power Line Transients (Surges)
	IEC 61000-4-6:1996 Immunity to Radio Frequency Induced Conducted Disturbances
	IEC 61000-4-11:1995 Immunity to Voltage Dips, Voltage Variations, and Short Voltage Interruptions
Network homologation	USA—TIA-968-A, T1.TRQ.6-2001
	Canada—CS-03
	European Union—RTTE Directive 5/99
	Argentina—CTR 21
	Australia—AS/ACIF S002, S003, S016 , S031, 3043

Cisco 1800 Series	Cisco 1841
	Brazil—225-540-788, CTR3, 225-100-717 Edition 3, NET 001/92 1990
	China—ITU-G.992.1, ITU-G.992.1, ITU-G.991.2, CTR3, ITU I.431 1993
	Hong Kong—HKTA 2033, HKTA 2033, HKTA 2014, HKTA 2017 Issue 3 2003, HKTA 2011 Issue 1, HKTA 2011 Issue 2, HKTA 2013 Issue 1
	India—I_DCA_18_02_Jun_99-199, S/ISN-01/02 Issue 1999 S/ISN-02 1 1998, IR/PRI-01/02 Issue 1 1998, S/INT-2W/02 MAY 2001, S/INT-2W/02 MAY 2001
	Israel—U.S. approval accepted
	Japan—Technical condition (DoC acceptance in process)
	Korea—U.S. approval accepted
	Mexico—U.S. approval accepted
	New Zealand—PTC 270/272, CTR 3, ACA 016 Revision 4 1997, PTC 200
	Singapore—IDA TS ADSL1 Issue 1, IDA TS ADSL 2, IDA TS HDSL, IDA TS ISDN 1 Issue 1 1999, IDA TS ISDN 3 Issue 1 1999, IDA TS PSTN 1 Issue 4 , IDA TS PSTN 1 Issue 4, IDA TS PSTN 1 Issue 4
	South Africa—U.S. approval accepted
	Taiwan—U.S. approval accepted

Modular Support

Table 6 gives the modules and interface cards that the Cisco 1841 router supports.

Table 6. Modules and Interface Cards the Cisco 1841 Router Supports

Items	Description	Cisco 1841
Ethernet Switching HWICs		
HWIC-4ESW	4-port single-wide 10/100 BaseT Ethernet switch HWIC	√
Serial WICs		
WIC-1T	1-port serial WIC	√
WIC-2T	2-port serial WIC	√
WIC-2A/S	2-port asynchronous or synchronous serial WIC	√
CSU/DSU WICs		
WIC-1DSU-T1-V2	1-port T1/Fractional-T1 CSU/DSU WIC	√
WIC-1DSU-56K4	1-port 4-wire 56-/64-kbps CSU/DSU WIC	√
ISDN BRI WICs		
WIC-1B-U-V2	1-port ISDN Basic Rate Interface (BRI) with integrated NT1 (U interface)	√
WIC-1B-S/T-V3	1-port ISDN BRI with S/T interface	√
DSL WICs		
WIC-1ADSL	1-port asymmetric DSL (ADSL) over basic-telephone-service WIC	√
WIC-1ADSL-DG	1-port ADSL over basic telephone service with dying-gasp[1] WIC	√
WIC-1ADSL-I-DG	1-port ADSL over ISDN with dying-gasp[1] WIC	√

[1] Feature that provides a signal to indicate that DSL line is down.

Items	Description	Cisco 1841
WIC-1SHDSL	1-port G.shdsl WIC (two wire only)	√
WIC-1SHDSL-V2	1-port G.shdsl WIC (two or four wire)	In first half of 2005
Analog Modem WICs		
WIC-1AM	1-port analog modem WIC	√
WIC-2AM	2-port analog modem WIC	√
T1, E1, and G.703 VWICs		
VWIC-1MFT-T1	1-port RJ-48 multiflex trunk—T1	√ (data only)
VWIC-2MFT-T1	2-port RJ-48 multiflex trunk—T1	√ (data only)
VWIC-2MFT-T1-DI	2-port RJ-48 multiflex trunk—T1 with drop and insert	√ (data only)
VWIC-1MFT-E1	1-port RJ-48 multiflex trunk—E1	√ (data only)
VWIC-1MFT-G703	1-port RJ-48 multiflex trunk—G.703	√ (data only)
VWIC-2MFT-E1	2-port RJ-48 multiflex trunk—E1	√ (data only)
VWIC-2MFT-E1-DI	2-port RJ-48 multiflex trunk—E1 with drop and insert	√ (data only)
VWIC-2MFT-G703	2-port RJ-48 multiflex trunk—G.703	√ (data only)
AIMs		
AIM-VPN/BPII-PLUS	Enhanced-performance DES, 3DES, AES, and compression VPN encryption AIM	√

Table 7 lists the modules and cards not supported on the Cisco 1800 Series.

