

Desarrollo de una red telemática para proveer acceso a Internet al municipio de Casariche

ALUMNO: FRANCISCO GÁLVEZ PANIAGUA

CONSULTOR: ANTONI MORELL PÉREZ

Índice

Desarrollo de una red telemática para proveer acceso a Internet al municipio de Casariche.....	1
Primera Parte: Definición del proyecto	5
Introducción.....	5
Justificación y objetivos del proyecto.....	5
Viabilidad del proyecto.....	6
Descripción del municipio.....	6
Aspectos legales.....	6
Viabilidad técnica.....	7
Viabilidad económica.....	7
Provisión de equipos e infraestructura.....	8
Estimaciones económicas.....	9
Segunda parte: análisis del proyecto	12
Necesidades de ancho de banda previstas.....	12
Descripción del sistema WiFi.....	19
Planificación.....	22
Infraestructura de red	24
Topología de la red.....	25
Estudio de la cobertura con Radio Mobile.....	25
Análisis de los radioenlaces Wimax.....	27
Tercera Parte: Configuración de equipos.....	30
Configuración de router Mikrotik para la red municipal.....	30
Configuraciones iniciales.....	30
Configurar DNS Cache.....	34
Configuración de un servidor Web proxy (proxy-cache).....	35
Configurando Full Caché.....	37
Configuración DHCP Server.....	39
Portal cautivo.....	39
Creando perfiles y usuarios.....	41
Limitando la velocidad de los usuarios del servicio gratuito.....	43
Seguridad de la red.....	44
Control del tráfico en nuestra red.....	44
Alertas.....	48
Conclusiones.....	50

Anexo: Hojas de características 52

Primera Parte: Definición del proyecto

Introducción

Justificación y objetivos del proyecto

Como consecuencia de los hábitos de vida actuales, se impone la necesidad, cada vez más urgente, de disponer de una administración ágil que permita al ciudadano realizar las gestiones que necesite proporcionándole una movilidad total, minimizando el número de desplazamientos y gestiones necesarias para el cumplimiento de sus deberes con las administraciones públicas. En este contexto y aprovechando la rápida implantación de los terminales móviles, ya sean ordenadores personales o teléfonos inteligentes, los ayuntamientos y el resto de organismos públicos están tomando medidas para facilitar y potenciar el uso de las tecnologías de la información entre los ciudadanos.

El objetivo de este TFC es el realizar un análisis, diseñar e implementar una

Red telemática que permita ofrecer acceso a Internet en el municipio de Casariche, en la provincia de Sevilla, mediante tecnologías inalámbricas.

En principio se proyecta la red para que se pueda dar acceso dentro del núcleo urbano, aunque con la previsión de poder ampliar en el futuro su cobertura a otras zonas dentro del término municipal.

Mediante este proyecto se ofrece al municipio una infraestructura de red para el acceso a Internet en dos modalidades, una gratuita aunque limitada en su velocidad y otra *Premium* con una velocidad mayor aunque sujeta a una cuota de suscripción. La finalidad del servicio *Premium* es que la red pueda quedar autofinanciada con las aportaciones de los propios usuarios, sin que suponga al Ayuntamiento ningún coste adicional.

Entre las principales ventajas de disponer de una red municipal destacan potenciar el uso de las tecnologías de la información dentro del municipio, contribuyendo de esta forma a la reducción de la brecha digital y acercar al ciudadano los servicios de la e-administración, que permita a los ciudadanos de una forma rápida y eficaz el acceso a los servicios municipales y en general a cualquier contenido que pueda ayudar al desarrollo comercial y empresarial, al intercambio cultural y el turismo en la zona.

Las tecnologías a emplear serán WiMax (Worldwide Interoperability for Microwave Access) basada en el estándar IEEE 802.16 y Wi-Fi basada en la norma IEEE 802.11b. La unión de ambas tecnologías va a permitir desarrollar una infraestructura fiable y eficiente.

Viabilidad del proyecto

Descripción del municipio

Casariche es un municipio español de la provincia de Sevilla, Andalucía. En el año 2011 contaba con 5.627 habitantes. Su extensión superficial es de 53 km² y tiene una densidad de 105,87 hab/km². Sus coordenadas geográficas son 37° 17' 38" Norte y 4° 45' 34" Oeste (37.29° Norte y 4.76° Oeste, expresadas en grados decimales). Se encuentra situada a una altitud de 296 metros y a 122 kilómetros al sureste de la capital de provincia, Sevilla.

Su término limita en la provincia con Estepa al noroeste, Lora de Estepa al oeste, La Roda de Andalucía al sur y Badolatosa al este. Casariche viene a ser, estadísticamente hablando, la villa media de la provincia de Sevilla, pues de los 105 municipios que conviven en la provincia, Casariche ocupa el puesto 58° en población, 59° por extensión y 46° en cuanto a densidad poblacional.



Relieve

Casariche se alza a 296 metros sobre el nivel del mar, aunque la altitud difiere considerablemente en distintos puntos del núcleo urbano debido a que no se encuentra en una llanura, sino en las escarpadas pendientes que acompañan al río Yeguas. El punto más alto se encuentra en el emplazamiento del polideportivo municipal, en la zona este con 359 metros.

Respecto a la orografía del término, la zona septentrional y occidental presenta escasas irregularidades, manteniéndose en el margen de los 200 a 300 metros. La zona noreste es más abrupta, ganando en altitud conforme se aproxima a la zona este, donde entre los cerros de La Atalaya de Casariche y La Estacada de las Monjas, registra los 400 metros de altura.

La zona meridional es la más elevada, con altitudes superiores a los 350 metros y cerros de más de 400. Cabe destacar la de Cerro Chirlanga (390 metros), Cañada del Hierro (405 m), Laguna de Juan Pérez (413 metros) y la más alta en Cortijo Santa Rita con sus 437 metros.

Aspectos legales

Las redes telemáticas de ámbito municipal, como la que se propone en este proyecto, están reguladas por la Comisión del Mercado de las Telecomunicaciones, en adelante CMT, la cual

establece una serie de requisitos para su desarrollo y puesta en funcionamiento, recogidos en la Circular 1/2010, por la que se regulan las condiciones de explotación de redes y la prestación de servicios de comunicaciones electrónicas por las Administraciones Públicas y que se puede consultar en la dirección <http://www.boe.es/boe/dias/2010/08/09/pdfs/BOE-A-2010-12831.pdf>

Entre los principales requisitos impuestos por la CMT se encuentran la obligación de registrarse ante la CMT como operador y establecer qué tipo de servicio se va a prestar.

En nuestro caso se van a prestar dos servicios diferenciados, por un lado un **servicio gratuito**, permitido por la CMT siempre que la velocidad no sea superior a 256 Kbps, y por otro lado un **servicio de pago**, mas completo, que no se va a ver afectado por esa limitación de velocidad.

En el primer caso, por la propia limitación de la conexión, el regulador entiende que no se afecta a la libre competencia, aunque requiere que los prestadores del servicio se sometan a ciertos principios generales de actuación y ciertas obligaciones legales. En el segundo, si va a requerir el cumplimiento de requisitos más exigentes, pues aquí si que se podría afectar a la libre competencia con empresas del sector.

Viabilidad técnica

En la actualidad existen proyectos similares para poblaciones de todo tipo, algunas de ellas ofreciendo servicio a zonas mucho más amplias que las que este proyecto pretende acometer. A medida que estos proyectos se han ido generalizando, los fabricantes han ido mejorando sus dispositivos y adaptándolos a las necesidades de un mercado que poco a poco iba desarrollándose, de manera que hoy disponemos de suficientes proveedores de equipos así como de proyectos en funcionamiento como para poder garantizar la viabilidad técnica del proyecto.

Viabilidad económica

La inversión necesaria por parte de las administraciones públicas para acometer el proyecto de implantación y mantenimiento de la red proporcionará a los ciudadanos beneficios inmediatos, como una disminución en los desplazamientos necesarios para la realización de las gestiones administrativas más frecuentes, así como una reducción en el tiempo necesario para comunicarse con las administraciones publicas. La comunicación más eficiente con los órganos de gobierno ya de por si justificaría el proyecto, pero además se obtienen otros beneficios derivados de la posibilidad de ofrecer a través de la red municipal información que contribuya al desarrollo económico, cultural, comercial y turístico de la zona así como a la alfabetización digital de los habitantes del municipio.

El coste de un proyecto de este tipo puede afrontarse de varias maneras, bien mediante un inversor privado que asuma el coste, bien mediante un sistema que permita otorgar una concesión a empresas del sector interesadas en la explotación de la red. En cualquier caso, por las propias características de la zona a cubrir y el bajo coste de los equipos, asumimos que se requerirá una cuota de mercado pequeña para que sea viable. Además se podría financiar mediante técnicas de crowdfunding o vendiendo espacios publicitarios a las empresas interesadas en aparecer en la página de inicio del portal cautivo.

Provisión de equipos e infraestructura

Se han considerado las soluciones propuestas por las principales compañías como AirSpan, Alvarion, Aperto Networks, Mikrotik, Ubiquiti, Albentia o Proxim, entre otras, buscando sobre todo:

- § Una buena relación calidad-precio
- § Una probada solvencia en el desarrollo de instalaciones similares
- § Facilidad en la instalación y mantenimiento de equipos
- § Escalabilidad

De entre las alternativas disponibles se ha optado por un despliegue basado en la tecnología Wimax para la red de transporte, proporcionado por Alvarion, y en la tecnología Wifi para la red de distribución, con equipos Mikrotik y antenas Ubiquiti.

Para nuestro proyecto no vamos a necesitar una gran inversión en equipos, ya que la zona a la que hay que dotar de cobertura es relativamente pequeña – un cuadrado de unos 2,5 Km. de lado- y es además bastante homogénea, sin que existan viviendas aisladas. Por otra parte disponemos de localidades cercanas – menos de 40 Km. - de las que poder obtener el acceso a Internet que después distribuiríamos en Casariche. La principal dificultad del proyecto está en los accidentes geográficos del casco urbano, que se encuentra en una ladera de un monte y además rodeado por un arroyo que dibuja un pequeño valle, por lo que desde algunas zonas no se va a disponer de visibilidad directa con los distintos puntos de acceso ya que hay varias pendientes pronunciadas.

Como una estimación inicial de equipos, necesitaríamos al menos un enlace desde el ISP hasta la estación base que pueda proporcionar como mínimo el ancho de banda proyectado de 140 Mbps, y desde la estación base distribuiríamos la señal a todo el pueblo.

Para la estación base se empleará **Alvarion BreezeMAX Extreme 5000** ya que este fabricante ya ha sido el proveedor elegido en otros proyectos que actualmente están funcionando con buenos resultados.

Para la estación base Wifi, así como para la gestión de la red se van a instalar equipos del fabricante **Mikrotik**, los cuales tienen como principales ventajas su bajo coste y la facilidad que aportan a la hora de configurar todos los aspectos relevantes a la hora de gestionar un Wireless Internet Service Provider (WISP) como el que se pretende abordar en este proyecto y entre los que destacamos:

- Los mecanismos de autenticación y cifrado.

- La gestión del ancho de banda asignado a cada usuario.
- La gestión del balanceo de carga
- La configuración de las reglas para el firewall de la red
- La configuración de las reglas para mantener una adecuada calidad de servicio.
- El seguimiento de los abonados (tipos de usuario, perfiles de uso, sistemas de facturación, etc.)

Este fabricante proporciona una solución que cuesta 10 veces menos que la que aportan sus competidores y que es muy empleada en situaciones en las que los recursos son muy limitados, siendo el proyecto guifi.net (<http://guifi.net>) el mejor ejemplo de su desarrollo, pues es donde ha encontrado numerosos adeptos que se han encargado de poner a prueba estas infraestructuras de bajo coste con buenos resultados hasta el momento. La enorme comunidad que apoya este tipo de dispositivos es otra ventaja fundamental.

Para las unidades de subscritor hemos optado por dispositivos de **Ubiquiti**, concretamente las **NanoStation 5**, acompañadas de un router neutro que permita distribuir la señal en el domicilio del cliente.

En la elección de frecuencias se ha optado por emplear la banda de 5 Ghz, ya que la banda de 2,4 Ghz suele estar mucho más saturada, lo que iba a afectar a la calidad de servicio. Por este motivo, los fabricantes, como Samsung, Lg o Apple entre otros, están incorporando la doble banda a sus dispositivos para tener la opción de conectar de forma nativa a ambas bandas de frecuencia. En cualquier caso, los equipos que se usaran como CPE para conectar con la estación base pueden conectarse simultáneamente a un equipo similar que trabaja en la banda de 2,4Ghz (**NanoStation 2**), permitiendo un punto de acceso a doble banda.

Estimaciones económicas

Los equipos que presentan los mayores costes son los que emplean la tecnología WIMAX por lo que hemos tratado de dar prioridad a los equipos Wi-Fi cuando fuese posible. Aun así se va a necesitar una estación base Alvarion BreezeMAX Extreme 5000 y un CPE para conectarlo a dicha base. Los equipos WiFi que se van a usar son de fabricantes que destacan por un buen rendimiento y bajo coste, como son Mikrotik y Ubiquiti.

La gestión de la red y la seguridad de la misma se confían también a equipos Mikrotik, que además cuenta con buen soporte técnico y una amplia comunidad de usuarios que mantienen los equipos actualizados.

Para el montaje de los equipos serán necesarias diversas estructuras, además de cableado y conectores.

El presupuesto que manejamos será el siguiente

Ítem	Concepto	Unidades	Precio Unitario	Importe
1	Estación Base Alvarion BreezeMax Extreme 5000	1	4500	4500
2	Estación subscriptora Alvarion BreezeMax Extreme PRO 5000	1	500	550
3	BASEBOX 5 (RB912UAG-5HPnD-OUT)	3	50,64	151,92
4	Antena AIRMAX AM-5G16-120 5GHz	3	47,60	142,8
5	Router RB1100AHx2	1	289,25	289,25
6	PC de sobremesa	1	700	700
7	Unidades de alimentación (PoE)	3	10,92	32,76
8	Cableado y conectores	1	500	500
9	Mástiles y elementos de sujeción	1	1000	1000
10	Mano de obra	1	2500	2.500
11	Cuota de instalación STI	1	10700	10700
12	Proyecto	1	2000	2000
	Subtotal			23066,73
	IVA			4844,02
	Total			27910,75

Por tanto tendremos unos gastos de instalación y puesta en marcha de 27910,75 euros a los que tendremos que sumar la cuota mensual del STI y los gastos asociados al mantenimiento de la infraestructura.

Para los gastos iniciales de puesta en marcha, hemos supuesto un periodo de amortización de 10 años, por lo que tenemos una cuota mensual por el total de los gastos de 232,59 euros al mes y al añadir la cuota mensual del STI de 4442 euros, hacen un total de **4674,59 euros al mes**.

Para que los 247 hogares del servicio Premium puedan soportar el coste total de la red, la cuota de servicio debe ser al menos de 18,925 euros al mes, por lo que se establece una **cuota inicial de 25 euros**, que permita cubrir los gastos de mantenimiento de la red.

En esta cuota no se incluyen los gastos derivados de la instalación en el domicilio del cliente ni de la adquisición de los equipos que se instalarán en el mismo. Estos equipos se le cederían en régimen de alquiler, pero con la obligación de devolverlos si diese de baja el servicio.

Como una fuente adicional de ingresos se puede establecer un servicio de publicidad a través de la página de inicio desde la que los usuarios del portal cautivo introducen el usuario y contraseña antes

de poder navegar. Las empresas interesadas pueden contratar un espacio publicitario en dicha página a cambio de contribuir al mantenimiento de la red.

Segunda parte: análisis del proyecto

Necesidades de ancho de banda previstas

Para el estudio de la carga de red nos vamos a basar en la información proporcionada por el Instituto Nacional de Estadística (INE), de donde obtendremos datos de la población del municipio como del equipamiento y uso de tecnologías de la Información y comunicación en los hogares.

Los datos que hemos obtenido nos indican que la población del municipio, para el año 2012, era de **5.627 habitantes**. Las encuestas indican que un 57% de los residentes en municipios de menos de 10.000 habitantes usaron Internet en algún momento en los últimos 3 meses, y que de ellos, el 69.7% lo usan diariamente (al menos 5 días por semana). Por otra parte, son las personas jóvenes los usuarios más habituales del servicio, uso que va disminuyendo según aumenta la edad.

Podemos suponer que el 57% de la población de Casariche es un usuario potencial de Internet. Al disponer de 2 tipos de servicio, uno gratuito y otro de pago estimamos que el primero tendrá mayor aceptación y por tanto más usuarios potenciales. Para el servicio gratuito estimamos una cuota de mercado del 80% de los usuarios potenciales, mientras que para el segundo estimaremos una cuota de mercado del 20%.

Podríamos resumir los usuarios potenciales que esperamos tener en la siguiente tabla:

Población total	5627
Usuarios de Internet	3208
Usuarios potenciales del servicio gratuito	2566
Usuarios potenciales del servicio Premium	641,6

Tabla: Población total y usuarios potenciales del servicio

El INE también aporta información de interés a la hora de establecer qué tipos de servicios son los más empleados por los usuarios de Internet, lo cual nos va a permitir saber qué ancho de banda van a necesitar para poder cubrir sus necesidades.

Servicios de comunicación y acceso a la información	
Recibir o enviar correo electrónico	85.5
Telefonar a través de Internet ó vídeo llamadas (vía webcam) a través de Internet	28.8
Envío de mensajes a chats, redes sociales, blogs, grupos de noticias o foros de discusión online, uso de mensajería instantánea	58.9
Leer o descargar noticias, periódicos o revistas de actualidad online	74.7
Buscar información sobre bienes y servicios	86.5
Servicios relacionados con el entretenimiento y la creatividad	
Escuchar la radio o ver TV emitidas por Internet	48.8
Jugar o descargar juegos, imágenes, películas ó música	47.8
Colgar contenidos propios (texto, fotos, música, videos, software, etc.) en una página Web para ser compartidos	45.3
Crear páginas Web o blogs	10.9
Otros servicios	
Concertar una cita con un médico a través de una página Web (de un hospital ó de un centro de salud, p.ej.)	26.5
Utilizar servicios relacionados con viajes y alojamiento	52.8
Vender bienes o servicios (venta directa, mediante subastas, etc.)	11.4
Banca electrónica	40.6

Tabla: Porcentaje de usuarios que acceden a diferentes servicios

En cuanto a los requisitos de ancho de banda de los servicios ofrecidos mediante la conexión de datos, podemos establecer como requisitos mínimos y deseables los que aparecen en la siguiente tabla:

	Capacidad	
	Mínima	Deseable
Email	4 Kbps	20 Kbps
Navegación WEB	64 Kbps	1,5 Mbps
VOIP	20 Kbps	256 Kbps
Videoconferencia	128 Kbps	768 Kbps
Transferencia de archivos	10 Kbps	600 Kbps
Streaming Video H.264 a 320x180	15 Kbps	250 Kbps
Streaming Video H.264/RTVideo a 1280x720	700 Kbps	2,5 Mbps

Tabla: ancho de banda requerido por diferentes servicios

Podemos decir por lo tanto que salvo el uso de contenido multimedia, la mayor parte de los servicios que necesitan los usuarios no suponen un ancho de banda especialmente importante, y podría verse totalmente cubierto con una velocidad de conexión de 1 MB por usuario en el servicio Premium, e incluso para la mayoría de los servicios con un acceso gratuito de 256 kbps.

Usuarios potenciales del servicio gratuito

Para el servicio gratuito, limitado a **256 kbps** partimos de un total de 2566 usuarios potenciales y asumimos que ni todos se van a conectar a la vez, ni todos van a usar la totalidad del ancho de banda disponible para acceder a Internet, por lo que introduciremos factores de corrección al calcular el número de usuarios simultáneamente conectados así como el uso del ancho de banda disponible. Hemos considerado que este servicio, a pesar de ser gratuito, no va a ser utilizado por el 100% de los usuarios de Internet ya que muchos de ellos podrían disponer de terminales que ya dispongan de acceso a Internet a mayor velocidad como tarifas de datos móviles, Modem USB, etc., o tener contratado el servicio Premium o alguna conexión a Internet en su hogar con tasas de transferencia superiores a los 256 kbps que este servicio proporciona, por lo que es probable que usen dichas conexiones para acceder a Internet en lugar de emplear la conexión gratuita a pesar de tenerla disponible. Establecemos como factor de corrección un 9,5% del total de usuarios potenciales, por lo que asumimos que el número máximo de usuarios que estarán utilizando el servicio de acceso a Internet gratuito al mismo tiempo será de 243,77 usuarios.

Usuarios potenciales del servicio gratuito * factor de corrección = usuarios simultáneos máximos

$2566 * 0.095 = 243,77 \approx 244$ usuarios.

Basándonos en el uso de los diferentes servicios y el ancho de banda que éstos necesitan, podemos ver que los servicios más utilizados no requieren un ancho de banda importante, y que pueden cubrirse con una tasa entre 56 y 128 kbps, por lo tanto asumiremos que los usuarios conectados estarán consumiendo en promedio un 25% del ancho de banda disponible, por tanto el ancho de banda total necesario para proveer del servicio será:

$244 \text{ usuarios} * 256 \text{ kbps} * 0,25 = 15616 \text{ kbps} = 15,616 \text{ Mbps}$

Necesitaremos un mínimo de **15,62 Mbps** para poder proveer del servicio de acceso a Internet gratuito para la población de Casariche.

