DISEÑO DE UNA RED WIRELESS PARA PROVEER SERVICIOS DE INTERNET (WISP) BASADA EN OPEN SOURCE PARA CONECTIVIDAD DE USUARIOS EMPRESARIALES, RESIDENCIALES Y RURALES DE SAN VICENTE DE CHUCURÍ

PEDRO ALBERTO ARIAS QUINTERO
MARIO GÓMEZ MORENO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESPECIALIZACIÓN EN TELECOMUNICACIONES
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2.010

DISEÑO DE UNA RED WIRELESS PARA PROVEER SERVICIOS DE INTERNET (WISP) BASADA EN OPEN SOURCE PARA CONECTIVIDAD DE USUARIOS EMPRESARIALES, RESIDENCIALES Y RURALES DE SAN VICENTE DE CHUCURÍ

PEDRO ALBERTO ARIAS QUINTERO
MARIO GÓMEZ MORENO

Monografía para optar al título de Especialista en Telecomunicaciones

Director
ING. FREDDY ALFONSO BELTRAN MIRANDA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESPECIALIZACIÓN EN TELECOMUNICACIONES
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2.010

DEDICATORIAS

Dedico este trabajo a Dios y a la Virgen por permitirme alcanzar este gran triunfo, a mi papá Arturo que desde el cielo me acompaña, a mi mamá Mercedes por su incondicional apoyo, a mi esposa Yuleny y a mi hijo Juan David que son mi gran inspiración y a quienes les debo mucho por su apoyo y dedicación, su fortaleza y sostén en todos los momentos difíciles no solo de este proyecto sino de mi vida familiar, a mis hermanos que me ayudan y apoyan incondicionalmente. Así como a mis estudiantes, en especial a mis niñas de quienes fui director de grupo y que de una u otra forma me ven como su punto de referencia, A todos ellos les dedico este triunfo para que lo hagan como suyo.

Pedro Arias Quintero

Dedico el presente Proyecto de vida a Dios, a los seres que más amo en este mundo: mi esposa, Mayra Alejandra Moreno Gutiérrez y mis hijos, María Camila Gómez Moreno y Carlos Mario Gómez Moreno, por ser la fuente de mi inspiración y motivación para superarme cada día más y así poder luchar para que la vida nos depare un futuro mejor.

Mario Gómez Moreno

AGRADECIMIENTOS

Agradezco a Dios y a la Virgen mi constancia y sabiduría para alcanzar cualquier reto; a mi familia Mama, papá y hermanos que siempre creen en mí, Gracias por corregirme y hacer de mi un gran hijo y hermano, gracias; a mi esposa Yuleny e Hijo por aconsejarme siempre, por tener paciencia los días de desvelo y por cosas del estudio las llegadas tarde y no verme en casa, gracias por su comprensión, les digo que son mi inspiración y mi fuente de energía, agradecerles a mis estudiante especialmente a mis niñas por su apoyo y alegría que son muy importantes en cada momento, decirles que siempre las llevo conmigo donde estén. Gracias a todos los que me ayudaron técnica mente en este proyecto, a la UIS y sus docentes, al ingeniero Freddy por su valiosa ayuda como asesor y al señor Héctor Ramírez por dedicarnos tiempo y apoyo logístico en pruebas de campo.

Pedro Arias Quintero

A Dios, por llevarme a su lado a lo largo de esta vida siempre llenándome de alegría y triunfos, a ti papá, que me enseñaste todo el valor y toda la fuerza en un solo abrazo, a mi mamá, que dentro de todas sus preocupaciones me dio la posibilidad de brillar. A mí amada Esposa y mis hijos, porque su amor y tus alegrías va más allá de un simple apoyo y compañía, porque cada uno de ustedes son la palabra de aliento y alegría que he necesitado, a mi Suegro y mi Suegra por ese apoyo incondicional, y así obtener un nuevo triunfo.

Al Ing. Fredy A. Beltrán Miranda, por cada una de esos concejos que compartimos opiniones y sentí el interés en cada una de la palabras escritas en este documento, mi Monografía.

Mario Gómez Moreno

CONTENIDO

LISTA DE IMAGENES

LISTA DE TABLAS

GLOSARIO

802.11 : 802.11, o IEEE 802.11, es un grupo de trabajo del IEEE que desarrolla distintos estándares para el uso de la tecnología de radiofrecuencia en las redes de área local (LAN). 802.11 se compone de distintas normas que operan a diferentes frecuencias, con distintas velocidades y capacidades.

Access Point (AP, Punto de Acceso): Estación base o "base station" que conecta una red cableada con uno o más dispositivos wireless.

Existen muchos tipos de Access Point en el mercado, con diferentes capacidades: bridge, hubs, gateway, router, y las diferencias entre ellos muchas veces no están claras, porque las características de uno se pueden incluir en otro. Por ejemplo, un router puede hacer bridge, y un hub puede hacer switch.Además, los Access Points pueden mejorar las características de la WLAN, permitiendo a un cliente realizar roaming entre distintos AP de la misma red, o compartiendo una conexión a Internet entre los clientes wireless.

Ancho de banda (Bandwidth): Fragmento del espectro radioeléctrico que ocupa toda señal de información.

Ad-Hoc, modo: Un tipo de topología de WLAN en la que sólo existen dispositivos clientes, sin la participación de ningún Access Point, de forma que los clientes se comunican de forma independiente punto a punto, peer-to-peer.

Dado que no existe un dispositivo central, las señales pueden ocasionar mayores interferencias reduciendo las prestaciones de la red.

Autentificación: Proceso de identificación de un equipo o usuario. El estándard 802.11 define dos métodos de autentificación: open system y shared key.

Bluetooth: Tecnología desarrollada para la interconexión de portátiles, PDAs, teléfonos móviles y similares a corta distancia (menos de 10 metros) con una velocidad máxima de 11Mbps a la frecuencia ISM de 2'4 GHz.

Bridge: Dispositivo que conecta dos segmentos de red que emplean el mismo protocolo de red (por ejemplo, IP) pero con distintos medios físicos (por ejemplo, 802.11 y 10baseT).

BSSID, Basic Service Set Identification: Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo Ad-Hoc.

Clave de encriptación: Conjunto de caracteres que se utilizan para encriptar y desencriptar la información que se quiere mantener en privado. El tipo de clave y la forma de emplearla depende del algoritmo de encriptación que se utilice.

Cliente, o dispositivo cliente: Cualquier equipo conectado a una red y que solicita servicios (ficheros, impresión, etc) de otro miembro de la red.
En el caso de las WLAN, se suele emplear para referirse a los adaptadores que proporcionan conectividad a través de la red inalámbrica, como tarjetas PCMCIA, PCI o USB, que permiten al equipo acceder a la red.

Decibelios, Db: Unidad logarítmica empleada habitualmente para la medida de potencias. Se calcula multiplicando por diez el resultado del logaritmo en base 10 de la potencia (en watios): $10 * \log_{10} (W)$. También puede usarse como medida relativa de ganancia o pérdida de potencia entre dos dispositivos.

Decibelios isotrópicos, dBi: Valor relativo, en decibelios, de la ganancia de una antena respecto a la antena isotrópica. Cuanto mayor sea este valor, más directividad tiene la antena y más cerrado será su ángulo de emisión.

DHCP, Dynamic Host Configuration Protocol: Protocolo para la configuración automática de los parámetros de red de los equipos. La información se almacena en un servidor DHCP al que los equipos, al encenderse, solicitan los parámetros de configuración.

Dipolo, antena: Antena de baja ganancia (2.2 dBi) compuesta por dos elementos, normalmente internos, cuyo tamaño total es la mitad de la longitud de onde de la señal que trata.

Directividad: Capacidad de una antena para concentrar la emisión en una determinada región del espacio. Cuanta más directiva sea la antena, se obtiene un mayor alcance a costa de un área de menor cobertura.

DSSS, Direct Sequence Spread Spectrum: Técnica de transmisión de la señal para paliar los efectos de las interferencias, que se basa en el uso de bits de redundancia.

Espectro radioeléctrico: El espectro radioeléctrico es toda la escala de frecuencias de las ondas electromagnéticas. Considerado como un dominio de uso público, su división y utilización esta regularizado internacionalmente.

ESSID, Extended Service Set Identification: Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo infraestructura.

Ethernet: Ethernet es el nombre común del estándard IEEE 802.3, que define las redes locales con cable coaxial o par trenzado de cobre.
Existen distintas versiones, desde la original 10Base5 (cable coaxial con 10 Mbps hasta 500 metros), pasando por la 10Base2 (coaxial, 10Mbps, 200m), 10BaseT (par trenzado, 10 Mbps, 100m) y 100BaseT (trenzado, 100Mbps, 100m) conocida como Fast Ethernet, el más utilizado hoy en día en redes locales.

FHSS, Frequency Hopping Spread Spectrum: Técnica de transmisión de la señal para paliar los efectos de las interferencias, que se basa en cambios sincronizados entre emisor y receptor de la frecuencia empleada.

Firewall: Sistema de seguridad que previene el acceso no autorizado a la red, restringiendo la información que entra o sale de la red. Puede ser un equipo específico o un software instalado en una máquina de uso general.

Gateway: Dispositivo que conecta a distintas redes entre sí, gestionando la información entre ellas.

Hot Spot: También conocidos como lugares de acceso público, un Hot Spot es un lugar donde se puede acceder a una red wireless pública, ya sea gratuita o de pago. Pueden estar en cyber-cafes, aeropuertos, centros de convenciones, hoteles, y otros lugares de encuentro, para proporcionar acceso a su red o a Internet a los visitantes o invitados.

Hub: Dispositivo de red multipuerto para la interconexión de equipos via Eterhnet o wireless. Los concentradores mediante cables alcanzan mayores velocidades que los concentradores wireless (Access Points), pero éstos suelen dar cobertura a un mayor número de clientes que los primeros.

Hz, Hertzios: Unidad internacional para la frecuencia, equivalente a un ciclo por segundo. Un megahertzio (MHz) es un millón de hertzios; un gigahertzio (GHz) son mil millones de hertzios.

IEEE, Institute of Electrical and Electronics Engineers (http://www.ieee.org): Organización formada por ingenieros, científicos y estudiantes involucrados en el desarrollo de estándares para, entre otros campos, las comunicaciones.

Este organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas. Así, el subgrupo 802 se encarga de las redes LAN y WAN, y cuenta con la subsección 802.11 para las redes WLAN.

IP, dirección: Un número de 32 bits que identifica a un equipo a nivel de protocolo de red en el modelo ISO. Se compone de dos partes: la dirección de red, común a todos los equipos de la red, y la dirección del equipo, única en dicha red.

ISO, modelo de red: La ISO, International Standards Organization (http://www.iso.org), desarrolló un modelo para describir a las entidades que participan en una red. Este modelo, denominado Open System Interconnection (OSI), se divide en 7 capas o niveles, que son: Físico, Enlace, Red, Transporte, Sesión, Presentación, Aplicación.

Con esta normalización de niveles y sus interfaces de comunicación, se puede modificar un nivel sin alterar el resto de capas. El protocolo 802.11 tiene dos partes, una denominada PHY que abarca el nivel físico, y otra llamada MAC, que se corresponde con la parte inferior del segundo nivel del modelo OSI.

Isotrópica, antena: Modelo teórico de antena consistente en un único punto del espacio que emite homogéneamente en todas las direcciones. Se utiliza como modelo de referencia para el resto de las antenas.

MAC (Media Access Control), dirección: En las redes wireless, el MAC es un protocolo de radiofrecuencia, corresponde al nivel de enlace (nivel 2) en el modelo ISO. Cada dispositivo wireless posee una dirección para este protocolo, denominada dirección MAC, que consiste en un número de 48 bits: los primeros 24 bits identifican al fabricante de la tarjeta, mientras que los restantes 24, a la tarjeta en sí. Este modelo de direccionamiento es común con las redes Ethernet (802.3).

Network name, nombre de red: Identificador de la red para su diferenciación del resto de las redes. Durante el proceso de instalación y configuración de dispositivos wireless, se requiere introducir un nombre de red o SSID para poder acceder a la red en cuestión.

Parabólica, antena: Antena en forma de disco curvado. Este tipo de antena ofrece la directividad más alta, lo que las hace ideales para enlaces punto a punto a larga distancias.

Omnidireccional, antena: Antena que proporciona una cobertura total en un plano (360 grados) determinado.

PHY: Nombre abreviado del nivel más bajo del modelo ISO, el nivel físico, que describe el medio físico en el que se transmite la información de la red.

En el caso de las redes inalámbricas, las normas 802.11 definen el nivel PHY que utilizan, el aire libre, y los parámetros empleados como la velocidad de transmisión, tipo de modulación, algoritmos de sincronización emisor/receptor, etc.

Roaming: Nombre dado a la acción de moverse del área de cobertura de un Punto de Acceso a otro sin pérdida de conectividad, de forma que el usuario no lo percibe.

Router: Dispositivo de red que traslada los paquetes de una red a otra. Basándose en las tablas y protocolos de enrutamiento y en el origen y destino, un router decide hacia dónde enviar un paquete de información.

SSID, Service Set Identification: Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos wireless se puedan comunicar, deber tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad.

Dependiendo de si la red wireless funciona en modo Ad-Hoc o en modo Infraestructura, el SSID se denomina ESSID o BSSID.

Velocidad de transmisión (Throughput): Capacidad de transmisión de un medio de comunicación en cualquier momento, se suele medir en bits por segundo (bps). Depende de múltiples factores, como la ocupación de la red, los tipos de dispositivos empleados, etc, y en el caso de redes wireless, se añaden los problemas de propagación de microondas a través de la que se transmite la información.

VPN, Virtual Private Network: Herramienta de seguridad que permite mantener en privado una comunicación a través de una red pública. Puede ofrece otros servicios como autentificación de los extremos involucrados, integridad, etc.

War chalking: Proceso de realizar marcas en las superficies (paredes, suelo, señales de tráfico, etc) para indicar la existencia de redes wireless y alguna de sus características (velocidad, seguridad, caudal, etc).

War driving: Localización y posible intrusión en redes wireless de forma no autorizada. Sólo se necesita un portátil, un adaptador wireless, el software adecuado y un medio de transporte.

Wi-Fi, Wireless Fidelity: Nombre dado al protocolo 802.11b para transmisión inalámbrica. Los dispositivos certificados como Wi-Fi son interoperables entre sí, como garantía para el

WPA, Wi-Fi Protected Access: Protocolo de seguridad desarrollado por la WECA para mejorar la seguridad de la información en las redes wireless y permitir la autentificación de usuario, puntos débiles del WEP.

Yagi, antena: Antena compuesta por varios dipolos en línea, obteniendo una mayor ganancia y directividad

RESUMEN

TITULO: DISEÑO DE UNA RED WIRELESS PARA PROVEER SERVICIOS DE INTERNET (WISP) BASADA EN OPEN SOURCE PARA CONECTIVIDAD DE USUARIOS EMPRESARIALES, RESIDENCIALES Y RURALES DE SAN VICENTE DE CHUCURÍ[1]

AUTOR: PEDRO ALBERTO ARIAS QUINTERO – MARIO GOMEZ MORENO[**]

PALABRAS CLAVES:, Linux, Mikrotik, portal cautivo, QoS, wi-fi, wireless, wisp.

DESCRIPCIÓN: La presente monografía consiste en analizar y diseñar una red wireless para proveer servicios de internet (WISP) basada en tecnologías open source para conectividad de usuarios empresariales, residenciales y rurales de San Vicente de Chucurí, garantizando calidad de servicios, administración de ancho de banda y políticas de seguridad mediante un portal cautivo. El proyecto está enfocado en un análisis y diseño de requerimientos y herramientas para la implementación de una red piloto para un WISP a través de la tecnología inalámbrica Wi-Fi y uso de open source.

En el proyecto se pretende diseñar una solución innovadora y de bajo costo para prestar servicios de Internet, que en la actualidad han sido implementados con soluciones dependientes de la tecnología cableada con todas sus desventajas en movilidad y mantenimiento, con este proyecto se pretende dejar un diseño que permita masificar internet, llegando a las sedes educativas rurales, centros poblados, veredas y caseríos que lo requieran, la alternativa de desarrollo en este campo brinda la posibilidad de ser líder en la distribución de servicios inalámbricos y dar origen a nuevos proyectos como gestión de redes de sensores inalámbricos (WSN) para las industrias agropecuarias, petrolera, o afines que funcionen en áreas rurales.

[1] Trabajo de Grado

[**] Facultad de Especialización en Telecomunicaciones. Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones. Director: Freddy Alfonso Beltrán Miranda

SUMMARY

TITLE: DESIGN OF A NETWORK WIRELESS TO PROVIDE SERVICES OF INTERNET (WISP) CRADLE IN OPEN SOURCE FOR CONNECTIVITY OF ENTERPRISE, RESIDENTIAL AND RURAL USERS OF SAN VICENTE CHUCURÍ[*]

AUTHOR: PEDRO ALBERTO ARIAS QUINTERO – MARIO GOMEZ MORENO[**]

KEY WORDS: Linux, Mikrotik, HotSpot, captive vestibule, QoS, wi-fi, wisp

DESCRIPCIÓN: The present monograph consists of analyzing and to design a network wireless to provide services of Internet (WISP) cradle in technologies open source for connectivity of enterprise, residential and rural users of San Vicente de Chucurí, guaranteeing quality of services, administration of bandwidth and policies of security by means of a captive vestibule. The project is focused in an analysis and design of requirements and tools for the implementation of a pilot network for a WISP through the wireless technology Wi-Fi and use of open source.

In the project it is tried to design an innovating solution and of low cost to serve of Internet, that at present has been implemented with dependent solutions of the technology twisted with all disadvantages in mobility and maintenance, with this project it is tried to leave a design that allows to amass Internet, arriving at you soothe educative rural, populated centers, paths and small villages require that it, the alternative of development in this field offers the possibility of being leader in the distribution of wireless services and to give rise to new projects like management of networks of wireless sensors (WSN) for the industries farming, oil, or compatible that work in rural areas.

[*] Grade project.
[**] Ability of Specialization in Telecommunications. Electric, Electronic school of Engineerings and of Telecommunications. Director: Freddy Alfonso Beltrán Miranda.

1 INTRODUCCION

El Proveedor de servicios Internet inalámbrico (WISP) se define como un conjunto de dispositivos en red con cubrimiento de área metropolitana (MAN) integrados entre sí para conectar usuarios clientes a internet. Las redes que utilizan comunicaciones inalámbricas de alta velocidad se usan para proveer acceso a internet punto a punto ó punto multipunto a clientes como empresas privadas, de gobierno, colegios, universidades, usuarios residenciales, rurales y todo tipo de cliente o instituciones que tienen Redes del Área Locales (LAN) y que requiera conectarse a internet.

En la actualidad las empresas de servicios WISP se encuentran en desarrollo y crecimiento, La implementación de las wireless basadas en software libre para mejorar procesos de acceso desde sitios remotos ofrece una significativa reducción de los costos y una amplia gama de servicios con el fin de brindar seguridad, administración de usuarios y balanceo de cargas.

El proyecto planteado, tiene por objeto Diseñar una red wireless para proveer servicios de internet (WISP) basada en tecnologías open source para ser utilizada en el acceso wifi de usuarios residenciales, empresariales y rurales de San Vicente de Chucurí, proporcionando

Actualmente la forma de acceso al servicio de Internet en esta zona y principalmente en las zonas rurales de San Vicente de Chucurí es a través de línea telefónica de baja velocidad ó en el mejor de los casos a través de empresas de servicio operador de celular, cualquier empresa que quiera prestar los servicios de carrier debe contar con una red de acceso inalámbrico móvil de alta velocidad, es por eso que se requiere diseñar una red con tecnología de banda ancha, alta capacidad de transmisión de datos y

amplio cubrimiento que sirva para llevar Internet a zonas que no lo tienen por culpa de las complicaciones del cableado o por los elevados costos de implementación, la presentación de una red con tecnología Wi-fi es un excelente complemento para las redes, que cada día son más difundidas en empresas, lugares públicos (restaurantes, aeropuertos, etc.) y hogares.

Existen empresas, usuarios locales y usuarios rurales que por sus actividades están en continuo movimiento, los cuales requieren enviar información en línea , con seguridad e integridad, que en el momento de no tener acceso continuo a internet deja ver la necesidad de contar con una red inalámbrica que permita dar acceso a internet en forma segura y confiable y así mismo que proporcione otros servicios de comunicación a los diferentes clientes empresariales, comerciales, residenciales y principalmente rurales, diseñar una red wireless para proveer servicios de internet (WISP) basada en open source se plantea como posible solución

1.1 JUSTIFICACION

La presente monografía consiste en analizar y diseñar una red wireless para proveer servicios de internet (WISP) basada en tecnologías open source para conectividad de usuarios empresariales, residenciales y rurales de San Vicente de Chucurí, garantizando calidad de servicios, administración de ancho de banda y políticas de seguridad mediante un portal cautivo.

El proyecto está enfocado en un análisis y diseño claro y exacto con el cual pueda implementarse un WISP que ofrezca los Servicios de Internet demandados por la mayoría de las empresas a través de la tecnología inalámbrica Wi-Fi y uso de open source, tecnologías que en este negocio son una innovación al no existir proveedores de este tipo en sitios remotos como San Vicente de Chucurí y su área rural.

Finalmente se pretende demostrar con este proyecto que existe una alternativa innovadora para el despliegue de servicios de Internet ofertados que hasta la fecha han sido implementados con soluciones dependientes de la tecnología cableada con todas sus desventajas en movilidad y mantenimiento, alternativa que como pionera en este campo se desenvuelva como líder en la distribución de servicios inalámbricos y de origen a nuevos proyectos como gestión de redes de sensores inalámbricos (WSN) para las industrias agropecuarias, petrolera, o afines que funcionen en áreas rurales.

Este proyecto da una idea clara de las ventajas que presenta la Implementación de la tecnología wireless y open source con respecto a la tecnología cableado y 3g para ingreso a internet, por ser una solución de código abierto como el SO Linux que trabaja algunas soluciones del mercado que serán analizadas y soluciones inalámbricas Wi-fi su implementación puede hacerse a un costo muy bajo con respecto a las soluciones comerciales de este tipo, logrando resultados que beneficien a las empresas y usuarios en general; adicionalmente este proyecto contribuye a la investigación de nuevas tecnologías y soluciones en proveedores de servicios de internet inalámbricos, siendo una fuente importante de información para los nuevos investigadores que estén interesados en este tema. Este trabajo permite al estudiante aplicar los conocimientos recibidos en la especialización de telecomunicaciones de la Universidad Industrial de Santander.

Durante el desarrollo de este proyecto se realiza una comparación de las diversas tecnologías inalámbricas, estándares para este tipo de redes wi-fi, el hardware a utilizar para la implementación de un WISP basado en open source; así como también de las diversas clases servicios y políticas de seguridad, balanceo etc, que requiere implementar un proveedor de servicios de internet inalámbrico. Luego del análisis, se diseñará la red piloto wireless para proveer servicios de internet (WISP) basada en tecnologías

open source para ser utilizada en el acceso remoto de usuarios móviles en sectores rurales de San Vicente de Chucurí, cuyo esquema estará basado en una configuración de redes punto a punto y punto multipunto, y que utilizará tecnología Wi-fi.

1.2 OBJETIVO GENERAL

Diseñar una red wireless para proveer servicios de internet (WISP) basada en open source para conectividad de usuarios empresariales, residenciales y rurales de San Vicente de Chucuri.

1.3 OBJETIVOS ESPECIFICOS

- Analizar las diversas tecnologías en redes inalámbricas para proveer servicios de internet.

- Comparar la mejor solución que permita diseñar una red wireless para proveer servicios de internet (WISP) basado en open source.

- Diseñar e Implementar una red piloto wireless para proveer servicios de internet (WISP) basada en open source para conectividad de usuarios empresariales, residenciales y rurales, garantizando, calidad de servicios, administración de ancho de banda y políticas de seguridad mediante un portal cautivo.
- Entrega de documentación como aporte académico, de consulta y apoyo a futuras investigaciones en el área de telecomunicaciones.

1.4 ANTECEDENTES

Las primeras redes inalámbricas IEEE 802.11 aparecieron a finales de la década de los noventa. Su aparición se debía principalmente al propósito de brindar un acceso inalámbrico a muchas computadoras ubicadas juntas en un ambiente cerrado; de tal forma se prescindirían de los actuales cables UTP para la conexión de los usuarios a la red. Si bien las velocidades de estas redes cuando aparecieron no les permitía competir contra las redes con cables de ese entonces (donde la tecnología Ethernet empezaría su reinado), poco a poco fueron éstas mejorando hasta llegar en la actualidad a velocidades lo suficientemente rápidas (25 a 30 Mbps de throughput real en el mejor de los casos para redes Wi-Fi basadas en el estándar IEEE 802.11g) como para brindar un acceso satisfactorio a los usuarios de la red.

Los proveedores de servicios de internet en Colombia son variados pero con restricciones de acceso a zonas rurales y en especial en las zonas de Santander como San Vicente de Chucurí no se ha realizado ningún diseño o piloto de red wireless para proveer servicios de internet (WISP).

Durante muchos años los sistemas de banda ancha inalámbricos han estado basados en tecnologías propietarias de las compañías que los instalaban, tenían un rendimiento limitado y en muchos casos eran demasiado caros para ser colocados de manera masiva; razones por las cuales se gesta el estándar Wi-fi para acceso inalámbrico a Internet.

Desde hace poco, existe una nueva tecnología que hace uso de las frecuencias libres de licencia: las redes de área local inalámbricas o redes wireless. Las LAN inalámbricas utilizan básicamente longitudes de onda correspondientes a las microondas (2,4 GHz y 5 GHz) y permiten tener anchos de banda apreciables (desde 1 MB/s en las primeras versiones hasta

llegar a los 54 MB/s de los últimos estándares). También es verdad que aunque la banda alrededor de los 5 GHz es abierta en todo el mundo, el ancho de banda que se puede ocupar depende de la situación particular que haya impuesto cada legislador. Es por ello que en Europa se pueden utilizar hasta 455 MHz, mientras que en Norteamérica el ancho de banda se restringe a 300 MHz y en Japón a 100 MHz.

En muchos sitios, las redes Ethernet de cable tradicionales han sido ampliadas con la implantación de este tipo de redes inalámbricas. La interconexión de varias redes locales (como por ejemplo en el caso de redes inalámbricas que se extienden en todo el campo universitario) ha propiciado que algunos visionarios hayan visto la posibilidad de crear una red metropolitana con gran ancho de banda y con la posibilidad de acceso a Internet, de forma que se pudiera acceder a cualquier servicio de los que comúnmente se utilizan en Internet (correo, web, ftp, etc.) desde cualquier lugar dentro del ámbito metropolitano.

En el contexto nacional, esta nueva tecnología wi-fi, ha permitido desarrollo de proyectos por algunas empresas de servicios d telecomunicaciones como GlobalNet implementó varios proyectos, uno de ellos es el proyecto para brindar servicio de Internet banda ancha wireless en la ciudad de Plato y localidades aledañas utilizando la banda ISM de 2.4GHz y 5.8GHz para enlaces repetidores; la solución se diseñó basada en un enlace en fibra de 3E1 y convertido en un enlace inalámbrico, para luego implementar el sistema Punto Multipunto hacia los usuarios finales.

Otro ejemplo de éxito de esta misma compañía fue el proveer Internet inalámbrico a las instituciones educativas del municipio de Maní Casanare y cubrimiento del 100% del casco urbano; el sistema consta de un primer enlace inalámbrico de tipo troncal transportando la señal de Internet de banda ancha desde la Alcaldía Municipal hacia un lugar estratégico usando

un equipamiento punto a punto distribuido, para luego implementar el sistema punto multipunto hacia los usuarios finales.

Estos proyectos demuestran que se han dado soluciones y han funcionado pero generalmente son soluciones hibridas entre redes basadas en Wi-Fi y Wimax, y han sido proyectos comerciales a los cuales la academia no tiene acceso y por tanto no permiten un mayor estudio y análisis por porte de futuros investigadores, la propuesta del diseño en este proyecto para el wisp en San Vicente pretende dejar documentación a la academia para futuros trabajos y mejoras en proyectos que usen este tipo de tecnologías.

2 CONCEPTUALIZACION DE REDES INALAMBRICAS

2.1 REDES

Una red es un conjunto de computadoras interconectadas entre sí, ya sea por medio de cables o de ondas de radio (Wireless). El principal propósito de armar una red consiste en que todas las computadoras que forman parte de ella se encuentren en condiciones de compartir su información y sus recursos con las demás. De esta manera, se estaría ahorrando dinero, debido a que si se colocara un dispositivo, por ejemplo, una impresora, todas las computadoras de la red podrían utilizarlo.

Los recursos que se pueden compartir en una red son:

- Procesador y memoria RAM, al ejecutar aplicaciones de otras PC.
- Unidades de disco duro.
- Unidades de disco flexible.
- Unidades de CD-ROM/DVD-ROM.
- Impresoras.
- Fax.
- Módem.
- Conexión a Internet.

También es posible compartir la información almacenada en las computadoras conectadas a la red, por ejemplo:

- Ejecución remota de programas de aplicación.
- Bases de datos.
- Documentos en general (archivos de texto, imagen, sonido, video, etc.).
- Directorios (carpetas).

Como ventaja adicional, la instalación de una red ofrece una interfaz de comunicación a todos sus usuarios. Esto se logra por medio de la utilización del correo electrónico, el chat y la videoconferencia.

2.2 REDES INALAMBRICAS

Tal como su nombre lo indica, las redes inalámbricas son aquéllas que carecen de cables. Gracias a las ondas de radio, se lograron redes de computadoras de este tipo, aunque su creación refirió varios años de búsqueda.

Esta tecnología facilita en primer lugar el acceso a recursos en lugares donde se imposibilita la utilización de cables, como zonas rurales poco accesibles. Además, estas redes pueden ampliar una ya existente y facilitar el acceso a usuarios que se encuentren en un lugar remoto, sin la necesidad de conectar

Las redes inalámbricas no es más que un conjunto de computadoras, o de cualquier dispositivo informático comunicados entre sí mediante soluciones que no requieran el uso de cables de interconexión. En el caso de las redes locales inalámbricas, es sistema que se está imponiendo es el normalizado por IEEE con el nombre 802.11b. A esta norma se la conoce más habitualmente como WI-FI (Wiriless Fidelity).

Con el sistema WI-FI se pueden establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzándose distancia de hasta cientos de metros. No obstante, versiones más recientes de esta tecnología permiten alcanzar los 22, 54 y hasta los 100 Mbps.

Imagen 1. Red inalámbrica

Fuente: autores

2.2.1 Ventajas de las Redes Inalámbricas[2]:

Las principales ventajas son:

2.2.1.1 Flexibilidad: Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados por el mundo Por ejemplo, para hacer esta presentación se podría haber colgado la presentación de la web y haber traído simplemente el portátil y abrirla desde Internet incluso aunque la oficina en la que estuviésemos no tuviese rosetas de acceso a la red cableada.

2.2.1.2 Poca planificación: Con respecto a las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica

[2] Fuente: www.intel.com/espanol

sólo nos tenemos que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.

2.2.1.3 Diseño: Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc.

2.2.1.4 Robustez: Ante eventos inesperados que pueden ir desde un usuario que se tropieza con un cable o lo desenchufa, hasta un pequeño terremoto o algo similar. Una red cableada podría llegar a quedar completamente inutilizada, mientras que una red inalámbrica puede aguantar bastante mejor este tipo de percances inesperados Inconvenientes de las Redes Inalámbricas

2.2.1.5 Calidad de Servicio: Las redes inalámbricas ofrecen una peor calidad de servicio que las redes cableadas. Estamos hablando de velocidades que no superan habitualmente los 10 Mbps, frente a los 100 que puede alcanzar una red normal y corriente. Por otra parte hay que tener en cuenta también la tasa de error debida a las interferencias. Esta se puede situar alrededor de 10-4 frente a las 10-10 de las redes cableadas. Esto significa que has 6 órdenes de magnitud de diferencia y eso es mucho. Estamos hablando de 1 bit erróneo cada 10.000 bits o lo que es lo mismo, aproximadamente de cada Megabit transmitido, 1 Kbit será erróneo. Esto puede llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad.

2.2.1.6 Costo: Aunque cada vez se está abaratando bastante aún sale bastante más caro. Recientemente en una revista comentaban que puede llegar a salir más barato montar una red inalámbrica de 4 ordenadores que una cableada si tenemos en cuenta costes de cablear una casa. El ejemplo era para una casa, aunque, todo hay que decirlo, estaba un poco forzado. Aún no merece la pena debido a la poca calidad de servicio, falta de estandarización y costo.

2.2.1.7 Soluciones Propietarias: Como la estandarización está siendo bastante lenta, ciertos fabricantes han sacado al mercado algunas soluciones propietarias que sólo funcionan en un entorno homogéneo y por lo tanto estando atado a ese fabricante. Esto supone un gran problema ante el mantenimiento del sistema, tanto para ampliaciones del sistema como para la recuperación ante posibles fallos. Cualquier empresa o particular que desee mantener su sistema funcionando se verá obligado a acudir de nuevo al mismo fabricante para comprar otra tarjeta, punto de enlace, etc.

2.2.2 Desventajas de las redes inalámbricas:

Evidentemente, como todo en la vida, no todo son ventajas, las redes inalámbricas también tiene unos puntos negativos en su comparativa con las redes de cable. Los principales inconvenientes de las redes inalámbricas son los siguientes:

2.2.2.1 Menor ancho de banda: Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tiene un precio superior al de los actuales equipos Wi-Fi.

2.2.2.2 Mayor inversión inicial: Para la mayoría de las configuraciones de la red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.

2.2.2.3 Seguridad: Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier

persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella.

Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de lo más fiables. A pesar de esto también es cierto que ofrece una seguridad válida para la inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA) que hace a Wi-Fi mucho más confiable.

2.2.2.4 Interferencias: Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 GAZ. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias.

Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias incluida la de los vecinos. Este hecho hace que no se tenga la garantía de nuestro entorno radioelectrónico este completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

2.2.2.5 Incertidumbre tecnológica: La tecnología que actualmente se esta instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE 802.11B). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad, es posible que, cuando se popularice esta nueva tecnología, se

deje de comenzar la actual o, simplemente se deje de prestar tanto apoyo a la actual.

Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades del cliente y, aunque existe una incógnita, los fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales. La historia nos ha dado muchos ejemplos similares.

2.3 Estándares para redes Wi-Fi[3]

Desde hace poco, existe una nueva tecnología que hace uso de las frecuencias libres de licencia: las redes de área local inalámbricas o redes wireless. Las LAN inalámbricas utilizan básicamente longitudes de onda correspondientes a las microondas (2,4 GHz y 5 GHz) y permiten tener anchos de banda apreciables (desde 1 MB/s en las primeras versiones hasta llegar a los 54 MB/s de los últimos estándares).

2.3.1 Descripción del estándar para redes Wi-Fi IEEE 802.11 genérico:

Las redes IEEE 802.11 suponen la apuesta del IEEE por las redes inalámbricas. Toda ellas se basan en una red tipo Ethernet y, aunque su filosofía es la misma, difieren en la banda de frecuencia utilizada, el ancho de banda que ofrecen, etc.

La especificación original de 802.11 preveía conexiones a velocidades de 1 ó 2 MB/s en la banda de los 2,4 GHz utilizando dos tipos de espectro expandido (spread spectrum): salto de frecuencias (FHSS) o secuencia directa (DSSS).

[3] Fuente www.interwifi.com Sistemas Inalámbricos

El objetivo principal a la hora de utilizar el espectro expandido es transmitir ocupando una banda de frecuencias mayor de la requerida. Su creación se debe a investigaciones militares durante la Segunda Guerra Mundial, ya que de esta forma se evitaban ataques y escuchas. FHSS (salto de frecuencias) se basa en que transmite en diferentes bandas de frecuencias, produciéndose saltos de una otra de una forma aleatoria que es imposible predecir. Por contra, con DSSS (secuencia directa) se envían varios bits por cada bit de información real.

Otra de las características comunes en las diferentes implementaciones del estándar 802.11 es el uso de WEP, Wireless Equivalent Privacy. WEP tiene como objetivo conseguir una seguridad equivalente a la de las redes convencionales (de cable).

El problema reside en que las redes tradicionales basan gran parte de su seguridad en que es difícil comprometer el cable, mientras que la comunicación de las redes inalámbricas va por el aire. WEP es un protocolo razonablemente fuerte y computacionalmente eficiente. Sin embargo, su uso no deja de ser opcional y recientemente se ha descubierto que no es del todo seguro, tal y como ha demostrado un estudio de una universidad americana.

Dentro de las redes 802.11 encontramos tres tipos, la 802.11a, la 802.11b y la 802.11g, de las cuales la primera trabaja en la banda de frecuencia de 5 GHz y las otras dos en la banda de 2.4 GHz. En la tabla que aparece a continuación se muestran las características de cada una de estas redes.

Tabla 1 Resumen de características de redes 802.11

Característica	**802.11a**	**802.11b**	**802.11g**
Velocidad Máxima	54 Mbps	11 Mbps	54 Mbps
Velocidad real	27 Mbps	4 o 5 Mbps	20 o 25 Mbps
Modulación	OFDM	CCK / DSSS	OFDM / DSSS

Característica	**802.11a**	**802.11b**	**802.11g**
Espectro	5 Ghz	2.4 – 2.483 Ghz	2.4 – 2.483 Ghz
Fecha aprobación	jul-99	jul-99	jun-03

2.3.2 Descripción del estándar para redes Wi-Fi IEEE 802.11 a

Mientras se desarrollaba la 802.11b, la IEEE crea una nueva extensión del estándar 802.11 denominada 802.11a. Debido a que la 802.11b ganó popularidad muy rápidamente, mucha gente cree que la 802.11a se creó después que ésta, aunque en realidad se desarrollaron a la vez. Debido a su alto costo, la 802.11a suele utilizarse en redes de empresas, mientras que la 802.11b se usa más en redes domésticas.

La 802.11a soporta velocidades de hasta 54Mbit/s y trabaja en la frecuencia regulada de 5GHz. Comparada con la 802.11b, esta mayor frecuencia limita el rango de la 802.11a. Además, el trabajar en una frecuencia mayor significa que la señal de la 802.11a tiene una mayor dificultad para atravesar muros y objetos.

Por otro lado, como la 802.11a y la 802.11b utilizan frecuencias distintas, ambas tecnologías son incompatibles entre ellas. Algunos fabricantes ofrecen híbridos 802.11a/b, aunque estos productos lo que tienen realmente son las dos extensiones implementadas.

Ventajas: Velocidad máxima alta, soporte de muchos usuarios a la vez y no produce interferencias en otros aparatos.

Inconvenientes: Alto costo, bajo rango de señal que es fácilmente obstruible. Para terminar, podemos ver un resumen de las características de esta red.

Tabla 2 Resumen de características de redes 802.11 a

802.11a	
Frecuencia longitud de onda	5GHz
Ancho de banda de datos	54Mbps, 48Mbps, 36Mbps, 24Mbps, 12Mbps, 6Mbps
Medidas de seguridad	WEP, OFDM
Rango de Operación óptima	50 metros dentro, 100 metros afuera
Adaptado para un propósito específico o para un tipo de dispositivo	Ordenadores portátiles móviles en entornos privados o empresariales, ordenadores de sobremesa allí donde cablear sea inconveniente

2.3.3 Descripción del estándar para redes Wi-Fi IEEE 802.11 b

En julio de 1999, la IEEE expande el 802.11 creando la especificación 802.11b, la cual soporta velocidades de hasta 11 Mbit/s, comparable a una Ethernet tradicional. La 802.11b utiliza la misma frecuencia de radio que el tradicional 802.11 (2.4GHz).

El problema es que al ser esta una frecuencia sin regulación, se podían causar interferencias con hornos microondas, teléfonos móviles y otros aparatos que funcionen en la misma frecuencia. Sin embargo, si las instalaciones 802.11b están a una distancia razonable de otros elementos, estas interferencias son fácilmente evitables. Además, los fabricantes prefieren bajar el costo de sus productos, aunque esto suponga utilizar una frecuencia sin regulación.

Ventajas: Bajo costo, rango de señal muy bueno y difícil de obstruir.

Inconvenientes: Baja velocidad máxima, soporte de un número bajo de usuarios a la vez y produce interferencias en la banda de 2.4 GHz. En la siguiente tabla vemos las características de esta red.

Tabla 3 Resumen de características de redes 802.11 b

802.11 b	
Frecuencia longitud de onda	2.4GHz (2.400-2.4835 in North America)
Ancho de banda de datos	11Mbps, 5Mbps, 2Mpbs, 1Mbps
Medidas de seguridad	WEP – Wireless Equivalency Protocol en combinación con espectro de dispersión directa
Rango de Operación óptima	50 metros dentro, 100 metros afuera
Adaptado para un propósito específico o para un tipo de dispositivo	Ordenadores portátiles, ordenadores de sobremesa donde cablear entraña dificultades, PDAs

2.3.4 Descripción del estándar para redes Wi-Fi IEEE 802.11 g

2002 y 2003 ha aparecido un nuevo estándar denominado 802.11g. Este nuevo estándar intenta aprovechar lo bueno de cada uno de los anteriores 802.11a y 802.11b. La 802.11g permite velocidades de hasta 54 Mbit/s y utiliza la banda de frecuencia de 2.4 GHz. Además, al trabajar en la misma banda de frecuencia, la 802.11g es compatibles con la 802.11b, por lo que puntos de acceso 802.11g pueden trabajar en redes 802.11b y viceversa.

Ventajas: Velocidad máxima alta, soporte de muchos usuarios a la vez, rango de señal muy bueno y difícil de obstruir.
Inconvenientes: Alto costo y produce interferencias en la banda de 2.4 GHz.

Tabla 4 Resumen de características de redes 802.11 g

802.11g	
Frecuencia longitud de onda	2.4GHz
Ancho de banda de datos	54 Mbps
Medidas de seguridad	WEP, OFDM
Rango de Operación óptima	50 metros dentro, 100 metros afuera
Adaptado para un propósito específico o para un tipo de dispositivo	Ordenadores portátiles, ordenadores de sobremesa donde cablear entraña dificultades, PDAs. Compatible hacia atrás con las redes 802.11b

2.3.5 Descripción del estándar para redes Wi-Fi IEEE 802.11 n[4]:

El networking inalámbrico basado en los estándares 802.11, también conocido con el nombre comercial Wi-Fi, se ha convertido en algo común en los hogares y disfruta de una significativa y creciente presencia en las infraestructuras corporativas. Pero el estándar de mayor velocidad actualmente en uso, 802.11g, fue ratificado hace tiempo, en 2003, y resulta ya claramente insuficiente para soportar las demandas de ancho de banda requeridas por las nuevas aplicaciones.

2.3.6 2002 y 2003 ha aparecido un nuevo estándar denominado 802.11g.

Este nuevo estándar intenta aprovechar lo bueno de cada uno de los anteriores 802.11a y 802.11b. La 802.11g permite velocidades de hasta 54 Mbit/s y utiliza la banda de frecuencia de 2.4 GHz. Además, al trabajar en la misma banda de frecuencia, la 802.11g es compatibles con la 802.11b, por lo que puntos de acceso 802.11g pueden trabajar en redes 802.11b y viceversa.

Por ejemplo, el streaming de vídeo –ya sea utilizado para la reproducción de una película en casa o para una sesión de videoconferencia en la empresa- es una proposición bastante arriesgada para 802.11g. Aunque los productos "g" tienen una velocidad máxima de rendimiento teórico de 54 Mbps, en la práctica soportan la mitad de este ancho de banda, o incluso menos, lo que resulta claramente insuficiente para el soporte de vídeo de calidad. Hoy en día la mayoría de los productos de redes inalámbricas (WLAN- Wireless LAN) desplegados se basan en las especificaciones 802.11 b y g. La norma

[4] Fuente: http://www.idg.es/cio/estructura/imprimir.asp?id=185432&cat=art

802.11n constituye el siguiente paso, diseñado para elevar la velocidad de las WLAN de máximos teóricos de 600 Mbps.

El estándar aún está pendiente de aprobación definitiva, pero ya existen diversos productos que cumplen con su primer borrador y alcanzan máximos de 300 Mbps. De hecho, la necesidad de productos de mayor ancho de banda es tan acuciante que Wi-Fi Alliance, encargada de probar y certificar la interoperatividad multifabricante Wi-Fi, ha creado un sello específico para garantizar la compatibilidad con el segundo borrador de 802.11n.

El rendimiento, ha sido uno de las principales desventajas tradicionales de las redes Wi-Fi frente a las redes Ethernet cableadas; así, en este momento, cuando Wi-Fi aún sólo puede ofrecer de manera estandarizada 54 Mbps, Ethernet sobre cable soporta ya 10 Gbps por segundo y está en camino el estándar a 100 Gbps. Pero no la única. La seguridad y el alcance también han representado importantes inconvenientes, actuando en muchos casos como inhibidores para un más amplio despliegue de Wi-Fi. Por eso, en 802.11n, además de al rendimiento, se ha prestado especial atención al incremento de la cobertura. En lo que respecta a la seguridad, el nuevo estándar no aportará nuevas capacidades, pero lo cierto es que las últimas generaciones de Wi-Fi ofrecían ya características avanzadas en este sentido.

A continuación se responde a diferentes preguntas que, sin duda, surgirán a muchos interesados en las nuevas posibilidades abiertas por 802.11n. Con estas respuestas, el usuario podrá hacerse una idea sobre lo que se puede esperar de 802.11n tanto en el hogar como en la empresa.

¿En qué se diferencia 802.11n de las actuales generaciones de Wi-Fi?

El estándar 802.11n utiliza algunas nuevas tecnologías y toma algunas características de otras ya existentes para dotar a Wi-Fi de mayor velocidad y alcance. Quizá entre las primeras la más destacable sea MIMO (Multiple

Input, Multiple Output). Esta tecnología se basa en la utilización de varias antenas para transportar múltiples corrientes de datos de un lugar a otro. Algo que permite la transmisión de mayor cantidad de datos en el mismo período de tiempo; es decir, un aumento de velocidad. MIMO también constituye la clave para el aumento de cobertura –distancia a la que los datos pueden transmitirse- en la próxima generación de productos WLAN.

Una segunda tecnología incorporada en 802.11n y directamente ligada también al aumento del rendimiento es “channel bonding” (unión o emparejamiento de canales). Este sistema permite utilizar simultáneamente dos canales no-superpuestos como si de uno con el doble de capacidad se tratara para transmitir los datos a mayor velocidad. Tales canales deben ser adyacentes o contiguos. Utilizando esta tecnología es posible sumar el ancho de banda de dos canales de 20 MHz para conseguir un enlace wireless de 40 MHz.

En tercer lugar, 802.11n implementa una tecnología denominada agregación de paquete o “payload optimization", que, en términos sencillos, permite meter más datos en cada paquete transmitido.

2.3.7 Descripción del estándar para redes Wi-Fi IEEE 802.16[5]

WiMAX (del inglés *Worldwide Interoperability for icrowave Access*, Interoperabilidad Mundial para Acceso por Microondas) es un estándar de transmisión inalámbrica de datos (802.16d) diseñado para ser utilizado en el área metropolitana o MAN proporcionando accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología portátil LMDS.

[5] Fuente http://www.wimaxforum.org/

Integra la familia de estándares IEEE 802.16 y el estándar HyperMAN del organismo de estandarización europeo ETSI. El estándar inicial 802.16 se encontraba en la banda de frecuencias de 10-66 GHz y requería torres LOS. La nueva versión 802.16a, ratificada en marzo de 2003, utiliza una banda del espectro más estrecha y baja, de 2-11 GHz, facilitando su regulación. Además, como ventaja añadida, no requiere de torres sino únicamente del despliegue de estaciones base (BS) formadas por antenas emisoras/receptoras con capacidad de dar servicio a unas 200 estaciones suscriptoras (SS) que pueden dar cobertura y servicio a edificios completos. Su instalación es muy sencilla y rápida (culminando el proceso en dos horas) y su precio competitivo en comparación con otras tecnologías de acceso inalámbrico como Wi-Fi: entre 5.000 euros y 25.000 euros.

Esta tecnología de acceso transforma las señales de voz y datos en ondas de radio dentro de la citada banda de frecuencias. Está basada en OFDM, y con 256 subportadoras puede cubrir un área de 48 kilómetros permitiendo la conexión sin línea vista, es decir, con obstáculos interpuestos, con capacidad para transmitir datos a una tasa de hasta 75 Mbps con una eficiencia espectral de 5.0 bps/Hz y dará soporte para miles de usuarios con una escalabilidad de canales de 1,5 MHz a 20 MHz. Este estándar soporta niveles de servicio (SLAs) y calidad de servicio (QoS).

WiMAX se sitúa en un rango intermedio de cobertura entre las demás tecnologías de acceso de corto alcance y ofrece velocidades de banda ancha para un área metropolitana.

El *WiMAX Forum* es un consorcio de empresas (inicialmente 67 y hoy en día más de 100) dedicadas a diseñar los parámetros y estándares de esta tecnología, y a estudiar, analizar y probar los desarrollos implementados.

En principio se podría deducir que esta tecnología supone una grave amenaza para el negocio de tecnologías inalámbricas de acceso de corto alcance en que se basan muchas empresas, pero hay entidades muy importantes detrás del proyecto.

Las principales firmas de telefonía móvil también están desarrollando terminales capaces de conectarse a estas nuevas redes. Después de la fase de pruebas y estudios cuya duración prevista es de unos dos años, se espera comenzar a ofrecer servicios de conexión a Internet a 4 Mbps a partir de 2007, incorporando WiMAX a los ordenadores portátiles y PDA.

El 7 de diciembre de 2005, el IEEE aprobó el estándar del WiMAX MÓVIL, el 802.16e, que permite utilizar este sistema de comunicaciones inalámbricas con terminales en movimiento.

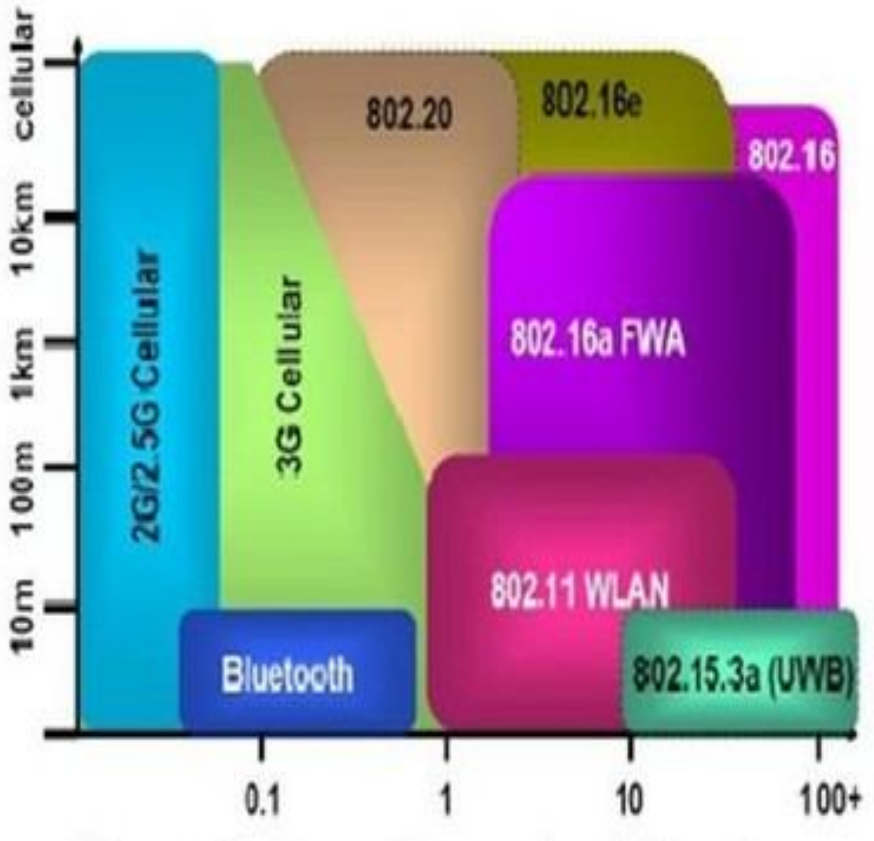
Lo que ocurría en la práctica es que pocos se atrevían a invertir en wimax bajo el único estándar aprobado hasta ahora, el 802.16d, que sólo sirve para aquellos terminales que están en un punto fijo. Ahora ya saben qué especificaciones técnicas debe tener el hardware del wimax móvil, que es mucho más jugoso económicamente, con lo que es posible diseñar infraestructuras mixtas fijo-móvil.

En Corea se ha materializado las ventajas de un WiMAX móvil trabajando en 2,3Ghz y se le ha acuñado el nombre de **WiBRO** (Wireless Broadband), esta iniciativa empieza sus despliegues comerciales en el 2006.

Tabla 5 Resumen de Características Estándar 802.16 (wimax)

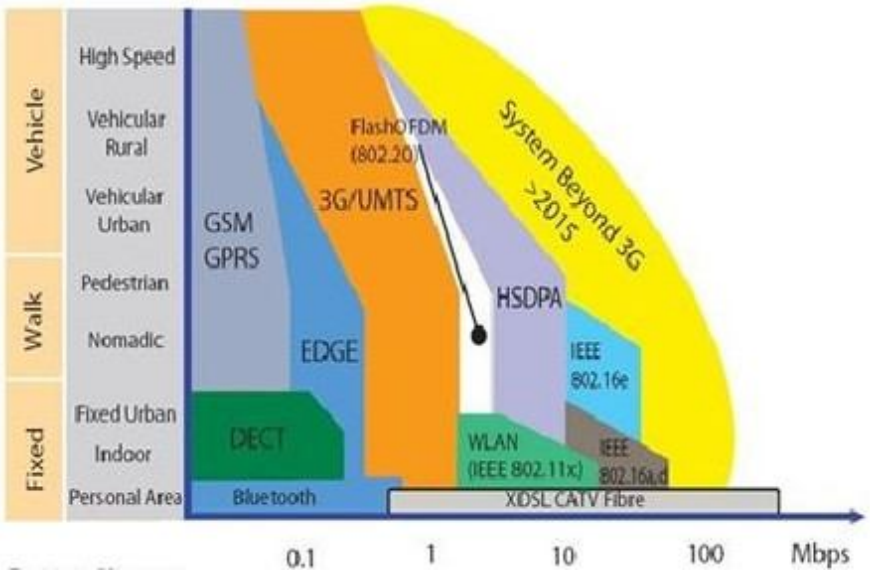
	802.16	802.16a	802.16e
Espectro	10 - 66 GHz	< 11 GHz	< 6 GHz
Funcionamiento	Solo con visión directa	Sin visión directa (NLOS)	Sin visión directa (NLOS)
Tasa de bit	32 - 134 Mbit/s con canales de 28 MHz	Hasta 75 Mbit/s con canales de 20 MHz	Hasta 15 Mbit/s con canales de 5 MHz
Modulación	QPSK, 16QAM y 64 QAM	OFDM con 256 subportadoras QPSK, 16QAM, 64QAM	Igual que 802.16a
Movilidad	Sistema fijo	Sistema fijo	Movilidad pedestre
Anchos de banda	20, 25 y 28 MHz	Seleccionables entre 1,25 y 20 MHz	Igual que 802.16a con los canales de subida para ahorrar potencia
Radio de celda típico	2 - 5 km aprox.	5 - 10 km aprox. (alcance máximo de unos 50 km)	2 - 5 km aprox.

Imagen 2 Cuadro comparativo Tasa de transferencia tecnologías inalámbricas



Fuente: SIMENS

Imagen 3 Cuadro comparativo Movilidad

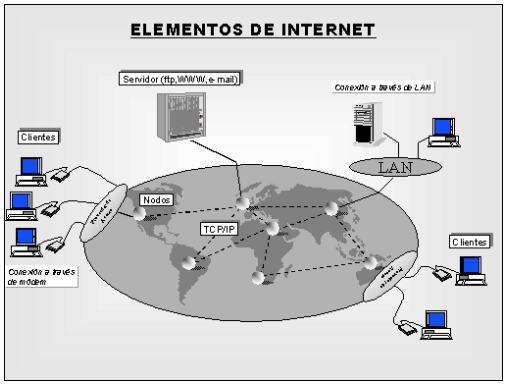


Fuente: SIMENS

3 PROVEEDOR DE SERVICIOS DE INTERNET

En esta sección del trabajo se describen los componentes principales de la infraestructura de un proveedor de servicios de Internet (ISP) y las directrices para el diseño de una arquitectura que satisfaga las necesidades de los usuarios.

Imagen 4 Elementos que intervienen en una conexión internet



Fuente: http://cockyytere1819.blogspot.es/i2009-06/

Un Proveedor de Servicio de Internet (ISP: Internet Service provider), es una empresa que ofrece a sus usuarios conexión a la red mundial Internet y su gama de servicios relacionados, tales como correo electrónico y navegación grafica, entre otros. Estos, para ofrecer sus servicios requieren de 2 conexiones:

- Conexión con la red internet (backbone),
- Conexión con el usuario de internet, que es proveído por las empresas que brinda infraestructura de acceso al ISP.

Desde el punto de vista del usuario, existen varias formas de conexión al ISP, y estas son:

- Bajo demanda o conmutado, que consiste en una conexión no permanente, entre la cual se destaca la conexión vía telefónica por ser la primera y la más común. Aquí se requiere marcar el número telefónico del ISP.
- Enlace dedicado o no conmutado, en la cual se tiene una conexión permanente las 24 horas del día. Se destacan: Enlace RDSI, ADSL, Cable módem, enlace satelital a enlaces inalámbricos, por ser servicios dedicados de banda ancha.

Sea cual sea el casa, es ISP salida al usuario a través de un nombre de identificación y una contraseña para verificar su acceso a la red y se le asigna una dirección IP temporal, para el acceso de conexión telefónica; o permanente, en el caso de un enlace dedicado. Hay que considerar que estas direcciones Ip son públicas.

La necesidad creciente de conectividad con Internet está imponiendo fuertes exigencias a los proveedores de servicios Internet, tanto en el número de conexiones de acceso de los usuarios como en los servicios que los usuarios requieren en cada conexión. La tasa de crecimiento del tráfico de Internet está en torno al 100 % anual, y hay una demanda creciente de aplicaciones que necesitan capacidades superiores a las de los servicios "best effort", exigiendo una mayor predecibilidad en la red. Entre estas aplicaciones podemos citar: Redes Privadas Virtuales de Nivel 3, Intranets, Extranets, Voz sobre IP, alquiler de aplicaciones, etc.

La calidad de servicio, incluyendo una rápida conectividad, es esencial en la prestación de servicios IP, de ahí que el diseño de las infraestructuras de los proveedores de Internet se caracterice actualmente por una elevada redundancia en todos los elementos - de alta escalabilidad y fiabilidad -, y por la presencia de múltiples enlaces de alta capacidad.

En el presente documento consideraremos el escenario más completo, es decir, el caso de un proveedor que disponga de infraestructura propia en los diferentes niveles de la red.

Se describen los componentes de la infraestructura y los principios típicos de diseño, así como algunas posibles evoluciones a medida que crezca la red, si bien es necesario indicar que en la práctica existen tantos diseños diferentes como ISP.

La estructura de red que se presenta sigue un modelo de red jerárquico que permite diseñar las redes por capas. La utilización de modelos jerárquicos presenta la ventaja de que la modularidad en el diseño permite crear elementos de diseño que se pueden replicar a medida que la red crece.

La estructura modular de la red también facilita el aislamiento de fallos y en consecuencia la operación de la red.

3.1 DESCRIPCIÓN DE LA INFRAESTRUCTURA[6].

Físicamente, Internet está compuesto por routers interconectados por enlaces de comunicación. Las redes IP más simples están formadas por unos pocos routers de propósito general interconectados por enlaces propios o alquilados. A medida que las redes se vuelven más complejas, con un número mayor de elementos, se requiere más estructura. Los elementos se especializan en sus aplicaciones, la gestión y la seguridad adquieren mayor importancia, la localización física es un factor a tener en cuenta, y la capacidad de manejar altas densidades de clientes es crítica.

Como los routers trabajan con direcciones de nivel 3, que tienen una estructura, al imponer una estructura jerárquica a una red los routers pueden

[6] Fuente: Infraestructura de un isp, Andoni Pérez de Lema Sáenz de Vigueras.

usar caminos redundantes y determinar rutas óptimas incluso en una red que cambia dinámicamente. Las estructuras de red jerárquicas también facilitan la separación de dominios de difusión.

Por otro lado, el mecanismo de enrutamiento del protocolo IP es el enrutamiento salto-a-salto (hop-by-hop) sin estado basado en el destino, que tiende intrínsecamente a agregar tráfico en las principales rutas troncales, lo que justifica la implantación de una estructura jerárquica. Un modo de imponer una estructura a una red compleja consiste en asignar tareas específicas a routers particulares. Una solución muy frecuente en las redes de ISP es realizar la siguiente división de routers :

• **Routers de concentración,** que proporcionan acceso a la red a los clientes individuales. Estos equipos tienden a centrarse en soportar números elevados de puertos de relativa baja velocidad conectados a los clientes.