Table 7. Modules and Cards Not Supported on Cisco 1841 Router

Item	Cisco 1841	Replacement
Data		
WIC-1DSU-T1	No	WIC-1DSU-T1-V2
WIC-1B-S/T	No	WIC-1B-S/T-V3
WIC-1B-U	No	WIC-1B-U-V2
WIC-1ENET	No	None; Cisco 1841 has two integrated Fast Ethernet 10/100BASE-T ports
WIC-4ESW	No	4-port HWICs (Ethernet switching)
WIC-1SHDSL-V2	Planned for Q1 CY '05	Support for WIC-1SHDSL
VPN Module		
MOD1700-VPN	No	AIM-VPN/BPII-PLUS

Availability

The Cisco 1800 Series currently consisting of the Cisco 1841 router will be orderable on September 16, 2004, with first customer shipments expected on September 30, 2004.

ORDERING INFORMATION

To place an order, visit the Cisco Ordering Home Page.

For more information about the Cisco 1800 Series, including Cisco 1700 Series to Cisco 1800 Series migration aids, visit www.cisco.com/go/1800.

Table 8 gives ordering information for the Cisco 1841 Router.

Table 8. Ordering Information for Cisco 1841 Router

Product Number	Product Description
Configurable Base Chassis	
Cisco 1841	Modular router with 2 WAN slots, desktop form factor chassis, IP BASE Cisco IOS Software image, 2 Fast Ethernet slots, 32-MB Flash, and 128-MB DRAM

For Cisco 1841 Security, DSL, and other bundle solutions, contact your Cisco representative or go to www.cisco.com/go/1800.

To download the Cisco IOS Software for the Cisco 1800 Series, visit the Cisco Software Center.

Table 9 gives the Cisco IOS Software images for the Cisco 1841 router.

Table 9. Cisco IOS Software Images for he Cisco 1841 Router

Cisco 1841 Image Name	Images	First Cisco IOS Software Release
Default image: c1841-ipbase	IP BASE	12.3(8)T
c1841-broadband	BROADBAND	12.3(11)T
c1841-advsecurityk9	ADVANCED SECURITY	12.3(8)T
c1841-entbase	ENTERPRISE BASE	12.3(8)T
c1841-entservicesk9-mz	ENTERPRISE SERVICES	12.3(8)T
c1841-advipservicesk9-mz	ADVANCED IP SERVICES	12.3(8)T
c1841-adventerprisek9-mz	ADVANCED ENTERPRISE SERVICES	12.3(8)T
c1841-spservicesk9	SP SERVICES	12.3(8)T

SERVICE AND SUPPORT

Leading-edge technology deserves leading-edge support. Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business.

Cisco SMARTnet® technical support for the Cisco 1800 integrated services routers is available on a one-time or annual contract basis. Support options range from help-desk assistance to proactive, onsite consultation.

All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access rights to Cisco.com technical libraries for technical assistance, electronic commerce, and product information
- Twenty-four-hour-a-day access to the industry's largest dedicated technical support staff

For more information about Cisco Services, refer to Cisco Technical Support Services or Cisco Advanced Services.

FOR MORE INFORMATION

For more information about the Cisco 1800 Series Integrated Services Router, visit www.cisco.com/go/1800 or contact your local account representative.

For more information about Cisco products, contact:

United States and Canada: 800 553-NETS (6387)

Europe: 32 2 778 4242

Australia: 612 9935 4107

Other: 408 526-7209

Web: www.cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

204064_ETMG_EC_08.04

Printed in the USA

CONFIGURACIONES SWITCH NODO PRINCIPAL

NOMBRE DEL SWITCH	MODELO	N° DE PUERTOS	UBICACIÓN	CONTRASEÑA ENABLE SECRET	CONTRASEÑAS ENABLE DE VTY Y DE CONSOLA	DIRECCIÓN IP VLAN1	IP GATEWAY	MASCARA DE SUBRED	NÚMEROS DE VLAN	ASIGNACIÓN DE PUERTOS DEL SWITCH
SwitchNP	Catalyst 2950	24	Nodo Principal	!ecua*	ecua2005	192.168.0.2	192.168.0.1	255.255.255.0	VLAN 1	Fa0/1
									VLAN 2	Fa0/2
									VLAN 3	Fa0/3
									VLAN 4	Fa0/4
									VLAN 5	Fa0/5
									VLAN 6	Fa0/6
									VLAN 7	Fa0/7
									VLAN 8	Fa0/8
									VLAN 9	Fa0/9
									VLAN 10	Fa0/10
									VLAN 23	Fa0/23
									VLAN 24	Fa0/24