Usuarios potenciales del servicio Premium

Para el acceso Premium, realizaremos un razonamiento similar partiendo de esos mismos 3208 usuarios potenciales. Hemos supuesto que podríamos acceder a una cuota de mercado del 20% ofreciendo un servicio de 1 Mbps. Si suponemos que cada hogar conectado tenga una media de 2,6 miembros, podemos calcular el número de usuarios del sistema la capacidad total necesaria como:

$(3208 \text{ clientes potenciales} / 2,6 \text{ miembros por hogar}) * 0.2 = 246,76 \approx 247$ hogares

Por tanto, para dotar del servicio Premium, con una velocidad de 2 Mbps a los 247 hogares necesitaríamos 494 Mbps, sin embargo, como ni van a estar todos conectados al mismo tiempo ni van a estar usando el 100% del ancho de banda en todo momento, introduciremos factores de corrección, asumiendo una carga de red máxima del 25% del total, por lo que estimamos que **necesitaríamos 123,5 Mbps** para poder dar un servicio adecuado a esos 247 hogares.

Con los datos aportados por el INE y las estimaciones realizadas pensamos que el ancho de banda necesario para satisfacer las necesidades de todos los usuarios de la red quedará establecido en **15,62 Mbps** para el servicio de acceso gratuito y **123,5 Mbps** para el servicio Premium, por tanto debemos contratar como mínimo **140 Mbps** para poder proveer del servicio de acceso a Internet.

Estimaciones del coste del ancho de banda necesario.

Para la contratación de 140 Mbps tenemos disponibles varias alternativas. La primera, por ser el operador de referencia a nivel nacional es Movistar. Para la contratación de este tipo de líneas esta compañía dispone de *Servicios para Operadores Nacionales* entre los que se encuentra el *Servicio de transporte interprovincial*, pensado para organizaciones que necesiten una conexión que puedan revender a sus abonados.

Movistar nos ofrece 3 tipos de circuitos que podremos combinar: circuitos de 2 Mbps, de 34 Mbps o de 155 Mbps. En nuestro proyecto sería suficiente con un circuito de 155 Mbps, la cual supondría un coste de instalación de **10700 €** y una cuota mensual de **4442 €**. Además este circuito nos permitiría afrontar ampliaciones en el futuro.

Descripción del sistema WiMAX

WiMAX, siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas), es una norma de transmisión de datos, basada en el estándar **IEEE 802.16**, que utiliza las ondas de radio en las frecuencias de 2,3 a 3,5 GHz y puede tener una cobertura de hasta 60 Km. ofreciendo velocidades similares o incluso superiores a las ofrecidas por el ADSL. Dentro de esta tecnología, también existe equipamiento que utiliza la frecuencia libre de licencia a 5,4 GHz, aunque es un equipo no estándar y no se garantiza la interoperabilidad entre distintos fabricantes.

Es una tecnología dentro de las conocidas como tecnologías de última milla y ofrece una solución adecuada para dar servicios de banda ancha en zonas donde el despliegue de redes de cobre o fibra óptica presenta unos costes demasiado elevados, como ocurre por ejemplo en algunas zonas rurales.

Actualmente se recogen dos variantes dentro del estándar 802.16:

- Uno de **acceso fijo** (802.16d), en el que se establece un enlace radio entre la estación base y un equipo de usuario situado en el domicilio del usuario. Para el entorno fijo, las velocidades teóricas máximas que se pueden obtener son de 70 Mbps. Es el único disponible en la banda libre.
- Otro de **movilidad completa** (802.16e), que permite el desplazamiento del usuario de un modo similar al que se puede dar en las redes GSM/UMTS.

Características principales de WiMAX

- Distancias de hasta 60 kilómetros.
- Velocidades de más de 70 Mbps
- Facilidades para añadir más canales.
- Anchos de banda configurables.
- Permite dividir el canal de comunicación en pequeñas subportadoras.
- Trabaja en banda libre
- Algoritmos para autenticación de usuarios y encriptación de datos. 3DES y RSA

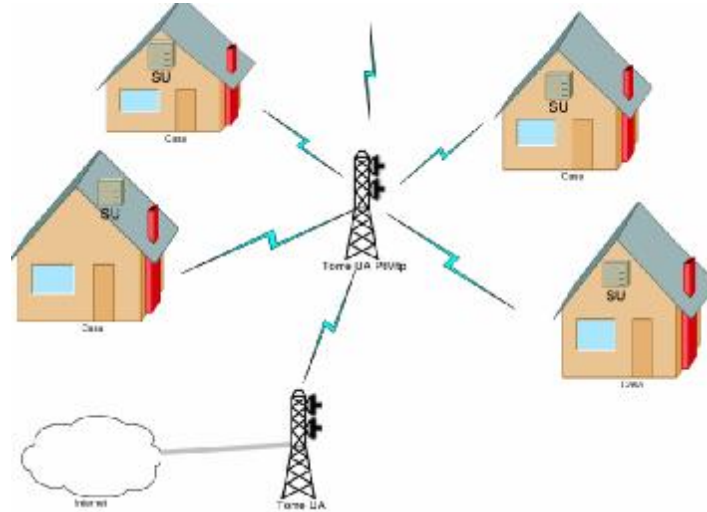
Aplicaciones principales

Aunque las primeras versiones de WiMax estaban pensadas como accesos fijos para ofrecer conectividad mediante radioenlaces punto a punto o punto a multipunto que permitieran conexiones de alta velocidad sin necesidad de realizar los costosos despliegues que requieren las redes cableadas, con el tiempo se ha ido desarrollando la tecnología hasta poder ofrecer soluciones en movilidad.

WiMax es un recurso muy apropiado para llevar Internet a zonas rurales, así como para interconectar edificios a grandes distancias de una forma rápida, sencilla y económica.

Interconexión de dispositivos

Una red metropolitana basada en esta tecnología va a estar formada por al menos una estación base (BS), también llamada unidad de acceso (UA), que será la que se conecte al backbone del proveedor y desde la que se van a crear las celdas de la red. Cada una de estas celdas tendrá uno o varios terminales de abonado (CPE) también llamados unidad de suscriptor (SU).



Esquema de conexión mediante WiMax

La **estación base**, también conocida como **unidad de acceso (AU)**, estará formada por tres subsistemas diferentes:



Figura: unidad de acceso (AU)

- **Unidad interior (IDU):** podrá ser autónoma o en rack y normalmente se conecta a la red mediante un interfaz Ethernet 10/100 BaseT con conectores RJ-45, y a la unidad exterior (ODU) mediante un cable CAT-5.
- **Unidad exterior (ODU):** Convierte la señal IP en inalámbrica. Se conecta a la IDU mediante un conector RJ-45 y a la antena mediante un conector RF
- **Antena:** Varios ángulos, 60°, 120°, 360° etc.

Las **unidades de abonado (SU)**, también incluyen tres elementos diferentes:



- **Unidad interior (IDU)**
- **Unidad exterior (ODU)**
- **Antena.**

Figura: unidad de abonado
(SU)

Descripción del sistema WiFi

WiFi es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Se creó en 1997 para proporcionar acceso inalámbrico a las redes de área local. El estándar en el que se basa es el 802.11 y se centra en las 2 capas inferiores del modelo OSI, la capa física y de enlace. Los dispositivos habilitados con esta tecnología pueden conectarse a Internet a través de un punto de acceso de red inalámbrica (hotspot) y ofrecen total compatibilidad con las redes cableadas basadas en las norma 802.3 (Ethernet).



Logotipo de WiFi

El alcance de este sistema de interconexión es de unos 20 metros en interiores, pudiendo llegar hasta los 300 metros al aire libre si las condiciones son óptimas. Para cubrir áreas mayores se pueden superponer múltiples puntos de acceso.

WiFi es una marca comercial de la WiFi Alliance, una organización formada por varias empresas de telecomunicaciones, como Nokia, 3com, o Lucent que se encarga de aprobar y certificar que los equipos cumplan la norma IEEE 802.11, garantizando de esta forma la compatibilidad entre equipos aunque pertenezcan a diferentes fabricantes. Para que un equipo pueda incluir el logotipo WiFi debe estar certificado por la WiFi Alliance.

Existen diversos tipos de WiFi, basado cada uno de ellos en un estándar IEEE 802.11 aprobado. La siguiente figura resume las principales extensiones de la familia 802.11

Normas (Capa física y de acceso al medio)	Velocidad de transmisión máxima	Throughput máximo típico	Número máximo de redes localizadas	Banda de frecuencia	Radio de cobertura típico (interior)	Radio de cobertura típico (exterior)
IEEE 802.11a/h	54 Mbps	22 Mbps	14 (5.7 GHz)	5 GHz	85 m.	185 m.
IEEE 802.11b	11 Mbps	6 Mbps	3	2.4 GHz	50 m.	140 m.
IEEE 802.11g	54 Mbps	22 Mbps	3	2.4 GHz	65 m.	150 m.
IEEE 802.11n (40MHz)	54 Mbps	22 Mbps	1 (2.4 GHz) 7 (5.7 GHz)	5 GHz	120 m.	300 m.
IEEE 802.11n (20MHz)	54 Mbps	22 Mbps	3 (2.4 GHz) 14 (5.7 GHz)	2.4 GHz y 5 GHz	120 m.	300 m.

Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutaron de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps, 54 Mbps y 300 Mbps, respectivamente, razón por la cual son las versiones más populares.

En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz, recientemente habilitada, la cual permite una comunicación más limpia al no existir otras tecnologías que la usen aunque su alcance es algo menor.

Seguridad

El éxito que ha tenido esta tecnología ha propiciado que haya una gran cantidad de redes disponibles, muchas de las cuales están abiertas o disponen de claves poco seguras. Con el tiempo se han ido desarrollando herramientas capaces de romper la seguridad en estas redes de forma casi instantánea, ya sea rompiendo la clave por fuerza bruta o empleando diccionarios y algoritmos capaces de determinar las claves por defecto del equipo. Esta situación ha obligado a tener algunas precauciones para aumentar la seguridad de estas redes y los dispositivos conectados a ellas, por ejemplo:

- Modificar el SSID que viene predeterminado.

- Utilización de cifrado WPA2 en lugar de cifrado WEP

- Uso de contraseñas seguras

- Cambios frecuentes de la contraseña de acceso a los equipos

- Establecer un filtrado de dispositivos autorizados mediante la MAC

Tipos de dispositivos

Podemos dividir los tipos de dispositivos en dos grupos: Dispositivos de Distribución, cuya función es la de establecer una zona de cobertura de red y Dispositivos Terminales cuya función es la de permitir la conexión de un dispositivo a la red.

Dispositivos de Distribución o Red:

Los puntos de acceso son dispositivos que crean una "Red WiFi" a la que se pueden conectar otros dispositivos. Van a permitir conectar dispositivos de forma inalámbrica a una red existente. Pueden agregarse más puntos de acceso a una red existente para aumentar la cobertura de la misma

Los repetidores inalámbricos son equipos que se utilizan para extender la cobertura de una red inalámbrica, éstos se conectan a una red existente que tiene señal más débil y crea una señal limpia a la que se puede conectar los equipos dentro de su alcance. Algunos de ellos funcionan también como punto de acceso.

Los routers inalámbricos son dispositivos que van a permitir interconectar varias redes. Por ejemplo van a permitir tomar la conexión a Internet por un lado y la red de área local por otro y conectarlas, de forma que los dispositivos que pertenecen a la red local puedan acceder a Internet.

Los dispositivos terminales abarcan tres tipos mayoritarios: tarjetas PCI, tarjetas PCMCIA y tarjetas USB, aunque hoy en día la mayor parte de los dispositivos diseñados para acceder a redes WiFi ya tienen la tarjeta de red integrada, por lo que algunos de estos dispositivos están cayendo en desuso.

Ventajas y desventajas

Las principales ventajas de las redes WiFi destacan:

- Comodidad y sencillez.
- Escalabilidad.
- Compatibilidad de dispositivos a nivel global garantizada por la WiFi Alliance.

Entre los principales inconvenientes tenemos:

- Menor velocidad en comparación a una conexión cableada.
- Debido a su amplia difusión pueden producirse muchas interferencias que afecten negativamente a la calidad de las conexiones.
- Menor seguridad. Las comunicaciones son fácilmente interceptables y ofrecen menos posibilidades de control que las redes cableadas.

Planificación

Para el desarrollo de la red se han identificado las siguientes tareas, estableciendo una primera estimación de los tiempos necesarios para su realización

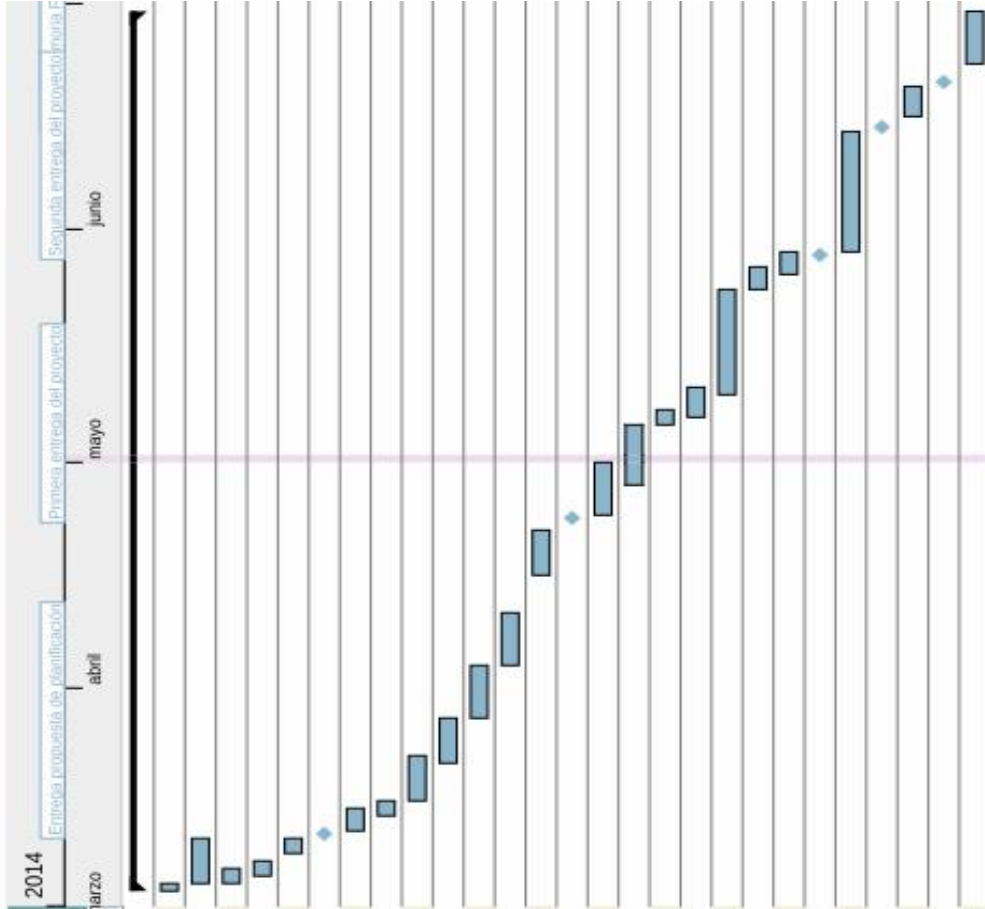
Lista de tareas a realizar y diagrama de Gantt

Nombre	Fecha de inicio	Fecha de fin
TFC Integracion de redes telematicas	5/03/14	29/06/14
Argumentacion eleccion TFC	5/03/14	5/03/14
Fase de Estudio	6/03/14	11/03/14
Descripcion y objetivos	6/03/14	7/03/14
Aspectos legales y técnicos	7/03/14	8/03/14
Planificacion inicial	10/03/14	11/03/14
Entrega propuesta de planificación	12/03/14	11/03/14
Analisis sistema Wimax	13/03/14	15/03/14
Analisis sistema WiFi	15/03/14	16/03/14
Estudio de las necesidades de la red	17/03/14	22/03/14
Analisis para implantación del equipo	22/03/14	27/03/14
Estudio de las zonas de cobertura	28/03/14	3/04/14
Estudio inicial alternativas de configuracion	4/04/14	10/04/14
Elaboración materiales para la primera entrega del proyecto	16/04/14	21/04/14
Primera entrega del proyecto	23/04/14	22/04/14
Diseño inicial de la red	24/04/14	30/04/14
Calculo de coberturas	28/04/14	5/05/14
Decision final del equipamiento a emplear	6/05/14	7/05/14
Políticas de seguridad y QoS	7/05/14	10/05/14
Diseño final de la red y configuracion de equipos	10/05/14	23/05/14
Presupuesto final	24/05/14	26/05/14
Elaboracion de materiales para la segunda entrega del proyecto	26/05/14	28/05/14
Segunda entrega del proyecto	28/05/14	27/05/14
Elaboración Memoria Final	29/05/14	13/06/14
Entrega Memoria Final	14/06/14	13/06/14
Elaboración de la presentación	16/06/14	19/06/14
Entrega de la presentación	20/06/14	19/06/14
Preguntas del tribunal	23/06/14	29/06/14

Diagrama de Gantt



Nombre

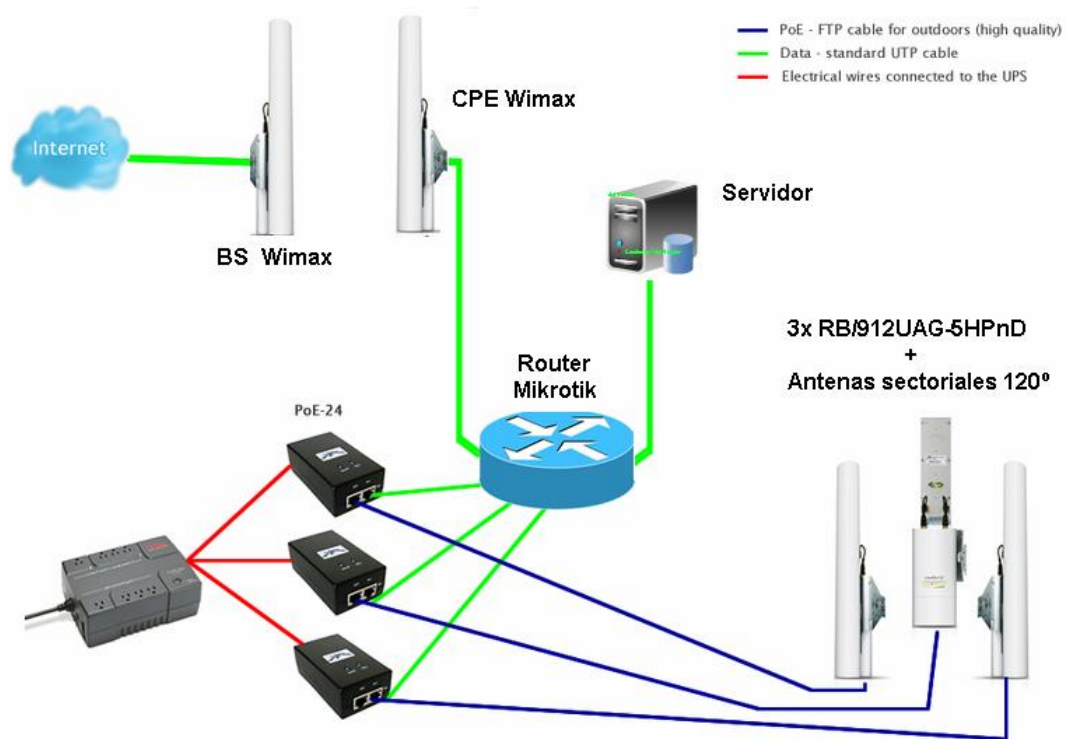


Infraestructura de red

Como proveedor de servicio se ha utilizado al operador de referencia, Movistar, a pesar de ofrecer precios por encima de los de la competencia, ya que ofrece también mayores garantías.

Se va a instalar un único nodo primario Wimax, formado por una estación base BreezeMAX Extreme 5000, del fabricante Alvarion, que permite el transporte a distancias de hasta 50km. En nuestro caso el CPE que se va a conectar a dicha estación no estará a más de 5 Km. de distancia, y además dispone de visibilidad directa, por lo que se va a poder garantizar un enlace estable.

Para la distribución en las zonas publicas montaremos una estación base WiFi, formada por un router RB1100AHx2 que se va a encargar de administrar las direcciones IP, gestionar el ancho de banda, la calidad de servicio, etc., y al que se van a conectar las routerboard **Mikrotik RB912UAG-5HPnD** a las que instalaremos 3 antenas sectoriales de 120° y 5Ghz. La razón de hacerlo de esta forma es que va a permitir dar servicio a muchos mas usuarios a un coste menor del que ofrecen las soluciones hibridas WIMAX-WIFI de Alvarion, ya que el coste de los dispositivos Mikrotik es mucho menor que el de sus equivalentes de otros fabricantes, como Cisco.



Este esquema permitirá montar una infraestructura a bajo coste sin por ello renunciar a un servicio de calidad para los usuarios de la red municipal.

Topología de la red

Inicialmente vamos a diferenciar dos servicios, uno gratuito que permite una velocidad de hasta 256kbps como máximo y otro de pago que permite una velocidad de 2 mbps. Para cada uno de ellos vamos a tener una red independiente, de manera que en el caso de necesitar realizar tareas de mantenimiento o control podamos tener bien diferenciados a cada tipo de cliente. Además crearemos otra red para direccionar los equipos de infraestructura, en la que se integraran los routers, servidores, puntos de acceso, etc.

