Trabajo final de carrera

Diseño de una red telemática para proporcionar acceso a Internet

Estudiante: José Martínez Campo
Consultor: Antoni Morell Pérez

1. Introducción

1.1- Descripción del proyecto.

En este TFC pretendo diseñar una red telemática que de acceso a Internet a un pequeño municipio (Llançà, Girona) mediante el uso de las tecnologías Wimax-Wifi. Dicha población se aproxima a las características necesarias para el proyecto, una población aproximada de 5000 habitantes, cuya densidad por Km² permita proporcionarles cobertura de una forma eficiente y además situada junto a la costa.

Por tanto se realizará un estudio de implantación de dicha red por parte del ayuntamiento en cuestión analizando los diversos aspectos involucrados en dicho diseño, tales como los requisitos legales debido a los conflictos que podemos ver con la CMT respecto a la libre competencia en casos ya acaecidos en algunas partes de nuestro territorio, y por supuesto los costes, requerimientos técnicos y funcionales, estudio de la población y topografía, descripción de las distintas tecnologías y características de los equipos, etc….

1.2.- Objetivos generales y específicos.

Se realizará por tanto el análisis y diseño de la red telemática teniendo en cuenta los siguientes aspectos:

- Legislación al respecto del acceso público gratuito a Internet.
- Estudio de la población en cuestión, tanto de su topografía, como de las características demográficas y de las ubicaciones y puntos de interés donde ubicar los equipamientos que den acceso a Internet.
- Descripción del funcionamiento y características de las distintas tecnologías inalámbricas que se ofrecen (WiFi-Wimax).
- Estudio de los equipamientos de red necesarios con sus características.
- Estudio de la cobertura necesaria para cubrir las zonas públicas.
- Estimación de costes en el diseño e implantación de la red.
- Simulación mediante un software de libre distribución de la cobertura en todo el municipio.

1.3.- Motivación, justificación.

He escogido dicha población no sólo por cumplir con los requerimientos del TFC sino porque como se puede ver, es un municipio bastante orientado al turismo ya que dispone de costa, club náutico y sitios de interés. Gracias a su privilegiada situación en la Costa Brava, Llançà se ha convertido en un importante centro turístico y residencial.

Por tanto, como principal motivación y justificación para la implantación de una red sin hilos gratuita en el municipio, me ha parecido razonable, el deseo del ayuntamiento de la localidad por ofrecer un servicio de valor añadido a sus habitantes y visitantes, de forma que incentive y fomente aún más el turismo y dinamice la economía de la localidad, además de facilitar el acceso en espacios públicos (parques, playas, plazas, etc) a sus habitantes, mejorando aún mas la fiabilidad y la cobertura ya existente con otras tecnologías en la zona (3G, ADSL, satélite o de otro tipo).

1.4.- Actores.

Como adjudicatario o cliente del proyecto que se hará cargo de los costes del proyecto y su implantación considero al propio ayuntamiento como principal interesado, ya que repercutirá en beneficios para el pueblo debido a los ingresos del turismo.

Los beneficiarios de acceder a dicha red serán tanto los vecinos del municipio como los turistas que visiten la zona.

Consideraremos que una empresa ficticia es quién realiza el estudio y viabilidad de este proyecto

1.5 - Situación actual.

En la actualidad es difícil encontrar municipios de este tamaño que no tengan acceso a la banda ancha aunque sea de forma limitada, debido a los esfuerzos que están realizando las administraciones públicas por dotar a la mayor parte de la población de acceso a Internet de banda ancha en los últimos años. Prueba de ello, es la aprobación a principios de este año del anteproyecto de la Ley General de Telecomunicaciones que actualiza la normativa vigente desde 2003 y resuelve determinadas cuestiones que afectaban negativamente a la competitividad de los operadores, penalizando el despliegue de nuevas redes, la inversión y la provisión de servicios. Las modificaciones incorporadas persiguen proporcionar una mayor facilidad para el despliegue de redes por los operadores y facilita la extensión de la banda ancha en el territorio (uno de sus principales, por no decir el principal de los objetivos de dicho anteproyecto).

Los usuarios verán mejoradas la cobertura, un incremento de la velocidad de Internet y la reducción de precios y costes junto con progresos en la protección.

No obstante, no es motivo para la no realización de este proyecto, ya que aún existiendo ya dicha cobertura en estos municipios, esta tecnología proporciona mayor cobertura y un servicio de valor añadido a los habitantes y turistas que dispongan de dispositivos inalámbricos, sin la necesidad de estar dados de alta con ningún operador, o que dispongan de poca o ninguna cobertura en la zona mediante otras tecnologías.

La existencia por otra parte de centrales en el municipio o sus cercanías, nos facilitará la implantación de esta red dada la necesidad de alquilar algún enlace a alguna operadora.

La tecnología móvil LTE (Long-Term Evolution), también conocida por 4G, comenzó a ser desplegada durante 2011 por varios operadores de todo el mundo: AT&T, Verizon y MetroPCS en Estados Unidos; Telia-Sonera y T-Mobile en Europa; NTT DoCoMo y KDDI en Japón, etc en competencia con Wimax. La evolución en los últimos tiempos ha hecho que WiMAX pierda fuerza frente a LTE como gran alternativa 4G. La tecnología WiMax es fácil y barata de comprar. WiMax requiere su propia red independiente. Los más interesados en LTE son mayormente, operadoras y fabricantes de equipos más acostumbrados a soluciones propietarias y entre los cuales los estándares abiertos no suelen ser precisamente su modus operandi. En teoría, tanto WiMax como LTE pueden proporcionar velocidades teóricas de pico de hasta 100Mbps, muy superiores al máximo de 14 Mbps de HSDPA. Aunque las velocidades del mundo real son muy inferiores a dicho máximo, y parece ser que rondan los 6 Mbps. Mientras que a las operadoras pequeñas les interesará más ofrecer WiMax por ser mucha más económica, como es el caso que nos ocupa para su implantación.

1.6 – Viabilidad técnica.

Dicha red debe ser capaz de mejorar la fiabilidad y cobertura existente en la zona. Además, es preciso que el ancho de banda de la red permita utilizar las aplicaciones que los usuarios utilicen más asiduamente (descarga de datos, mail, navegación, videos, etc..).

Dentro del ancho de banda a ofrecer a los usuarios y el espacio radioeléctrico utilizado, también tendremos que tener en cuenta el marco legal en el cual estamos, según la Ley General de Telecomunicaciones (como se dijo anteriormente, está en curso la aprobación de unas modificaciones a la ley de 2003, sin embargo a fecha de realización de este proyecto, me regiré por la normativa vigente, la de 2003, por no estar vigente aún el anteproyecto actual).

Se deberá tener en cuenta también el estudio de la población por tramos de edades, la densidad en cada zona y la simultaneidad de las conexiones soportadas en cada una de las ubicaciones para evitar un rendimiento bajo en cualquiera de los puntos de acceso. Como sabemos, no todos los usuarios utilizarán la red simultáneamente.

Habrá que tener en cuenta también el coste del proyecto, la implantación, el equipamiento, alquiler de enlaces necesarios a alguna operadora y que todo esto pueda ser asumible por el ayuntamiento, así como la infraestructura necesaria y la viabilidad de su instalación en las ubicaciones adecuadas.

1.7 – Datos generales de la población.

Llançá es un municipio catalán situado en la comarca del Alt Empordà en la provincia de Girona, Catalunya. Ocupa un área de 28,625 Km² y tiene una población de 5102 habitantes (INE 2012), con una densidad de 182,45 hab./km².

Casi limítrofe con Francia, esta situado al norte del parque natural del Cap de Creus, al sur del Paraje Natural de La Albera y a una distancia de unos 20 km de Figueres.

Como se dijo anteriormente gracias a su privilegiada situación en la Costa Brava, se ha convertido en un importante centro turístico y residencial. Dispone de un puerto con multitud de actividades náuticas además de la pesca, un patrimonio natural que visitar de distintas épocas históricas, rutas para realizar, playas y calas pequeñas, museos y variedad de restaurantes y hoteles.

En la primera imagen tomada con el Google Maps vemos las zonas que deseamos cubrir inicialmente marcadas con elipses. En la segunda foto apreciamos que en las zonas periféricas de la zona urbana tenemos relieve montañoso. Sin embargo, aunque el pueblo se eleva desde la costa vemos que esta libre de obstáculos ya que las montañas quedan detrás. Por tanto el desnivel que hay no debería suponer ningún problema en dicho entorno para cubrir la zona urbana si elegimos de forma adecuada la ubicación de las antenas.

1.7.1- Demografía.

Como hemos dicho anteriormente, es preciso conocer el número de usuarios potenciales en el municipio para conocer la carga teórica aproximada que vamos a tener en la red. Para obtener dicha información nos basamos en los datos obtenidos en la página del Instituto de Estadística de Cataluña.

Población	Llançà
Población. Por grupos de edad. 2012	
De 0 a 14 años	**717**
De 15 a 64 años	**3.326**
De 65 a 84 años	**912**
De 85 años y más	**150**
Total	**5.105**

Población	Llançà
Población ETCA (equivalente a tiempo completo anual). 2011	
Población residente	**5.140**
Población estacional ETCA	**1.844**
Total	**6.984**

Vemos que el principal grupo de usuarios potenciales los tenemos en la franja entre los 15 y los 64 años. También observamos el incremento estacional de población debido al turismo que habrá que tener en cuenta adicionalmente, ya que el acceso inalámbrico es también para los visitantes.