CONFIGURACIONES SWITCH NODO 1

NOMBRE DEL SWITCH	MODELO	N° DE PUERTOS	UBICACIÓN	CONTRASEÑA ENABLE SECRET	CONTRASEÑAS ENABLE DE VTY Y DE CONSOLA	DIRECCIÓN IP VLAN1	IP GATEWAY	MASCARA DE SUBRED	NÚMEROS DE VLAN	ASIGNACIÓN DE PUERTOS DEL SWITCH
SwitchN1	Catalyst 2950	24	Nodo 1	!ecua*	ecua2005	192.168.12.2	192.168.12.1	255.255.255.0	VLAN 1	Fa0/1
									VLAN 2	Fa0/2
									VLAN 3	Fa0/3
									VLAN 4	Fa0/4
									VLAN 5	Fa0/5
									VLAN 24	Fa0/24

CONFIGURACIONES SWITCH NODO 2

NOMBRE DEL SWITCH	MODELO	Nº DE PUERTOS	UBICACIÓN	CONTRASEÑA ENABLE SECRET	CONTRASEÑAS ENABLE DE VTY Y DE CONSOLA	DIRECCIÓN IP VLAN1	IP GATEWAY	MASCARA DE SUBRED	NÚMEROS DE VLAN	ASIGNACIÓN DE PUERTOS DEL SWITCH
SwitchN2	Catalyst 2950	24	Nodo 2	lecua*	ecua2005	192.168.18.2	192.168.18.1	255.255.255.0	VLAN 1	Fa0/1
									VLAN 2	Fa0/2
									VLAN 3	Fa0/3
									VLAN 4	Fa0/4
									VLAN 5	Fa0/5
									VLAN 6	Fa0/6
									VLAN 7	Fa0/7
									VLAN 8	Fa0/8

CONFIGURACIONES SWITCH NODO 3

NOMBRE DEL SWITCH	MODELO	Nº DE PUERTOS	UBICACIÓN	CONTRASEÑA ENABLE SECRET	CONTRASEÑAS ENABLE DE VTY Y DE CONSOLA	DIRECCIÓN IP VLAN1	IP GATEWAY	MASCARA DE SUBRED	NÚMEROS DE VLAN	ASIGNACIÓN DE PUERTOS DEL SWITCH
SwitchN3	Catalyst 2950	24	Nodo 3	lecua*	ecua2005	192.168.26.2	192.168.26.1	255.255.255.0	VLAN 1	Fa0/1
									VLAN 2	Fa0/2
									VLAN 3	Fa0/3
									VLAN 4	Fa0/4
									VLAN 5	Fa0/5
									VLAN 6	Fa0/6

CONFIGURACIONES RUTEADOR PRINCIPAL

NOMBRE DEL RUTEADOR	MODELO	UBICACIÓN	CONTRASEÑA ENABLE SECRET	CONTRASEÑAS ENABLE DE VTY Y DE CONSOLA	DIRECCIÓN FASTH ETHERNET 0/0	MASCARA DE SUBRED	SUBINTERFACES	VLAN ASIGNADA	DIRECION IP	MASCARA DE SUBRED	ENCAPSULAMIENTO	ANCHO DE BANDA
RouterP	1841	Nodo Principal	lecua*	ecua2005	216.226.233.14	255.255.255.248	Fa0/1.1	VLAN 1	192.168.0.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.2	VLAN 2	192.168.1.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.3	VLAN 3	192.168.2.1	255.255.255.0	802.1q	128 Kbps
							Fa0/1.4	VLAN 4	192.168.3.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.5	VLAN 5	192.168.4.1	255.255.255.0	802.1q	128Kbps
							Fa0/1.6	VLAN 6	192.168.5.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.7	VLAN 7	192.168.6.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.8	VLAN 8	192.168.7.1	255.255.255.0	802.1q	256 Kbps
							Fa0/1.9	VLAN 9	192.168.8.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.10	VLAN 10	192.168.9.1	255.255.255.0	802.1q	512 Kbps
							Fa0/1.11	VLAN 23	216.226.233.81	255.255.255.252	802.1q	-
							Fa0/1.12	VLAN 24	216.226.233.85	255.255.255.252	802.1q	-