Las direcciones que se van a asignar a las diferentes redes serán:

Red Infraestructura

Dirección de red: 192.168.1.0

Dirección de broadcast: 192.168.1.255

Rango de direcciones disponibles: 192.168.1.1 - 192.168.1.254

Red WiFi-Gratis

Dirección de red: 192.168.10.0

Dirección de broadcast: 192.168.10.255

Rango de direcciones disponibles: 192.168.10.5 - 192.168.10.254

Red WiFi-Premium

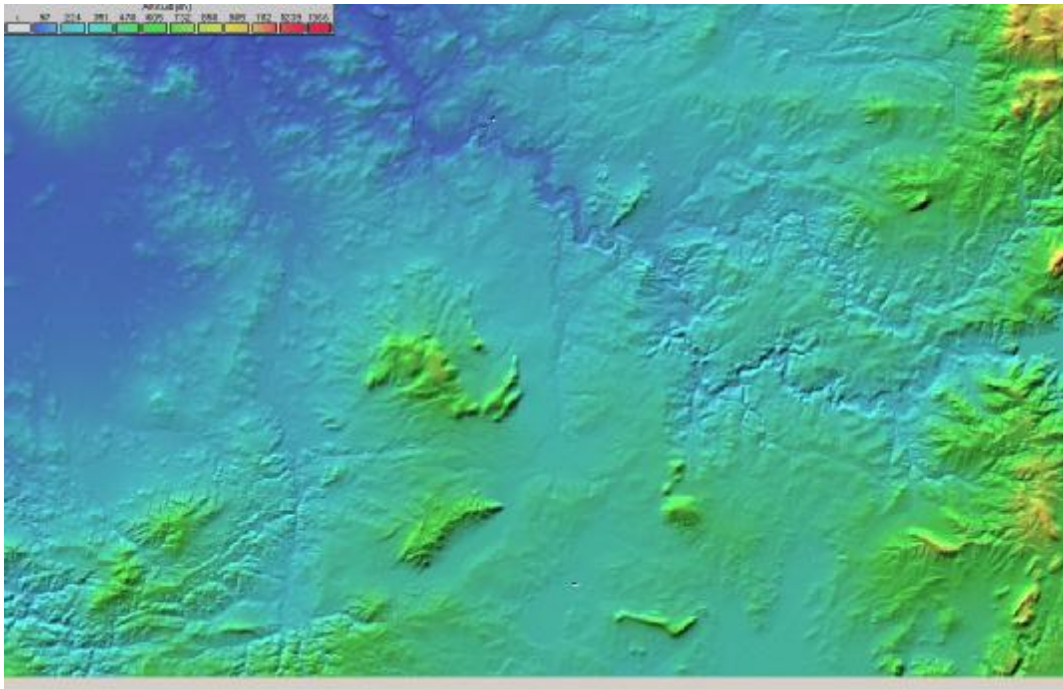
Dirección de red: 192.168.20.0

Dirección de broadcast: 192.168.20.255

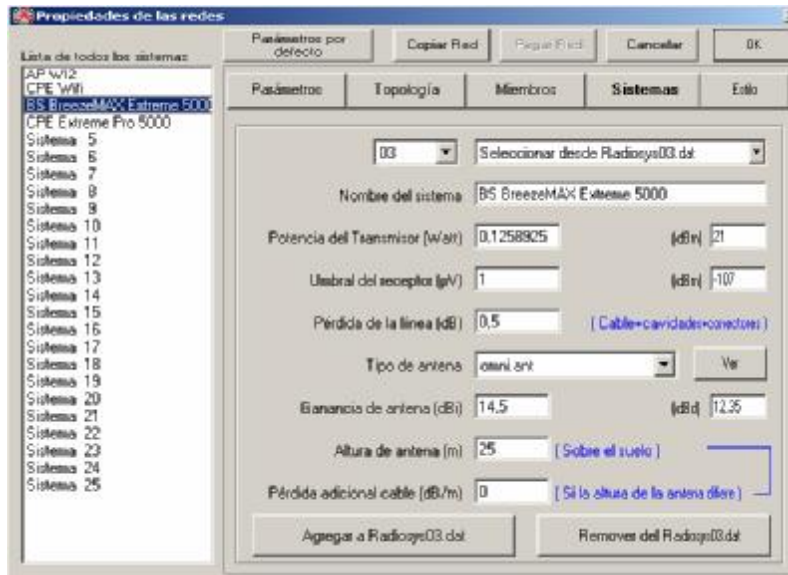
Rango de direcciones disponibles: 192.168.20.5 - 192.168.20.254

Estudio de la cobertura con Radio Mobile

Tras descargar la aplicación de la página oficial <http://www.cplus.org/rmw/english1.html> y descargar los datos relativos a las alturas, los cuales están disponibles en <http://dds.cr.usgs.gov/srtm/> hemos configurado el mapa de la zona en la que queremos realizar el despliegue.

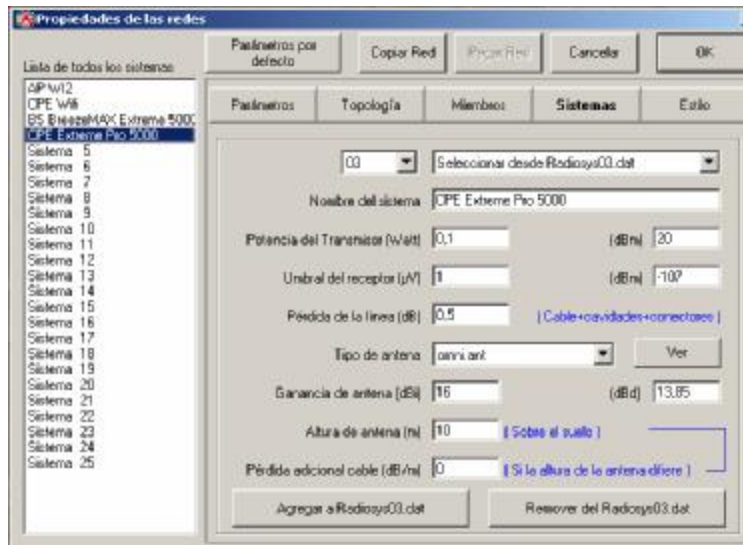


En nuestro estudio de la cobertura para la localidad de Casariche empezaremos valorando los resultados obtenidos para los radioenlaces utilizando una estación base Alvarion BreezeMAX Extreme 5000, que se va a configurar basándonos en la hoja de características del dispositivo que adjuntamos como documento en el anexo. La configuración se muestra en la figura:



Configuración estación base Alvarion BreezeMAX Extreme 5000

Nuestro sistema se basa en unidades Wi2 las cuales incluyen tanto un punto de acceso WiFi como una unidad subscriptora Wimax, BreezeMAX Extreme Pro 5000, que se montan en el mismo dispositivo. Para el estudio de cobertura del radioenlace Wimax se usan los siguientes parámetros:

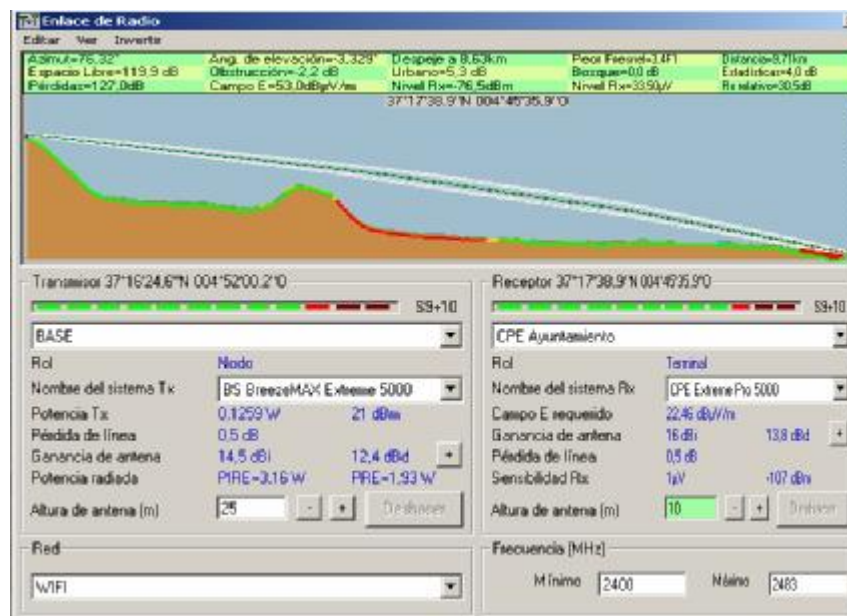


Configuración unidad de subscriber SU

Análisis de los radioenlaces Wimax

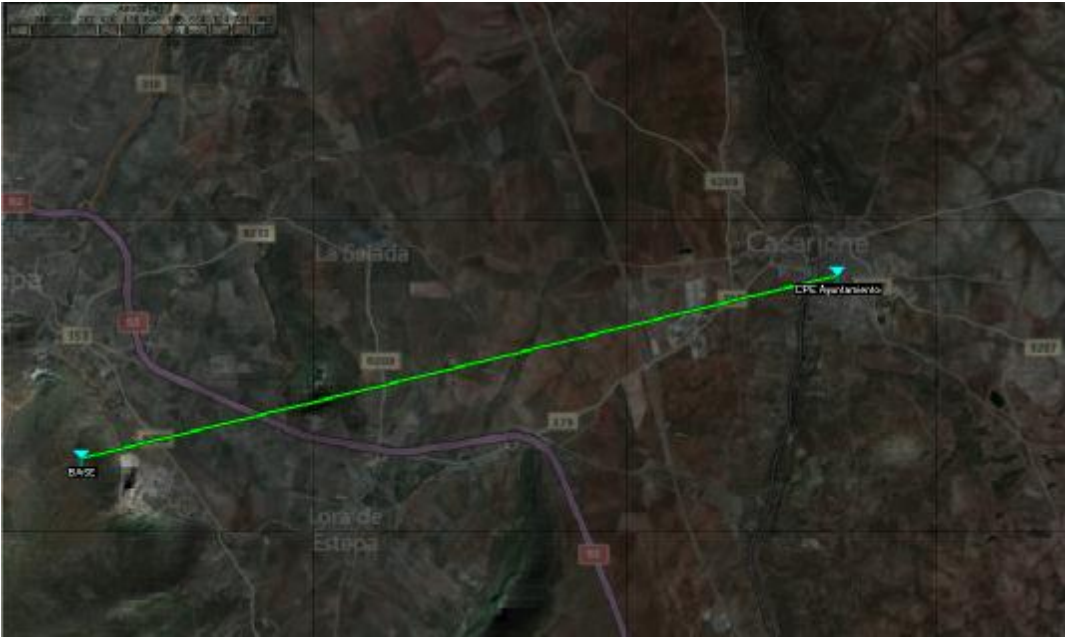
La estación base se va a situar en una localidad cercana, Estepa, donde ya existe la infraestructura necesaria para el despliegue., mientras que el CPE Wimax se va a conectar en el propio ayuntamiento, que es desde donde conectaremos nuestra estación base WiFi.

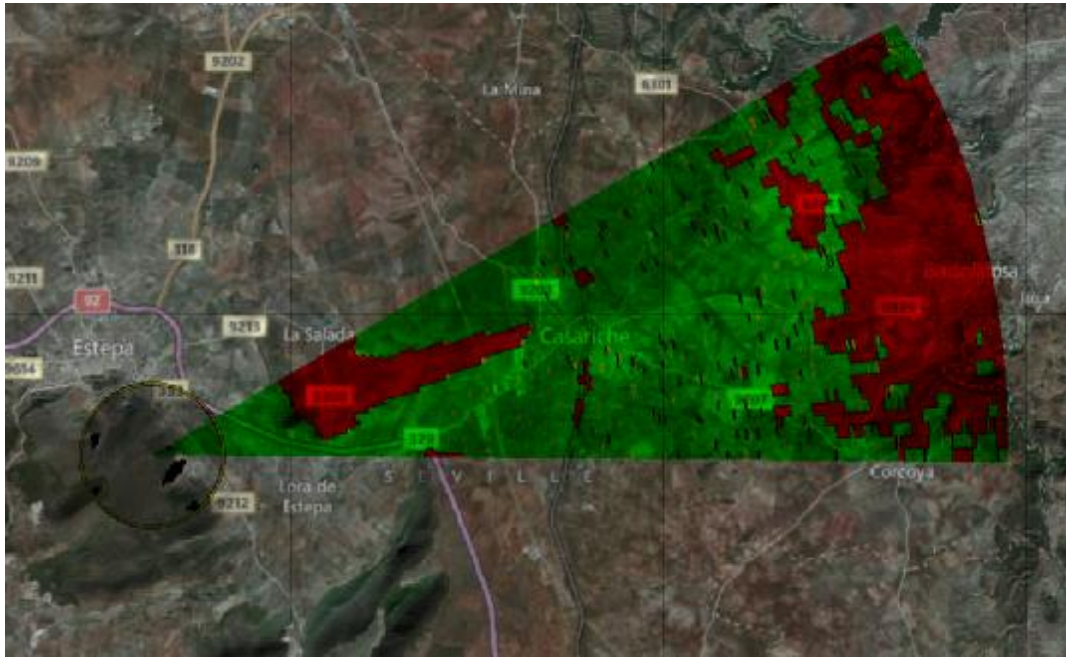
BS WIMAX - CPE Ayuntamiento



Los equipos emisor y receptor se encuentran a una distancia relativamente cercana entre ellos, además de contar con visibilidad directa y casi sin obstáculos, por lo que vamos a poder configurar

el enlace considerando la zona de Fresnel para que la cobertura sea optima, tal como se observa en la siguiente imagen.





Tercera Parte: Configuración de equipos

Configuración de router Mikrotik para la red municipal

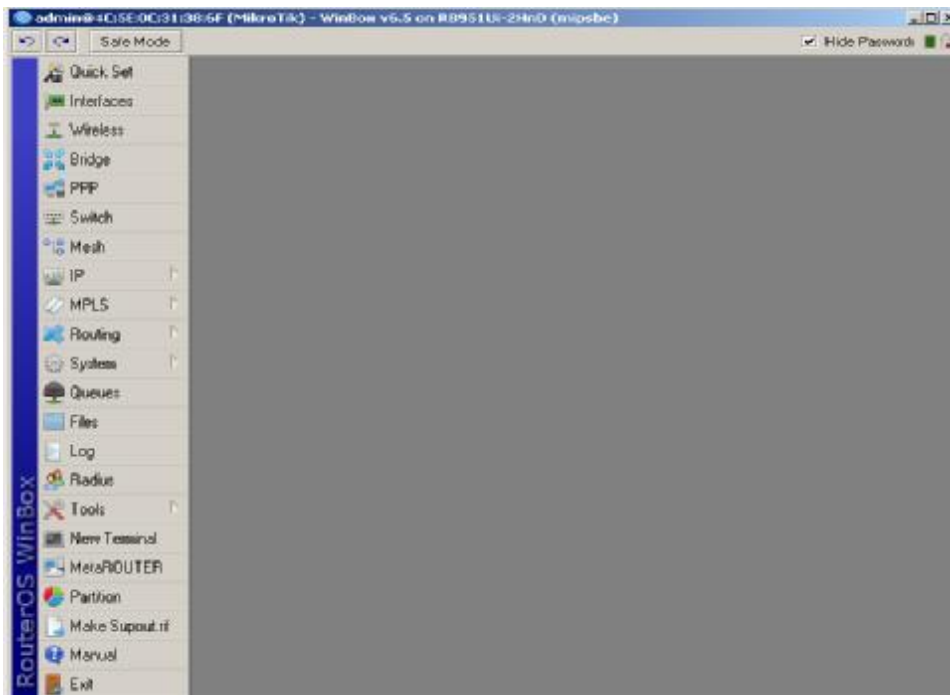
Para la gestión de la red emplearemos un router del fabricante Mikrotik, que proporciona suficiente potencia y versatilidad a bajo coste, el modelo RB1100AHx2



Configuraciones iniciales.

Para las configuraciones podemos emplear un navegador Web y acceder al dispositivo indicando en la barra de navegación la IP del mismo, aunque nosotros usaremos un programa específicamente diseñado para esta tarea (Winbox) que nos va a permitir realizar los cambios oportunos de una manera más cómoda.

Winbox dispone de un panel lateral desde el que se puede acceder a la mayoría de las opciones de configuración, aunque a veces deberemos realizar algunas tareas mediante línea de comandos desde un terminal.



Para eliminar la configuración por defecto del dispositivo abrimos un nuevo terminal desde **New Terminal** en el panel lateral y usamos el comando

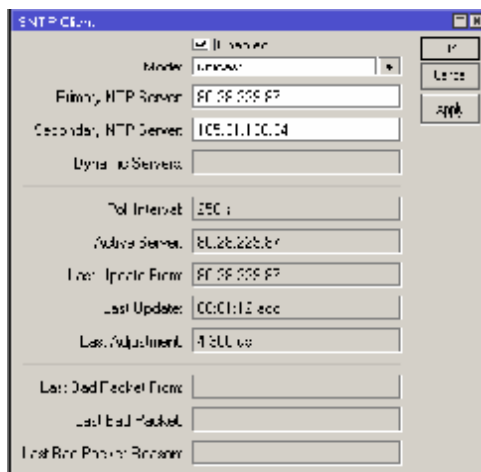
```
/system reset no-defaults=yes
```

Esto nos deja el equipo totalmente limpio, y a partir de aquí podremos configurarlo según nuestras necesidades.

Lo primero que haremos será configurar el reloj de sistema, de manera que cada evento que ocurra quede registrado con la hora correcta.

Para la configuración usamos un cliente NTP al que accedemos desde el panel lateral de Winbox, en la ruta **System -> SNTP Client**

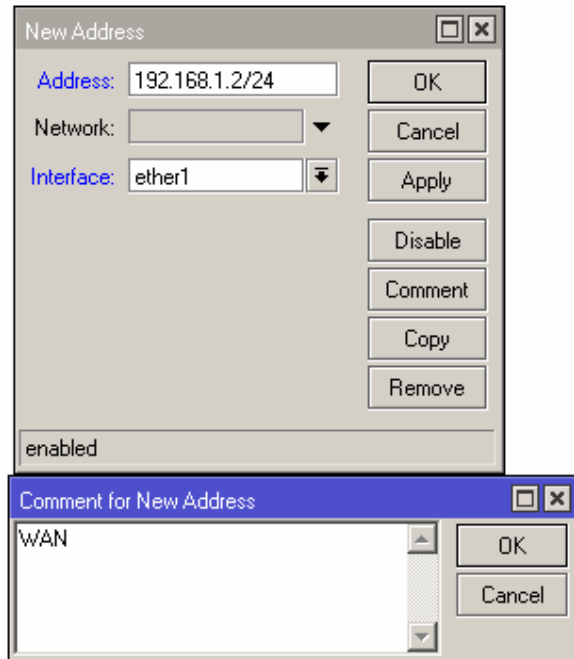
Marcaremos la casilla Enabled para activarlo indicando como servidor primario **es.pool.ntp.org** y como servidor secundario **europa.pool.ntp.org** y activando el modo unicast. Tras aplicar los cambios debe quedar algo así:



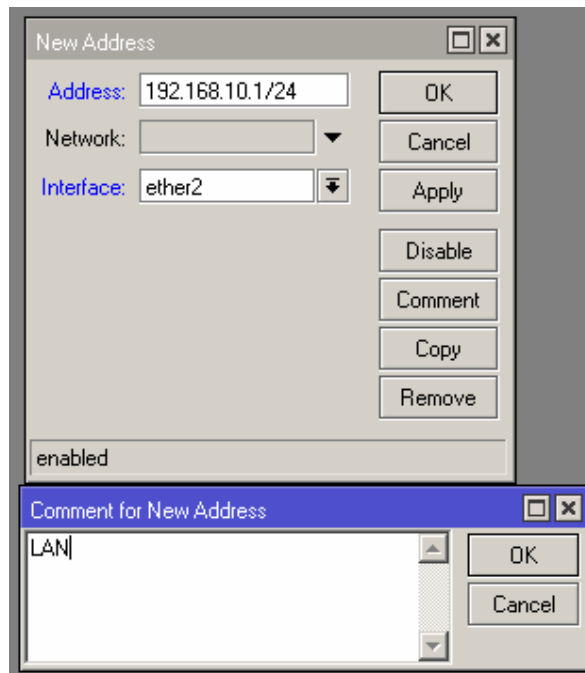
Configuración de nuestra red.

La IP del equipo desde el que obtenemos la conexión que vamos a distribuir estará en la IP 192.168.1.1 y a esta red 192.168.1.0 la llamaremos “WAN”, para distinguirla de la red local a la que se conectarán los clientes, la 192.168.10.0, y a la que llamaremos “LAN”. Cada red tendrá asignada una tarjeta de red (NIC) diferente en nuestro servidor, ether1 para la red WAN y ether2 para la red LAN.