1.7.2.- Puntos de interés de acceso a la red (cobertura y ubicación)

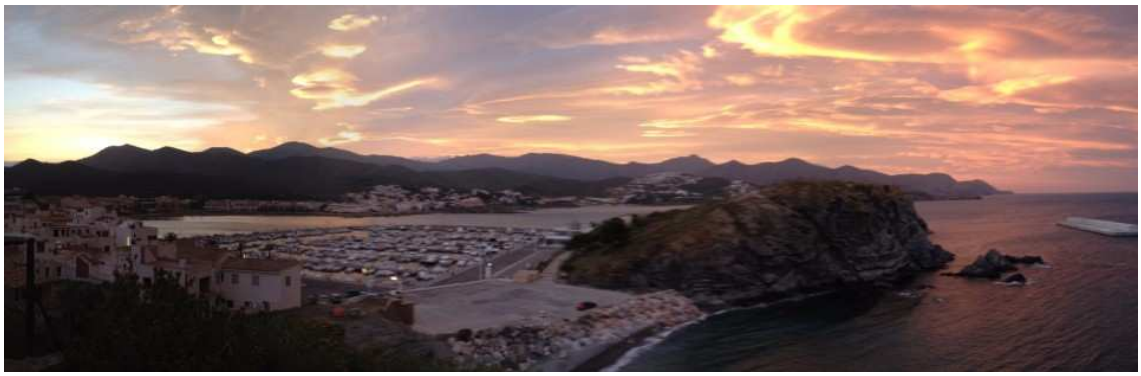
En el siguiente plano podemos ver una perspectiva general de la población:

Para catalogar los diferentes lugares de interés en los que sería interesante prestar servicio de cobertura para la población, dividimos en cuatro áreas diferenciadas.

AREA1: PLAYAS DE LA ZONA SUR

En esta área hay algunas playas con un tamaño y una densidad de ocupación en época vacacional suficientes como para justificar la instalación de un servicio de acceso a Internet. Consideramos puntos de interés:
Platja del Cau del Llop
Platja la Farella
Platja del Morer

AREA2: ZONA DEL PUERTO



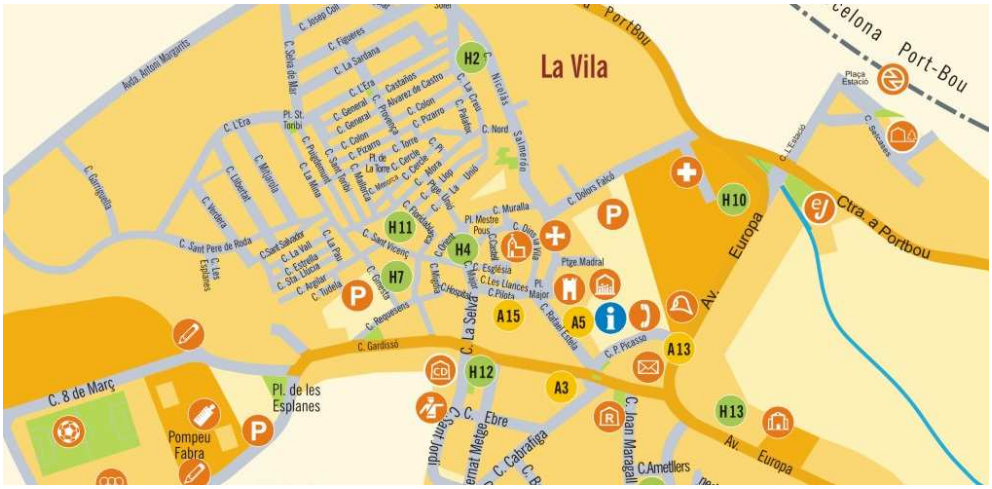
En el área del puerto hay muchos puntos de interés que deben disponer de cobertura.

Tenemos en primer lugar el club náutico, ubicado en la zona del malecón del puerto. En el club hay instalaciones de marcado carácter turístico que se verían revalorizadas con una conexión disponible en todo momento. Incluso el valor de los amarres del puerto puede verse incrementado por esta nueva posibilidad, por lo que la conexión podría dar un nuevo enfoque y aumentar las posibilidades del puerto deportivo.

En la misma zona encontramos las playa del puerto y L'Argilera de marcado carácter céntrico, con todo tipo de instalaciones turísticas. Siendo las playas más grandes y céntricas de la población deben contar con estos nuevos servicios para aumentar el atractivo turístico de Llançà.

Por lo tanto los puntos de interés de esta área serían:
Club náutico
Platja del Port
Platja de L'Argilera

AREA3: CENTRO DE LA POBLACIÓN



En esta área tendríamos varias zonas de mucho interés. Comenzamos por el centro de la población la plaza de la Libertad, centro neurálgico donde se ubican los monumentos históricos, el museo de la Acuarela, el ayuntamiento y las zonas comerciales y de restauración principales.

La zona del polideportivo, con sus instalaciones de usos múltiples y la zona de la estación, donde también está ubicada la oficina de turismo, son también sectores con necesidad de cobertura.

Puntos de interés:
Centro histórico: plaza de la libertad. Ayuntamiento y área monumental.
Zona polideportiva.
Estación del tren y oficina de turismo.

AREA4: PLAYAS DE LA ZONA NORTE

Puntos de interés:
Platja de Sota d'en Canals
Platja de Canyelles

1.8- Legislación vigente (Ley general de las telecomunicaciones).

Como hemos indicado anteriormente dado que vamos a proporcionar un acceso inalámbrico gratuito debemos tener en cuenta el marco legal en el que nos movemos (como se dijo anteriormente, está en curso la aprobación de unas modificaciones a la ley de 2003, sin embargo a fecha de realización de este proyecto, me regiré por la normativa vigente, la de 2003, por no estar vigente aún el anteproyecto actual).

Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (Publicado en: Boletín Oficial del Estado, núm. 264 de 4 de noviembre de 2003, páginas 38890 a 38924 (35 pags.)

Los puntos principales que debemos tener en cuenta son los siguientes:

Artículo 6. Requisitos exigibles para la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas.

"2. Los interesados en la explotación de una determinada red o en la prestación de un determinado servicio de comunicaciones electrónicas deberán, con anterioridad al inicio de la actividad, notificarlo fehacientemente a la Comisión del Mercado de las Telecomunicaciones en los términos que se determinen mediante real decreto, sometiéndose a las condiciones previstas para el ejercicio de la actividad que pretendan realizar. Quedan exentos de esta obligación quienes exploten redes y se presten servicios de comunicaciones electrónicas en régimen de autoprestación."

Artículo 8. Condiciones para la prestación de servicios o la explotación de redes de comunicaciones electrónicas.

"4. La explotación de redes o la prestación de servicios de comunicaciones electrónicas por las Administraciones públicas, directamente o a través de sociedades en cuyo capital participen mayoritariamente, se ajustará a lo dispuesto en esta ley y sus normas de desarrollo y se realizará con la debida separación de cuentas y con arreglo a los principios de neutralidad, transparencia y no discriminación. La Comisión del Mercado de las Telecomunicaciones podrá imponer condiciones especiales que garanticen la no distorsión de la libre competencia."

ANEXO I
Tasas en materia de telecomunicaciones
Tasa por reserva del dominio público radioeléctrico

"Las Administraciones públicas estarán exentas del pago de esta tasa en los supuestos de reserva de frecuencia del dominio público radioeléctrico para la prestación de servicios obligatorios de interés general sin contrapartida económica directa o indirecta, como tasas, precios públicos o privados, ni otros ingresos derivados de dicha

prestación, tales como los ingresos en concepto de publicidad. A tal efecto, deberán solicitar, fundadamente, dicha exención al Ministerio de Ciencia y Tecnología. Asimismo, no estarán sujetos al pago los enlaces descendentes de radiodifusión por satélite, tanto sonora como de televisión".

Además debemos tener en cuenta la siguiente circular en la que se determinan ciertos aspectos no indicados en la anterior ley, que determinan en que caso las administraciones públicas no necesitan informar a la CMT en caso de que no haga el papel de inversor privado. O cumpla ciertos requerimientos técnicos con los que se considera que se respeta la libre competencia.

Resolución de 18 de junio de 2010, de la Presidencia de la Comisión del Mercado de las Telecomunicaciones, por la que se publica la Circular 1/2010, de la Comisión del Mercado de las Telecomunicaciones, por la que se regulan las condiciones de explotación de redes y la prestación de servicios de comunicaciones electrónicas por las Administraciones Públicas.

"Con el objeto de que las Administraciones Públicas puedan determinar con facilidad cuándo su actuación no afecta a la libre competencia por respetar el principio del inversor privado en una economía de mercado, esta Circular concreta los criterios que va a aplicar la Comisión del Mercado de las Telecomunicaciones para su comprobación."

" Se considera autoprestación y, por lo tanto, no será necesario llevar a cabo la notificación prevista en el artículo 6.2 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones a la Comisión del Mercado de las Telecomunicaciones, la explotación de redes y la prestación de servicios de comunicaciones electrónicas por una Administración Pública para la satisfacción de sus necesidades, esto es, las vinculadas al desempeño de las funciones propias del personal al servicio de la Administración Pública de que se trate y que contribuyan al cumplimiento de los fines que le son propios"

"En los supuestos en que aprovechando la misma infraestructura a través de la cual la Administración Pública se presta los servicios en régimen de autoprestación, se proveen servicios, mayoristas o minoristas, a terceros, la Administración Pública será considerada, en cuanto a estos últimos, explotadora de redes o prestadora de servicios de comunicaciones electrónicas a terceros, quedando por tanto sujeta a lo establecido en la presente Circular."

ANEXO DE LA CIRCULAR

Explotación de redes y prestación de servicios de comunicaciones electrónicas que no afectan a la competencia.

Se entiende que no afectan a la competencia los siguientes servicios:

1. El servicio de acceso a Internet limitado a las páginas web de las Administraciones que tengan competencias en el ámbito territorial en que se preste este servicio.

2. Servicio general de acceso a Internet en bibliotecas en tanto que resulte indispensable para cumplir sus fines y siempre que los usuarios acrediten su vinculación con el servicio mediante algún documento que permita su identificación.

3. Servicio general de acceso a Internet en centros de fomento de actividades docentes o educativo-culturales no incluidos en el artículo tercero de esta Circular, en tanto que resulte indispensable para cumplir sus fines y siempre que los usuarios acrediten su vinculación con el servicio mediante algún documento que permita su identificación.