CONFIGURACIONES RUTEADOR NODO 1

NOMBRE DEL RUTEADOR	MODELO	UBICACIÓN	CONTRASEÑA ENABLE SECRET	CONTRASEÑAS ENABLE DE VTY Y DE CONSOLA	DIRECCIÓN FASTH ETHERNET 0/0	MASCARA DE SUBRED	SUBINTERFACES	VLAN ASIGNADA	DIRECION IP	MASCARA DE SUBRED	ENCAPSULAMIENTO	ANCHO DE BANDA
RouterN1	1841	Nodo 1	lecua*	ecua2005	216.226.233.82	255.255.255.252	Fa0/1.1	VLAN 1	192.168.12.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.2	VLAN 2	192.168.13.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.3	VLAN 3	192.168.14.1	255.255.255.0	802.1q	128 Kbps
							Fa0/1.4	VLAN 4	192.168.15.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.5	VLAN 5	192.168.16.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.6	VLAN 24	216.226.233.5	255.255.255.252	802.1q	-

CONFIGURACIONES RUTEADOR NODO 2

NOMBRE DEL RUTEADOR	MODELO	UBICACIÓN	CONTRASEÑA ENABLE SECRET	CONTRASEÑAS ENABLE, DE VTY Y DE CONSOLA	DIRECCIÓN FASTH ETHERNET 0/0	MASCARA DE SUBRED	SUBINTERFACES	VLAN ASIGNADA	DIRECION IP	MASCARA DE SUBRED	ENCAPSULAMIENTO	ANCHO DE BANDA
RouterN2	1841	Nodo 2	!ecua*	ecua2005	216.226.233.86	255.255.255.252	Fa0/1.1	VLAN 1	192.168.18.1	255.255.255.0	802.1q	256 Kbps
							Fa0/1.2	VLAN 2	192.168.19.1	255.255.255.0	802.1q	128 Kbps
							Fa0/1.3	VLAN 3	192.168.20.1	255.255.255.0	802.1q	128 Kbps
							Fa0/1.4	VLAN 4	192.168.21.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.5	VLAN 5	192.168.22.1	255.255.255.0	802.1q	128Kbps
							Fa0/1.6	VLAN 6	192.168.23.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.7	VLAN 7	192.168.24.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.8	VLAN 8	192.168.25.1	255.255.255.0	802.1q	64 Kbps

CONFIGURACIONES RUTEADOR NODO 3

NOMBRE DEL RUTEADOR	MODELO	UBICACIÓN	CONTRASEÑA ENABLE SECRET	CONTRASEÑAS ENABLE, DE VTY Y DE CONSOLA	DIRECCIÓN FASTH ETHERNET 0/0	MASCARA DE SUBRED	SUBINTERFACES	VLAN ASIGNADA	DIRECION IP	MASCARA DE SUBRED	ENCAPSULAMIENTO	ANCHO DE BANDA
RouterN3	1841	Nodo 3	!ecua*	ecua2005	216.226.233.6	255.255.255.252	Fa0/1.1	VLAN 1	192.168.26.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.2	VLAN 2	192.168.27.1	255.255.255.0	802.1q	256 Kbps
							Fa0/1.3	VLAN 3	192.168.28.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.4	VLAN 4	192.168.29.1	255.255.255.0	802.1q	512 Kbps
							Fa0/1.5	VLAN 5	192.168.30.1	255.255.255.0	802.1q	64 Kbps
							Fa0/1.6	VLAN 6	192.168.31.1	255.255.255.0	802.1q	64 Kbps

más significativamente en una dirección en particular antes que en forma uniforme.

AP.- Access Point o punto de acceso.

Asincrónica.- En una Transmisión Asincrónica la información se envía en forma de caracteres para solucionar el problema de sincronización entre el Tx y Rx. El receptor tiene la oportunidad de re-sincronizarse al inicio de cada nuevo carácter el cual se delimita mediante el uso de bits de inicio y parada.

ATM.- Asynchrony Transfer Modo o Modo de Transferencia Asincrónico.

Backbone.- El backbone es una línea de gran capacidad a la que se conectan otras líneas de menor capacidad a través de puntos de conexión llamados nodos. La traducción literal es "columna vertebral" o "espina dorsal".

Bridging.- Consiste en interconectar dos puntos distantes mediante dispositivos inalámbricos.

Broadcast.- Las tramas tipo broadcast son aquellas que están destinadas a todas las estaciones de una red.

BSS.- Basic Service Set o Conjunto de Servicio Básico.

CAR.- CAR (Committed Access Rate), es una característica presente en los dispositivos de capa 3 de Cisco Systems. En los ruteadores se encuentra a partir de las series 1000.

CBC-MAC.- Cipher Block Chaining Message Authentication Code, es un método de autenticación que se utiliza en el estándar IEEE 802.11i.

CCK .- Complementary Code Keying.

CCMP.- Counter-Model/CBC-MAC Protocol, es un protocolo de confidencialidad de datos que maneja autenticación de paquetes y cifrado.

CF.- Contention Free o Libre de Contención.