• **Routers de backbone,** que proporcionan transporte óptimo entre nodos de la red, enviando paquetes a gran velocidad de un dominio a otro o de un proveedor de servicios a otro.

El énfasis se pone en alcanzar las mayores tasas de transmisión o forwarding rates sobre los interfaces más rápidos disponibles. Así pues, la infraestructura de red necesaria para proveer los servicios IP se puede descomponer a alto nivel en 4 partes:

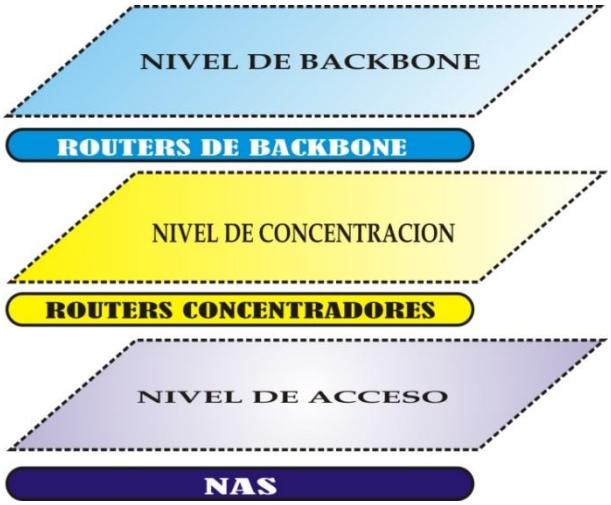
- Red de acceso.
- Red de concentración.
- Backbone o red troncal, que incluye la interconexión con otros proveedores y salida a Internet.
- Red de gestión, DNS, Radius/Autenticación. Estas aplicaciones críticas para un ISP se centralizan en un CPD o Centro de Proceso de Datos.

La mayor parte de los ISP también imponen una estructura física a sus redes organizándolas en Puntos de Presencia (POP). Un POP es una ubicación física donde se dispone, como veremos en los apartados siguientes, de una serie de equipos :

- Nodos de acceso o RAS.
- Routers concentradores de RAS.
- Routers concentradores de clientes con líneas dedicadas.
- Routers de backbone.

La interconexión de los usuarios con la red de datos del proveedor se realiza en estos POP. Actualmente, de acuerdo con esta estructura de red, en la mayor parte de las redes de los ISP se perfilan tres niveles jerárquicos de interconexión, como se muestra en la figura siguiente:

Imagen 5 Niveles jerárquicos de interconexión en un ISP



Fuente: Infraestructura de un isp, Andoni Pérez de Lema Sáenz de Vigueras, pag 3

A medida que se incrementen la capacidad de procesamiento y las funcionalidades de los routers, se tenderán a equiparar las funcionalidades de los routers de concentración y backbone.

No obstante, se cree que se mantendrá en el futuro la diferenciación entre los niveles de concentración y backbone, porque la eliminación de los routers troncales implicaría que los routers restantes tuvieran que comunicarse en una red mallada, sobrecargando el plano de control IP y limitando el crecimiento de la red.

3.2 RED DE ACCESO.

Los clientes pueden acceder por:

- **Líneas conmutadas o dial-up ,** que representan actualmente más del 90 % de los clientes. Este tráfico (sobre enlaces portadores + enlace señalización número 7) llega al Punto de Interconexión del operador de acceso, que está conectado con nuestra central de conmutación.

La central toma como argumento el número de destino y saca en interfaces primarios (ISDN PRI) el tráfico de Internet. Estos primarios se suministran a los equipos RAS (Remote Access Server) situados en los POP de la Red de Datos.

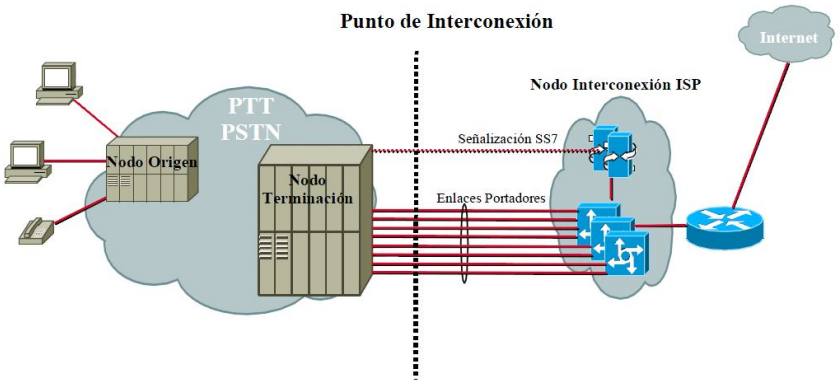
El usuario final dispone de un equipo de cliente (modem o router) que establece una sesión PPP con el RAS. El RAS es un dispositivo de acceso remoto que dispone de un pool de modems y que realiza funciones de cliente RADIUS, autentificando al usuario y terminando la sesión PPP. RADIUS es un estándar de Internet adoptado de manera generalizada en las situaciones en las que un dispositivo de acceso remoto necesita autenticar a un usuario de acceso conmutado frente a un servicio de directorio.

La salida del RAS se enlaza con un router concentrador de acceso mediante VLAN. Para incrementar el nivel de servicio se realiza un diseño redundante (ver figura 4), en el que cada RAS tiene dos salidas - una Fast Ethernet y otra Ethernet- y se conecta a dos VLAN. Cada una de las VLAN tiene conexión con dos routers concentradores de acceso diferentes.

Los RAS tendrán dos rutas por defecto. La ruta por defecto a través de la interfaz Ethernet tendrá una métrica superior a la ruta a través de la interfaz Fast Ethernet.

En los últimos años han surgido los gateways SS7. Estos equipos realizan las funciones de un RAS pero se pueden conectar directamente con señalización SS7 al punto de Interconexión, eliminando la necesidad de puertos de conmutación y de interfaces primarios. Además estos equipos permiten reducir la congestión de red y aumentar las tasas de conexión.

Imagen 6 Escenario de un proveedor con un Gateway SS7



Fuente: Infraestructura de un isp, Andoni Pérez de Lema Sáenz de Vigueras, pag 5

Para incrementar el nivel de servicio es conveniente considerar una doble conexión física entre el Gateway SS7 y el router.

- **Líneas dedicadas:** uno de los componentes de más rápido crecimiento del acceso a Internet es la conectividad entre negocios mediante líneas alquiladas. El tráfico de líneas alquiladas se define como DSO, N*64,

E1, E3 ó STM-1. En este caso los clientes disponen de un router que se enlaza directamente mediante una línea dedicada con un router concentrador de acceso, por el que entra a la red de datos del proveedor. El router concentrador de acceso realiza la agregación del tráfico procedente de líneas alquiladas.

El enlace entre el router de cliente y el router concentrador se soporta actualmente sobre anillos de fibra óptica de área metropolitana. Los POPs diseñados antes de la generalización de los interfaces SDH en los routers requerían una multitud de bastidores de DSU (data service units) para terminar E1 sobre pares de cobre tradicionales. Los routers concentradores de acceso actuales proporcionan una alta densidad de terminaciones para conexiones DS1 y DS3, de modo que una sola tarjeta de línea puede terminar cientos de circuitos DS1 transportados sobre una sola fibra.

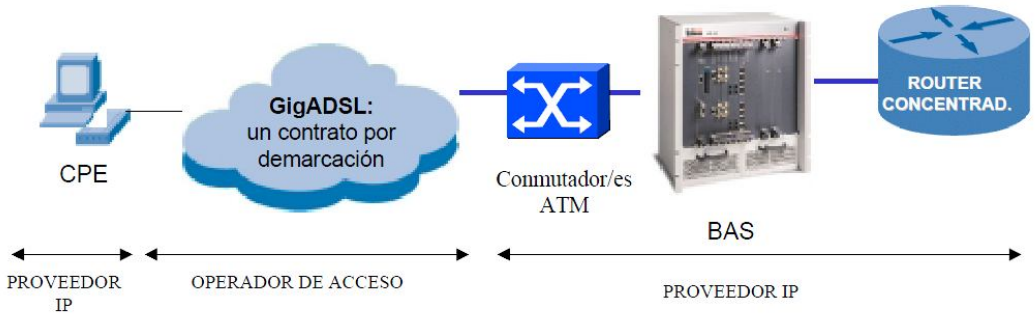
- **Líneas ADSL**, que permiten a los clientes disponer de acceso permanente de banda ancha sobre una línea telefónica convencional. El usuario es provisto de un equipo de cliente que incluye un módem ADSL. Este equipo se conecta al punto de terminación telefónica en el domicilio del usuario.

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 de conmutar las celdas ATM transportándolas hacia la red de acceso. El ISP de Internet se conecta mediante un enlace ATM al Punto de Acceso Indirecto (PAI) del operador de acceso, que establece un PVC (circuito virtual permanente) de ATM entre el usuario y el PAI.

Para soportar el acceso por líneas ADSL es necesario introducir en la red de datos un nuevo elemento denominado BAS o Broadband Access Server

(siguiente figura). Este equipo concentra el tráfico y actúa como frontera entre los niveles 2 y 3, teniendo funcionalidades de enrutamiento, autenticación y control de tráfico.

Imagen 7 Esquema de un ISP mediante ADSL



Fuente: Designing Large-Scale IP Internetworks, http:\\www.cisco.com

En las redes de ISP se tiende actualmente a desplegar ATM únicamente en el borde de la red, con la misión de agregar tráfico ADSL de los DSLAM, así como servicios de Frame Relay, en switches ATM. La mayor parte de ISP ya no despliegan ATM en la red troncal, que está basada íntegramente en IP. La demanda de servicios de ADSL exige que los conmutadores ATM tengan capacidad para soportar un número elevado de VC (circuitos virtuales). Los conmutadores ATM no estaban diseñados inicialmente para un contrato por demarcación soportar múltiples DSLAM, que pueden tener cientos de circuitos virtuales por cada circuito DSLAM-conmutador.

3.3 RED DE CONCENTRACION.

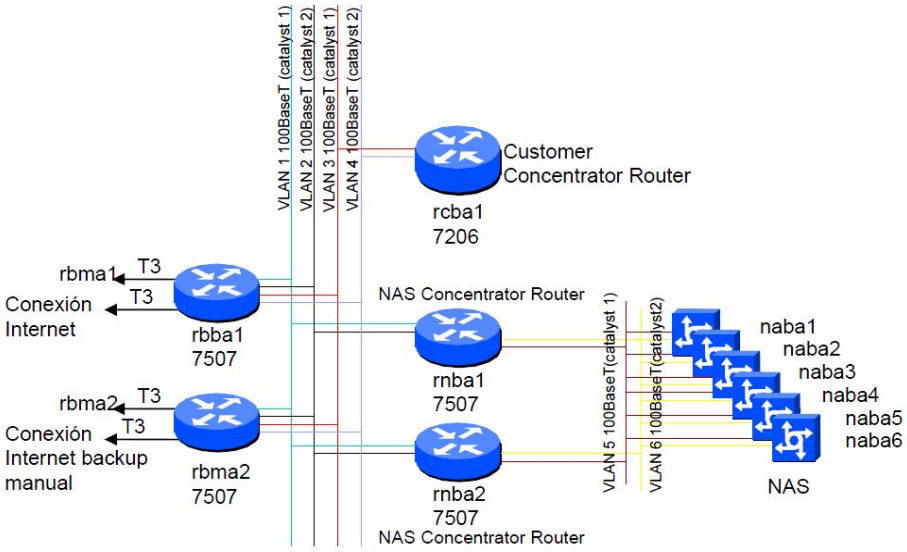
La misión de esta red, situada en el borde de la red de datos, es agregar las conexiones de los clientes en los puntos de presencia del proveedor. Dentro del POP, en el nivel de concentración tenemos dos tipos de routers de concentración, unos dedicados a la concentración de clientes conmutados y otros dedicados a la concentración de clientes dedicados.

Las características clave de los routers concentradores de acceso son:

- Escalabilidad y alto ancho de banda para satisfacer la demanda creciente de transmisión de datos, voz y video.
- Alta densidad de puertos para satisfacer el crecimiento continuado del número de clientes.
- Procesador optimizado para gestionar agregaciones de tráfico de gran volumen y nuevas funcionalidades software.
- Prestaciones de valor añadido adicionales al enrutamiento de paquetes de alta velocidad: redes privadas virtuales, seguridad con listas de acceso extendidas y firewalls, diferenciación de calidad de servicio, soporte multicast, etc.
- Mecanismos para flexibilizar las velocidades de acceso permitidas, como Multilink PPP. Este estándar de Internet (IETF RFC 1990) usa cabeceras de paquetes y procedimientos especiales para distribuir un único flujo de paquetes sobre varios enlaces en paralelo y recomponerlo en el extremo receptor. Esto permite a los clientes cuyas necesidades han sobrepasado una línea E1 (2Mb/s), utilizar varias líneas E1 en vez de pasar a una línea E3 (34 Mb/s), lo cual supone un salto excesivo. Este protocolo también se emplea para permitir que un cliente pueda conectarse a Internet utilizando a la vez los 2 canales B de un acceso básico RDSI.

Si tomamos el caso de los clientes dial-up, los routers concentradores disponen en ambos extremos de interfaces Fast Ethernet o Gigabit Ethermet con redundancia física, conectándose en un extremo a las VLAN de los RAS y en el otro extremo a las VLAN de los routers de backbone (ver siguiente figura). La siguiente figura representa la estructura y conexiones lógicas de un POP :

Imagen 8 Estructura y conexiones lógicas de un POP



Fuente: Designing Large-Scale IP Internetworks, http:\\www.cisco.com

Como vemos, en este escenario se emplea el switching Ethernet (tecnología IP/Ethernet) tanto en la interconexión entre el nivel de acceso y el de concentración como entre el nivel de concentración y el troncal.

Se puede optimizar este escenario reemplazando el switching Ethernet por enlaces punto a punto (tecnología PACKET OVER SONET) en la interconexión entre el nivel de concentración y el troncal. En este caso sería necesario disponer de GigaRouters en el nivel troncal con capacidad para concentrar un gran número de interfaces de fibra. Este nuevo escenario presentaría los siguientes beneficios:

1. Reducir el retardo de los paquetes en el POP, por la supresión del proceso de tramas (SWITCH LEVEL 2) entre la capa de concentración y la capa troncal.
2. Reducir puntos de fallo en la interconexión entre la capa de concentración y backbone.

3. Optimizar las interconexiones mediante un entorno VLAN conmutado entre la capa de acceso y concentración.

Volviendo a las características de los routers de concentración, estos deben disponer de funcionalidades de routing OSPF y BGP, y políticas de control de tráfico. En los bordes de la red la política de control de tráfico más empleada es CAR (Committed Access Rate), que limita la tasa máxima de tráfico transmitido o recibido, y también puede marcar la Precedencia IP de los paquetes. Los dispositivos del interior de la red pueden usar la precedencia IP para determinar cómo se trata el tráfico para entregar la calidad de servicio requerida, usando algoritmos de planificación como WFQ (Weighted Fair Queing).

DWRED (Distributed Weighted Random Early Discard) es un algoritmo inteligente de gestión de colas para tráfico TCP que establece en función de la precedencia IP la probabilidad de que un paquete sea descartado, evitando congestiones de los enlaces y mejorando su utilización. No es propiamente un mecanismo de control de congestión, sino más bien un mecanismo para prevención de congestiones, que evita la sincronización entre sesiones de transporte y las oscilaciones.

Sin embargo, la activación de estos mecanismos incrementa la carga en los procesadores de los routers, y limita por tanto el ancho de banda de los enlaces que son capaces de gestionar. Se pueden instalar en los routers módulos con procesadores adicionales para ejecutar estos algoritmos en modo distribuido, con lo que se podrían gestionar anchos de banda más elevados (45 Mb/s o incluso 155 Mb/s).

Si se desea implementar un control de tráfico más refinado en la red, se requieren mecanismos de diferenciación de servicios como Diffserv, o MPLS.

En cuanto a las políticas de Routing en la red de datos, los RAS implementan generalmente rutas estáticas y usan RIPv2 para la publicación de las direcciones de las sessiones PPP. Los routers concentradores de clientes "sumarizan" las direcciones que reciben por RIPv2 y las publican vía OSPF a los demás routers de la red.

Los routers de backbone no necesitan conocer cada red individual en el nivel de acceso. Por eso los routers concentradores, en lugar de anunciar al backbone una gran cantidad de información detallada sobre destinos individuales, "sumarizan" o concentran grupos de destinos del nivel de acceso en prefijos de ruta únicos más cortos, y anuncian estas rutas "sumarizadas" al backbone. Asimismo, esta técnica (address summarization) permite que cada vez que se produzcan cambios topológicos la información no tenga que ser transmitida por toda la red, sino sólo por la región de concentración local, y hace que las tablas de enrutamiento se reduzcan de modo significativo.

3.4 RED TRONCAL.

La red troncal se encarga de:

- Agregar el tráfico procedente de las redes de acceso y concentración.
- Interconexión con el resto de POP de la Red.
- Interconexión a otras Redes, proveedores de tránsito y puntos neutros.
- En uno de los POP se efectuará también la interconexión con el entorno del Centro de Proceso de Datos.

En la tabla siguiente contrastamos las principales diferencias entre los routers de concentración y los routers de backbone:

Tabla 6 Diferencias entre routers

VARIABLE	ROUTER BACKBONE	ROUTER CONCENT.
Throughput en paquetes/seg	Extemadamente alto	Alto
Conjunto de funcionalidades de procesamiento de paquetes	Mínimo, centrado en el reenvío rápido	Funcionalidades de alto valor añadido
Tipos de interfaces	Número modesto de interfaces de muy alta velocidad	Número elevado de interfaces de relativamente baja velocidad
Patrones de tráfico	Cualquier interfaz a cualquier interfaz	Predominantemente cliente-troncal y troncal-cliente

Las diferencias listadas en esta tabla no son absolutas, y frecuentemente un router concreto puede desempeñar ambos papeles. No obstante, a medida que el tráfico de Internet siga creciendo la exigencia de que los routers de concentración tengan una mayor densidad y los routers troncales manejen throughputs más elevados se irá acentuando.

Otra cuestión importante es que la existencia de un número de elevado de interfaces, es decir la densidad, en los routers de concentración mejora el rendimiento estadístico de la red. Ello es debido a que las redes de paquetes están diseñadas para aprovechar la multiplexación estadística, basándose en el hecho de que todos los enlaces no están activos al mismo tiempo.

El tener más enlaces disponibles reduce la probabilidad de que un pico de tráfico simultáneo de varias fuentes cause una congestión de red temporal.
Otros beneficios de la densidad son:

- El coste del metro cuadrado en un POP es elevadísimo. El gasto en alquiler de locales se rebaja al disminuir el número de bastidores necesarios para conectar un número elevado de clientes.
- La gestión de red se simplifica al desplegar un número menor de routers de mayor potencia. Disponer de menos routers individuales que configurar, gestionar y monitorizar produce una operación más eficiente.

3.5 EVOLUCION DE LOS ROUTERS E IMPLEMENTACIÓN DE MPLS.

Los routers están constantemente evolucionando y adquiriendo nuevas prestaciones. Las últimas tendencias de los principales fabricantes de routers, que denominan en la actualidad a a estos equipos NextGen Routers o routers de nueva generación, son las siguientes :

- **Routers de concentración:** se está integrando MPLS en los routers, para establecer en los bordes de la red la calidad de servicio. Los routers del backbone deberán soportarla. MPLS también permite ofrecer servicios customizados para Ethernet (por ejemplo, mapeo de VLAN a MPLS). Algunos fabricantes hablan de nuevos servicios de emulación de circuitos sobre IP, otros soportan funcionalidades de billing sofisticadas basadas en identidades de grupos de trabajo, aplicaciones o zonas geográficas.
- **Routers de backbone:** sus funcionalidades de gestión de tráfico evolucionan con la inclusión de MPLS, y sus capacidades se incrementan con la adopción de interfaces STM-64. La orientación a conexión de MPLS, a diferencia de IP, y la conmutación basada en etiquetas posibilitan las siguientes oportunidades :
- **Ingeniería de tráfico:** el enrutamiento salto a salto ("hop-by-hop") de IP no tiene por qué ser el más eficiente o adecuado, sobre todo teniendo en cuenta los requisitos actuales de calidad de servicio en Internet. Una de las principales ventajas que aporta la implantación de MPLS en la red de datos es la ingeniería de tráfico para optimizar la utilización de los enlaces entre los routers. En ausencia de ingeniería de tráfico, el tráfico IP sigue el camino más corto, ignorando rutas alternativas a través de la red. Esto conduce a cuellos de botella en enlaces fuertemente cargados ("hipergagregación"), mientras que otros enlaces permanecen infrautilizados. La utilización del enrutamiento basado en restricciones de red y caminos conmutados conduce a una red cargada de forma más

uniforme y permite realizar un control de congestión. Una red con ingeniería de tráfico basada en MPLS tendrá los enlaces igualmente cargados, dando como resultado una red con mayor robustez contra los picos de tráfico y unas mayores prestaciones globales.

- **Servicios de conectividad VPN multitecnología**. Los caminos conmutados de MPLS o LSP (Label Switched Path) permiten provisionar servicios de interconexión corporativos de forma segura, puesto que los paquetes son conmutados mirando sólo las etiquetas, sin entrar en el contenido IP ni de nivel superior. Esto es, MPLS permite transportar de forma transparente y conmutada cualquier tipo de información entre dos puntos. MPLS va a permitir, por consiguiente, proporcionar múltiples servicios de transporte de modo muy similar a como se pueden proporcionar mediante una red ATM.
- **Calidad de servicio:** por medio de los LSP's, se podrán proporcionar calidades de servicio diferenciadas, de modo similar a como se hace en ATM. Sin embargo, en la actualidad ATM tiene definidas calidades de servicio cuantitativas en los estándares, que son implementadas en "hard" e interoperables con los diferentes fabricantes, mientras que de momento MPLS sólo ofrece la promesa de proporcionar al tráfico IP un cierto nivel de calidad de servicio "soft".

  Esta se implementará inicialmente como un grado de priorización alta o baja en base a una clase de servicio (CoS) cualitativa, mediante una combinación de MPLS con el modelo de Servicios Diferenciados del IETF.

- **Posibilidad de ofrecer servicios orientados a conexión en entornos LAN/MAN**. MPLS permite ofrecer Redes Privadas Virtuales de Nivel 2 (también denominadas TLS o Transparent LAN Services), en las que el que el camino MPLS a través de la red del ISP es un circuito virtual entre dos ubicaciones de cliente. Los circuitos virtuales de nivel 2 son una red superpuesta (overlay) MPLS sobre la red troncal del proveedor.

En la terminología de las Redes Privadas Virtuales MPLS existen 3 tipos de routers :

- **Router de cliente o CPE**. La utilización de MPLS es completamente transparente a estos equipos. Los CPE intercambian rutas con la red en RIP (también pueden tener rutas estáticas) de manera transparente a MPLS.

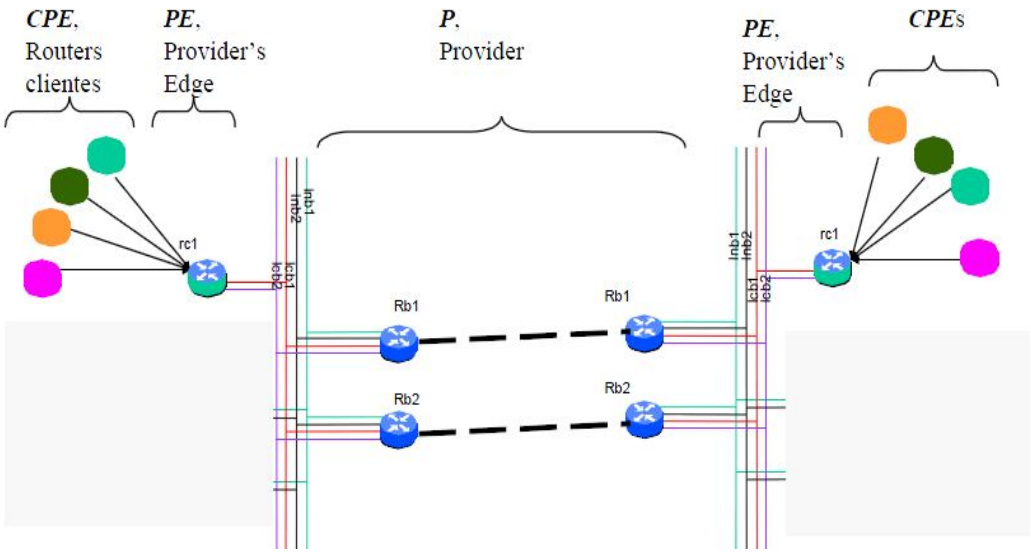
- **Provider Edge (PE) router**, ubicados en el borde de la red MPLS. Son los routers que tienen conocimiento de la Red Privada Virtual. Tienen conexión directa con los routers de los clientes e implementan una tabla de enrutamiento virtual (VRF, Virtual Routing and forwarding). Cuando el CPE envía un paquete al PE, el PE consulta la VRF para saber el PE al que enviará al paquete, y a continuación encapsula el paquete dentro de un LSP hacia este PE.

  Para mantener el nivel de seguridad necesario en una red privada virtual el ISP establece túneles L2TP entre el NAS y el PE.

- **P (Provider) router**, que forman el núcleo de la red MPLS. Sólo conocen los LSP. Los P conmutan los paquetes recibidos a través de la etiqueta más exterior que los encapsula, por lo que no tienen conocimiento de las Redes Privadas Virtuales. Su única función es conmutar los paquetes de cada LSP que los atraviesa.

Con la introducción de MPLS en la red de datos del ISP, los Routers Concentradores de acceso pasarán a actuar como PE y los Routers de Backbone harán funciones de P, como se refleja en la siguiente figura:

Imagen 9 Esquema de routers en un ISP



Fuente: Designing Large-Scale IP Internetworks, http:\\www.cisco.com

3.6 CONSIDERACIONES GENERALES DE DISEÑO

Para favorecer una alta calidad de acceso a Internet, la topología interna de la red de datos de un ISP se diseña de manera que el número máximo de saltos en toda la red es reducido (idealmente, 3). Asimismo, se utilizan equipos de altas prestaciones y se establecen políticas de routing que favorecen el reparto de carga entre todos los enlaces.

Se han realizado distintos modelos teóricos para optimizar el diseño de una red de paquetes en base a la reducción del retardo medio de tránsito. Este parámetro es crucial para las aplicaciones en tiempo real, multimedia y streaming. Las variables que se pueden ajustar en el diseño son la capacidad de los enlaces y la topología, y se considera como condición de contorno adicional el coste de la red.

Las topologías ideales que resultan son las de alta conectividad, es decir, aquellas que tienden a conectar los routers del backbone con todos los demás. El ejemplo extremo es la topología en malla, en la que el número medio de saltos en el backbone es 1.

Sin embargo, en esa topología el número de conexiones varía con el cuadrado del número de nodos. Por otro lado, una topología completamente mallada sobrecarga el protocolo de enrutamiento IGP (Interior Gateway Protocol) del ISP. Esta sobrecarga resulta del número de relaciones entre pares que es necesario mantener, del reto de procesar ncubo actualizaciones de estado de enlace en caso de un fallo, y de la complejidad de realizar el cálculo de Dijkstra sobre una topología con un número elevado de enlaces.

En la práctica se tiende a un compromiso, empezando con una topología de red suficiente para las necesidades del momento (por ejemplo, una topología en estrella con cada nodo de conexión con proveedores de tránsito, en la que el número medio de saltos en el backbone tiende a 2), y se va mallando en función de la utilización de los enlaces y de las necesidades cambiantes de los clientes.

Asimismo, se habilitan enlaces redundantes que protejan frente a la caída o saturación de los enlaces principales, y todos los enlaces se sobredimensionan para hacer frente al crecimiento del tráfico, toda vez que en la práctica desde la solicitud de un enlace a un operador de acceso hasta su disponibilidad transcurren varias semanas.

Para la conectividad internacional se dispone de varios proveedores de tránsito. La conexión con los proveedores de tránsito internacionales o puntos neutros nacionales se efectúa por POPs distintos, consiguiendo de este modo:

- Ofrecer un mejor balanceo de carga en el interior de la red , con la consiguiente mejora de calidad de servicio a los clientes al no centralizar en un único punto de la red todo el tráfico de Internet.
- Proteger el acceso internacional frente a desastres en un único POP.
- Los ISP simplifican el diseño y mantenimiento de la red usando un mismo patrón para todos sus POP. Un diseño de POP típico es el reflejado en la figura 8, que tiene las siguientes ventajas:
- Los routers de concentración y backbone están separados, por lo que la configuración de los routers de backbone puede permanecer relativamente estable en el tiempo. Los routers de backbone no se ven afectados cuando se añaden o eliminan clientes individuales de los routers de concentración, o cuando clientes individuales contratan servicios de valor añadido.
- Se emplean dos routers de backbone en cada POP para aumentar la disponibilidad de red.
- Hay redundancia en los enlaces entre los routers y entre los RAS y los routers de acceso, mejorando la disponibilidad de red.

- Se pueden añadir fácilmente routers de concentración a medida que crece el número de usuarios.

3.7 CENTRO DE PROCESO DE DATOS.

Alberga los servidores de : gestión de red IP, gestión de equipos de cliente, DNS, Radius. Todos ellos son sistemas de elevada disponibilidad en balanceo de carga, altamente escalables, y protegidos por firewalls.

Al tratarse de sistemas críticos, encontrar las causas de posibles fallos en el menor tiempo posible se convierte en una prioridad. En consecuencia, se

recomienda no instalar sistemas heterogéneos en un mismo segmento de LAN. Asimismo, es necesario realizar un diseño con el mínimo número de equipos entre la red de acceso y los servidores finales, para eliminar puntos de fallo.

En el caso de sistemas que lleven un tráfico reducido o no sean críticos (por ejemplo, sistemas de News) se puede reemplazar la instalación de un firewall por la implantación de listas de control de acceso (ACL) en los routers y la seguridad a nivel de sistema operativo.

En la figura 10 se representa un ejemplo de estructura de CPD de un ISP.
Como se ve, el CPD se conecta a un router del backbone por dos líneas redundantes y está compuesto por las siguientes redes de área local:

- **LAN de gestión**: incluye los servidores de gestión de red IP, gestión de equipos deL cliente, estadísticas y acuerdos de nivel de servicio, y máquinas de visualización. El acceso desde la red IP a esta LAN está protegido por un firewall dedicado.

- **LAN DNS/ Radius:** incluye los servidores de DNS principal, DNS caché y Radius. Debido a que esta LAN incluye los servidores más críticos, el acceso desde la red IP está protegido por dos firewalls dedicados en balanceo de carga. El balanceo de carga hace que la carga máxima posible se duplique.

Para tener una alta disponibilidad de servicio, se recomienda instalar un servidor DNS en cada POP, o al menos un servidor DNS en cada uno de los POP de más tráfico de la red. Por ejemplo, un ISP nacional podría instalar un DNS en Bogotá y otro en Bucaramanga, de tal manera que parte de los usuarios del territorio nacional tendrían como DNS primario Bogotá y la otra parte de los usuarios Bucaramanga, y como DNS secundario el DNS del otro POP.

Con esta estructura se ha conseguido separar el tráfico de gestión del resto del tráfico. Además, se puede aprovechar la presencia de dos firewalls en la subred de DNS y Radius para evolucionar posteriormente a un escenario con una LAN específica para DNS y otra para Radius, separando también estos dos tipos de tráfico.

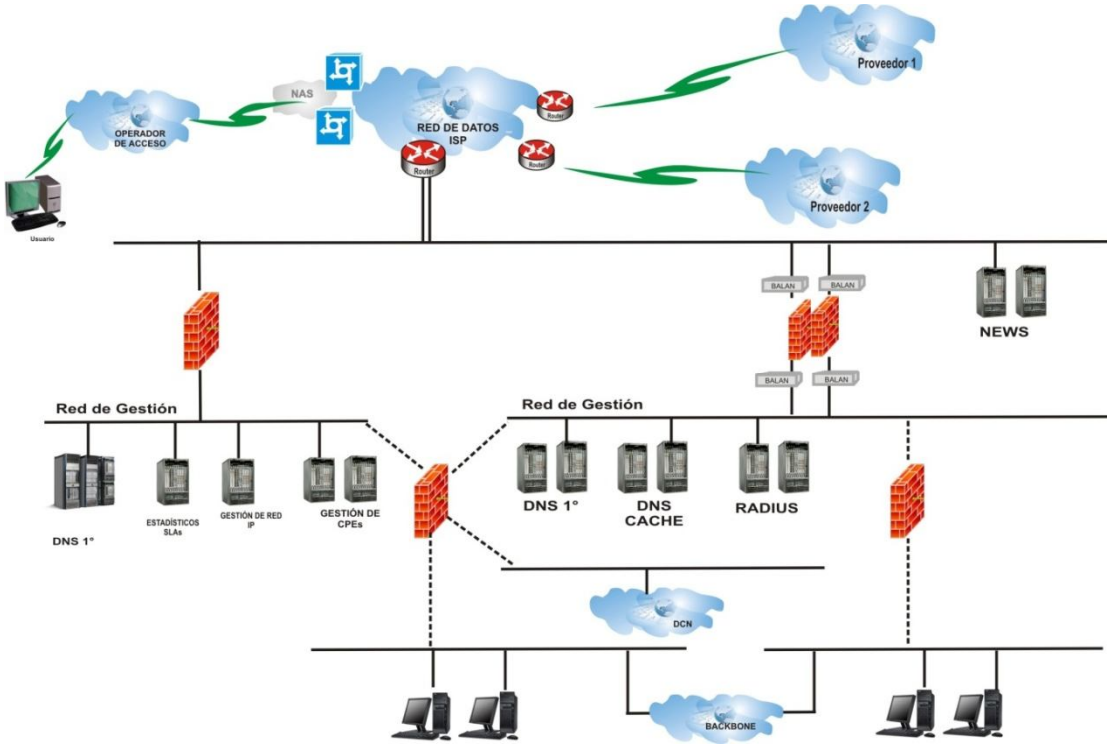
En la figura siguiente también se han representado las consolas ubicadas en dos centros remotos de operación de red, desde las que los operadores de la red realizan la operación y mantenimiento de la misma. El acceso se realiza sobre Redes Privadas Virtuales u otros enlaces encriptados, como Secure Shell (SSH).

A comienzos de los 90, las redes de ISP se componían de routers interconectados por líneas alquiladas -enlaces E1 (2 Mb/s) y E3 (34 Mb/s). A medida que Internet comenzó su crecimiento exponencial, los ISP respondieron a este reto provisionando más enlaces para proporcionar ancho de banda adicional.

En este contexto, la ingeniería de tráfico adquirió cada vez más importancia para los ISP, a fin de poder usar eficientemente el ancho de banda agregado cuando se disponía de varios caminos paralelos o alternativos[7].

[7] Infraestructura de un ISP, Andoni Pérez de Lema

Imagen 10 Estructura general de un ISP



Fuente: Infraestructura de un isp, Andoni Pérez de Lema Sáenz de Vigueras, pag 18

En las redes troncales basadas en routers, la ingeniería de tráfico se efectuaba simplemente manipulando las métricas de enrutamiento. El control de tráfico basado en métricas supuso una solución adecuada para la ingeniería de tráfico hasta 1994 ó 1995, momento en el que las redes adquirieron una dimensión tal que hacía cada vez más difícil asegurar que un ajuste de métrica en una parte de una red extensa no creaba un problema en otra parte de la red. Los routers de backbone no ofrecían los enlaces de alta velocidad ni el rendimiento determinista que los ISP requerían para el crecimiento planificado para sus redes troncales.

Además, el cálculo de rutas IGP estaba basado en la topología y en una métrica aditiva simple como el número de saltos o un valor administrativo. IGP no distribuía información como la disponibilidad de ancho de banda o las características del tráfico. Por consecuencia de esto, el tráfico no se distribuía equitativamente entre los enlaces de la red, causando un uso ineficiente de recursos costosos. Unos enlaces podían estar congestionados mientras otros seguían infrautilizados. En definitiva, la política más común entre los ISP para solventar estos problemas era sobredimensionar la capacidad de sus redes troncales, lo que no siempre era posible debido a las limitaciones de capacidad de los routers.

En 1995 el volumen del tráfico de Internet alcanzó un punto en el que los ISP necesitaban migrar sus redes para soportar enlaces troncales superiores a E3 (34 Mb/s). Afortunadamente, en ese momento aparecieron los interfaces ATM STM-1 (155 Mb/s) en conmutadores y routers. Los ISP se vieron forzados a rediseñar sus redes para poder usar las mayores velocidades soportadas por una red troncal ATM. Después de un período de un año, los enlaces entre conmutadores ATM se tuvieron que actualizar a STM-4 (622 Mb/s).

Los ISPs que migraron a redes troncales ATM comprobaron que los PVC (circuitos virtuales permanentes) de ATM proporcionaban una herramienta que permitía efectuar un control preciso del tráfico que fluía por sus redes. Los ISP confiaban en los interfaces de alta velocidad, el rendimiento determinista, y la funcionalidad de PVC de los conmutadores ATM para gestionar con éxito la operación de sus redes.

Una red troncal basada en ATM soportaba la ingeniería del tráfico, porque permitía enrutar explícitamente PVCs. Esto se efectuaba provisionando una topología virtual arbitraria por encima de una topología física de red dada, en la que los PVC se definían con el fin de distribuir precisamente el tráfico entre todos los enlaces de modo que estuvieran igualmente cargados.

Actualmente, sin embargo, las características que eran exclusivas de ATM (interfaces de alta velocidad, rendimiento determinista, ingeniería del tráfico mediante definición de PVC) se pueden encontrar también en los routers de backbone.

Estos avances han hecho que los ISP se replanteen continuar con un modelo de red superpuesta IP / ATM, cuya principal limitación es que requiere gestionar dos redes diferentes, una infraestructura ATM y un overlay lógico IP. Asimismo, el enrutamiento y la ingeniería de tráfico se producen en dos tipos de sistemas diferentes - enrutamiento en los routers e ingeniería del tráfico en los conmutadores ATM -, por lo que resulta muy difícil integrar completamente el enrutamiento y la ingeniería de tráfico.

Además, ATM tiene limitaciones debido a la función SAR (ensamblado y reensamblado de segmentos), que hace que la velocidad máxima de los interfaces ATM disponibles en los routers sea inferior a la disponible en las jerarquías más elevadas de SDH. Los fabricantes raramente ofrecen interfaces ATM superiores a STM-16 (2,5 Gb/s).

Por lo demás, una red superpuesta IP / ATM con una malla completa de PVC tiene importantes problemas de escalabilidad, porque las conexiones varían con el cuadrado de los nodos, y por la sobrecarga resultante sobre IGP.

La alternativa de MPLS supone un mecanismo flexible y prometedor para soportar ingeniería de tráfico, calidad de servicio extremo y enrutamiento

basado en políticas sobre las redes de ISP. MPLS provee una clara separación entre el enrutamiento y la conmutación, y permite el despliegue de un único plano de control -MPLS- que puede utilizarse para múltiples servicios y tipos de tráfico, y sobre distintas redes -incluyendo SDH, DWDM, ATM e IP. En el futuro, a medida que los ISP necesiten desarrollar nuevos servicios, la infraestructura MPLS podrá mantenerse cambiando simplemente el modo de asignar paquetes a un LSP.

MPLS todavía no se ha desplegado masivamente en las redes de los ISP porque los routers concentradores desplegados anteriormente carecen del rendimiento, escalabilidad y capacidad de proceso por flujo necesario para implementarlo eficazmente. En paralelo a los avances en el hardware, la próxima generación de routers concentradores inteligentes con soporte de MPLS podrá actuar como PE y examinar flujos de tráfico individuales, proporcionando las funciones de calidad de servicio y forwarding a la velocidad del cable que requieren los ISP para poder implantar sus servicios.
Las principales incertidumbres en torno a MPLS son la escalabilidad de las redes privadas virtuales, debido a la dimensión que adquirirían las tablas de enrutamiento en los PE con cientos o miles de clientes conectados, y la interoperabilidad entre distintos fabricantes, que es un requisito necesario para la interconexión de redes.

Por otro lado, las redes IP/MPLS no están preparadas todavía para soportar toda la gama de servicios de ATM, y aunque el tipo de tráfico que crece más rápidamente en la actualidad es IP, los servicios de ATM y Frame Relay siguen creciendo. Para aquellos proveedores que disponen de una plataforma ATM, y quieren desarrollar nuevos servicios IP manteniendo el soporte de sus servicios ATM y Frame Relay, se ha creado la funcionalidad "Ships In The Night" en los conmutadores ATM.

"Ships In The Night" permite la coexistencia de un plano de control ATM y un plano de control MPLS en el mismo equipo. Los dos planos de control son co-residentes en el mismo equipo, pero operan independientemente y simultáneamente sobre cada puerto. Esto permite a los ISP introducir MPLS gradualmente en la red, dividiendo una red física ATM en dos topologías disjuntas - una mantenida por el plano de control ATM tradicional y otra por el plano de control MPLS.

4 PROVEEDOR DE SERVICIOS DE INTERNET INALAMBRICO (WISP)

El Proveedor deservicios Internet inalámbrico (WISP) es un sistema de red de área metropolitana (MAN) integrado para conectar clientes al Internet con conexiones inalámbricas de alta velocidad. estas conexiones pueden ser punto a punto o punto-multipunto, y puede ser implementado en compañías, organizaciones gubernamentales, colegios, universidades y otras instituciones que tengan Redes des Área locales (LAN).

Las conexiones inalámbricas toman el lugar de las líneas dedicadas ó arrendadas, líneas telefónicas y conexiones DSL, donde las mismas no son posibles, son lentas o son demasiado caras. El Sistema de ISP Inalámbrico es un servicio terrestre que opera como una MAN con células de 8 a 10 Km. de radio de acción. Además, es un servicio bi-direccional, donde ambos, el cliente y el nodo central envían y reciben datos.

Un WISP es un servicio inalámbrico fijo entre el nodo central y el cliente. No es un servicio móvil, porque:

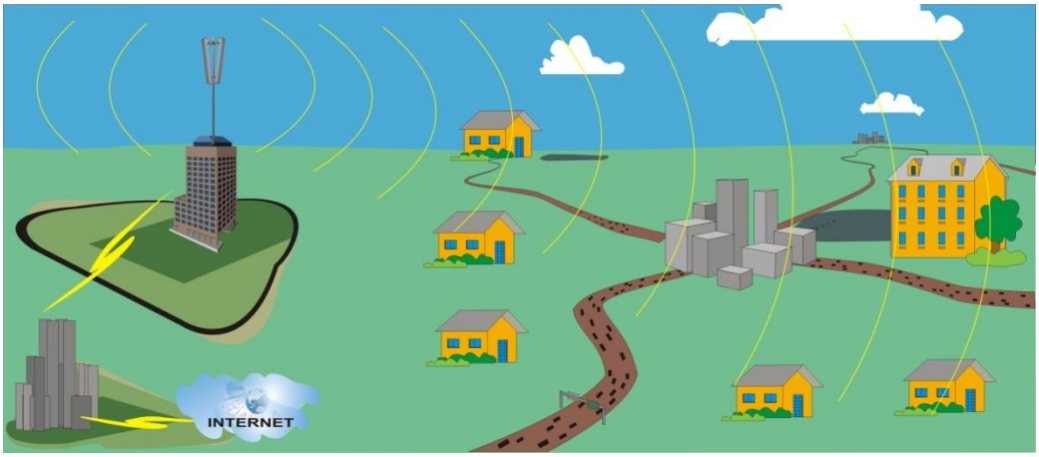
- Se requiere una línea de vista directa entre el nodo central y el cliente, y;
- Se usan radios de baja potencia y antenas de alta ganancia para los enlaces inalámbricos.

4.1 COMO INICIAR UN WISP?[8]

Como se ha mencionado anteriormente, un proveedor de servicios de internet inalámbrico, ISP, es un sistema de red de área metropolitana integrado para conectar clientes a la Internet. Las conexiones inalámbricas de alta velocidad se usan para proveer acceso a Internet punto a punto ó punto multipunto en compañías, organizaciones gubernamentales, colegios, universidades y otras instituciones que tienen Redes del Área Locales (LAN). Este sistema va dirigido a todas aquellas personas y empresas que necesitan un acceso a Internet más rápido y confiable.

Las redes de acceso inalámbrico, entre las que se figuran el WLL, LMDS yMMDS, han nacido como una alternativa a las redes físicas terrestres de banda ancha, De fibra óptica o híbridas de fibra y coaxial, y a las tecnologías que suplantan el viejo par de cobre (tecnologías XDSL), ante las limitaciones que éstas presentan para responder a las necesidades y demandas de la nueva sociedad.

Imagen 11 Muestra del alcance de un WISP



Fuente: autores

Para poder ser un proveedor de servicios de internet inalámbrico, se deben cumplir ciertos requisitos básicos, los mismos que detallaremos a continuación:

[8] Fuente: http://www.ldc.usb.ve/~figueira/Cursos/redes2/em01/EXPO-em01/LMDS_WLL/

La primera y principal característica es la de ya ser un proveedor de servicios de internet plenamente constituido. Es decir, debe cumplir todos los requisitos mencionados en el capítulo anterior respecto a cómo iniciar un ISP. Es un paso fundamental pues, con esto se puede decir que:

Primero que todo, se debió haber cumplido todo lo expuesto, con respecto al diseño, seguridades, acceso a internet, gestión, flexibilidad y protección y recuperación de la inversión, para así brindar un servicio que sea de calidad y rentabilidad aceptable.

- Se debe cumplir con todos los requisitos legales y normas que rigen en el marco de las telecomunicaciones a nivel local, para proveer este tipo de servicios a los usuarios, así como de tener los respectivos permisos de funcionamiento, uso de frecuencias, uso de equipos, etc.
- Se debe tener experiencia en ofrecer servicios de internet a un usuario final mediante un tipo de conexión dada: dial-up, enlace dedicado o enlaces de banda ancha. De este modo se podría decir que este ISP ya cuenta con un número dado de usuarios, a los que se ha sabido ofrecer el servicio.
- Se debe tener una conexión permanente a internet de por lo menos, unos 128kbps. Es decir, no necesariamente debe tener ni proveer una conexión de banda ancha.
- Se debe tener un servidor de nombres de dominio (DNS), servidores de correo, de servicios HTTP y FTP, que son servidores quienes ofrecen a los usuarios los distintos servicios provenientes desde internet.
- Debe poseer un rango de direcciones o bloques IP públicas, asignados por el ARIN (Registro Americano de Números de Internet), los que se distribuirán entre las redes constituidas por el cable troncal (backbone) local y los usuarios finales.

En caso de que la empresa no haya sido un proveedor de servicios de internet, pues se recomienda que lo sea, o que entienda lo que es un proveedor de servicios de internet, o bien, se debe recibir asesoramiento por parte de personal calificado y capacitado.

En el caso de que ya sea un ISP, o por lo menos ya entienda lo que implica el serlo, así como de haber cumplido con los requisitos básicos, para pasar a proveer internet inalámbrico, se debe considerar también lo siguiente:

- Considerar que un WISP es un servicio inalámbrico fijo, no móvil, por ello, no deben operar en la banda de telefonía celular.
- Se requiere de una línea de vista entre el nodo central y el cliente. A grandes distancias, esto representa problemas debido a la curvatura de la tierra. En este caso, se requieren hacer los estudios de propagación respectivos.
- En cuanto a los equipos, se deben usar radios de baja potencia y antenas de alta ganancia, éstas deben estar ubicadas en lugares altos y despejados, para así poder tener una línea de vista directa.
- En caso de sobrepasar la distancia óptima de operación, se deben usar repetidores para recuperar la señal. Un nodo debe tener línea de vista directa con un nodo repetidor.
- En cuanto a configuración de redes, networking, se debe considerar a la red inalámbrica como otra red o subred que opera bajo el protocolo TCP/IP, por lo tanto, será similar a configurar una red cableada.
- Se deben tener los permisos de uso de frecuencias en las bandas a las cuales trabajan tanto WLL, LMDS y MMDS, aunque por el momento, estas bandas están libres y no necesitan licencia.
- Se deben preparar bien los sitios para las instalaciones tanto en el lado del proveedor como en el lado del cliente, cumpliendo todos los requisitos de seguridad y protección de los equipos, antenas, cables y conectores,

contra descargas eléctricas o condiciones ambientales, como la humedad.

De seguro, quien cumple con todos estos requisitos, será un proveedor de servicios de internet inalámbrico, lo que resta, es hacer los estudios respectivos, los análisis técnicos, estudiar los estándares que rigen en este tipo de redes, elaborar un diseño, adquirir los equipos y los servicios, y por último, realizar la implementación del prototipo y ponerlo en marcha. En base a todo esto, es que un proveedor se diferenciará de otro y el cliente distinguirá la calidad de servicio y el precio que ofrezca determinado proveedor y se sabrá inclinar por el cual éste considere el mejor, analizando la relación costo-beneficio, de acuerdo a sus necesidades. Aquí radicará la diferencia y por eso, en el próximo capítulo presentaremos un diseño, el cual consideramos que será óptimo, eficiente y barato.

La tecnología Wi-Fi ha sido un "boom" también en las casas (si se tiene más de un computador), pues Wi-Fi permite que todas las máquinas compartan el internet sin necesidad de tender cable alguno.

El Wi-Fi también puede tener aplicaciones militares, siempre y cuando se aseguren de que nadie va a espiar la información transmitida (pues es incómodo hacer un tendido de cable en una guerra, por ejemplo). En este caso, las regulaciones deben ser más estrictas que para un usuario común o un cyber.

No es ningún secreto que una red Wi-Fi sin modificar posee agujeros gigantes de seguridad. Aunque no ha habido escasez de ataques en las redes tradicionales, las redes inalámbricas son más vulnerables a los hackers, puesto que la información se transmite a través del aire. Si éstos usan el equipo adecuado, pueden colectar suficiente información como para descifrar contraseñas o claves de encriptación, particularmente en redes ocupadas con mucho tráfico. Además, seres inescrupulosos pueden usar estas contraseñas para meterse en un acceso a internet de una organización, o incluso interceptar comunicaciones.

En las redes tradicionales, la única seguridad existente es la contraseña de red que se pide (la que una empresa proporciona a cada empleado para entrar a la red corporativa, por ejemplo). En un ambiente inalámbrico, el usuario también necesita verificar que está accediendo desde la red correcta. Es decir, antes de ingresar el "user" y el "password", se debe estar seguro de que está en la red correcta y de que nadie más haya creado un punto de acceso en un parqueadero (por ejemplo) y haya "secuestrado" a la red de este usuario. En Febrero del 2003, se empezaron a certificar productos Accesos protegidos a Wi-Fi. Se está trabajando además, en mejorar la seguridad integrada a los accesos inalámbricos.

En conclusión, 802.11b se ha convertido en el único estándar desplegado para redes públicas de corto alcance, tales como las que hallamos en aeropuertos, hoteles, cybers, centros de conferencias o restaurantes. Varias compañías ofrecen este servicio en tarifas por horas, por consumo o ilimitado mensual. Por ello, y pese a los criterios de seguridad mencionados anteriormente, se prefiere la tecnología inalámbrica, porque es mucho más barato que hacer un tendido de cables (en un salón de clase por ejemplo).

4.2 ANALISIS TECNICO PARA UNA SOLUCIÓN WISP

4.2.1 Como funciona un wisp?

Como una solución de banda ancha el WISP provee acceso a Internet de alta velocidad a través de una conexión inalámbrica fija y un puerto dedicado al backbone de la red mundial, por ello, la ventaja radical de un proveedor de servicios de internet inalámbrico respecto al alámbrico está sin duda en el hecho de no depender de cableado alguno para llegar al usuario. Sin embargo, debido a que se trata de un servicio de banda ancha, la parte del backbone y de la conexión con el proveedor internacional es bastante similar a la de un proveedor de servicios de internet de banda ancha, los cuales ya analizamos con detalles en el capítulo anterior.

Los equipos que aquí se utilizan cumplen el estándar IEEE 802.11. El backbone principal de estas redes está formado por una serie de nodos que disponen de conexión a Internet de banda ancha (cable, o ADSL generalmente). Los nodos más pequeños, los que no disponen de conexión a Internet, se conectan con los primeros mediante una tarjeta de red inalámbrica y una antena direccional. Así estos nodos hacen las funciones de repetidores. De esta manera cada uno de los nodos principales tiene a su alrededor una serie de nodos secundarios que permiten la conexión de cualquier usuario en un radio de aproximadamente 100 metros. Finalmente los usuarios finales se conectan con sus equipos y tarjetas de red inalámbricas a cualquiera de estos nodos.

Los nodos por lo general dispondrán de antenas omnidireccionales para expandir la señal inalámbrica por toda la zona. Las antenas direccionales se utilizarán para apuntar directamente hacia un punto en concreto, recordando que debe haber línea de vista entre las antenas transmisora y receptora.

Estas son las utilizadas para conectar con nodos lejanos, dado que aumentan la distancia a cubrir hasta unos 3 o 4 Km, según el modelo.

Como ya se indicó anteriormente, hemos visto que existen dos tecnologías de redes inalámbricas, una que utiliza la banda de 5,8 Ghz y otra la banda de 2,4 Ghz. Las condiciones de propagación de las señales radioeléctricas en esas bandas determinan la aplicabilidad de estas tecnologías. Así, la de 5,8 Ghz tiene un alcance desde una estación base de 5 a 10 Km, lo que significa que para atender la demanda de una determinada área geográfica hacen falta instalar muchas estaciones base. La de 2,4 Ghz tiene un alcance de 10 a 15 Km, lo que permite atender la demanda en dicha área con 3 a 5 veces menos estaciones base. Sin embargo, la tecnología de 5,8 Ghz es capaz de ofrecer capacidades de transmisión de hasta 54 Mbps, mientras que la de 2,4 Ghz limita su capacidad a 22 Mbps. La aplicación destinada dependerá de la tecnología utilizada.

El acceso al Internet es ilimitado y siempre está disponible, es decir, el servicio puede ser entregado de forma dedicada, con ancho de banda disponible las 24 hrs. La conexión compartida entre el ISP y el cliente, comienza desde 128kbps, y es simétrica, esto quiere decir que las velocidades de transmisión son iguales en ambas direcciones: de subida y de bajada. El enlace inalámbrico punto a punto puede soportar velocidades equivalentes a fracciones de un T1 (1.544Mbps), hasta velocidades equivalentes a un STM-1 (155.52Mbps), con una conexión directa al Backbone de Internet.

El diseño de una red inalámbrica es una cuestión de hacer coincidir los componentes idóneos con sus necesidades de conexión en red. En todo diseño de red inalámbrica hay dos módulos de montaje fundamentales: la infraestructura y las tarjetas cliente.

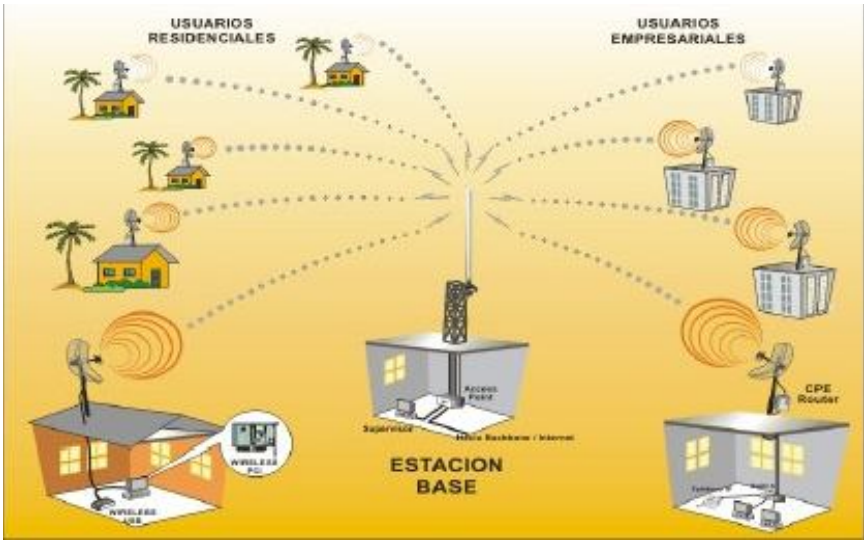
En cuanto a la infraestructura, los dispositivos que la conforman funcionan como conductos de datos para componentes de una red inalámbrica. Asimismo, sirven de puente entre la red inalámbrica y una red conectada existente. La pasarela inalámbrica y los puntos de acceso inalámbrico pueden tener un puesto en el diseño de la red, según los datos exclusivos y las necesidades de red de una empresa individual. La pasarela inalámbrica es utilizada en pequeñas empresas, en cambio que los puntos de acceso se emplean en empresas medianas, grandes o en crecimiento.

En cuanto a las tarjetas para el cliente, todas las redes la deben usar y ésta debe ser inalámbrica, como por ejemplo, tarjetas Airport, tarjetas para portátiles, tarjetas PCI, entre otras.

El adaptador proporciona el enlace entre el ordenador y la red, y también convierte los datos a un formato que la red puede utilizar. La elección del adaptador depende del tipo de dispositivo que se utilice. El adaptador, como cualquier otro adaptador de red alámbrica, le proporciona una dirección física o dirección de capa 2, la cual debe ser reconocida por cualquier otro dispositivo en la red.

En teoría, conectarse a una de estas redes debería de ser algo tan simple como llegar con una portátil y una tarjeta WLAN. En la práctica esto no es tan sencillo, puesto que, además de la falta de compatibilidad WiFi de muchos equipos, cada nodo mantiene su propia política de acceso. Esta política está condicionada a las particularidades de cada nodo, ancho de banda y rendimiento de los equipos. Una vez instalada la tarjeta WLAN en los equipos, es necesario configurar una serie de parámetros que dependerán de cada proveedor y de cada equipo.

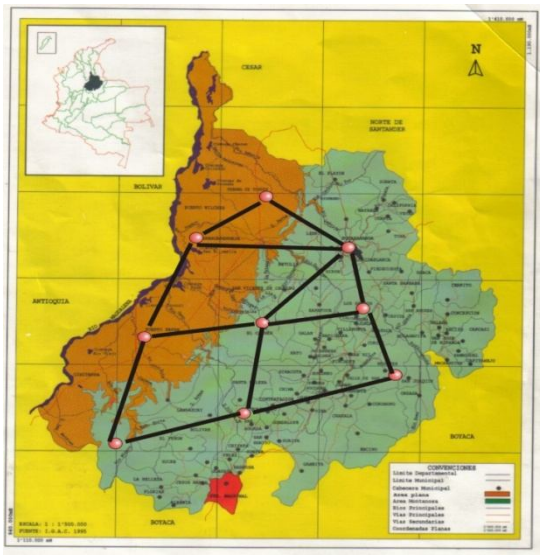
Imagen 12 Esquema de una conexión inalámbrica desde una estación base



Fuente: http://tamax.com.ar/blog/?p=158

Un proveedor de servicios de internet inalámbrico, basados en una plataforma IP de alta velocidad, está soportado en nodos distribuidos en zonas estratégicas de una localidad geográfica determinada, los mismos que están interconectados por un Backbone de alta velocidad.

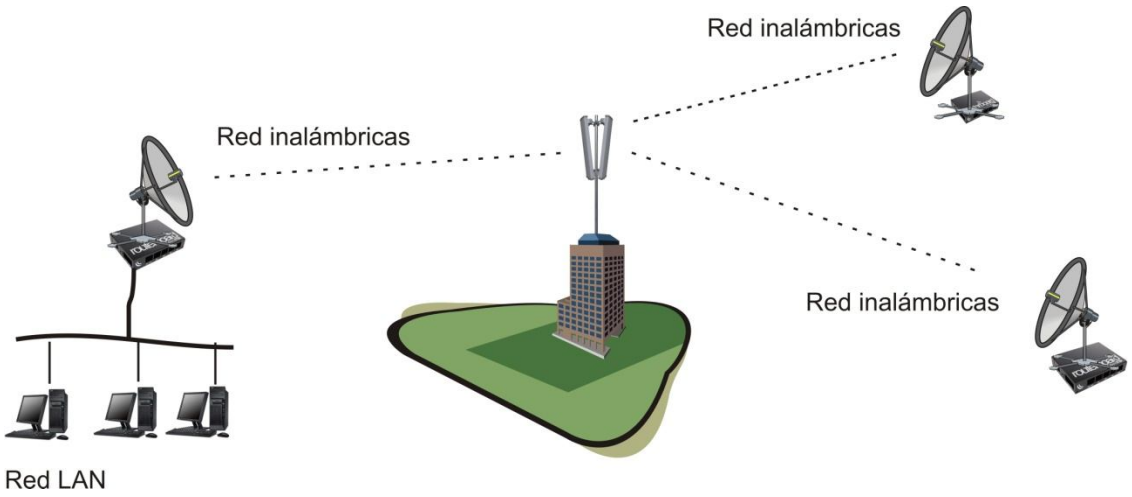
Imagen 13 Distribución de nodos en un área geográfica



Fuente: Autores

Los nodos son parte fundamental en cualquier red de telecomunicaciones, son los encargados de realizar las diversas funciones de procesamiento que requieren cada una de las señales o mensajes que circulan o transitan a través de los enlaces de la red. Desde un punto de vista topológico, los nodos proveen los enlaces físicos entre los diversos canales que conforman la red.