4. La explotación de redes inalámbricas que utilizan bandas de uso común y la prestación de servicios de comunicaciones electrónicas disponibles para el público a través de las mismas siempre que la cobertura de la red excluya los edificios y conjuntos de edificios de uso residencial o mixto

En términos generales, se entiende por edificio o vivienda de uso residencial aquél cuyos bienes de dominio particular se encuentren destinados a la vivienda de personas y por edificio de uso mixto aquel cuyos bienes se destinan a actividades de diferente naturaleza, tales como oficina, comercio o vivienda. y se limite la velocidad red-usuario a 256 Kbps.

Por tanto serían necesarios el siguiente trámite en caso de cumplir el papel de inversor privado: Ponerlo en conocimiento de la CMT y darse de alta en el registro general de operadores. Sólo en el caso de que lo ofreciera en régimen de autoprestación como indica la circular, estaría exento de realizar dicho trámite, además de cumplir los puntos del anexo de dicha circular.

El último punto a tener en cuenta en caso de que almacenemos información de los usuarios conectados aunque sea temporalmente, es la LOPD (ley orgánica de protección de datos de carácter personal).

1.9.- Planificación del TFC.

La planificación se seguirá en función a las fechas propuestas durante el semestre y que se detallan en el siguiente calendario temporal realizado con Microsoft Project 2010.

Es difícil determinar la duración de cada una de las etapas para la realización de cada una de las partes a desarrollar. Por tanto en este estado inicial del TFC, las tareas y sus fechas propuestas en el Project presentado, son bastante estimativas y pueden diferir a lo largo del tiempo por exigencias o cambios debidos a alguna mejora o petición de modificación del alcance del TFC por parte del tutor o mía, o debido a algún retraso imprevisto debido a cuestiones personales.

Diagrama de Gantt

	Nombre de tarea	Duración	Comienzo	Fin
1	**TFC-Diseño de una red telemática**	**83 días**	**mié 27/02/13**	**vie 21/06/13**
2	**PAC1-Plan de trabajo**	**8 días**	**lun 04/03/13**	**mié 13/03/13**
3	Validar temática del TFC con el consultor	3 días	lun 04/03/13	mié 06/03/13
4	Descripción del TFC, objetivos y planificación.	6 días	mié 06/03/13	mié 13/03/13
5	Entrega del plan de trabajo.	0 días	mié 13/03/13	mié 13/03/13
6	**PAC2.**	**30 días**	**jue 14/03/13**	**mié 24/04/13**
7	Legislación	3 días	jue 14/03/13	lun 18/03/13
8	Estudio población, topografía, demografía y puntos de interes.	4 días	jue 21/03/13	mar 26/03/13
9	Estudio tecnologías WiFi-Wimax	7 días	mié 27/03/13	jue 04/04/13
10	Estudio de cobertura y ubicación de los puntos de acceso a la red	12 días	vie 05/04/13	lun 22/04/13
11	Entrega de PAC2	1 día	mié 24/04/13	mié 24/04/13
12	**PAC3.**	**24 días**	**vie 26/04/13**	**mié 29/05/13**
13	Esquema del mapa de red	6 días	vie 26/04/13	vie 03/05/13
14	Equipamientos de acceso a la red y descripción	4 días	lun 06/05/13	jue 09/05/13
15	Simulación mediante software de la cobertura.	7 días	vie 10/05/13	lun 20/05/13
16	Estimación de los costes.	3 días	mar 21/05/13	jue 23/05/13
17	Glosario, bibliografía y anexos.	2 días	vie 24/05/13	lun 27/05/13
18	Entrega de PAC3	1 día	mié 29/05/13	mié 29/05/13
19	**Memoria, presentación.**	**17 días**	**jue 30/05/13**	**vie 21/06/13**
20	Entrega de la memoria.	13 días	jue 30/05/13	sáb 15/06/13
21	Entrega de la presentación.	5 días	lun 17/06/13	vie 21/06/13

2. Definiciones técnicas.

2.1.- Características WiFi.

Wi-Fi es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

Existen diversos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11 aprobado. Son los siguientes:

Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbit/s , 54 Mbit/s y 300 Mbit/s, respectivamente.

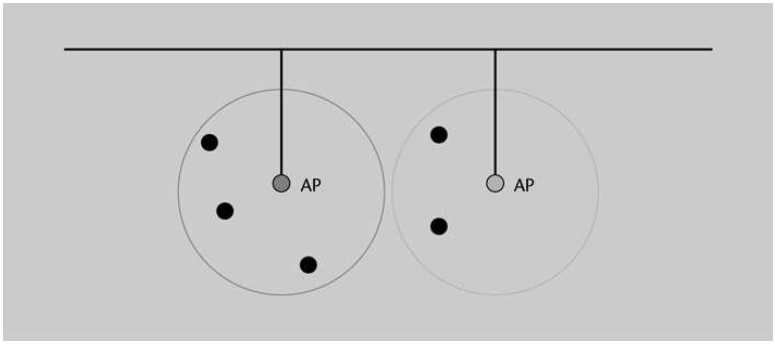
En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y,

además, no existen otras que la estén utilizando, por lo tanto existen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2.4 GHz (aproximadamente un 10%), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

Existe un primer borrador del estándar IEEE 802.11n que trabaja a 2.4 GHz y a una velocidad de 108 Mbit/s. Sin embargo, el estándar 802.11g es capaz de alcanzar ya transferencias a 108 Mbit/s, gracias a diversas técnicas de aceleramiento. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados Pre-N.

- **Arquitectura:**

La arquitectura 802.11 consta de estaciones (figura siguiente), y una de ellas puede hacer funciones de AP (access point). Un AP es una estación que permite el acceso a otras redes. Una BSS (basic service set) es el conjunto de estaciones conectadas a un mismo AP. Un ESS (extended service set) es el conjunto de BSS interconectadas. Dependiendo de la necesidad se pueden definir coberturas disjuntas (para cubrir más área) o solapadas (para mejorar el servicio en un área). Si queremos que varios AP formen parte de la misma red, les pondremos el mismo SSID (identificador de ESS o service set identifier). La medida de seguridad más básica cuando un usuario quiere acceder a una red es mirar su SSID.



- **Acceso al medio**

Cuando varias estaciones quieren acceder al medio se utiliza la técnica CSMA/CA para resolver las colisiones. CSMA (carrier-sense multiple access): el mecanismo carrier-sense determina si la energía de señal en un determinado ancho de banda supera un cierto umbral.

CA (colision avoidance): la estación destino confirma cada trama que recibe (eso lo hace enviando un ACK inmediatamente después de cada trama recibida). Si el emisor no recibe el ACK, se retransmitirá la trama.

Mecanismo CSMA/CA del 802.11.

Hay dos modos de transmisión:

• DCF (distributed coordination function)

• PCF (point coordination function) Hay un Access Point, que hace pollings a las estaciones (tareas de coordinación). Se tiene que configurar.

- **Estándares y características.**

En la siguiente tabla tenemos los estándares 802.11 más importantes y sus características:

Normas (capa física y de acceso al medio)	Velocidad transmisión máxima (Mbps)	*Throughput* máximo típico (Mbps)	Numero máximo de redes colocalizadas	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 (40 MHz)*	>300 Mbps	>100 Mbps	1 (2.4 GHz) 7 (5.7 GHz)	5 GHz	120 m	300 m
IEEE 802.11n (20 MHz)*	144 Mbps	74 Mbps	3 (2.4 GHz) 14 (5.7 GHz)	2.4 GHz y 5 GHz	120 m	300 m

Las notas UN-85 y UN-128 del CNAF (Cuadro Nacional de Atribución de Frecuencias) determinan las condiciones de uso de las bandas WiFi:

a) **UN-85**

• De 2.400 a 2.483,5 MHz.
• Potencia hasta 100 mW PIRE.
• Aplicaciones de interiores (o exteriores de corto alcance).

b) **UN-128**

• de 5.150 a 5.350 MHz:
– Sólo en interiores.
– Potencia entre 30 mW y 200 mW, dependiendo de si hay control de potencia (TPC) y/o selección dinámica de frecuencia (DFS).

• de 5470 a 5.725 MHz:
– Interiores y exteriores.
– Potencia hasta 1 W PIRE (con TPC y DFS).

En 2,4 GHz hay más interferencias que en 5,8 GHz. En cambio, cuanta más frecuencia, es necesaria la visión directa. Por eso se permite emitir con más potencia a 5,8 GHz.

Hay que tener presente que a distancias máximas se utilizará la velocidad mínima (y más robusta ante errores).

El estándar 802.11 define trece canales separados 5 MHz en la banda de 2,4 GHz. Un canal 802.11b tiene un ancho de 11 MHz a derecha e izquierda de la frecuencia central (total: 22 MHz). Por lo tanto, en un mismo espacio sólo podremos tener tres canales sin solapamiento.

Según lo anterior, en una misma área podemos tener sin problemas 3 x 11 Mbps, seleccionando los canales 1, 6 y 11 (este último viene por defecto). Con cierto solapamiento podríamos tener cinco canales (1, 4, 7, 10, 13). Observamos que con tres canales podemos hacer una estructura "celular" para que dos BSS con la misma frecuencia no se toquen.

En cambio, el estándar 802.11a define ocho canales de 25 MHz (pueden convivir diferentes operadores en una misma área). En los 25 MHz, y gracias a OFDM podemos transmitir 54 Mbps.

Las modulaciones que utilizan estos estándares son las siguientes:

802.11: tiene dos versiones, la DSSS (1 y 2 Mbps) y el FHSS (1 y 2 Mbps). La FHSS está obsoleta. La DSSS funciona como el 802.11b de 1 Mbps y 2 Mbps que comentamos a continuación.

802.11b: tiene dos versiones, la DSSS (1, 2, 5,5 y 11 Mbps) y la FHSS (1 y 2 Mbps). La FHSS está obsoleta. La DSSS se comporta de manera diferente dependiendo de la velocidad.