Core.- Las redes de core permiten la interconectividad a nivel regional por lo cual deben ser muy rápidas, muy estables, capaces de manejar inmensas cantidades de tráfico, y con un alto índice de disponibilidad y confiabilidad.

CP.- Contention Period o Periodo de Contención.

CRC.- Cyclic Redundancy Check o Control de Redundancia Cíclica.

CSMA/CA.- Carrier Sense Multiple Access with Collision Avoidance o Acceso Múltiple por Detección de Portadora con Evasión de Colisiones.

CSMA/CD.- Carrier Sense Multiple Access with Collision Detection o Acceso Múltiple por Detección de Portadora con Detección de Colisiones.

CTS.- Clear to Send, es una señal que da autorización al módem para transmitir.

Datagrama.- Es un paquete individual de datos que es enviado al computador receptor sin ninguna información que lo relacione con ningún otro posible paquete enviado.

DBPSK. - Differential Binary Phase Shift Keying.

DCF.- Distributed Coordination Function o Función de Coordinación Distribuida.

DES.- DES (Data Encryption Standard; Estándar de Encriptación de Datos), es un estándar prototipo para el cifrado de bloque (es decir genera n-palabras en lugar de letras), que toma un texto sin cifrar y lo transforma en un texto cifrado de la misma longitud. El tamaño de bloque de DES es de 64 bits y hace uso de una

clave criptográfica de 64 bits para cifrado y descifrado de datos.

DHCP.- Dynamic Host Configuration Protocol o Protocolo de Configuración Dinámica de Host, es un protocolo de red que permite que un servidor provea los parámetros de configuración a todas las computadoras conectadas a la red.

Dial Backup.- Es una topología dispersa complementada con un circuito de respaldo dial o dial backup.

DIFS.- Espaciado entre Tramas DCF.

DMZ.- Una DMZ (Demilitarized Zone; Zona Desmilitarizada), es una área de una red de computadoras que está entre la red LAN de una organización y una red exterior, generalmente la Internet. La zona desmilitarizada permite que servidores interiores (Servidores Web, Servidores FTP, Servidores de Mail y Servidores DNS), provean servicios a la red exterior, mientras protege la red interior de intromisiones.

DNS.- Domain Name Service o Servicio de Nombres de Dominio, es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y viceversa.

DQPSK.- Differential Quadrature Phase Shift Keying.

DSLAM.- Digital Subscriber Line Access Multiplexer, es el encargado de terminar las conexiones ADSL de un nivel físico de múltiples usuarios y conmutar las celdas ATM.

DSSS.- Espectro Expandido por Secuencia Directa es un técnica de espectro expandido de fácil aplicación y de alta velocidad de transmisión.

EAP.- Extensible Authentication Protocol o Protocolo de Autenticación Extensible, es un protocolo para autenticación que soporta múltiples métodos de autenticación como MD5, Kerberos, OneTime Paswword, etc.

EIFS.- Espaciado entre Tramas Extendido.

ESS.- Extended Service Set o Conjunto de Servicio Extendido.

ETSI.- European Telecommunications Standards Institute, es una organización sin fines de lucro cuya misión es producir los Estándares de Telecomunicaciones que serán usados por toda Europa.

FCC.- La FCC (Federal Communications Commission; Comisión Federal de Comunicaciones), es una agencia gubernamental independiente de los Estados Unidos. Esta agencia elabora las leyes dentro de las cuales los dispositivos WLAN deben operar.

FCS.- Frame Check Sequence o Secuencia de Chequeo de Trama.

FHSS.- Espectro Expandido por Salto de Frecuencia es una técnica de espectro expandido que utiliza saltos de frecuencia para expandir los datos sobre un ancho de banda superior a los 83MHz.

Firewall.- Es un componente o conjunto de componentes que restringen el acceso entre una red interna protegida y cualquier otra red, comúnmente Internet.

Firmware.- El firmware es un programa que se graba dentro de los circuitos electrónicos del equipo o en su memoria ROM y que no puede ser modificado por el usuario a menos que se realice una actualización.

FTP.- File Transfer Protocol o Protocolo de Transferencia de Archivos, es un servicio que se utiliza en Internet y en otras redes para transmitir archivos desde servidores o entre un usuario y un servidor.

FTT.- Fast Fourier Transformation o Transformada Rápida de Fourier.

GPS.- Es un dispositivo que permite determinar la posición geográfica en

cualquier lugar del planeta, mediante el uso del sistema GPS (Global Positioning System; Sistema de Posicionamiento Global), que es un sistema compuesto por una red de 24 satélites denominada NAVSTAR.

Hacker.- Se denomina hacker a cualquier persona experta en varias o algunas ramas relacionadas con la computación y las telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red, voz, etc., que busca defectos y puertas traseras en cualquier tipo de sistema ya sea con fines maliciosos o no.