Para la configuración de las redes accedemos desde el menú lateral de Winbox a **IP -> Addresses** y añadimos una nueva regla pulsando en el botón con el signo “+”, la configuración que definiremos es la que se ve en la imagen:



Tras aplicar los cambios, guardamos la configuración y pasamos a la siguiente interfaz de red, que definiremos como se muestra en la imagen:



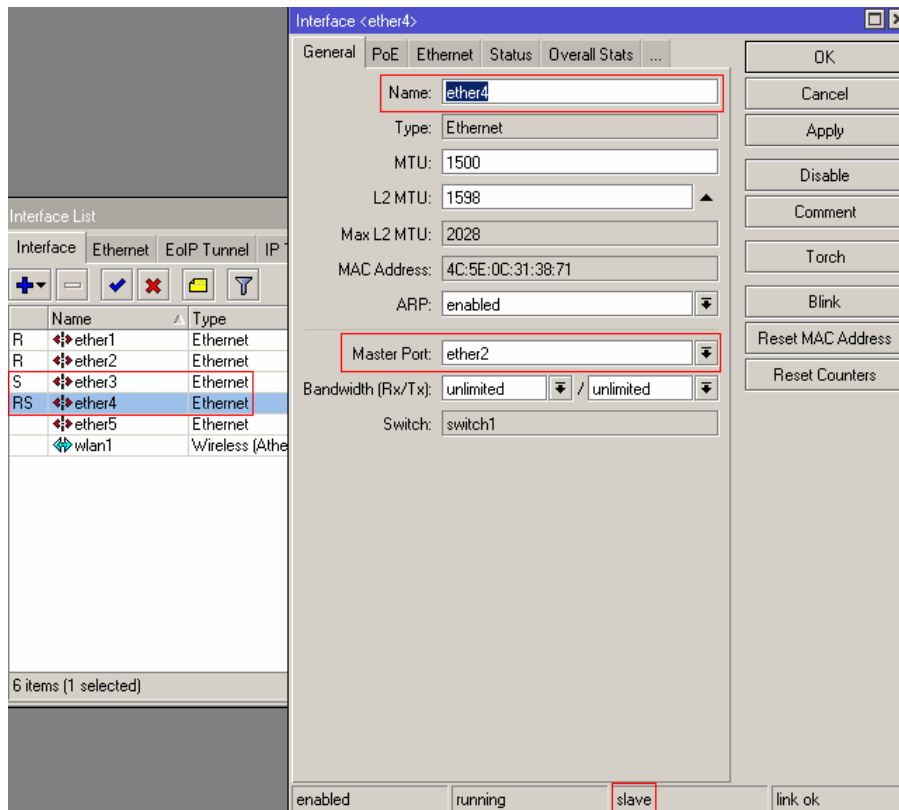
Tras aplicar y guardar los cambios ya tendremos ambas redes disponibles.

Para crear la red asignada al servicio Premium seguimos los mismos pasos, pero modificando la dirección para que se asigne a 192.168.20.0 en lugar de 192.168.10.0

Tras aplicar y guardar los cambios ya tendremos las redes disponibles.

Tras esta configuración básica, dejaremos a ether2 como maestro y al resto de puertos Ethernet del router los configuraremos como esclavos, de esta forma funcionan como un switch y permitan trabajar dentro de la misma red local. Esto se hace desde el menú lateral de Winbox, marcando Interfaces, y en el listado que aparece a continuación haciendo doble click en la interfaz que queramos modificar y seleccionando quien será el maestro en la opción "Master Port"

Podemos fijarnos en la lista de interfaces que aparecen marcadas con una S indicando "slave"



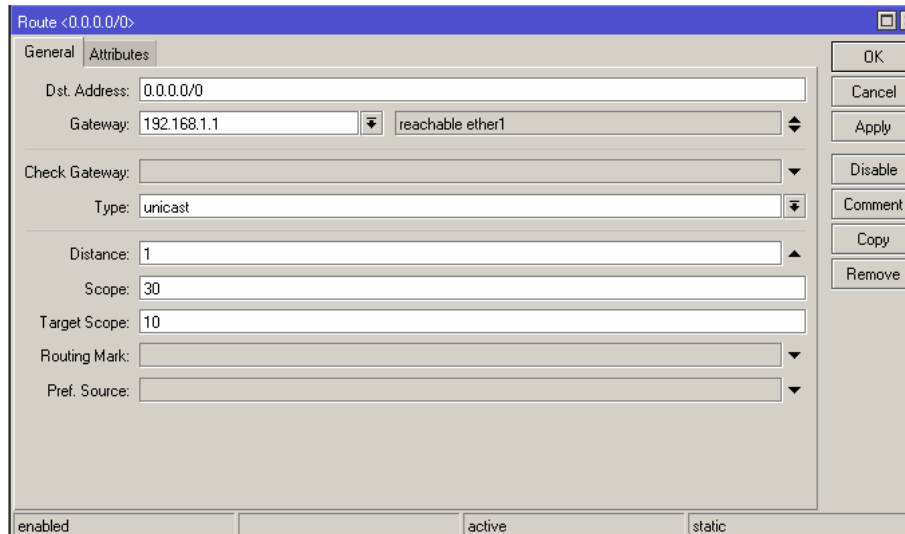
El siguiente paso sería el de enmascarar las direcciones para que podamos intercambiar los paquetes entre ambas interfaces. Lo haremos desde el menú lateral, siguiendo la ruta **IP -> Firewall -> NAT**, y creamos una nueva regla indicando:

Chain: srcnat

Out. Interface: ether1

Action: masquerade

Guardamos los cambios y ya sólo nos queda indicar cual será el gateway o puerta de enlace para enrutar los paquetes, opción que vamos a configurar accediendo desde el menú lateral a **IP -> Routes** y creando una nueva regla:

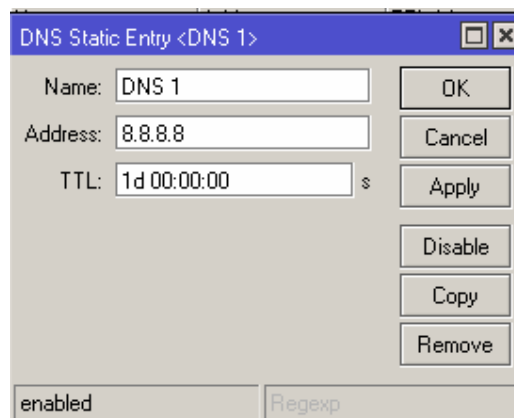


Con esto se completa la configuración básica del router, y sólo necesitaremos configurar las tarjetas de red en los equipos que se van a conectar a nuestra red LAN. Un aspecto a tener en cuenta en dicha configuración es que como servidor DNS indicaremos la IP del router, donde vamos a configurar un servicio de DNS cache.

Configurar DNS Cache

Los servidores DNS permiten realizar una traducción entre el nombre de un dominio, por ejemplo google.es y su dirección IP. La utilidad que nos brinda el DNS cache es que nos va a permitir almacenar en un registro las direcciones IP de las paginas Web que se han visitado recientemente, lo cual va a contribuir a agilizar la navegación en los clientes pues en lugar de tener que preguntar por dicha dirección para realizar la traducción, podremos almacenarla nosotros de manera local y disponer de ella inmediatamente cuando se requiera.

Desde el menú lateral vamos a **IP -> DNS** y pulsamos en el botón **Static**, donde crearemos una nueva regla pulsando sobre el botón con el signo + e indicaremos la IP y el nombre que asignamos a los servidores DNS que queramos usar.



Configuración de un servidor Web proxy (proxy-cache)

Un Web proxy nos va a permitir por un lado ahorrar ancho de banda y por otro servir las páginas de manera mas eficiente, mejorando aspectos como la velocidad, la seguridad, el control y el rendimiento.

Mikrotik nos permite configurar un Web proxy de forma local y transparente a los usuarios, y lo usaremos para proporcionar una cache que permita mejorar el tiempo de acceso para consultas similares por parte de los usuarios, de manera que cuando un usuario realiza una petición se le sirve el recurso que ha pedido y se almacena una copia. Cuando el mismo u otro usuario realice una petición similar, se pueda comprobar si dicho recurso se ha modificado respecto a la versión almacenada y si no ha sido así se le envía dicha versión sin necesidad de acceder de nuevo al recurso a través de la red. Si la versión almacenada es antigua o no hay ninguna, se descarga y se almacena para futuras peticiones.

Para crear nuestro servidor proxy accedemos desde el menú lateral a **IP -> Web Proxy** y establecemos una configuración como se muestra en la figura:

The image shows the 'Web Proxy Settings' dialog box with the following configuration:

- Enabled:**
- Src. Address:** [Empty]
- Port:** 8080
- Parent Proxy:** [Empty]
- Parent Proxy Port:** [Empty]
- Cache Administrator:** webmaster
- Max. Cache Size:** unlimited K*B*
- Max Cache Object Size:** 2048 K*B*
- Cache On Disk:**
- Max. Client Connections:** 600
- Max. Server Connections:** 600
- Max Fresh Time:** 3d 00:00:00
- Serialize Connections:**
- Always From Cache:**
- Cache Hit DSCP (TOS):** 4
- Cache Drive:** system

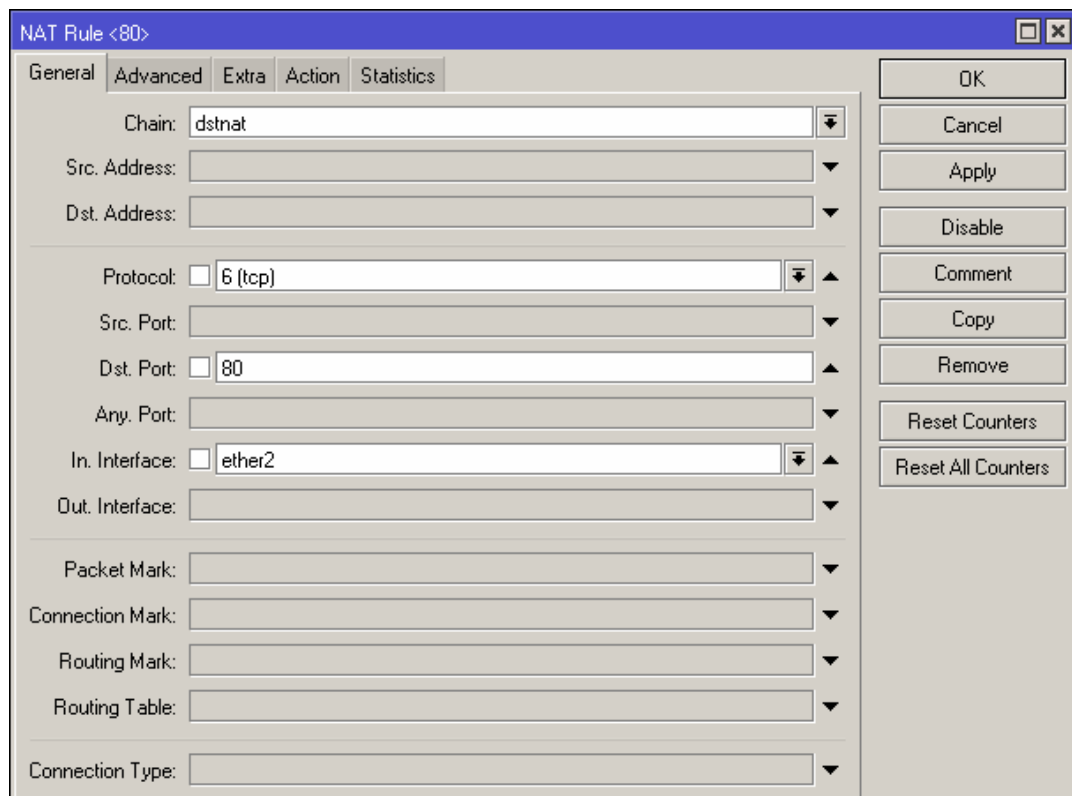
Buttons on the right: OK, Cancel, Apply, Clear Cache, Reset HTML, Access, Cache, Direct, Connections, Cache Contents.

Status bar: running

Una vez configurado pulsamos Apply y a continuación OK.

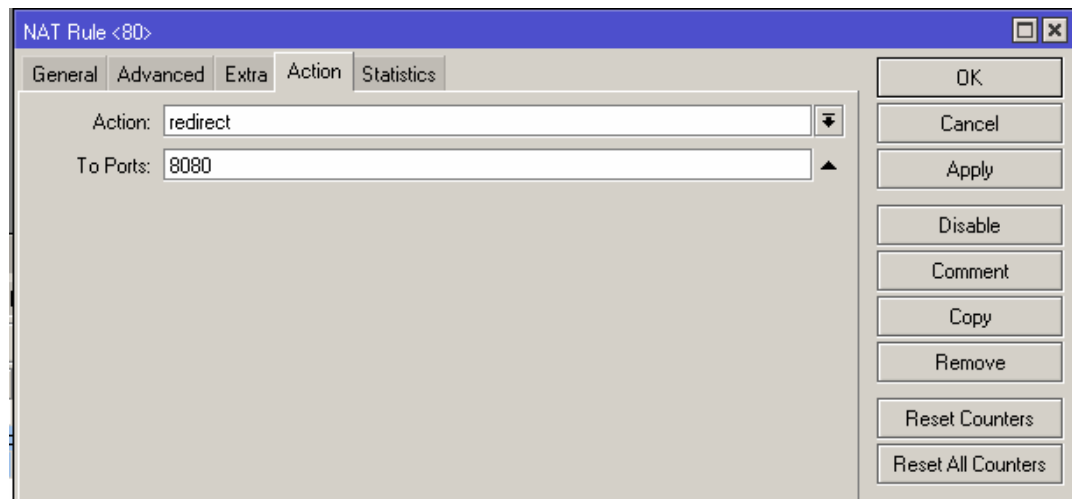
Después necesitaremos hacer una redirección del tráfico http que emplea el puerto 80 hacia el puerto 8080 asignado a nuestro proxy, para ello desde el menú lateral accedemos a **IP -> Firewall** y marcamos la pestaña NAT.

Aquí vamos a crear una regla como la que se muestra en la figura;



The screenshot shows the 'NAT Rule <80>' configuration window. The 'General' tab is active. The 'Chain' is set to 'dstnat'. The 'Src. Address' and 'Dst. Address' fields are empty. The 'Protocol' is set to '6 (tcp)'. The 'Src. Port' is empty, and the 'Dst. Port' is set to '80'. The 'Any. Port' is empty. The 'In. Interface' is set to 'ether2', and the 'Out. Interface' is empty. The 'Packet Mark', 'Connection Mark', 'Routing Mark', 'Routing Table', and 'Connection Type' fields are all empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'.

Y a continuación marcaremos la pestaña Action, donde seleccionamos como acción "redirect" y como puerto el 8080.



The screenshot shows the 'NAT Rule <80>' configuration window with the 'Action' tab selected. The 'Action' is set to 'redirect'. The 'To Ports' is set to '8080'. The other fields from the previous screenshot remain empty. The buttons on the right side are the same as in the previous screenshot.

Con esto ya tendríamos configurado nuestro proxy, aunque vamos a establecer una última configuración que nos va a permitir aumentar aun más la velocidad de navegación de los usuarios, especialmente cuando éstos tienen limitada la velocidad máxima disponible.

Configurando Full Caché

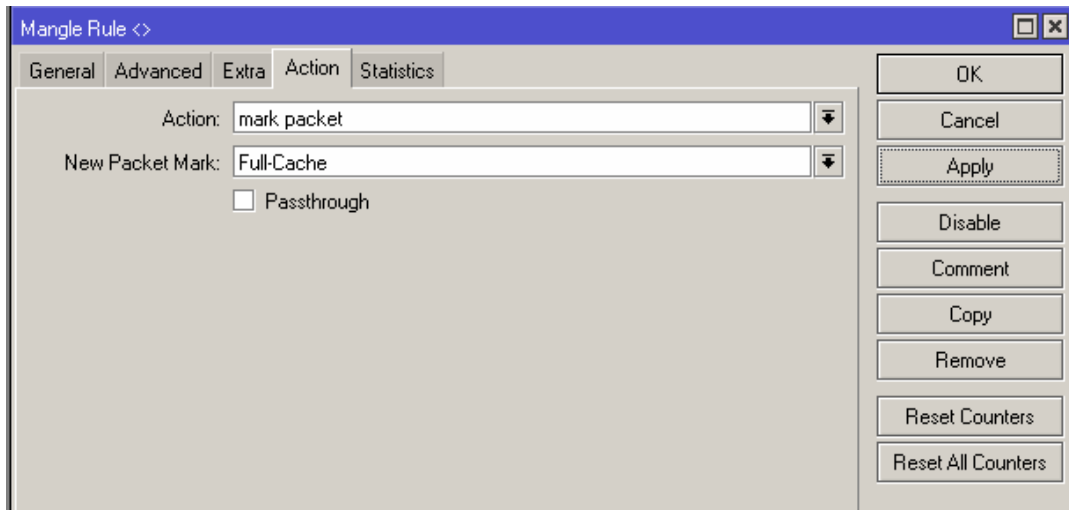
Vamos a usar Full cache para que cuando limitemos la velocidad de descarga o de navegación de un cliente, esa limitación no se aplique a los elementos que sean servidos desde nuestro servidor Web proxy. Esto se consigue poniendo una marca a los elementos que se almacenan en la caché y definiendo una regla para que la limitación de velocidad no se aplique a dichos elementos.

Para establecer estas marcas accedemos al panel lateral, en **IP -> Firewall** y pulsamos en la pestaña Mangle, a continuación creamos la siguiente regla:

En la pestaña General, seleccionamos en el campo Chain la opción output.

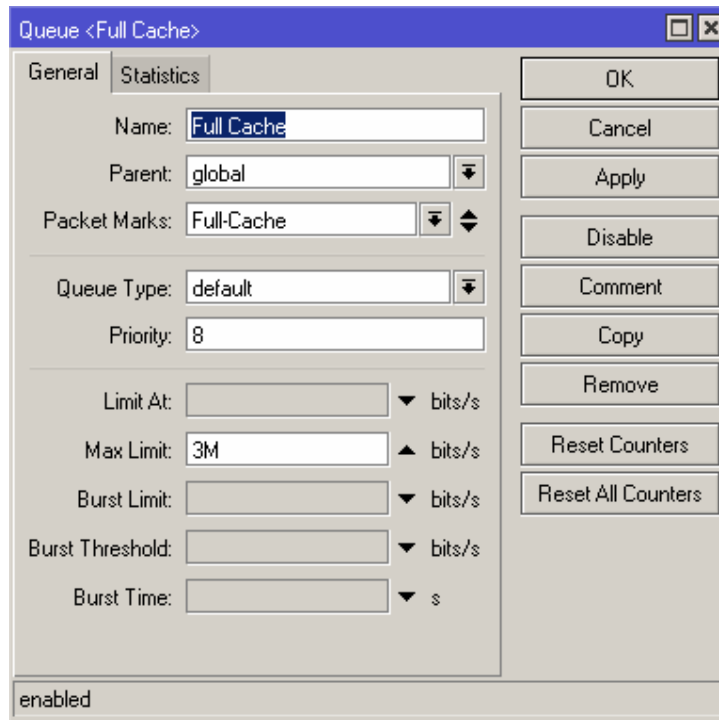
En la pestaña Advanced, establecemos en el campo DSCP (TOS) el valor 4.

En la pestaña Action, seleccionamos en el campo Action la opción mark packet, y en el campo New Packet Mark indicamos cual será nuestra marca, en este caso "Full-Cache", como se muestra en la figura:



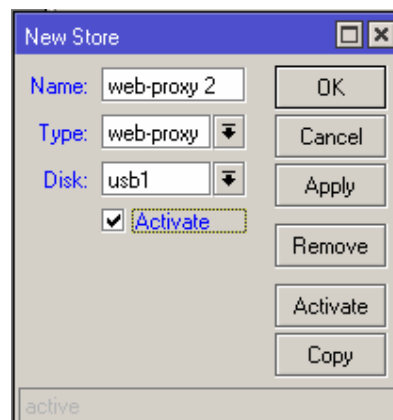
Por ultimo pulsamos en Apply y después en OK para terminar.

Una vez tenemos marcados los paquetes que se pueden servir desde nuestra cache, tenemos que establecer una regla que indique como se va a proceder con estos elementos. Para ello nos vamos al menú lateral, **Queues** y seleccionamos la pestaña **Queue Tree**, desde donde crearemos una nueva regla tal como se muestra en la imagen:



Aquí **Max Limit** hace referencia a la velocidad máxima a la que se sirven los recursos marcados previamente, si no ponemos nada se sirve al máximo que permita la infraestructura creada, pero para evitar saturar la red, hemos establecido un límite máximo de 3 mbps

Para terminar hemos conectado un disco duro externo usb a nuestro routerboard para almacenar los datos del Web Proxy. Para ello accedemos desde el menú lateral **System** -> **Stores** y pulsamos en la pestaña **Disks**, donde ya debe aparecer el dispositivo, con el nombre usb1. Lo formateamos y una vez completada la tarea añadimos una nueva regla:



De esta forma se activa por defecto el almacenamiento cache en este dispositivo y la configuración anterior que almacenaba los datos del servidor proxy en la memoria interna de la routerboard queda como respaldo.

Configuración DHCP Server

Un servidor **DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)** nos va a permitir asignar automáticamente tanto direcciones IP como el resto de parámetros de configuración a los usuarios de la red. Nuestro servidor almacena un conjunto de direcciones previamente establecido y las irá asignando según se vayan necesitando. La configuración y detalles de este protocolo se pueden ver en el RFC 2131.