802.11a: aplica OFDM sobre cada canal de 20 MHz y lo divide en cuarenta y ocho portadoras (decimos que el símbolo OFDM es de 48 bits). Se comporta de manera diferente dependiendo de la velocidad.

802.11g: es la evolución de 802.11b. Este utiliza la banda de 2,4 Ghz (al igual que 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s. Es compatible con el estándar b y utiliza las mismas frecuencias. Existe una variante llamada 802.11g+ capaz de alcanzar los 108Mbps de tasa de transferencia. Generalmente sólo funciona en equipos del mismo fabricante ya que utiliza protocolos propietarios.

802.11n: es una propuesta de modificación al estándar IEEE 802.11-2007 para mejorar significativamente el rendimiento de la red más allá de los estándares anteriores, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps.

Actualmente la capa física soporta una velocidad de 300Mbps, con el uso de dos flujos espaciales en un canal de 40 MHz. Dependiendo del entorno, esto puede traducirse en un rendimiento percibido por el usuario de 100Mbps. El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 Ghz y 5 Ghz. Es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada. Añade el uso de Multiple-Input Multiple-Output (MIMO). MIMO usa múltiples antenas transmisoras y receptoras para mejorar el rendimiento del sistema.

- **Escucha del canal.**

Cada BSS transmite paquetes beacon con información de red. La escucha puede ser pasiva o activa:

• Escucha pasiva (escucha de beacons): Cuando detectamos un beacon con el SSID que queremos, negociamos la incorporación.

• Escucha activa (los terminales siempre escogen la mejor EB).

- **Autenticación (control de accesos):**

• *Con clave compartida (shared key authentication*): todas las estaciones de un BSS la han conocido por un canal seguro (normalmente, de forma manual). No es seguro, porque cifra una respuesta conocida.

• *Sistema abierto (open system authentication):* no hay contraseña y sólo se indica la intención de acceder. Es el más sencillo (y más inseguro).

También se puede autenticar utilizando la dirección de dispositivo (MAC). El AP tendrá una lista con las MAC permitidas. Pero alguien nos puede escuchar la MAC.

2.2- Características Wimax.

La norma IEEE 802.16 (wireless metropolitan area networks), publicada en diciembre del 2001, sirvió para fomentar la operatibilidad entre los sistemas LMDS, ya que define un estándar para redes metropolitanas (LMDS era una tecnología propietaria, no un estándar).

En las frecuencias del 802.16 (entre 10 GHz y 66 GHz), es necesaria visión directa. En enero del 2003 apareció el 802.16a, que trabajaba entre 2 y 11 GHz. Como la frecuencia es menor, a veces podemos tener cobertura con visión directa parcial. Este estándar también se llama WiMax (o 802-16-2004).

WiMax está pensado para reducir el vacío digital que limita la difusión de información de banda ancha en zonas de baja densidad. WiFi no podía hacer eso porque, entre otras cosas:

- Tiene un acceso al medio poco eficiente (en WiFi, si un usuario quiere transmitir mientras lo hace otro, debe esperarse). No permite calidad de servicio (a no ser que se desarrolle el 802.11e).
- Sólo está pensado para bandas libres (nos pueden interferir).
- Ámbito reducido (local).

Las principales características de WiMax, que lo hacen apropiado para una red metropolitana:

Modulación adaptativa. Si el canal tiene un buen comportamiento (pocas pérdidas), la velocidad aumenta porque utilizamos una modulación que lleva más bits en cada símbolo. Por ejemplo, si la relación señal- ruido (SNR) es de 6 dB, utilizamos BPSK, pero si la SNR llega a 9 dB, entonces utilizamos QPSK.

Banda frecuencial. Se puede trabajar en banda libre a 5,4 GHz, pero con poca potencia (poca cobertura) y con visión directa. Pero también hay una banda licenciada en 3,5 GHz donde no es imprescindible la visión directa.

Elementos. De manera similar a las unidades de abonado y a los puntos de acceso WiFi, aquí tenemos estaciones base (BS) y unidades de usuario (CPE).

Perfiles. Se definen cinco:

– *SC (single carrier):* entre 10 y 66 GHz, con licencia y visión directa (LOS) para hacer enlaces punto a punto (PaP).
– SCa: entre 2 y 11 GHz, con licencia y LOS para hacer enlaces PaP.
– OFDM: utiliza FFT de 256 puntos para tener enlaces punto-multipunto (PmP) con licencia sin necesidad de visión directa (NLOS).
– OFDMA: utiliza FFT de hasta 2.048 puntos para tener enlaces punto-multipunto (PmP) con licencia sin necesidad de visión directa (NLOS).
– HUMAN: abarca los tres perfiles anteriores pero en banda libre.

Antenas. Puede utilizar antenas adaptativas que controlan el haz en la dirección de las CPE.

Diversidad. En recepción utiliza diversidad MRC (ved el módulo 1). En transmisión también utiliza dos antenas (si en el instante t se transmite la información X en la antena 1 e Y en la antena 2, en el instante t + 1 se transmite Y en la antena 1 y X en la 2).

Selección dinámica de frecuencia (DFS). Si detecta interferencias, tiene que cambiar de frecuencia (obligatorio si se trabaja en banda libre, para evitar interferir los radares).

Permite calidad de servicio (QoS). Cada trama es para un CPE. Como WiMax está orientado a la conexión, permite QoS. Los enlaces ascendente y descendente pueden ser asimétricos, pero en la misma trama (en modo TDD).

- **Topologías de red.**

PaP. Podemos conseguir enlaces punto a punto entre 20 Mbps y 300 Mbps a distancias de 2 km (visión directa). Una aplicación de esta topología es alimentar enlaces PmP.

PmP. En enlaces punto a multipunto disponemos de antenas sectoriales en la BS (en el enlace ascendente) donde cada sector apunta a una unidad de usuario. Las unidades de usuario disponen de antenas directivas.

Mesh. Como su nombre indica, en una estructura mallada hay varias BS cubriendo una zona, de manera tal que la comunicación entre un CPE y una BS lejana se puede hacer mediante saltos entre BS intermedias.

Será objeto de estudio para este Tecla banda de 5.4 Ghz por ser una banda libre y la topología mallada (Mesh).

2.3 Seguridad en redes WiFi (estándar 802.11)

Cuando hablamos de seguridad, hay dos aspectos que debemos abordar: la autenticación y el cifrado.

1) Autenticación (control de accesos):

• Con clave compartida (shared key authentication): todas las estaciones de un BSS la han conocido por un canal seguro (normalmente, de forma manual). No es seguro, porque cifra una respuesta conocida.

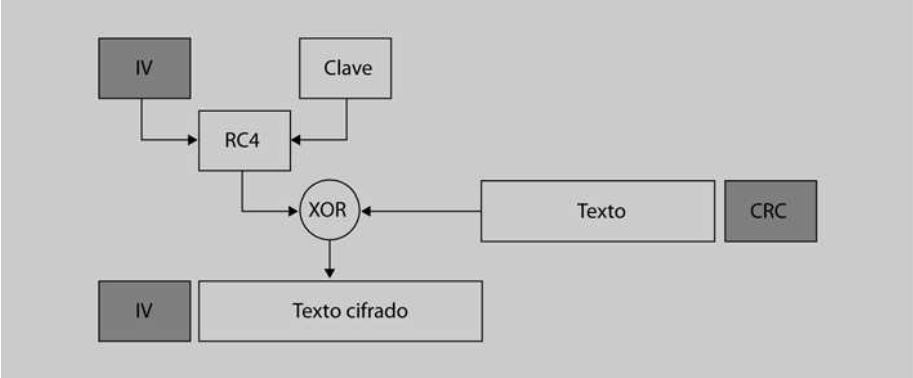
• Sistema abierto (open system authentication): no hay contraseña y sólo se indica la intención de acceder. Es el más sencillo (y más inseguro). También se puede autenticar utilizando la dirección de dispositivo (MAC). El AP tendrá una lista con las MAC permitidas. Pero alguien nos puede escuchar la MAC.

2) Cifrado (hay que tener en cuenta que, por defecto, no se cifra):

El método de cifrado más básico es el WEP, que comentamos a continuación. WEP (wired equivalente privacy) hace un cifrado de 64 bits (estándar) o de 128-256 bits. Cuantos más bits mejor, pero no se puede aumentar más, porque, si incrementamos la longitud, hace falta más CPU.

En WEP:

• La clave es estática y simétrica (por lo tanto, no hay gestión de claves).
• Se cifra con RC4 (algoritmo criptográfico simétrico).
• Se protege la integridad de los datos (MIC, message integrity code) con CRC- 32 (el cifrado pretende evitar que se vean los datos; la integridad pretende evitar que se cambien los datos durante el camino).



En la figura anterior tenemos la estructura de cifrado en WEP. Las claves WEP son de 40 + 24 bits o 104 + 24 bits, donde los 24 bits son el vector de inicialización (IV). La clave debe ser conocida por todos. Se puede poner manualmente o se puede generar automáticamente. El CRC es independiente de la clave y del IV.

Los mecanismos de seguridad de WEP son muy simples (e inseguros). Esta técnica presenta muchas vulnerabilidades (clave estática, vector de inicialización que se repite y no se cifra,...) que hacen que hoy en día una protección WEP pueda ser violada muy fácilmente.