HFC.- Híbrida Fibra Óptica-Coaxial, es una red de telecomunicaciones bidireccional por cable que combina la fibra óptica y el cable coaxial como soporte de transmisión de las señales.

Hipermedia.- Es la integración de gráficos, sonido y vídeo en un sistema que permite el almacenamiento y recuperación de la información de manera relacionada, por medio de referencias cruzadas.

Host.- Son los computadores cliente/servidor.

Hotspot.- Es una localidad geográfica específica en la cual un punto de acceso provee servicios de red inalámbrica banda ancha.

HTML.- Hypertext Markup Language.

HTTP.- Hypertext Transfer Protocol, es el encargado de hacer llegar las diferentes páginas desde los servidores remotos al equipo del usuario que lo solicita.

IBSS.- Independent Basic Service Set o Conjunto de Servicio Básico Independiente.

ICV.- Integrity Check Value es un código de integridad que se calcula mediante el algoritmo CRC-32 dentro de WEP.

IEEE.- Institute of Electrical and Electronic Engineers o Instituto de Ingenieros Eléctricos y Electrónicos.

IFS.- Interframe Space o Espaciado entre Tramas.

IFTT.- Inverse Fast Fourier Transformation o Transformación Inversa Rápida de Fourier.

IMAP4.- Internet Message Access Protocol version 4 o Protocolo de Mensajes de Internet.

IPSec.- El protocolo IPSec (Internet Protocol Security; Protocolo de Seguridad de Internet), es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y cifrado, y de esta manera asegurar las comunicaciones a través de dicho protocolo. IPsec ha sido desarrollado ampliamente para implementar Redes Privadas Virtuales (VPNs).

IPX.- IPX (Internetwork Packet Exchange; Intercambio de Paquetes en Red Interna), es un protocolo de red no orientado a la conexión utilizado por el sistema operativo Novell Netware.

IRC.- Internet Relay Chat, es un servicio que permite intercambiar mensajes por escrito en tiempo real entre usuarios que estén simultáneamente conectados a la red.

ISDN.- Integrate Service Digital Network o Red Digital de Servicios Integrados.

ISL.- Inter-Switch es un protocolo propietario de Cisco para el etiquetado de tramas en una VLAN.

ISM.- Banda libre para uso de la Industria, la ciencia y la medicina.

ISP.- Internet Service Provider o Proveedor de Servicio de Internet, es una

empresa que permite el acceso de otras empresas o personas al Internet, ofreciendo servicios de Internet y conectividad.

IV.- Initialization Vector o Vector de Inicialización.

Jamming.- Es una técnica de ataques a redes WLAN usada simplemente para detener a las redes inalámbricas.

L2TP.- El protocolo L2TP (Layer 2 Tunneling Protocol; Protocolo de creación de Túneles de Capa 2), como su nombre lo indica, es un protocolo para la creación de túneles de tráfico entre dos entidades sobre una red existente, soportando VPNs a nivel de la capa de enlace (capa 2 del modelo OSI).

LAN.- Local Area Network o Red de Área Local.

LLC.- Logical Link Control.

MAC.- Medium Access Control o Control de Acceso al Medio.

Main-in-the-middle.- Es una situación en la cual un individuo malicioso usa un punto de acceso para secuestrar nodos móviles.

MDI.- MDI (Medium Dependent Interface), es un tipo de conexión a un puerto Ethernet que permite a dispositivos de red conectarse a otros mediante el uso de un cable directo.

MDIX.- MDIX (Medium Dependent Interface Crossover), es un tipo de conexión a un puerto Ethernet que permite a dispositivos de red conectarse a otros mediante el uso de un cable cruzado o null-modem.

MIB.- Management Information Base o Base de Información para la Administración.

MIC.- Message Integrity Check o Chequeo de Integridad de Mensaje, es un mecanismo de TKIP para ayudar a determinar si un usuario no autorizado ha modificado los paquetes luego de la transmisión.

MPDU.- MAC Sublayer Protocol Data Units o Unidades de Datos del Protocolo de la Subcapa MAC.

MSDU.- MAC Service Data Unit o Unidad de Datos de Servicios MAC

Multicast.- Las tramas tipo multicast son aquellas que están destinadas únicamente a un grupo de estaciones.

NAP.- Network Access Point o Punto de Acceso a la Red, es un punto de intercambio de tráfico local al cual se conectan todos los ISPs locales para intercambiar tráfico entre ellos sin hacer uso de enlaces internacionales. Su finalidad es ahorrar costes en transito internacional, mejorar retardos, perdidas de paquetes, etc.