Imagen 14 Enlace multipunto desde un punto de acceso hacia clientes fijos

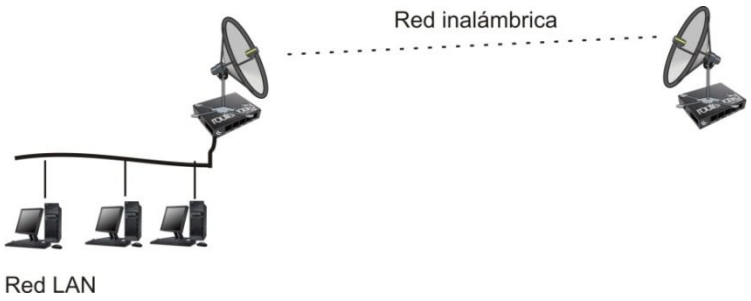


Fuente: Autores

En este tipo de enlace se vincula varios puntos (remotos) congruentes en uno solo (punto central). Dentro del esquema de nodos o puntos de acceso, tenemos otro tipo de esquemas en aquellas aplicaciones donde deseamos realizar una conexión con un ancho de banda determinado o un canal dedicado con algún cliente que así lo requiera.

En este tipo de enlace se vincula varios puntos (remotos) congruentes en un solo (punto central). Dentro del esquema de nodos o puntos de acceso, tenemos otro tipo de esquemas en aquellas aplicaciones donde deseamos realizar una conexión con un ancho de banda determinado o un canal dedicado con algún cliente que así lo requiera.

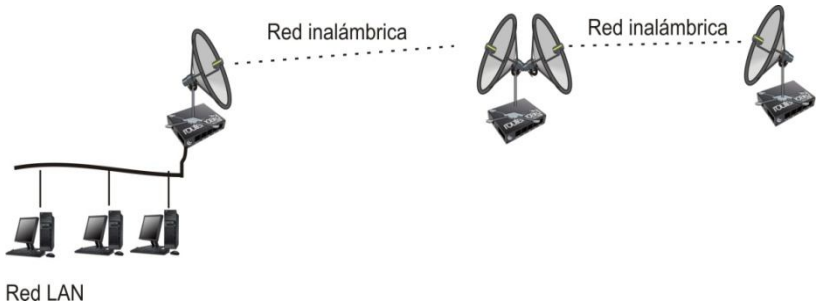
Imagen 15 Enlace punto a punto entre el ISP y cliente dedicado



Fuente: Autores

Las conexiones punto a punto son las que conectan directamente dos puntos entre sí, por ejemplo sucursales de una empresa. Este tipo de conexiones se puede realizar dentro de un mismo edificio, o dos puntos en distantes en la misma ciudad o diferentes ciudades hasta más o menos 50 Km.

Imagen 16 Enlace usando repetidores



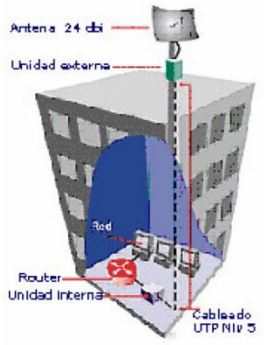
Fuente: Autores

Cuando queremos enlazar ciudades o puntos muy lejanos entre sí se puede utilizar otro punto intermedio desde el que podemos retransmitir una señal. Se debe tener en cuenta que estos esquemas son abiertos a la posibilidad de combinarlos entre sí y nos permite enlazar redes punto a punto con redes punto a multipunto, etc. Cada punto de una red inalámbrica puede poseer también una Red LAN que necesiten compartir su información con el resto de la red inalámbrica. Con esto se puede ofrecer enlaces punto a punto y punto a multipunto para soluciones de voz, datos, video y servicios de Internet. La

red de un WISP, se basa en tecnología inalámbrica con frecuencia de banda ancha dinámica para Internet, datos, voz y transmisiones de video.

Es una conexión permanente y directa desde un punto dado hasta el punto de acceso del ISP y permite capacidades desde 64 Kbps hasta 94 Mbps. La asignación de direcciones IP públicas fijas para servidores: HTTP, Mail, FTP y enrutadores, le permite estar permanentemente en la red mundial de internet. Cada dispositivo transmite y recibe en la frecuencia de 2,45 GHz (2,402 hasta 2,480 GHz en saltos de 1 MHz) basado en el estándar IEEE 802.11 para LAN inalámbricas.

Imagen 17 Esquema general de un usuario



Fuente: www.google.com, imágenes isp

Las conexiones son 1:1 con un rango máximo de 4Km., aunque utilizando amplificadores se puede llegar hasta los 10 Km, pero se introduce alguna distorsión. Sin embargo, un esquema de "frequency hopping" (saltos de frecuencia aleatorios) permite a los dispositivos comunicarse en áreas donde existe gran interferencia electromagnética (el hecho de que los paquetes sean más cortos y los saltos más rápidos reducen el impacto nocivo de otros dispositivos que trabajan en la misma banda), y provee mecanismos de encriptación (con longitud de clave hasta 64 bits) y autenticación, para controlar la conexión y evitar que cualquier dispositivo no autorizado pueda acceder a los datos o modificarlos.

4.2.2 Medios sobre los cuales funciona un wisp

Como se ha venido tratando desde el inicio de este capítulo, el medio físico a través del cual va a viajar la información entre usuario e ISP es el aire. Esto evita el molesto cableado existente entre el proveedor y los usuarios, lo único que se necesita es cumplir ciertos requisitos que son necesarios en un medio de transmisión inalámbrica, tales como:

- Línea de vista entre el cliente y el proveedor, entre cliente y el repetidor, o entre proveedor y repetidor (si se da el caso), es decir, sin obstrucciones físicas, climáticas o electromagnéticas;
- Autorización para el uso de una frecuencia por parte de la regulación local, que dependerá del tipo de tecnología inalámbrica a emplear;
- Que el radio de acción de este tipo de enlace no sobrepase de los 10 o 12 Km. para así no disminuir notablemente la señal transmitida.

Sin embargo, el hecho de que el ISP sea inalámbrico no equivale a decir que todo se va a prescindir completamente de cables, por ejemplo el medio para el backbone o red troncal puede ser un enlace satelital o se puede usar fibra óptica, como ya se analizó anterior mente. Así mismo en el lado del usuario este puede tener una red de acceso local dentro de sus dependencias (WLAN), o bien puede ser un solo punto.

4.2.3 Técnicas de acceso al medio[9]

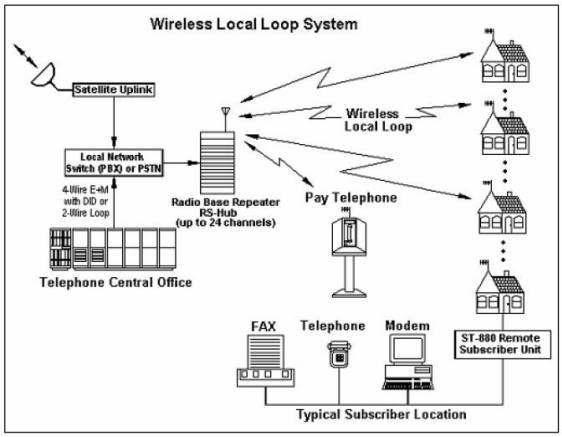
En cuanto a las técnicas o métodos de acceso inalámbrico, los sistemas que se presentan y desarrollan en la actualidad para el acceso a los servicios de banda ancha son los siguientes:

[9] Fuente: http://upcommons.upc.edu/pfc/bitstream/2099.1/4575/1/memoria.pdf

4.2.3.1 WLL (Wireless Local Loop: Se trata de un medio que provee enlaces locales sin cables. Mediante sistemas de radio omnidireccional de bajo poder, WLL permite a las operadoras una capacidad de transmisión mayor a 1 Megabit por usuario y más de 1 Gigabit de ancho de banda agregado por área de cobertura.

La principal característica de WLL es que proporciona un servicio alternativo a la telefonía alámbrica, por ello, es altamente beneficioso para los operadores que entran en mercados competitivos, dado que éstos pueden llegar a los usuarios sin tener que pasar por las redes de los operadores tradicionales. Por último, los costos de despliegue y de mantenimiento son relativamente bajos. Estas ventajas hacen de WLL, una solución altamente competitiva. Las principales tecnologías que maneja WLL pueden ser: tecnología celular (GSM. TDMA, CDMA), Servicios de comunicaciones personales (PCS) y telefonía sin cables.

Imagen 18 Acceso a internet vía WLL



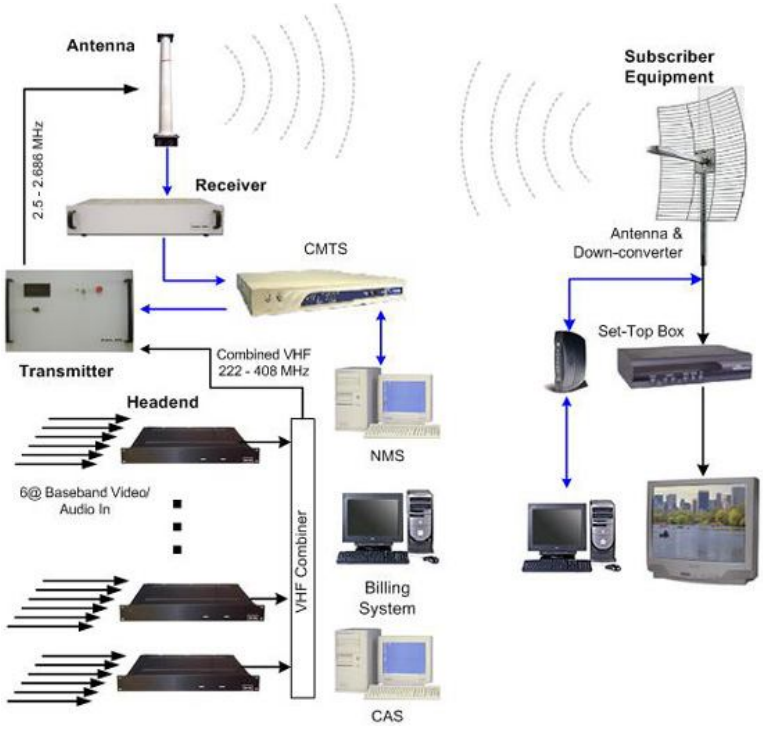
Fuente: http://www.cableaml.com/esp_wirelesstriple_integrated_system_description.html

4.2.3.2 MMDS (Multichannel Multipoint Distribution Systems): Es un sistema inalámbrico para la difusión de datos mediante señales de radiocomunicaciones de microondas punto a multipunto funciona a frecuencias entre 2 y 3 GHz, aunque la asignación de un ancho de banda

específico depende de la regulación de cada país. El radio de cobertura puede ser de hasta 120 Km en terreno llano (y bastante menor en zonas onduladas o montañosas).

Cada abonado del sistema está equipado con una pequeña antena y un convertidor que puede situarse cerca del aparato receptor de televisión convencional o encima del mismo. MMDS estaba orientado a entornos rurales o de baja densidad, en donde el tendido de cable convencional para distribución de TV podía resultar antieconómico, por ello, a esta tecnología se la denomina también cable inalámbrico. Sin embargo, también puede utilizarse para proporcionar comunicaciones integradas de voz, vídeo y datos.

Imagen 19 Acceso a internet vía MMDS



Fuente: http://www.cableaml.com/esp_wirelesstriple_integrated_system_description.html

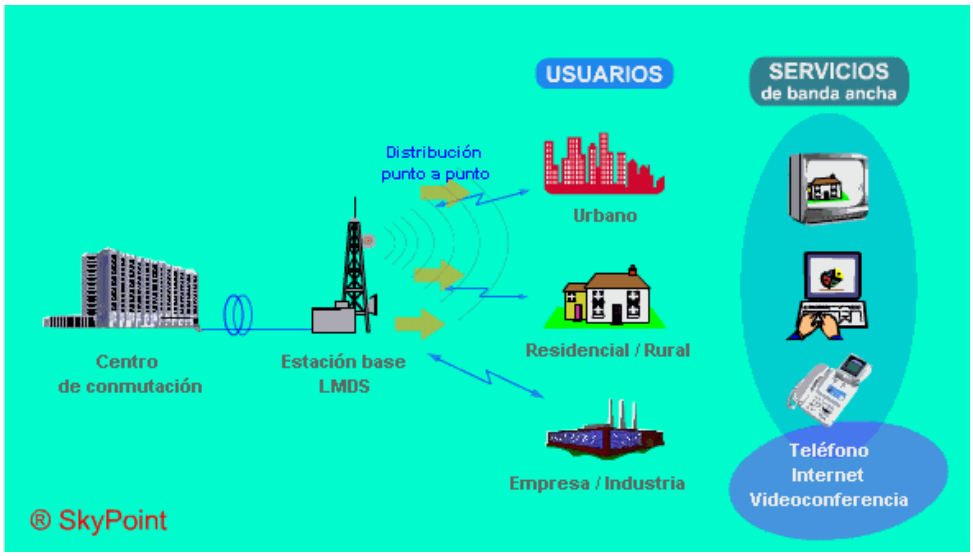
4.2.3.3 LMDS (Local Multipoint Distribution Systems): Es una tecnología similar al MMDS, pero con más potencial para la interactividad con

el usuario debido a su mayor ancho de banda. Este sistema opera a frecuencias superiores a 26 GHz, aunque su distancia de operación es bastante inferior en relación al MMDS, puesto que solo operan a radios inferiores a 6 Km.

A diferencia de los MMDS, los sistemas LMDS no llegaron a desarrollarse en la práctica para la aplicación inicialmente concebida de distribución de TV, viéndose rápidamente su gran potencial como solución de acceso de gran capacidad en aplicaciones de voz y datos, de Internet y de vídeo, con una velocidad de transmisión de 54 Mbit/s.

Debido al gran ancho de banda que maneja, a más de la atenuación que puede darse por el factor distancia, hay que considerar el factor clima, puesto que, a estas frecuencias una simple lluvia puede producir una gran atenuación.

Imagen 20 Acceso a internet vía LMDS



Fuente: SkyPoint

4.2.3.4 Spread Spectrum: La última milla de banda ancha inalámbrica utiliza un desarrollo basado en esta técnica, cuya idea es la de transmitir

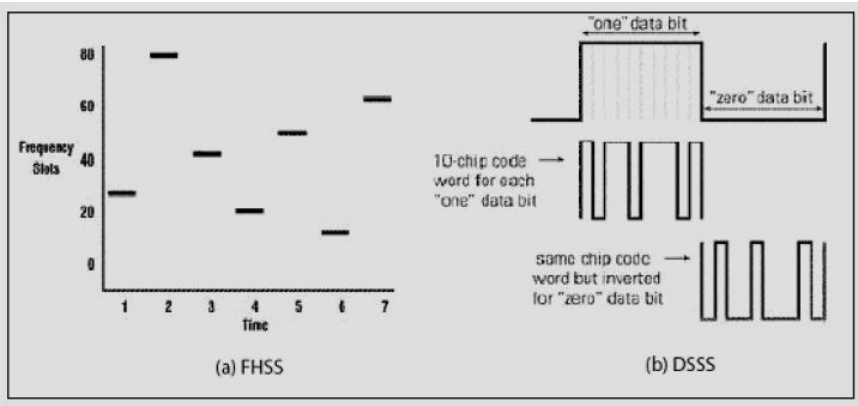
ocupando una banda de frecuencias mayor que la requerida. Trabaja en 3 bandas de frecuencias: 902 – 928 MHz, 2400 – 2483.5 MHz y 5725 – 5850 MHz, siendo las 2 últimas bandas, las que trabajan con los estándares de la familia 802.11x. Existen 2 tipos de transmisión

4.2.3.5 FHSS (Frecuency Hopping Spread Spectrum): la cual transmite en diferentes bandas de frecuencias, saltando de una a otra, pero de forma predecible. Tanto el dispositivo emisor, como el receptor deben compartir el generador de números aleatorios. El estándar 802.11 establece 75 bandas de 1MHz.

4.2.3.6 DSSS (Direct Sequence Spread Spectrum): El cual usa un "multicódigo", que es una técnica que permite transmitir varios bits por cada bit de información real para expandir el espectro.

4.2.3.7 Esta técnica también permite corregir posibles errores en la transmisión. El estándar 802.11 permite un multicódigo de 11 bits para proporcionar 2 Mbps, mientras que el 802.11b utiliza la modulación CCK para proporcionar 11 Mbps.

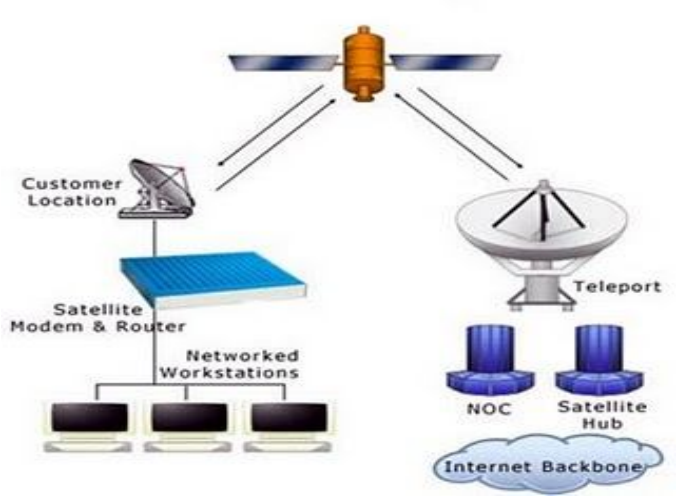
Imagen 21 Técnicas de acceso a internet vía espectro ensanchado



Fuente: http://sites.google.com/site/comunicacionesiiingtelecom/unidad-v-2

4.2.3.8 Acceso por satélite: En zonas rurales o en lugares donde no existe un enlace terrestre para el acceso por marcación a un punto de presencia Internet, el acceso a Internet por satélite puede ser una gran opción.

Imagen 22 Acceso a internet vía satélite



Fuente: http://www.cableaml.com/esp_wirelesstriple_integrated_system_description.html

En estos sistemas, los usuarios rurales acceden a Internet a través de una conexión por satélite bidireccional. Hay que considerar que los costos de explotación del segmento espacial, teniendo en cuenta que el costo es por ancho de banda y tiempo de uso del satélite, así como los costos producidos en la estación terrena: módems, antenas, multiplexores, etc., pueden representar un gasto considerable. Sin embargo, hay que tener en cuenta que cada vez están apareciendo sistemas por satélites más modernos y menos costosos. El alquiler de la capacidad del satélite puede extrapolarse adecuadamente a las necesidades del usuario permitiendo el acceso a la cantidad exacta de anchura de banda necesaria sin que ello suponga un gasto significativo de capital. El ancho de banda asignado a este tipo de enlace es variable y depende de los requerimientos del usuario, y que va a partir de los 128 Kbit/s.

En este proyecto nos centraremos en las primeras 3 técnicas, dado que un acceso a internet vía satélite, la cual también definimos, constituye una solución demasiado costosa para el cliente y para el proveedor, por lo que no resultaría conveniente, considerando que sólo se usa en casos extremos, es decir, en lugares de difícil y casi imposible acceso por algún medio físico.

4.2.4 Protocolos

Mediante los protocolos se define la forma de transmisión de información usando ondas radioeléctricas, entre los protocolos que rigen en las transmisiones inalámbricas tenemos:

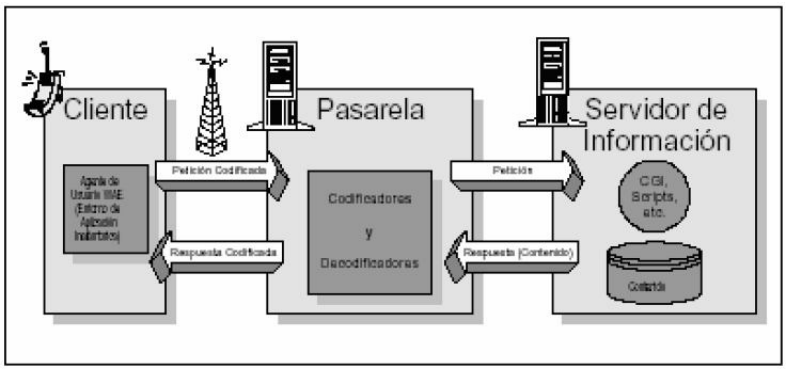
El Protocolo de Aplicaciones Inalámbricas o WAP, surge como la combinación de dos tecnologías de amplio crecimiento y difusión durante los últimos años:

Las Comunicaciones Inalámbricas e Internet. Más allá de la posibilidad de acceder a los servicios de información contenidos en Internet, el protocolo pretende proveer de servicios avanzados adicionales como, por ejemplo, el desvío de llamadas inteligentes, en el cual se proporcione una interfaz al usuario en el cual se le pregunte la acción que desea realizar: aceptar la llamada, desviarla a otra persona, desviarla a un buzón vocal, etc.

Para ello, se parte de una arquitectura basada en la arquitectura definida para el World Wide Web (WWW), pero adaptada a los nuevos requisitos del sistema: De esta forma, en el terminal inalámbrico existiría un “micro navegador” que actúe de interfaz con el usuario de la misma forma que lo hacen los navegadores estándar. Este micro navegador está encargado de la coordinación con la pasarela. Una vez procesada la petición de información en el servidor, se envía esta información a la pasarela que de nuevo procesa adecuadamente para enviarlo al terminal inalámbrico.

La función de la pasarela es codificar y decodificar la información intercambiada con el cliente, para así minimizar la cantidad de datos radiados, así como minimizar el proceso de la información por parte del cliente, la pasarela realiza peticiones de información que son adecuadamente tratadas y redirigidas al servidor de información adecuado.

Imagen 23 Modelo del funcionamiento del WAP



Fuente: http://www.cableaml.com/esp_wirelesstriple_integrated_system_description.html

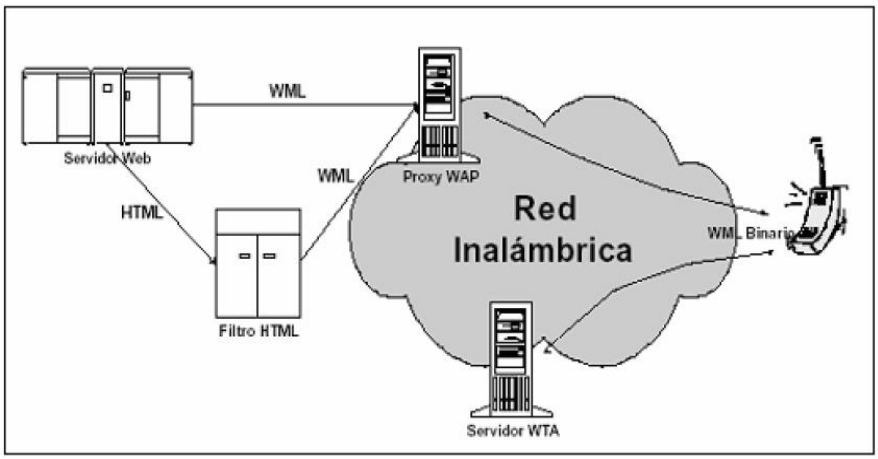
Un agente de usuario es todo aquel software o dispositivo que interpreta un contenido, como en el caso de WML. Esto incluye navegadores de texto, navegadores de voz, sistemas de búsqueda, etc.

Para conseguir consistencia en la comunicación entre el terminal móvil y los servidores de red que proporcionan la información, WAP define un conjunto de componentes estándar:

- Un modelo de nombres estándar, en las que se utilizan las URIs (Universal/Uniform Resource Identifier) definidas en WWW para identificar los recursos locales del dispositivo tales como funciones de control de llamada y las URLs (Universal/Uniform Resource Location) también definidas en el WWW para identificar el contenido WAP en los servidores de información.

- Un formato de contenido estándar, basado en la tecnología WWW.
- Unos protocolos de comunicación estándares, que permitan la comunicación del micro navegador del terminal móvil con el servidor Web en red.

Imagen 24 Ejemplo de una red WAP



Fuente: http://www.cableaml.com/esp_wirelesstriple_integrated_system_description.html

En el ejemplo de la figura, nuestro terminal móvil tiene dos posibilidades de conexión: a un proxy WAP, o a un servidor WTA. El primero de ellos, el proxy WAP traduce las peticiones WAP a peticiones Web, de forma que el cliente WAP (el terminal inalámbrico) pueda realizar peticiones de información al servidor Web.

Adicionalmente, este proxy codifica las respuestas del servidor Web en un formato binario compacto, que es interpretable por el cliente. Por otra parte, el segundo de ellos, el Servidor WTA (Wireless Telephony Application) está pensado para proporcionar acceso WAP a las facilidades proporcionadas por la infraestructura de telecomunicaciones del proveedor de conexiones de red.

La arquitectura WAP está diseñada de tal forma que proporcione un “entorno escalable y extensible para el desarrollo de aplicaciones para dispositivos de comunicación móvil”. Para ello, se define una estructura en capas, en la cual cada capa es accesible por la capa superior así como por otros servicios y aplicaciones a través de un conjunto de interfaces muy bien definidos y especificados.

Imagen 25 Arquitectura del WAP

Fuente: http://members.tripod.com/a_pizano/html/cap4.html

4.2.5 Topologías inalámbricas

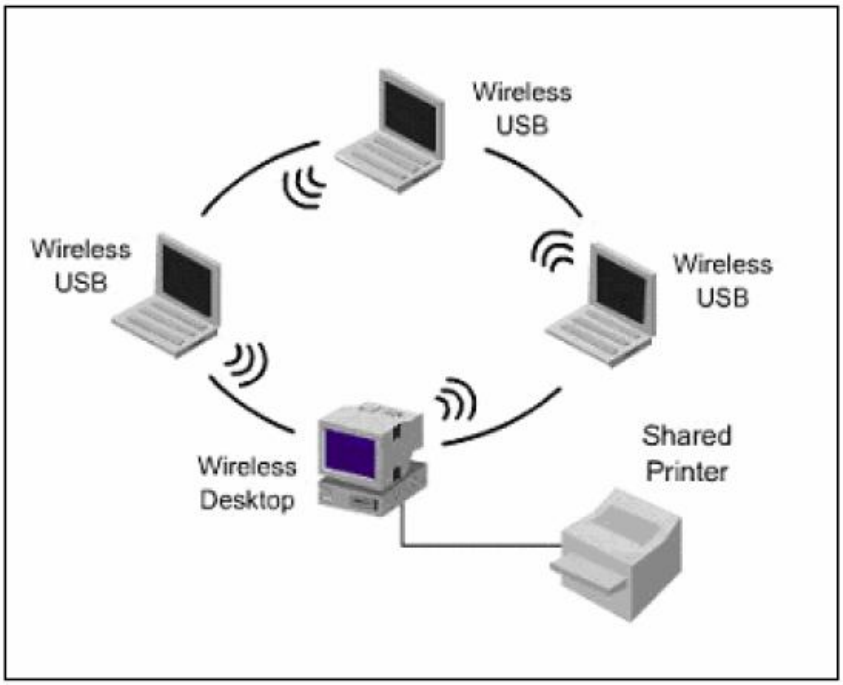
Es conveniente el hacer una división entre la topología y el modo de funcionamiento de los dispositivos Wi-Fi. Con topología nos referimos a la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos, mientras que el modo de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida. En el mundo inalámbrico existen dos topologías básicas:

4.2.5.1 Topología Ad-Hoc: En esta topología, cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red Peer to

Peer o de igual a igual, para lo cual sólo vamos a necesitar el disponer de un SSID o identificador de red inalámbrica, que debe ser igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento.

4.2.5.2 A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre si. No se requiere de puntos de acceso.

Imagen 26 Topología de acceso Ad-Hoc



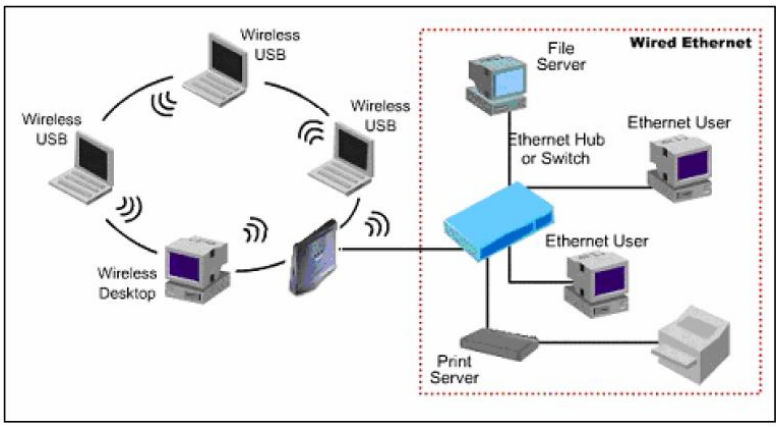
Fuente: http://www.cableaml.com/esp_wirelesstriple_integrated_system_description.html

4.2.5.3 Topología Infraestructura: En este caso existe un nodo central (Punto de Acceso Wi-Fi) que sirve de enlace para todos los demás (Tarjetas de Red Wi-Fi). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas.

Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del Punto de acceso. Esta topología es más

eficaz que el Ad-Hoc, puesto que hay mayor confiabilidad en el envío de paquetes, y además, su velocidad de transmisión es mayor.

Imagen 27 Topología de acceso Infraestructura



Fuente: http://wifiw.com/2010/02/topologia-de-red/

Existe una variante de esta última, denominada Roaming, en la cual se colocan varios puntos de acceso inalámbricos con el mismo SSID, de forma que un cliente puede pasar a trabajar con uno o con otro. Así se crean áreas de cobertura básicas y áreas de cobertura superpuestas, donde se elige automáticamente con qué punto de acceso inalámbrico se trabaja.

4.2.6 Equipos utilizados

En lo que respecta al equipamiento, así como en el funcionamiento, todo WISP consta de 2 partes importantes: el backbone, cuya estructura es similar a la de un ISP cualquiera, por ende su equipamiento es bastante similar; y, la red de acceso al usuario, en donde se marca la real diferencia, puesto que aquí debemos considerar todos los equipos necesarios para realizar un enlace inalámbrico.

En lo que respecta al backbone, tenemos como componentes principales:

- Router de banda ancha, que nos brindará la conexión con la red internet.

- Administrador de ancho de banda, para garantizar un ancho de banda determinado a cada nodo.
- Switch de capa 3, para segmentar la red interna.
- Firewalls, para brindar seguridad a nuestra red y a nuestros clientes.
- Servidores: DNS, de datos, http, Mail, de noticias, FTP, SMTP, Web.
- Componentes para enlace satelital, tales como antenas, módems, amplificadores, entre otros.

En lo relacionado al enlace netamente inalámbrico, esto es, hacia el cliente, los componentes principales son los siguientes:

Tarjetas de red, o Tarjetas Wi-Fi: Estas serán las que tengamos adaptadas en nuestro ordenador, o bien integradas mediante un conector PCMCIA ó USB si estamos en un portátil o en un slot PCI si estamos en un ordenador de sobremesa. Estas sustituyen a las tarjetas de red Ethernet o Token Ring a las que estábamos acostumbrados. Recibirán y enviarán la información hacia su destino desde el ordenador en el que estemos trabajando. La velocidad de transmisión / recepción de los mismos es variable dependiendo del fabricante y de los estándares que cumpla.

Puntos de Acceso, o Access Points: Es el equipo en donde se conectan los equipos de la red y son éstos quienes reparten los paquetes. En sí un Punto de acceso es un dispositivo que gestiona los paquetes lanzados por otras estaciones inalámbricas, haciéndolas llegar a su destino. Complementan a los Hubs, Switches y Routers, es más, los puntos de acceso pueden sustituir a los últimos pues muchos de ellos ya incorporan su funcionalidad, como Routers inalámbricos.
La velocidad de transmisión / recepción de los mismos es variable, las diferentes velocidades que alcanzan varían según el fabricante y los estándares que cumpla.

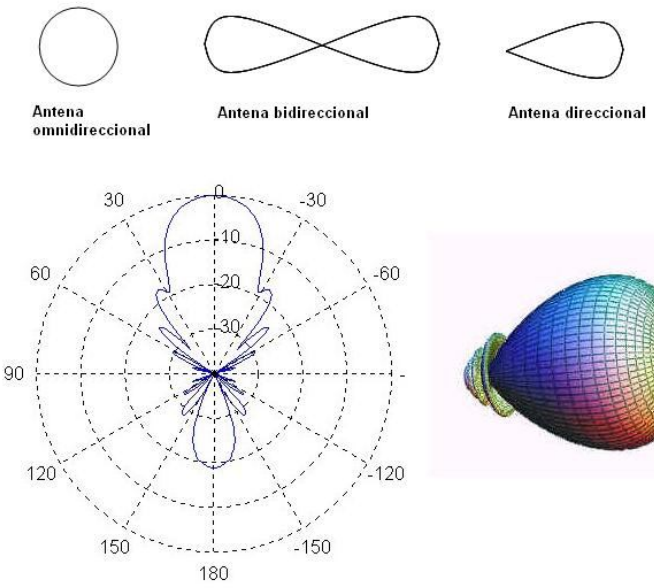
Antenas: Se encuentran dentro de los puntos de acceso, y también se aplican para las tarjetas de red inalámbricas, son dispositivos capaces de modificar enormemente la capacidad de transmisión/recepción de la señal.
Para el presente proyecto se andará un poco en las antenas, sus características y tipos

4.2.7 Parámetros de una antena[10]

Las antenas se caracterizan por una serie de parámetros, estando los más habituales descritos a continuación:

4.2.7.1 Diagrama de radiación (Patrón de radiación): Es la representación gráfica de las características de radiación de una antena, en función de la dirección (coordenadas en azimut y elevación). Lo más habitual es representar la densidad de potencia radiada, aunque también se pueden encontrar diagramas de polarización o de fase.

Imagen 28 Diagrama de radiación



[10] http://electromagnetic-fields.wikispaces.com/ANTENAS

Fuente: http://electromagnetic-fields.wikispaces.com/ANTENAS

Atendiendo al diagrama de radiación, podemos hacer una clasificación general de los tipos de antena y podemos definir la directividad de la antena (antena isotrópica, antena directiva, antena bidireccional, antena omnidireccional,…) Dentro de los diagramas de radiación podemos definir diagrama copolar aquel que representa la radiación de la antena con la polaridad deseada y contrapolar al diagrama de radiación con polaridad contraria.

Los parámetros más importantes del diagrama de radiación son:

- Dirección de apuntamiento: Es la de máxima radiación. Directividad y Ganancia.
- Lóbulo principal: Es el margen angular en torno a la dirección de máxima radiación.
- Lóbulos secundarios: Son el resto de máximos relativos, de valor inferior al principal.
- Ancho de haz: Es el margen angular de direcciones en las que el diagrama de radiación de un haz toma un valor de 3dB por debajo del máximo. Es decir, la dirección en la que la potencia radiada se reduce a la mitad.
- Relación de lóbulo principal a secundario (SLL): Es el cociente en dB entre el valor máximo del lóbulo principal y el valor máximo del lóbulo secundario.
- Relación delante-atrás (FBR): Es el cociente en dB entre el valor de máxima radiación y el de la misma dirección y sentido opuesto.
-

4.2.7.2 Ancho de banda: Es el margen de frecuencias en el cual los parámetros de la antena cumplen unas determinadas características. Se

puede definir un ancho de banda de impedancia, de polarización, de ganancia o de otros parámetros.

4.2.7.3 Directividad: La Directividad (D) de una antena se define como la relación entre la intensidad de radiación de una antena en la dirección del máximo y la intensidad de radiación de una antena isotrópica que radia con la misma potencia total.

$D = U(max) / U(iso)$

La unidad de Directividad (D) son los dBi.

4.2.7.4 Ganancia: Se define como la ganancia de potencia en la dirección de máxima radiación. La Ganancia (G) se produce por el efecto de la directividad al concentrarse la potencia en las zonas indicadas en el diagrama de radiación.

$G = 10log[4pi * U(max) / P(in)]$

La unidad de Ganancia (G) de una antena es el dB al ser una unidad de potencia.

4.2.7.5 Eficiencia: Relación entre la potencia radiada y la potencia entregada a la antena. También se puede definir como la relación entre ganancia y directividad.

$e = P(r) / P(in) = G / D$

El parámetro e (eficiencia) es adimensional

4.2.7.6 Impedancia de entrada: Es la impedancia de la antena en sus terminales. Es la relación entre la tensión y la corriente de entrada. La impedancia es un número complejo. La parte real de la impedancia se denomina Resistencia de Antena y la parte imaginaria es la Reactancia. La resistencia de antena es la suma de la resistencia de radiación y la

resistencia de pérdidas. Las antenas se denominan resonantes cuando se anula su reactancia de entrada.

4.2.7.7 Anchura de haz: Es un parámetro de radiación, ligado al diagrama de radiación. Se puede definir el ancho de haz a -3dB, que es el intervalo angular en el que la densidad de potencia radiada es igual a la mitad de la potencia máxima (en la dirección principal de radiación). También se puede definir el ancho de haz entre ceros, que es el intervalo angular del haz principal del diagrama de radiación, entre los dos ceros adyacentes al máximo.

4.2.7.8 Polarización: Las antenas crean campos electromagnéticos radiados. Se define la polarización electromagnética en una determinada dirección, como la figura geométrica que traza el extremo del vector campo eléctrico a una cierta distancia de la antena, al variar el tiempo. La polarización puede ser lineal, circular y elíptica. La polarización lineal puede tomar distintas orientaciones (horizontal, vertical, +45º, -45º). Las polarizaciones circular o elíptica pueden ser a derechas o izquierdas (dextrógiras o levógiras), según el sentido de giro del campo (observado alejándose desde la antena).

En el marco de antenas se define un coeficiente de desacoplo por polarización. Este mide la cantidad de potencia que es capaz de recibir una antena polarizada de una forma con una longitud efectiva $\vec{l}_{ef}$de un campo eléctrico incidente con una determinada polarización $\vec{E}_{in}$. De este modo, el coeficiente de desacoplo por polarización se define como:

$$C_p = \frac{|\vec{E}_{in} \cdot \vec{l}_{ef}|}{|\vec{E}_{in}| \cdot |\vec{l}_{ef}|}$$

De esta manera, obtenemos la fracción de potencia que finalmente la antena es capaz de recibir, multiplicando la potencia incidente en la antena por este coeficiente definido anteriormente, de la forma:

$$P_{rec} = P_{in} \cdot C_p$$

Se llama diagrama copolar al diagrama de radiación con la polarización deseada y diagrama contrapolar (crosspolar, en inglés) al diagrama de radiación con la polarización contraria.

4.2.7.9 Relación Delante/Atrás: Este parámetro se define como la relación existente entre la máxima potencia radiada en una dirección geométrica y la potencia radiada en la dirección opuesta a esta.
Cuando esta relación es reflejada en una gráfico con escala en dB, el ratio F/B (Front/Back) es la diferencia en dB entre el nivel de la máxima radiacción y el nivel de radiacción a 180 grados. Este parámetro es especialmente útil cuando la interferencia hacia atrás es crítica en la elección de la antena que vamos a utilizar. Esta relación, además lo podemos ver desde otro punto de vista, indicando lo buena que es la antena en el rechazo de las señales provenientes de la parte trasera. Rara vez es verdaderamente importante, ya que la interferencias por la parte trasera no ocurren habitualmente, pero puede suceder.

La relación F / B no es un número muy útil, ya que a menudo varía enormemente de un canal a otro. Por supuesto, si se tiene el patrón de radiación, entonces no se necesita la relación F/B.

Comparando una antena yagui con una parabólica, podemos ver que para la antena yagui tenemos una relación F/B de aproximadamente 15 dB (según modelo y fabricante) mientras que para la parabólica la relación F/B es >35dB (según modelo y fabricante). De esta forma observamos como es "de buena" una antena respecto al rechazo de señales por la parte trasera. Cuanto mayor sea este paramentro en las antenas parabolicas mejor será.

Los 15 dB de la antena yagui lo podemos interpretar también como la atenuación que tendríamos en el sistema, en caso de captar una onda rebotada por ejemplo de un edificio, por la parte trasera de esta.

4.2.7.10 Clasificación clásica de las antenas: Existen tres tipos básicos de antenas: antenas de hilo, antenas de apertura y antenas planas. Asimismo, las agrupaciones de estas antenas (arrays) se suelen considerar en la literatura como otro tipo básico de antena.

Antenas de hilo: Las antenas de hilo son antenas cuyos elementos radiantes son conductores de hilo que tienen una sección despreciable respecto a la longitud de onda de trabajo. Las dimensiones suelen ser como máximo de una longitud de onda. Se utilizan extensamente en las bandas de **MF**, **HF**, **VHF** y **UHF**. Se pueden encontrar agrupaciones de antenas de hilo. Ejemplos de antenas de hilo son:

- El monopolo vertical
- El dipolo y su evolución, la antena Yagi
- La antena espira
- La antena helicoidal es un tipo especial de antena que se usa principalmente en VHF y UHF. Un conductor describe una hélice, consiguiendo así una polarización circular.

Las antenas de hilo se analizan a partir de las corrientes eléctricas de los conductores.

Antenas de apertura: La antenas de apertura son aquellas que utilizan superficies o aperturas para direccionar el haz electromagnético de forma que concentran la emisión y recepción de su sistema radiante en una dirección. La más conocida y utilizada es la antena parabólica, tanto en enlaces de radio terrestres como de satélite. La ganancia de dichas antenas está relacionada con la superficie de la parábola, a mayor tamaño mayor colimación del haz tendremos y por lo tanto mayor directividad.

El elemento radiante es el alimentador, el cual puede iluminar de forma directa a la parábola o en forma indirecta mediante un subreflector. El alimentador está generalmente ubicado en el foco de la parábola. El alimentador, en sí mismo, también es una antena de apertura (se denominan antenas de bocina) que puede utilizarse sin reflector, cuando el objetivo es una cobertura más amplia (e.g. cuando se pretende cubrir la totalidad de la superficie de la tierra desde un satélite en órbita geoestacionaria).

Se puede calcular la directividad de este cierto tipo de antenas, D_0, con la siguiente expresión, donde Ses el área y λes la longitud de onda:

$$D_0 = 4\pi \frac{S}{\lambda^2}$$

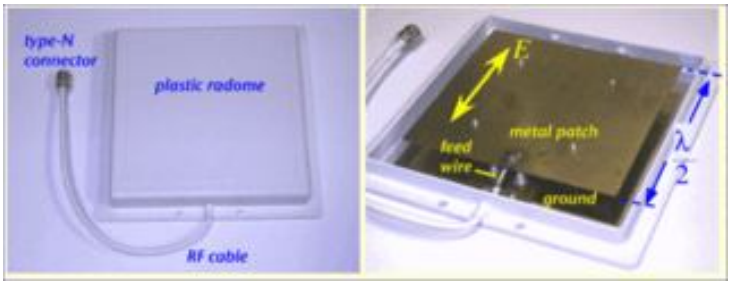
Imagen 29 Reflectores parabólicos

Fuente: http://electromagnetic-fields.wikispaces.com/ANTENAS

Hay varios tipos de antenas de apertura, como la antena de bocina, la antena parabólica, la antena parabólica del Radar Doppler y superficies reflectoras en general.

Antenas planas: Un tipo particular de antena plana son las antenas de apertura sintética, típicas de los radares de apertura sintética (SAR).

Imagen 30 Antena plana



Fuente http://electromagnetic-fields.wikispaces.com/ANTENAS

Las antenas de array: están formadas por un conjunto de dos o más antenas idénticas distribuidas y ordenadas de tal forma que en su conjunto se comportan como una única antena con un diagrama de radiación propio.

Imagen 31 Antena de Array

http://electromagnetic-fields.wikispaces.com/ANTENAS

La característica principal de los arrays de antenas es que su diagrama de radiación es modificable, pudiendo adaptarlo a diferentes aplicaciones/necesidades. Esto se consigue controlando de manera individual la amplitud y fase de la señal que alimenta a cada uno de los elementos del array.

Atendiendo a la distribución de las antenas que componen un array podemos hacer la siguiente clasificación:

- Arrays lineales: Los elementos están dispuestos sobre una línea.
- Arrays Planos: Los elementos están dispuestos bidimensionalmente sobre un plano.
- Arrays conformados: Los elementos están dispuestos sobre una superficie curva.

A nivel de aplicación los arrays de antenas se utilizan para la construcción de antenas inteligentes.
Una definición básica de un sistema de antenas inteligentes es cualquier configuración adaptativa de múltiples antenas que mejoran el rendimiento de un sistema de comunicaciones inalámbricas. Las características de las antenas inteligentes con unos haces de radiación con una mayor directividad (es decir, mayor ganancia y mayor selectividad angular), proporcionan múltiples ventajas:

- Incremento de la zona de cobertura: Dado que la ganancia es mayor que en el caso de antenas omnidireccionales o sectorizadas.

- Reducción de la potencia de transmisión: La mayor ganancia de la antena permite incrementar la sensibilidad.

- Reducción del nivel de interferencia: La mejor selectividad espacial de la antena permitirá al receptor discriminar las señales de usuarios interferentes a favor de la señal del usuario deseado. Incluso se pueden utilizar antenas inteligentes con configuración antena principal y secundarias donde las secundarias anulan las interferencias.

- Reducción de la propagación multitrayecto:Debido a la menor dispersión angular de la potencia radiada, se reduce el número de trayectorias que debe seguir la señal antes de llegar al receptor.

- Mejora de la seguridad: Gracias a que la transmisión es direccional, hay una probabilidad muy baja de que un equipo ajeno intercepte la comunicación.

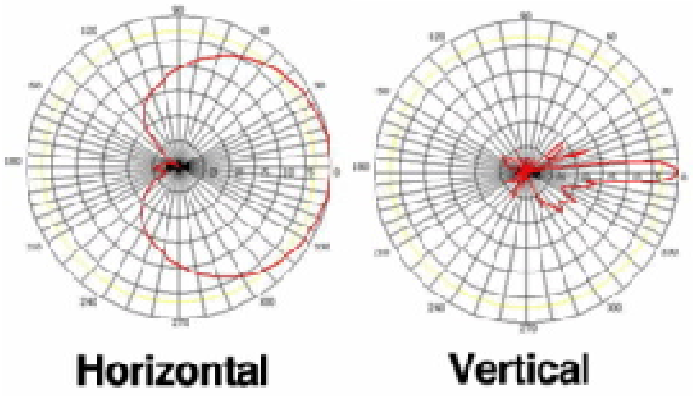
- Introducción de nuevos servicios: Al poder identificar la posición de usuarios se puede aplicar a radiolocalización, tarificación geográfica, publicidad en servicios cercanos...

Antenas sectoriales: Son la mezcla de las antenas direccionales y las omnidireccionales. Es una solución tecnológica ideal para la planificación de redes móviles celulares. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la omnidireccional pero algo menor que la direccional.

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

A continuación podemos ver el diagrama patrón de una antena sectorial:

Imagen 32 diagrama patrón de una antena sectorial

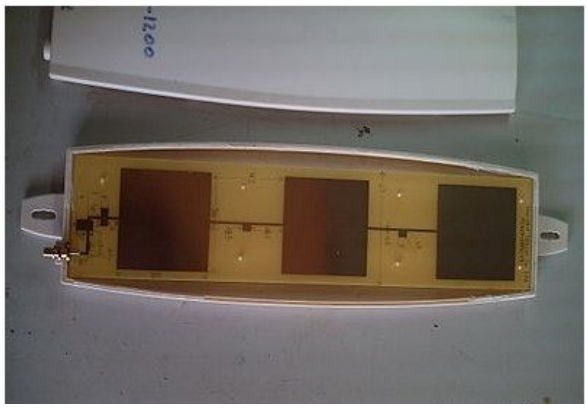


Fuente: http://electromagnetic-fields.wikispaces.com/ANTENAS

Combinando varias antenas en un mismo mástil, podemos lograr cubrir un territorio amplio, mitigando el efecto del ruido y ampliando el ancho de banda:

Ejemplo cálculo antenas sectoriales: Para simular un simple ejemplo de cálculo de antenas sectoriales utilizamos el siguiente applet: Applet cálculo antenas sectoriales
Calcularemos los diagramas para la siguiente antena real:

Imagen 33 Antena real vista en su interior



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

Estudiando la fotografía vemos que el número de elementos es 3, por lo que N=3

Por otro lado, para el funcionamiento del Applet necesitamos conocer la distancia d.

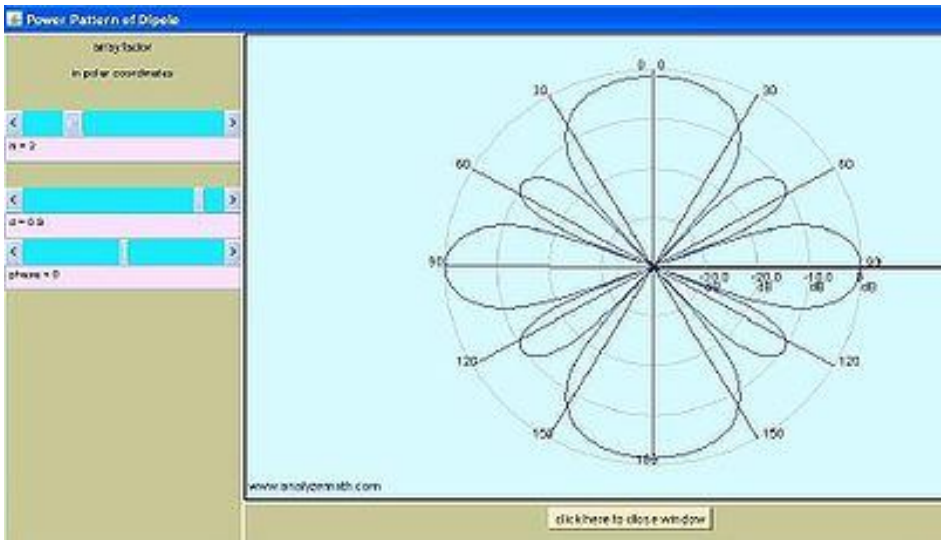
Esta distancia, es la distancia en mm entre los dos centros de dos antenas contiguas. Esta distancia es por lo tanto una lambda (longitud de onda).

Si nos fijamos en nuestro caso d = 0,92*lambda.

Para conocer su fase Beta = K * d , siendo d conocida y K=2*Pi / lambda.
De esta maner vemos que Beta es igual a Beta = 2*Pi*distancia, siendo en nuestro caso Beta=2*Pi*0,92 radianes. En grados Beta= 2*Pi*0,92*Pi / 180 = 0,1º, es decir prácticamente cero.

Para estos parámetros obtenemos el siguiente patrón:

Imagen 34 Patrón obtenido con los parámetros anteriores



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

Cables y conectores: Aunque sea difícil de creer, éstos pueden constituirse en un factor crítico en este tipo de enlaces. Estos sirven para transmitir la señal entre el amplificador y la antena.

Distintos tipos de cables y conectores, producen distintos niveles de atenuación. Para seleccionar el par apropiado cable/conector, se debe recurrir a manuales de fabricantes que especifican un conector adecuado para un tipo de cable dado, a más de cerciorarse bien del nivel de pérdida que éstos presenten a la señal.

4.2.8 Frecuencias de Operación

4.2.8.1 Espectro de frecuencias: El espectro radioeléctrico es un recurso natural de propiedad exclusiva del Estado y como tal constituye un bien de dominio público, inalienable e imprescriptible, cuya gestión, administración y control corresponde al Estado, dicho espectro se subdivide en nueve bandas de frecuencias, que se designan por números enteros, en orden creciente, de acuerdo con el siguiente cuadro. Dado que la unidad de frecuencia es el hertzio (Hz), las frecuencias se expresan:

- En kilohertzios (KHz) hasta 3000 KHz, inclusive;
- En megahertzios (MHz) por encima de 3 MHz hasta 3000 MHz, inclusive;
- En gigahertzios (GHz) por encima de 3 GHz hasta 3000 GHz, inclusive.

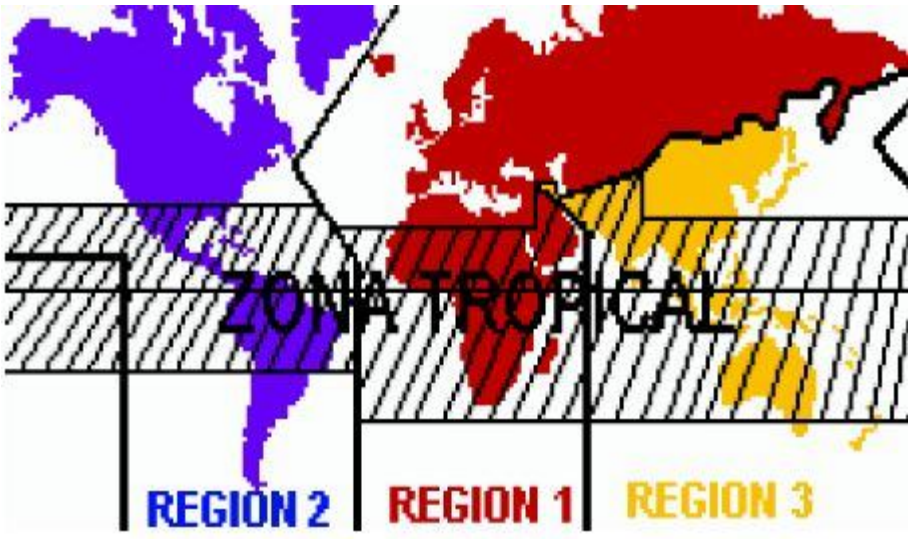
Las emisiones se denominarán conforme a su anchura de banda necesaria y su clase, a saber:

Tabla 7 Clasificación del espectro de frecuencias

Número de la banda	Simbología	Gama de frecuencias	Subdivisión Métrica	Abreviatura Métrica
4	VLF	3 a 30 Khz.	Ondas Miriamétricas	B.Mam.
5	LF	30 a 300 Khz.	Ondas Kilométricas	B.Km.
6	MF	300 a 3000 Khz.	Ondas Hectométricas	B.Hm.
7	HF	3 a 30 MHz.	Ondas Decamétricas	B.Dam.
8	VHF	30 a 300 MHz.	Ondas Métricas	B.m.
9	UHF	300 a 3000 MHz.	Ondas Decimétricas	B.dm
10	SHF	3 a 30 GHz.	Ondas Centimétricas	B.cm
11	EHF	30 a 300 GHz.	Ondas Milimétricas	B. mm
12		300 a 3000 GHz.	Ondas Decimilimétricas	

Desde el punto de vista de la atribución de las bandas de frecuencias, se ha dividido el mundo en tres Regiones. Colombia, al igual que el resto del continente americano, se encuentra ubicada en la Región 2.

Imagen 35 División del mundo en 3 regiones según la UIT



Fuente: http://www.oas.org/en/citel/infocitel

4.2.9 Uso de frecuencias para transmisión inalámbrica[11]

Como se analizó anteriormente en lo que respecta al uso de frecuencias para los servicios inalámbricos, podemos observar que las bandas asignadas a los servicios WLL, LMDS, MMDS, o Spread Spectrum, según la regulación propia de nuestro país, están indicados a continuación:

Nota EQA.205: Aquí hace referencia al MMDS, y tienen asignadas las siguientes bandas:

- En la banda 2.500 – 2.520 MHz, atribuida a los servicios FIJO, FIJO POR SATÉLITE (espacio-Tierra), MÓVIL salvo móvil aeronáutico y MÓVIL POR SATÉLITE (espacio-Tierra), operan Sistemas de Distribución Multicanal Multipunto (MMDS).
- En la banda 2.520 – 2.655 MHz, atribuida a los servicios FIJO, FIJO POR SATÉLITE (espacio-Tierra), MÓVIL salvo móvil aeronáutico y RADIODIFUSIÓN POR SATÉLITE, operan Sistemas de Distribución Multicanal Multipunto (MMDS).
- En la banda 2.655 – 2.670 MHz, atribuida a los servicios FIJO, FIJO POR SATÉLITE (Tierra-espacio) (espacio-Tierra), MÓVIL salvo móvil aeronáutico y RADIODIFUSIÓN POR SATÉLITE, operan Sistemas de Distribución Multicanal Multipunto (MMDS).
- En la banda 2.670 – 2.686 MHz, atribuida a los servicios FIJO, FIJO POR SATÉLITE (Tierra-espacio) (espacio-Tierra), MÓVIL salvo móvil aeronáutico y MÓVIL POR SATÉLITE (Tierra-espacio), operan Sistemas de Distribución Multicanal Multipunto (MMDS).

Nota EQA.210: Aquí hace referencia al WLL, y tienen asignadas las siguientes bandas:

- En la banda 3.400 – 3.500 MHz, atribuida a los servicios FIJO, FIJO POR SATÉLITE (espacio-Tierra), operan Sistemas de Acceso Fijo Inalámbrico (FWA).

[11] Fuente: http://www.isp-planet.com

- En la banda 3.500 – 3.700 MHz, atribuida a los servicios FIJO, FIJO POR SATÉLITE (espacio-Tierra) y MÓVIL salvo móvil aeronáutico, operan Sistemas de Acceso Fijo Inalámbrico (FWA).

Nota EQA.245.- Aquí hace referencia al LMDS, y tienen asignadas las siguientes bandas:

- En las bandas 25,5 – 27,5GHz; 27,5 – 28,35 GHz y 29,1 – 29,25 GHz, atribuidas a los servicios FIJO, FIJO POR SATÉLITE (Tierra-espacio) y MÓVIL, operan Sistemas de Distribución Multipunto Local(LMDS).
- En la banda 31 – 31,3 GHz, atribuida a los servicios FIJO y MÓVIL, operan Sistemas de Distribución Multipunto Local (LMDS).

Spread Spectrum: Aquí hace referencia al espectro ensanchado, el cual es una banda de uso libre en nuestro país y además nos permite trabajar con estándares de la familia 802.11x, y tienen asignadas las siguientes bandas:

Nota EQA.195: El uso de la banda 2.400 – 2.483,5 MHz, está atribuida a los servicios FIJO, MOVIL y RADIOLOCALIZACIÓN, operan Sistemas de Seguridad Pública compartido con Sistemas de Espectro Ensanchado (Spread Spectrum).

Nota EQA.215: El uso de la banda 5.725 – 5.850 MHz, está atribuida al servicio de RADIOLOCALIZACIÓN, se comparte con los servicios FIJO y MÓVIL que operan con Sistemas de Espectro Ensanchado (Spread Spectrum).

Como se puede apreciar, las bandas de frecuencia correspondiente a una transmisión inalámbrica básicamente trabajan en las bandas UHF, SHF o EHF, dependiendo de la tecnología a implementar, será la banda en la que se trabaje.

Independientemente del rango de alcance o de la frecuencia a la cual trabaje un enlace, un conjunto de enlaces puede únicamente dar servicio a una parte del área total debido a la frecuencia con la cual se trabaja, para brindar una cobertura total del área ésta debe reutilizarse, es decir, se deben usar canales independientes, derivados por frecuencia, código o tiempo. No es fácil minimizar el número de canales independientes o conjunto de enlaces para una cobertura total, aquí se usa el factor de reuso, que es una técnica muy utilizada en interferencia limitada.

4.2.10 Estaciones Bases

Una estación base es el punto o puntos de acceso donde los usuarios del WISP se conectan para tener acceso a internet. El número de estaciones bases con el que cuente el WISP dependerá del tamaño geográfico del área a proveer el servicio.

En zonas amplias con un radio (desde la celda central) mayor que el del alcance máximo del punto de acceso se hace una división del terreno en celdas hexagonales en igual forma que en la cobertura de telefonía celular, por lo tanto, al igual que éstas, también se emplean técnicas de reutilización de frecuencias. Estas celdas no necesariamente deben estar en sectores adyacentes, pueden ser zonas aisladas interconectadas a un punto central.

En sí, una estación base consiste en una torre de varios metros de altura en la cual todos los clientes puedan tener línea de vista directa con ésta, donde se instalan dos antenas que dan cobertura a los usuarios ubicados en las cercanías (hasta 10 Km).

Se pretende que la estación base proporcione cobertura omnidireccional, por lo que se emplean dos antenas que cubren sectores de 180 grados cada

una. Se colocan 2 antenas direccionales en lugar de una omnidireccional, dado que éstas proveen mayor alcance que las omnidireccionales.

La mejor ubicación de la antena en una estación base puede ser:

- La cima de un edificio alto ubicado en alguna parte de la ciudad
- La cima de un edificio o caseta ubicada en una colina
- Una torre alta ubicada en un lugar bien despejado

Una vez montada y apuntada la antena, se debe colocar y proteger los cables, se deben configurar los equipos correspondientes como routers, radios, switches, y se debe asignar un identificador de sistema (SSID) para que todos los clientes puedan trabajar con esta estación. Además de la antena, se debe ubicar el radio de la estación base lo más cerca posible de la antena, para que la atenuación debido al cable que conectará a ambos, sea la menor posible.

La arquitectura de una estación base simplemente provee enlace a la infraestructura del backbone. Todo el tráfico dentro del backbone debe terminar en switches ATM o en equipos de oficina central. Bajo este escenario, si dos consumidores conectados a una misma estación base desean comunicarse entre ellos, la comunicación se lleva a cabo en una zona centralizada. Las funciones de autenticación, registro y administración de tráfico se realizan centralizadamente.