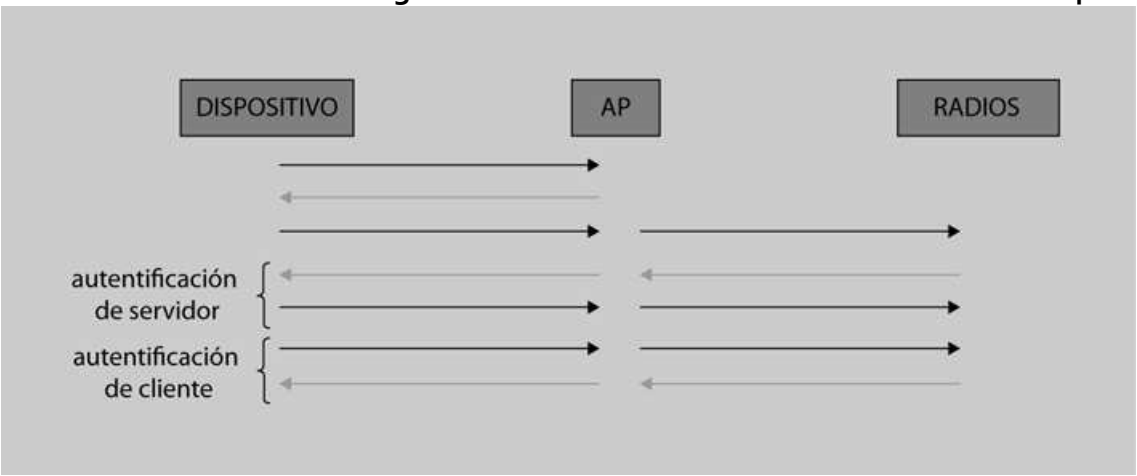
El WEP+ (WPA, wireless protected area), que es compatible con WEP y apareció en noviembre del 2002, incorpora:

a) Autenticación con 802.1x + EAP.

Puede utilizarse un servidor RADIUS como servidor de autenticación (todos los AP piden el inicio de sesión-contraseña, login-password, a este servidor; antes poníamos la contraseña en todos los AP).

La comunicación entre servidor y AP se hace con protocolos EAP (extensible authentication protocol). Algunos protocolos EAP existentes son TLS, TTLS, LEAP y PEAP.

La autenticación es recíproca entre cliente y servidor (y al revés).



Autenticación 802.1x

Si no disponemos de servidor, también podemos introducir unas claves (PSK, pre-shared key) en cada elemento.

b) Claves dinámicas (en WEP eran estáticas; conocer una implica conocerlas todas), gestionadas con el protocolo de recálculo de claves TKIP (temporal key integrity protocol):

– La primera clave es el punto de partida para las siguientes.
– Seguimos cifrando con RC4 y una clave de 128 bits.
– Mecanismo de integridad MIC (también llamado Michael) con claves de 64 bits. Si hay dos errores en un segundo, borra las claves, se disocia y reasocia (supone un ataque).

También se pueden añadir otros mecanismos de seguridad en red, como podría ser una contraseña para acceder a ciertos servicios, etc.

El 802.11i (también llamado WPA2), aprobado en junio del 2004, se diferencia de WPA en lo siguiente:
– WPA2 utiliza AES (advanced encryption standard) para cifrar, en lugar de RC4. Las claves pueden ser de 128, 192 ó 256 bits.
– WPA2 utiliza un mecanismo de integridad de tipo CCMP (algoritmo de cifrado CCMP (AES) (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol + Advanced Encription Standard).

Entre sus defectos, citaremos que TKIP presenta ciertas vulnerabilidades, ya que permite el acceso a algunos de los paquetes que van desde el AP hasta los terminales de red.

** No es objeto de estudio dentro de este TFC el profundizar más en los métodos de encriptación y sus algoritmos asociados pero sí el considerarlos para la toma de decisión del tipo de tecnología a utilizar.

En la siguiente tabla podemos ver de manera esquemática las características de los tres estándares de seguridad:

	WEP	WPA	WPA2 o 802.11i
Autenticación	Muy básica	802.1x + EAP	802.1x + EAP
Gestión de claves	No hay (claves estáticas)	EAP	EAP
Cifrado	RC4	RC4	AES
Integridad	CRC-32	Michael	CCMP

Hay que ser conscientes de que la seguridad total no existe, pero deben aplicarse algunos de los mecanismos de seguridad. Todavía hoy en día hay un porcentaje muy alto de redes que no aplican ninguna protección.

2.4 Seguridad en redes WiMAX (estándar 802.16.2009)

WiMAX basa su sistema de seguridad en los principios de Autenticación y Cifrado, los cuales hacen de ella una tecnología a día de hoy prácticamente invulnerable.

Autenticación.

El estándar IEEE 802.16-2009 define dos filosofías de autenticación:
• OSA (Open System Authentication): el cliente realiza una solicitud de autenticación asociada a su dirección MAC, a lo que sigue una respuesta de la Estación Base (en adelante, BS) con la aceptación o denegación. La BS realiza únicamente y de forma opcional un filtrado por dirección MAC.
• SKA (Shared Key Authentication): se utilizan en el proceso claves compartidas que ambos extremos deberán conocer para garantizar una autenticación más segura. De aquí en adelante comentaremos estos mecanismos de autenticación.

Para la autenticación mediante claves compartidas, WiMAX define el protocolo PKM (Privacy Key Management) para que una Estación de Usuario (en adelante, SS) pueda intercambiar claves y obtener autorización de la BS. PKM también se encarga de otras cuestiones relacionadas como el refresco de las claves, la re-autorización periódica,... El proceso de Autenticación entre BS y SS se puede describir de forma simple de la siguiente forma:

1) Una SS envía un mensaje PKM (Privacy Key Management) solicitando autenticación a la BS e incluyendo su certificado digital X.509. Este certificado es único por equipo e infalsificable, con lo que le define de forma unívoca y evita los ataques por suplantación de MAC.
2) La BS procede a autenticar y a verificar el certificado comprobando la firma digital del fabricante incluida en el certificado.

3) Si el certificado X.509 es aceptado, la BS genera la clave de autenticación (AK) y la cifra mediante la clave pública de 1024 bits contenida en el propio certificado X.509.

Cifrado.

Después de que la BS autorice a la SS, son necesarios también mecanismos de cifrado para velar por la confidencialidad y la integridad de los datos. Para ello, la SS envía a la BS una solicitud de claves de cifrado llamadas TEKs (Traffic Encryption Keys), que son enviadas por la BS en un mensaje de respuesta. Estos mensajes a su vez están cifrados con una clave conocida por ambas partes. El algoritmo empleado para el cifrado de las TEKs puede ser de tipo 3DES (Triple Data Encryption Standard), AES (Advanced Encryption Standard), o RSA. Una vez conocidas las TEKs, diversas técnicas pueden ser utilizadas para cifrar los datos: CBC(DES), CBC (AES), CTR(AES), CCM(AES).

Algunas de las ventajas de los mecanismos de cifrado que implementa WiMAX respecto a los de otras tecnologías son:

- Los algoritmos empleados son muy robustos
- Soportan generación de claves dinámicas con tiempos de vida variables
- Permiten realizar un cifrado independiente para cada flujo de datos

Todo esto se realiza con el objetivo de garantizar la confidencialidad en las redes WiMAX.

3. Diseño e implementación de la red.

3.1- Bandas de frecuencia utilizadas.

Las bandas de frecuencia usadas en este proyecto son las de 2.4 GHz y 5.4 GHz que corresponden a las notas UN-85 y UN-128 respectivamente de la orden en vigencia actual del Ministerio de Industria **(Orden IET/787/2013, de 25 de abril (CNAF 2013) que deroga a las anteriores vigentes (Orden ITC/332/2010, de 12 de febrero (CNAF 2010) y Orden ITC/658/2011, de 18 de marzo, por la que se modifica la anterior).**

UN - 85 RLANs y datos en 2400 a 2483,5 MHz

Podrá ser utilizada también para los siguientes usos de radiocomunicaciones bajo la consideración de uso común:

a) Sistemas de transmisión de datos de banda ancha y de acceso inalámbrico a redes de comunicaciones electrónicas incluyendo redes de área local.

Estos dispositivos pueden funcionar con una potencia isotrópica radiada equivalente (PIRE) máxima de 100 mW conforme a la Decisión de la Comisión 2011/829/UE y la Recomendación CEPT ERC/REC 70-03, anexo 3.

Además, la densidad de potencia (PIRE.) será de 100 mW/100 kHz con modulación por salto de frecuencia y de 10 mW/MHz con otros tipos de modulación. En

ambos casos, se deberán utilizar técnicas de acceso y mitigación de interferencias con rendimiento al menos equivalente a las técnicas descritas en las normas armonizadas según la Directiva 1999/5/CE.

En cuanto a las características técnicas de estos equipos, la norma técnica de referencia es el estándar ETSI EN 300 328 en su versión actualizada.

b) Dispositivos genéricos de baja potencia en recintos cerrados y exteriores de corto alcance, incluyendo aplicaciones de video.

La potencia isotrópica radiada equivalente máxima será inferior a 10 mW conforme a la Decisión de la Comisión 2011/829/UE y la Recomendación CEPT ERC/REC 70-03, Anexo 1, siendo la norma técnica de referencia el estándar ETSI EN 300 440.

UN – 128 RLANs en 5 GHz

Aplicaciones de uso común en las bandas de 5150-5350 MHz y 5470-5725 MHz. Espectro armonizado según la Decisión 2005/513/CE, modificada por la Decisión 2007/90/CE, en la banda de 5 GHz para sistemas de acceso inalámbrico a redes de Comunicaciones electrónicas, incluidas las redes de área local (WAS/RLAN).

Las bandas de frecuencia indicadas seguidamente podrán ser utilizadas por el servicio móvil en sistemas y redes de área local de altas prestaciones, de conformidad con las condiciones que se indican a continuación.

Los equipos utilizados deberán disponer del correspondiente certificado de conformidad de cumplimiento con la norma EN 301 893 o especificación técnica equivalente.

***Banda 5470 - 5725 MHz**:*

Esta banda puede ser utilizada para sistemas de acceso inalámbrico a redes de comunicaciones electrónicas, así como para redes de área local en el interior o exterior de recintos, y las características técnicas deben ajustarse a las indicadas en la Decisión de la CEPT ECC/DEC(04)08. La potencia isotrópica radiada equivalente será inferior o igual a 1 W (PIRE). Este valor se refiere a la potencia promediada sobre una ráfaga de transmisión ajustada a la máxima potencia. Adicionalmente, en esta banda de frecuencias el transmisor deberá emplear técnicas de control de potencia (TPC) que permitan como mínimo un factor de reducción de 3 dB de la potencia de salida. En caso de no usar estas técnicas, la potencia isotrópica radiada equivalente máxima (PIRE) deberá ser de 500 mW (PIRE.).