Para establecer la configuración, desde el panel lateral de Winbox marcamos **IP -> DHCP Server** y pulsamos sobre el botón **DHCP Setup**, lanzando de esta manera un asistente de configuración en el que tendremos que indicar algunos datos:

La interfaz asociada a la red LAN: ether2

La dirección de red del servidor DHCP: 192.168.10.1/24

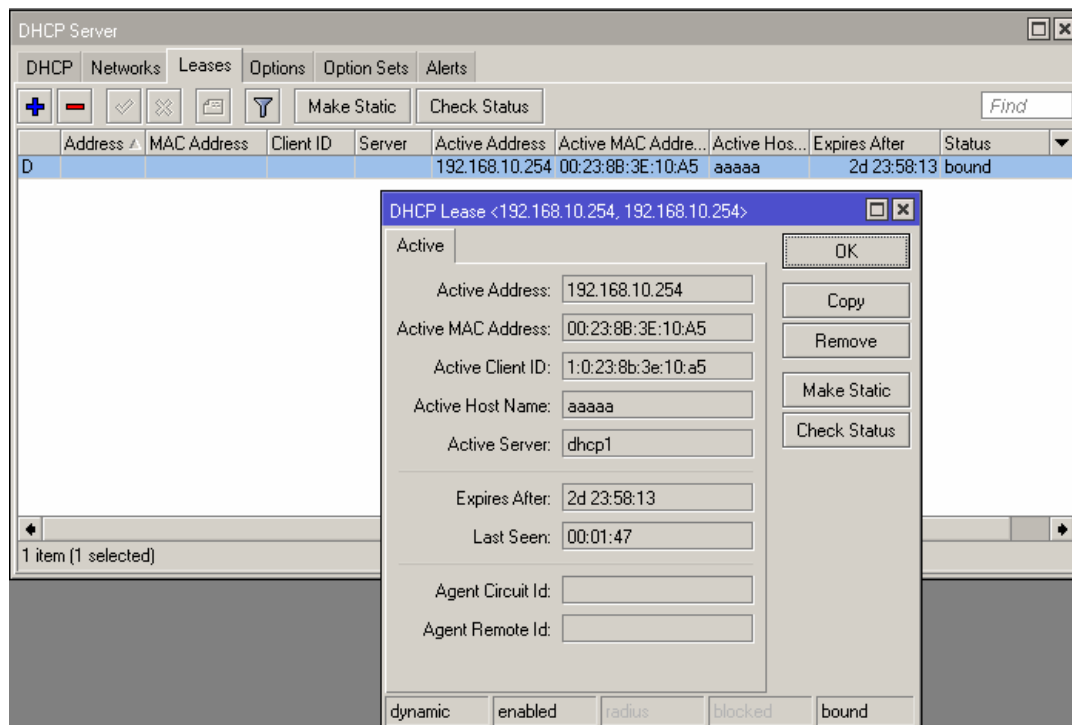
La puerta de enlace predeterminada o Gateway: 192.168.10.1

El rango de direcciones a asignar: 192.168.10.50 – 192.168.10.254

Los servidores DNS que se van a usar: 80.58.61.250, 80.58.61.254

El lease time: 3d 00:00 (indica cuanto tiempo puede usar la misma configuración el cliente)

Una vez terminada la configuración, ya tendremos el servidor funcionando, y podremos ver los clientes a los que se les ha asignado una IP en la pestaña **Leases**



Portal cautivo

Un portal cautivo es un sistema que controla el tráfico HTTP y fuerza a los usuarios a pasar por una página especial donde deberá autenticarse antes de poder navegar por Internet con normalidad. El portal cautivo permite además limitar el tiempo de cada sesión, así como controlar el ancho de banda usado por cada cliente.

Con el acceso a través del portal cautivo podemos informar a los usuarios de las normas de uso y las condiciones de acceso en la red municipal, para prevenir así un mal uso por parte de los mismos.

El equipo Mikrotik nos va a permitir implementar un portal cautivo empleando para ello un asistente, lo cual facilita enormemente la tarea, para ello desde el menú lateral de Winbox accedemos a **IP -> Hotspot** y pulsamos en **Hotspot Setup** para lanzar el asistente de configuración en el que tendremos que indicar algunos datos:

La interfaz asociada a la red LAN: ether2

La dirección de red del HotSpot: 192.168.10.1/24

El rango de direcciones a asignar: 192.168.10.50 – 192.168.10.254

Si usaremos certificado SSL para las conexiones

Si usaremos un servidor SMTP

Los servidores DNS que se van a usar: 80.58.61.250, 80.58.61.254

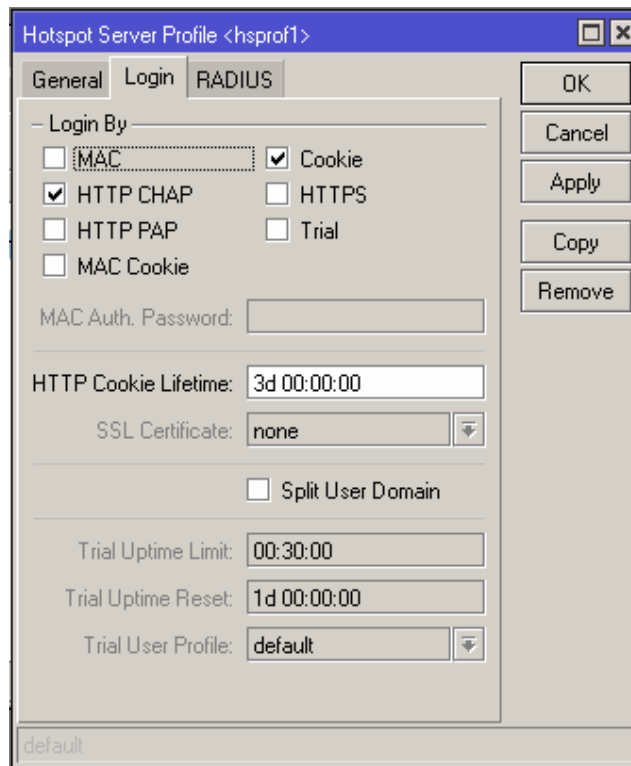
La dirección que verán los usuarios al conectar al hotspot: login.portal.net

Los datos de usuario y contraseña para acceder por primera vez: admin/admin

Tras la configuración, el router se reinicia y ya esta disponible nuestro portal cautivo:



Dentro de la opción **Server Profiles**, podemos configurar el tipo de autenticación de nuestros usuarios, pudiendo elegir entre diversas opciones:



Por defecto la opción marcada es **HTTP CHAP** que autenticará mediante usuario y contraseña.

Creando perfiles y usuarios

Para el alta de usuarios disponemos de varias modalidades. Una totalmente libre que no requiere de registro, pero que solo da acceso al portal Web del ayuntamiento y a páginas que se consideren por parte del mismo como de interés general para los habitantes del municipio.

Por otra parte, podremos usar el WiFi gratuito, aunque aquí se requiere de un registro previo. El registro de usuarios podrá realizarse de forma presencial presentando el DNI en las instalaciones del Ayuntamiento, en las dependencias de la **Delegación de Servicios Municipales** o en las instalaciones de la **Biblioteca Municipal**.

Por ultimo es posible también registrarse de forma telemática desde la sede electrónica del Ayuntamiento. A esta zona se puede acceder libremente, si bien se precisa del Dni electrónico para completar el registro.

En lo que respecta a la activación de estos usuarios en el sistema, podemos crear tantos usuarios como sean necesarios desde la ruta **System -> Users** del menú lateral de WinBox, así como definir los distintos perfiles que sean necesarios desde la pestaña **User Profiles**.

Server	Name	Address	MAC Address	Profile	Uptime
all	admin			default	00:32:59
all	user1			default	00:00:00
hotspot1	user2			default	00:00:00
hotspot1	user3			default	00:00:00
hotspot1	user4			default	00:00:00
hotspot1	user5			default	00:00:00

6 items

Mediante los perfiles podemos establecer por ejemplo el tiempo máximo que puede utilizarse la conexión, la velocidad de bajada y subida, etc.

Al conectar a los usuarios a través de un portal cautivo, tenemos la posibilidad de establecer páginas Web que pueden ser visitadas sin necesidad de estar autenticados en el sistema, es decir, sin necesidad de habernos registrado previamente como usuarios del servicio. Nosotros hemos establecido que la Web del ayuntamiento, www.casariche.es, este disponible para todo el mundo. Para configurar esta opción lo hacemos desde la pestaña **Walled Garden**, tal como se indica en la figura:

Walled Garden Entry <www.casariche.es>

Action: allow deny

Server: hotspot1

Src. Address:

Dst. Address:

Method:

Dst. Host: www.casariche.es

Dst. Port:

Path:

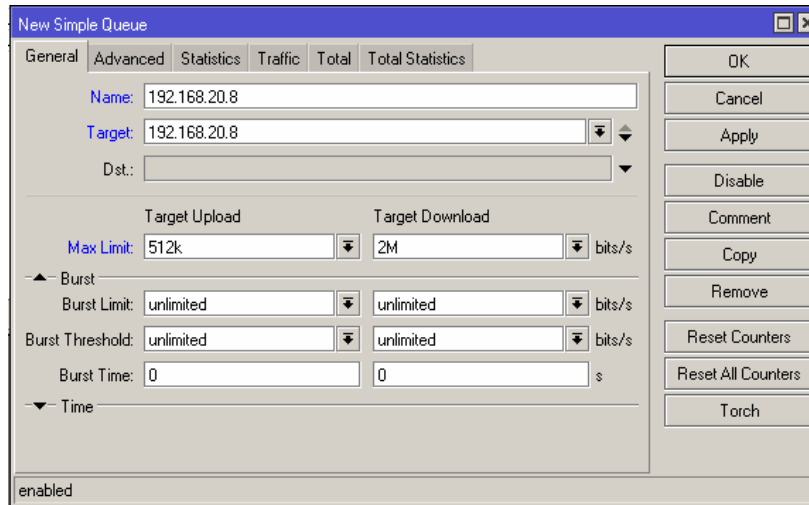
Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters

enabled

No obstante teniendo en cuenta que una parte de los usuarios que tendremos van a pagar por el servicio es necesario disponer de algún sistema que nos permita realizar su registro de forma automática y que permita además establecer las cuotas que se les asignan y controlar la facturación. Para estas tareas hay varios programas disponibles, muchos de ellos se pueden usar gratuitamente aunque con un número de usuarios limitado. Nosotros recomendamos Mikrowisp (<http://mikrowisp.net>) que dispone de una versión de prueba de hasta 100 usuarios.

Limitando la velocidad de los usuarios del servicio gratuito.

Para asegurarnos que ningún usuario consuma más de 256 kbps usaremos la opción Queues del menú lateral de Winbox, y desde allí creamos una regla en la que configuramos la IP a la que queremos limitar la velocidad y el tipo de limitación que le asignaremos. Es una opción bastante versátil que permite agrupar IPs, permite establecer diferentes limitaciones según el uso de la red, etc.



Nosotros de inicio asignamos un limite de 128 kbps de subida y 256 kbps de bajada a cualquier usuario que acceda desde el hotspot, mientras que los usuarios que acceden desde el servicio Premium tendrán una cuota de 2 Mbps de bajada y 512 kbps de subida.

The screenshot shows the 'Simple Queue' configuration window. The 'Simple Queue' tab is selected. The table below shows the configuration for various queues:

Queue	Name	Target	Upload Rate	Download Rate	Total Rate
0	192.168.0.0/24	192.168.0.0/24	128k	256k	384k
1	192.168.0.0/24	192.168.0.0/24	128k	256k	384k
2	192.168.0.0/24	192.168.0.0/24	128k	256k	384k
3	192.168.0.0/24	192.168.0.0/24	128k	256k	384k
4	192.168.0.0/24	192.168.0.0/24	128k	256k	384k
5	192.168.0.0/24	192.168.0.0/24	128k	256k	384k
6	192.168.0.0/24	192.168.0.0/24	128k	256k	384k
7	192.168.0.0/24	192.168.0.0/24	128k	256k	384k

Seguridad de la red

Por la propia naturaleza de este tipo de redes, cualquier persona puede tener acceso a los datos que se transmiten, lo que hace que se deban tomar medidas para garantizar la seguridad de la red. Ya se ha hablado antes de las pautas a seguir en este tipo de redes:

Modificar el SSID que viene predeterminado.

Utilización de cifrado WPA2 en lugar de cifrado WEP

Uso de contraseñas seguras

Cambios frecuentes de la contraseña de acceso a los equipos

Establecer un filtrado de dispositivos autorizados mediante la MAC

Control del tráfico en nuestra red

Se dispone de un firewall integrado en Mikrotik que utilizaremos para establecer que tráfico permitiremos y que tráfico bloquearemos.

Además se va a complementar este cortafuegos con un servidor que realizara tareas de seguimiento y control de los equipos, Este equipo se instala en el PC de sobremesa, donde instalaremos una distribución Linux, por ejemplo **Debian**, y que nos permitirá instalar programas como snort, nmap, mikrowisp, etc.

Al no ser una red abierta, sino que requiere registro antes de poder usarse, por lo general se va a permitir casi todo el tráfico y solo se bloqueara aquel que suponga una amenaza directa, así como el que se sospeche que puede ser consecuencia de un ataque.

Para crear las reglas del cortafuegos, tenemos dos opciones, o bien accedemos al Terminal desde el menú lateral en Winbox y allí las escribimos, o bien lo hacemos desde IP -> Firewall de manera gráfica. En este caso se va a utilizar la primera opción por comodidad.

Hacemos un listado de las direcciones que se asocian a las redes disponibles:

```
/ip firewall address-list
```

```
add address=192.168.1.0/24 list=Estructura
```

```
add address=192.168.10.0/24 list=WiFi-Gratis
```

```
add address=192.168.20.0/24 list=WiFi-Premium
```



```
Terminal
[admin@MikroTik] > /ip firewall address-list
[admin@MikroTik] /ip firewall address-list>
[admin@MikroTik] /ip firewall address-list> add address=192.168.1.0/24 list=Estructura
[admin@MikroTik] /ip firewall address-list> add address=192.168.10.0/24 list=WiFi-Gratis
[admin@MikroTik] /ip firewall address-list> add address=192.168.20.0/24 list=WiFi-Premium
[admin@MikroTik] /ip firewall address-list>
```

Definimos que sólo se pueda hacer ping desde la red de estructura:

```
/ip firewall filter

add chain=input src-address=192.168.1.0/24 protocol=icmp action=accept

add chain=input protocol=icmp action=drop

[admin@MikroTik] > /ip firewall filter
[admin@MikroTik] /ip firewall filter> add chain=input src-address=192.168.1.0/24 protocol=icmp action=accept
[admin@MikroTik] /ip firewall filter> add chain=input protocol=icmp action=drop
[admin@MikroTik] /ip firewall filter>
```

No se permite usar el servicio ftp a los usuarios gratuitos

```
/ip firewall filter

add chain=input src-address=192.168.1.0/24 protocol=tcp dst-port=21
action=accept

add chain=input src-address=192.168.20.0/24 protocol=tcp dst-port=21
action=accept

add chain=input protocol=tcp dst-port=21 action=drop
```

Sólo se permite usar telnet desde la red de estructura

```
/ip firewall filter

add chain=input src-address=192.168.1.0/24 protocol=tcp dst-port=23
action=accept

add chain=input protocol=tcp dst-port=23 action=drop
```

Regla para detectar y clasificar ataques spam conocidos

```
/ip firewall filter

add action=add-src-to-address-list address-list=spammer address-list-timeout=1d chain=forward
comment="Detecta virus o spammers SMTP "

connection-limit=10,32 disabled=no dst-port=25 limit=50,5 protocol=tcp

src-address-list=!spammer
```

Bloqueamos accesos SSH por fuerza bruta

```
/ip firewall filter

add action=drop chain=input comment="Denegamos accesos SSH por fuerza
bruta" disabled=no dst-port=22 protocol=tcp src-address-
list=ssh_blacklist

add action=add-src-to-address-list address-list=ssh_blacklist address-
list-timeout=1w chain=input connection-state=new disabled=no dst-
port=22 protocol=tcp src-address-list=ssh_stage2

add action=add-src-to-address-list address-list=ssh_stage2 address-
list-timeout=1m chain=input connection-state=new disabled=no dst-
port=22 protocol=tcp src-address-list=ssh_stagel

add action=add-src-to-address-list address-list=ssh_stagel address-
list-timeout=1m chain=input connection-state=new disabled=no dst-
port=22 protocol=tcp
```

Bloqueamos accesos externos a servicios DNS ya que tenemos configurado nuestro servidor DNS en el router

```
/ip firewall filter

add action=drop chain=input comment="Denegamos accesos DNS remotos"
dst-port=53 in-interface=ether1 protocol=tcp

add action=drop chain=input dst-port=53 in-interface=ether1
protocol=udp
```

Bloqueamos Netbios

```
/ip firewall filter

add action=drop chain=drop comment="Drop NetBios" connection-
mark=netbios

disabled=no protocol=tcp

add action=drop chain=drop connection-mark=netbios disabled=no
protocol=udp
```

Bloqueamos paquetes inválidos

```
/ip firewall filter

add action=drop chain=input comment="Bloquea paquetes inválidos"

connection-state=invalid disabled=no
```

Bloqueamos escaneos de puertos

```
/ip firewall filter

add action=drop chain=input comment="detecta y bloquea scan de
puertos"

disabled=no protocol=tcp psd=21,3s,3,1
```

Permitimos paquetes de conexiones existentes y relacionadas

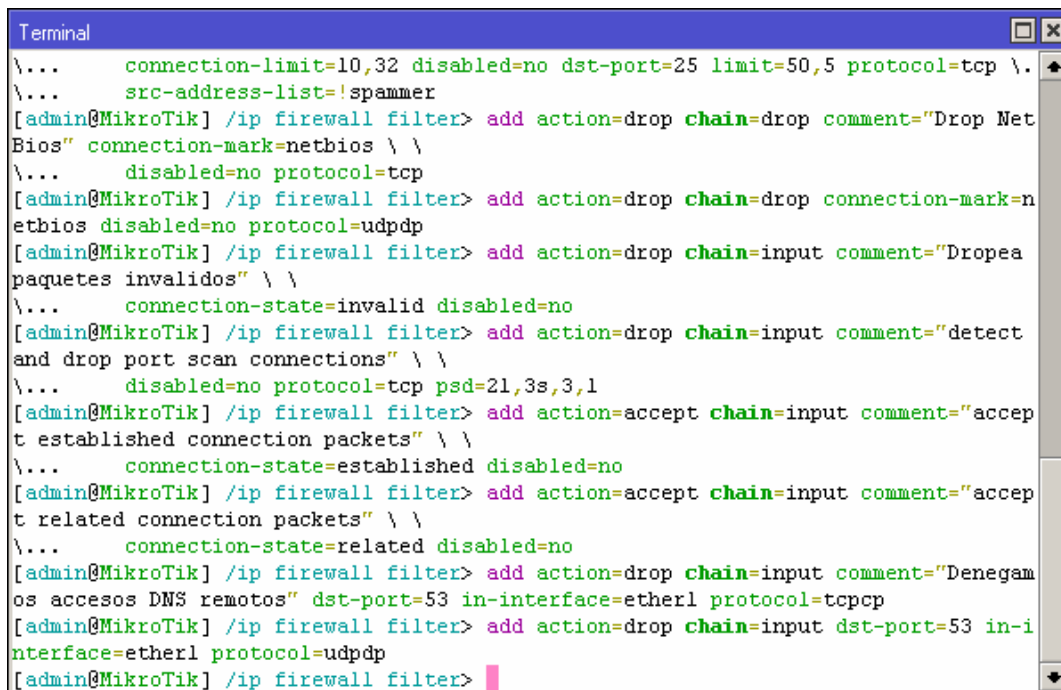
```
/ip firewall filter

add action=accept chain=input comment="acepta conexiones establecidas"

    connection-state=established disabled=no

add action=accept chain=input comment="acepta paquetes de conexiones
relacionadas"

    connection-state=related disabled=no
```



```
Terminal
\...    connection-limit=10,32 disabled=no dst-port=25 limit=50,5 protocol=tcp \.
\...    src-address-list=!spammer
[admin@MikroTik] /ip firewall filter> add action=drop chain=drop comment="Drop Net
Bios" connection-mark=netbios \ \
\...    disabled=no protocol=tcp
[admin@MikroTik] /ip firewall filter> add action=drop chain=drop connection-mark=n
etbios disabled=no protocol=udpdp
[admin@MikroTik] /ip firewall filter> add action=drop chain=input comment="Dropea
paquetes invalidos" \ \
\...    connection-state=invalid disabled=no
[admin@MikroTik] /ip firewall filter> add action=drop chain=input comment="detect
and drop port scan connections" \ \
\...    disabled=no protocol=tcp psd=21,3s,3,1
[admin@MikroTik] /ip firewall filter> add action=accept chain=input comment="accep
t established connection packets" \ \
\...    connection-state=established disabled=no
[admin@MikroTik] /ip firewall filter> add action=accept chain=input comment="accep
t related connection packets" \ \
\...    connection-state=related disabled=no
[admin@MikroTik] /ip firewall filter> add action=drop chain=input comment="Denegam
os accesos DNS remotos" dst-port=53 in-interface=ether1 protocol=tcp
[admin@MikroTik] /ip firewall filter> add action=drop chain=input dst-port=53 in-i
nterface=ether1 protocol=udpdp
[admin@MikroTik] /ip firewall filter>
```

Tras aplicar las reglas quedarían configuradas como sigue:

id	acción	protocolo	origen	destino	estado	log	bytes	packets
0	accept	icmp	any	any	in:out		72	199
1	accept	icmp	any	any	in:out		0	0
2	accept	icmp	any	any	in:out		53	906
3	drop	icmp	any	any	in:out	C (tcp)	0	0
4	accept	icmp	any	any	in:out		53	906
5	accept	icmp	any	any	in:out	I? (tcp)	125	996
6	accept	icmp	any	any	in:out	C (tcp)	53	906
7	accept	icmp	any	any	in:out		460	42
8	reject	icmp	any	any	in:out	C (tcp)	43	105
9	reject	icmp	any	any	in:out		64	96
0	reject	icmp	any	any	in:out		0	0
... place hotspots here								
1	accept	icmp	any	any	in:out		0	0
2	drop	icmp	any	any	in:out		0	0
... Detecta virus o spammer: SMTP								
3	accept	icmp	any	any	in:out	C (tcp)	25	0
... Detecta NetDios								
4	drop	icmp	any	any	in:out	C (tcp)	0	0
5	drop	icmp	any	any	in:out	I? (tcp)	0	0
... Detecta paquetes invalidos								
6	drop	icmp	any	any	in:out		90	23
... detecta y bloquea conexiones								
7	drop	icmp	any	any	in:out	C (tcp)	0	0
... acepta established connection packets								
8	accept	icmp	any	any	in:out		105	610
... acepta related connection packets								
9	accept	icmp	any	any	in:out		0	0
... Detectamos acciones: DNS remotos								
20	drop	icmp	any	any	in:out	C (tcp)	50	0
21	drop	icmp	any	any	in:out	I? (tcp)	50	0
22	drop	icmp	any	any	in:out	I? (tcp)	0	0
... detecta y bloquea escaneos								
23	drop	icmp	any	any	in:out	C (tcp)	0	0
... acepta paquetes de conexiones establecidas								
24	accept	icmp	any	any	in:out		0	0
... acepta paquetes de conexiones relacionadas								

Alertas

Aunque el firewall de Mikrotik permite configurar y registrar un sistema de alertas que se almacenarían en el mismo dispositivo, teniendo en cuenta que vamos a necesitar un PC externo para configurar el sistema de facturación, hemos decidido almacenar allí también los logs y definir el sistema de alertas en ese equipo, ya que es mucho más potente y dispondrá también de más espacio de almacenamiento, lo que nos permitirá guardar esa información el tiempo necesario. Para establecer alertas que nos informen de un uso que pueda ser potencialmente peligroso usamos **Snort**, donde configuraremos las reglas necesarias en función del tráfico que queramos controlar.