4.2.11 Estaciones remotas

Una estación remota o suscriptora es el equipamiento del usuario final, cuya antena debe tener línea de vista directa con la antena de la estación base. Básicamente consta de: antenas, amplificadores transmisores/receptores, adaptadores de señal, cables, conectores y equipos terminales.

Aquí se requerirá de una antena direccional que apunte directamente a la antena de la estación base. Ésta debe conectarse también al router inalámbrico del cliente, y la longitud del cable que interconecta a ambos, debe ser la menor posible para minimizar el nivel de atenuación. Es mejor considerar el uso de un cable de antena más corto y extender el cable de la LAN hasta el lugar donde se instale el Router.

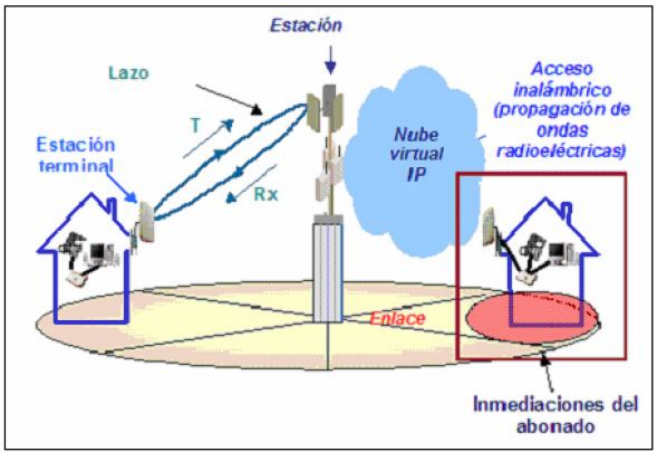
La ubicación típica de la antena de un cliente puede ser:

- El techo del edificio o vivienda, la antena empotrada al mástil o tubo de cañería que sostiene la antena de televisión, o un mástil o tubo de cañería especialmente instalada para la antena.
- La pared lateral de un edificio o vivienda, o el marco de la ventana de éste, ubicado muy cerca del cuarto donde se halla el router inalámbrico.

Una vez montadas estas antenas, se debe apuntar directamente a la antena de la estación base, para ello, se hace una prueba de radiación, donde se tomará la dirección en la que éste apunte cuando la potencia de su lóbulo central sea la mayor posible.

También se deben hacer pruebas de rendimiento de la conexión entre ésta y el router inalámbrico para últimos ajustes.En lo que se refiere a los equipos ubicados en este lado, se los debe configurar de acuerdo a la frecuencia, modulación, demodulación, velocidad de datos y el identificador de sistema (SSID), éste último debe ser el mismo que en la estación base para que puedan trabajar con ésta. Cada configuración varía de acuerdo al proveedor y a las necesidades del cliente.

Imagen 36 Enlace inalámbrico entre una estación base y una estación remota.



Fuente: http://www.isp-planet.com

Por último, vendrá la configuración interna dentro de la red del cliente en lo que respecta a los equipos terminales, que puede ser sólo un solo host, o bien pueden formar una LAN, cuyo direccionamiento habrá que configurar. Además, aquí se especificará el tipo de servicio de banda ancha que cada equipo terminal recibirá, de acuerdo con lo que el proveedor ofrezca. Luego de esto se hacen las pruebas pertinentes del caso para ver si existe o no la conexión con el WISP y en caso de que haya, probar que tan rápido es ésta, y en caso de que no, ver los problemas que pueden existir y aplicar las posibles soluciones.

4.2.12 Seguridad en redes inalámbricas

La seguridad es uno de los temas más importantes cuando se habla de redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito. Por ello es conveniente el seguir puntual y escrupulosamente una serie de pasos que nos permitan disponer del grado máximo de seguridad del que seamos capaces de asegurar. Este es el “talón

de Aquiles” de este tipo de redes. Por ello, si una red inalámbrica está bien configurada nos podemos ahorrar muchos disgustos y estar más tranquilos.

Asegurar una red no es un proceso simple, y no existe una receta simple para hacerlo. Sin embargo, los siguientes puntos básicos se deben cumplir:

Seguridad Física: El primer paso para considerar una red segura es asegurarla físicamente, tanto para evitar intrusiones como para asegurar la conectividad. En una red inalámbrica es mucho más difícil asegurar físicamente nuestra red. De todos modos, utilizando las capacidades de cifrado de las redes inalámbricas, ubicando nuestros puntos de acceso tan al centro de nuestras instalaciones como sea posible para evitar "derramar" señal, y en general utilizando el sentido común al instalar nuestra red, podremos evitar exponernos de más. Hay que recordar que una red inalámbrica puede ser muy conveniente y económica, pero si es instalada sin el cuidado necesario, puede ser nuestra mayor vulnerabilidad.

Seguridad Perimetral: Una vez que tenemos confianza en nuestra instalación de red, tenemos que definir perímetros de seguridad, los cuales serán divididos por uno o varios firewalls. La configuración más simple consiste en solamente poner un firewall entre nuestra red local y nuestra salida a Internet, permitiendo únicamente la entrada y salida a las conexiones autorizadas. Para una red importante y de complejidad mediana, les recomiendo fuertemente tener delimitados cuando menos los siguientes perímetros: Servidores de uso interno, servidores de uso externo, red local, y red inalámbrica.

Monitoreo de la red y equipos: Parte importante de la seguridad en una red consiste en monitorearla activamente. Hay muchas condiciones que pueden llevarnos a fallas, y muy fáciles de corregir, o por lo menos diagnosticar, si contamos con herramientas de monitoreo. Otro aspecto importante a

monitorear es los intentos de ataque que estemos recibiendo, para saber de qué protegernos, cuáles son nuestros principales riesgos, quién está intentando atacarnos, por qué medios, y qué es lo que buscan. En cuanto a los equipos terminales, debemos mantener actualizados nuestros sistemas operativos, programas y herramientas, puesto que es muy frecuente en los softwares, tanto libre como propietario, que sean encontradas fallas de programación que pueden traducirse en agujeros de seguridad un administrador de redes responsable debe mantener sus sistemas con los al día, para no sufrir ataques prevenibles.

Además, se puede implementar otros mecanismos de seguridad en una red inalámbrica, tales como:

WEP. Significa Wired Equivalet Privacy. Fue introducido para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos. Puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y algunas marcas están introduciendo el WEP256. Es inseguro debido a su arquitectura, por lo que el aumentar los tamaños de las claves de encriptación sólo aumenta el tiempo necesario para romperlo. 802.11 permite la encriptación WEP en la capa de enlace de datos.

OSA VS. SKA. OSA (Open System Authentication), cualquier interlocutor es válido para establecer una comunicación con el AP (Access Point). SKA (Shared Key Authentication) es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

ACL. Significa Access Control List. Es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

CNAC. Significa Closed Network Access Control. Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.

SSID. Significa Service Set Identifier. Es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Las tarjetas de red deben conocer el nombre de la red para poder unirse a ella.

Para poder asegurar una red inalámbrica se recomienda seguir los siguientes pasos:

A. Activar el WEP.
B. Seleccionar una clave de cifrado para el WEP.
C. Uso del SKA e inmediatamente después, uso del OSA.
D. Desactivar el DHCP y activar las ACL.
E. Cambiar el SSID y modificar su intervalo de difusión.
F. Hacer uso de VPNs (Redes Privadas Virtuales), para seguridad extra.
G. Aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional.
H. Montar un firewall que filtre el tráfico entre 2 segmentos de red.

Actualmente el IEEE está trabajando en la definición del estándar 802.11i que permita disponer de sistemas de comunicación entre dispositivos inalámbricos realmente seguros.

4.2.13 Propagación de ondas[12]

El proceso de propagación de ondas es muy importante en el estudio del radioenlace, y que nos permitirá establecer los equipos a utilizar en la transmisión la cual debe soportar todo el viaje entre transmisor y receptor sin perder la integridad de la información. Cabe recordar que la propagación se la hace a la velocidad de la luz (3x108 metros/segundo en vacío).

En cuanto a la propagación de ondas en la tierra, vemos que, cuando una onda viaja de un punto a otro, se pueden presentar cualquiera de los siguientes casos:

- Onda directa.- Viaja en línea recta entre el transmisor y el receptor.
- Onda reflejada.- Rebota en la superficie de la tierra antes de llegar al receptor.
- Dispersión de onda.- Liberación de energía sobre puntos diferentes al receptor y transmisor en el camino de ambos.

A frecuencias mayores a 30MHz, que es nuestro caso, ya son considerados microondas y el tipo de propagación será una línea de vista, y se usan antenas elevadas.

4.2.13.1 Pérdidas: En esta sección describiremos las principales pérdidas de un radioenlace, sin embargo, para efectos prácticos hay ciertos factores que producen pérdidas adicionales y cuyo resultado puede ser obtenido en tablas y gráficos empíricos. Los factores más relevantes que producen pérdidas son: Atenuación por espacio libre, refracción, reflexión, difracción, geografía del terreno y clima, pero a estos 2 últimos factores, los analizaremos con más detalle mas adelante.

[12] http://electromagnetic-fields.wikispaces.com/ANTENAS

4.2.13.2 Pérdida por espacio libre: Se define como espacio libre como el camino entre el transmisor y el receptor libre de obstáculos donde la única atenuación será la del recorrido. La relación de pérdidas es proporcional al inverso de la distancia entre las antenas. Es decir, al aumentar la distancia, el frente de ondas se amplía en la radiación y la distribución de energía en el receptor será menor.

En forma general este tipo de pérdida depende de la frecuencia de transmisión **(f)** y de la distancia de separación entre las antenas **(d).**

$P_{espacio\ libre}$ [dB] = 32.44 + 20 log f[MHz] + 20 log d [Km]

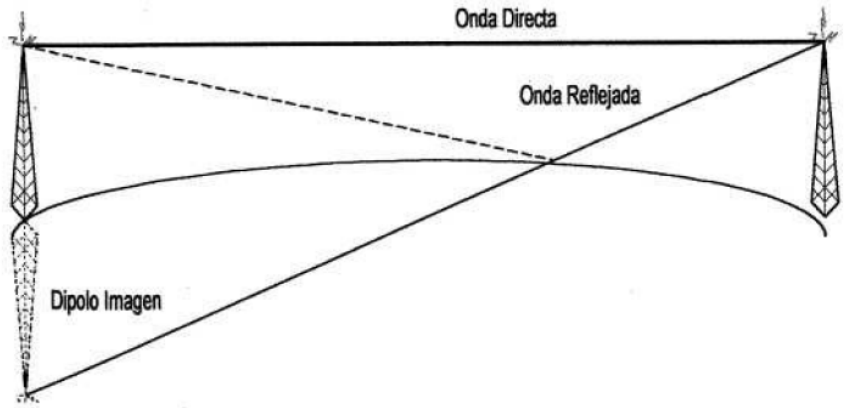
4.2.13.3 Difracción: La mayor parte de la energía irradiada se concentra en el primer lóbulo de transmisión, llamado también Zona de Freznel y en el cálculo del enlace es la zona sobre la cual no debe haber ni interferencia ni obstáculos para poder definir al trayecto como despejado. Difracción se define como el torcimiento de un rayo luminoso al pasar por el borde de un cuerpo opaco.

Consideremos el caso de que la obstrucción se cause por la curvatura terrestre, entonces se producirá una componente superficial de onda, sin embargo para frecuencias altas la atenuación de esta componente es demasiado alta como para tener alguna influencia, por tanto la tierra misma impedirá el paso libre de la señal.

Si las antenas están muy separadas, se puede ir aumentando la altura de éstas hasta obtener una atenuación menor y que se siga manteniendo la línea de vista. Para que la comunicación se dé entre 2 puntos (sin uso de repetidoras), la atenuación debe ser menor a 40 dB.

4.2.13.4 Reflexión: El problema principal está en hallar el punto de reflexión. Para hallar este punto, se emplea geometría, basado en la figura 3.24, y que básicamente dependerá de la altura de las antenas, la distancia de separación, el tipo de superficie sobre la cual se refleja y la frecuencia y potencias transmitidas. Este fenómeno provocará un desfasamiento entre la onda directa y la onda reflejada, puesto que la última recorrerá una mayor distancia hasta llegar al receptor.

Imagen 37 Reflexión de la onda y formación del dipolo



Fuente: http://electromagnetic-fields.wikispaces.com/ANTENAS

La reflexión en sí forma un dipolo imagen en el lado del transmisor, que tendrá una altura exactamente igual a la altura de la antena transmisora y ubicada debajo de ésta, creando así una línea de vista directa con la antena receptora, sin considerar la superficie de la tierra. La distancia de separación entre la antena dipolo y la receptora es igual a la distancia recorrida por la antena transmisora, que se refleja en la superficie de la tierra y llega a la receptora.

A frecuencias altas (microondas), se usan las antenas elevadas, por ello, se encuentra más alejada de la superficie terrestre, por lo que el frente de onda que llegará a la tierra será plano y por tanto, la onda no se refleja, por ello, este factor no es relevante en este caso.

4.2.13.5 Ondas planas: La propagación de ondas se hace en esferas concéntricas en el medio que viaja. Se hace evidente pensar que en un tiempo pequeño dicha esfera se vuelva lo suficientemente grande como para que un observador lo considere plana, igual que la superficie terrestre. Una onda que al alejarse de su fuente parece lisa, se denomina onda plana.
Se define como frente de onda al conjunto de puntos donde el campo tiene la misma fase, y la longitud de onda es la distancia que separa a 2 frentes de onda de fases iguales en un instante dado.

Una onda polarizada es la que mantiene líneas de campo eléctrico en una dirección. En radiocomunicaciones es muy común utilizar la polarización (horizontal o vertical) tomando como referencia el plano de la superficie terrestre. La polarización tiene su efecto en la propagación, pero a frecuencias altas este factor disminuye, no por ello pierde importancia. No debemos confundir el plano de polarización con el plano de incidencia, puesto que el primero sólo contiene al campo eléctrico, mientras que el segundo es aquel que contiene los rayos incidente, reflejado y refractado.

4.2.13.6 Calidad de la señal: Al realizar la medición de la calidad de señal en un enlace existen 2 factores básicos que debemos considerar: BER (Tasa de bits erróneos) y la relación señal a ruido (SNR). Estos parámetros permitirán saber la eficiencia real de un enlace digital y la búsqueda a posibles alteraciones a esta información.

BER.- Es la probabilidad de que un solo bit esté alterado en un intervalo de tiempo definido. Tiene su importancia el tipo de errores, porque los diferentes esquemas de detección identifican tipos diferentes, además el número de bits empleados en algunos esquemas determina la longitud de las ráfagas que se detectan. Los 3 esquemas más utilizados son la paridad, verificación de suma de bloques y la verificación de redundancia cíclica (CRC).

Relación señal a ruido.- Definiremos el ruido de línea al grupo de perturbaciones eléctricas que se encuentran en el enlace, aún cuando no esté transmitiéndose información. La relación señal a ruido es por tanto, la relación entre la cantidad de potencia contenida en la información deseada y aquella que se transporta en el ruido. Una alta tasa SNR indica una señal de buena calidad, lo contrario implica que el ruido tendrá una incidencia notable sobre la información transmitida. Dado que el ruido eléctrico tiene menor probabilidad de incidir sobre su calidad, es más importante para el diseñador conocer la tasa de bits erróneos y buenos que pasan, por ello es importante conocer el BER de la señal.

4.2.13.7 Especificaciones geográficas: Para la realización del diseño de un WISP una de las primeras consideraciones a tener en cuenta es el sector donde se va a implementar el sistema. Los factores que permiten optimizar la capacidad de una comunicación inalámbrica dentro de un área geográfica y del espectro de ancho de banda, son considerados más importantes que la forma de como son implementadas.

Los diseñadores buscan montar el enlace en lugares en los cuales no presenten mayores accidentes geográficos, o bien un área residencial totalmente plana; pero las áreas urbanas no se han diseñado pensando en los sistemas inalámbricos, por lo que un diseño bien planeado podría evitar gastos y una optimización de los recursos tecnológicos. Además, se supone que un diseño de este tipo de red debe llegar a zonas donde el cableado no lo haga, de ahí, que entran en juego otros factores como área de cobertura, potencia de transmisión y recepción, línea de vista, uso de repetidores, etc.

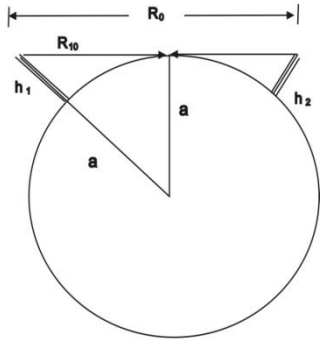
Como procedimiento previo al diseño debería hacerse un estudio detallado del lugar donde se va a trabajar, un mapa cartográfico del sector ayudaría mucho, pero un reconocimiento de la zona es de vital importancia puesto que en muchas ocasiones más que los accidentes geográficos los factores que

más problemas ocasionan a los WISP son las grandes construcciones en zonas de mayor concentración urbana, tales como los grandes edificios, y esto no puede ser leído en dichos mapas.

El área de cobertura de un enlace inalámbrico está determinada por la potencia del transmisor, las frecuencias en las cuales la radio base y las radios terminales del suscriptor funcionan, la ganancia y polarización de las antenas, las características locales asociadas de la propagación en función de la geografía local, del terreno, y los modelos de radiación de las antenas de la terminal de la estación base y del cliente.

El área de cobertura para este tipo de enlaces oscila entre unos 8 y 12 Km. promedio sin uso de repetidores, pero dependiendo de las condiciones anteriores, siempre y cuando, exista línea de vista directa entre la antena del cliente y la antena de la estación base. Para mayores distancias puede haber problemas para asegurar la línea de vista debido a la curvatura de la Tierra que se convierte en un obstáculo natural que no dejará pasar la onda y, mientras la distancia incrementa, se origina que la señal de radio disminuya, debido a la curvatura de la Tierra o a obstáculos físicos naturales existente.

Imagen 38 Línea de vista de un enlace microondas



R0= Alcance máximo entre antenas para linea de vista
R10= Linea de vista para la antena 1
a= radio de la tierra
h1, h2 = Altura de las antenas 1 y 2, respectivamente sobre el nivel del mar

Fuente: http://electromagnetic-fields.wikispaces.com/antenas

La figura anterior se muestra la distancia máxima para obtener una línea de vista entre 2 antenas, considerando el efecto obstáculo producido por la curvatura de la tierra. Esta distancia mínima Ro, está dada por:

$$Ro = 3.57 \{h1^{1/2}\,[m] + h2^{1/2}\,[m]\}\,[Km]$$

La siguiente tabla muestra el efecto “obstáculo” que presenta la curvatura de la tierra, en función de la distancia a la cual se encuentran 2 puntos.

Tabla 8 Efecto de la curvatura de la tierra en función de la distancia entre dos puntos

DISTANCIA	ALTURA
5 Km.	78 cm
10 Km.	3,1 m
30 Km.	17 m
50 Km.	78 m
100 Km.	310 m
500 Km.	7800 m
1000 Km.	31000 m

Fuente: http://electromagnetic-fields.wikispaces.com/antenas

Cuando se presenta esta situación, o algo similar que afecte el área de cobertura, sin embargo, se desea cubrir un poco más de terreno, se necesitará el uso de estaciones repetidoras, las cuales se encargarán de tomar la señal debilitada, amplificarla y regenerarla para así poder llevarla hasta el punto final. Estas deben comportarse como si fuera una estación base, desde la perspectiva del cliente; o una estación remota, desde la perspectiva del punto central, es decir, deben cumplir los mismos criterios de enlace tal como si fuera único: debe haber línea de vista directa entre las antenas, éstas deben estar ubicadas en lugares altos o despejados, la antena de transmisión y recepción, deben ser de buena ganancia, sus equipos amplificadores deben filtrar la mayor cantidad de ruido posible, etc.

Otra consideración importante a tomar es el factor del terreno sobre el cual se monta el enlace, puesto que éste presenta una superficie sobre la cual la onda también viajará y por tanto, producirán efectos de reflexión, refracción y difracción, y por ende, producirán interferencia y pérdidas de señal. Estas incidencias variarán en el tipo de superficie sobre el cual viaja (conductivo, semiconductivo o dieléctrico), la longitud de onda de la señal, y la polarización de las antenas.

4.2.13.8 Especificaciones climáticas: Aparte de la geografía del terreno, también debemos especificar todo lo referente a los factores climáticos o ambientales que afectan a las redes inalámbricas, y sobre todo a altas frecuencias. Los factores que aquí influyen son: temperatura, humedad, precipitaciones, ruidos vehiculares o industriales, entre otros.

A frecuencias mayores de 5 GHz (especialmente LMDS) hay que considerar además la intensidad instantánea de lluvia y el nivel de precipitación que ésta pueda alcanzar, en vista que estos factores producen absorción o dispersión de las ondas electromagnéticas por medio del vapor de agua. A frecuencias superiores a 10 GHz, la señal es totalmente sensible a lluvias, niebla, nieve, polvo y al oxígeno del aire, todos estos factores se comportan como dipolos eléctricos o magnéticos que absorberán parte de la energía irradiada. Mientras mayor sea la frecuencia transmitida, mayor será la influencia de estos factores. Sin embargo, este tipo de problemas es solucionable aumentando la potencia de transmisión.

Para tener una medida exacta de cuánto se pierde por condiciones climáticas o ambientales, este valor se lo obtiene de la siguiente fórmula:

Pamb = [7.19*10$_{-3}$ + 6.09/{f$_2$+0.227} + 4.81/{(f-57)$_2$+1.5}] * f $_2$*10$_{-3}$ + [0.067 + 3/{f-22.3)$_2$+7.5}] * f$_2$* p **** 10$_{-4}$ [dB/KM]**

Donde:

- P < 12 g/m3 (siendo un valor típico 7.5); y,
- f (frecuencia en GHz) < 30 GHz.

Como se ve, obtener el valor exacto de este tipo de pérdidas resulta muy complicado, sin embargo, estos valores pueden obtenerse en tablas, y el resultado es muy confiable.

5 PROPUESTA DISEÑO E IMPLEMENTACIÓN DE UNA RED PILOTO PARA EL WISP EN SAN VICENTE DE CHUCURI

El objetivo del proyecto es brindar acceso a Internet Wi-fi, transmisión de datos, y algunos otros servicios propios de un isp, utilizando como medio de transmisión el aire, prescindiendo de cables entre usuario y proveedor. El sistema de acceso a internet inalámbrico a desarrollar se cimenta en una plataforma totalmente nueva, en la actualidad depende de dos proveedores locales, sin embargo la proyección es llevar la señal directamente sin intermediarios.

Nos enfocaremos especialmente en los accesos inalámbricos a los usuarios residenciales, salas de internet, usuarios empresariales, gubernamentales y usuarios rurales conjunto que es el objetivo de nuestro estudio.

5.1 UBICACIÓN ESPACIAL DEL PROYECTO

El lugar elegido para el desarrollo del proyecto, por razones de costos y facilidad técnica para el prototipo es la ciudad de San Vicente de Chucurí. San Vicente de Chucurí[13] es un municipio del Departamento de Santander, que limita por el Norte con Betulia, por el Sur con el Carmen de Chucurí, al Oriente con Zapatota y Galán y al Occidente con Barrancabermeja. San Vicente se encuentra ubicado en las siguientes coordenadas: 6° 52”57” latitud norte y a 73° 24” 46” longitud occidental.

El Municipio tiene partes planas, cerros, valles, páramos y una meseta; accidentes geográficos que influyen en el clima, por lo cual encontramos

[13] Fuente: Pagina web del municipio de San Vicente de Chucuri http://www.sanvicentedechucuri-santander.gov.co

desde el caliente en la zona de llanura al occidente, hasta clima frío o de páramo en la zona montañosa al oriente.
Sus mayores alturas son el Cerro de Pan de Azúcar (2.026 metros de altura sobre el nivel del mar) y el Cerro de Coconucos.

Extensión total: 1.195,41Km2 [14]

Extensión área urbana: 11,96km2 (1% de extensión total) Km2

Extensión área rural: 1.183,45km2 Km2

Altitud de la cabecera municipal (metros sobre el nivel del mar): 692m

Temperatura media: 13 o y 27 oC. º C

En cuanto a la tecnología que vamos a implementar en nuestra red, vamos a acceder desde nuestra estación base o punto central, ubicado en un edificio alto que está en el centro de la ciudad, hacia el usuario, por medio del estándar 802.11, que fue analizado previamente, y más particularmente, el 802.11ª, 8022.11b, 802.11g, que trabaja en la banda de 5.8 GHz, y transmite datos a una velocidad de hasta 54 Mbps (nuestros equipos pueden soportar una transmisión de hasta 60 Mbps).

La banda de 5.8 GHz corresponde a la banda de Spread Spectrum o Espectro Ensanchado, la cual es de uso libre en nuestro país. En relación a la conexión desde los proveedores (Telecom) hasta nuestro punto central se realizará mediante línea dedicada.

Los equipos que usaremos en el presente proyecto deben tener la certificación Wi-Fi, para así interoperar entre equipos de distintos fabricantes.

Ofertaremos básicamente 2 tipos de conexiones: enlaces dedicados y no dedicados, gestionando así de mejor forma el ancho de banda demandado por el usuario, el cual será variable y acorde a la necesidad de cada cliente. Orientaremos el servicio a nivel corporativo y para aplicaciones SOHO (Small

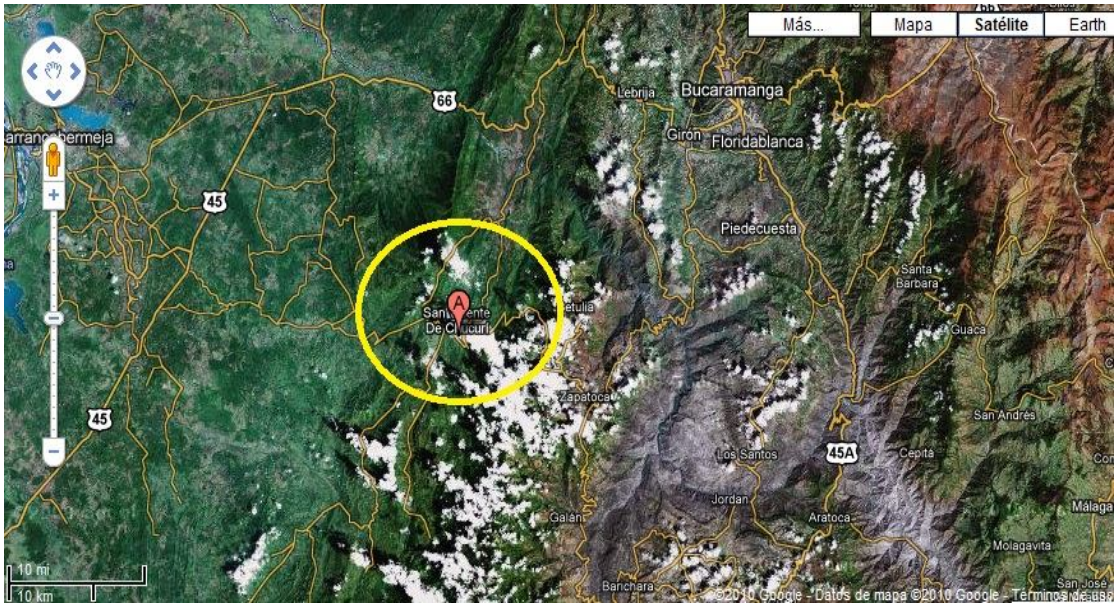
[14] Fuente: Gaceta de Santander, 2340 del 18 agosto de 1890. Plan Básico de Ordenamiento Territorial

Office/Home Office). Luego describiremos, aunque no de una manera profunda, la conexión del ISP hacia el internet, puesto que, nuestro interés se centra en el acceso hacia el usuario por medios inalámbricos y tecnología económica.

Para nuestro diseño, independientemente del tipo de enlace, ubicaremos como punto central el techo del edificio Real de San Vicente de Chucurí cuya altura máxima está a 44 m. sobre el nivel de la ciudad, ésta construcción es la más alta de esta ciudad. Geográficamente este punto se halla a 6º52'45.4'' de Latitud Norte y 73º24'31.2'' de Longitud Oeste, 657 metros sobre el nivel del mar, y desde aquí irradiará y recibirá las señales de datos de forma inalámbrica desde y hacia los usuarios.

Se irradiará a una antena rural ubicada en el cerro La Ciberia que permitirá radiar a usuarios rurales en este caso se implementa para un red de esculas rurales. Las figuras siguientes se muestran el mapa de San Vicente de Chucurí y la ubicación geográfica ampliada de los nodos central y rural.

Imagen 39 Ubicación geográfica San Vicente de Chucurí



Fuente: WWW.Googleeart.com

Imagen 40 Ubicación de nodo central y Rural

Fuente: WWW.Googleeart.com

5.2 PLANIFICACIÓN DEL ISP INALÁMBRICO

La propuesta de diseño de una Red Inalámbrica que provea de servicios de Internet a usuarios finales dentro de un radio de 4 kilometros en sector urbano de San Vicente de Chucurí y dos kilómetros más en sector Rural, debe tomar en cuenta ciertas consideraciones, las mismas que sirvan para desarrollar la red ISP.

El diseño a ser implementado debe satisfacer todas las expectativas y necesidades para lograr un correcto desenvolvimiento y planificación de la red, permitiendo así cumplir con la prestación de servicios con calidad y seguridad ante el usuario.

La realización de la red Inalámbrica, está basado en un esquema punto punto y punto multi punto, debido a que estas redes presentan características tales como:

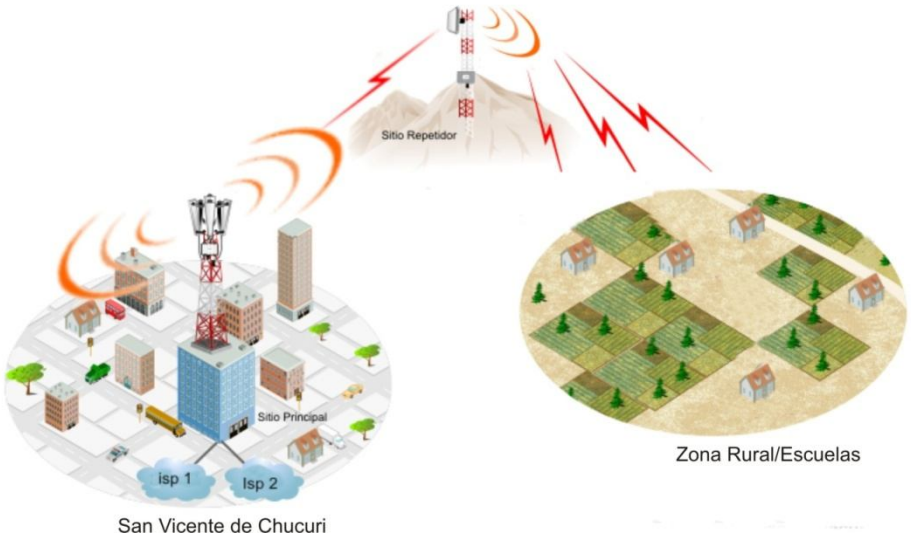
- Tolerantes a fallos
- Mayor área de cobertura
- Administración más simple y eficiente, etc.

La arquitectura de la red inalámbrica, tiene como objetivo de su implementación proveer a los usuarios el acceso a Internet, donde cada usuario podrá acceder a este servicio mediante un equipo portátil independientemente del lugar donde se encuentre, siempre y cuando esté dentro del área de cobertura de la red. Para lo cual se utilizará equipos y dispositivos que utilizan *tecnología Wi-Fi*, se pretende cubrir la mayor parte del área total del área urbana y repetidores para el área Rural.

Los puntos de acceso, tanto el número, como las características de cada uno se las realizará mediante una planificación de estudio, asumiendo detalles para el dimensionamiento de los mismos, y que sean capaces de satisfacer la demanda de cada usuario estimado que pretenda utilizar este servicio y se maneje valores aceptables de eficiencia y confiabilidad, para la seguridad interna de los datos.

El diseño de la red inalámbrica en San Vicente y su área rural, tecnología open source y tecnología económica pero confiable, se adquirirán los equipos y demás elementos que se necesitaren, para permitir un funcionamiento del sistema acorde con las expectativas requeridas.

Imagen 41 Diseño Grafico de red Planeada San Vicente y su área rural



Fuente: http://www.netkrom.com/es/sol_rural_internet.html- Modificado por Autores

5.2.1 Diseño de radioenlaces

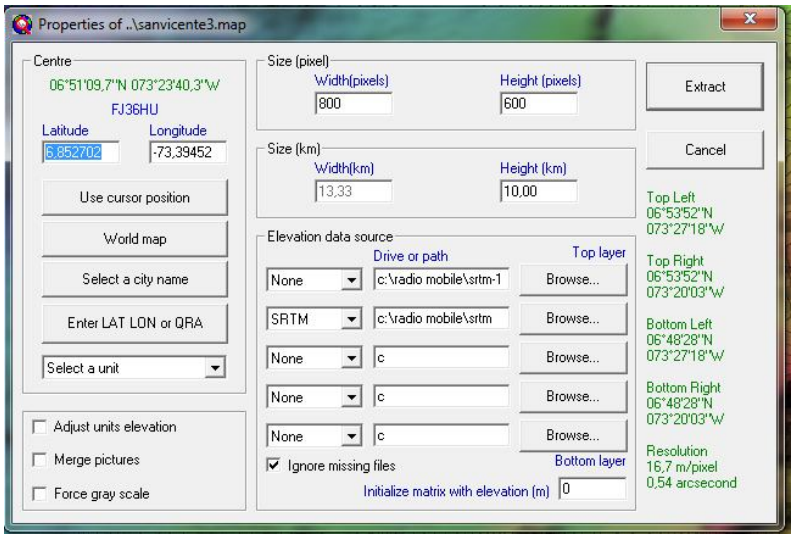
En el diseño a implementar se utilizarán antenas sectoriales Iperlink para radiar 360 grados en la zona urbana y rara recepción y transmisión en la zona rural se utilizará lo Nono Station y PowerStation de Ubiquiti, estos se detallará más adelante, el diseño del radioenlace se realizó de forma preliminar con el google eart y en forma definitiva con el con el software radio Mobile.

Imagen 42 muestra de elevaciones en enlace San Vicente a Zona rural

Fuente: WWW.Googleeart.com

Para el diseño desde radio Mobile primero que todo se establecen las propiedades del mapa y la cobertura o radio a extraer, como se muestra en la siguiente figura.

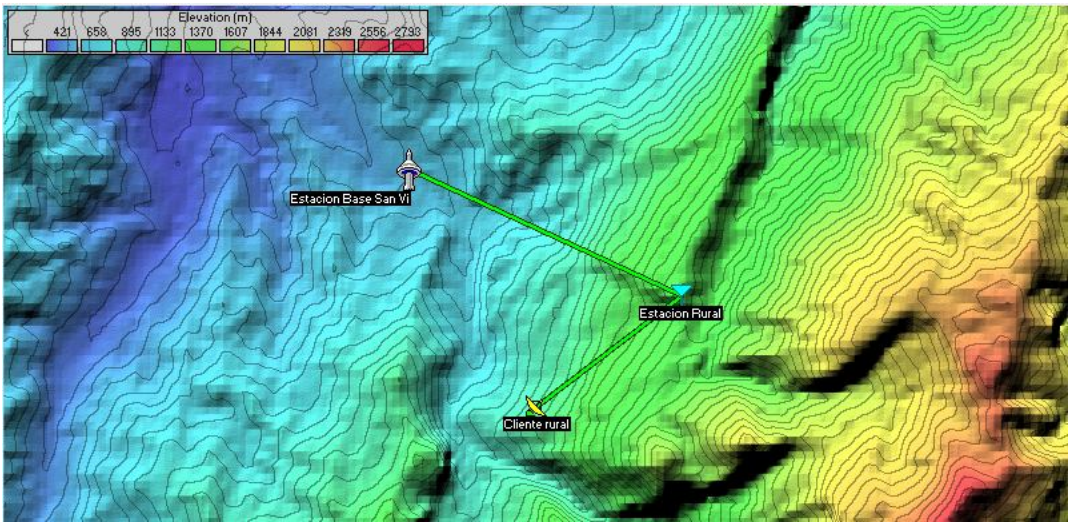
Imagen 43 Especificación de mapa en Radio Mobile



Fuente: Imagen generada en Radio mobile - por Autores

Una vez especificada las características del mapa se especifican cada uno de los nodos, se grafican sobre el mapa extraído en Radio Mobile

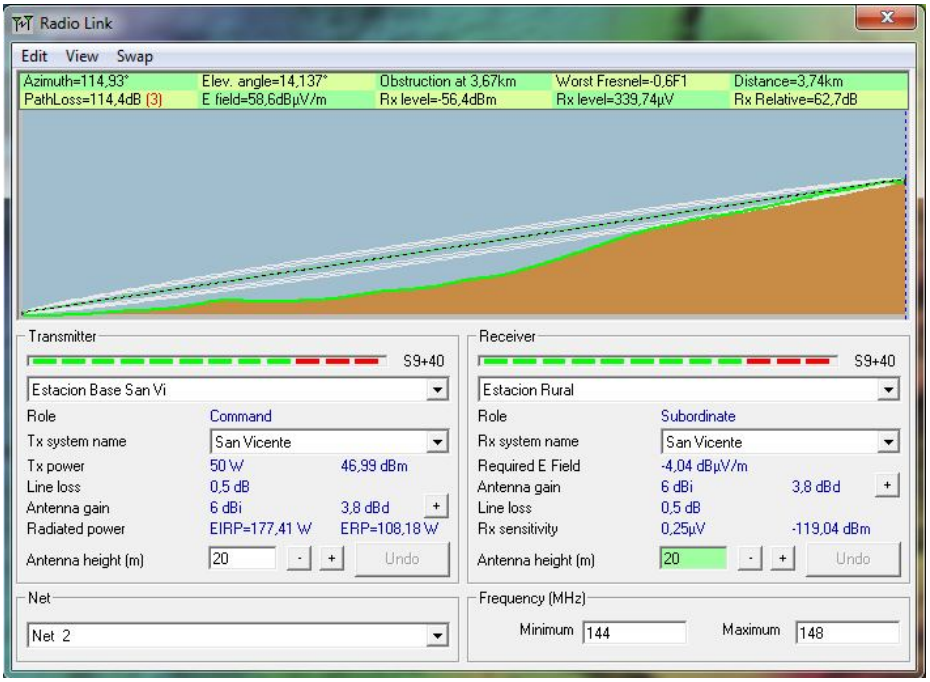
Imagen 44 Diseño de enlaces mediante Radio Mobile



Fuente: Imagen generada en Radio Mobile - por Autores

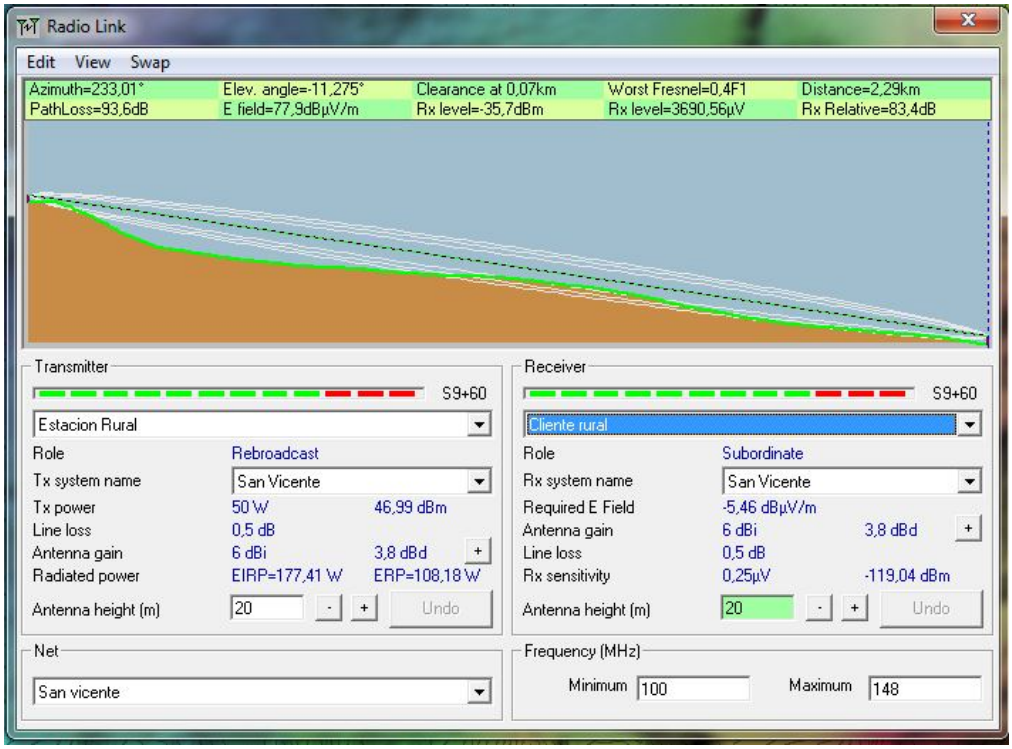
Una vez diseñado en Radio Mobile se verifica las características de cada enlace.

Imagen 45 Enlace de Base San Vicente a Zona rural



Fuente: Imagen generada en Radio Mobile - por Autores

Imagen 46 Imagen de enlace de Estación Rural a Cliente



Fuente: Imagen generada en Radio Mobile - por Autores

Las anteriores imágenes nos permiten ver que cada enlace tiene línea de vista y permite analizar variables como la elevación de antenas para que haya dicha vista, la distancia promedio desde un punto a otro, la elevación de cada punto y la zona de fresnel en dichos radio enlaces.

También muestra la topografía del terreno y otras características como ganancia de cada antena etc.

5.2.2 Equipos para la red inalámbrica planteada

Para la implementación del diseño de la Red Inalámbrica, se describen equipos basados en el estándar 802.11g, los mismos que permitan una estructura y una configuración mallada. Y así permitir una mayor cobertura

del sistema cuando se desee brindar los servicios de Internet a usuarios externos al campus universitario.

Se describen algunas opciones de equipos que puede tener el diseño de la red inalámbrica, se analizará las mejores alternativas que brinden una solución unificada y centralizada de los recursos, para permitir una fácil administración y escalabilidad de la red.

5.2.2.1 MikroTik RouterOS

Imagen 47 Mokrotik Router Board

Fuente: Autores

Dicha red se implementara con Mikrotik RouterOS que es el sistema operativo y software del router, el cual convierte a una PC Intel ó un Mikrotik RouterBOARD en un router dedicado.

Se toma esta decisión ya que estos equipos brindan seguridad, flexibilidad y son muy económicos, lo cual es un gran beneficio para la empresa ya que la red es de un tamaño considerable el RouterOS es un sistema operativo y software que convierte a una PC en un ruteador dedicado, bridge, firewall, controlador de ancho de banda, punto de acceso inalámbrico, por lo tanto

puede hacer casi cualquier cosa que tenga que ver con las necesidades de red, además de ciertas funcionalidad como servidor.

El software RourterOS puede ejecutarse desde un disco IDE memoria tipo FLASH. Este dispositivo se conecta como un disco rígido común y permite acceder a las avanzadas características de este sistema operativo.

Características principales

- El Sistema Operativo es basado en el Kernel de Linux y es muy estable.
- Puede ejecutarse desde discos IDE o módulos de memoria flash.
- Diseño modular
- Módulos actualizables
- Interfaz grafica amigable.

Características de ruteo

- Políticas de enrutamiento. Ruteo estático o dinámico.
- Bridging, protocolo spanning tree, interfaces multiples bridge, firewall en el bridge.
- Servidores y clientes: DHCP, PPPoE, PPTP, PPP, Relay de DHCP.
- Cache: web-proxy, DNS.
- Gateway de HotSpot.
- Lenguaje interno de scripts.

Características del RouterOS

- Filtrado de paquetes por:
- Origen, IP de destino.
- Protocolos, puertos.
- Contenidos (seguimiento de conexiones P2P).
- Puede detectar ataques de denegación de servicio (DoS)
- Permite solamente cierto número de paquetes por periodo de tiempo.

Calidad de servicio (QoS)

- Tipos de colas
- RED
- BFIFO
- PFIFO

- PCQ

Colas simples

- Por origen/destino de red.
- Dirección IP de cliente.
- Interfase

Árboles de colas

- Por protocolo.
- Por puerto.
- Por tipo de conexión.

Interfases del RouterOS

- Ethernet 10/100/1000 Mbit.
- Inalámbrica (Atheros, Prism, CISCO/Airones)
- Punto de acceso o modo estación/cliente, WDS.
- Síncronas: V35, E1, Frame Relay.
- Asíncronas: Onboard serial, 8-port PCI.
- ISDN
- xDSL
- Virtual LAN (VLAN)

Imagen 48 Router Board Mikrotik 433

Fuente: Autores

Herramientas de manejo de red

- Ping, traceroute.
- Medidor de ancho de banda.
- Contabilización de tráfico.
- SNMP.
- Torch.
- Sniffer de paquetes.

Estas son las principales características del sistema operativo y software Mikrotik RouterOS elegido para la implementación de la red.

5.2.2.2 Mini PCI para MikrotiK: La tarjeta mini pci Atheros se inserta en una placa Mikrotik Routerboard, o en cualquier computadora con adaptador de mini pci a Slot Pci, cada tarjeta mini PCI es un access point independiente, en una Mikrotik RB433 o 433AH puede agregar hasta 3 tarjetas mini pci (3 access points independientes) con antenas sectoriales totalmente diferenciados con canales diferentes.

- Cumple completamente con los estándares IEEE 802.11a/b/g proporcinando una velocidad de datos en conexión inalámbrica de hasta 108Mbps Alta Potencia.
- Permite autoconfiguración de la velocidad en función de la conexión, rango de transmisión y capcidad de: 54/ 48/ 36/24/ 18/ 12/11/ 9/ 6/ 5.5/ 2 / 1 Mbps.
- El modo Super A/G soporta hasta 108 Mbps para 802.11a/g Alta seguridad de red con 802.1x, Encriptación Wi-Fi Protected Access (WPA) y WEP.

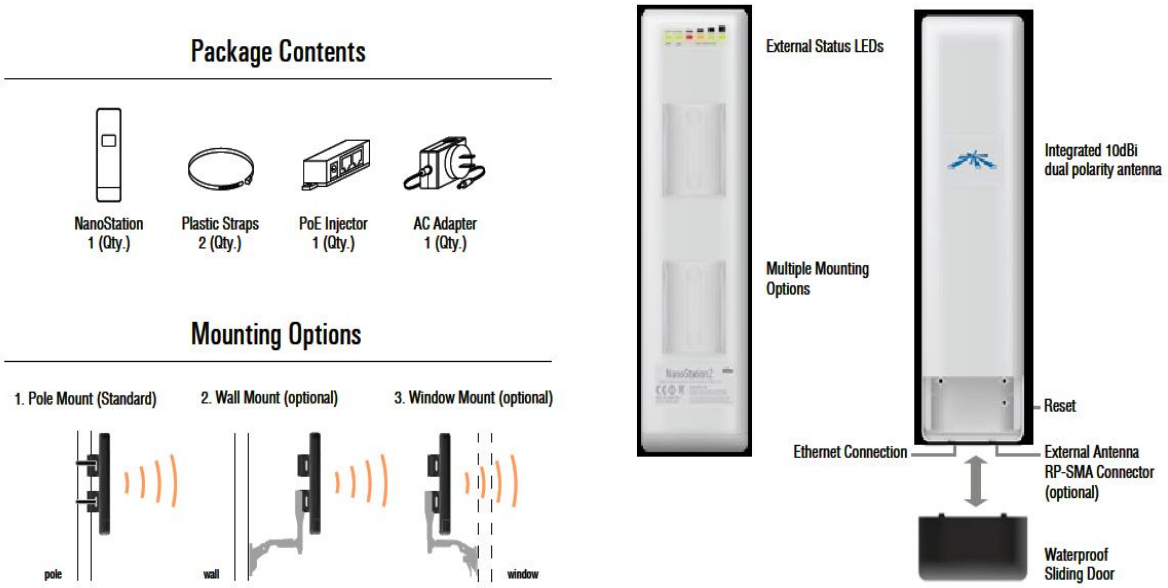
- Soporta los sistemas operativos más habituales: Windows 98SE/ME/2000/XP/Vista, LInux, RouterOS e Ikarus. Tarjeta Mini PCI de Tipo III-B. Mismo chipset que Ubiquiti XR2. Mayor sensibilidad.

Imagen 49 Mini PCI para MikrotiK

Fuente: Autores

5.2.2.3 Ubiquiti Networks Nanoestation2

Imagen 50 Ubiquiti NanoStation2



Fuente: www.ubnt.com/airos- manual técnico Ubiquiti Nano Station 2

Información del sistema

Procesador: Atheros AR2315 SOC, MIPS 4KC, 180MHz

Informacion de Memoria: 16MB SDRAM, 4MB Flash

Interfaces de red: 1 X 10/100 BASE-TX (Cat. 5, RJ-45) Ethernet Interface

Operación de Radiofrecuencia 2412-2462 MHz

Tabla 9 Especificaciones de frecuencia de un NanoStation2

TX SPECIFICATIONS				RX SPECIFICATIONS			
	DataRate	TX Power	Tolerance		DataRate	Sensitivity	Tolerance
802.11b	1Mbps	26 dBm	+/-1dB	802.11b	1Mbps	-97 dBm	+/-1dB
	2Mbps	26 dBm	+/-1dB		2Mbps	-96 dBm	+/-1dB
	5.5Mbps	26 dBm	+/-1dB		5.5Mbps	-95 dBm	+/-1dB
	11Mbps	26 dBm	+/-1dB		11Mbps	-92 dBm	+/-1dB
802.11g OFDM	6Mbps	26 dBm	+/-1dB	802.11g OFDM	6Mbps	-94 dBm	+/-1dB
	9Mbps	26 dBm	+/-1dB		9Mbps	-93 dBm	+/-1dB
	12Mbps	26 dBm	+/-1dB		12Mbps	-91 dBm	+/-1dB
	18Mbps	26 dBm	+/-1dB		18Mbps	-90 dBm	+/-1dB
	24Mbps	26 dBm	+/-1dB		24Mbps	-86 dBm	+/-1dB
	36Mbps	24 dBm	+/-1dB		36Mbps	-83 dBm	+/-1dB
	48Mbps	23 dBm	+/-1dB		48Mbps	-77 dBm	+/-1dB
	54Mbps	22 dBm	+/-1dB		54Mbps	-74 dBm	+/-1dB

Fuente: www.ubnt.com/airos- manual técnico Ubiquiti Nano Station 2

Resumen de Características técnicas del Nanostation2

Imagen 51 Integridad adaptativa

INTEGRATED ADAPTIVE ANTENNA POLARITY + EXTERNAL ANTENNA SUPPORT (4 OPTIONS TOTAL)			
Gain	10dBi (2400-2483.5MHz)	External Connector	RP-SMA
Polarization	Multi-Polarized	3dB Beamwidth Elevation	30 degrees
Polarization Selection	Software Controlled	3dB Beamwidth Azimuth	60 degrees

Azimuth

Elevation

PHYSICAL / ELECTRICAL / ENVIRONMENTAL	
Enclosure Size	26.4 cm x 8 cm x 3cm
Weight	0.4kg
Enclosure Characteristics	Outdoor UV Stabalized Plastic
Mounting Kit	Pole Mounting Kit included
Max Power Consumption	4 Watts
Power Supply	12V, 1A (12 Watts). Supply and injector included
Power Method	Passive Power over Ethernet (pairs 4,5+; 7,8 return)
Operating Temperature	-20C to +70C
Operating Humidity	5 to 95% Condensing
Shock and Vibration	ETSI300-019-1.4

Fuente: www.ubnt.com/airos- manual técnico Ubiquiti Nano Station 2

- CPU: Atheros 180MHz MIPS
- RAM:16MB RAM

- Flash: 4MB FLASH
- Wireless: 2.4GHz, 802.11b/g
- Channel width: 5/10/20MHz
- Antenna Gain: 10dBi x2
- Polarity: Adaptive Vertical/Horizontal
- Ext. Ant. Option: Yes, RP-SMA Connector
- Range: 15km+ (100km using ext ant.)
- Throughput: 25Mbps+ TCP/IP
- Mounting: Pole Mount (straps included)
- Accessories: Ubiquiti Window/Wall Mount (sold seperately)
- Size: 26.4cm x 8cm x 3cm
- Weight: 0.4 kg
- Power Supply: 12V, 1A POE (included)
- Approvals: FCC 15.247, IC, CE

5.2.2.4 Antena sectorial Hiperlink 120° HG2420P-120

Imagen 52 Antena sectorial Hiperlink 120° utilizada

Fuente: http://www.l-com.com/multimedia/datasheets/DS_HG2420P-120.PDF

Para este proyecto se Utilizan 3 antenas sectoriales descritas a continuación.

Aplicaciones:

- 2.4 GHz ISM Band
- IEEE 802.11b and 802.11g Wireless LAN
- Bluetooth®
- Public Wireless Hotspot
- WiFi
- Wireless Video Systems
- Wireless Internet Provider "cell" sites

La antena sectorial de panel HyperGain HG2420P-120 WiFi verticalmente polarizado combina una alta ganancia con una onda ancha de 120° . Su calidad profesional "cell site" está diseñada principalmente para proveedores de servicio en la banda ISM de 2.4 GHz. También se incluyen las aplicaciones para redes inalámbricas IEEE 802.11b y 802.11g , compatible con todas las marcas de AccessPoint (AP).

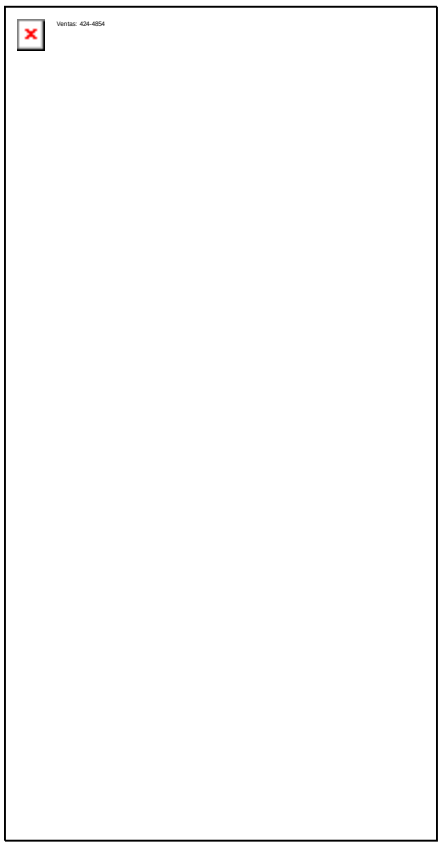
Debido a que esta antena está verticalmente polarizada, es ideal para uso en áreas suceptibles a interferencia donde operan equipos inalámbricos horizontalmente polarizados. Con la reducción de esta interferencia se puede lograr una mejor recepción de la señal inalámbrica.

Durable a Prueba de Mal Tiempo. Esta antena WiFi ofrece una cobertura de plástica durable y fuerte para operar en todo tipo de clima. El sistema de montaje permite instalaciones ajustables de 0 a 20 grados de inclinación. Ideal para proveedores de servicio inalámbrico, la cobertura Horizontal es total a 120 grados.

Especificaciones Eléctricas

Imagen 53 Patrón de radiación entena Hiperlink

- Frecuencia: 2400-2500 MHz
- Ganancia: 20 dBi
- Polarización: Vertical
- Ancho del lobulo Vertical: 5°
- Ancho del lobulo Horizontal: 120º
- Impedancia: 50 Ohm
- Max. Entrada de Poder : 250 Watts
- VSWR: < 1.3:1 avg.
- Protección Antirrayos: DC Short.



Especificaciones Mecánicas

- Conector: Integrado N-Hembra
- Peso : 12 lbs (5.44 kg)
- Dimensiones: 99 x 22.9 x 6.4 cm
- Material de la antena: Polimero UV
- Montaje : 2.0" diametro mastil max.
- Resistencia a vientos: Hasta 216 Km/h
- Temperatura de Operación: -40° C a 85° C
- RoHS Compliant: Si.

Fuente: http://www.l-com.com/multimedia/datasheets/DS_HG2420P-120.PDF

5.2.3 Dispositivos wi-fi suplementarios necesarios en el cliente

5.2.3.1 Adaptadores Inalámbricos PCMCIA: Los adaptadores PCMCIA y PCI ofrecen conectividad inalámbrica a los equipos portátiles, PDAs y PC de escritorio respectivamente de cada uno de los usuarios, permitiendo tener

un acceso confiable y seguro de acuerdo a las características de cada adaptador.

D-Link DWA-620 108 G: Impulsado por la tecnología 108 G de D-link, este adaptador proporciona un rendimiento inalámbrico de hasta 108Mbps. Al trabajar en conjunto con otros dispositivos Router o Access Point Wireless 108 G de D-Link, es posible lograr un rendimiento superior inalámbrico operando en el modo Turbo. Este adaptador PCMCIA de alto rendimiento es diseñado para usuarios que exigen un mayor rendimiento en sus redes.

Imagen 54 PCMCIA D-Link DWA-620

Fuente: http:// MEC-4923983-tarjeta-wireless-pcmciad-link-de-para-laptop-modelo-dwa-620-_JM

El adaptador Wireless PCMCIA DWA-620 108 G entrega un rendimiento inalámbrico sin igual y rentable para el PC portátil. Los usuarios pueden mejorar fácilmente la conexión a sus redes inalámbricas añadiendo este adaptador basado en el estándar 802.11g.

Una vez establecida la conexión es posible compartir en forma inalámbrica fotos, archivos, música, vídeo, impresoras, almacenamiento y acceso a internet. Además tendrá una conexión inalámbrica más rápida para realizar llamadas telefónicas digitales, juegos, descargas y streaming de video.

Linksys Wireless-G Notebook Adapter WPC54G: Es un Adaptador de red que posee un módulo para inserción tipo bus (CardBus), se utiliza para brindar conectividad inalámbrica a los usuarios de portátiles. Es compatible

con IEEE 802.11b, IEEE 802.11g, con una velocidad de transferencia de datos de 54 Mbps; que usa el protocolo TCP/IP.

Imagen 55 PCMCIA LINKSYS WPC54G

Fuente: http://www.linksysbycisco.com/US/en/products/WPC54G

Opera en la frecuencia de 2.4 GHz, y posee soporte DHCP. Además tiene una antena interna integrada, utiliza un algoritmo de cifrado: WEP de 128 bits, y una encriptación de 64 bits WEP, TKIP. El sistema operativo que requiere puede ser Microsoft Windows 98 Segunda Edición / Windows Milenium, Microsoft Windows 2000 / Windows XP.

CISCO PCMCIA Wireless 54 Mbps RANGEBOOSTE WPC200-EU: El adaptador de portátil Wireless-G con RangeBooster se puede instalar en la mayoría de los portátiles, y permite una conexión a internet en cualquier lugar de un edificio sin el coste y las molestias que supone la instalación de un cable. La tecnología RangeBooster es compatible con el estándar Wireless-G que incrementa la velocidad de la red en 2 veces, llegando incluso hasta 35% más.

Imagen 56 CISCO PCMCIA WPC200-EU

Fuente:http://www.markit.eu/es/es/wirelessg-notebook-adapter-rangebooster/v2p267229c455

En cuanto a seguridad el WPC200 usa un acceso protegido Wi-Fi (WPA2 Enterprise) de encriptación hasta 256-bit. Trabaja con una velocidad 54 Mbps, posee una interfaz (BUS) CardBus de 32 bits. Compatible con IEEE 802.11b y IEEE 802.11g y opera en la banda de frecuencia 2.4 GHz, y es compatible con Microsoft Windows 2000 y XP. La tabla 3.11 compara las cualidades de cada PCMCIA, a ser utilizada por los usuarios inalámbricos.

5.2.3.2 Adaptadores Inalámbricos PCI: Los adaptadores PCI, sirven para interconectar desktops o PC de escritorio, permitiendo al igual que los equipos portátiles la ventaja de tener una conexión inalámbrica fiable y segura.

D-link DWA-520 Wireless 108g PC: Este adaptador PCI opera hasta 108 Mbps de velocidad inalámbrica en modo Turbo, es compatible con 802.11b y 802.11g, con un rango extendido para ampliar cobertura inalámbrica. Además posee un asistente de Instalación Rápida Quick Router Setup.

Imagen 57 PCI D-LINK DWA-520

Fuente: http://www.markit.eu/es/es/tarjetas-inalambricos-enchufables/v1c457

utiliza una encriptación wep de 128 bits, wpa-psk, wpa2-psk, wpa-ea, wpa2-ea. trabaja en la frecuencia de 2.4/2.497 ghz, y soporta windows 98 se, me, 2000, xp, vista.

CISCO PCI WiFi 54 Mbps BUSINESS Rangebooster WMP200-EU La tarjeta PCI Wireless-G con RangeBooster se puede instalar en la mayoría de

los PCs, y le permite tener una conexión en cualquier punto de casa sin el coste y la incomodidad de instalar cables.