NAT.- El NAT (Network Address Translation; Traducción de la Dirección de Red), es una aplicación por la que determinado dispositivo o aplicación de software es capaz de cambiar la dirección IP de origen o destino por otra dirección definida previamente. Se puede utilizar para dar salida a redes públicas a computadores que se encuentran con direccionamiento privado o para proteger máquinas públicas.

NAV.- Network Allocation Vector o Vector de Asignación de la Red.

NetBIOS.- NetBIOS (Network Basic Input Output System; Sistema de Red Básico de Entrada y Salida), es un protocolo de red originalmente creado para redes LAN con computadoras IBM.

NIC.- Network Interface Card o Tarjeta de Interfaz de Red.

NNTP.- Network News Transfer Protocol o Protocolo de Transferencia de Noticias de Red, es el encargado de enviar, distribuir y recuperar mensajes de un servidor de Noticias USENET.

NVRAM.- Non Volatile Random Memory Access o Memoria no Volátil de Acceso Ramdómico.

OFDM.- Orthogonal Frequency Division Multiplexing o Multiplexación por División de Frecuencia Ortogonal.

Omni-direccional.- El término conectividad omni-direccional significa conectividad uniforme en todas las direcciones.

OSI.- Open System Interconnection o Sistema de Interconexión abierto.

PCF.- Point Coordination Function o Función de Coordinación Puntual.

PCI.- Peripheral Component Interconnect o Conector de Componentes Periféricos.

PCMCIA.- Las ranuras PCMCIA (Personal Computer Memory Card International Association; Asociación Internacional de Tarjetas de Memoria para Computadores Personales), permiten alojar tarjetas PCMCIA que pueden ser módems, adaptadores de red, memorias, etc.

PIFS.- Espaciado entre Tramas PCF.

Pigtail.- Es un cable pequeño que sirve para adaptar la tarjeta de red inalámbrica, un punto de acceso y la antena o el cable que vaya hacia la antena.

PLCP.- Physical Layer Convergence Procedure o Procedimiento de Convergencia de la Capa Física.

PMD.- Sistema Dependiente del Medio Físico.

PoP.- Los puntos de presencia o PoPs son la misma red de la oficina central de un ISP que se ha extendido debido a la demanda de usuarios.

POP3.- Post Office Protocol version 3.

PPP.- El protocolo PPP (Point to Point Protocol; Protocolo Punto a Punto), es un protocolo que se usa en redes punto a punto el cual se encuentra definido en el RFC-2284. Permite multiplexar diferentes protocolos de capa de red y admitir diferentes protocolos de autenticación para establecer medidas de control de acceso y así proteger a la red de usuarios no autorizados.

PPTP.- PPTP (Point-to-Point Tunneling Protocol; Protocolo de Creación de Túneles Punto a Punto), es una nueva tecnología para implementar Redes Privadas Virtuales (VPNs). Esta tecnología es usada para garantizar que los mensajes transmitidos de un nodo VPN a otro sean seguros.

PRNG.- Pseudo Random Number Generator o Generador de Números Seudo Aleatorios.

PSK.- Preshared Key o Modo Personal, es un modo de operación de WPA2 para redes caseras y redes SOHO en las cuales no se dispone de un servidor de autenticación.

PSTN.- Public Switched Telephone Network o Red Telefónica Pública Conmutada.

PVC.- Permanent Virtual Connection o Conexión Permanente Virtual.

RADIUS.- RADIUS (Remote Access Dial-In User Server), es un servidor que presta los servicios de autenticación, autorización y contabilidad para aplicaciones de acceso a la red o movilidad.

Redes.- Son grupo de computadores y dispositivos asociados que permiten a los usuarios transferencia electrónica de información.

Roaming.- Significa moverse físicamente de un área de cobertura inalámbrica a otra, sin que se produzca una perdida de la conectividad.

RTS.- Request to Send, es una petición de permiso para transmitir.

SAP.- Service Access Point o Punto de Acceso de Servicio.

SIFS.- Espaciado Corto entre Tramas.

Sincrónica.- En la Transmisión Sincrónica la información se transmite como caracteres uno tras de otro de una manera secuencial y sin pausas entre caracteres. Los caracteres a ser transmitidos no incluyen bits de inicio ni de parada, pero en su lugar la sincronización es provista o bien usando caracteres de sincronismo o bien usando señales de reloj, prefiriéndose la primera alternativa.

SMTP.- Simple Mail Transfer Protocol o Protocolo Simple de Transferencia de Correo.

Sniffer.- Un Sniffer (también conocido como Analizadores de Redes), son herramientas de software que permiten capturar paquetes que viajan a través de una red para decodificarlos y poder observar su contenido.