Estas utilizaciones son de uso común, por lo que no se garantiza la protección frente a otros servicios legalmente autorizados ni puede causar perturbaciones a los mismos. Los sistemas de acceso sin hilos incluyendo RLAN que funcionen en las bandas 5250- 5350 MHz y 5475-5725 MHz deberán utilizar técnicas de mitigación que proporcionen al menos la misma protección que los requisitos de detección, operación y respuesta descritos en la norma EN 301 893.

*He omitido un rango en la norma UN-128 un rango que no usaré.

3.2- Comparativa entre sistemas WiMAX trabajando tanto en Banda Libre como en Banda Licenciada, para el caso particular de un entorno rural.

Esta comparativa se hace para justificar el uso de la banda libre en lugar de la licenciada en este proyecto:

Banda licenciada:

El equipamiento de infraestructura (BS - Estación Base) en la banda de 3,5 GHz se suele caracterizar por los siguientes aspectos:

- Ofrecen la posibilidad de altas potencias de transmisión al carecer esta banda de limitación de potencia. Esta mayor potencia de transmisión se consigue a cambio de un importante incremento en el coste del equipamiento.
- El ancho de canal más empleado es el de 3,5 MHz, lo que permite una capacidad máxima a nivel físico de 13.1 Mbps (ráfaga 64QAM-3/4). Mayores anchos de banda no son viables debido a la escasez de espectro y a la necesidad de reutilización de frecuencias, por lo que la mayor parte de las estaciones base sólo soportan ese ancho de banda.
- Las estaciones base pueden operar en modo Full-Duplex, lo que teóricamente duplica la capacidad, a cambio de un importante aumento de coste debido al uso de duplexores. En la realidad, para aplicaciones de acceso radio en banda ancha, el ancho de banda no se duplica, ya que la demanda de tráfico ascendente es muy inferior a la de tráfico descendente.

Banda libre:

Para el caso de operar en banda libre (5475—5725 MHz en Europa), las características del equipamiento se resumen a continuación:

- La potencia de transmisión suele ser baja, ya que está limitada por aspectos regulatorios, por lo que el equipamiento suele tener una arquitectura ligera en la que el coste se ha optimizado.
- La gran disponibilidad de espectro (200 MHz) permite el uso de anchos de canal mayores, siendo 10 MHz el ancho de banda más empleado, lo que permite una capacidad máxima a nivel físico de 37.7 Mbps (ráfaga 64QAM-3/4).
- El método de duplexado es siempre TDD, lo que obliga a repartir el throughput disponible entre tráfico ascendente y descendente, pero permite establecer una asimetría en el tráfico ascendente/descendente que se adapte a la demanda concreta, lo que se traduce en un mayor aprovechamiento del espectro.

Tras lo expuesto en los puntos anteriores, se observa que la principal diferencia radica en la potencia y espectro disponible:

Potencia (afecta al coste): Mayor potencia implica mayor alcance, y en 3,5 GHz se puede optar a equipamiento de alta potencia (alto coste).

Espectro (no afecta al coste): Mayor disponibilidad de espectro implica mayor capacidad. La banda de libre de 5,6GHz permite anchos de banda de 10 MHz, mientras que en 3,5 GHz se limita a 3,5 MHz.

El operador deberá elegir básicamente entre conseguir una mayor potencia con canales de 3,5 MHz, o tener canales de 10 MHz con menor potencia.

Tras este estudio o comparativa de ambas bandas podemos concluir que para el escenario que se plantea en este proyecto el rendimiento de la banda libre es mayor que el de la banda licenciada. Si los usuarios se sitúan a distancias inferiores a 25 km, el rendimiento del sistema en banda libre es superior.

Aunque no pueda quedar clara esta última afirmación, con el ejemplo práctico que se puede consultar en el siguiente documento, que se puede extraer del enlace indicado en la bibligrafía, se puede justificar tal afirmación:

(WiMAX vs WiFi en enlaces PtP en banda libre, Enero 2010).

3.3- Cálculos estimativos de uso de la red inalámbrica.

Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares en 2012 realizada por el INE.

Uso de Internet en los últimos 3 meses por características demográficas y redes utilizadas al conectarse a Internet en ese periodo con un dispositivo móvil fuera de la vivienda habitual o centro de trabajo

Cualquier tipo de dispositivo móvil: Vía red inalámbrica (p.ej., WiFi)							
Total Personas	Edad: De 16 a 24 años	Edad: De 25 a 34 años	Edad: De 35 a 44 años	Edad: De 45 a 54 años	Edad: De 55 a 64 años	Edad: De 65 a 74 años	Hábitat: Menos de 10.000 habitantes
44,0	67,4	52,3	39,7	32,5	24,8	16,1	40,3

Fuente: Instituto Nacional de Estadística

Como podemos ver en dicho estudio podemos hacer un cálculo estimativo de las necesidades de ancho de banda para nuestra población, teniendo en cuenta las características demográficas presentadas anteriormente y cruzándolos con estos porcentajes.

Vemos que el rango de edades que nos interesa se encuentra localizado principalmente entre 15 y 64 años. Según cálculos de 2012, la franja en esta edad supone en Llança el 65% de la población (3326 habitantes), sin embargo lo consideraremos con el porcentaje similar de la población estacional en periodo

vacacional, considerando que las proporciones de edades se mantienen, ya que tendremos que cubrir esta demanda (65% de 6984 habitantes, 4540 habitantes).

Vemos que en el total nacional un 44% de la población hace uso de dispositivos móviles, 40% si nos ceñimos a poblaciones de menos de 10000 habitantes, como es nuestro caso. Para no diseñarlo con un ancho de banda insuficiente consideraremos el 50% de la población en periodo vacacional, 2270 habitantes.

Sabemos por diseños de redes similares que los usuarios no están todos conectados simultáneamente y se suele considerar usualmente un porcentaje del 10% de la población objetivo. Es decir, unos 227 usuarios. Redondearemos a un 15%, 341 usuarios.

Teniendo en cuenta que tendremos una limitación de velocidad de 256 Kbps por usuario como hemos indicado anteriormente nos da un ancho de banda total de:
314 x 256 Kbps = 87296 Kbps = 87 Mbps

3.4 Elección del ISP.

Para proporcionar dicho caudal he consultado la cobertura con el operador con mayor presencia, que es Movistar aunque se podrían barajar otras opciones. La cobertura que nos ofrece es de ADSL y VDSL. Con VDSL nos ofrece 30 Mbps por línea por lo que tendríamos suficiente con 3 líneas (90 Mbps) ya que hemors redondeado los porcentajes al alza. No obstante se podrían considerar contratar 4 para evitar posibles saturaciones en la red en caso de un aumento de usuarios en el futuro (120 Mbps).

He optado además por la opción de líneas residenciales minoristas ya que el ayuntamiento por el momento no se va a dar de alta como operador al proporcionar el servicio de acceso gratuito y proporcionar el ancho de banda dentro de los márgenes legales.

Tendríamos la opción de contratar circuitos de mayor capacidad y con mayor tráfico garantizado a diferencia de las líneas residenciales, sin embargo, como se puede apreciar en las tablas de precios de Movistar, el coste "mensual" es demasiado elevado si no consideramos cobrar por el servicio a los usuarios (a pesar de tener un descuento del 10% por el área geográfica ya que además hay un coste asociado a la instalación de cada circuito que no está reflejado en la tabla de la figura.

TABLA I: Cuotas de abono mensual (€/mes) Servicio Transporte Metropolitano

Velocidad	Circuito hasta 10 km	Incremento por km adicional a 10km (máximo 30 km adicionales)
2Mbps	428	25
34Mbps	2375	125
155Mbps	5130	290

3.5 Administración de la red, equipamiento.

Teniendo en cuenta las consideraciones expuestas anteriormente sobre las siguientes cuestiones:

- Seguridad en la red.
- Autenticación.
- Limitación del ancho de bando por usuarios.
- Líneas proporcionadas por el ISP.

Dado que tendremos que usar 4 routers VDSL para las conexiones con el ISP haremos uso de un balanceador de carga para agrupar las 4 líneas y distribuir el tráfico entre los usuarios.

Para la parte de seguridad, utilizaré un firewall para proteger la red de accesos indeseados, ataques y de un uso fraudulento.

Para ello he elegido un firewall de gama alta, Cisco ASA 5525-X, que pertenece a la nueva generación de Cisco 5500-X. Como se puede ver en el anexo de especificaciones, quizás exceda un poco de los requerimientos necesarios respecto a la generación anterior. Sin embargo, la generación 5500 termina su ciclo de vida en septiembre de 2013 por lo que estará fuera de soporte y no es recomendable elegirlos en la fecha de realización de este proyecto.

Cisco ASA 5525-X Firewall Edition

Entre sus características más destacadas por las que he realizado la elección de este equipo están las siguientes:

- Puede inspeccionar hasta 2 Gbps de tráfico de tipo TCP (HTTP, SMTP, DNS, etc) que será el más habitualmente utilizado en este entorno por sus características de uso.

- Incorpora algoritmos de cifrado y encriptación 3DES y AES para aportar mayor seguridad en las comunicaciones.
- Soporta hasta 200 VLANs configuradas.
- Admite hasta 500.000 sesiones simultáneas.

Además ofrece la posibilidad de realizar funciones de balanceo de carga mediante la técnica de EtherChannel, propietaria de Cisco tanto en los puertos como en las VPNs por lo que no sería necesario un equipo adicional para realizar el balanceo de las líneas del ISP. De esta forma, todas las líneas pueden ser agrupadas como un solo troncal que actúe con la capacidad total o balancear la carga de un puerto a otro en caso de fallo de una de los enlaces.