Imagen 58 CISCO PCI WMP200-EU

Fuente: http://www.markit.eu/es/es/tarjetas-inalambricos-enchufables/v1c457

La tecnología RangeBooster es compatible con el estándar Wireless-G y además incrementa el alcance 2 veces más. Trabaja a una velocidad de 54Mbps. Posee dos antenas exteriores omnidireccionales, con una ganancia de 2 dBi. Compatible con las normas IEEE 802.11b, IEEE 802.11g. Con un sistema operativo Windows 2000, Xp y un protocolo de seguridad WEP, WPA.

Linksys Wireless-G PCI Card WMP54G: La tarjeta PCI Card Wireless-G de Linksys se puede instalar en la mayoría de ordenadores de escritorio y permite situar el equipo en prácticamente cualquier lugar. Una vez conectado, puede utilizar el correo electrónico, acceder a Internet, utilizar servicios de mensajería instantánea para charlar con amigos y compartir archivos y otros recursos (impresoras y almacenamiento de red) con otros ordenadores de la red.

Imagen 59 PCI LINKSYS WMP54G

Fuente: http://www.markit.eu/es/es/tarjetas-inalambricos-enchufables/v1c457

La tarjeta PCI Card Wireless-G le permite conectar a las redes Wireless-G a 54 Mbps. Su versatilidad le permite funcionar con todos los productos Wireless-B (802.11b) de 11 Mbps y Wireless-G (802.11g) de 54 Mbps. Sea cual sea la opción que elija, las comunicaciones inalámbricas están protegidas por encriptación de 128 bits, por lo que los datos permanecen seguros. Además tiene una velocidad de transferencia de datos de 54 Mbps, con protocolo de transporte TCP/IP, IPX/SPX, NetBEUI/NetBIOS.

5.3 ESTUDIO DESCRIPTIVO DE LA RED ISP MAGOTIK

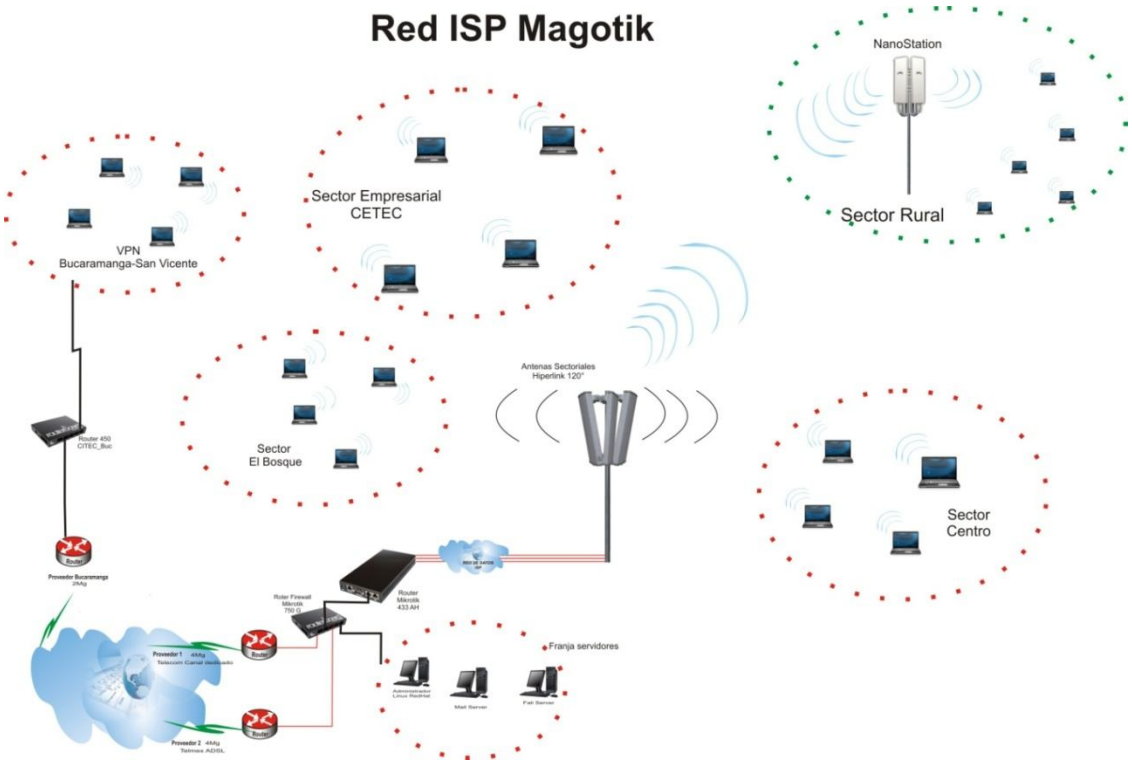
La red Magotik Wireless planteada para el Wisp posee cinco sub-redes (5).

- La Sub-Red 1- La franja de Servidores que cuenta el centro de centro de cómputo del Wips Magotik con Mail Server, File Server, Ftp, Bases de Datos y SNMP Server
- La Sud- Red 2 - El barrio el Centro cuenta con 20 clientes residenciales y 3 salas y 6 hoteles con conexión a internet.
- La Sub- Red 3 – Del Sector Empresarial se cuenta con la Empresa CITEC que se encuentra interconecta con la sede de la ciudad de Bucaramanga.
- La Sub- Red 4 – El barrio el Bosque cuenta con 30 clientes residenciales con conexión a internet.

- La Sub- Red 5 – El Sector Rural cuenta una escuela con 10 Equipos que tienen conexión a internet.

El Prototipo de Wips Magotik se encuentra en la oficina del Municipio de San Vicente de Chucuri- Santander, cuenta con router- Board 450G que poseen 5 puertos 10/100 Ethernet cada una. El sistema operativo para la implementación será Mikrotik RouterOs.

Imagen 60 Diagrama de equipos en la red inalámbrica planteada



Fuente: Autores

El router proveerá de varios servicios para la red. En los cuales podemos encontrar Servidor DHCP, Firewall, Servidor PPPoE, Cliente PPPoE, Servidor PPTP Server, Modelado de colas, Cliente NTP, Servidor NTP, Web Proxy, Hotspot.

El servidor DHCP, nos brindara las dirección de IP, Gateway, broadcast, dns para cada una de a las sub redes.

El Firewall se utilizará para las siguientes actividades:

- Bloqueo del cliente Comerciales MSN Live Messenger.
- Bloqueo P2P para redes comerciales Producción y Ventas.
- Re direccionamiento de puertos.
    - Puerto 80 WEB.
    - Puerto 110 POP3.
    - Puerto 25 SMTP.
    - Puerto 1723 PPTP.
- Descartar conexiones inválidas.
- Aceptar conexiones establecidas.
- Acepta Trafico UDP.
- Acepta paquetes de icmp Limitados.
- Descarta excesivos paquetes de icmp
- Descarta el resto de las conexiones externas

El servidor PPTP, será utilizado para interconectar las Empresa CITEC con la sede que está ubicada en la ciudad de Bucaramanga.

El modelado de colas se utilizará para asignarle un determinado ancho de banda a cada una de las sub redes. Al igual se utilizará el modelado de colas para el control de ancho de banda para los clientes P2P

El cliente NTP, se utilizará para sincronizar la hora de nuestro mikrotik. El servidor NTP se utilizará para que las computadoras de la red estén sincronizadas.

El Web Proxy se utilizará para filtrar el contenido que los usuarios realicen al navegar a través de Internet. Para ello se aplicaran las siguientes políticas:

- Bloqueo Pornografía.
- Bloqueo páginas que brinden el servicio de Web Messenger.
- Bloqueo del Live Messenger A Través del Proxy
- Bloqueo de páginas que brinden webmail
- Bloqueo descarga directa de archivos MP3 y AVI
- Bloqueo descarga directa de archivos RAR, ZIP, EXE

5.3.1 Sub Red Centro

La interconexión de la sub-red de Centro se dio debido al alto tráfico que tenían entre todos los clientes y como una mejor forma de administración.

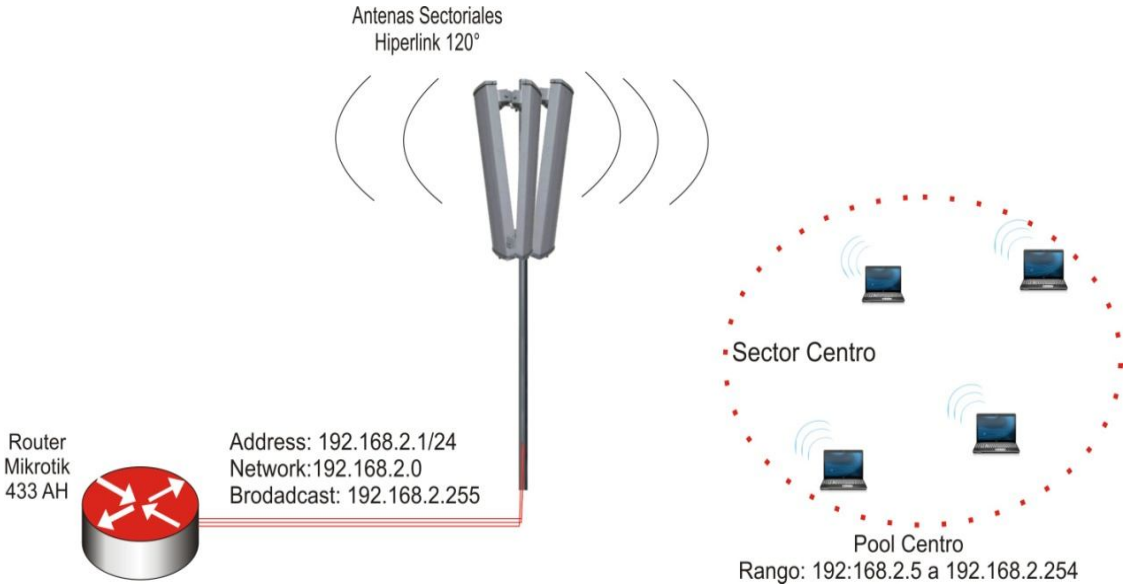
Las Direcciones de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde 192.168.2.5/24 al 192.168.2.254/24. Se decidió dejar las direcciones desde el 192.168.2.2/24 al 192.168.2.4/24 fuera de este rango para el caso de que se quieran instalar algún Dispositivos que nos irradien más en dicha área en un futuro próximo.

La red de Centro será conectada a través de las antenas Sectoriales y al router Board mediante un backbone de 10/100 Ethernet. El cual será limitado mediante teoría de colas simples a 64 Kb de subida y 64 Kb de descarga de bajada.

Debido a que dentro del sector Centro se encuentran Clientes que requieren acceso a programas de descarga como Ares y otros, se le deja configurada la utilización de los P2P para dichos clientes.

El trafico P2P será modelado para que no ocupe gran cantidad de ancho de banda.

Imagen 61 Esquema Sub red Centro



Fuente: Autores

5.3.2 Sub Red Empresarial CITEC

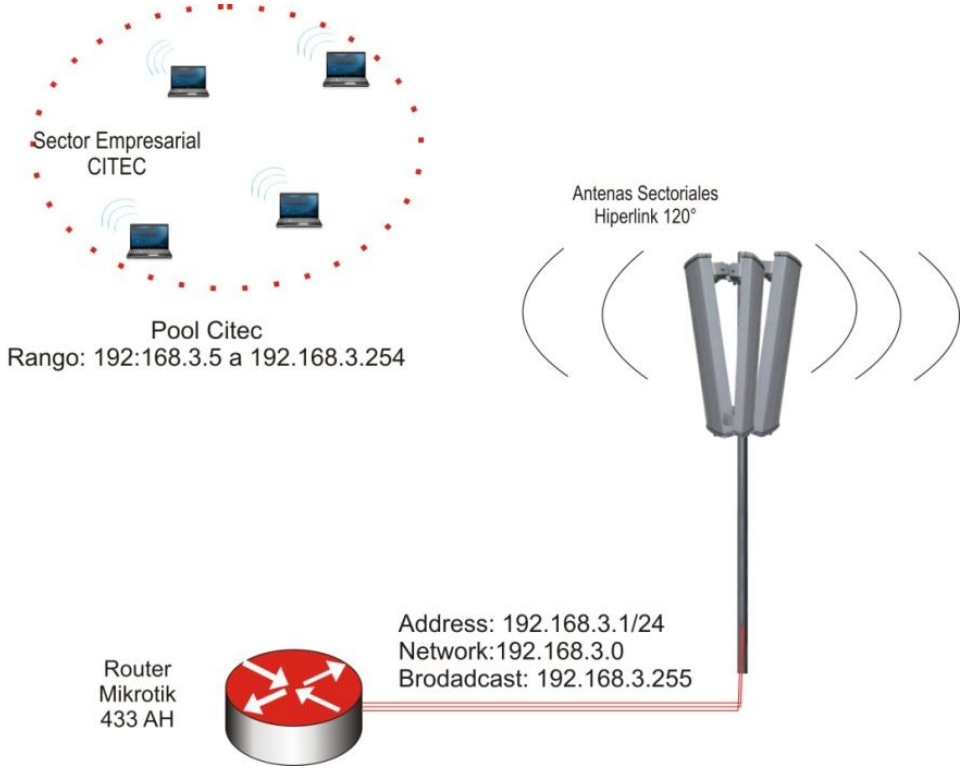
La interconexión inalámbrica de la sub-red de empresarial se estable que la mayoría de empresas necesita un alto rendimiento entre las sedes, en donde se va implementar una comunicación por medio de una Vpns entre Sede Principal San Vicente y la sede Bucaramanga, a estos clientes un buen servicio y una alta disponibilidad.

Las Direcciones de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde

192.168.3.5/24 al 192.168.3.254/24. Se decidió dejar las direcciones desde el 192.168.3.2/24 al 192.168.3.4/24 fuera de este rango para el caso de que se quieran instalar algún Servidor en el sector empresarial, dicha área en un futuro próximo.

La red de Empresarial será conectada inalámbricamente a través de las antenas Sectoriales y al router Board 450G mediante un backbone de 10/100 Ethernet. El cual será limitado mediante teoría de colas simples a 64 Kb de subida y 512 Kb de bajada. Debido a que dentro del sector Empresarial se encuentran Clientes que requieren una alta disponibilidad de sus sistemas de información.

Imagen 62 Esquema Sub red Emp. Citec

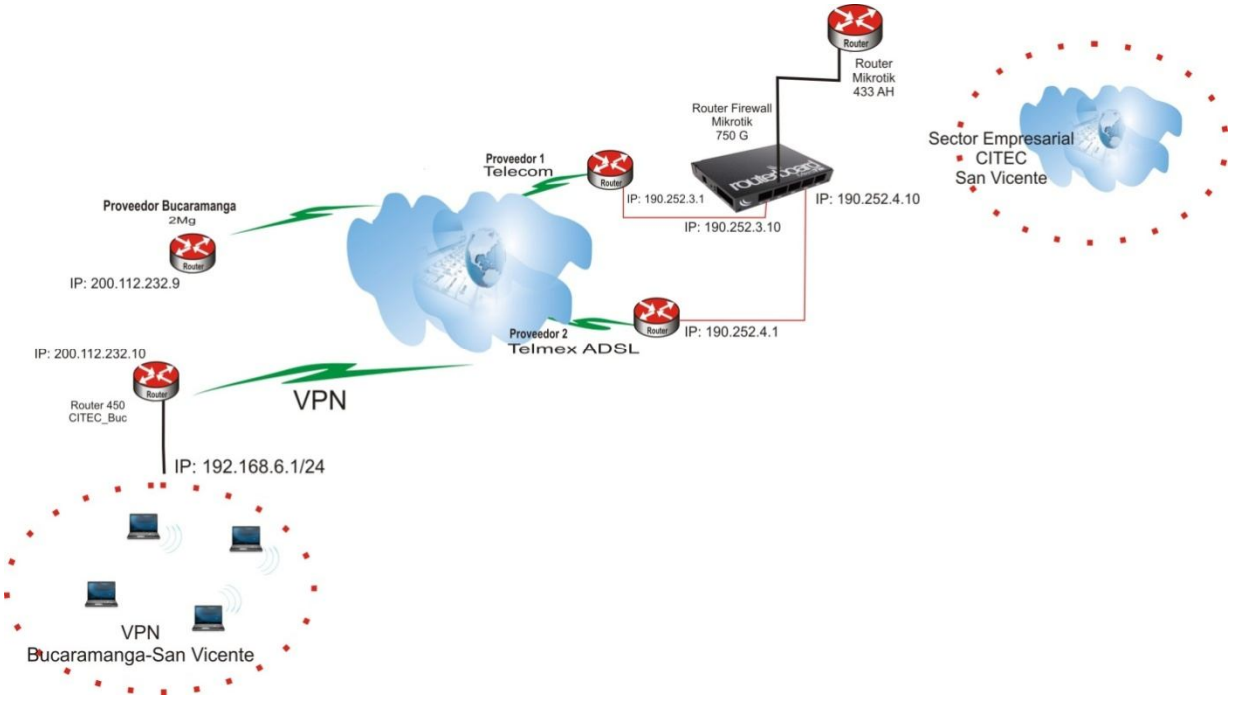


Fuente: Autores

5.3.3 VPN Bucaramanga – San Vicente (CITEC)

El Wisp Magotik en petición de un cliente empresarial que tiene la necesita de interconectar a su sede en B/ga. El Wisp Procede a establecerle una VPN, donde se le va a garantizar que su información sea priorizada por su túnel, en el cual su sistema de información dispondrá de un alto rendimiento del tráfico, garantizando los datos cliente Servidor.

Imagen 63 VPN Bucaramanga - San Vicente



Fuente: Autores

5.3.4 Sub Red Sector El bosque

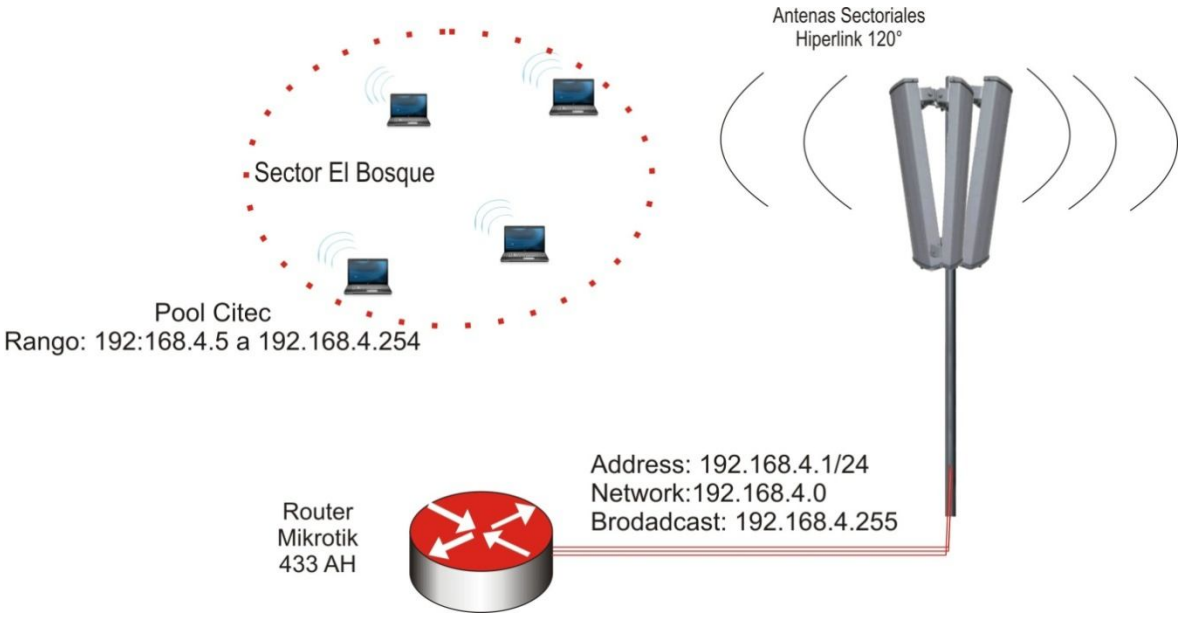
A la sub-red del Sector el Bosque se tiene un potencial de clientes residenciales alrededor de 30 usuarios que están navegando a todo momento visitando a sitio de descarga, paginas como YouTube, Facebook y

chats se mantiene un monitoreo del rendimiento de la red, que nos brinde una alta disponibilidad del canal para la Sub-Red.

Los Direcciones de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde 192.168.4.5/24 al 192.168.4.254/24 Se decidió dejar las direcciones desde el 192.168.4.2/24 al 192 .168.4.4/24 fuera de este rango para el caso de que se quieran instalar más dispositivos AP que irradien a mas cobertura a clientes se le serán asignadas estas Ip's.

La red del Sector el Bosque será conectada a través de las antenas Sectoriales principales y al router mediante un backbone de 10/100 Ethernet. El cual será limitado mediante calidad de servicio Qos en colas simples a 64 kb de subida y 64 Kb de bajada.

Imagen 64 Esquema Sub red El bosque



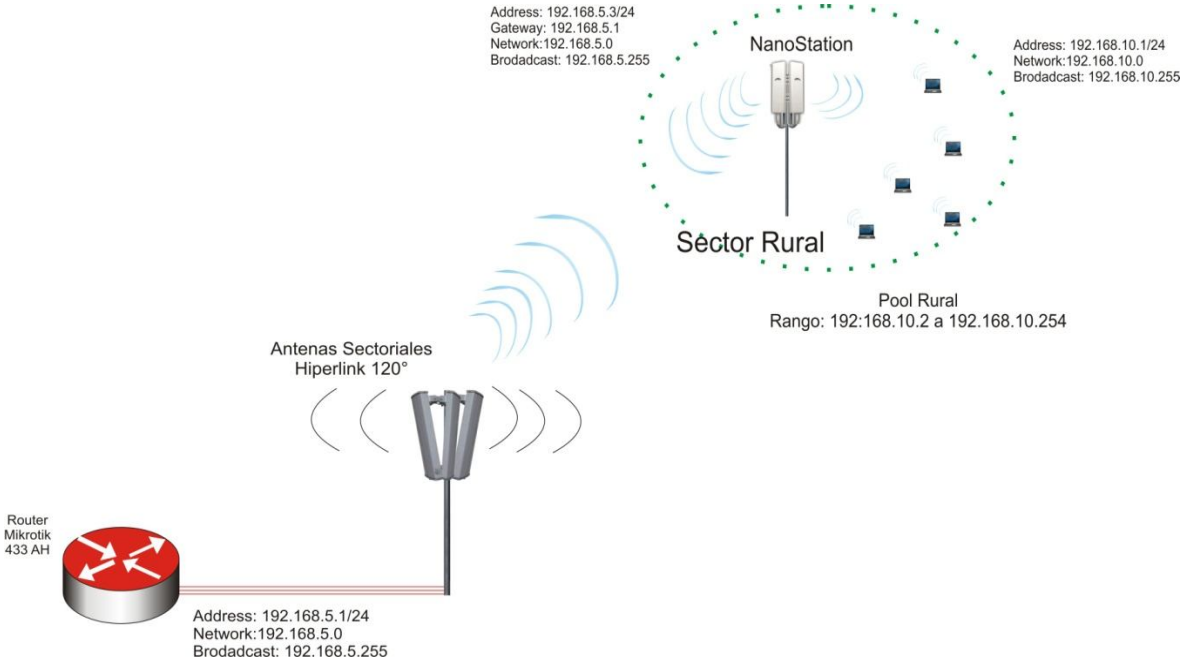
Fuente: Autores

5.3.5 Sub Red Rural

La red del Internet Rural es una nueva red que nos permitirá llevarle el internet a una Escuela Rural y demás fincas que alcancen la potencia la Wisp.; En donde se tiene una sala de informática con 10 pc´s que se configuraran sus tarjetas inalámbricas para tener la conexión al internet y al hotspot Magotik. Los números de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde 192.168.1.3/24 al 192.168.1.254/24.

Para la protección de los datos en la sección wireless se decidió asegurarlos mediante WPA PSK o WPA2 PSK. Esto nos dará fiabilidad y seguridad en los mismos. No obstante la seguridad WPAx que se desee implementar, todos los usuarios que se conecten al hotspot deberán ser autenticados la mac de los clientes.

Imagen 65 Esquema subred Rural



Fuente: Autores

La red del Internet Rural es una nueva red que nos permitirá llevarle el internet a una Escuela Rural y demás fincas que alcancen la potencia la Wisp.; En donde se tiene una sala de informática con 10 pc´s que se configuraran sus tarjetas inalámbricas para tener la conexión a internet y al hotspot Magotik.

Los números de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde 192.168.1.3/24 al 192.168.1.254/24.

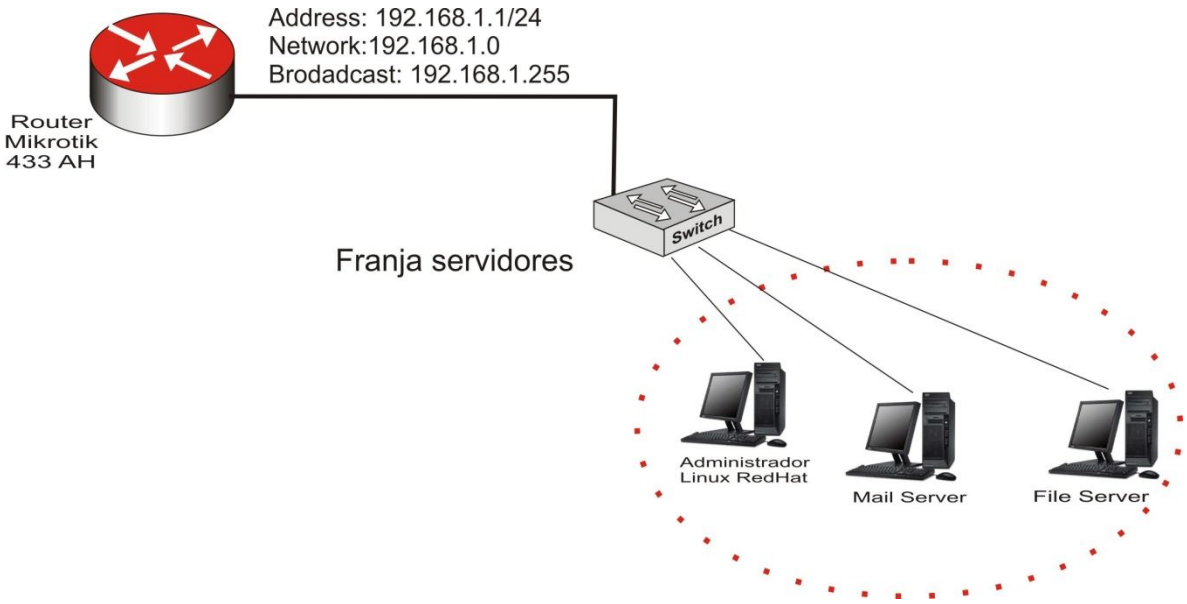
Para la protección de los datos en la sección wireless se decidió asegurarlos mediante WPA PSK o WPA2 PSK. Esto nos dará fiabilidad y seguridad en los mismos. No obstante la seguridad WPAx que se desee implementar, todos los usuarios que se conecten al hotspot deberán ser autenticados la mac de los clientes.

5.3.6 Sub Red Servidores

A la sub-red Franja de Servidores es donde se encuentras los diferentes servicios que puede prestar un Wisp desde Servicio de Hosting , Correo, Server Archivos, donde el backbone de interconexión entre el router y los Servidores se decidió que los puertos de conexión se trabaje 10/100/1000 Ethernet en donde se tiene un alto tráfico de información, eso nos permite una mejor disponibilidad de la administración de los Servicios de Internet.
Nuestra sub-red poseerá un pool de Servidores de red para esta sola área. Esto disminuirá el tráfico de los Servidores, al igual que el tráfico de personal ajeno a Administración.

Los números de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde 192.168.1.5/24 al 192.168.1.254/24. Los números de ip asignados a los servidores serán asignado mediante la dirección mac de cada uno. Asimismo se le instalará un servidor de archivos propio de administración en el cual se encontrará exclusivamente los archivos de dicha área.

Imagen 66 Esquema sub red Servidores



Fuente: Autores

5.3.7 Instalación y configuración de equipos

5.3.7.1 Instalación de Mikrotik RouterOS: A continuación vamos a mostrar paso por paso como se realiza la instalación de Mikrotik sobre una plataforma x86. La plataforma cuenta con 2 placas de red pci que poseen 4 bocas de red gigabyte Ethernet. Utilizaremos 2 bocas para conectarnos a dos proveedores de Internet distintos y una tercera para conectarnos a un proveedor de ADSL. El resto de las placas se utilizaran para la distribución de nuestra red interna.

Imagen 67 Instalación de paquetes de RouterOs

Utilizaremos la versión 2.9.27 Nivel 6 del software Mikrotik Router Os.

- Booteamos con un CD que contenga la imagen del Mikrotik RouterOs ya quemada.Luego nos aparecerá el menú de instalación que nos

Fuente: Autores – instalación mikrotik

- preguntará que paquetes deseamos instalar.
- Para desplazarnos por el menú utilizamos las tecla ´P´ o ´N´ o sino las flechas del teclado. Para seleccionar o deseleccionar los paquetes a instalar utilizamos la Barra Espaciadora.
- Luego presionamos la tecla ´I´ para comenzar la instalación local en nuestra plataforma.

Los paquetes seleccionados para nuestra configuración son los siguientes:

System: Paquete principal que posee los servicios básicos al igual que los drivers básicos.

- Ppp: Provee de soporte para PPP, PPTP, L2TP, PPPoE e ISDN PPP.
- Dhcp: Servidor y cliente DHCP.

- Hotspot: provee de un hot spot.
- Hotspot-fix: Provee el parche para actualizar el modulo hot spot que tiene problemas en las versión 2.9.27.
- Ntp: Servidor y cliente NTP.
- Routerboard: provee de las utilidades para el routerboard.
- Routing: Provee soporte para RIP, OSPF y BGP4.
- Rstp-bridge-test: provee soporte para Rapid Spanning Tree Protocol.
- Security: Provee soporte para IPSEC, SSH y conectividad segura con Winbox.
- Telephony: Provee soporte para H.323.
- Ups: provee soporte para UPS APC.
- User-manager: Servicio de usuario del RouterOs
- Web-Proxy: Paquete para realizar un Web Proxy.
- wireless-legacy: Provee soporte para placas Cisco Aironet, PrismII, Atheros entre otras.

Luego la instalación nos pregunta si deseamos quedarnos con la configuración anterior, contestamos que no ´N´.

La siguiente pregunta hace referencia a que perderemos todos los datos que se encuentran en el disco fijo le contestamos que si ´Y´.

Imagen 68 Aceptación de borrado de configuración antigua

Fuente: Autores – instalación mikrotik

A continuación comienza el proceso de particionado y formateado del disco fijo que es automático y no nos hace ningún tipo de preguntas. Luego nos dice que presionemos ´Enter´ para que el sistema se reinicie.

Seguidamente que se reinicia el sistema, nos pregunta si deseamos chequear la superficie del disco fijo le contestamos que si ´Y´. Luego comienza la instalación de los paquetes seleccionados con anterioridad. Al finalizar dicho proceso nos pide que presionemos ´Enter´ nuevamente para reiniciar el sistema

Imagen 69 Orden de rebuteo del sistema

Fuente: Autores – instalación Mikrotik

Con el sistema reiniciado e instalado, la consola nos pide el usuario y contraseña. Por defecto dicho nombre de usuario es: admin y para la contraseña se deja el casillero en blanco y se presiona enter.

Imagen 70 Ingreso a Mikrotik

Fuente: Autores – instalación Mikrotik

A continuación nos da la bienvenida y nos pregunta si deseamos leer la licencia lo cual contestamos que si ´Y´.

Imagen 71 Autorización de Verificación de licencia Mikrotik

Fuente: Autores – instalación Mikrotik

Luego de haber leído la licencia ya nos queda la consola para comenzar a configurar nuestro Mikrotik.

Imagen 72 Verificación de licencia Mikrotik

Fuente: Autores – instalación Mikrotik

5.3.7.2 Logueo al Mikrotik: Hay varias maneras para acceder a la administración del Mikrotik sin haber configurado nada en un principio.

La primera es directamente desde la consola finalizada la instalación, otro método es utilizando una consola Telnet a través del el puerto serie o Ethernet por mac o ip, sino mediante la utilización del software winbox, el cual lo brinda los desarrolladores de Mikrotik.

Debido a la flexibilidad, rapidez y ventajas que presenta la utilización de winbox respecto a los otros métodos, éste será la manera con la cual realizaremos la configuración de la red.

Desde una PC remota con Windows xp instalado. Conectados mediante un cable cruzado al Mikrotik al puerto Ethernet.

Hacemos correr el soft Winbox, el cual nos brindara una ventana para loguearse al Mikrotik.

Imagen 73 Ventana de Winbox

Fuente: Autores – Configuración WinBox

En esta ventana nos deja introducir las direcciones Mac o ip de la placa del Mikrotik a la cual estamos conectados. Debido a que no hemos configurado el Mikrotik desde la consola. Hacemos clic en (…) esto hará que el software

nos devuelva las direcciones Mac de las interfases de red que posean un Mikrotik instalado y corriendo.

Seleccionamos la interfase y luego utilizaremos de Login: admin y como Password: (nada).

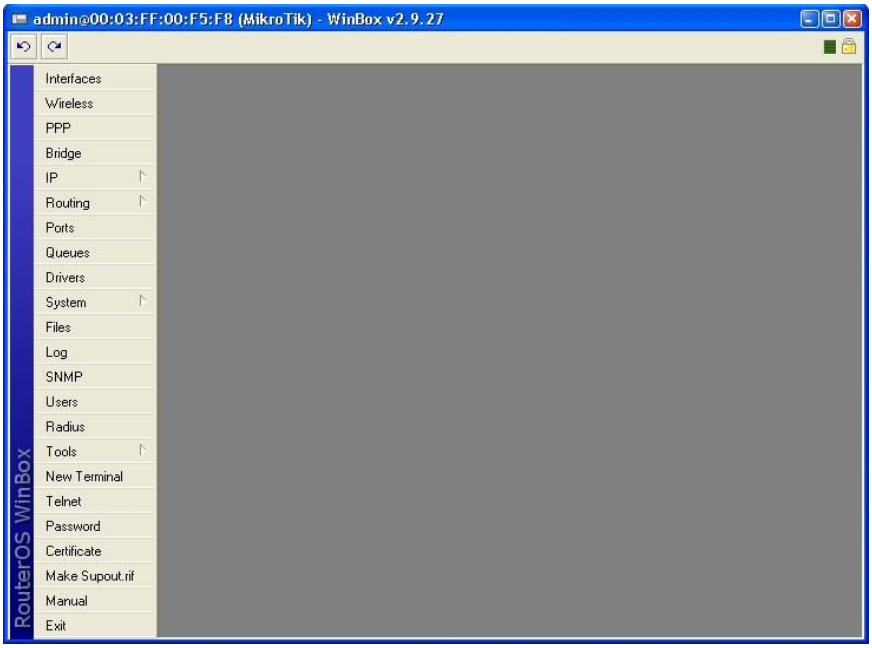
Al finalizar esta carga de datos hacemos clic en Connect. Luego cuando el soft se conecta al Mikrotik automáticamente empieza a descargar los plugins instalados en el Mikrotik para poder administrarlos remotamente.

Imagen 74 actualización de plugins para la mac seleccionada

Fuente: Autores – Configuración WinBox

Al finalizar la descarga de los plugins nos aparece la pantalla de configuración del Mikrotik. En la cual a mano izquierda se encuentra el menú de configuración de cada uno de los módulos instalados.

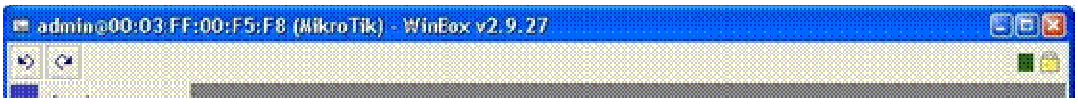
Imagen 75 Ventada de configuración de Mikrotik



Fuente: Autores – Configuración Mikrotik

En la barra superior del software nos encontramos con la barra de herramienta. En la misma sobre mano izquierda posee las opciones de undo y redo. Sobre mano derecha podemos encontrar dos iconos, el primero muestra la utilización del Mikrotik y el segundo nos indica si la conexión que estamos realizando es segura o no.

Imagen 76 Barra de herramientas

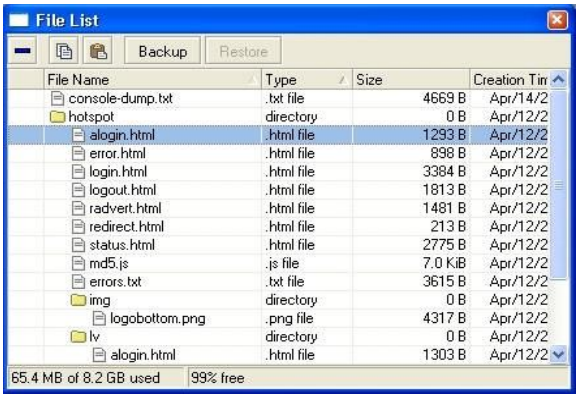


Fuente: Autores – Configuración Mikrotik

5.3.7.3 Backup y Restore de Configuración: Debido a los problemas que pueden producirse en los equipamientos, siempre es buena política tener back up de todas las configuraciones de los sistemas. Ahora mostraremos como se realizar un backup de la configuración y como se recupera.

5.3.7.4 Backup de la configuración: Primero nos Dirigimos al menú FILES allí se nos abrirá una ventana y nos mostrará los archivos que se encuentran almacenados. Debemos hacer clic sobre el botón de BACKUP para realizar nuestro backup.

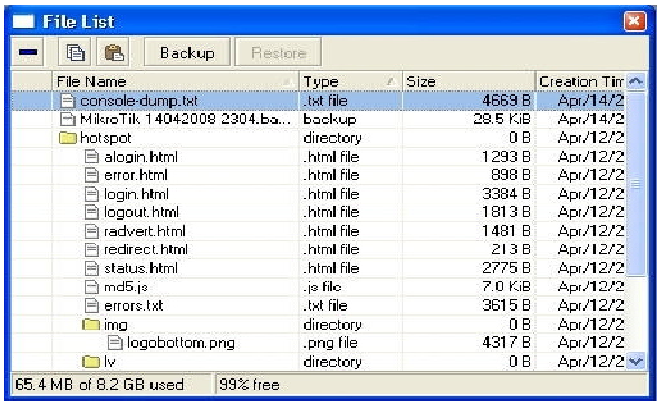
Imagen 77 Ventana de configuración de Backup de la Mikrotik



Fuente: Autores – Configuración Mikrotik

Luego de haber hecho clic nos aparece un nuevo archivo en la lista que poseíamos, que es nuestro backup de toda la configuración del Mikrotik.

Imagen 78 Lista de archivos en la Mikrotik

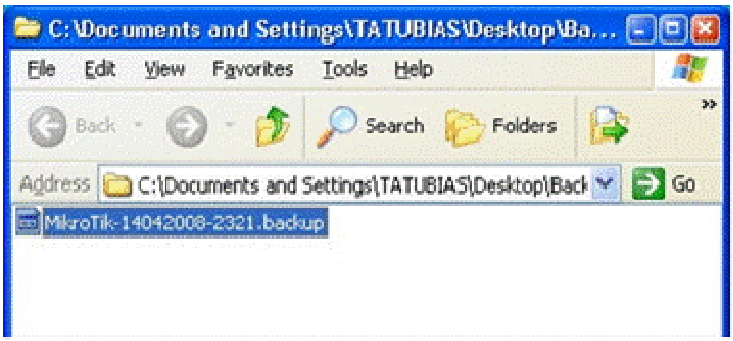


Fuente: Autores – Configuración Mikrotik

Sabiendo que el almacenamiento puede fallar, siempre es bueno tener una copia de resguardo en otro sitio. Para ello debemos hacer lo siguiente. Seleccionamos el archivo de backup que deseamos y luego hacemos clic

sobre el icono de COPY. Esto hará que nuestro archivo de configuración quede almacenado en el porta papeles de Windows. A continuación creamos una carpeta en el disco fijo de la PC y pegamos el archivo. Nos aparecerá y ya tendremos el backup de nuestro archivo de configuración en nuestra PC.

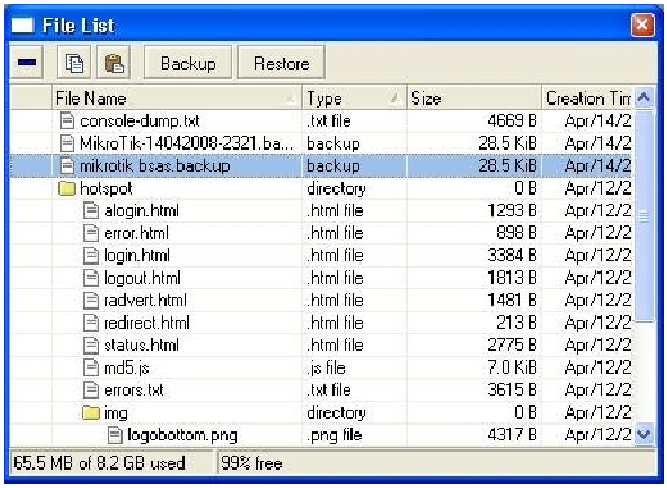
Imagen 79 Archivo Backup de Microtik en el disco local



Fuente: Autores – Configuración Mikrotik

5.3.7.5 Restore de la configuración: Si estamos recuperando el archivo de configuración que está dentro del Mikrotik. Simplemente debemos ir al menú FILES. En la ventana que nos aparece debemos seleccionar la versión del backup que deseamos recuperar y hacer clic sobre el botón de RESTORE.

Imagen 80 Lista de archivos a restaurar en Router Mikrotik

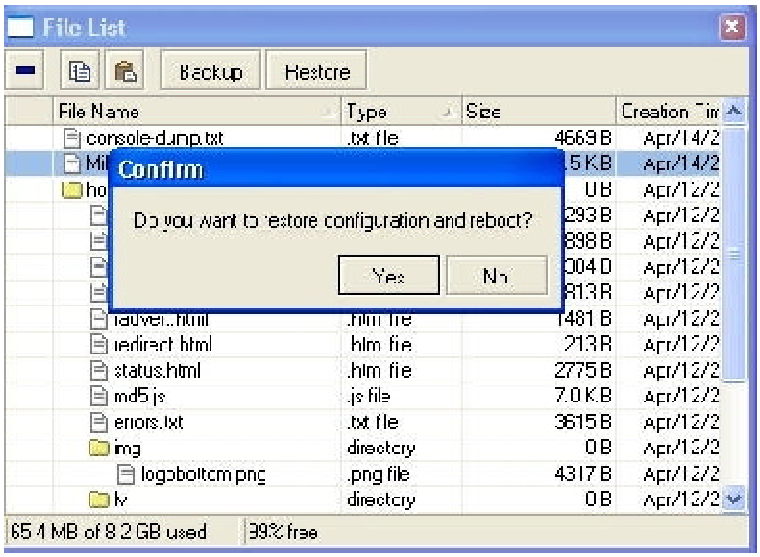


Fuente: Autores – Configuración Mikrotik

Para el caso que el archivo de back up se encuentre en nuestro disco fijo. Seleccionamos el archivo de backup, luego hacemos clic con el botón derecho del mouse y seleccionamos copiar. Luego en el winbox, simplemente debemos ir al menú FILES.

En la ventana que nos aparece, debemos hacerle clic en el icono de pegar y nos aparecerá nuestra nueva configuración. A continuación seleccionamos nuestra nueva con figuración y apretamos el botón de restore. Se nos abrirá una nueva ventana que nos aplicara la nueva configuración y nos hará reiniciar nuestro Mikrotik.

Imagen 81 Configuración de Reinicio de sistema tras restauración de Backup



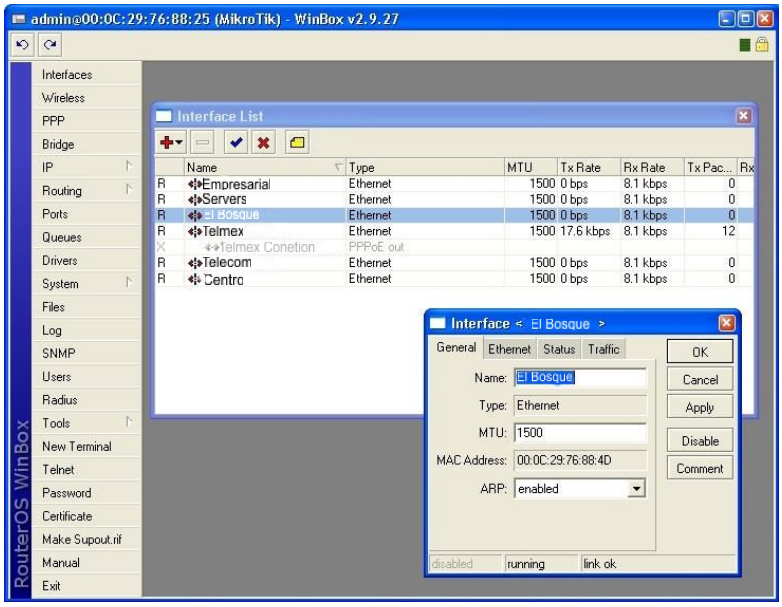
Fuente: Autores – Configuración Mikrotik

5.3.8 Asignación de nombres a las interfaces

Nos dirigimos al menú y elegimos INTERFACES. A continuación nos aparece la lista de interfases que posee nuestro sistema. Hacemos doble clicks sobre las interfaces y les vamos cambiando el nombre asignándole los nombres correspondientes a cada una. En nuestro caso utilizaremos:

- Telecom, para nuestra conexión dedicada con IP fijo.
- ADSL: Será la interface para conectarse al ADSL de Telmex, otro proveedor de internet.
- Centro: Será la interface exclusiva de usuarios centro ciudad.
- Empresarial: Será la interface exclusiva empresas en este caso Citec.
- Bosque: Será la interface exclusiva de Clientes sector bosque
- Servers: Será la interface para la granja de servidores
- Rural: será la interface que proveerá acceso a la red mediante el hotspot

Imagen 82 Definición de interfaces en Mikrotik



Fuente: Autores – Configuración Mikrotik

Interface: Telmex

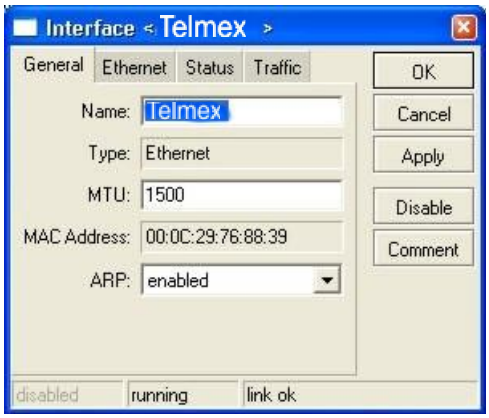
Pestaña General:

Name: Telmex

MTU: 1500

ARP: Enable

Imagen 83 Configuración de Interface Telmex



Fuente: Autores – Configuración Mikrotik

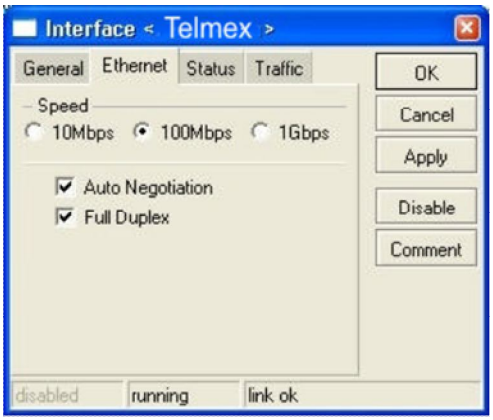
Pestaña Ethernet: 100

Mbps: Seleccionado

Auto negotiation: seleccionado

Full duplex: seleccionado.

Imagen 84 Configuración de velocidad

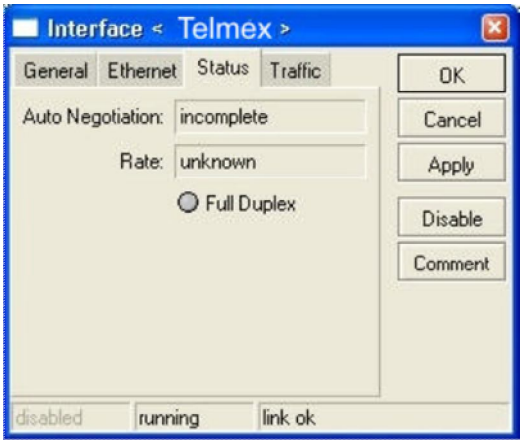


Fuente: Autores – Configuración Mikrotik

Pestaña Status:

En esta ventana podemos ver el estatus la interface actual.

Imagen 85 Estado de la interfaz



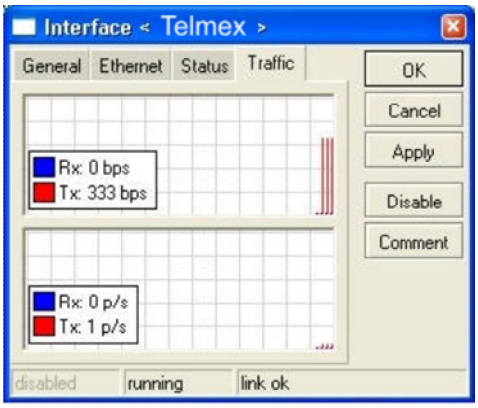
Fuente: Autores – Configuración Mikrotik

Pestaña Traffic:

Vemos la grafica de kbps enviados y recibidos por dicha interface.

Vemos la grafica de p/s enviados y recibidos por la interface.

Imagen 86 Ventana de tráfico de la interfaz



Fuente: Autores – Configuración Mikrotik

Interface: Telecom

Pestaña General:

Name: Telecom

MTU: 1500

ARP: Enable

Imagen 87 Configuración de interfaz Telecom

Fuente: Autores – Configuración Mikrotik

Interface: Centro

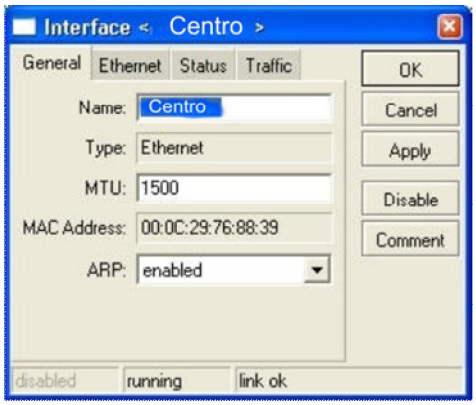
Pestaña General:

Name: Centro

MTU: 1500

ARP: Enable

Imagen 88 Configuración interfaz Centro



Fuente: Autores – Configuración Mikrotik

Interface: Rural

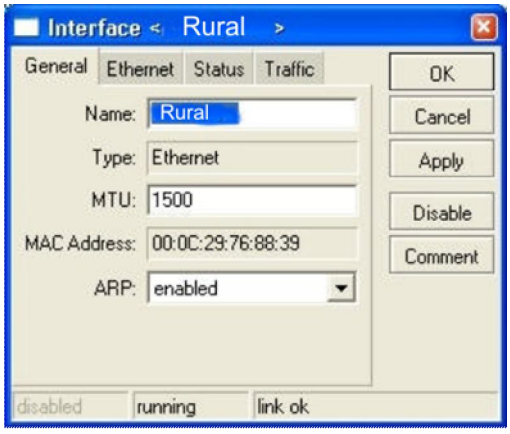
Pestaña General:

Name: Rural

MTU: 1500

ARP: Enable

Imagen 89 Configuración interfaz Rural



Fuente: Autores – Configuración Mikrotik

Interface: Empresarial

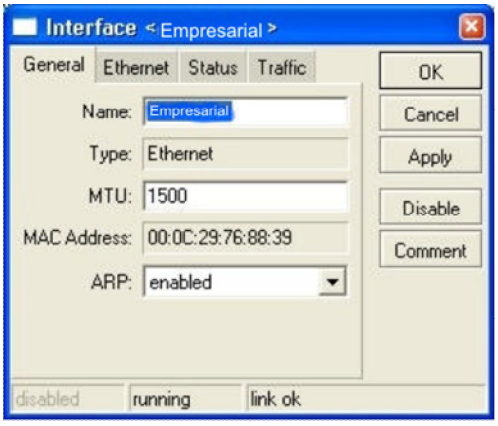
Pestaña General:

Name: Empresarial

MTU: 1500

ARP: Enable

Imagen 90 Configuración interfaz Empresarial



Fuente: Autores – Configuración Mikrotik

Interface: Bosque

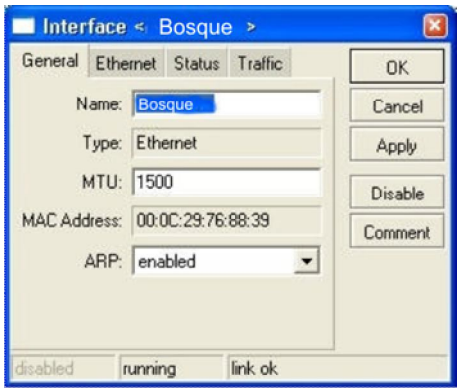
Pestaña General:

Name: Bosque

MTU: 1500

ARP: Enable

Imagen 91 Configuración interfaz Bosque



Fuente: Autores – Configuración Mikrotik

5.3.9 Definición de Vlans

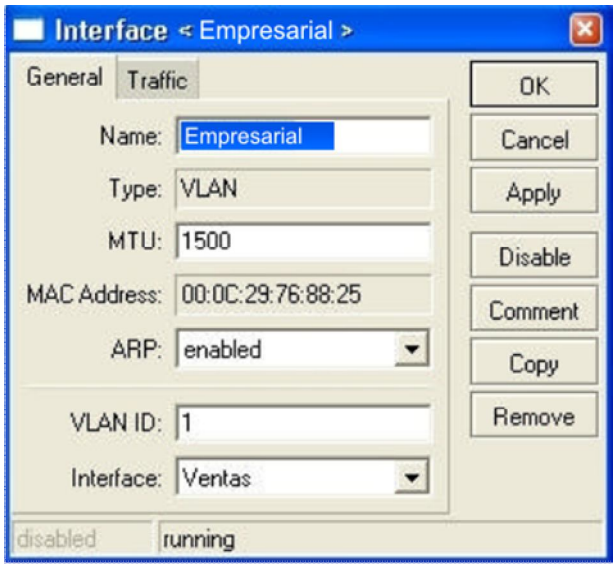
Debido a las características de la red debemos realizar 5 vlans para sectorizar y dar mayor rendimiento a nuestros clientes:

- Centro
- Empresarial
- Bosque
- Rural
- servers

Para configurar las vlans debemos ir al menú Interfaces, se nos abrirá la ventana de configuración de interfaces. Hacemos clic sobre el icono (+) y se nos desplegará un menú, elegimos la opción Vlan y entramos a la ventana de configuración de las mismas.

Vlan Empresarial

Imagen 92 Configuración de Vlan



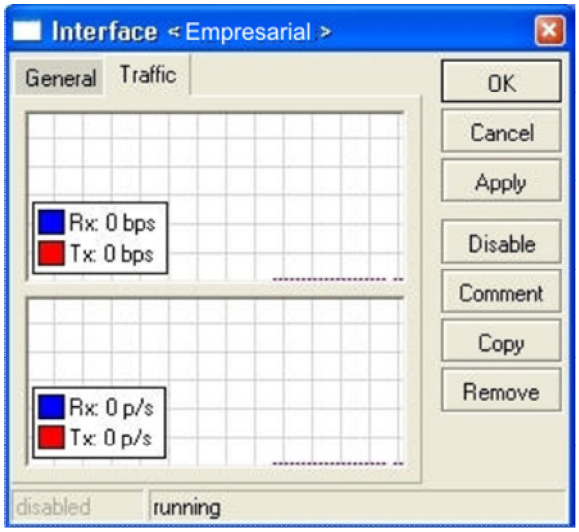
Fuente: Autores – Configuración Mikrotik

Pestaña Traffic:

Ver la grafica de kbps enviados y recibidos por dicha vlan

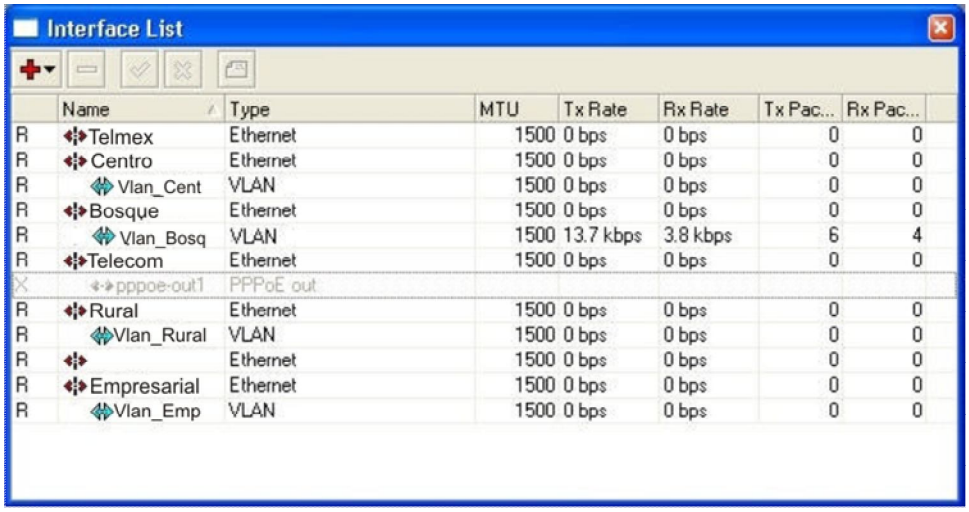
Ver la grafica de p/s enviados y recibidos por la vlan

Imagen 93 Ventana de trafico Interfaz Empresarial



Fuente: Autores – Configuración Mikrotik

Imagen 94 Imagen de Vlans finales

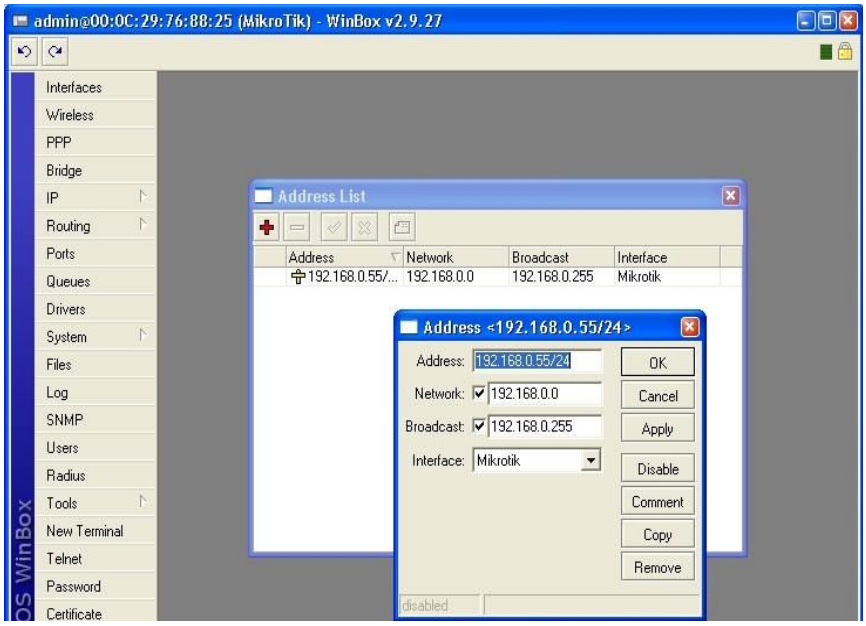


Fuente: Autores – Configuración Mikrotik

5.3.10 Asignación de Direcciones IP´s a las interfaces

Con los nombres asignados a las interfaces, debemos asignarle el IP a las mismas. Para ello debemos ir al menú IP / Addresses

Imagen 95 Asignación de IP a las interfaces



Fuente: Autores – Configuración Mikrotik

Haciendo clic sobre el icono (+) nos abre una ventana que nos deja introducir los datos necesarios para nuestras interfaces.