Por ejemplo, si queremos que el sistema registre cuando se hace ping a algún equipo de la red de estructura, podemos escribir la regla:

```
alert icmp any any -> 192.168.1.0/24 any (msg: "Ping ICMP detectado";
sid:977977977)
```

Si se desea controlar algún puerto en concreto podemos especificarlo. Por ejemplo con las siguientes reglas se indica cuando se intenta escanear el puerto que usa Winbox para acceder a los equipos Mikrotik:

```
alert tcp any any -> 192.168.1.0/24 8291 (msg:" Escaneo de puertos
WinBox TCP";sid:12345678)
```

```
alert udp any any -> 192.168.1.0/24 8291 (msg:" Escaneo de puertos
WinBox UDP ";sid:1234567)
```

Podemos emplear reglas similares para monitorizar intentos de acceso via telnet, ssh, etc

Contenido sensible

El programa Snort también nos avisa sobre intentos de acceso a programas p2p, paginas Web de descargas o con contenido no apto a menores de edad, etc. Sobre todo lo vamos a usar para controlar el uso que se hace de la red gratuita.

Algunas **reglas** podrían ser:

```
alert tcp 192.168.10.0/24 any -> any any (flow: to_server,established; uricontent:".torrent";  
msg:"Alerta: Posible acceso a Web de descargas p2p"; sid:998077772)
```

```
alert tcp 192.168.10.0/24 any -> any any (flow: to_server,established; uricontent:"rapidshare";  
msg:"Alerta: Posible acceso a Web de descargas directas "; sid:998077962)
```

```
alert tcp 192.168.10.0/24 any -> any any (flow: to_server,established; uricontent:"piratebay";  
msg:"Alerta: Posible acceso a Web de descargas p2p"; sid:998077532)
```

```
alert tcp 192.168.10.0/24 any -> any any (flow: to_server,established; uricontent:"porn";  
msg:"Alerta: Posible acceso a contenido para adultos"; sid:998077534)
```

Las reglas anteriores son sólo a título de ejemplo y las iremos adaptando a las circunstancias.

Conclusiones

Los municipios que hasta ahora tenían dificultades para acceder a Internet a alta velocidad tienen en las redes municipales una alternativa real para acercarse a las TIC, con unos costes de infraestructura y mantenimiento mucho más bajos que su equivalente en redes cableadas, por lo que pueden afrontar el despliegue por si mismos en lugar de estar a la espera de que los operadores de telecomunicaciones obtengan los retornos mínimos necesarios para afrontar la inversión e iniciar el proyecto.

La tecnología inalámbrica esta hoy lo suficientemente madura como para permitir tasas de transferencia suficientes para cualquiera de los servicios que los usuarios puedan demandar, y además permite cubrir zonas muy amplias de terreno empleando para ello muy pocos recursos.

La posibilidad de emplear las bandas libres de frecuencia es otra de las ventajas de estas redes, pues cualquier organización o comunidad puede desarrollar su propia red sin la necesidad de adquirir costosas licencias. La banda de 5 GHz debe ser la opción adecuada para estos despliegues, pues aunque en zonas rurales pueden obtenerse buenos resultados en la banda de 2,4 GHz, es de esperar que sean siempre peores que los obtenidos trabajando en la banda alta.

Los municipios tienen con estos proyectos la posibilidad de estar a la vanguardia de las últimas tendencias, desarrollando “smart cities” y preparando el terreno para el desarrollo del “Internet de las cosas”, creando proyectos culturales basados en la red y fomentando el desarrollo tecnológico, social y económico en sus comarcas.

Bibliografía y referencias

<http://es.wikipedia.org>

<http://www.wimaxforum.org/>

Página Web del programa Radio Mobile <http://www.cplus.org/rmw/english1.html>

Datos srtm: <http://dds.cr.usgs.gov/srtm/>

Página Web de la CMT <http://www.cmt.es>

SERVICIO DE TRANSPORTE METROPOLITANO EN ALTA VELOCIDAD PARA OPERADORES CON LICENCIA, Movistar

https://www.movistar.es/operadores/acceso_y_transporte/servicios_de_transporte/

Página Web de Mikrotik: <http://www.mikrotik.com>

Página Web de Alvarion: <http://www.alvarion.com>

Página Web de Ubiquiti: <http://www.ubnt.com>

Página Web de Movistar: <http://www.movistar.es>

Comunidades online

<http://forum.mikrotik.com>

<http://www.ryohnosuke.com>

<http://guifi.net>

www.zero13wireless.net

Anexo: Hojas de características



**WiMAX™ 16e
for the license-
exempt market**

BreezeMAX® Extreme 5000

WiMAX 16e for the License-exempt Market

BreezeMAX Extreme 5000 is part of the carrier-class, field-proven BreezeMAX product family and brings WiMAX 16e technology to the 5 GHz license-exempt market. This base station is designed for use in both data-intensive applications such as Internet access as well as high-capacity, mission-critical applications such as video surveillance, transportation management and real-time and nomadic services. BreezeMAX Extreme is ideally suited for smart cities, education, public safety, smart utilities, oil & gas, enterprises and wireless Internet service providers (WISPs).

BreezeMAX Extreme 5000 Advantages

- WiMAX 16e QoS for license-exempt frequencies
- Advanced interference mitigation techniques for leading performance and reliability
- MIMO A/B support for increased coverage and capacity
- Reliable video transmission and inherent multicast support
- Compact all-outdoor, easily installed single unit
- Secure connectivity with embedded encryption mechanisms
- Reliable and ruggedized infrastructure for extreme outdoor conditions
- Fast ROI with reduced TCO by utilizing an all-in-one, single platform with ASN gateway and dual sector support
- Mobile, portable and fixed services



Main Features and Highlights

Carrier-class WiMAX 16e Solution for the 5 GHz License-exempt Market

BreezeMAX Extreme 5000 brings carrier-class, standardized technology to the license-exempt market providing WiMAX Quality of Service (QoS) and enhanced coverage and capacity. BreezeMAX Extreme 5000 is designed to support interoperability and certification and complies with WiMAX Forum® guidelines, enabling ecosystems to benefit from WiMAX 16e economy-of-scale.

All-in-One, All Outdoor Solution for Profitable Up & Go Services

The compact design of BreezeMAX Extreme 5000 enables reduced CAPEX and OPEX for low total cost of ownership (TCO) and accelerated ROI. This all-in-one solution integrates the base station, antenna, ASN gateway and GPS receiver to provide an all outdoor solution that is easy to deploy on communication towers, rooftops and street poles.

Leverage WiMAX QoS for Enhanced and Swift Delivery of Triple Play Services

Featuring inherent WiMAX QoS, BreezeMAX Extreme 5000 enables simultaneous support of multiple applications using service differentiation for real-time triple play (voice, video and data) and non real-time applications.

Markets



WISP / Rural Broadband



Public Safety & Security



Smart Cities



Transportation



Oil & Gas



Mining



Ports



Corporate



Smart Utilities

Support Anytime, Anywhere Services

BreezeMAX Extreme offers MIMO, advanced antenna systems and air protocols to ensure reliable and resilient connections even in non line-of-site (NLOS) conditions. A variety of features support the system's network-level integrity, including encryption, authentication, extensive security and networking rules and AAA redundancy with failover.

Powerful Interference Mitigation Techniques for Overcoming Obstacles

BreezeMAX Extreme 5000 supports MIMO, providing STC and MRC advanced antenna techniques in both the base station and end user devices. Designed with state-of-the-art OFDMA and error correction coding techniques (leveraging 16e PHY) as well as an integrated spectrum analyzer, DFS and dynamic channel selection, BreezeMAX Extreme 5000 offers best Non-Line-of-Sight (NLOS) and interference resilience.

Efficient Delivery of Broadband Applications to Any Environment

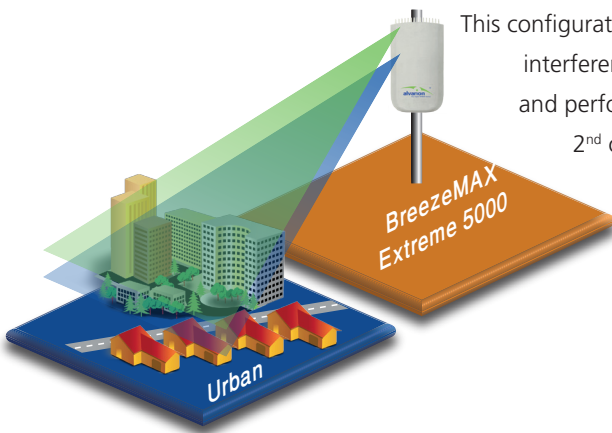
BreezeMAX Extreme 5000 supports unmatched sector capacity, coverage and deployment variety for enhanced implementation of fixed, nomadic and mobile applications in rural and urban deployments.

BreezeMAX Extreme 5000 Models

MIMO Single Sector 2x2

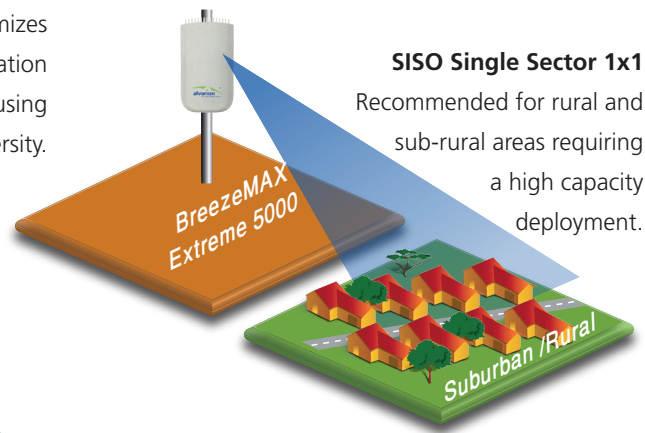
Recommended for high-capacity urban, video-driven and NLOS deployments.

This configuration maximizes interference mitigation and performance using 2nd order diversity.



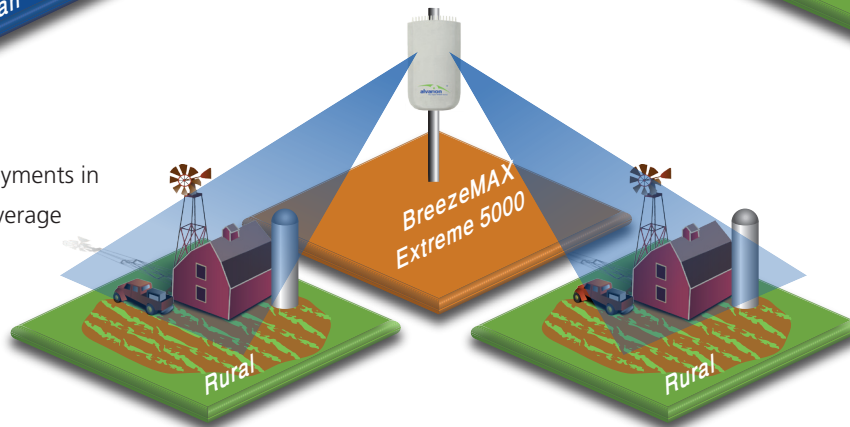
SISO Single Sector 1x1

Recommended for rural and sub-rural areas requiring a high capacity deployment.



SISO Dual Sector 1x1

Recommended for deployments in rural areas with large coverage requirements and lower capacity demands per sector.



Headquarters

International Corporate HQ
Tel: +972.3.645.6262
Email: corporate-sales@alvarion.com
North America HQ
Tel: +1.650.314.2500
Email: n.america-sales@alvarion.com

Sales Contacts

Australia:
anz-sales@alvarion.com
Asia Pacific:
ap-sales@alvarion.com
Brazil:
brazil-sales@alvarion.com
Canada:
canada-sales@alvarion.com
Caribbean:
caribbean-sales@alvarion.com
China:
cn-sales@alvarion.com
Czech Republic:
czech-sales@alvarion.com
France:
france-sales@alvarion.com
Germany:
germany-sales@alvarion.com
Italy:
italy-sales@alvarion.com
Ireland:
uk-sales@alvarion.com
Japan:
jp-sales@alvarion.com
Latin America:
lasales@alvarion.com
Mexico:
mexico-sales@alvarion.com
Nigeria:
nigeria-sales@alvarion.com
Philippines:
ph-sales@alvarion.com
Poland:
poland-sales@alvarion.com
Portugal:
sales-portugal@alvarion.com
Romania:
romania-sales@alvarion.com
Russia:
info@alvarion.ru
Singapore:
asean-sales@alvarion.com
South Africa:
africa-sales@alvarion.com
Spain:
spain-sales@alvarion.com
U.K.:
uk-sales@alvarion.com
Uruguay:
uruguay-sales@alvarion.com

For the latest contact information
in your area, please visit:
www.alvarion.com/company/locations

Specifications

Radio & Modem

Unit type	All outdoor base station	
Configuration options	Single sector MIMO – integrated / external antenna Single sector SISO+ – integrated / external antenna Dual sector SISO – external antenna	
Frequency	Base station 4900-5350 MHz 5470-5950 MHz	CPE 4900-5950 MHz
Channel bandwidth	5 MHz, 10 MHz, 2x10 MHz	5 MHz, 10 MHz
Number of channels	MIMO: 2Rx, 2Tx SISO: 1Rx, 1Tx	2Rx, 1Tx
Radio access method	IEEE 802.16-2005 (16e OFDMA)	
Operational mode	TDD	
Central frequency resolution	2.5 MHz (for 5 MHz channel), 5 MHz (for 10,2x10 MHz channel)	
FFT size	512/1024	
Supported modulation	QPSK 1/2, 3/4 + Rep QAM16 1/2, 3/4 QAM64 2/3, 3/4, 5/6	
Air link optimization support	HARQ, CTC, compressed DL / UL Maps.	
Diversity	2x2, MIMO Matrix A, MRC, MIMO Matrix B	

Transmit Power

Transmit power	Base Station 0-21 dBm, 1dB resolution	CPE QAM64: 18 dBm QAM16: 20 dBm QPSK: 21 dBm ATPC of 20 dB, 1 dB resolution 16 dBi
Integrated antenna gain	14.5 dBi	

Security

Authentication	Centralized over RADIUS, MS chap v.2 EAP TTLS over RFC-2865
Data encryption	AES WiMAX 16e

Interfaces

Network	IEEE 802.3 CSMA/CD
Standard compliance	10/100 Mbps, half/full duplex with auto negotiation
Data interface	In: PoE (55V DC) In: 48V DC
Power	Out: PoE (55V DC) feeding backhaul CPE
GPS	Antenna (TNC), receiver integrated in unit GPS chaining support

Mechanical

Dimensions (H x D x W)	Base Station 51 x 28 x 14.7 cm	CPE 23 x 23 x 6.3 cm
Weight:		
Extreme 5000 unit	11 kg	2 kg
Mounting Kit	5 kg	

Environmental

Operating temperature	-40°C to 55°C
Operating humidity	5%-95% non condensing, weather protected

Standard Compliance

EMC	ETSI EN 301 489-1, FCC p15
Safety	CE EN 60950-1/22, UL 60950-1/22
Environmental	ETS 300 019 part 2-1, 2-2, 2-4, IP67
Radio	ETSI EN 302 326, ETSI EN 301 390 ETSI EN 301 893, ETSI EN 302 502 FCC part 15.247, FCC part 15.407, RSS-111, RSS-210 ETSI 300 019-2-4 Class T4.1E (IEC-60068-2-56)
Humidity	ROHS
Regulatory compliance	

+ Not available in North America



© Copyright 2011 Alvarion Ltd. All rights reserved.
Alvarion® its logo and all names, product and service names referenced herein are either registered trademarks, trademarks, tradenames or service marks of Alvarion Ltd. in certain jurisdictions.
All other names are or may be the trademarks of their respective owners. The content herein is subject to change without further notice.
Any purchase orders submitted and actual supply of products and/or grant of licenses are subject to Alvarion's General Term and Conditions and/or any other effective agreement between the parties.

About Alvarion

Alvarion Ltd. (NASDAQ:ALVR) provides optimized wireless broadband solutions addressing the connectivity, capacity and coverage challenges of telecom operators, smart cities, security, and enterprise customers. Our innovative solutions are based on multiple technologies across licensed and unlicensed spectrums.
www.alvarion.com

BreezeMAX Extreme

CPE

PRO 5000

Technical Specification

Version 1.4

Alvarion Ltd. All rights reserved.

The material contained herein is proprietary, privileged, and confidential. No disclosure thereof shall be made to third parties without the express written permission of Alvarion. Alvarion reserves the right to alter the specifications in this publication without prior notice.

Alvarion.