SNMP.- SNMP (Simple Network Management Protocol; Protocolo Simple de Gestión de Redes), es aquel que permite la gestión remota de dispositivos de red, tales como switches, ruteadores y servidores.

SOHO.- Small Office/Home Office.

Spread Spectrum.- Espectro Extendido, es una técnica de comunicación que se caracteriza por utilizar un gran ancho de banda para reducir la probabilidad de

que los datos sean corrompidos y una baja potencia de transmisión.

SSID.- El SSID (Service Set Identifier; Identificador de Conjunto de Servicio), es un conjunto de 32 caracteres el cual se programa dentro de cada punto de acceso y debe ser conocido por el usuario para poder asociarse con éste.

SWAP.- Shared Wireless Access Protocol.

TCP/IP.- TCP/IP (Transmission Control Protocol/Internet Protocol; Protocolo de Control de Transmisión/Protocolo de Internet), es un conjunto de protocolos de comunicaciones que definen cómo se pueden comunicar entre sí computadores y otros dispositivos de distinto tipo.

TELCO.- Compañía de Telecomunicaciones.

Telnet.- Es un protocolo de comunicaciones que permite al usuario de un computador con conexión a Internet establecer una sesión como terminal remoto de otro sistema de la red.

TKIP.- Temporal Key Integrity Protocol o Protocolo de Integridad de Clave Temporal, es un protocolo diseñado para mejorar las deficiencias del algoritmo WEP especialmente el reuso de las claves de encriptación.

Triple DES.- El Triple DES (3DES), es un esquema que resuelve el problema de corta longitud de la clave criptográfica en DES, para lo cual hace uso de tres iteraciones sucesivas del algoritmo DES con lo que se consigue una longitud de clave de 128 bits, la cual es compatible con DES.

Unicast.- Las tramas tipo unicast son aquellas destinadas únicamente a una estación.

UNII.- Unlicensed National Information Infrastructure.

Uptime.- El uptime, es el tiempo en el que un servicio se encuentra disponible sin ningún tipo de interrupción o degradación.

URL.- Universal Resource Locator o Localizador Universal de Recursos, es un método de identificación de documentos o lugares en Internet. Básicamente es una cadena de caracteres que identifica el tipo de documento, el host, la ruta de acceso y su nombre.

USB.- Universal Serial Bus o Bus de Serie Universal, son adaptadores usados en dispositivos con puertos USB para conectarlos en una red WLAN.

USENET.- Es un grupo de noticias que son clasificados dentro de jerarquías de similar interés en su contenido y a su vez se dividen en subjerarquías.

VLAN.- Una VLAN (Virtual Local Area Network; Red de Área Local Virtual) es una tecnología que se utiliza para crear redes virtuales las cuales permitan conectar computadores o dispositivos de red entre sí, a pesar de que físicamente se encuentren en diversos segmentos de una red.

VPN.- Virtual Private Networks o Red Privada Virtual.

WAN.- Wide Area Network o Red de Área Extendida.

Warchalking.- Es un método de detección de redes WLAN las cuales son marcadas por símbolos en los alrededores de la misma.

Wardriving.- Es un método de detección de redes WLAN con el fin de ubicar a las mismas en mapas.

Web Hosting.- Consiste en proveer al cliente un espacio para alvergar sus paginas web en un servidor denominado web host para su posterior publicación en la WWW.

WECA.- Wireless Ethernet Compatibility Alliance.

WEP.- Wired Equivalent Privacy o Privacidad Equivalente a una Cableada, es un algoritmo de encriptación que utiliza un proceso de clave compartida.

Wi-Fi.- Wireless Fidelity, es una asociación internacional creada para certificar la interoperabilidad de los productos WLAN basados en la especificación IEEE 802.11.

WISP.- Wireless Internet Service Providers o Proveedores de Servicio de Internet Inalámbrico.

WLAN.- Wireless Local Area Network o Red Inalámbrica de Área Local.

WLANA.- Wireless LAN Association, es una asociación de comercio educativa sin fines de lucro conformada por líderes e innovadores de la industria de la tecnología WLAN.

WLIF.- Wireless LAN Interoperatibility Forum.

WPA.- Wi-Fi Protected Access o Acceso Protegido para Wi-Fi, es una especificación propuesta por los miembros de la alianza Wi-Fi para incrementar los niveles de protección de datos y control de acceso de las actuales y futuras redes Wi-Fi.

WPA2.- Wi-Fi Protected Access 2 o Acceso Protegido para Wi-Fi 2, es la última generación en estándares de seguridad de la alianza Wi-Fi.

WPAN.- Wireless Personal Area Network o Red Inalámbrica de Área Personal

WWW.- World Wide Web, es un mecanismo proveedor de información electrónica para usuarios conectados a Internet.