Interfase Telecom:

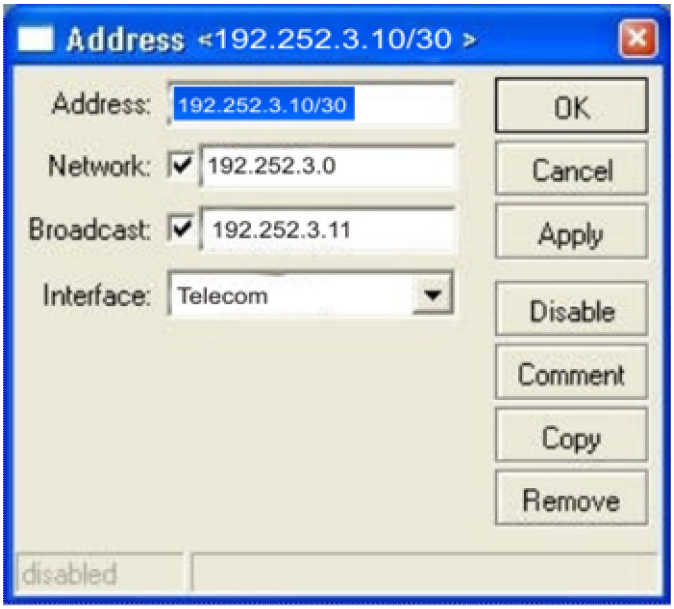
Address: 190.252.3.10/30

Network 190.252.3.0

Broadcast: 190.252.3.11

Interfase: Telecom

Imagen 96 Ventana de asignación de IP a la interfaz Telecom



Fuente: Autores – Configuración Mikrotik

Interface Centro:

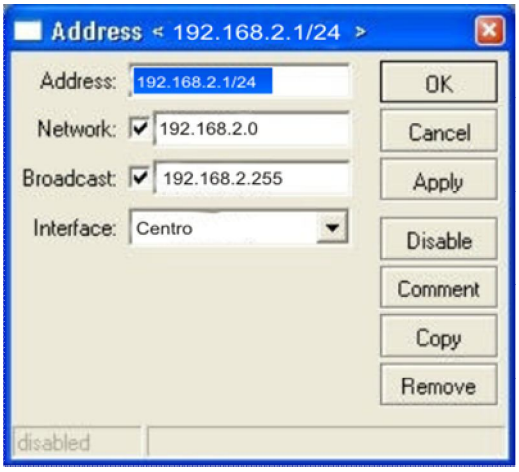
Address: 192.168.2.1/24

Network: 192.168.2.0

Broadcast: 192.168.2.255

Interface: Centro

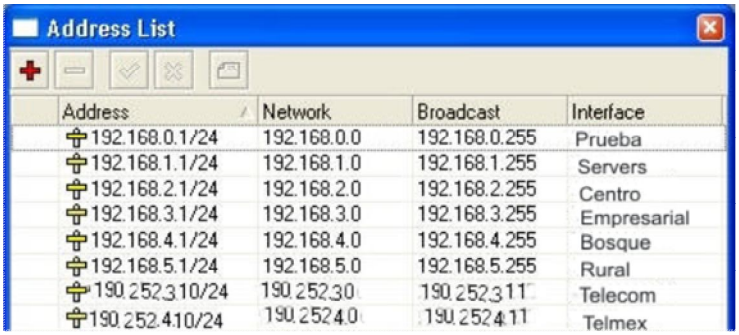
Imagen 97 Ventana de asignación de IP en interfaz Centro



Fuente: Autores – Configuración Mikrotik

La configuración de Interfaces es igual para todas, luego la Tabla Final de asignación de Ips a las interfaces queda como se muestra en la imagen.

Imagen 98 Lista final de asignación de ip a las interfaces



Fuente: Autores – Configuración Mikrotik

5.3.11 Definición de UPnP para las interfaces

En este segmento simplemente tenemos que definir cuáles de nuestras interfaces van a “mirar hacia Internet” y cuáles van a estar dentro de nuestra red. Nosotros configuraremos a las conexiones como:

Empresarial: interna.

Centro: Interna

Bosque: Interna

Servers: Interna

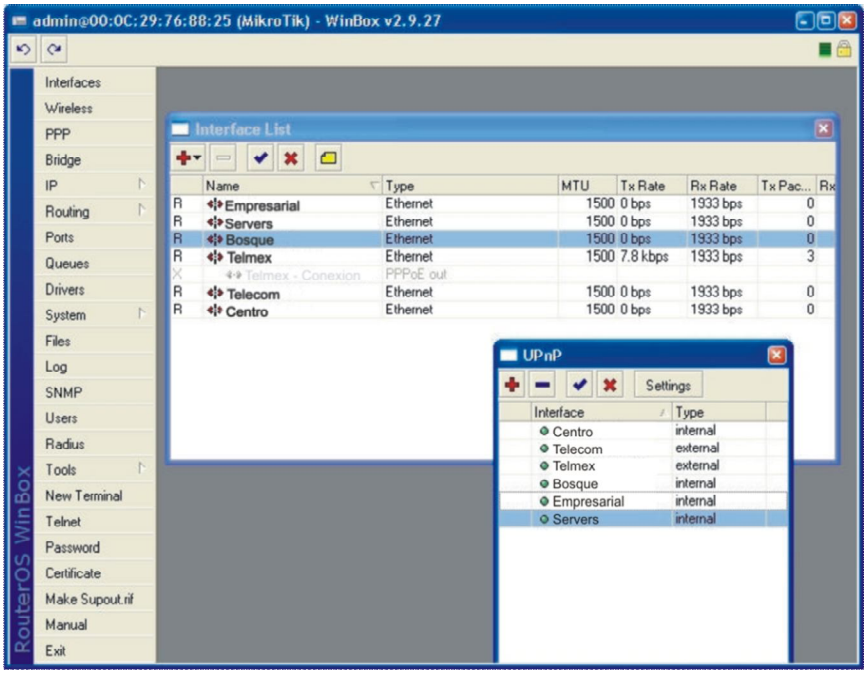
Rural: Interna

Telecom: Externa.

Telmex: Externa

Para realizar dicha configuración debemos ir en el menú a: IP / UNPnP. Hacemos clic sobre el icono (+) y asignamos a cada una de las interfaces si es interna o externa.

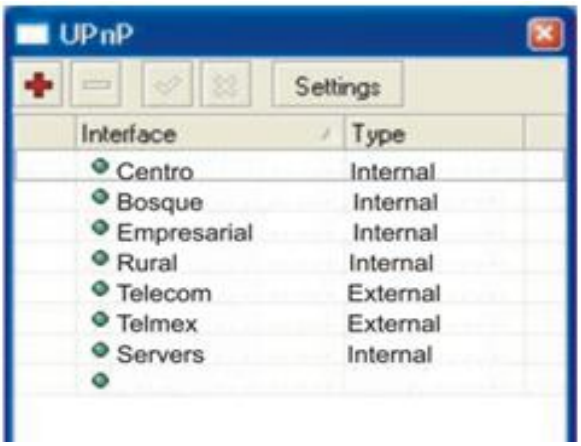
Imagen 99 Ventana de configuración de UPnp



Fuente: Autores – Configuración Mikrotik

Luego de haber asignado los tipos de interface debemos configurar un último detalle en settings. Le deseleccionamos la opción “allow to disable External Interfase”

Imagen 100 Tipos de interfaces



Fuente: Autores – Configuración Mikrotik

5.3.12 Configuración Pools de Direcciones de IP

En una primera instancia hay que crear los pool's de ip´s que van a poseer los grupos de Centro, Empresarial, Bosque y servers.

Para ello Vamos al menú IP / POOL. Se nos abre la ventana de configuración de pool y hacemos clic en el icono (+). En la nueva ventana creamos cada pool para cada una de los grupos. La configuración de los mismos es:

Nombre: Pool Servers

Rango de ip: 192.168.1.5 a 192.168.1.254

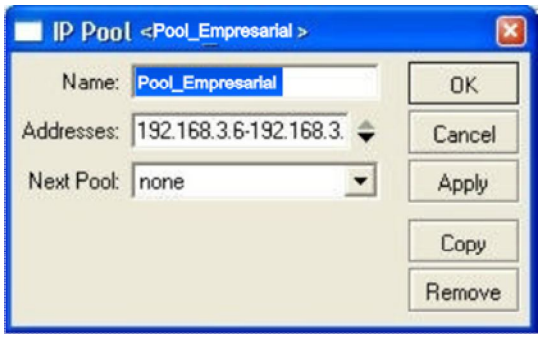
Imagen 101 Pool de direcciones segmento servers

Fuente: Autores – Configuración Mikrotik

Nombre: Pool Empresarial

Rango de ip: 192.168.2.5 a 192.168.2.254

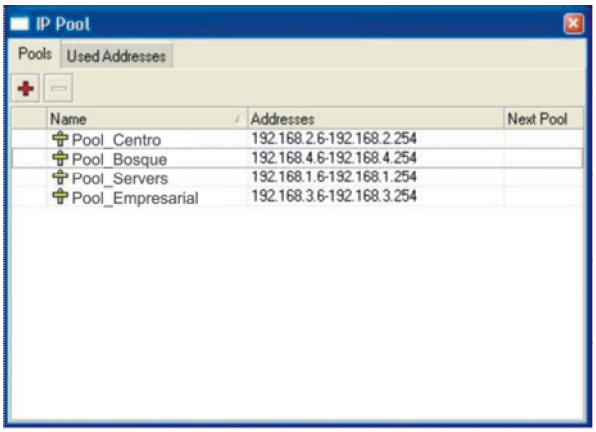
Imagen 102 Pool de direcciones Segmento Empresarial



Fuente: Autores – Configuración Mikrotik

Final mente la tabla de Pool de direcciones queda de la siguiente manera:

Imagen 103 Pool de direcciones final

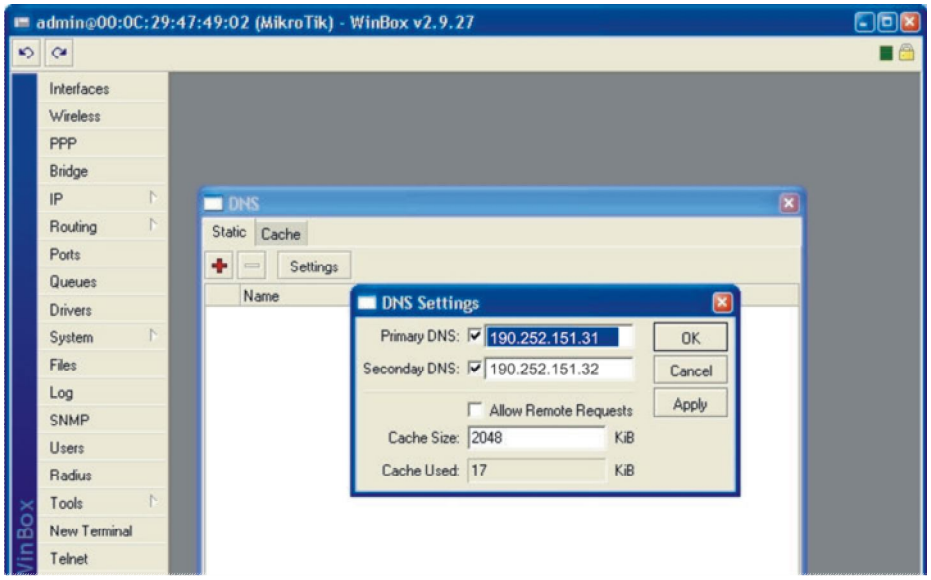


Fuente: Autores – Configuración Mikrotik

5.3.13 Configuración de DNS

Para definir los DNS simplemente hay que ir al menú IP / DNS. Se nos abre una ventana de configuración. Hacemos clic en Settings y escribimos los dns del proveedor de Internet.

Imagen 104 Configuración de DNS



Fuente: Autores – Configuración Mikrotik

Los datos que ingresados son:

Primary DNS: 190.252.151.31

Secondary DNS: 190.252.151.32

5.3.14 Nat Masquerade para todas las redes

Par realizar el nat transparente entre todas las redes debemos ir al menú IP/FIREWALL. Ahí en la nueva ventana nos dirigimos a la pestaña NAT y hacemos clic sobre el icono (+). A continuación aparece una ventana nueva de configuración para políticas de NAT y la configuramos de la siguiente manera:

Pestaña General:

Chan: srcnat

Imagen 105 Configuración de NAT Mascarade

Fuente: Autores – Configuración Mikrotik

Pestaña Action:

Action: masquerade

Imagen 106 Action del NAT

Fuente: Autores – Configuración Mikrotik

5.3.15 Configuración Servidor DHCP

A continuación daremos de alta el servidor de DHCP en si. Para ello debemos ir al menú IP / DHCP Server. Se nos abrirá una ventana de configuración de servidores dhcp. Hacemos clic en el icono (+) y creamos nuestros servidores de dhcp para cada una de las áreas ya mencionadas.

Ventana de configuración DHCP:

En esta ventana iremos introduciendo todos los requisitos necesario para ir levantado los servidores de dhcp. La configuración para cada uno de los servidores dhcp fue la siguiente:

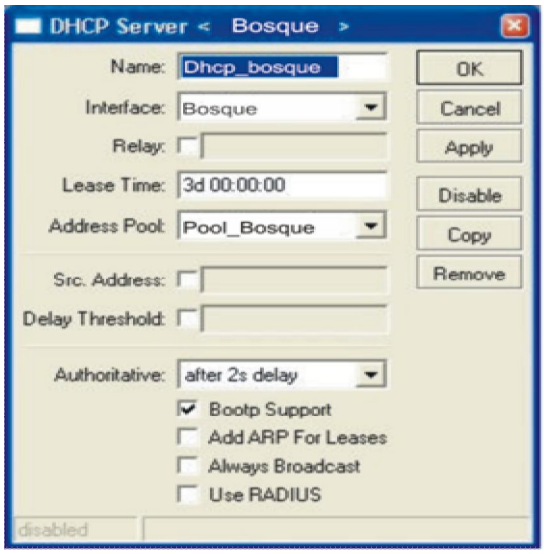
DHCP Bosque:

Nombre: DHCP Bosque

Interface: Bosque

Address Pool: Pool Bosque

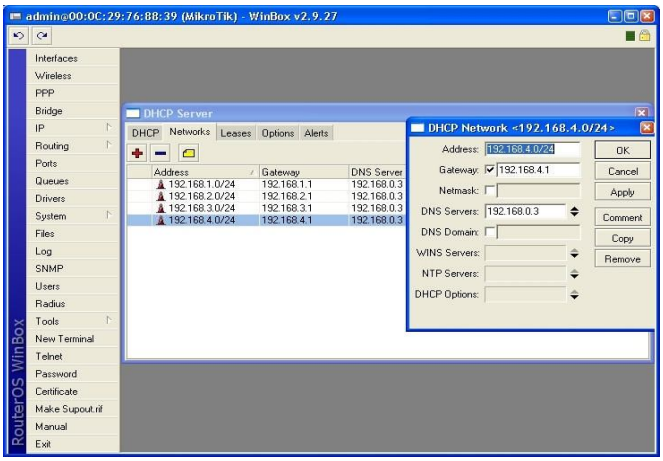
Imagen 107 Configuración de DHCP sector Bosque



Fuente: Autores – Configuración Mikrotik

La configuración de las demás áreas es de la misma forma, para nuestro caso se omiten en la explicación. Una vez configurados los servidores, necesitamos configurar las ´redes´. Para ello en la ventana de DHCP Server hacemos clic en la pestaña Network. Luego hacemos clic en el icono (+) y cargamos los datos de la red.

Imagen 108 Configuración final de DHCP en todas las áreas



Fuente: Autores – Configuración Mikrotik

Configuración:

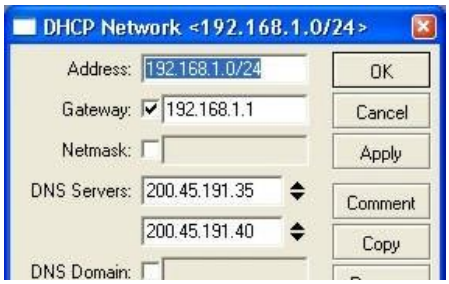
Red Servers:

Address: 192.168.1.0/24

Gateway: 192.168.1.1

Dns Server: 192.168.0.3

Imagen 109 Definición de DNS



Fuente: Autores – Configuración Mikrotik

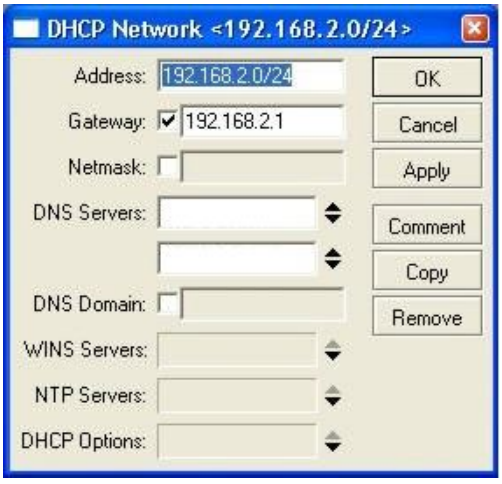
Red Centro:

Address: 192.168.2.0/24

Gateway: 192.168.2.1

Dns Server: 192.168.0.3

Imagen 110 Definición DNS red Centro



Fuente: Autores – Configuración Mikrotik

La configuración de las demás redes es similar para efecto de este documento se omitirán.

5.3.16 Asignación de direcciones de ip fijas a partir de direcciones MAC

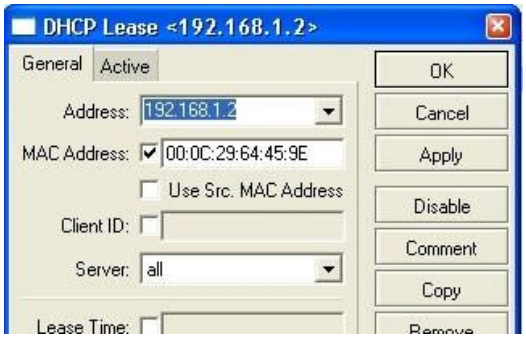
Debemos asignarle ip fijo a nuestros servidores para que sea más simple nuestra configuración del sistema. Para ello la asignación de ip fijo la hacemos mediante el servidor de dhcp, asignando una dirección de ip fija a una Mac.

Los pasos de configuración son los siguientes. Nos dirigimos al menú IP / DHCP Server. En la ventana que nos aparece hacemos clic en la pestaña LEASES. En mencionada pestaña hacemos clic en el icono (+). La configuración de la ventana es:

Server de snmp:

Address: 192.168.1.2
MAC Address: 00:0C:29:64:45:9E (MAC del servidor snmp)
Servers: all

Imagen 111 Asignación de direcciones de ip fijas a partir de direcciones MAC



Fuente: Autores – Configuración Mikrotik

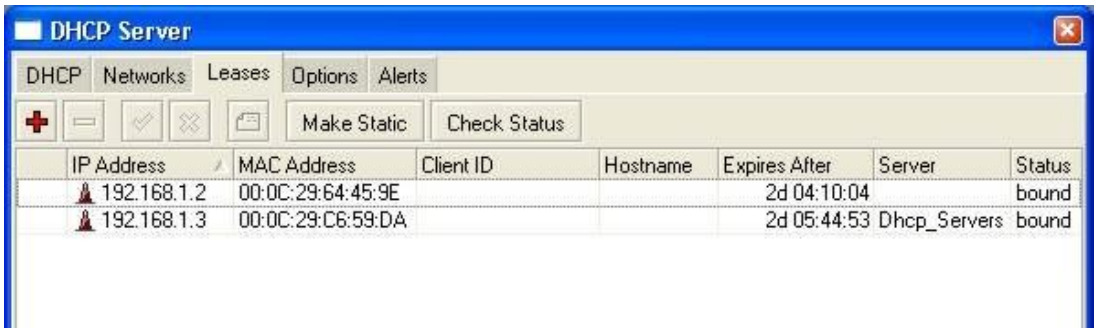
Server RADIUS:
Address: 192.168.1.3
MAC Address: 00:0C:29:C6:59:DA (MAC del servidor)
Servers: all

Imagen 112 Asignación de IP fija para servidor

Fuente: Autores – Configuración Mikrotik

Luego para que esta asignación quede estática debemos hacer clic en el botón de MAKE STATIC. De la pestaña LEASES.

Imagen 113 Lista final de DHCP para Servidores



Fuente: Autores – Configuración Mikrotik

5.3.17 Servidor – Cliente PPTP

5.3.17.1 Configuración Servidor PPTP: Debido a que tenemos clientes Empresariales con sucursal fuera de san Vicente de Chucurí, surgió la necesidad de realizar una VPN entre Bucaramanga y San Vicente. Para ello se necesita configurar el servidor de PPTP en la ciudad de San Vicente. Los pasos para dicha con figuración son:

Debemos ir al menú PPP, se nos abrirá la ventana de configuración de conexiones PPP. Luego hacemos clic en la pestaña PROFILES. A continuación hacemos clic en icono (+). Con la nueva ventana de profiles abierta la configuramos de la siguiente manera:

Name: Profile_VPN

Local Address: Pool_Empresarial

Remote Address: Pool_Empresarial

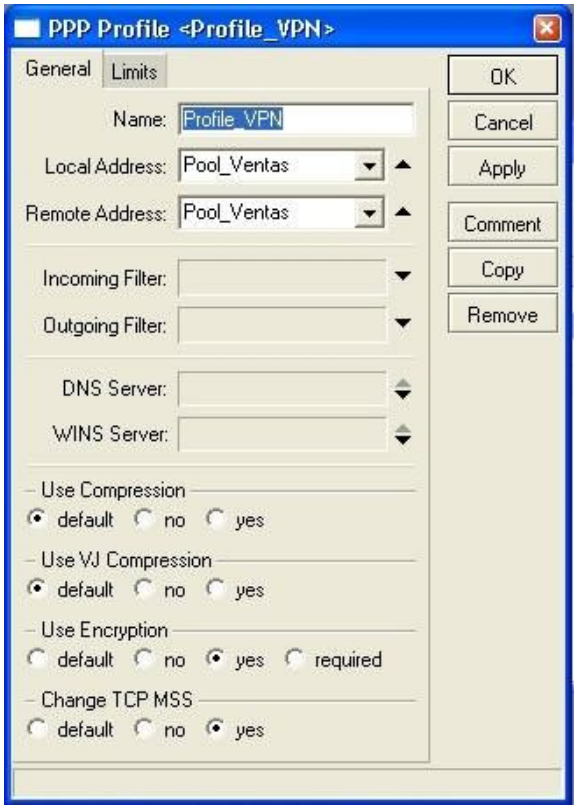
Use compresión: Default

Use Vj Compression: Default

User Encryption: Yes

Change TCP MMS: Yes

Imagen 114 Configuración de VPN



Fuente: Autores – Configuración Mikrotik

Con el profile ya generado para VPN debemos crear el usuario que utilizara dicho profile. Para ello vamos al menú PPP, hacemos clic en la pestaña SECRESTS. Hacemos clic sobre el icono (+) y en la nueva ventana la configuramos de la siguiente manera:

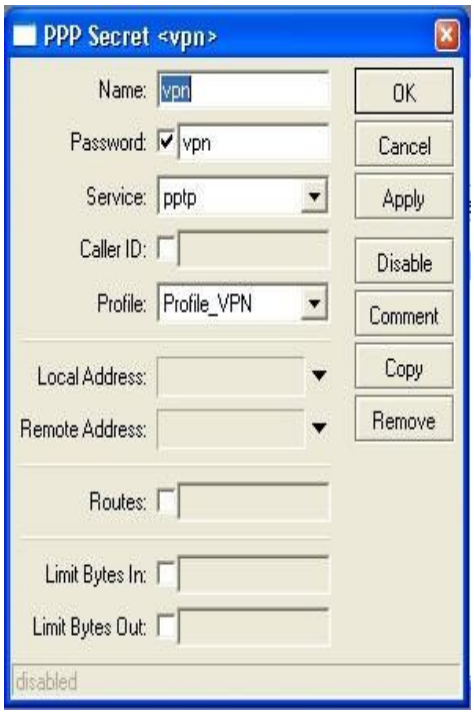
Name: vpn

Password: vpn

Service: pptp

Profile: Profile_VPN

Imagen 115 Asignación de profile para VPN



Fuente: Autores – Configuración Mikrotik

Finalmente debemos dar de alta el servidor de PPTP. Para ello nos dirigimos al menú PPP, en la pestaña Interfases hacemos clic sobre el botón PPTP Server. En la nueva ventana la configuramos de la manera siguiente:

Enable (seleccionado)

Max MTU: 1460

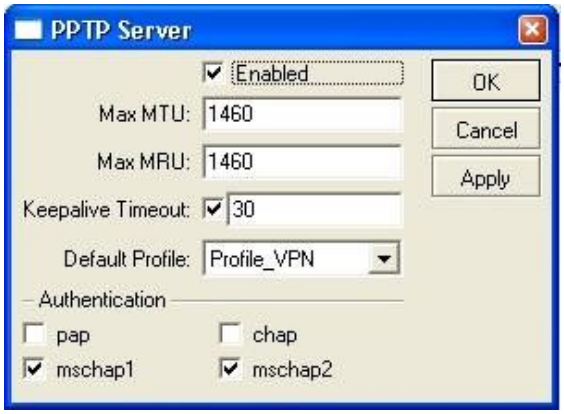
Max MRU: 1460

Keepalive Timeout:30

Default Profile: Profile_VPN

Mschap1 y mschap2 (seleccionados)

Imagen 116 Finalización de configuración VPN



Fuente: Autores – Configuración Mikrotik

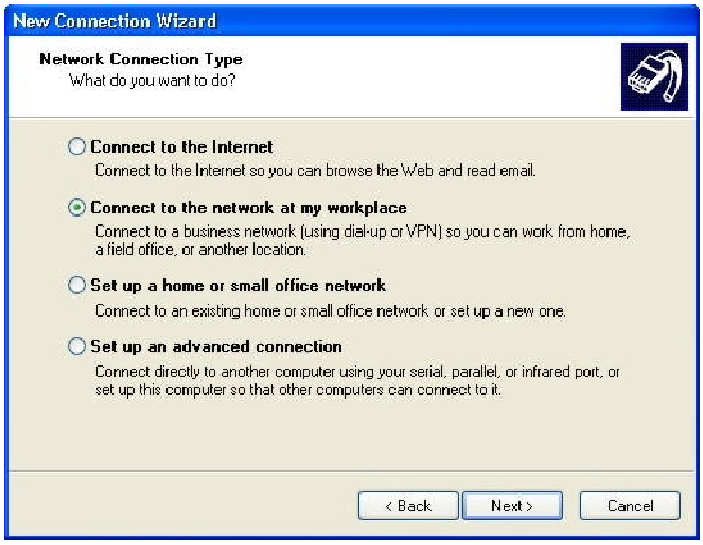
5.3.17.2 Configuración Cliente PPTP: utilizaremos la conexión de vpn de windows xp para el ejemplo. en el escritorio de windows nos dirigimos a inicio/panel de control/conexiones de red. Creamos una conexión nueva siguiendo los próximos pasos. Hacemos clic en siguiente

Imagen 117 Wizard de configuración cliente pptp

Fuente: Autores – Configuración cliente pptp

Se selecciona Connect to the network at my place

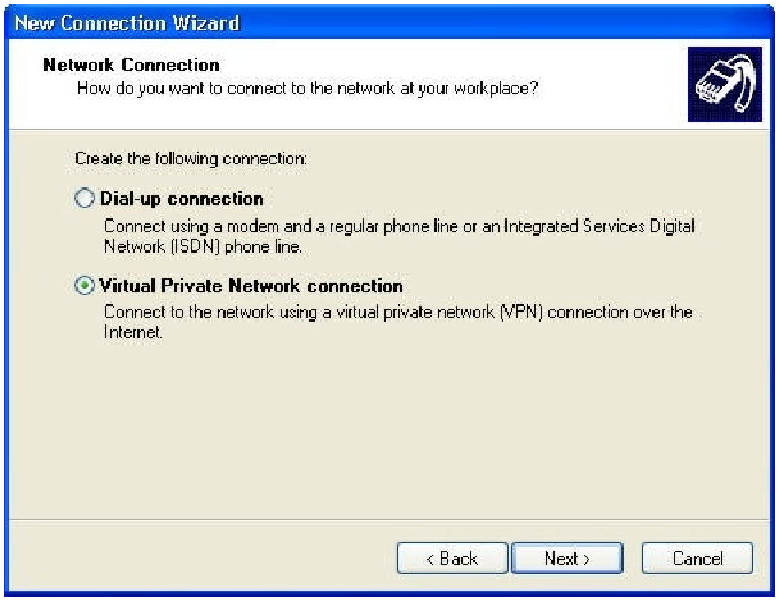
Imagen 118 Wizard para tipo de conexión pptp cliente



Fuente: Autores – Configuración cliente pptp

Seleccionamos Virtual Private Network Connection

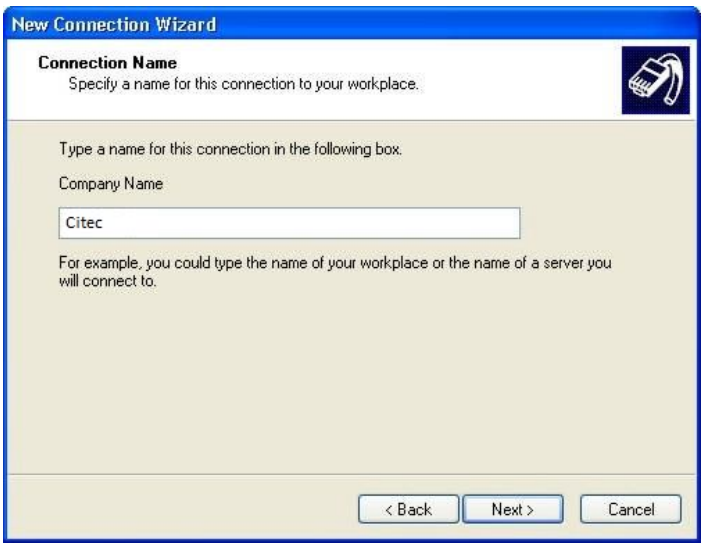
Imagen 119 wizard tipo de conexión cliente VPN



Fuente: Autores – Configuración cliente

Escribimos el nombre de la conexión: Citec

Imagen 120 Ventana de Wizard nombre de la conexión VPN



Fuente: Autores – Configuración cliente

Seleccionamos que no nos disque una conexión inicial. Para el caso de que utilicemos el ip fijo en nuestras oficinas en Bucaramanga. Luego clic en Siguiente

Fuente: Autores – Configuración cliente

Finalmente escribimos la dirección web de nuestro servidor.

Imagen 121 Ventana Wizard para configuración de dirección web de servidor empresarial

Fuente: Autores – Configuración cliente

A continuación hay que configurar el tipo de autenticación que vamos a utilizar para ello nos paramos sobre la conexión Royaltech, la abrimos. A la ventana la configuramos de la siguiente manera:

Nombre de usuario: victor

Contraseña: victor

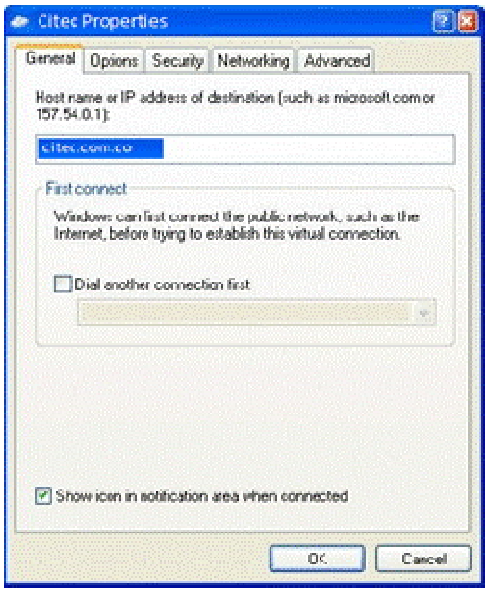
Guardar nombre de usuario y contraseña (seleccionado)

Imagen 122 Ventana de conexión a VPN desde el cliente

Fuente: Autores – Configuración cliente vpn

Luego hacemos clic en propiedades.

Imagen 123 Propiedades de conexión VPN en cliente



Fuente: Autores – Configuración cliente vpn

Hacemos clic en la pestaña Seguridad.

Imagen 124 configuración de seguridad en VPN para conexión cliente

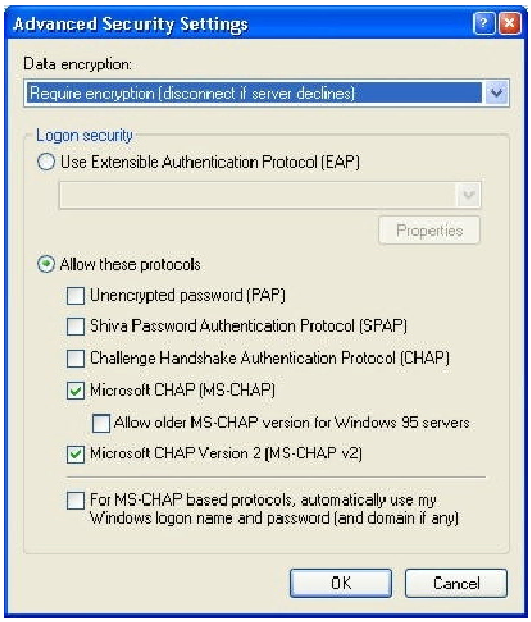
Fuente: Autores – Configuración cliente vpn

Seleccionamos Avanzado y luego clic en Settings.

En nuestra ventana de configuración avanzada de seguridad la seteamos de la siguiente manera:

Allow this Protocols: Seleccionado
Uncrypted Password: Deseleccionado
Shiva Autenticación Password Protocol : Deseleccionado
Chalenge handshake authentication protocol: Deseleccionado
Microsoft CHAP : Seleccionado
Microsoft CHAP Versión 2 : Seleccionado
Luego hacemos clic en OK

Imagen 125 Seguridad avanzada en cliente VPN



Fuente: Autores – Configuración cliente vpn

Luego hacemos clic en la pestaña Networking y Editamos las propiedades de Internet Protocol (TCP/IP)

Imagen 126 edición de propiedades de protocolo TCP/ip para cliente VPN

Fuente: Autores – Configuración cliente vpn

En dicha ventana hacemos clic en Avanzado.

Imagen 127 Ventana de propiedades Tcp/ip cliente VPN

Fuente: Autores – Configuración cliente vpn

En la ventana de avanzado la configuramos así:

User default Gateway on remote network: Deseleccionado.

Imagen 128 Configuración avanzada de propiedades Tcp/ip cliente VPN

Fuente: Autores – Configuración cliente vpn

5.3.18 Configuración de Proxy Server

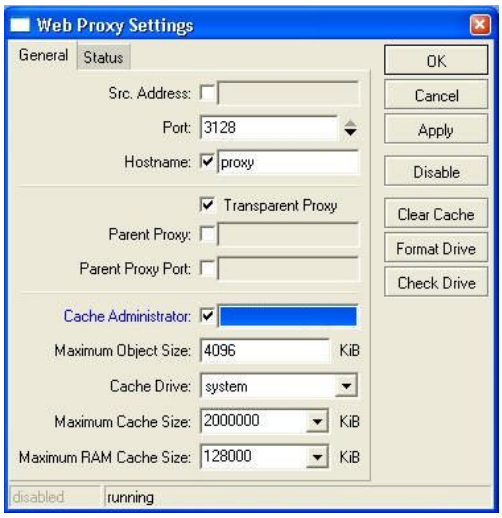
Se decidió utilizar un servidor Web Proxy para ahorrar ancho de banda utilizado por los usuarios en Internet. Para ello nos dirigimos al menú IP / WEB-PROXY.

Imagen 129 Configuración de Proxy server

Fuente: Autores – Configuración Mikrotik

En nuestra ventana de configuración hacemos clic en SETTINGS. Se esta manera entramos a la ventana de configuración del servidor Proxy. Dicha ventana la configuraremos de la siguiente manera.

Imagen 130 Ventana de configuración de Proxy Server



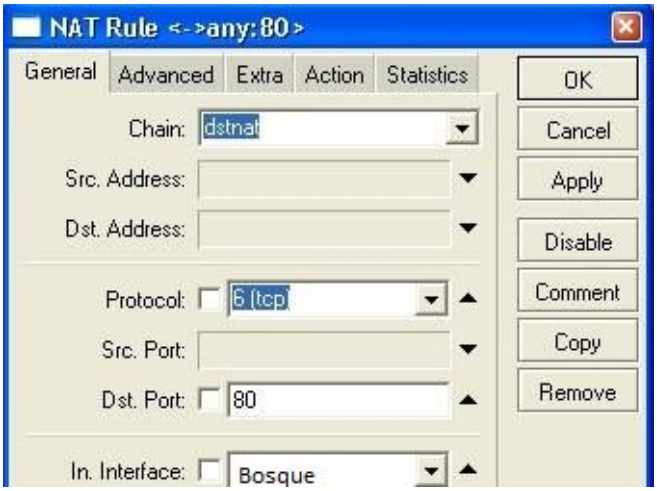
Fuente: Autores – Configuración Mikrotik

A continuación hacemos clic en ENABLE. Se nos abre una ventanita y le hacemos clic en ok.

Como segundo paso debemos generar un una regla en el firewall para que haga un re direccionamiento al servidor Proxy. Para ello nos dirigimos al menú IP / FIREWALL en nuestra ventana de configuración hacemos clic en la pestaña NAT, luego clic en el botón (+). La ventana la configuramos todas las sub redes de la siguiente manera:

Interface Bosque:
Chain: dstnat
Protocol: 6 (tcp)
Interface Bosque.

Imagen 131 Configuración de regla para interfaces



Fuente: Autores – Configuración Mikrotik

Luego hacemos clic sobre la pestaña ACTION y la configuramos de la siguiente manera:

Action: Redirect

To ports: 3128

Imagen 132 Ventana de acciones para reglas NAT

Fuente: Autores – Configuración Mikrotik

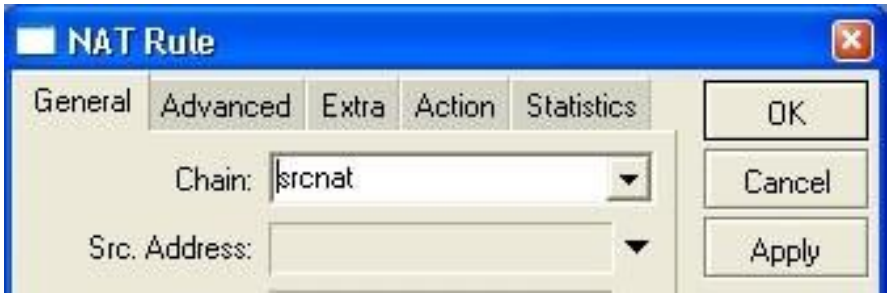
Realizamos esta misma configuración para cada una de las interfaces de nuestra red.

Por último configuraremos el NAT para el ruteo entre todas las subredes. Para ello nos dirigimos al menú IP / FIREWALL en nuestra ventana de configuración hacemos clic en la pestaña NAT, luego clic en el botón (+). La ventana la configuramos de la siguiente manera.

Pestaña General:

Chain: srcnat

Imagen 133 Reglas NAT



Fuente: Autores – Configuración Mikrotik

Pestaña Action:

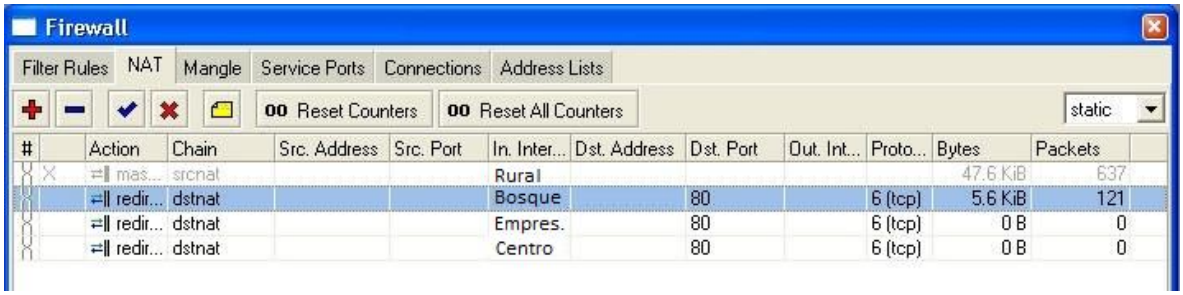
Action: Masquerade

Imagen 134 Action mascarade de la regla NAT

Fuente: Autores – Configuración Mikrotik

Nuestra configuración de políticas de NAT se ven de la siguiente manera:

Imagen 135 Ventana de configuración final de reglas NAT

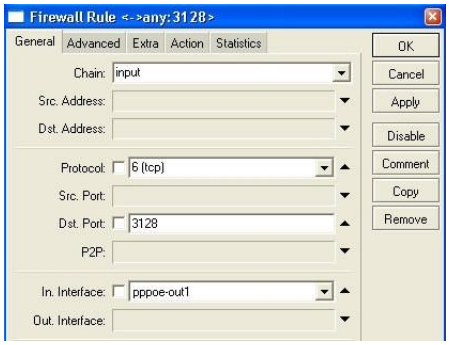


Fuente: Autores – Configuración Mikrotik

A continuación debemos proteger nuestro servidor de cualquier utilización desde el exterior de la red. Para ello nos dirigimos al menú IP / FIREWALL. En la ventana nueva hacemos clic en la pestaña FILTER RULES, a continuación hacemos clic en el icono (+). Nuestra nueva política de filtrado de paquetes la configuramos así:

Pestaña: General:
Chain: input
Protocol: 6 (tcp)
Dst. Port.: 3128
In. Interface: Ciudanet

Imagen 136 Ventana General de reglas Firewall



Fuente: Autores – Configuración Mikrotik

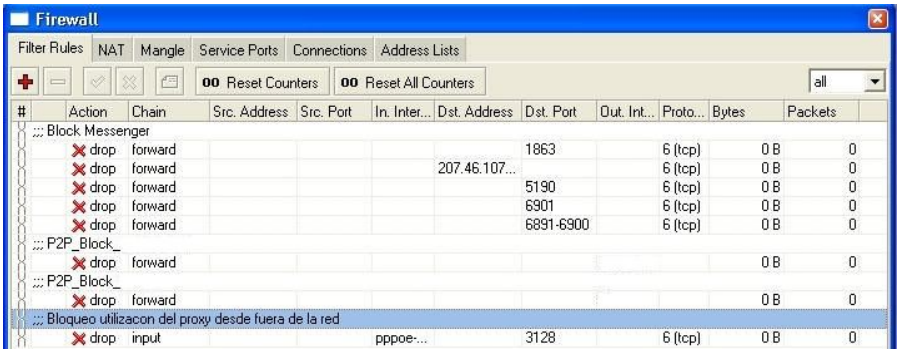
Pestaña Action:
Action: Drop

Imagen 137 Ventana de configuración avanzada de reglas firewall

Fuente: Autores – Configuración Mikrotik

Nuestras políticas de filtrado se ven de la siguiente manera:

Imagen 138 Ventana final de políticas de filtrado



Fuente: Autores – Configuración Mikrotik

Bloquearemos algunas páginas con la utilización del Web Proxy como muestra del procedimiento a seguir. Para ello se definió que no se podrá ingresar a sitios pornográficos desde la red ni la utilización de páginas que tengan el servicio de Web Messenger al igual que Yahoo u otros.

5.3.18.1 Bloqueo de pornografía: Nos dirigimos al menú IP / Web proxy. En la nueva ventana dentro de la pestaña Access hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente forma:

Src. Address: 0.0.0.0/0

Dst. Address: 0.0.0.0/0

URL: *porn*

Method: any

Action: deny

Imagen 139 Bloqueo de pornografía mediante webproy

Fuente: Autores – Configuración Mikrotik

Este filtro nos bloqueara cualquier site que posea la palabra *porn* en su nombre. También nos sirve debido a que si el usuario busca algo con la palabra porn en Google o cualquier otro buscador también nos bloquee la búsqueda.

Política 2
Src. Address: 0.0.0.0/0
Dst. Address: 0.0.0.0/0
URL: *sex*
Method: any
Action: deny

Imagen 140 Política 2 para bloqueo de pornografía

Fuente: Autores – Configuración Mikrotik

Cada política se debe configurar de la forma anterior.

5.3.18.2 Bloqueo descarga directa de archivos MP3 y AVI

Para e bloqueo de descarga directa de archivos MP3 y avi debemos utilizamos la siguiente política en el Web Proxy para bloquearlo.

Para ello realizamos los siguientes pasos. Nos dirigimos al menú IP / Web Proxy. En la nueva ventana dentro de la pestaña Access hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

Imagen 141 Bloqueo de archivos mp3

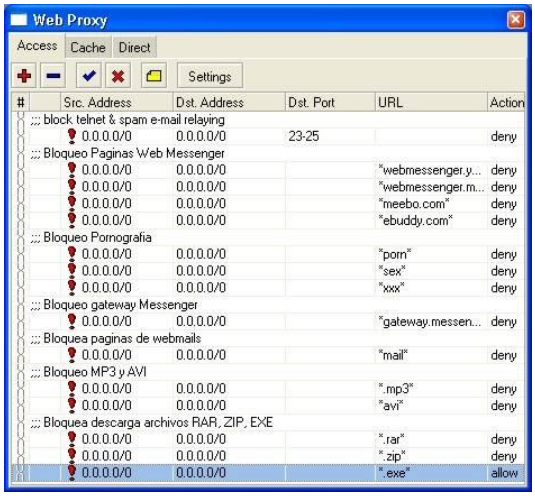
Fuente: Autores – Configuración Mikrotik

Imagen 142 Bloqueo de archivos .avi

Fuente: Autores – Configuración Mikrotik

Las políticas del servidor web Proxy se ven de la siguiente manera dependiendo de las restricciones dadas.

Imagen 143 Políticas de un WepPoxy



Fuente: Autores – Configuración Mikrotik

5.3.19 Balanceo de carga

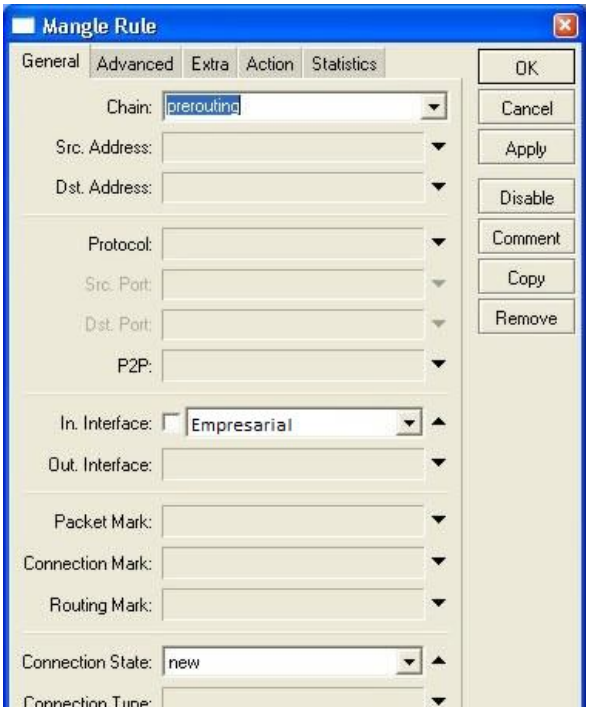
Debido a que poseemos dos conexiones a los proveedores de Internet utilizaremos el balanceo de carga para optimizar el tráfico en la red. Debido a que la sub red Empresarial genera grandes volúmenes de tráfico hacia Internet el balanceo de carga Será aplicado a ella.

Para configurar nuestro balanceo debemos realizar los siguientes pasos. Nos dirigimos al menú IP / FIREWALL. De ahí vamos a la pestaña Mangle. Hacemos clic en el icono (+) y comenzamos nuestra configuración de las políticas para el balaceo de cargas. A la nueva ventana la configuramos de la siguiente manera.

Pestaña General:

Chain: prerouting
In. Interfase Empresarial
Connection State: new

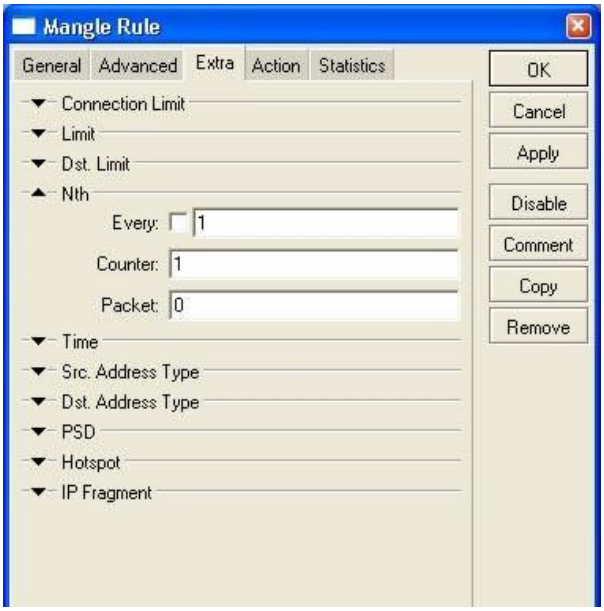
Imagen 144 Configuración de Balanceo de Carga en Mikrotik



Fuente: Autores – Configuración Mikrotik

Pestaña Extra:

Imagen 145 Configuración de políticas extra para balanceo de carga



Fuente: Autores – Configuración Mikrotik

Pestaña Action:

Action: mark connection

New Connection Mark: Salida_Telmex

Pass thought: seleccionado

Imagen 146 Acciones a tomar en balanceo de carga

Fuente: Autores – Configuración Mikrotik

Creamos una segunda política y la configuramos así:

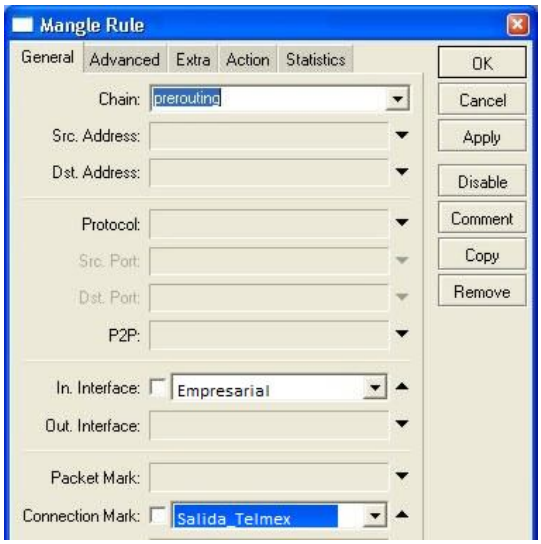
Pestaña General:

Chain: prerouting

In. Interfase: Empresarial

Connection mark: Salida_Telmex

Imagen 147 Segunda política de balanceo de carga



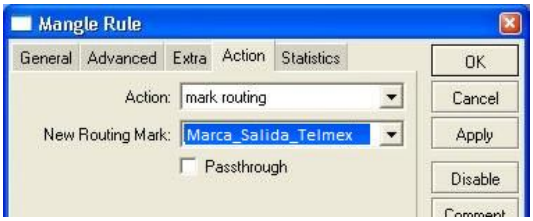
Fuente: Autores – Configuración Mikrotik

Pestaña Action:

Action: mark routing

New Routing Mark: Marca_Salida_Telmex

Imagen 148 acción de marca para la segunda regla de balanceo



Fuente: Autores – Configuración Mikrotik

Tercera política de mangle. Se configura así:

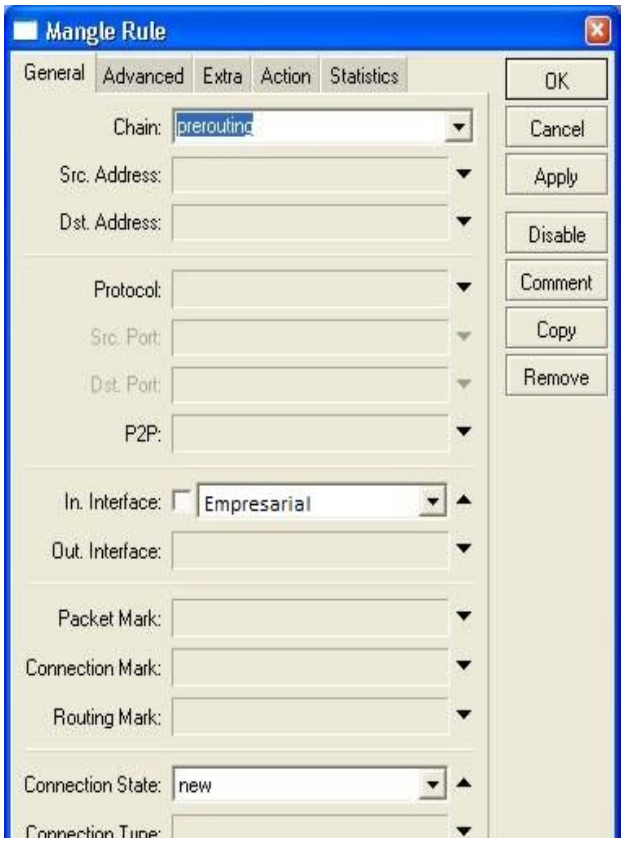
Pestaña General:

Chain: prerouting

In. Interfuse: Empresarial

Connection State: New

Imagen 149 Tercera política para balanceo



Fuente: Autores – Configuración Mikrotik

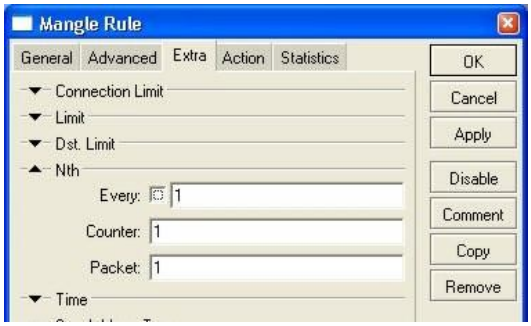
Pestaña Extra:

Every: 1

Counter:1

Packet:1

Imagen 150 extras de la tercera política de balanceo



Fuente: Autores – Configuración Mikrotik

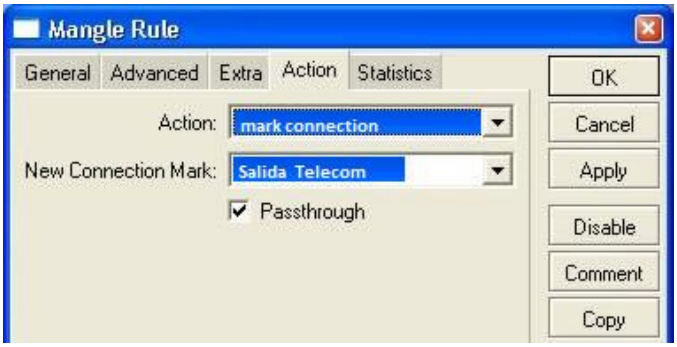
Pestaña Action:

Action: mark connection

New Connection Mark: Salida_Telecom

Pass thought (seleccionado)

Imagen 151 acciones de la tercera política de balanceo



Fuente: Autores – Configuración Mikrotik

Cuarta política de mangle se configura así:

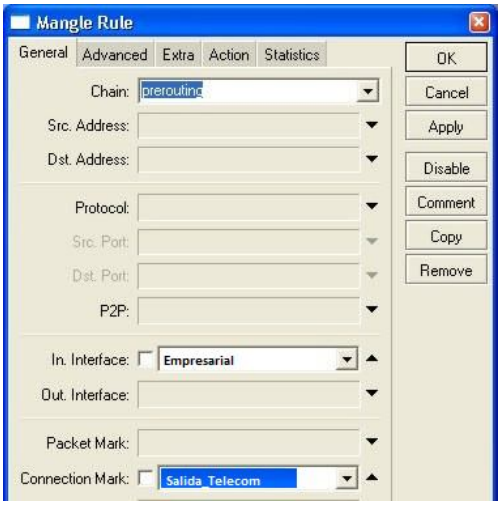
Pestaña general:

Chain: prerouting

In. Interface: Empresarial

Connection mark: Salida Telecom

Imagen 152 cuarta política de balanceo



Fuente: Autores – Configuración Mikrotik

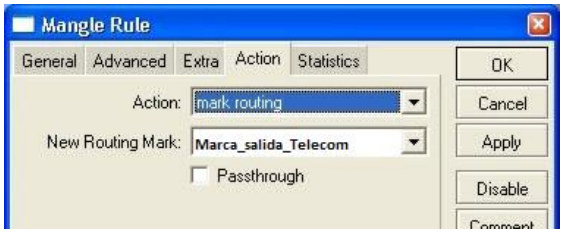
Pestaña Action:

Action: mark routing

New routing Mark: Marca_Salida_Telecom

Pass Thought: (No Seleccionado)

Imagen 153 Marcado de la acción para la cuarta política de balanceo



Fuente: Autores – Configuración Mikrotik

A continuación debemos crear dos políticas de NAT para continuar con la configuración. Para ello nos dirigimos al menú IP / FIREWALL. Hacemos clic en la pestaña NAT, luego clic en el icono (+).

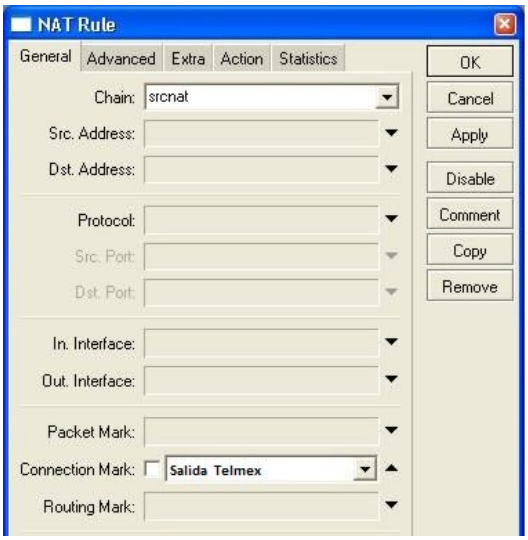
La primera política de NAT se configura así:

Pestaña General:

Chain: srcnat

Connection Mark: Salida_Telmex

Imagen 154 Configuración de política NAT para salida mediante un proveedor



Fuente: Autores – Configuración Mikrotik

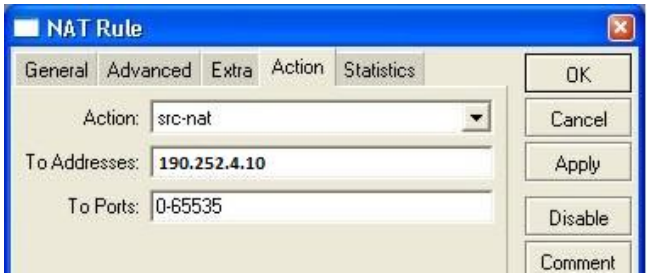
Pestaña Action:

Action: src-nat

To addresses: 192.252.4.10

To Ports: 0-65535

Imagen 155 Acción de la regla NAT



Fuente: Autores – Configuración Mikrotik

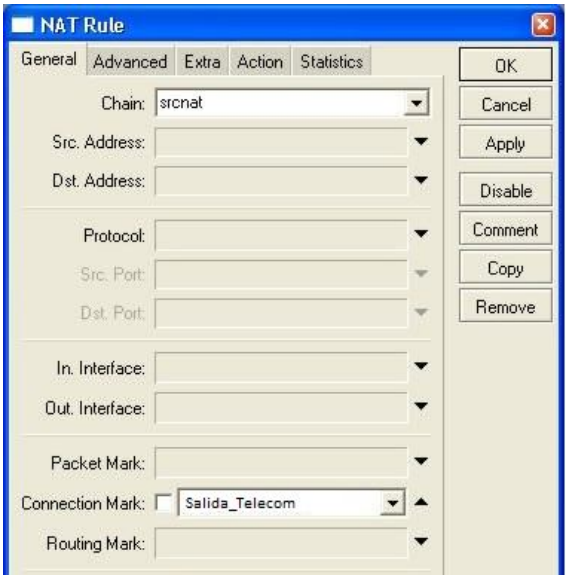
La segunda política de NAT se configura así:

Pestaña General:

Chain: srcnat

Connection Mark: Salida_Telecom

Imagen 156 Segunda política NAT para salida por medio de un proveedor



Fuente: Autores – Configuración Mikrotik

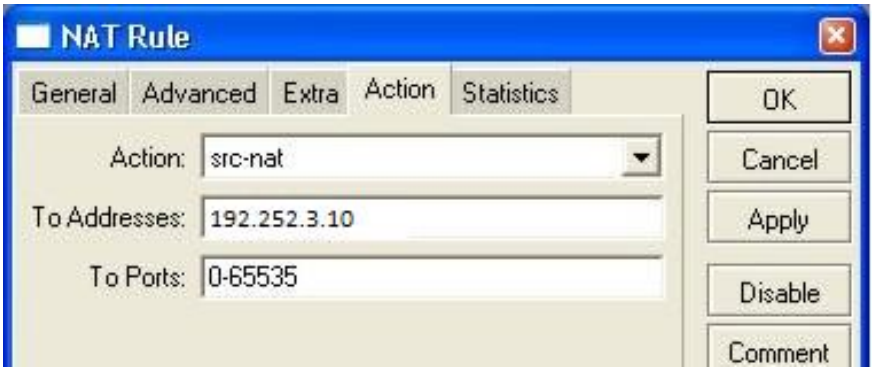
Pestaña Action:

Action: src-nat

To addresses: 192.252.3.10

To Ports: 0-65535

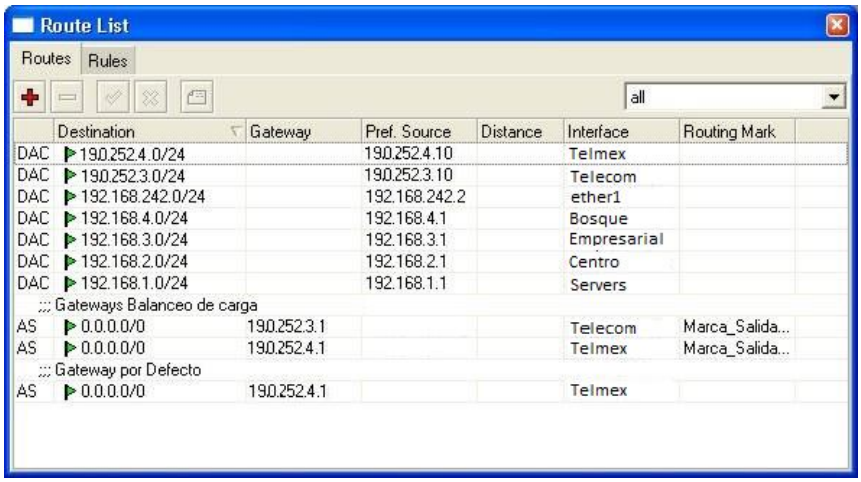
Imagen 157 Acción para la segunda regla NAT de salida por proveedor



Fuente: Autores – Configuración Mikrotik

Nuestras políticas de NAT se verán así:

Imagen 158 Ventana de políticas NAT



Fuente: Autores – Configuración Mikrotik

Por último para finalizar la configuración debemos realizar unas últimas políticas de ruteo. Para ello entramos en el menú NEW TERMINAL. En la terminal que nos aparece tipeamos lo siguiente:

/ip route add dst-address=0.0.0.0/0 gateway=190.252.3.1 scope=255 target-scope=10 routing-mark=Marca_Salida_Telecom comment="" disabled=no
/ip route add dst-address=0.0.0.0/0 gateway=190.252.4.1 scope=255 target-scope=10 routing-mark=Marca_Salida_Telmex comment="" disabled=no

/ip route add dst-address=0.0.0.0/0 gateway=190.252.4.1 scope=255 target-scope=10 comment="Gateway por Defecto" disabled=no

5.3.20 Control de ancho de banda (Asignación de ancho de banda por sub red)

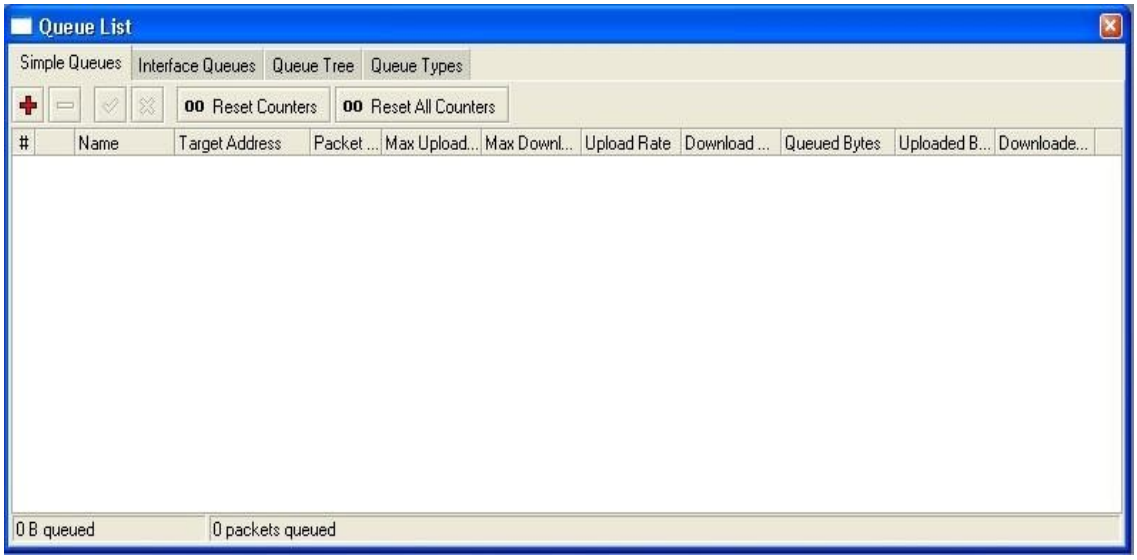
Debido a que muchas veces los usuarios realizan malos usos de los anchos de banda, hemos decidido agregarle políticas al router para poder controlar dicho problema.