21a HaBarzel St. Tel Aviv, 69710 Israel

Main Line / Fax: + 972 3 645 6262 / 6222

www.alvarion.com

Radio & Modem	3
Configuration and Management.....	4
Data Communications and services.....	4
Electrical.....	4
Interfaces	5
Mechanical.....	5
Indoor Unit	5
Outdoor Unit.....	5
Environmental.....	6
Indoor Unit	6
Outdoor Unit.....	6
Standard Compliance	7

Radio & Modem

Parameter	Value
WiMAX certification	WiMAX Forum 802.16e Wave 2 ready
Frequency	4900-5950GHz
Radio Access Method	Scheduled
Channel bandwidth (software selectable)	5Mhz 10Mhz
Duplexing Technologies	TDD
Antenna	Integral dual polarization antenna, 16dBi, 15°AZ x 15°EL.
Modulation Techniques	<ul style="list-style-type: none"> • Scalable OFDMA (512/1024 FFT) employing Time-Division Duplex (TDD) mechanism • PRBS subcarrier randomization • Contains pilot, preamble, and ranging modulation
FEC Coding Rates	QPSK, 16 QAM, 64 QAM
Radio Technology	Single Tx, Double Rx Downlink Rx methods: MIMO Matrix A, MRC, SISO
Maximum Output Power ¹ (At antenna port)	64QAM: 18dBm 16QAM: 20dBm QPSK: 21dBm
ATPC range	-20dBm to maximum

¹ Maximum Transmitted Power in use may vary based on country code

Configuration and Management

Management Options	<ul style="list-style-type: none"> • Web based (HTTP/HTTPS) • TR-069 • TFTP
Management access	From Wired LAN, Wireless Link
Management access protection	Access password
Allocation of IP parameters	<ul style="list-style-type: none"> • LAN – configurable • WAN – DHCP, option 43, 60
Software upgrade	HTTP/TFTP, controls by TR069
Configuration Upload/Download	HTTP/TFTP, controls by TR069 or web

Data Communications and services

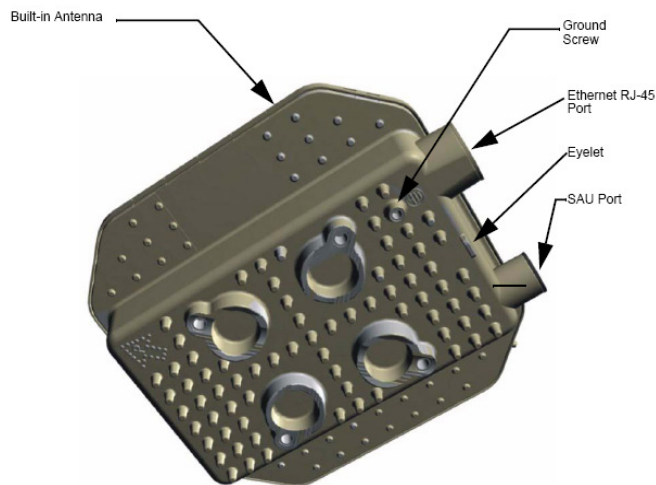
LAN interface	IEEE 802.3, 802.1Q, 802.1P IP CS bridge mode with transparent DHCP traffic Selective Proxy ARP
Air Interface	IEEE 802.16e IP CS with traffic classifier DSCP. Eth. CS (future release)

Electrical

AC power supply	Input: 100-240 VAC, 50-60 Hz, maximum power consumption 0.5A, Output: 55VDC, maximum power consumption 1A Power consumption with 70% duty-cycle 4.5W
MTBF	200,000 hrs for indoor and outdoor, GB 25°C Calculated Per Bellcore SR332

Interfaces

Ethernet Port	RJ-45 PoE
SAU Port	Mini USB connector with proprietary protocol



Mechanical

Indoor Unit

Dimensions	156mm (L) X 60mm (W) X 33mm (T)
Weight	0.32 Kg
Mounting	Desktop
Cabling	PoE cable connection

Outdoor Unit

Dimensions	230mm (H) X 230mm (W) X 63 (T) mm
Weight	2 Kg
Mounting	Pole-Mount
Cabling	Category 5 cable connection

Environmental

Indoor Unit

Operating Temperature	-5 ⁰ C to 45 ⁰ C
Storage Temperature	-40 ⁰ C to 70 ⁰ C
Humidity	Maximum 95%, non condensing

Outdoor Unit

Operating Temperature	-40 ⁰ C to 55 ⁰ C
Storage Temperature	-40 ⁰ C to 70 ⁰ C
Humidity	Maximum 95%, non condensing
Rain	IEC 67
Random Vibrations	IEC 68-2-64
Shock	IEC-68-2-29
Salt Fog	IEC-68-2-11
Ice Loading	25mm radial ice density 7kN/m ³
Solar Radiation	IEC-68-2-5, MIL-STD-810D
Wind Speed	160Km/Hr required for antenna stability under operation

Alvarion.

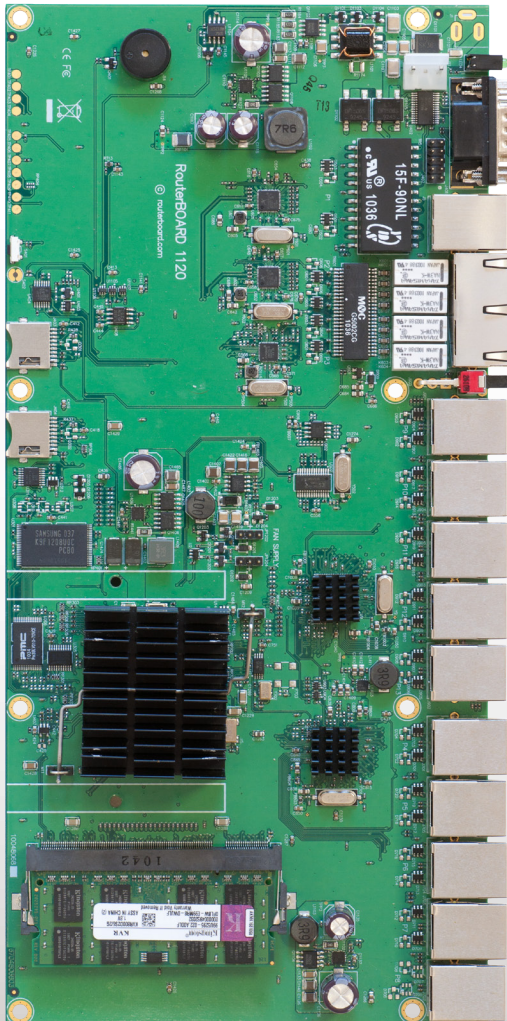
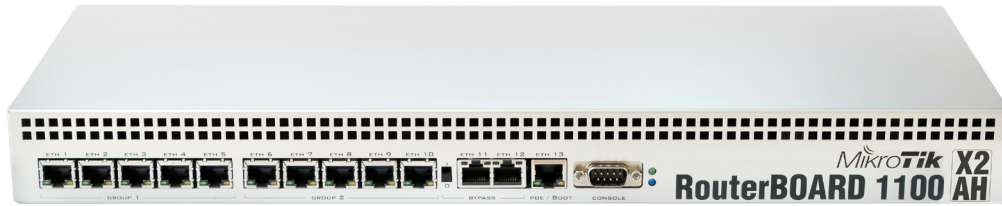
21a HaBarzel St. Tel Aviv, 69710 Israel
Main Line / Fax: + 972 3 645 6262 / 6222

www.alvarion.com

Standard Compliance

Type	Standard
EMC	FCC part 15B Class B EN 55022 Class B ETSI EN 301 489-1/4
Safety	IEC/EN 60950-1/-22 UL 609501-1/-22
Standards	EN 302 326 EN 301 893 v1.5.1 FCC p.27
Environmental	ETS 300 019 part 2-1,2-2,,2-4 IP67
Radio Signal	IEEE 802.16e-2005 WAVE 1 and WAVE 2 IEEE 802.3-2005 10BASE-T and 100BASE-TX FCC-06-96A1
Regulatory compliance	ROHS, WEEE

RB1100AHx2



This device is our best performance 1U rackmount Gigabit Ethernet router. With a dual core CPU, it can reach up to a million packets per second.

It has thirteen individual gigabit Ethernet ports, two 5-port switch groups, and includes Ethernet bypass capability.

2GB of SODIMM RAM are included, there is one microSD card slot, a beeper and a serial port.

The RB1100AH comes preinstalled in a 1U aluminium rackmount case, assembled and ready to deploy.

CPU	PowerPC P2020 dual core 1066MHz network CPU with IPsec accelerator
Memory	SODIMM DDR Slot, 2GB installed (RouterOS will use only up to 1.5GB)
Boot loader	RouterBOOT, 1Mbit Flash chip
Data storage	Onboard NAND memory chip, one microSD card slot
Ethernet	Thirteen 10/100/1000 Mbit/s Gigabit Ethernet with Auto-MDI/X
Ethernet	Includes switch to enable Ethernet bypass mode in two ports
miniPCI	none
Serial port	One DB9 RS232C asynchronous serial port
Extras	Reset switch, beeper, voltage and temperature sensors
Power options	Built-in power supply (IEC C14 standard connector 110/220V), PoE (12-24V on port 13)
Fan	Built in fans, and Fan headers
Dimensions	1U case: 44 x 176 x 442 mm, 1275g. Board only: 365g
Operating System	MikroTik RouterOS, Level 6 license

BaseBox

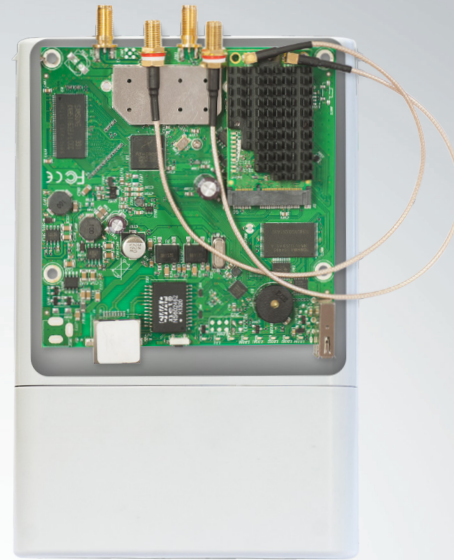
The BaseBox in an outdoor wireless device, based on our popular RB912 model, fitted with two SMA connectors for antennas, and a cable hood for protection against moisture. Also available are three additional places for antenna connectors, in case you wish to use the BaseBox miniPCIe slot for one more wireless interface to make a dual band device, or a 3G/4G modem.

The case can be opened with one hand, and is protected against the elements. USB, Ethernet and a Grounding wire exits are provided on the bottom, behind a protective door. Two models are available - BaseBox 2 and BaseBox 5 (2 or 5GHz wireless, respectively).

Comes with a mounting loop for tower/pole mounting, and a separate DIN rail mount is also provided. Package also includes a PoE injector and power supply unit.

Model	BaseBox 5	BaseBox 2
Order code	RB912UAG-5HPnD-OUT	RB912UAG-2HPnD-OUT
Features	1 Ethernet, 1 miniPCIe, USB, Additional memory, Gigabit, High power, Dual chain, Outdoor case	
CPU	Atheros AR9342 600MHz network processor	
Memory	64MB DDR onboard memory	
Ethernet	One Gigabit port with Auto-MDI/X	
Wireless	Built in 5GHz 802.11a/n, 2x RP-SMA connectors	Built in 2GHz 802.11b/g/n, 2x RP-SMA connectors
Connector type	RP-SMA Female (outside thread)	
Extras	beeper, signal and status LEDs, SIM slot (requires 3g miniPCIe card), voltage and temperature sensors	
Expansion	miniPCIe slot for 802.11 or 3G (using 3G disables the USB port), USB 2.0 port	
Power options	PoE: 8-30V DC on Ether1 (Non 802.3af). Consumption: 14W at 24V	
Dimensions	246x135x50mm; Weight: 390g	
OS	MikroTik RouterOS, Level4 license (supports wireless AP mode)	
Kit includes	RB912 outdoor unit, PSU, PoE injector, mounting loop, DIN rail mount, mounting ring	

	RB912UAG-5HPnD-OUT	RB912UAG-2HPnD-OUT
TX/RX at MCS0	30dBm / -96dBm	30dBm / -96dBm
TX/RX at MCS7	24dBm / -78dBm	24dBm / -78dBm
TX/RX at 6Mbit	30dBm / -96dBm	30dBm / -96dBm
TX/RX at 54Mbit	27dBm / -80dBm	27dBm / -80dBm
Frequency range	4900-5920MHz	2400MHz-2500MHz



Rendered image shows internals of BaseBox with optional second wireless card



Using the optionally available Flexguide cable, you can use the Basebox with any 3rd party antenna



24V 0.8A Adapter Mounting loops Metal ring
Gigabit PoE injector DIN mount



airMAX™

2x2 MIMO BaseStation Sector Antenna

Models: AM-9M13, AM-2G15-120, AM-2G16-90, AM-3G18-120,
AM-5G16-120, AM-5G17-90, AM-5G19-120, AM-5G20-90

High Performance, Long Range

Seamlessly Integrates with RocketM

Excellent Cross-Polarization Isolation



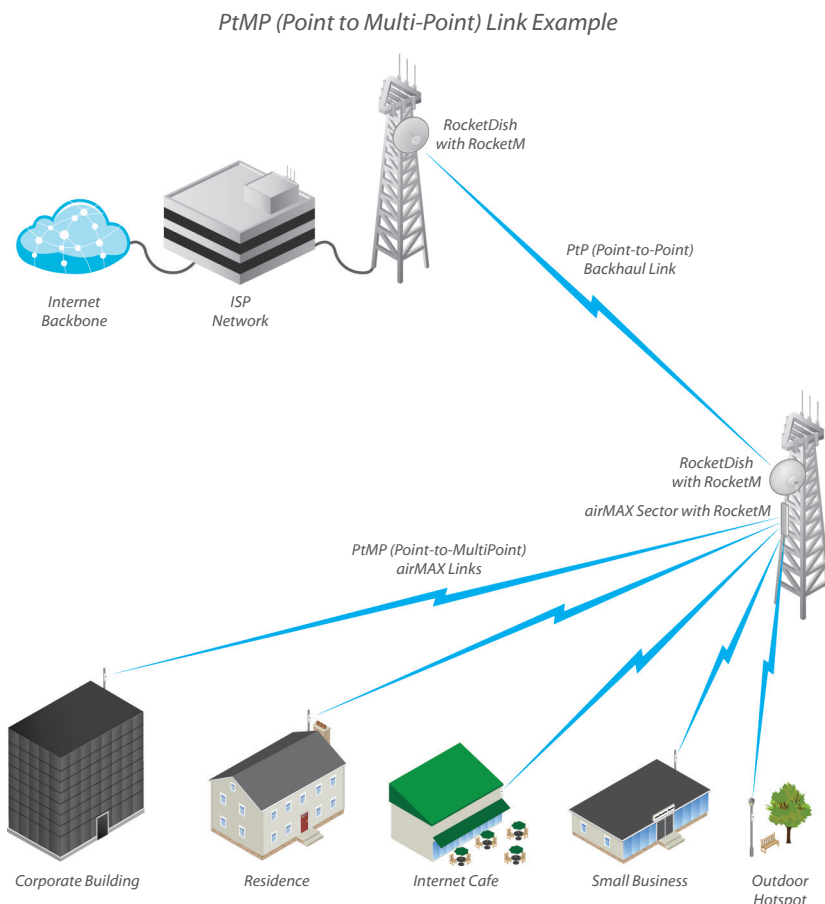
Overview

Sector Coverage

The airMAX Sector Antenna is a Carrier Class 2x2 Dual Polarity MIMO Sector Antenna that was designed to seamlessly integrate with RocketM radios (RocketM sold separately).

Pair the RocketM's radio with the airMAX Sector Antenna's reach to create a powerful basestation. This versatile combination gives network architects unparalleled flexibility and convenience.

On the right is one example of how the airMAX Sector Antenna can be deployed:



airMAX Sector Antennas provide sector-wide coverage and utilize airMAX technology to produce carrier-class performance and power.

Utilize airMAX Technology*

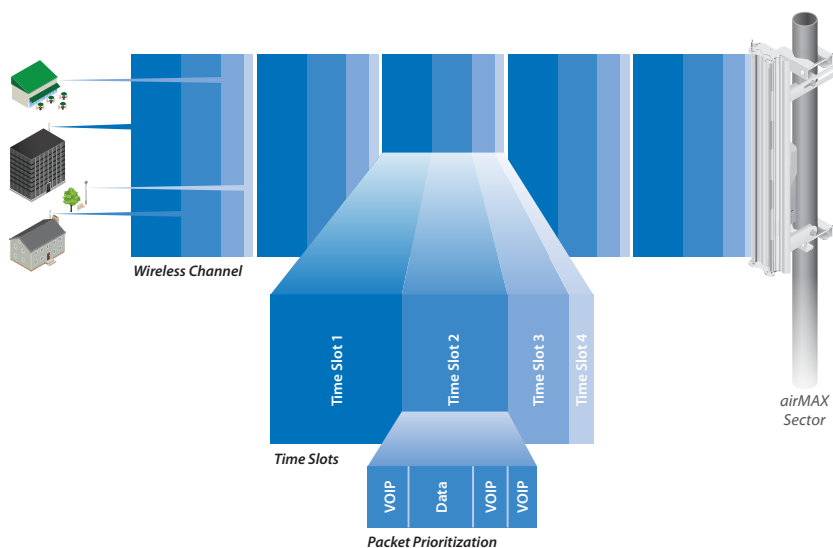
Unlike standard Wi-Fi protocol, Ubiquiti's Time Division Multiple Access (TDMA) airMAX protocol allows each client to send and receive data using pre-designated time slots scheduled by an intelligent AP controller.

This "time slot" method eliminates hidden node collisions and maximizes airtime efficiency. It provides many magnitudes of performance improvements in latency, throughput, and scalability compared to all other outdoor systems in its class.

Intelligent QoS Priority is given to voice/video for seamless streaming.

Scalability High capacity and scalability.

Long Distance Capable of high-speed, carrier-class links.



Up to 100 airMAX clients can be connected to an airMAX Sector; four airMAX clients are shown to illustrate the general concept.

* When airMAX Sector is paired with RocketM

Models



AM-9M13
(900 MHz, 13 dBi)



AM-2G15-120
(2.4 GHz, 15 dBi)



AM-2G16-90
(2.4 GHz, 16 dBi)



AM-3G18-120
(3 GHz, 18 dBi)



AM-5G16-120
(5 GHz, 16 dBi)



AM-5G17-90
(5 GHz, 17 dBi)



AM-5G19-120
(5 GHz, 19 dBi)



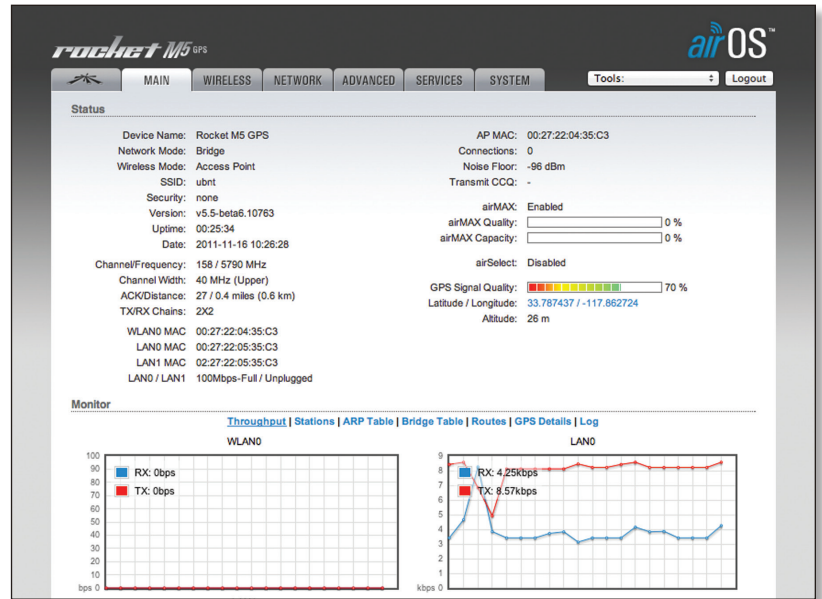
AM-5G20-90
(5 GHz, 20 dBi)

Software

airOS™

airOS is an intuitive, versatile, highly developed Ubiquiti firmware technology. It is exceptionally intuitive and was designed to require no training to operate. Behind the user interface is a powerful firmware architecture, which enables high-performance, outdoor multipoint networking.

- Protocol Support
- Ubiquiti Channelization
- Spectral Width Adjustment
- ACK Auto-Timing
- AAP Technology
- Multi-Language Support



airView™

Integrated on all Ubiquiti M products, airView provides Advanced Spectrum Analyzer Functionality: Waterfall, waveform, and real-time spectral views allow operators to identify noise signatures and plan their networks to minimize noise interference.

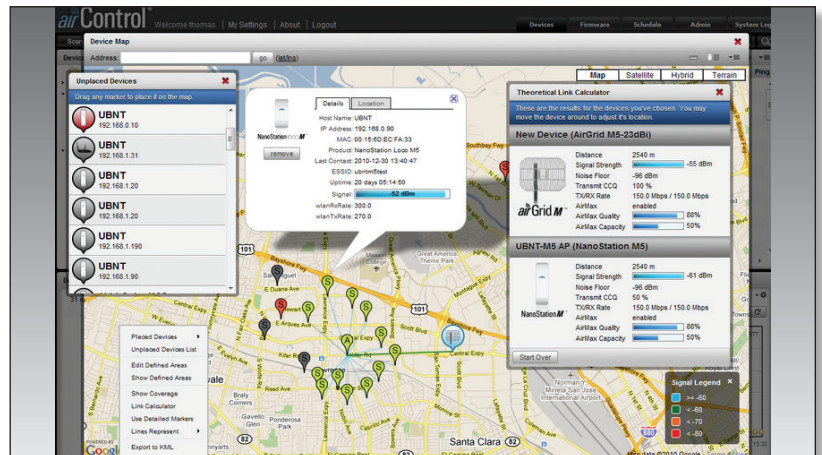
- **Waterfall** Aggregate energy over time for each frequency.
- **Waveform** Aggregate energy collected.
- **Real-time** Energy is shown in real time as a function of frequency.
- **Recording** Automate airView to record and report results.



airControl™

airControl is a powerful and intuitive, web-based server network management application, which allows operators to centrally manage entire networks of Ubiquiti devices.