Para los distintos grupos de usuarios les asignaremos distinto ancho de banda:

Centro: Subida 64 kb, Bajada 64 kb
Bosque: Subida 64 Kb, Bajada 64 Kb
Empresarial: Subida 64 Kb, Bajada 512 Kb
Rural: Subida 64 Kb, Bajada 64 Kb

Para el control del ancho de banda debemos ir al menú QUEUES. Allí se nos abrirá una ventana de configuración.

Imagen 159 Ventana de configuración de Quotas de navegación



Fuente: Autores – Configuración Mikrotik

Hacemos clic en el icono (+) de la pestaña Simple Queues. Se nos abre la nueva para configurar la nueva cola.

Cola Centro:
Pestaña General:
Name: Queue_Centro
Target Address: 192.168.2.0/24

Max Limit: 64Kb (upload) , 64 Kb (download)

Imagen 160 Pestaña general de configuración de Quotas

Fuente: Autores – Configuración Mikrotik

Cola Empresarial:

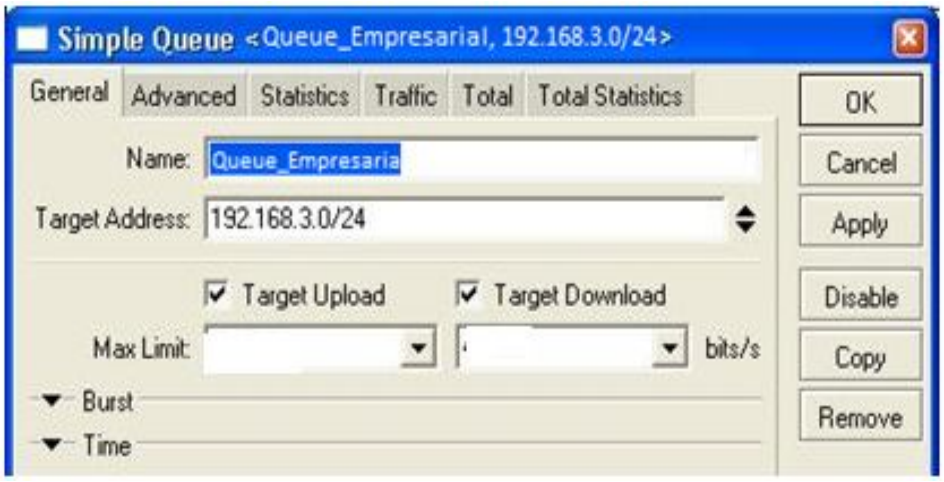
Pestaña General:

Name: Queue_Empresarial

Target Address: 192.168.3.0/24

Max Limit: 256Kb (upload) , 256Kb (download)

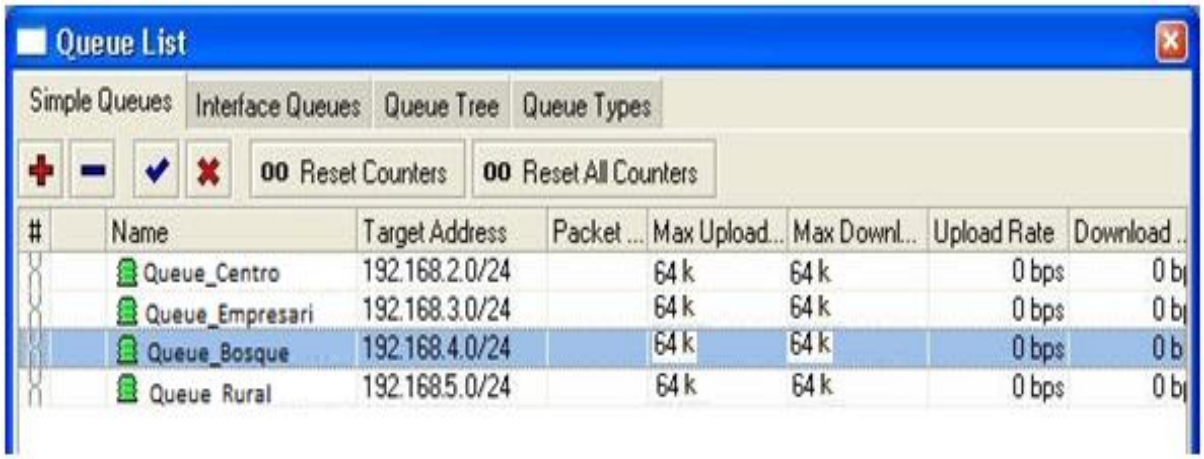
Imagen 161 Configuraciones generales de Quotas segmento empresarial



Fuente: Autores – Configuración Mikrotik

Al finalizar, las colas configuradas se verán de la siguiente manera:

Imagen 162 Lista final de configuración de Colas de los sectores



Fuente: Autores – Configuración Mikrotik

5.3.21 Traffic Shaping de (P2P)

Dentro de las políticas de la empresa se plantea que las áreas utilicen con moderación lo P2P, para la prueba se realizará en el área Centro. Anteriormente habíamos asignado un cierto ancho de banda para el área Centro ahora deberemos modelar las colas del trafico para que los p2p no se consuman todo el tráfico.

Debemos ir al menú IP / FIREWALL. Ahí se nos abrirá nuestra ventana de configuración de políticas del firewall. Hacemos clic sobre la pestaña Mangle, a continuación hacemos clic sobre el botón (+).

En la ventana de mangle con figuramos lo siguiente:
Chain: prerouting
P2P: all-p2p

Imagen 163 Configuración de políticas en el firewall para P2P

Fuente: Autores – Configuración Mikrotik

A continuación hacemos clic en la pestaña Action. Allí la configuración es la siguiente:

Action: mark_connection

New Connection Mark: (tipeamos) connexion_p2p

Passthough (seleccionado).

Imagen 164 Acción de marcado para conexión de regla p2p

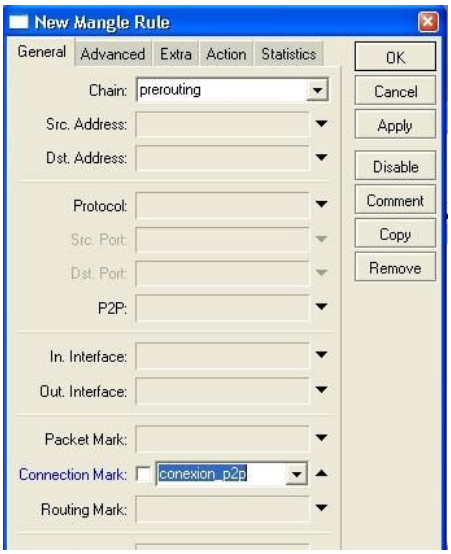
Fuente: Autores – Configuración Mikrotik

A continuación dentro de la pestaña mangle hacemos clic nuevamente en el botón (+) para crear una nueva regla. La configuración para la ventana es:

Chan: prerouting

Connection Mark: conexión_p2p (la que habíamos creado anterior mente)

Imagen 165 configuración de nueva regla p2p



Fuente: Autores – Configuración Mikrotik

Luego nos dirigimos a la pestaña Action, en la misma la configuramos de la siguiente manera:

Action: Mark Packet

New Packet Mark: (tipeamos) p2p

Imagen 166 Marca de nueva regla p2p

Fuente: Autores – Configuración Mikrotik

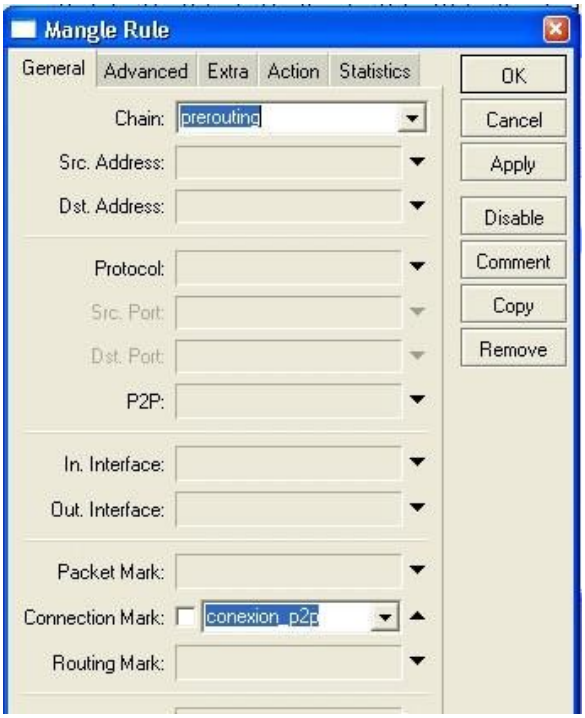
Ahora deberemos configurar las políticas para que nos marque los paquetes p2p para poder bloquearlos en las otras redes.

Para ello debemos ir al menú IP /FIREWALL. Hacemos clic en la pestaña mangle y luego clic en el icono (+).

En la pestaña General de la nueva ventana la configuramos de la siguiente manera:

Chain: prerouting
Connection Mark: conexión_p2p

Imagen 167 Regla de prerouting



Fuente: Autores – Configuración Mikrotik

Luego nos dirigimos a la pestaña Action y la configuramos de la siguiente manera:

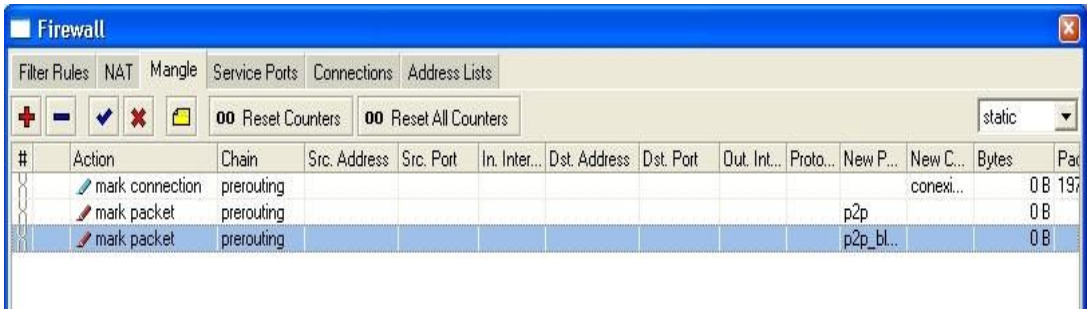
Action: mark packet
Packet mark: (tipeamos) p2p_bloqueado
Pass though: (seleccionado)

Imagen 168 acción de marca para bloqueo de p2p

Fuente: Autores – Configuración Mikrotik

Las reglas creadas se verán de la siguiente manera.

Imagen 169 Reglas creadas



Fuente: Autores – Configuración Mikrotik

Nos dirigiremos al menú QUEUES. En la ventana que nos aparece, crearemos cuatro nuevas colas para la política de los p2p. Hacemos clic sobre la pestaña Queue Tree. Y luego clic sobre el botón (+).

La configuración de la cola de entrada será la siguiente:

Name: Queue_p2p_in

Parent: Global-in

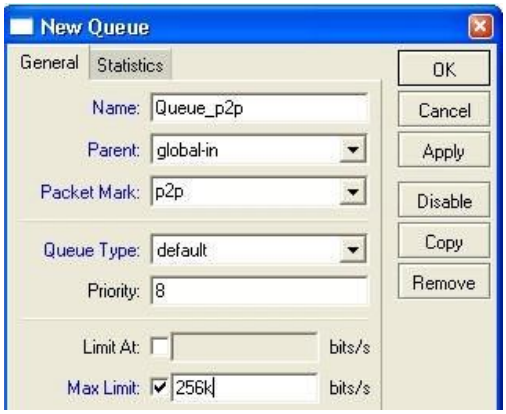
Packet Mark: p2p

Queue Type: default

Priority: 8

Max Limit: 256k

Imagen 170 configuración general de cola de entrada p2p



Fuente: Autores – Configuración Mikrotik

Hacemos clic en el botón (+) y generamos una nueva cola La configuración de la cola de salida será:

Name: Queue_p2p_out

Parent: global-out

Packet Mark: p2p

Queue type: default

Priority: 8

Max Limit: 256k

Imagen 171 Cuotas de salida p2p

Fuente: Autores – Configuración Mikrotik

5.3.22 Redireccionamiento de puertos

A continuación debemos redireccionar puertos para que el tráfico que se genere hacia adentro de la red obtengan las respuestas deseadas. Por ejemplo que nuestro servidor web muestre las páginas correspondientes, que el servidor de SMTP y POP3 puedan enviar y recibir mails etc.

5.3.22.1 Puerto 80 WEB: Para redireccionar el puerto 80 desde el exterior a nuestro servidor web ip: debemos realizar los siguientes pasos. Ir al menú IP / FIREWALL. Hacer clic en la pestaña NAT. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera.

Pestaña General:

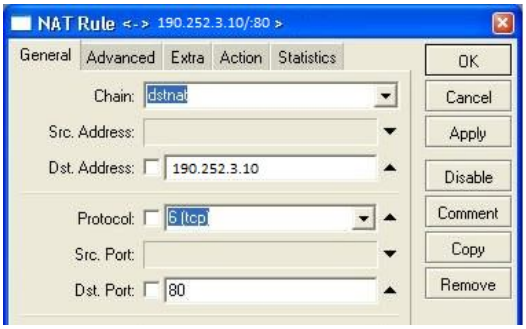
Chain:dstnat

Dst. Address: 190.252.3.10

Protocol: 6 (tcp)

Dst. Port: 80

Imagen 172 Re direccionamiento de puerto 80



Fuente: Autores – Configuración Mikrotik

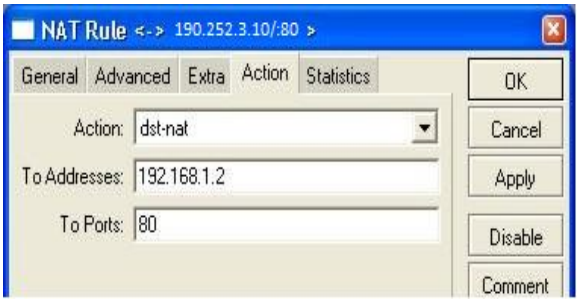
Pestaña Action:

Action: dst-nat

To Addresses: 192.168.1.2

To Port: 80

Imagen 173 Acción de la regla NAT para redireccionamiento de puerto 80



Fuente: Autores – Configuración Mikrotik

5.3.22.2 Puerto 110 POP3: Para redireccionar el puerto 110 desde el exterior a nuestro servidor pop3 ip: debemos realizar los siguientes pasos. Ir al menú IP / FIREWALL. Hacer clic en la pestaña NAT. Luego hacer clic en el icono (+).

A la nueva ventana la configuramos de la siguiente manera.

Pestaña General:

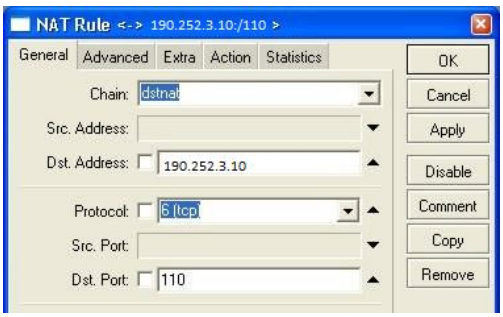
Chain: dstnat

Dst. Address: 190.252.3.10

Protocol: 6 (tcp)

Dst. Port: 110

Imagen 174 Regla Nat para re direccionamiento de puerto 110



Fuente: Autores – Configuración Mikrotik

Pestaña Action:

Action: dst-nat

To Addresses: 192.168.1.2

To Port: 110

Imagen 175 Acción de redireccionamiento de puerto 110

Fuente: Autores – Configuración Mikrotik

5.3.22.3 Puerto 25 SMTP: Para redireccionar el puerto 25 desde el exterior a nuestro servidor pop3 ip: 192.168.1.2 debemos realizar los siguientes pasos. Ir al menú IP / FIREWALL. Hacer clic en la pestaña NAT. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera.

Pestaña General:

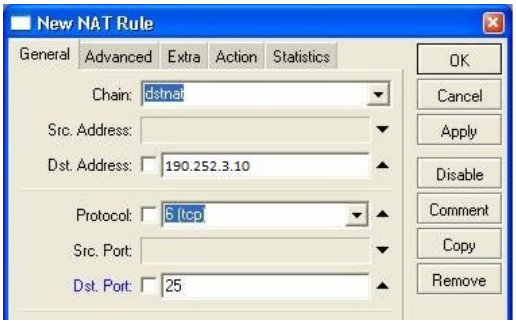
Chain:dstnat

Dst. Address: 190.252.3.10

Protocol: 6 (tcp)

Dst. Port: 25

Imagen 176 regla Nat para redireccionamiento de puerto 25



Fuente: Autores – Configuración Mikrotik

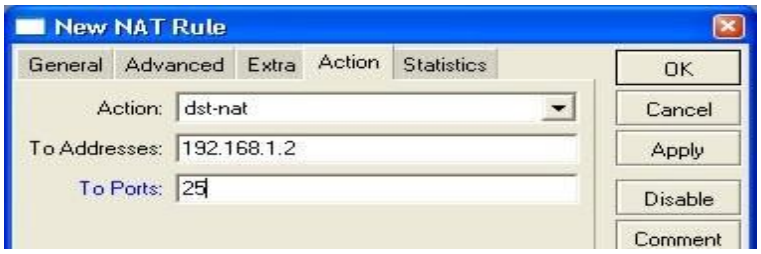
Pestaña Action:

Action: dst-nat

To Addresses: 192.168.1.2

To Port: 25

Imagen 177 Acción para redireccionamiento de puerto 25



Fuente: Autores – Configuración Mikrotik

5.3.22.4 Puerto 1723 PPTP: Para aceptar conexiones al puerto 1723 desde el exterior debemos realizar los siguientes pasos. Ir al menú IP / FIREWALL. Hacer clic en la pestaña FILTER RULES.

Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera.

La primer política es para aceptar el tráfico al puerto 1723 tcp

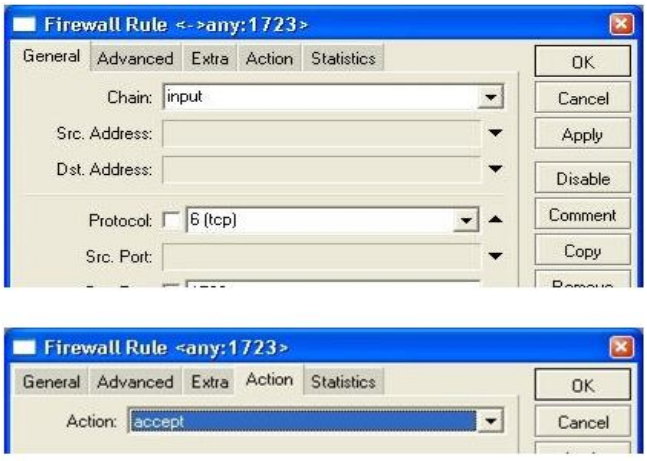
Pestaña General:

Chain: input

Protocol 6 (tcp)

Dst. Port: 1723

Imagen 178 Política para aceptar trafico al puerto 1723 tcp



Fuente: Autores – Configuración Mikrotik

La segunda política es para aceptar todo el trafico al puerto 1723 UDP

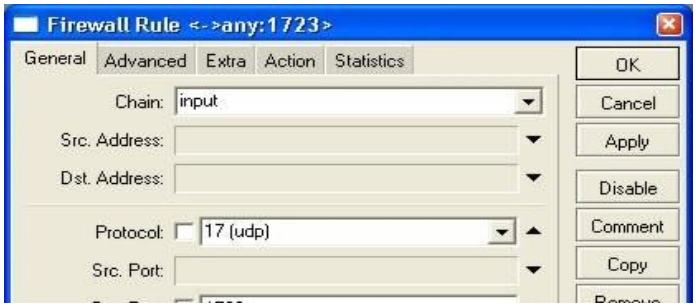
Pestaña General:

Chain: input

Protocol 17 (udp)

Dst. Port: 1723

Imagen 179 Regla para aceptar trafico al puerto UDP



Fuente: Autores – Configuración Mikrotik

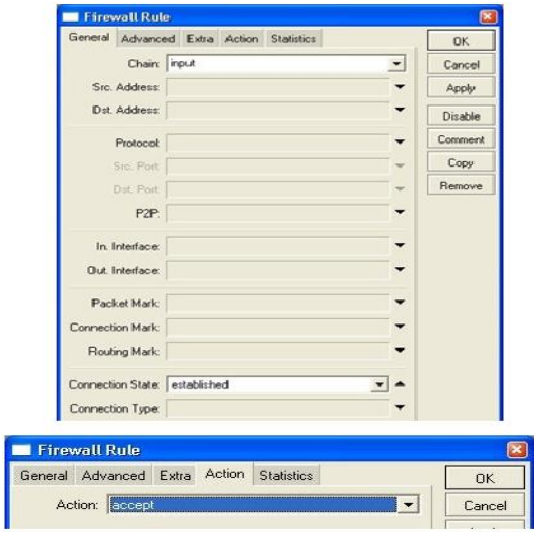
Por último aceptaremos todas las comunicaciones que estén establecidas.

Pestaña General:

Chain: input

Connection State: established

Imagen 180 Aceptación de comunicaciones establecidas

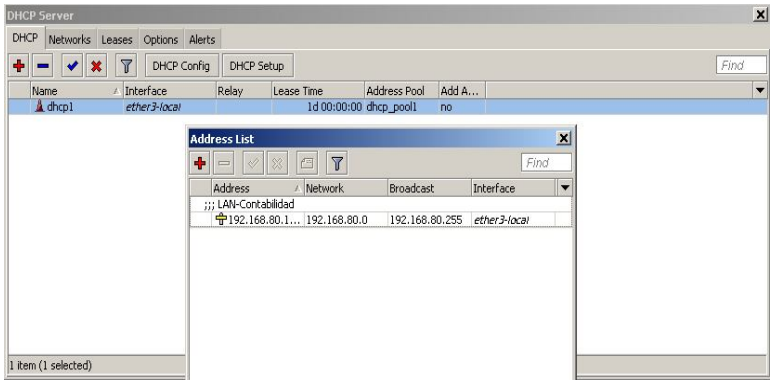


Fuente: Autores – Configuración Mikrotik

5.3.23 Configuración Hot Spot

Se debe tener en cuenta antes de empezar que la interfaz de creación del hotspot debe tener dirección IP y al mismo tiempo tener habilitado el server DHCP sobre esta misma interfaz para nuestro ejemplo es la ether1 como lo muestra la figura:

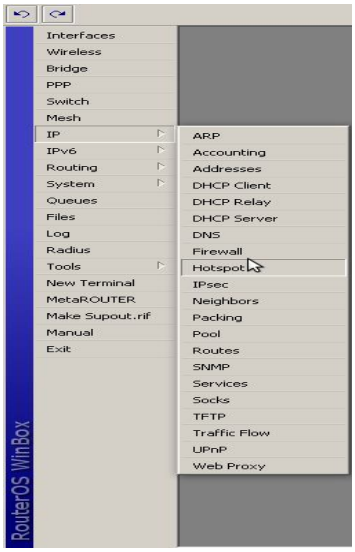
Imagen 181 Interfaz de hospot



Fuente: Autores – Configuración Mikrotik

Se procede al ingreso a la pestaña Menú Ip—Hotspot.

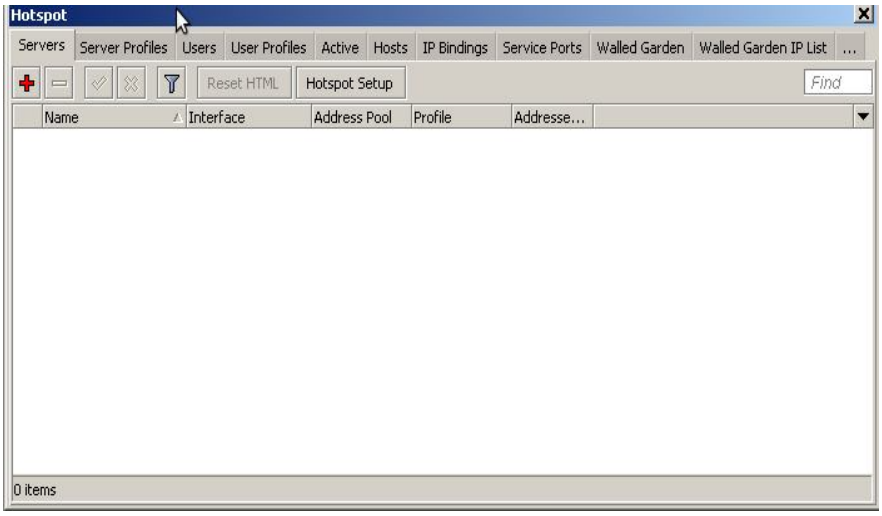
Imagen 182 Ingreso a configuración de hotspot



Fuente: Autores – Configuración Mikrotik

Se Ingresa al botón hotspot Setup, se inicia la Configuración del Hotspot.

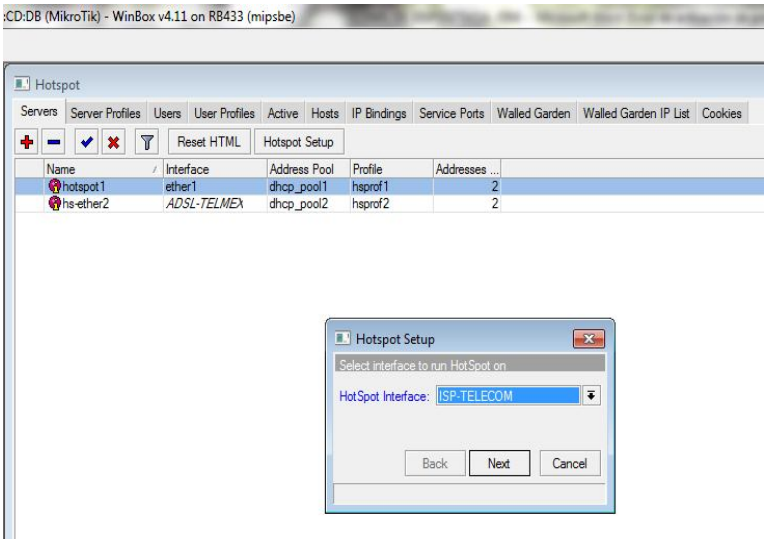
Imagen 183 Ventana de configuración Hotspot



Fuente: Autores – Configuración Mikrotik

Se activa la interfaz que quiero que facilite la interfaz Web de autenticación de los usuarios en este caso la ether1 como lo muestra la figura:

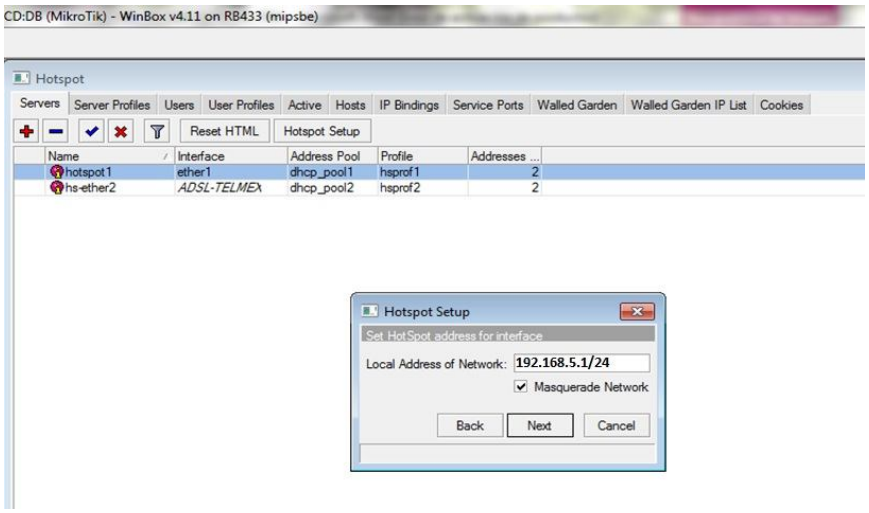
Imagen 184 Activación de interfaz web de autenticación



Fuente: Autores – Configuración Mikrotik

Damos click en next para visualizar la IP que usara el hotspot y la activo la casilla que automáticamente crea las reglas de masquerade (NAT) en el firewall para que permita su salida a internet.

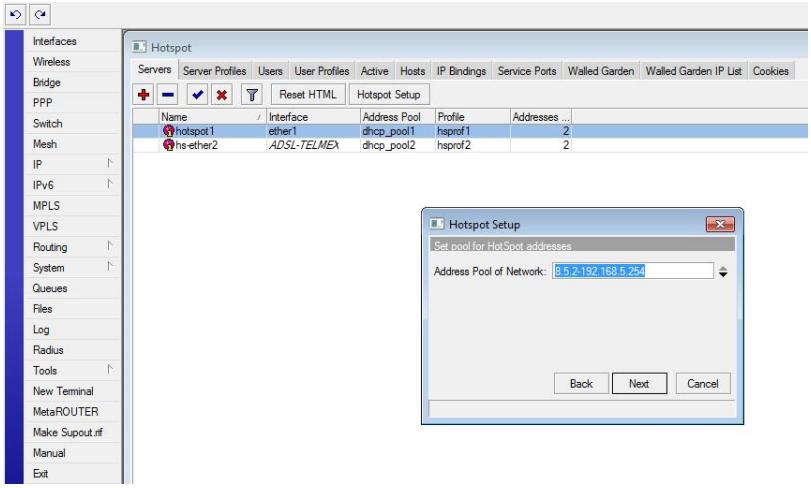
Imagen 185 Creación de las reglas mascarade NAT en firewall



Fuente: Autores – Configuración Mikrotik

Se define el rango que va hacer utilizado para asignación dinámica de direcciones IP a todos los clientes que se quieran conectar al portal cautivo (Aquí se hace referencia al DHCP server)

Imagen 186 definición de rango de direcciones ip para asignación dinámica

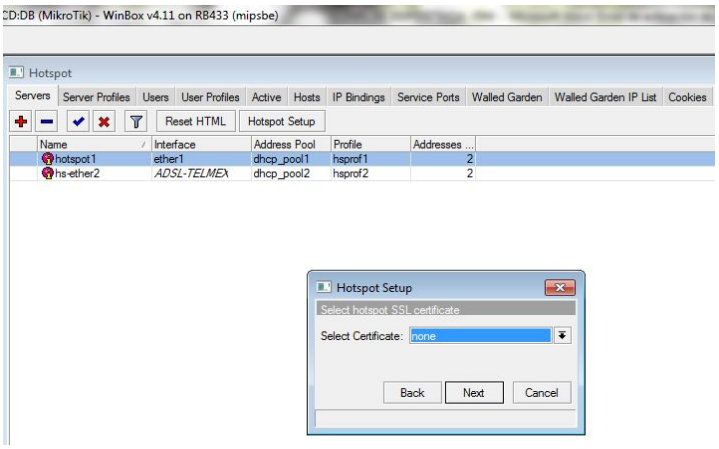


Fuente: Autores – Configuración Mikrotik

Damos Click en siguiente.

En este paso nos pide si queremos validar con algún certificado SSL lo definimos de lo contrario dejamos este valor de none por defecto:

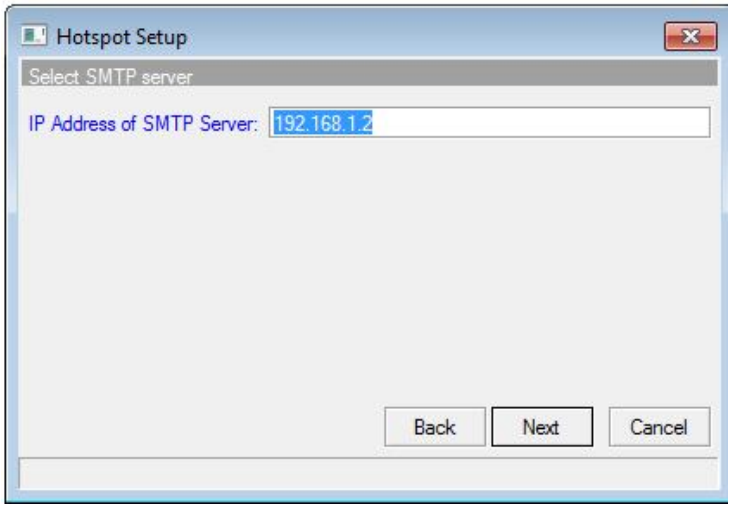
Imagen 187 Selección de certificado



Fuente: Autores – Configuración Mikrotik

Si quiero definir algún servidor smtp para salida de los correos lo especifico en esta página de lo contrario no lo hago, Next.

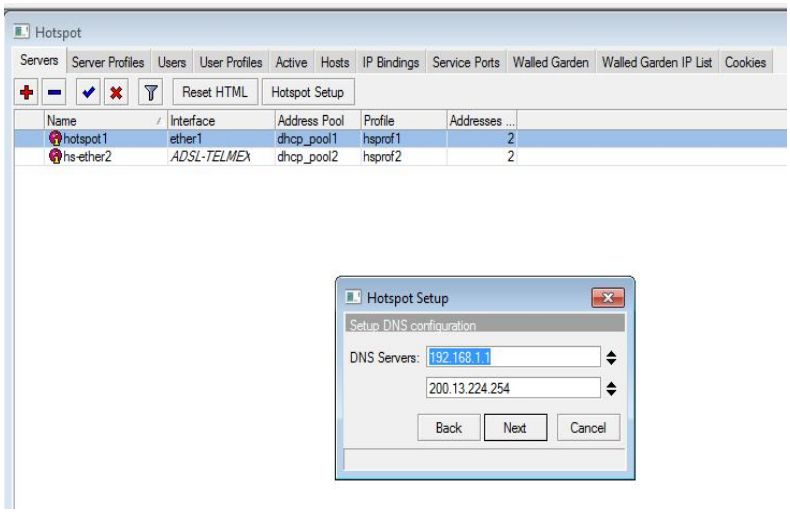
Imagen 188 Definición de smtp para el hostpot



Fuente: Autores – Configuración Mikrotik

Siguiente click en next para visualizar la ventana de definir los dns que usa la compañía o los del proveedor

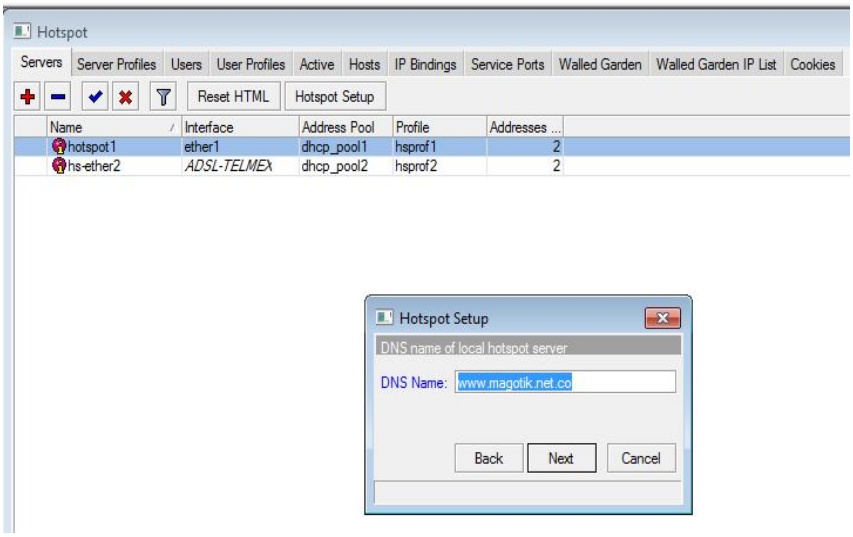
Imagen 189 Definición de DNS para hotspot



Fuente: Autores – Configuración Mikrotik

Siguiente Click en next para definir el nombre del dns que me permite resolver nombres

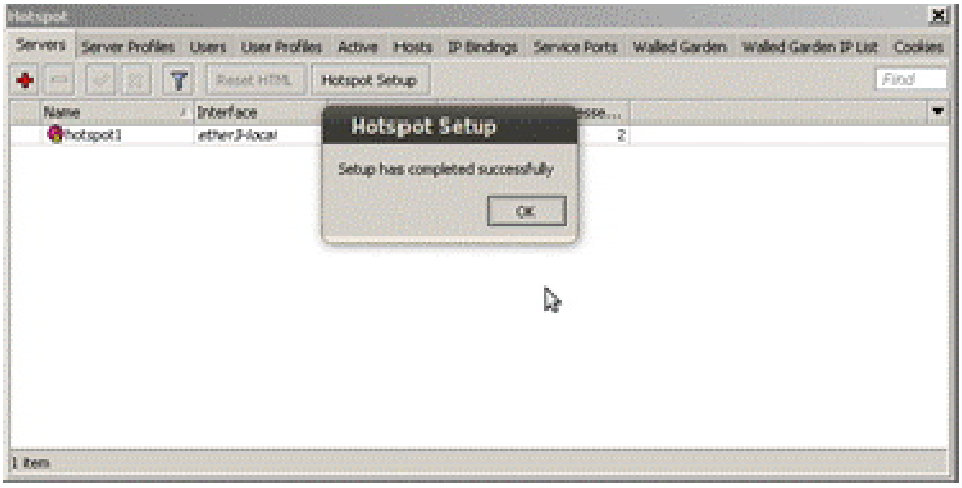
Imagen 190 definición de nombre del DNS



Fuente: Autores – Configuración Mikrotik

Por último observamos que el hotspot se ha configurado satisfactoriamente

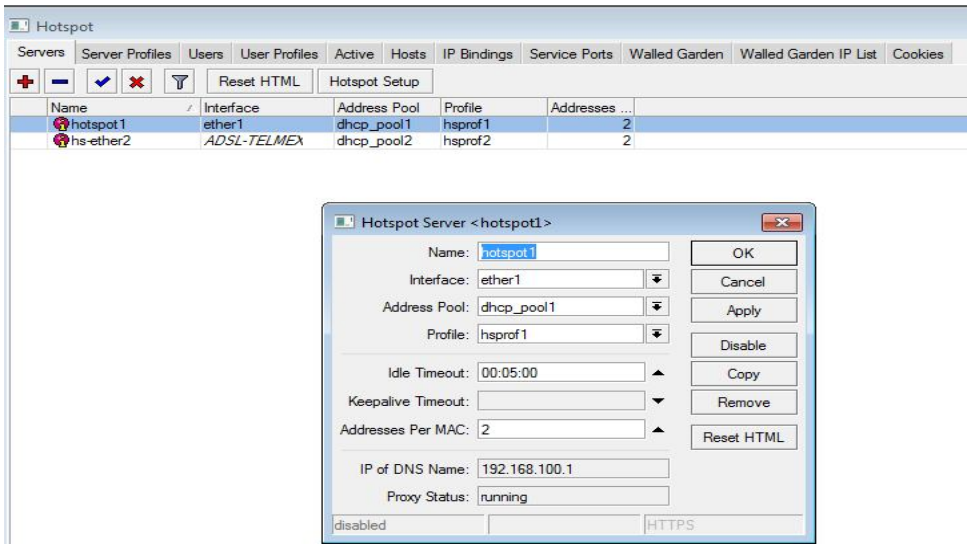
Imagen 191 Finalización de la configuración de hotspot



Fuente: Autores – Configuración Mikrotik

Aquí se observa el hotspot creado llamado hotspot1 sobre la interfaz local 1, ether1 y con el pool de dhcp, el cual tiene un perfil de conexión hsprof1 Si se da doble click sobre el hotspot observo el detalle:

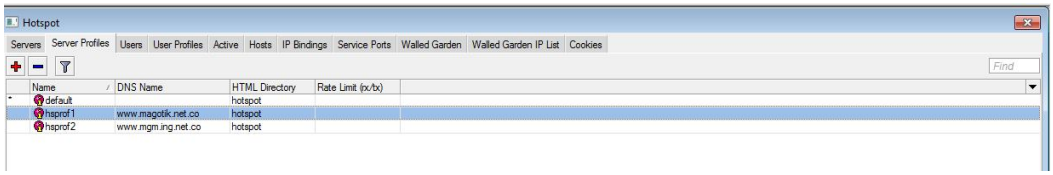
Imagen 192 Detalles del Hotspot



Fuente: Autores – Configuración Mikrotik

Se ingresa dando click en el tag server Profile, observo que tengo una configuración default para el server y para el nuevo creado el hsprof1, se da doble click sobre el hsprof1

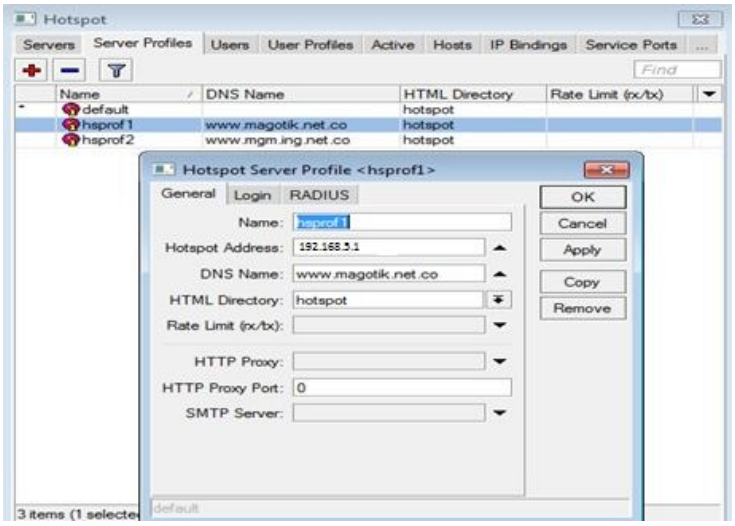
Imagen 193 Ventana server profile



Fuente: Autores – Configuración Mikrotik

Se observa que se autentica en la dirección 192.168.5.1

Imagen 194 autenticación de ip en el Hotspot

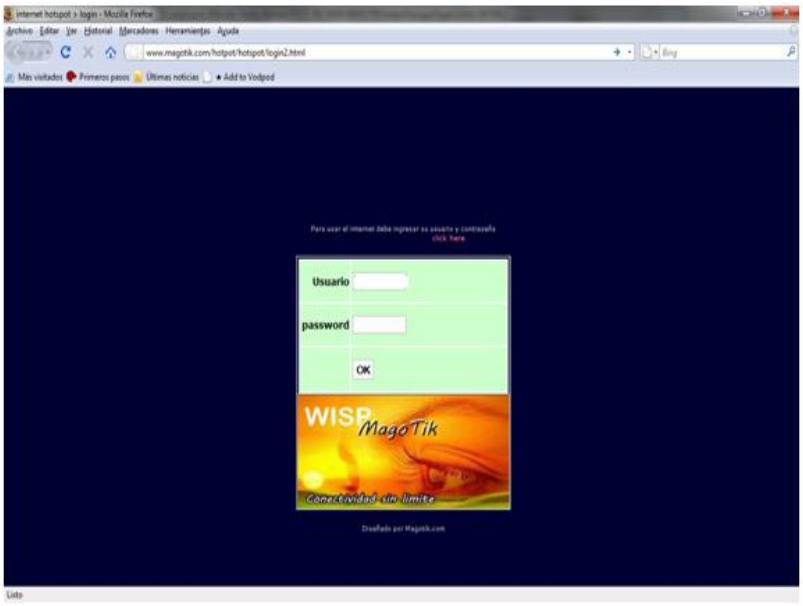


Fuente: Autores – Configuración Mikrotik

Luego pruebo con el usuario default me conecto físicamente con el cable directo o cruzado al puerto 1 del mikrotik y solicito al dhcp server una dirección Ip automática como lo muestra la figura:

Seguimos a abrir un navegador o browser invoco la página de acceso del hotspot 192.168.5.1, ingreso el usuario Internet Rural y password 911

Imagen 195 Página principal del hotspot



Fuente: Autores – Configuración Mikrotik

Imagen 196 ventana de logueo al Hotspot

Fuente: Autores – Configuración Mikrotik

Se observa que se ha logreado el usuario INTERNET RURAL en el sistema:

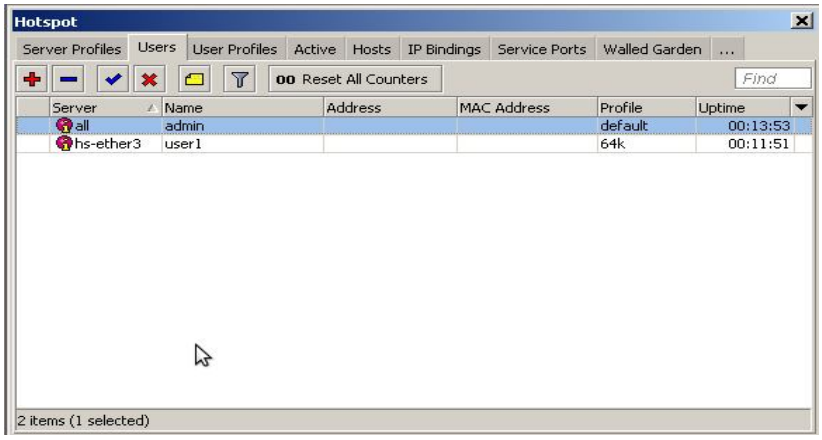
Imagen 197 ventana de autenticación establecida con el Hotspot

Fuente: Autores – Configuración Mikrotik

Luego si quiero asignarle password al usuario admin hago lo siguiente:

Ingreso al Menú voy al tab user: y le doy doble click en el usuario admin para invocar la interfaz de configuración como lo muestra la figura:

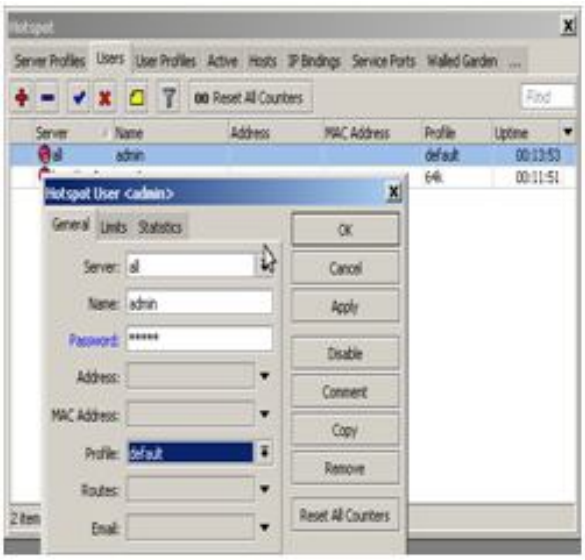
Imagen 198 Interfaz de configuración de usuarios del Hotspot



Fuente: Autores – Configuración Mikrotik

Ingresamos a la tag- Users, no despliega un menú donde nos permite visualizar la configuración del admin nombre de usuario y password y cuál es el perfil al que pertenece el usuario.

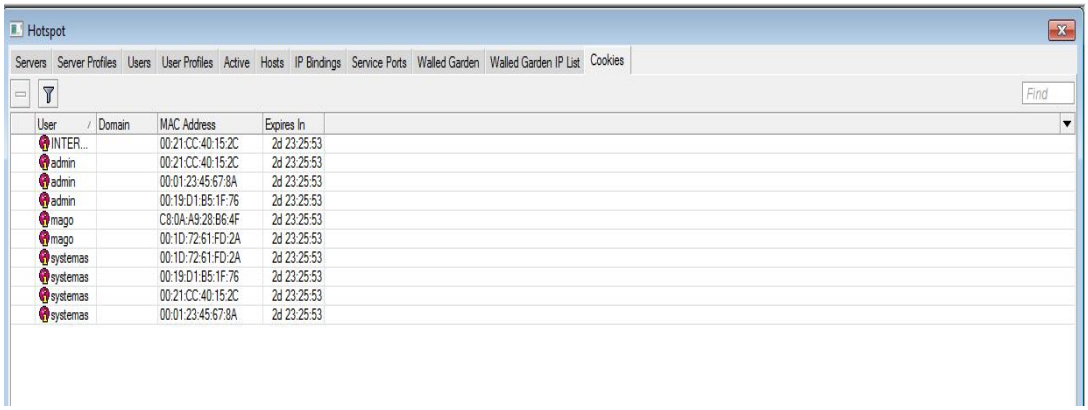
Imagen 199 Administración de perfil de usuario Hotspot



Fuente: Autores – Configuración Mikrotik

Se le asignó el password que para este caso es 911, por último se le da apply y OK para cerrar la ventana, seguimos a probar este nuevo cambio hay que ir al tab de cookies y borrar la cookie de la sesión establecida y borro con el signo menos color azul parte superior derecha y nos queda así:

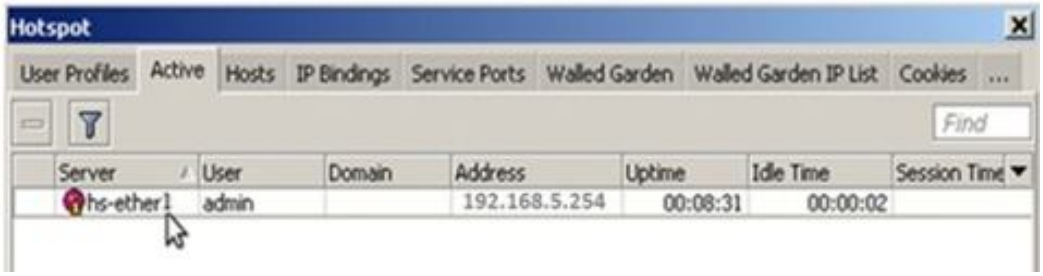
Imagen 200 Ventana de cookies creados por las sesiones establecidas al hotspot



Fuente: Autores – Configuración Mikrotik

Luego se dirige a la Pestaña al tab de active, la selección admin que es la sesión activa y la borro.

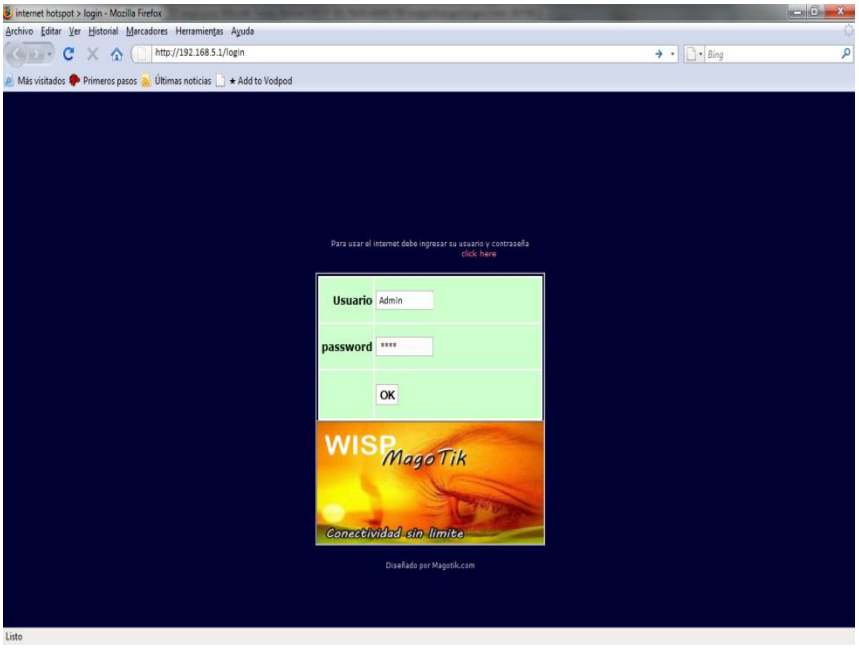
Imagen 201 actividad del hotspot



Fuente: Autores – Configuración Mikrotik

Ingresamos por el navegador así:

Imagen 202 ingreso de administrador a hotspot

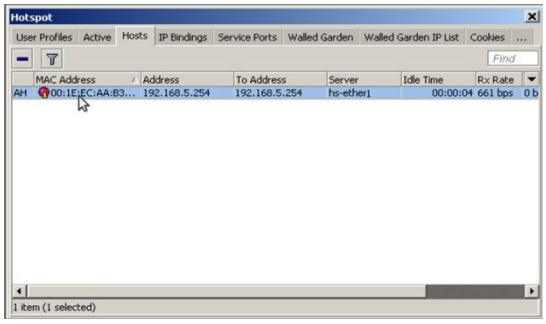


Fuente: Autores – Configuración Mikrotik

Nuevamente pruebo el ingreso al hotspot del usuario admin y la nueva clave 911 ingresando al navegador.

Y por último observo que se ha conectado correctamente:

Imagen 203 Estado de conexión al hotspot



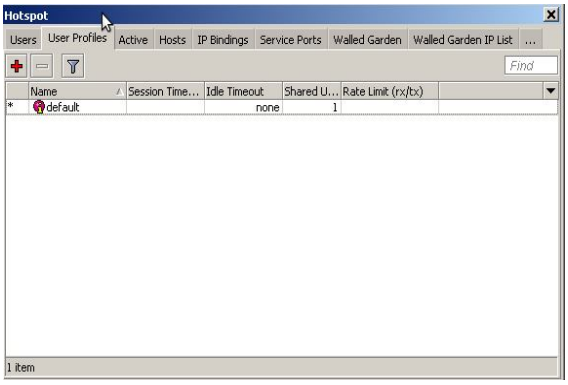
Fuente: Autores – Configuración Mikrotik

Si quiero visualizar los hosts que se están conectando al hotspot, voy al tab hosts que nos muestra que MAC se está conectando asociada al a Ip 192.168.5.254, sobre a interfaz ether1 y server hotspot hs-ether1

Creación de perfiles de Usuarios:

Este paso es para crear perfiles de conexión para usuarios conectados al hotspot hago lo siguiente me paro en el tab User Profiles y hago click en boton + color rojo

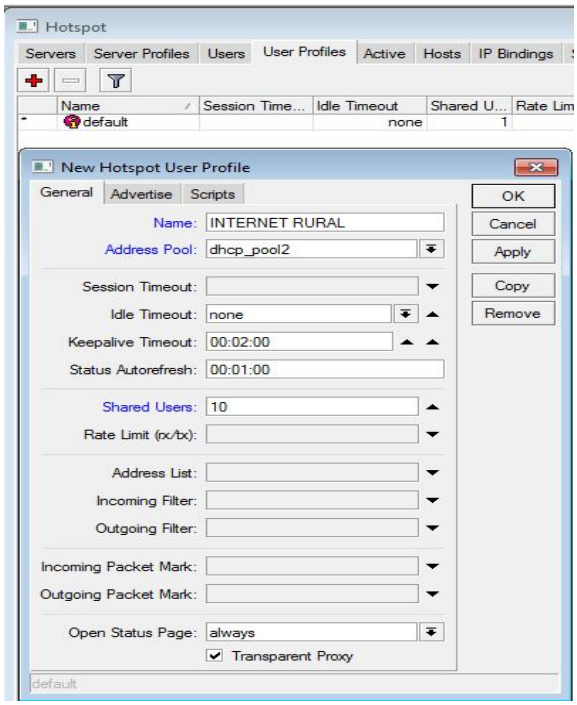
Imagen 204 Creación de perfil de usuario



Fuente: Autores – Configuración Mikrotik

Se crea un nuevo perfil de usuario llamado INTERNET RURAL.

Imagen 205 Creación de perfil de usuario Internet rural

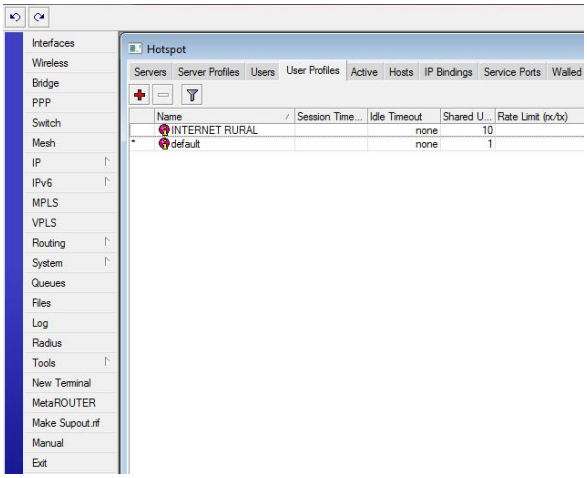


Fuente: Autores – Configuración Mikrotik

Bueno aquí se puede decir que el nombre del perfil es INTERNET RURAL, el dhcp -pool es dhcp-pool-2 pero si tuviéramos otro dhcp lo definiríamos como tal que el número de usuarios que van a compartir este Profile va a ser 10 y que el rate limit (control de ancho de banda) para cada usuario va a ser 64k en RX y 64k en TX.

En esta grafica se puede observar que ha sido creado dicho perfil de usuario:

Imagen 206 Ventana de usuarios Hotspot Internet rural



Fuente: Autores – Configuración Mikrotik

PARA ASOCIAR UN USUARIO AL PERFIL DE INTERNET RURAL

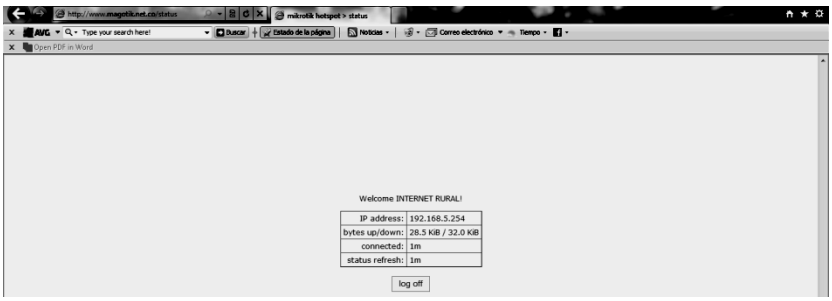
Ingresamos al menú al tab de user y agrego el usuario con el boton más + color rojo a este le defino el nombre del usuario Internet rural con clave 1234 y defino el perfil de usuario de conexión:

Doy click en apply y después ok para salir de esta interfaz y observamos que se ha agregado el usuario **INTERNET RURAL.**

Ahora pruebo la configuración del perfil ingreso el usuario **INTERNET RURAL** y password **911,** en un cliente de la escuela rural.

Se observa que ha sido autenticado por la **Mikrotik** al cliente y lo ingresa al perfil del **INTERNET RURAL** en donde se le asigna el segmento de la red asignado la ip 192.168.5.254/24 para una mejor administración de su cliente y prioridad del servicio del internet.

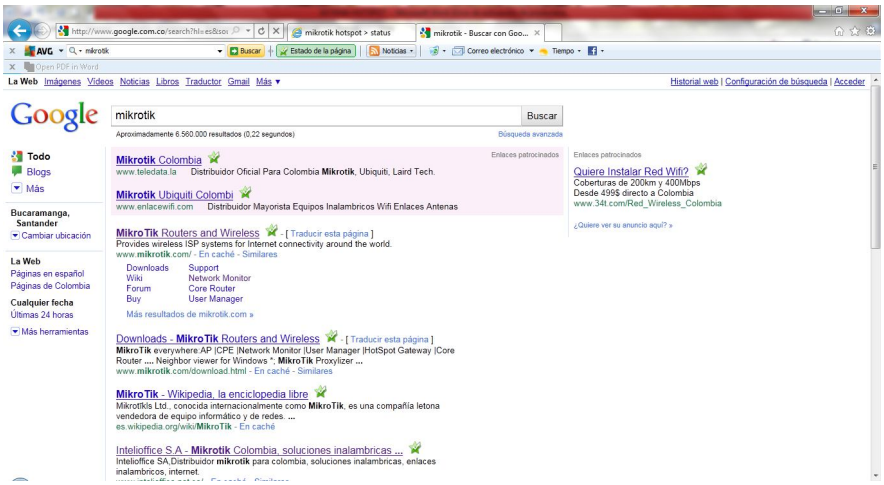
Imagen 207 prueba de ingreso de usuario de internet rural mediante el Hotspot



Fuente: Autores – Configuración Mikrotik

Realizamos la prueba de navegación del pc, abrimos el navegador para probar la navegación.

Imagen 208 Prueba de navegación desde internet Rural



Fuente: Autores – Pruebas de ingreso

Quedando el servicio de internet Rural configurado en los cliente de la escuela rural para su navegación hacia el internet.

Para este caso se le aplican las reglas del firewall de restricción de página no permitidas para los estudiantes y así garantizar un internet sano para los estudiantes.

5.3.24 Servidor de SNMP

Debido a los beneficios que brinda el monitoreo remoto de los servicios de una red. Hemos decidido implementar y habilitarle el servidor de snmp de un router Mikrotik.

Para poder realizar dicha implementación la dividiremos en dos partes. Primero la habilitación o activación del snmp en el router de San Vicente para la red 192.168.1.0. Luego utilizando la aplicación mrtg instalada en el servidor de la dirección de ip raficaremos algunos datos obtenidos.

5.3.24.1 Configuración Servidor SMNP: Dentro del winbox, nos dirigimos al menú SNMP, se nos abre la ventana de configuración, hacemos clic en el botón Settings y le cargamos los siguientes datos.

Enabled (marcado)
Contact info: pedroadmin@server
Location: SanVicente

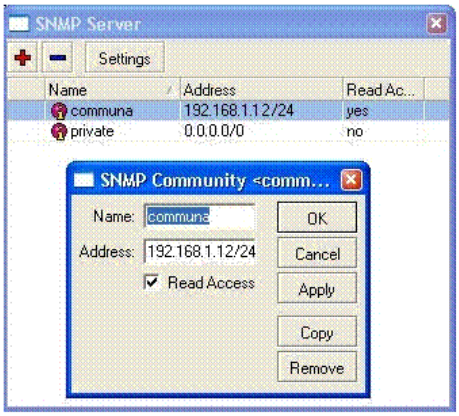
Imagen 209 Configuración de servidor SMNTP

Fuente: Autores – Configuración Mikrotik

Llenando esos casilleros ya tendremos habilitado el servidor de snmp del mikrotik.Luego hay que crear la comunidad snmp, la cual la llamaremos servers. Para ello hacemos clic en el icono (+) y se nos abre la ventana de configuración de comunidad y le cargamos los siguientes datos:

Name: communa
Address: 192.168.1.12/24
Read Access (marcado)
Para una configuración básica esto nos alcanza para poder obtener cierta información del Mikrotik

Imagen 210 Configuración de comunidad SMNTP



Fuente: Autores – Configuración Mikrotik

Dentro de winbox ir al menú New Terminal se nos abre una ventana de terminal.
Ahí dentro debemos escribir lo siguiente para obtener las oid del sistema

 # /interfase print oid

Dicho comando nos mostrara la salida de pantalla con los datos de oid requeridos.

[admin@MikroTik]interfase print oid
0 R name=.1.3.6.1.2.1.2.2.1.2.1 mtu=.1.3.6.1.2.1.2.2.1.4.1
mac-address=.1.3.6.1.2.1.2.2.1.6.1 admin-status=.1.3.6.1.2.1.2.2.1.7.1
oper-status=.1.3.6.1.2.1.2.2.1.8.1 bytes-in=.1.3.6.1.2.1.2.2.1.10.1
packets-in=.1.3.6.1.2.1.2.2.1.11.1 discards-in=.1.3.6.1.2.1.2.2.1.13.1
errors-in=.1.3.6.1.2.1.2.2.1.14.1 bytes-out=.1.3.6.1.2.1.2.2.1.16.1
packets-out=.1.3.6.1.2.1.2.2.1.17.1 discards-out=.1.3.6.1.2.1.2.2.1.19.1
errors-out=.1.3.6.1.2.1.2.2.1.20.1
1 R name=.1.3.6.1.2.1.2.2.1.2.2 mtu=.1.3.6.1.2.1.2.2.1.4.2
mac-address=.1.3.6.1.2.1.2.2.1.6.2 admin-status=.1.3.6.1.2.1.2.2.1.7.2
oper-status=.1.3.6.1.2.1.2.2.1.8.2 bytes-in=.1.3.6.1.2.1.2.2.1.10.2
packets-in=.1.3.6.1.2.1.2.2.1.11.2 discards-in=.1.3.6.1.2.1.2.2.1.13.2
errors-in=.1.3.6.1.2.1.2.2.1.14.2 bytes-out=.1.3.6.1.2.1.2.2.1.16.2
packets-out=.1.3.6.1.2.1.2.2.1.17.2 discards-out=.1.3.6.1.2.1.2.2.1.19.2
errors-out=.1.3.6.1.2.1.2.2.1.20.2
2 R name=.1.3.6.1.2.1.2.2.1.2.3 mtu=.1.3.6.1.2.1.2.2.1.4.3
mac-address=.1.3.6.1.2.1.2.2.1.6.3 admin-status=.1.3.6.1.2.1.2.2.1.7.3
oper-status=.1.3.6.1.2.1.2.2.1.8.3 bytes-in=.1.3.6.1.2.1.2.2.1.10.3

packets-in=.1.3.6.1.2.1.2.2.1.11.3 discards-in=.1.3.6.1.2.1.2.2.1.13.3
errors-in=.1.3.6.1.2.1.2.2.1.14.3 bytes-out=.1.3.6.1.2.1.2.2.1.16.3
packets-out=.1.3.6.1.2.1.2.2.1.17.3 discards-out=.1.3.6.1.2.1.2.2.1.19.3
errors-out=.1.3.6.1.2.1.2.2.1.20.3
3 R name=.1.3.6.1.2.1.2.2.1.2.7 mtu=.1.3.6.1.2.1.2.2.1.4.7
mac-address=.1.3.6.1.2.1.2.2.1.6.7 admin-status=.1.3.6.1.2.1.2.2.1.7.7
oper-status=.1.3.6.1.2.1.2.2.1.8.7 bytes-in=.1.3.6.1.2.1.2.2.1.10.7
packets-in=.1.3.6.1.2.1.2.2.1.11.7 discards-in=.1.3.6.1.2.1.2.2.1.13.7
errors-in=.1.3.6.1.2.1.2.2.1.14.7 bytes-out=.1.3.6.1.2.1.2.2.1.16.7
packets-out=.1.3.6.1.2.1.2.2.1.17.7 discards-out=.1.3.6.1.2.1.2.2.1.19.7
errors-out=.1.3.6.1.2.1.2.2.1.20.7
4 R name=.1.3.6.1.2.1.2.2.1.2.10 mtu=.1.3.6.1.2.1.2.2.1.4.10
mac-address=.1.3.6.1.2.1.2.2.1.6.10 admin-status=.1.3.6.1.2.1.2.2.1.7.10
oper-status=.1.3.6.1.2.1.2.2.1.8.10 bytes-in=.1.3.6.1.2.1.2.2.1.10.10
packets-in=.1.3.6.1.2.1.2.2.1.11.10 discards-in=.1.3.6.1.2.1.2.2.1.13.10
errors-in=.1.3.6.1.2.1.2.2.1.14.10 bytes-out=.1.3.6.1.2.1.2.2.1.16.10
packets-out=.1.3.6.1.2.1.2.2.1.17.10 discards-out=.1.3.6.1.2.1.2.2.1.19.10

errors-out=.1.3.6.1.2.1.2.2.1.20.10

Observemos los valores obtenidos:

packets-in=.1.3.6.1.2.1.2.2.1.11.10
packets-out=.1.3.6.1.2.1.2.2.1.17.10
packets-in=.1.3.6.1.2.1.2.2.1.11.7
packets-out=.1.3.6.1.2.1.2.2.1.17.7
packets-in=.1.3.6.1.2.1.2.2.1.11.3
packets-out=.1.3.6.1.2.1.2.2.1.17.3
packets-in=.1.3.6.1.2.1.2.2.1.11.2
packets-out=.1.3.6.1.2.1.2.2.1.17.2

Dichos valores los utilizaremos mas adelante en la configuración del mrtg Concluida la primera parte de la configuración, deberemos instalar el software mrtg en el servidor de debian que tenemos en la red. Damos por entendido que el servidor apache ya está instalado y corriendo.

Para la instalación seguiremos los siguientes pasos.
 # apt-get install mrtg

Con el software ya instalado editamos el archivo de configuración que se encuentra en /etc/mrtg.cfg.

EnableIPv6: no
WorkDir: /var/www/mrtg
##
 # System: 192.168.1.1
 # Description: router
 # Contact: pedroadmin@server
 # Location: Sanvicente
##

Target[192.168.1.1_cpu]:
1.3.6.1.2.1.25.3.3.1.2.1&1.3.6.1.2.1.25.3.3.1.2.1:communa@192.168.1.1:
AbsMax[192.168.1.1_cpu]: 100
MaxBytes[192.168.1.1_cpu]: 100
Title[192.168.1.1_cpu]: 192.168.1.1 CPU load
PageTop[192.168.1.1_cpu]: <H1>192.168.1.1 CPU load</H1>
Options[192.168.1.1_cpu]: gauge,growright,nopercent, noo
YLegend[192.168.1.1_cpu]: CPU load
ShortLegend[192.168.1.1_cpu]: %
LegendI[192.168.1.1_cpu]: CPU load (percentage)
Paquetes in out
Target[192.168.1.1_2]:
1.3.6.1.2.1.2.2.1.11.2
&1.3.6.1.2.1.2.2.1.17.2:communa@192.168.1.1:
MaxBytes[192.168.1.1_2]: 64000
Title[192.168.1.1_2]: Paquetes in / out interfase 1
PageTop[192.168.1.1_2]: <H1>Paquetes in / out</H1>
<TABLE>
<TR><TD>System:</TD> <TD>PMI 192.168.1.1 </TD></TR>
<TR><TD>Description:</TD><TD> Paquetes in / out </TD></TR>
</TABLE>

Paquetes in out
Target[192.168.1.1_2]:
1.3.6.1.2.1.2.2.1.11.3
&1.3.6.1.2.1.2.2.1.17.3:communa@192.168.1.1:
MaxBytes[192.168.1.1_2]: 64000
Title[192.168.1.1_2]: Paquetes in / out interfase 2
PageTop[192.168.1.1_2]: <H1>Paquetes in / out</H1>
<TABLE>
<TR><TD>System:</TD> <TD>PMI 192.168.1.1 </TD></TR>
<TR><TD>Description:</TD><TD> Paquetes in / out </TD></TR>
</TABLE>

Paquetes in out
Target[192.168.1.1_2]:
1.3.6.1.2.1.2.2.1.11.7
&1.3.6.1.2.1.2.2.1.17.7:communa@192.168.1.1:
MaxBytes[192.168.1.1_2]: 64000
Title[192.168.1.1_2]: Paquetes in / out interfase 3
PageTop[192.168.1.1_2]: <H1>Paquetes in / out</H1>

<TABLE>
<TR><TD>System:</TD> <TD>PMI 192.168.1.1 </TD></TR>
<TR><TD>Description:</TD><TD> Paquetes in / out </TD></TR>
</TABLE>

Paquetes in out
Target[192.168.1.1_2]:
1.3.6.1.2.1.2.2.1.11.10
&1.3.6.1.2.1.2.2.1.17.10:communa@192.168.1.1:
MaxBytes[192.168.1.1_2]: 64000
Title[192.168.1.1_2]: Paquetes in / out interfase 4
PageTop[192.168.1.1_2]: <H1>Paquetes in / out</H1>
<TABLE>
<TR><TD>System:</TD> <TD>PMI 192.168.1.1 </TD></TR>
<TR><TD>Description:</TD><TD> Paquetes in / out </TD></TR>
</TABLE>

Esta configuración nos mostrara la carga del CPU y los paquetes enviados y recibidos por 4 interfases. A continuación deberá crear el archivo index.html para que sea visualizada la información en forma de gráficos en una pagina Web.

*indexmaker /etc/mrtg.cfg --columns=1 --output *
/var/www/mrtg/index.html

Finalmente debe correr 3 veces el comando mrtg para que se generen los archivos de base de datos necesarios.

#mrtg

Esta configuración será ejecutada cada 5 minutos mediante el cron Redireccionando nuestro navegador a la dirección http://192.168.1.2/mrtg nos dará las graficas obtenidas.

5.3.25 Configuración del NanoStation-PowerStation

Imagen 211 NanoStation

Fuente: www.ubnt.com/airos- manual técnico Ubiquiti Nano Station 2

El Nanostation 2 y el PowerStation 2, han sido elegidos, por siguientes motivos, ser un dispositivo compacto, apto para el uso exterior, utilizar un chip ampliamente extendido en dispositivos wifi como es el chip Ateros, tener un precio competitivo, y además se han realizados mejoras continuas en el firmware y publicando el código fuente del sistema operativo, para que sus usuarios puedan también realizar mejoras.

5.3.25.1 Características Técnicas: El Nanostation 2 es un dispositivo robusto, con una antena integrada de 10db, resistente para el uso en el exterior y una potencia de transmisión de 400mw. Dispones también de conector SMA para la conexión de una antena exterior más potente, y se le suministra CA a través del cable de red, con un POE ya integrado en el paquete.

El PowerStation 2, se tiene un tamaño más grande, integra antena de 17db, también es resistente para el uso en el exterior con una potencia de 400mw. No Dispone de un conector para antena exterior, y tiene dos interfaces de

red LAN. Como el Nanostation, se alimenta con un POE ya incluido, a través del primer conector de cable de red.

5.3.25.2 Sistema Operativo: Tanto el Nanostation como el PowerStation, comparten el mismo sistema operativo, llamado AisOS, y suministrado por el fabricante, Ubiquiti, al que realizan mejoras continúas. Con el Sistema Operativo AisOS, tenemos las funciones básicas del dispositivo Wireless, podemos configurarlo como servicios de Route, Servicio de DHCP, DNS, Firewall.

¿Por qué se necesita un PowerStation, O un Nanostation?

Siempre se recomienda el PowerStation, pero si se está **a menos de 1km del repetidor**, y tenemos **visión directa y sin obstáculos**, se podrá hacer uso del NanoStation. También recalcar que estos dispositivos no hacen milagros, hay que buscar siempre la mejor posición, con la que se obtenga mejor señal, y que tenga los menos obstáculos posibles.

Recordar que operar en la red con un dispositivo con muy baja señal, puede afectar al rendimiento de la red, pudiendo expulsar a ese cliente, hasta que la situación quede subsanada.

5.3.25.3 Configuración Rápida: Tanto el Nanostation como el PowerStation, tienen como ip inicial 192.168.1.20, por lo que tendremos que configurar en el PC una ip del mismo rango, por ejemplo, 192.168.1.200. Una vez encendido y conectado al PC, introducimos en el navegador la dirección del router wifi (192.168.1.20), introduciendo el usuario y contraseña que trae por defecto de fábrica: Usuario: ubnt y Contraseña: ubnt.

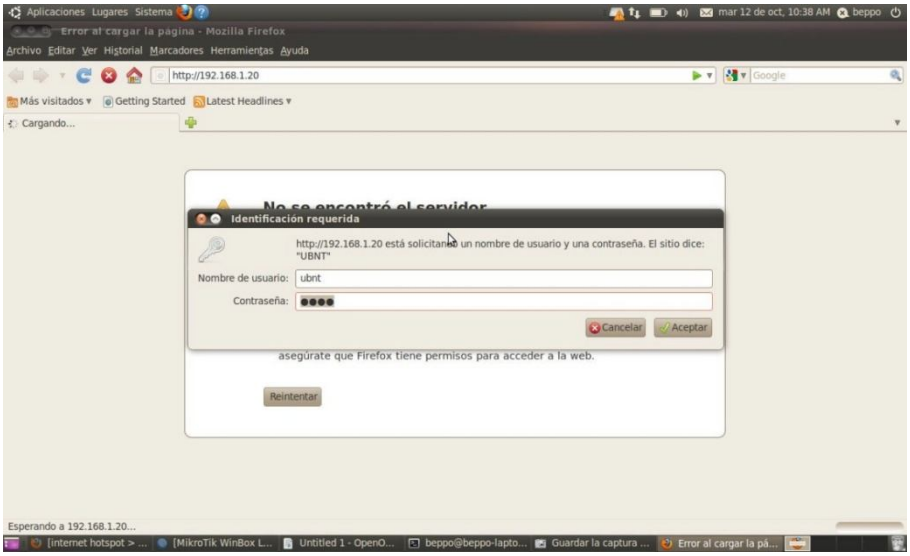
Comprobamos la versión del firmware es la que se recomienda para el uso en la red “MAGOTIK”, si no es así, se procederá a actualizar el sistema operativo, con el firmware proporcionado. Una vez actualizado el firmware, procederemos a introducir la configuración por defecto a través de un archivo

de configuración básica, también disponible en el foro arriba nombrado, o en el Departamento de Informática del Concello. Este archivo, una vez cargado y aplicado, modificara el comportamiento del dispositivo de la siguiente manera:

Se cambia el modo de funcionamiento de Bridge a modo router, siendo ahora su dirección 192.168.5.1, y activando el servidor dhcp para la red interna. El servidor dhcp repartirá ip desde el rango 192.168.5.3 hasta 192.168.5.255. Se deja fuera del rango la ip 192.168.5.2, para que esta ip sea para el PC que suministre algún ip o de servidor a la red wifi, como por ejemplo el Direct Connect.

También se activa el re direccionamiento del puerto 3000 TCP y 3001UDP hacia la ip 192.168.5.2 para el uso del servicio Direct Connect, que se tendrá que configurar para usar estos puertos.

Imagen 212 Ventana inicial de acceso a configuración de Ubiquiti



Fuente: Autores – Configuración Ubiquiti

Conociendo esto, una vez aplicado el archivo de configuración, sólo quedara para el usuario modificar la contraseña por defecto del Power/Nano, y en la pestaña Link Setup, cambiar el nombre de usuario y la contraseña, donde pone El Usuario y La Contraseña, y aplicar los cambios, evidentemente. Una vez hecho esto, el dispositivo ya está listo para usar.

Esto sólo ha sido una guía rápida, desde luego, en el capítulo Configuración Avanzada, se explicaran con más detalle como configurar nuestro Nano/PowerStation.

Configuración Avanzada

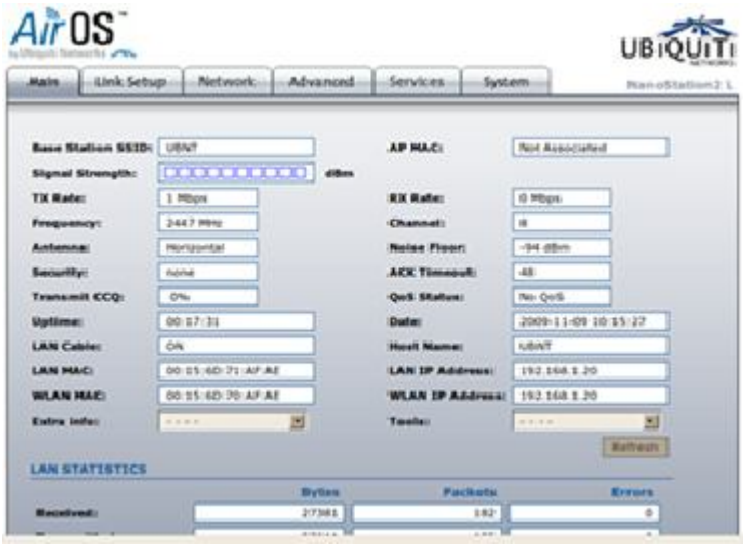
Tanto el PowerStation como el NanoStation, por defecto, esto es, cuando lo acabamos de comprar, o cuando lo reseteamos, viene en modo bridge, con la ip 192.168.1.20, y como usuario para el control de acceso llamado ubnt y contraseña ubnt.
A continuación procederé a explicar cómo deben estar todas las opciones del sistema operativo AirOS.

La mayoría de las opciones ya están incluidas en el archivo de configuración base. Tendremos como regla que para efectuar un cambio le daremos a cambiar, y para aplicarlo, una vez dado a cambiar, en la parte superior pulsaremos a Aplicar para activar los cambios en el sistema.

Pestaña Main
En esta pestaña se nos mostrara el estado del dispositivo.

Automáticamente me aparece la interfaz de administración del Ubiquiti

Imagen 213 Interfaz de configuración Ubiquiti



Fuente: Autores – Configuración Ubiquiti Air OS

Información a destacar:

- SSID Estación Base: Nombre de la red a la que estamos conectados.
- Mac AP: Mac del AP al que estamos conectado, bastante útil para saber con qué repetidor enlazamos, sería como el DNI del repetidor.
- Fuerza de la Señal: Es el nivel con la cual recibimos la señal del repetidor. Para actualizar pinchar en Actualizar.
- Alinear Antena: Utilidad que nos informa del nivel de señal actualizándose constantemente.

Imagen 214 Nivel de señal del Ubiquiti

Fuente: Autores – Configuración Ubiquiti Air OS

- Lan Dirección IP: dirección ip interna del Nano/PowerStation.

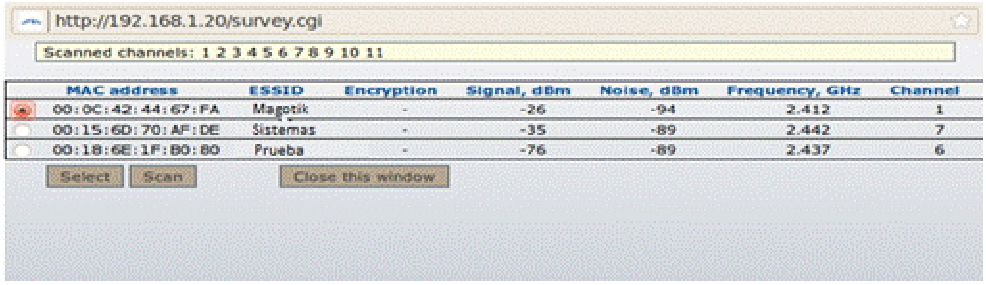
- Dirección IP WLAN: dirección ip que tenemos en la rede wifi, dato bastante útil, ya que es la que tendremos que poner por ejemplo en la casilla ip externa del DC++, para que pueda funcionar correctamente.

Pestaña Link Setup: En esta pestaña configuraremos las opciones básicas del enlace Wireless, así como los datos para validarnos en la red.

Datos a destacar:

- Modo Inalámbrico: seleccionaremos Estación.
- ESSID: Nombre de la red a la cual queremos conectarnos, en nuestro caso ubtn.
- Seleccione Abre el cuadro de búsqueda de AP como se muestra en la siguiente imagen.

Imagen 215 Búsqueda de Ap



Fuente: Autores – Configuración Ubiquiti Air OS

- Vincular al MAC AP: en caso de recibir señal de dos o más APs de ubtn, pondremos aquí la MAC del AP con el cual queramos enlazar, el que tenga señal más fuerte normalmente.
  - Código País: Spain, para disponer de los 13 canales.
  - Modo IEEE 802.11: elegimos B/G mixto, el modo B no es recomendable, ya que no está muy pulido.
  - Potencia de Salida: por defecto lo pondremos al máximo, debe estar la casilla de obedecer potencia reglamentaria desactivada. En caso de estar muy cerca del repetidor, o estar en una zona con muchas

construcciones, se recomienda bajar algo la potencia, para evitar rebotes.

- Velocidad de Datos: marcaremos Auto por defecto.
  Seguridad: WPA-TKIP.
- WPA Identity: Pondremos aquí el usuario suministrado por el Administrador del Dispositivo, para el acceso a la red.
- WPA User Name: anonymous.
- WPA User Password: Contraseña suministrada por el Administrador del Dispositivo

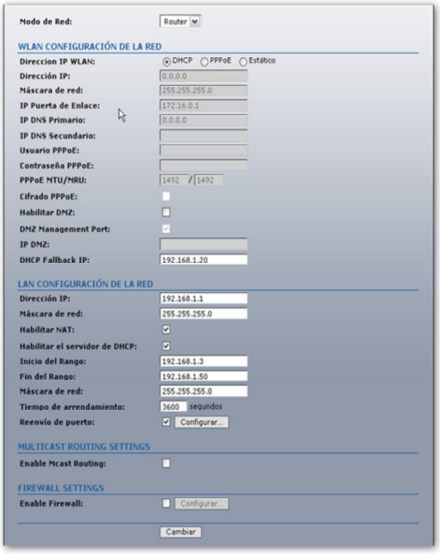
Imagen 216 Asociación de la Mac del Ap a la configuración

Fuente: Autores – Configuración Ubiquiti Air OS

Esto sería la configuración básica para acceder a la red del Magotik.

Configuración básica recomendada para el acceso a la rede Magotik de las interfaces de red. Como podrán ver será en modo Router y no en Bridge como viene por defecto el Power/Nanostation.

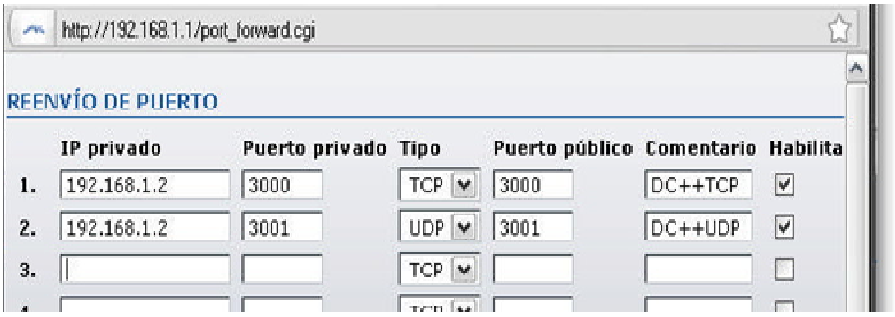
Imagen 217 Configuración de NanoStation en modo router



Fuente: Autores – Configuración Ubiquiti Air OS

- Dirección IP WLAN: marcaremos DHCP, para que el router obtenga ip del servidor central de la red Magotik.
- Dirección IP: pondremos 192.168.1.1, esta será la dirección local del router.
- Habilitar NAT: con esta casilla, diremos al router que traduzca las direcciones de la red wireless (192.168.5.1) a las direcciones de nuestra red local(192.168.1.0)
- Habilitar el servidor de DHCP: Activado par el rango 192.168.1.3-192.168.1.50 para que el router nos envíe ips a los PCS de nuestra red local. Se saca la ip 192.168.1.2, para que esta ip la tenga el PC destinado a servidor.
- Reenvío de puerto: Activado, en el archivo de configuración básica estarán activados dos reenvíos de puertos para usar en el DC. Estas redirecciones se dirigirán a la ip 192.168.1.2 como se muestra en la siguiente imagen.

Imagen 218 Reenvío de Puertos para el Ap

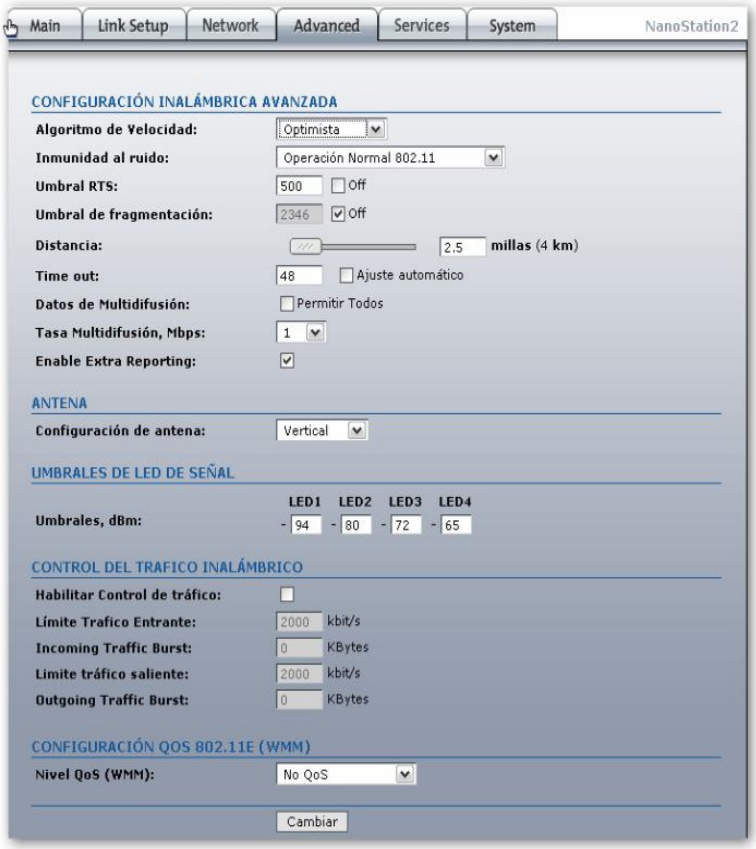


Fuente: Autores – Configuración Ubiquiti Air OS

Pestaña Advanced

- Algoritmo de Velocidad: elegiremos Optimista o Conservativo en caso de tener baja señal.
- Inmunidad al ruido: Operación Normal
- Umbral RTS: 500 Muy importante que este valor este activado.
- Time Out: Usaremos la cifra estándar de 48 y la casilla Ajuste Automático desactivado.
- Tasa Multidifusión: 1
- Configuración de Antena: Vertical.
- Umbrales, dbm: aquí marcamos los umbrales de señal a partir de donde se encenderán los leds del
- Power/Nanostation.

Imagen 219 Configuración avanzada de NanoStation



Fuente: Autores – Configuración Ubiquiti Air OS

Pestaña System

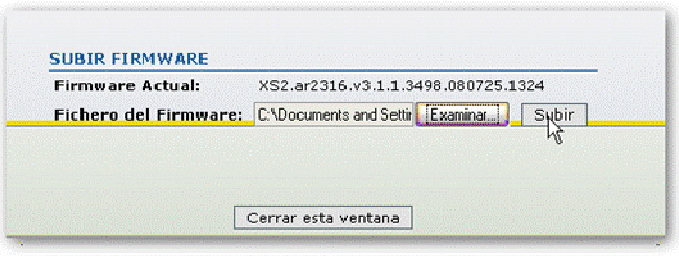
Imagen 220 cambio de valores del sistema para el NanoStation

Fuente: Autores – Configuración Ubiquiti Air OS

En esta pestaña podremos cambiar valores del sistema, como actualizar el firmware, cambiar la contraseña de acceso, resetear los valores del sistema, cargar el archivo de configuración por defecto o reiniciar el router.

Podremos ver la versión del firmware, en la imagen, v3.1.1.1, para actualizar pincharemos en Actualizar.

Imagen 221 Vista de la Actualización de Firmware del NanoStation



Fuente: Autores – Configuración Ubiquiti Air OS

Elegimos el firmware pinchado en Examinar… que queremos instalar, por norma, los firmwares que empiecen por NS2 serán para el Nano y los que empiecen por PS2 para el Power. Si empieza por XS2 valdrán para ambos. Una vez elegido pinchamos en Subir.

Imagen 222 actualización de Firmware del NonoStation

Fuente: Autores – Configuración Ubiquiti Air OS

Y Actualizamos

Una vez actualizado, se reiniciara el Router, y mantendrá la misma configuración, si queremos cargar la configuración por defecto proporcionada por el Concello, iremos al apartado Administración de la Configuración de la pestaña System.

Imagen 223 Administrar configuración del NonoStation

Fuente: Autores – Configuración Ubiquiti Air OS

Como en el caso del firmware, pincharemos en Examinar, elegimos el archivo de configuración adecuado, y subimos, y solo quedaría aplicar los cambios para que surtan efecto y que quede el Router configurado como se ha explicado arriba.

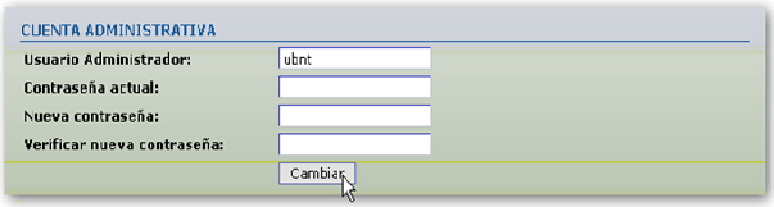
Imagen 224 Aplicación de cambios en la configuración del Nanostation

Fuente: Autores – Configuración Ubiquiti Air OS

Recordar que una vez aplicados los cambios el PowerStation o el Nanostation pasarían a modo router, con una ip 192.168.1.1, por lo que tendremos que configurar el PC o como cliente dhcp, o asignarle una ip fija. Tan solo quedaría cambiar el usuario y contraseña de usuario de red, y la contraseña del dispositivo.

Para cambiar la contraseña del dispositivo, en la misma pestaña de System solo tendremos que introducir la antigua contraseña en Contraseña Actual, y poner la contraseña nueva en las dos siguientes casillas, y como no pinchar en Cambiar y Aplicar los cambios.

Imagen 225 cambio de contraseña del dispositivo NanoStation

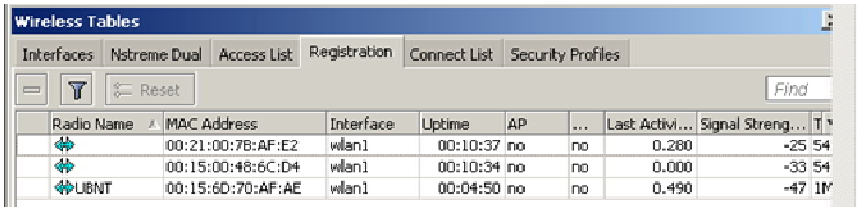


Fuente: Autores – Configuración Ubiquiti Air OS

También podremos cambiar el nombre de usuario si queremos.
En el archivo de configuración básica ya viene definido como idioma el español, pero para cambiarlo antes de cargar el archivo si quiere solo tendrá que seleccionarlo en la Pestaña System.

Ahora en el mikrotik principal observo los siguiente: ingreso a la opcion de wireless y observo en el tag registration las Mac asociadas junto con la estación UBNT que fue la que acabe de enganchar.

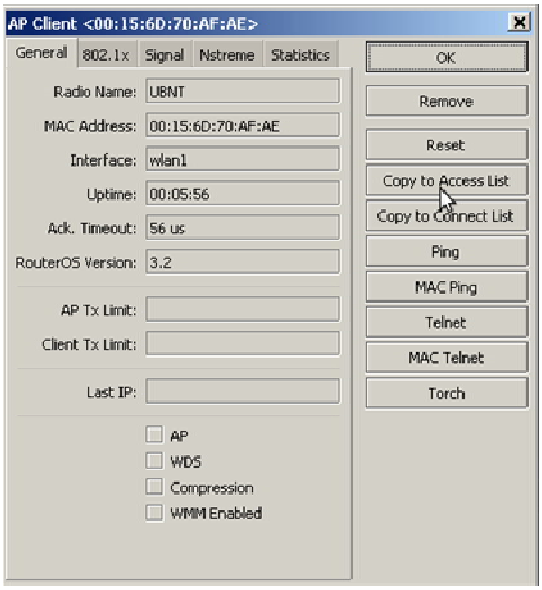
Imagen 226 Lista de dispositivos conectados



Fuente: Autores – Configuración Ubiquiti Air OS

Para establecerle seguridad lo que debo hacer es lo siguiente, selección el AP (doble click) y lo meto a la lista de Connect list y a la access List.

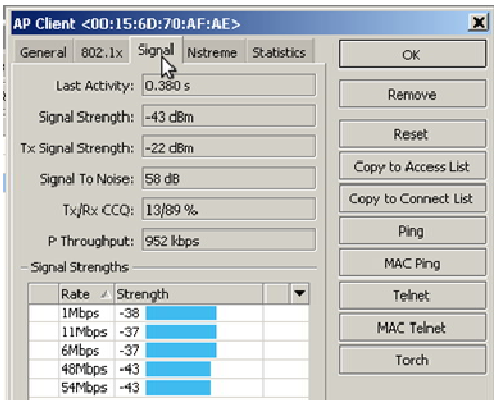
Imagen 227 Establecimiento de seguridad para el AP



Fuente: Autores – Configuración Ubiquiti Air OS

Hay dos botones copy to access list copy to connect list doy click sobre cada uno de estos si quiero ver e nivel de intensidad de la señal de cada uno de estos AP doy click en el tab signal.

Imagen 228 Nivel de intensidad de los AP

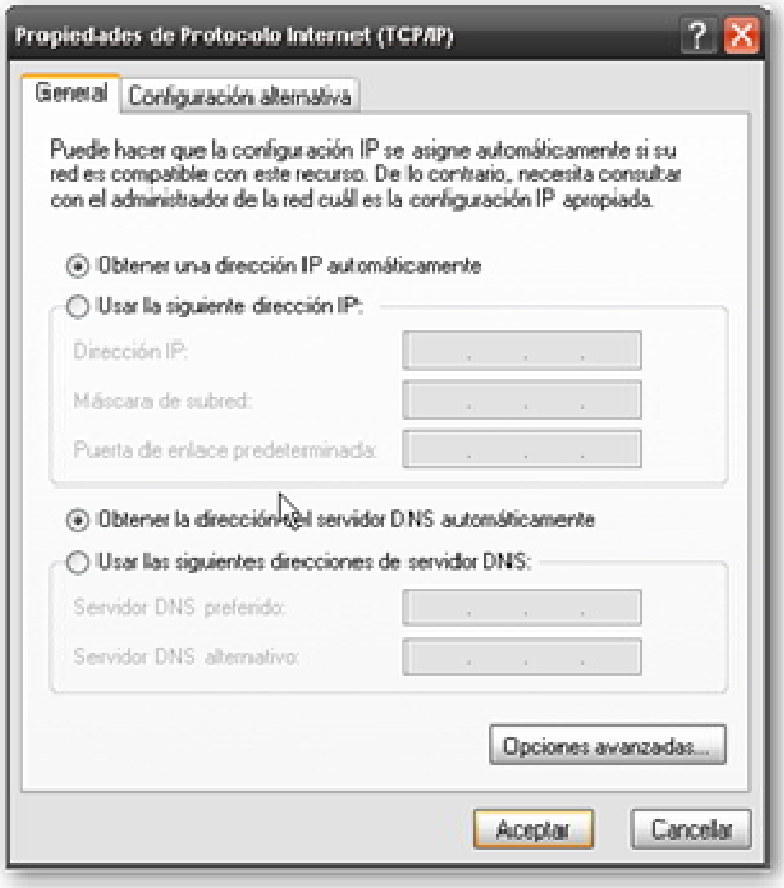


Fuente: Autores – Configuración Ubiquiti Air OS

Configuración del PC cliente

Con el archivo de configuración por defecto del Concello, solo tendremos que configurar la interfaz de red, como cliente dhcp, esto es así:

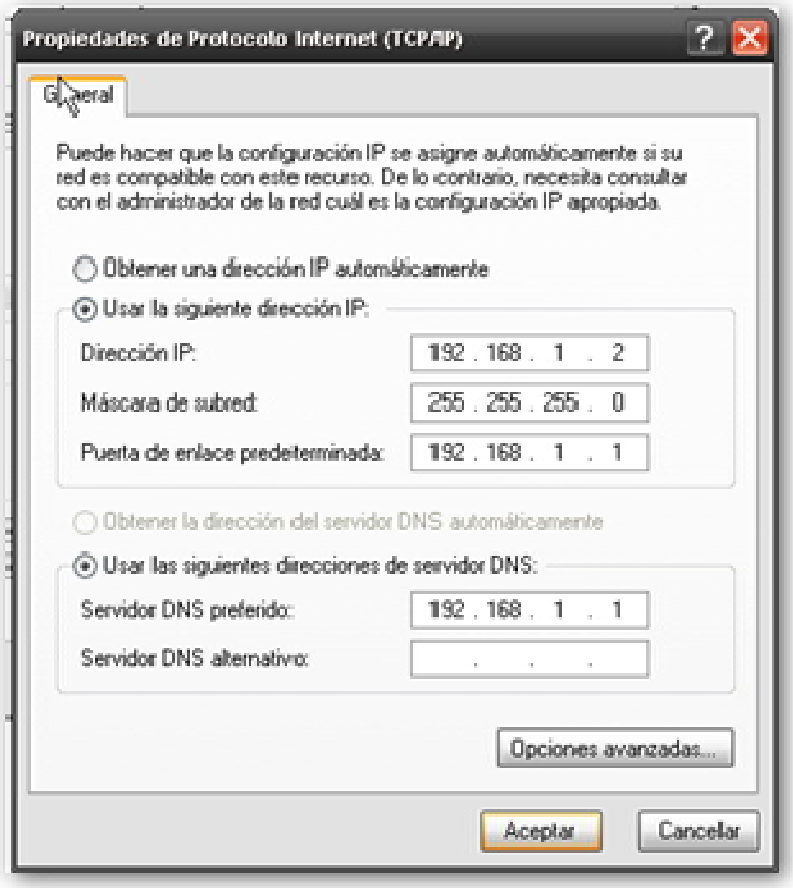
Imagen 229 Propiedades de tcp/ip para clientes del AP



Fuente: Autores – Configuración pc cliente wi fi

Recordar que el PC que vaya hacer uso del Direct Connect, debe tener ip fija, que será la 192.168.1.2, máscara 255.255.255.0, puerta de enlace 192.168.1.1 y servidor DNS preferido 192.168.1.1

Imagen 230 direccionamiento del Cliente para conexión al AP



Fuente: Autores – Configuración pc cliente wi fi

Esto es así porque las redirecciones hechas en el router para los puertos del Direct Connect se dirigen a esta dirección.

Para configurar el Direct Connect para usar estos puertos, solo debéis ir al menú Archivo>Opciones del Direct Connect, y en el apartado Opciones de Conexión, marcar la opción Cortafuegos con mapeo manual de puertos, y poner el puerto TCP como 3000 y el UDP como 3001.

5.3.26 Instalación y configuración de equipos en terreno

5.3.26.1 Instalación de antenas Sectoriales

Imagen 231 Interior de las Antenas a utilizar

Fuente: Autores – revisión de antenas e instalación

Imagen 232 Configuración de antenas en la Torre de metálica

Fuente: Autores – revisión de antenas e instalación

Imagen 233 Revisión de Antenas

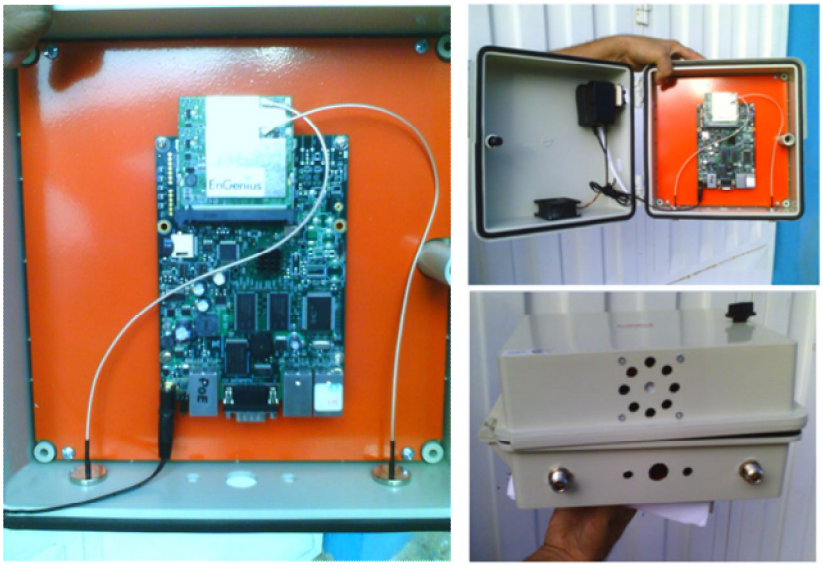
Fuente: Autores – revisión de antenas e instalación

Imagen 234 Zonas radiadas por las antenas

Fuente: Autores – Visual de zonas a radiar

5.3.26.2 Instalación de Mikrotik y pictails a las antenas

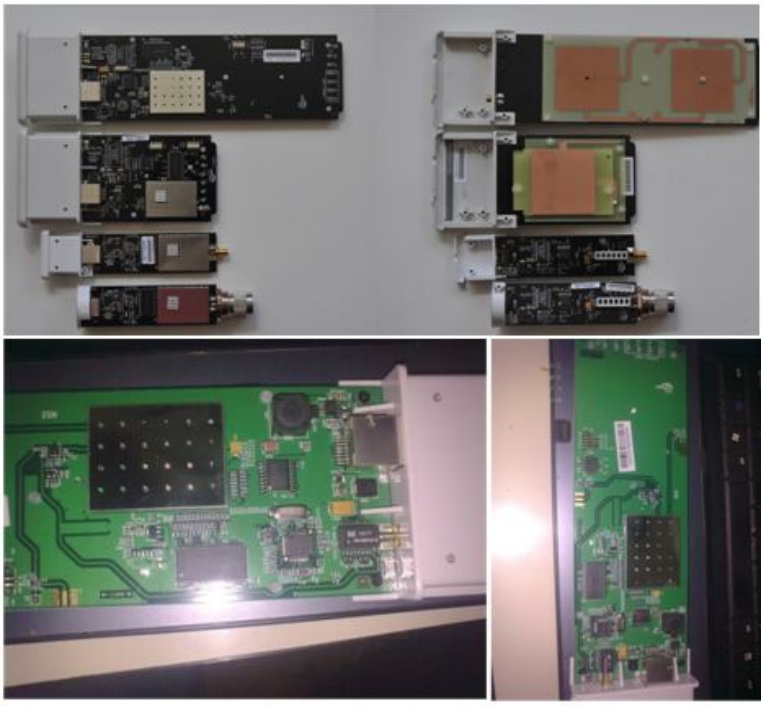
Imagen 235 Muestra de mikrotiks en caja Exterior



Fuente: Autores – Montaje de Mikrotik en la caja exterior

5.3.26.3 Instalación Ubiquity Nanostation2 y PowerStation

Imagen 236 Interior de los Ubiquitis



Fuente: http://redlibrepy.wordpress.com/page/7/

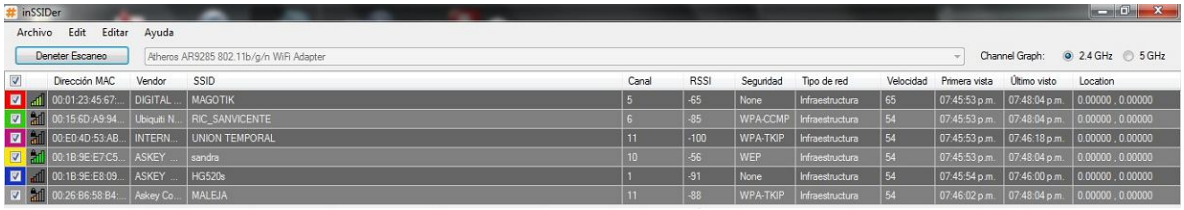
Imagen 237 Instalación de NanoStation

Fuente: Autores – Montaje de Ubiquitis

5.3.27 Análisis de señal mediante software

El análisis se realizo mediante el software gratuito InSSIDer, con el cual se verifico la radiación y potencia de la señal en distintos puntos de la ciudad dentro del rango establecido.

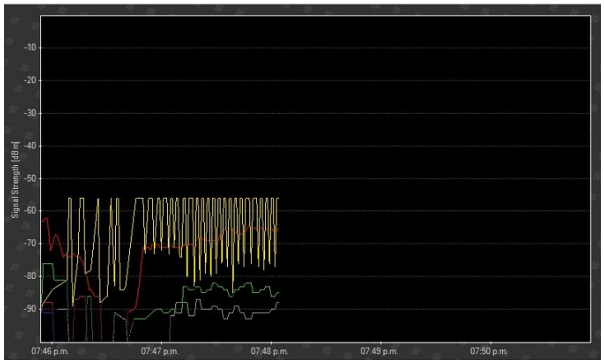
Imagen 238 Grafica de canales mediante software InSSIDer



Dirección MAC	Vendor	SSID	Canal	RSSI	Seguridad	Tipo de red	Velocidad	Primera vista	Último visto	Location
00:01:23:45:67:...	DIGITAL ...	MAGOTIK	5	-65	None	Infraestructura	65	07:45:53 p.m.	07:48:04 p.m.	0.00000 , 0.00000
00:15:6D:A9:94:...	Ubiquiti N...	RIC_SANVICENTE	6	-85	WPA-CCMP	Infraestructura	54	07:45:53 p.m.	07:48:04 p.m.	0.00000 , 0.00000
00:E0:4D:53:AB:...	INTERN...	UNION TEMPORAL	11	-100	WPA-TKIP	Infraestructura	54	07:45:53 p.m.	07:46:18 p.m.	0.00000 , 0.00000
00:1B:9E:E7:C5:...	ASKEY ...	sandra	10	-56	WEP	Infraestructura	54	07:45:53 p.m.	07:48:04 p.m.	0.00000 , 0.00000
00:1B:9E:E8:09:...	ASKEY ...	HG520s	1	-91	None	Infraestructura	54	07:45:54 p.m.	07:46:00 p.m.	0.00000 , 0.00000
00:26:B6:58:B4:...	Askey Co...	MALEJA	11	-88	WPA-TKIP	Infraestructura	54	07:46:02 p.m.	07:48:04 p.m.	0.00000 , 0.00000

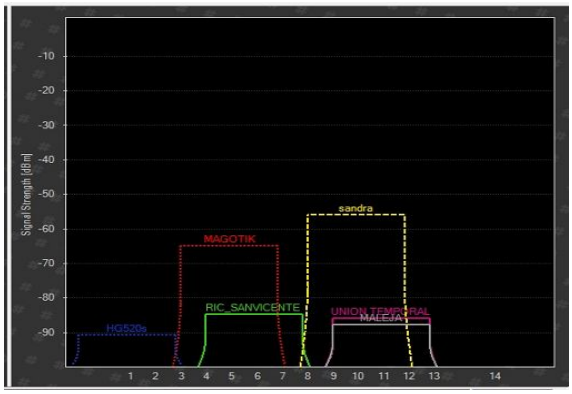
Fuente: Autores – Verificación con Software InSSIDer

Imagen 239 Grafico de tiempos de las señales captadas



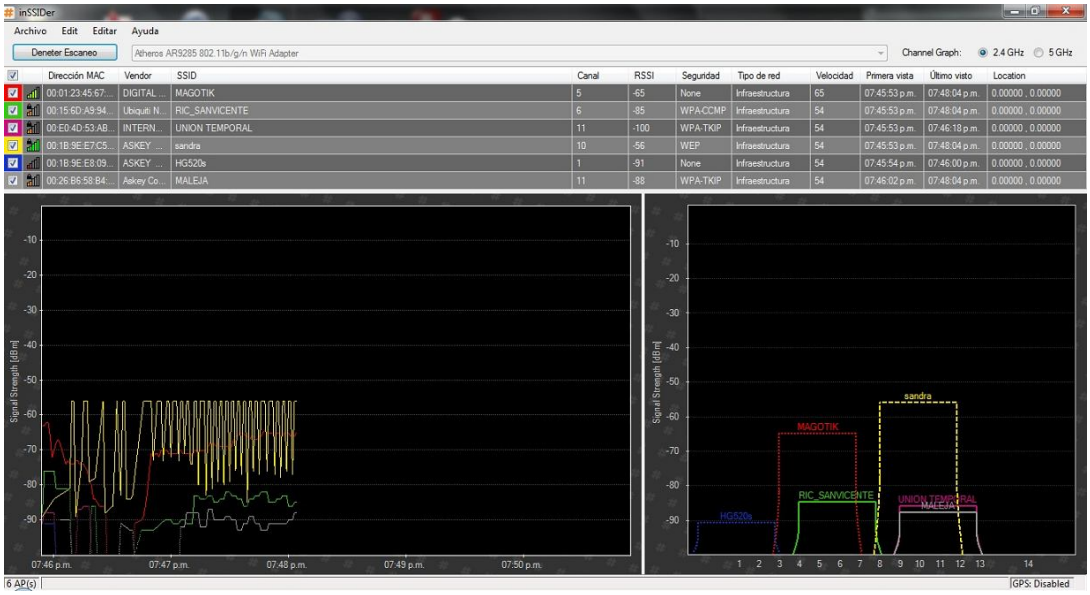
Fuente: Autores – Verificación con Software InSSIDer

Imagen 240 Grafico de intensidad de los Canales



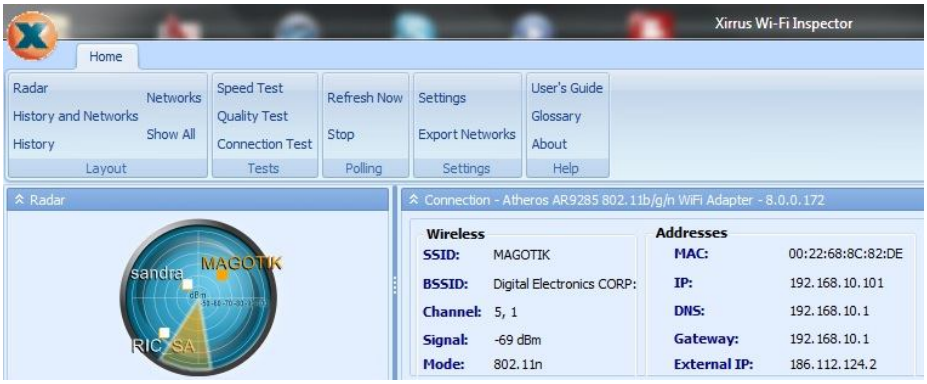
Fuente: Autores – Verificación con Software InSSIDer

Imagen 241 Ventana general de análisis de señales Wifi simulando un cliente



Fuente: Autores – Verificación con Software InSSIDer

Imagen 242 Análisis de rango de acción de red Magotik WISP



Fuente: Autores – Verificación con Software Xirrus

Imagen 243 Análisis de Adaptadores wifi del ISP

Fuente: Autores – Verificación con Software Xirrus

6 Conclusiones

- Se realizo el diseño e implemento un piloto para el WISP de San Vicente y su zona rural.

- Para la implementación de la red se utilizó herramientas open source como el sistema operativo Mikrotik RouterOS basado en Linux que viene con el dispositivo, sistema operativo Linux obunto en franja de servidores, sistema operativo de Ubiquitis Air OS, software de análisis de señal InSSIDer y Xirrus, y software para radio enlaces RadioMobile.

- Se definió la configuración de las interfaces. Asignando nombres, direcciones de IP a las mismas y definición de las Vlan.

- Se configuró el servidor de DHCP para cada una de las sub redes definidas por sectores y requerimientos de clientes. En el cual se definieron los pools de ip para cada una. También la asignación direcciones de IP fijas a partir de direcciones MAC de los servidores.

- Se configuró un servidor de VPN para comunicar la red Empresarial en nuestro caso las oficinas de Citec San Vicente con las de Citec de Bucaramanga.

- Se configuró un servidor de Web Proxy para optimizar la utilización de los recursos hacia Internet. En el mismo se configuro políticas de bloqueo de tráfico hacia ciertas páginas al igual que el bloqueo de descarga de ciertos archivos.

- Se realizó un balanceo de carga entre los dos proveedores de Internet seleccionados. Para la optimización del recurso.

- Se realizaron políticas de control de ancho de banda para los clientes P2P.

- Se implemento políticas de firewall como bloqueo de p2p, bloqueo del Msn Messenger, redireccionamiento de puertos y bloqueo de paquetes no deseados.

- Este trabajo permitió aplicar los conocimientos recibidos en la especialización de telecomunicaciones de la Universidad Industrial de Santander.

- este proyecto contribuye a la investigación de nuevas tecnologías y soluciones en proveedores de servicios de internet inalámbricos, siendo una fuente importante de información para los nuevos investigadores que estén interesados en este tema.

- Este trabajo sirve como referencia para generación de nuevos proyectos basados en redes inalámbricas como

BIBLIOGRAFIA

AGUILAR L, Roy: GUERRERO M, melissa, Análisis y diseño para la creación de un proveedor de servicios de internet inalámbrico (wisp). Ecuador, 2004

AGUILAR M, Gustavo, Sistema detección de intrusos para una red inalámbrica de una pyme. Mexico 2007.

ARRAYA C, Alberto, Análisis comparativo y conclusiones técnico-económicas para una posible implementación de los estándares WiMAX 802.16d ó WiMAX 802.16e en la Zona Metropolitana de Costa Rica. Noviembre de 2007.

CONDE, L. Instalación de una red LAN con tecnología PLC en una escuela del sistema de educación cubano, Revista Técnica de la Empresa de Telecomunicaciones de Cuba S.A, Cuba, N°2, 2006.

DOSTERT, K. Powerline Communications , Prentice Hall, USA, 2001.

ENRÍQUEZ HARPER, Gilberto, Líneas de Transmisión y Redes de Distribución de Potencia Eléctrica Vo 1 y Vo 2 , Editorial LIMUSA S.A.

ESPINOSA, Andrés: GONZALES, Miriam: VERA, Christiam, Análisis y diseño para la creación de un proveedor de servicios de internet inalámbrico (wisp). Julio 2008.

HUIDROBO José m y Davis Roldán.:"Serie Telecomunicaciones REDES Y SERVICIOS DE BANDA ANCHA, Tecnología y Aplicaciones, Primera Edición, Editorial MCGraw-Hill, 2005, 133-134, 255-259

HRASNICA, H. Broadband Powerline Communications: Network Design, John Wiley & Sons, USA, 2004.

IEEE Std 802.1Q-199 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks," Mar, 1999.

JOCHEN Schiller, "Mobile Communications", Addison-Wesley

LOPEZ M, Jorge, Diseño e implementación de un sistema de gestión de accesos a una red wi-fi utilizando software libre. Lima 2008.

PEREZ, Henry. Interference Characteristics of Broadband Power Line Communication Systems Using Aerial Medium Voltage Wires", IEEE Communications Magazine, USA, Vol 43 N°4, 2005.

TANEBAUM, Andrew. Computer Network, Third Edition, Prentice Hall, New Jersey, 1996. Page 102-169

VELASCO R, Milton René, Diseño de un wisp (Wireless Internet Service Provider) en el campus de la universidad técnica del norte para proveer servicios de internet inalámbrico utilizando un esquema wireless mesh con tecnología wi-fi. Noviembre 2009 Director. Ing. Erwin Barriga.

CYBERGRAFIA

http://www.palowireless.com/

http://www.80211-planet.com/

http://www.wirelessdevnet.com/

http:www.redeswimax.jimdo.com.

http://www.irontec.com/qos.html

http://qos.iespana.es/capitulo2.htm

http://www.scielo.org.co/

http://www.netfilter.org/

http://koalasoft.wordpress.com/manuales/distribucion-del-ancho-de-banda-utilizando-htb-e-iptables/

http://usuarios.multimania.es/ccd_illusions/QoS-3.pdf

http://www.mikrotik.org

http://www.ankaa.com.br

http://www.laniway.com.br/

http://www.mikrotik.com/