- Network Map
- Monitor Device Status
- Mass Firmware Upgrade
- Web UI Access
- Manage Groups of Devices
- Task Scheduling



Specifications

	Antenna Characteristics			
Model	AM-9M13	AM-2G15-120	AM-2G16-90	AM-3G18-120
Dimensions* (mm)	1290 x 290 x 134	700 x 145 x 93	700 x 145 x 79	735 x 144 x 78
Weight**	12.5 kg	4.0 kg	3.9 kg	5.9 kg
Frequency Range	902 - 928 MHz	2.3 - 2.7 GHz	2.3 - 2.7 GHz	3.3 - 3.8 GHz
Gain	13.2 - 13.8 dBi	15.0 - 16.0 dBi	16.0 - 17.0 dBi	17.3 - 18.2 dBi
HPOL Beamwidth	109° (6 dB)	123° (6 dB)	91° (6 dB)	118° (6 dB)
VPOL Beamwidth	120° (6 dB)	118° (6 dB)	90° (6 dB)	121° (6 dB)
Electrical Beamwidth	15°	9°	9°	6°
Electrical Downtilt	N/A	4°	4°	3°
Max. VSWR	1.5:1	1.5:1	1.5:1	1.5:1
Wind Survivability	125 mph	125 mph	125 mph	125 mph
Wind Loading	95 lbf @ 100 mph	24 lbf @ 100 mph	19 lbf @ 100 mph	21 lbf @ 100 mph
Polarization	Dual-Linear	Dual-Linear	Dual-Linear	Dual-Linear
Cross-pol Isolation	30 dB Min.	28 dB Min.	28 dB Min.	28 dB Min.
ETSI Specification	N/A	EN 302 326 DN2	EN 302 326 DN2	EN 302 326 DN2
Mounting	Universal Pole Mount, RocketM Bracket, and Weatherproof RF Jumpers Included			

* Dimensions exclude pole mount and RocketM (RocketM sold separately)

** Weight includes pole mount and excludes RocketM (RocketM sold separately)

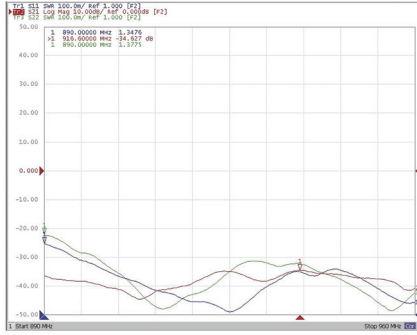
	Antenna Characteristics			
Model	AM-5G16-120	AM-5G17-90	AM-5G19-120	AM-5G20-90
Dimensions* (mm)	367 x 63 x 41	367 x 63 x 41	700 x 135 x 73	700 x 135 x 70
Weight**	1.1 kg	1.1 kg	5.9 kg	5.9 kg
Frequency Range	5.10 - 5.85 GHz	4.90 - 5.85 GHz	5.15 - 5.85 GHz	5.15 - 5.85 GHz
Gain	15.0 - 16.0 dBi	16.1 - 17.1 dBi	18.6 - 19.1 dBi	19.4 - 20.3 dBi
HPOL Beamwidth	137° (6 dB)	72° (6 dB)	123° (6 dB)	91° (6 dB)
VPOL Beamwidth	118° (6 dB)	93° (6 dB)	123° (6 dB)	85° (6 dB)
Electrical Beamwidth	8°	8°	4°	4°
Electrical Downtilt	4°	4°	2°	2°
Max. VSWR	1.5:1	1.5:1	1.5:1	1.5:1
Wind Survivability	125 mph	125 mph	125 mph	125 mph
Wind Loading	6 lbf @100 mph	6 lbf @100 mph	20 lbf @ 100 mph	26 lbf @ 100 mph
Polarization	Dual-Linear	Dual-Linear	Dual-Linear	Dual-Linear
Cross-pol Isolation	22 dB Min.	22 dB Min.	28 dB Min.	28 dB Min.
ETSI Specification	EN 302 326 DN2	EN 302 326 DN2	EN 302 326 DN2	EN 302 326 DN2
Mounting	Universal Pole Mount, RocketM Bracket, and Weatherproof RF Jumpers Included			

* Dimensions exclude pole mount and RocketM (RocketM sold separately)

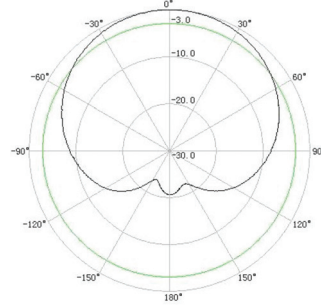
** Weight includes pole mount and excludes RocketM (RocketM sold separately)

AM-9M13 Antenna Information

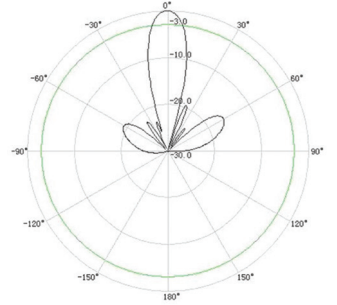
Return Loss



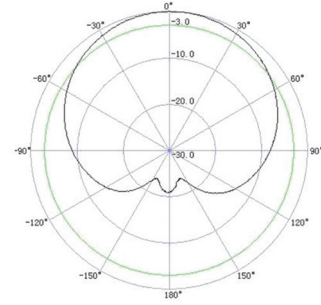
Vertical Azimuth



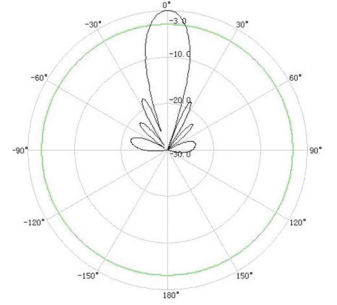
Vertical Elevation



Horizontal Azimuth

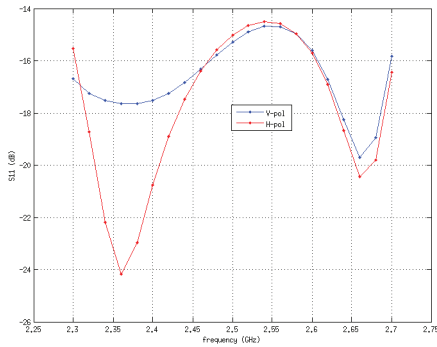


Horizontal Elevation

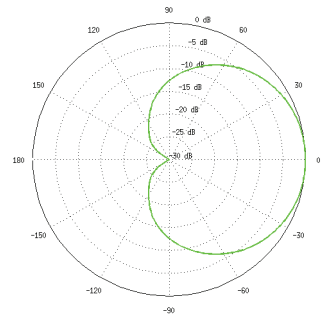


AM-2G15-120 Antenna Information

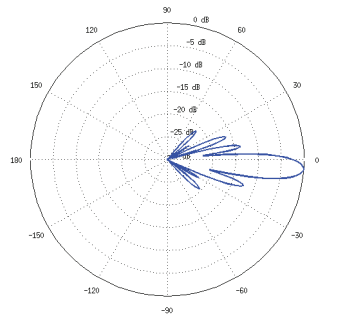
Return Loss



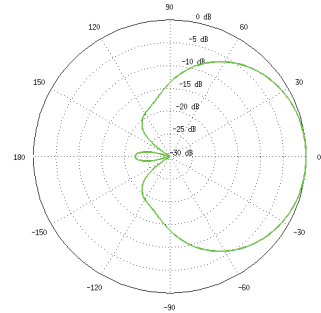
Vertical Azimuth



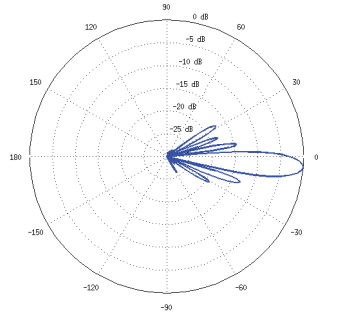
Vertical Elevation



Horizontal Azimuth

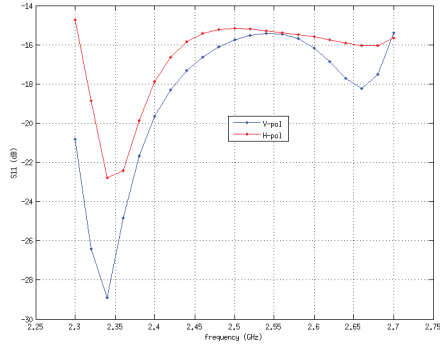


Horizontal Elevation

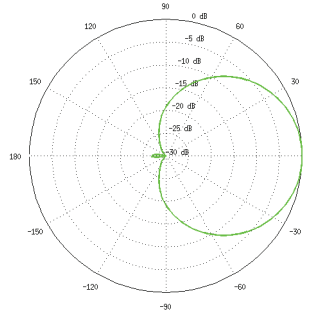


AM-2G16-90 Antenna Information

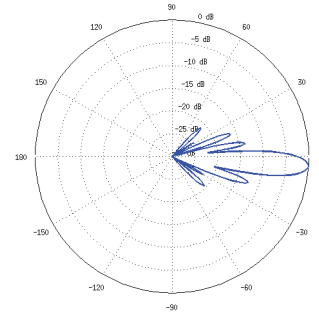
Return Loss



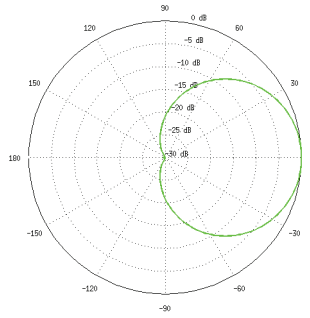
Vertical Azimuth



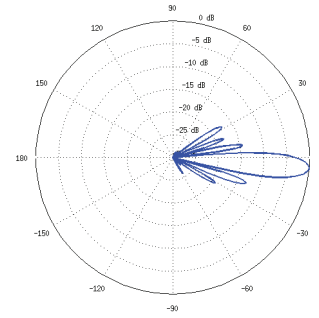
Vertical Elevation



Horizontal Azimuth

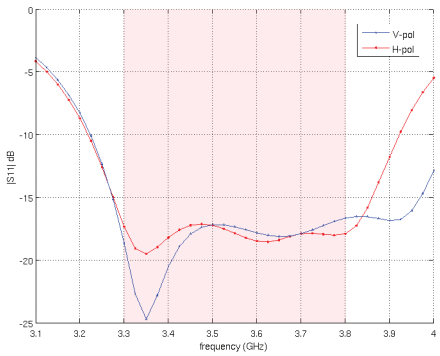


Horizontal Elevation

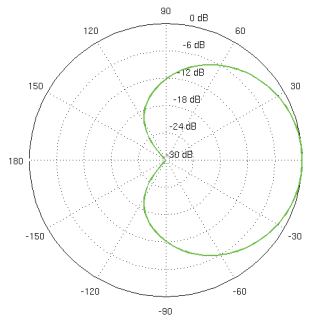


AM-3G18-120 Antenna Information

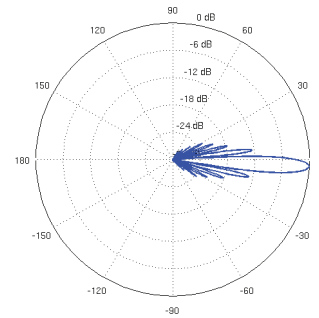
Return Loss



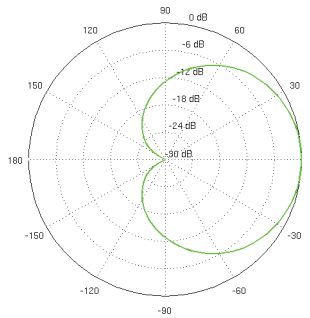
Vertical Azimuth



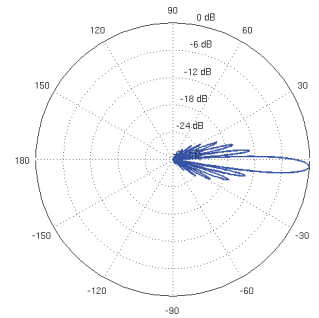
Vertical Elevation



Horizontal Azimuth

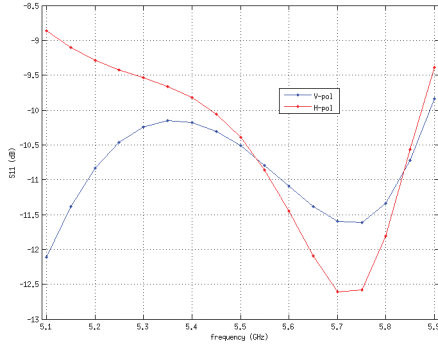


Horizontal Elevation

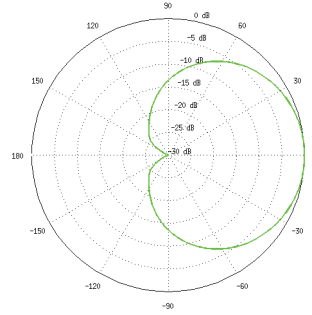


AM-5G16-120 Antenna Information

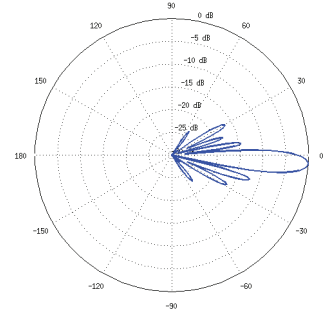
Return Loss



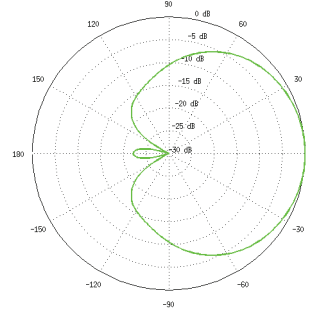
Vertical Azimuth



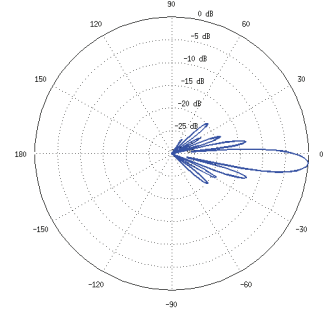
Vertical Elevation



Horizontal Azimuth

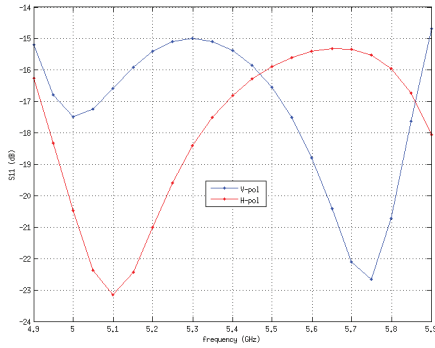


Horizontal Elevation

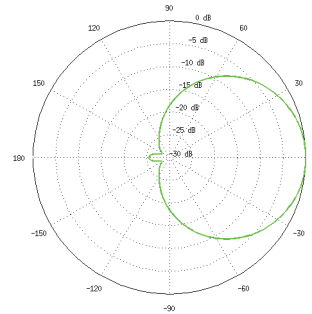


AM-5G17-90 Antenna Information

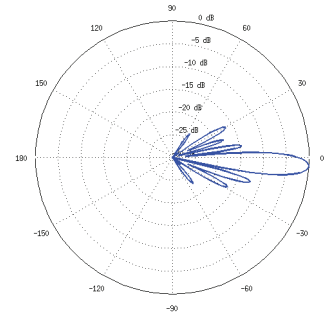
Return Loss



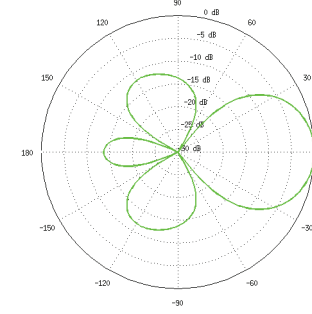
Vertical Azimuth



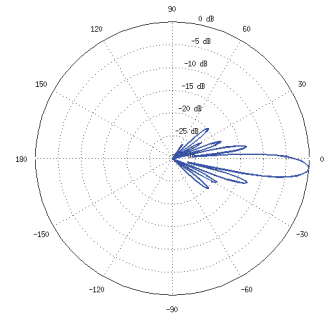
Vertical Elevation



Horizontal Azimuth

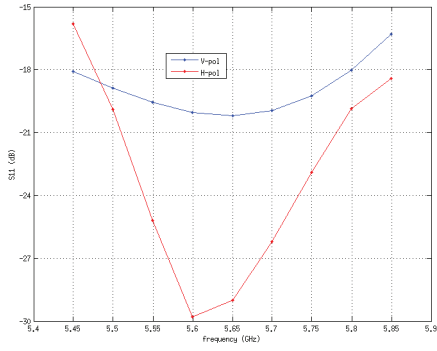


Horizontal Elevation

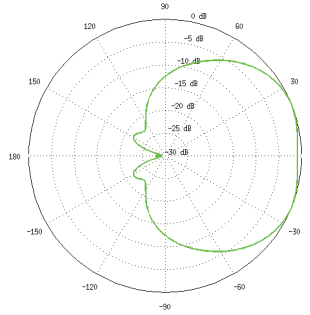


AM-5G19-120 Antenna Information

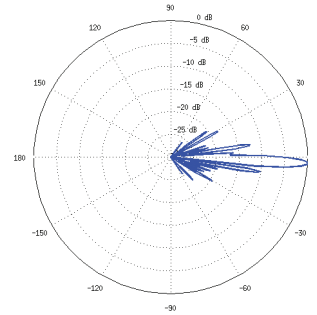
Return Loss



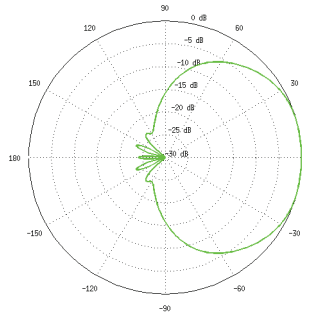
Vertical Azimuth



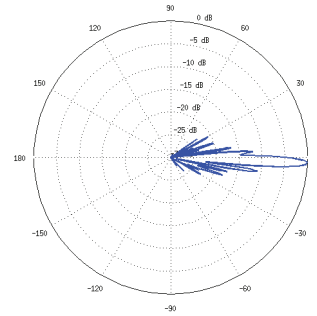
Vertical Elevation



Horizontal Azimuth

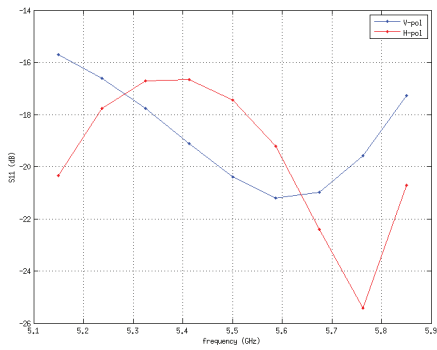


Horizontal Elevation

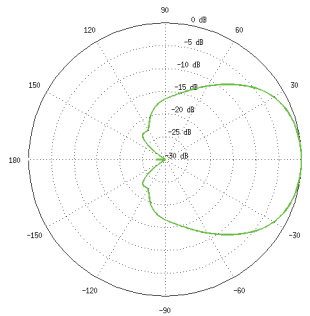


AM-5G20-90 Antenna Information

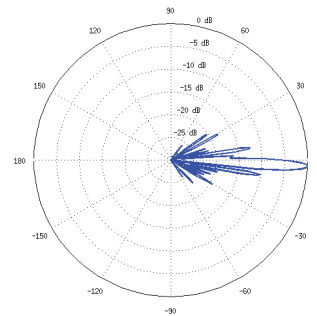
Return Loss



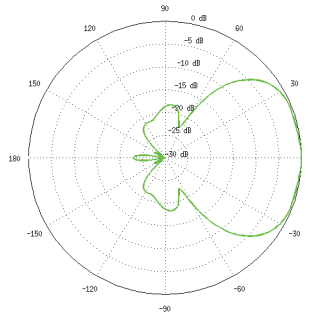
Vertical Azimuth



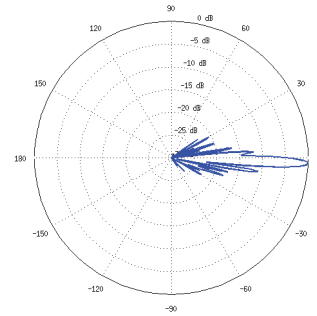
Vertical Elevation



Horizontal Azimuth



Horizontal Elevation



TOUGH Cable™

OUTDOOR CARRIER CLASS SHIELDED

Protect your networks from the most brutal environments with Ubiquiti Networks' industrial-grade, shielded Ethernet cable, TOUGH Cable.

Increase Performance

Dramatically improve your Ethernet link states, speeds, and overall performance with Ubiquiti TOUGH Cables.

Extreme Weatherproof

Designed for outdoor use, TOUGH Cables have been built to perform even in the harshest weather and environments.

ESD Damage Protection

Protect your networks from devastating electrostatic discharge (ESD) attacks.

Extended Cable Support

TOUGH Cables have been developed to increase power handling performance for extended cable run lengths.

Bulletproof your networks

TOUGH Cable is currently available in two versions: PRO Shielding Protection and CARRIER Shielding Protection.

TOUGH Cable PRO is a Category 5e, outdoor, carrier-class shielded cable with an integrated ESD drain wire.

TOUGH Cable CARRIER is a Category 5e, outdoor, carrier-class shielded cable that features an integrated ESD drain wire, anti-crosstalk divider, and secondary shielding. It is rated to provide optimal performance on Gigabit Ethernet networks.

Additional Information:

- 24 AWG copper conductor pairs
- 26 AWG integrated ESD drain wire to prevent ESD attacks and damage
- PE outdoor-rated, weatherproof jacket
- Multi-layered shielding
- Available in lengths of 1000 ft (304.8 m)



TOUGH Cable Connectors

Specifically designed for use with Ubiquiti TOUGH Cables, TOUGH Cable Connectors protect against ESD attacks and Ethernet hardware damage, while allowing rapid field deployment without soldering. The standard TOUGH Cable Connectors are available in 100-pc. bags, while the TC-GND versions include ground wires and are available in 20-pc. bags.

ESD attacks are the leading cause for device failures. The diagram below illustrates the areas vulnerable to ESD attacks in a network.

By using a grounded Ubiquiti Power over Ethernet (PoE) Adapter along with Ubiquiti TOUGH Cable and TOUGH Cable Connectors, you can effectively protect against ESD attacks.