Respecto a la autenticación, aunque va a ser una red pública de acceso libre, es recomendable mantener un registro de las conexiones realizadas por un servidor Radius que a su vez haga la autenticación de los usuarios. Hay varios programas en el mercado gratuitos para el servicio Radius como FreeRadius (http://freeradius.org//) que puede ejecutarse bajo Linux. Además en este mismo servidor podemos instalar un servidor web con un portal cautivo:

El portal cautivo va a ser la pagina web desde la cual el usuario se autentica para acceder al servicio de conexión internet del hotspot. Esa pagina web puede:

- dar la bienvenida.
- obligar el usuario a aceptar condiciones de uso particular.
- indicar el tiempo de navegación gratis.
- ejecutar una publicidad.
- obligar a ingresar una identificación y/o clave asignada
- limitar el ancho de banda por usuario y tamaño de archivo que se puede bajar.
- redirigir tráfico web a URLs arbitrarias.

Para esto destinaremos un nuevo equipo, un servidor para efectuar ambas funciones, la de servidor Radius y Apache donde alojar el portal cautivo. Dado que no se requiere una maquina de muy altas prestaciones para el nivel de servicio que se debe prestar considero adecuado un servidor Dell PowerEdge T620.

Dell PowerEdge T620

Dado que debemos interconectar este servidor, el equipos de la estaciones base de WiMAX y el firewall será necesario un conmutador de capa 2. He seleccionado un Cisco SG300-28P ya que además tiene funcionalidades de capa 3 pudiendo realizar funciones de routing IPv4-IPv6, , configurar ACLs , etc. Tiene 26 puertos Ethernet que se pueden configurar a 10/100/1000 Mbps y una capacidad de gestionar 56 Gbps.

Cisco SG300-28P

3.6 Infraestructura de red, equipamiento.

Vamos a utilizar una red mixta formada por equipos WiMAX y WiFi. Hay muchos equipos que pueden servir para este proyecto. Por ejemplo, se pueden consultar los productos de AirSpan, Alvarion, Aperto Networks y Proxim.

El precio de los equipos de Aperto Networks y Airspan son los más elevados y esto, en principio, nos hace descartar los. Respecto a Proxim y Alvarion, el primero es ligeramente más económico. De todos modos, entre estos dos escojo Alvarion porque:

- Alvarion es líder en WiMax.
- Se tiene constancia de instalaciones actualmente en funcionamiento con equipamiento Alvarion. Por ejemplo, los Ayuntamientos de Olot (la Garrotxa), Begues (el Garraf) y Girona.
- Dispone de un modelo de APs que pueden suministrar tanto acceso WiFi b/g como acceso WiMAX de forma simultánea.

Como estación base elegiremos la BreezeMAX Extreme 5000. Opera en la banda libre de de 5Ghz , lleva BreezeMAX Extreme 5000directa), soporta MIMO para ofrecer diversidad de canales en transmisión y recepción duplicándolo y soporta varios tipos de modulación.

BreezeMAX Extreme 5000

Como enlaces entre la estación base y los puntos de acceso WiMAX/WiFi se utilizarán los CPEs Alvarion BreezeMAX PRO 5000 los cuales son compatibles con la estación base anteriormente seleccionada. También pueden aplicar técnicas MIMO para poder realizar diversidad y duplicar la cobertura. La antena que tiene incorporada abarca un sector de 15 grados por lo que se debe colocar correctamente en dirección a la BS.

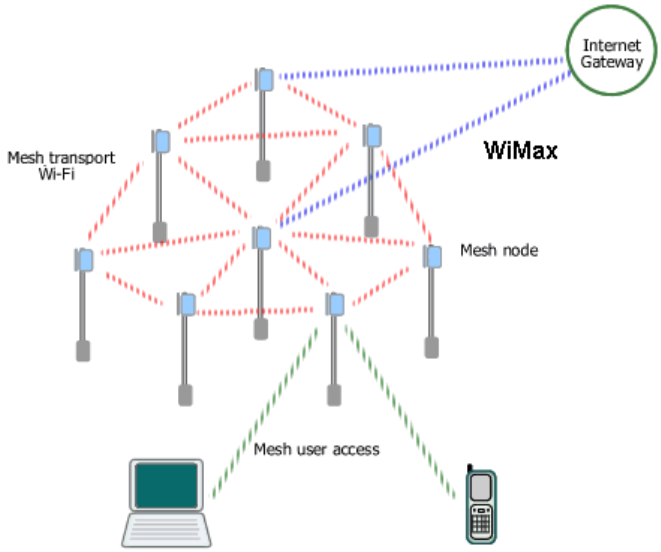
Alvarion BreezeMAX PRO 5000

Como puntos de acceso para conectar con el usuario utilizaremos Alvarion BreezeMax Wi2. que puede actuar como punto de acceso WiFi o WiMAX de forma simultánea. El estándar que soporta es 802.11.g que puede proporcionar hasta a 54 Mbps pero después de haber hecho el estudio de carga de tráfico anteriormente, creo que es suficiente para cubrir las necesidades, no siendo necesario utilizar WiFi.n.

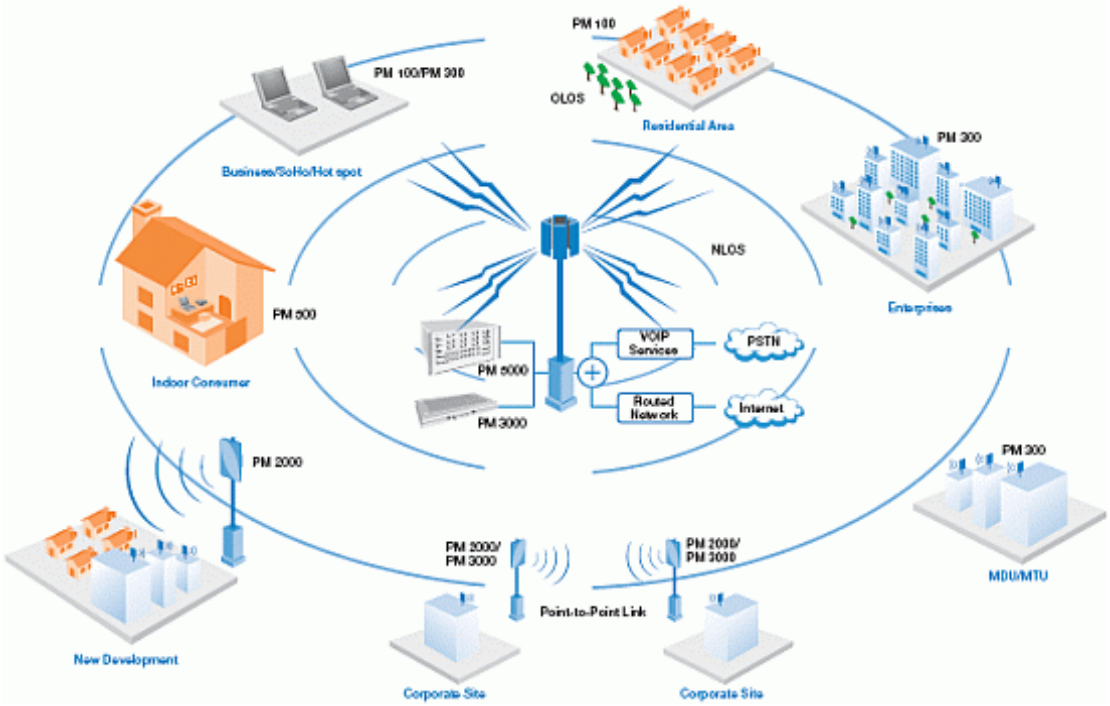
BreezeMax Wi2

3.7 Topología de la red.

Como se indico en las topologías anteriormente descritas, la red de este proyecto será una mezcla de red mesh y PmP como las que vemos en las figuras:

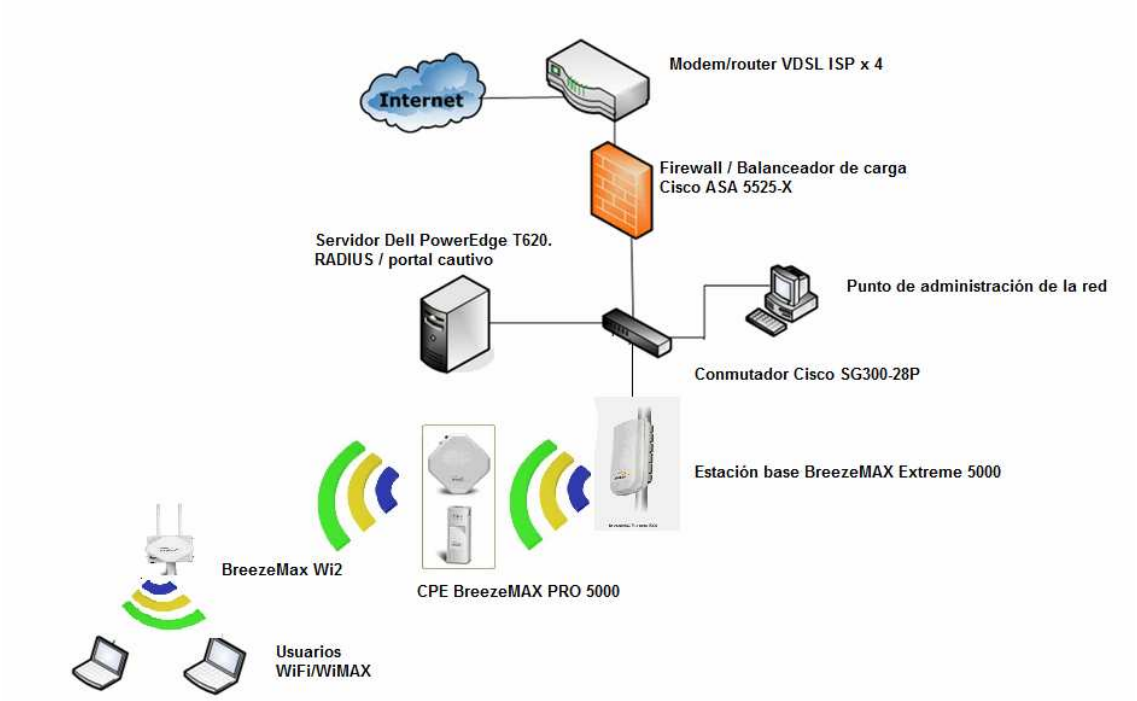


Red mesh o mallada.
http://bligoo.com/media/users/0/1038/images/mesh-WiMAX.jpg



Red PmP.
http://wikitel.info/images/8/81/Wimax-tech.gif

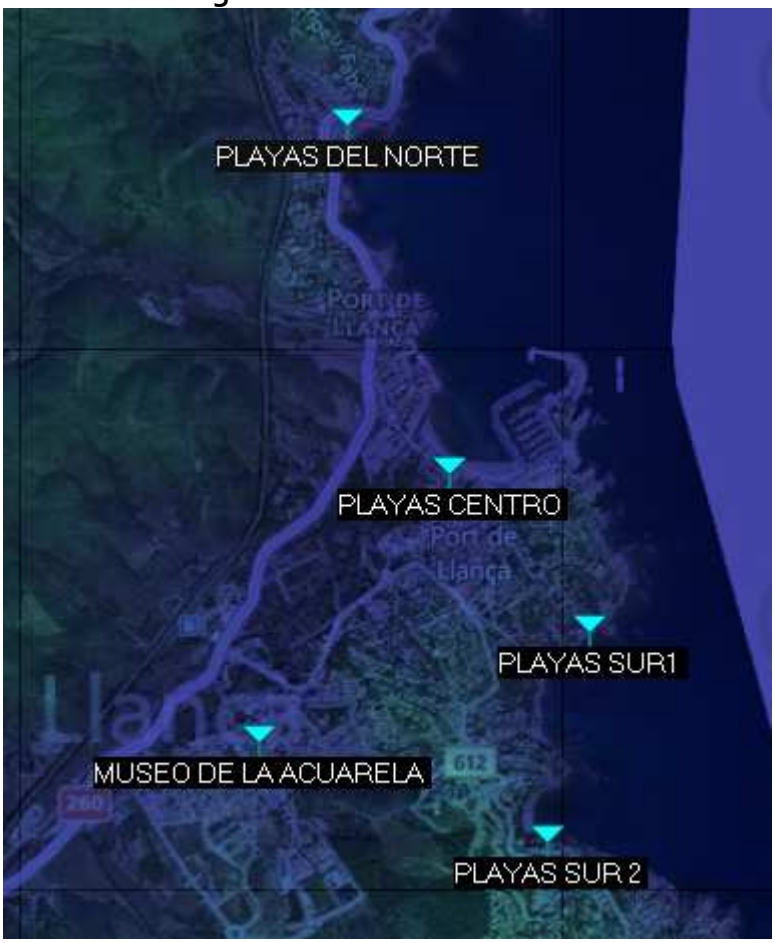
Teniendo en cuanta la topología y los equipos indicados anteriormente para la realización de este proyecto el esquema general y simplificado de la red, sería como en la figura siguiente:



La conexión a Internet se efectúa con los 4 routers VDSL del ISP. Estos irán conectados mediante cableado UTP al Firewall que realizará las funciones de seguridad y balanceo de carga. Mediante el conmutador conectaremos mediante cableado UTP, el servidor que alojará el portal cautivo y realizará las funciones de autenticación, PCs para administración si lo deseamos y la/s estaciones base. Estas últimas se comunicarán mediante enlaces WiMAX con las estaciones subscriptoras, las cuales se conectará a su vez con los APs también mediante WiMAX. Los APs proporcionarán acceso a los usuarios mediante WiFi.

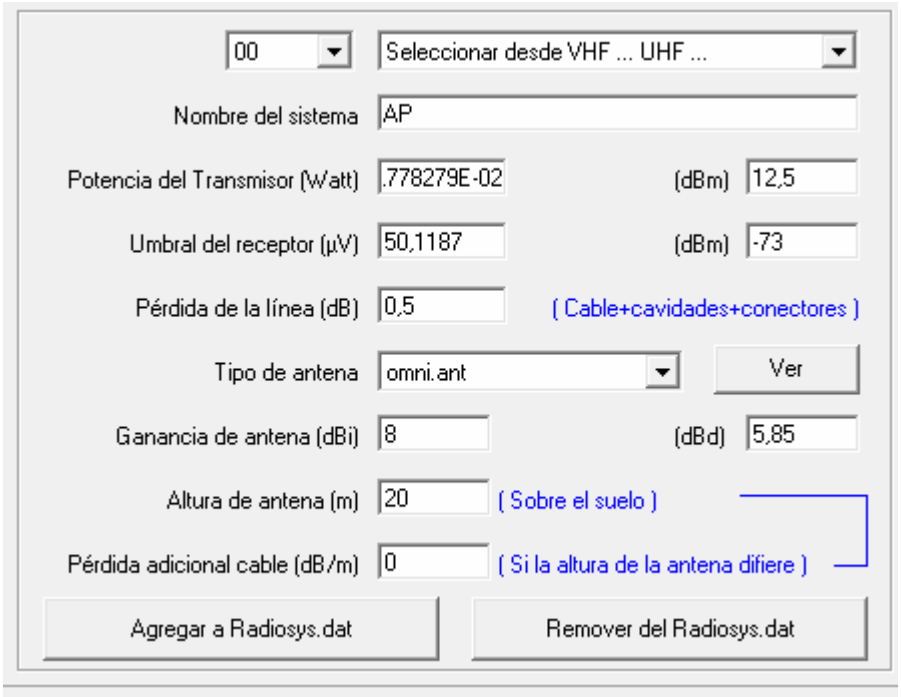
3.8 Estudio de la cobertura con radio mobile

Para realizar el estudio de la cobertura en este proyecto utilizaremos el programa Radio Mobile. Para ello superponemos un mapa importado con fotografías aéreas y caminos al mapa topográfico de Radio Mobile. Esto nos permitirá hacer una primera estimación de cuales deben ser las ubicaciones de los diferentes equipamientos.

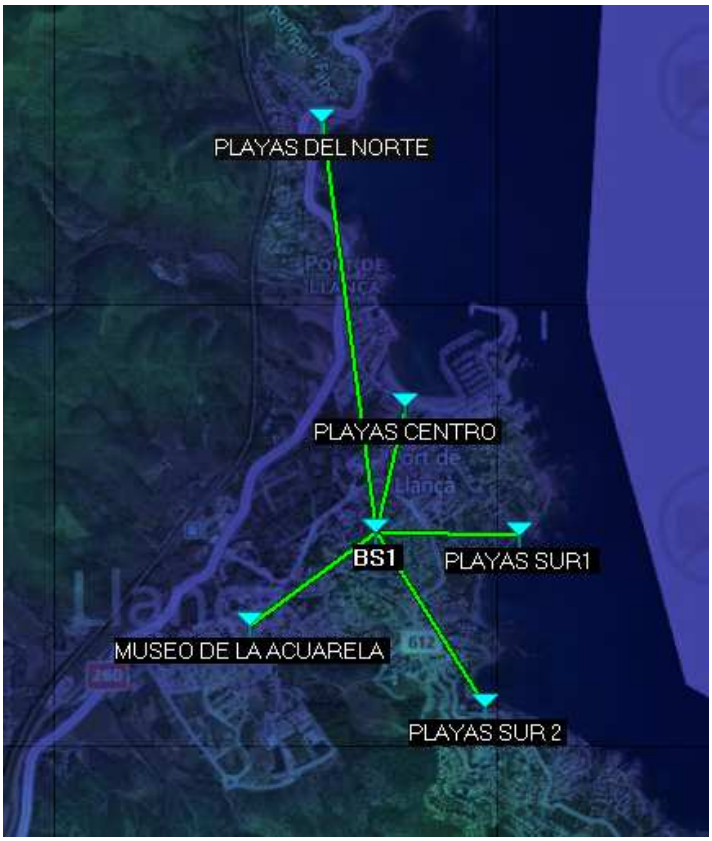


En esta figura podemos ver la ubicación de los diferentes equipos que proporcionan acceso WiFi en los lugares significativos de la población. En las siguientes figuras apreciamos las zonas de cobertura que ofrecen.

Para ellos hemos tomado los siguientes parámetros para los equipos ***BreezeMax Wi2***



Los parámetros significativos son el tipo de antena, la ganancia de la antena, la potencia de transmisión, el umbral de recepción, la frecuencia a 2,4 Ghz y la altura.



En esta captura se puede ver la ubicación de las dos estaciones base en el centro de la estrella y de los CPEs en las puntas. Se ha decidido la instalación de dos para repartir el caudal de tráfico entre los CPEs. Las antenas de las CPEs tienen un ángulo de 15 grados orientado hacia las estaciones base.

Una de las estaciones base esta orientada a playas del norte y playas del centro y la otra a playas del sur 1 y 2 y museo de la acuarela. Como se puede ver hay conectividad entre los equipos con los parámetros introducidos.

Como se puede ver en el anexo del fabricante se han tomado los siguientes valores para los CPEs ***BreezeMAX PRO 5000*** :

Potencia de transmisión 20 dBm
Ganancia de antena 16 dBi direccionables a 15 grados
Se ha establecido una altura de 15m sobre el terreno

Como se puede ver en el anexo del fabricante se han tomado los siguientes valores para las estaciones base ***BreezeMAX Extreme 5000:***

Potencia de transmisión 21 dBm
Ganancia de antena 14,5 dBi
Se ha establecido una altura de 15m sobre el terreno

Los valores que se han tomado para la potencia de transmisión están dentro del marco legal del nivel de PIRE.

MODULACIÓN	SENSIBILIDAD	TASA TRANSMISIÓN
BPSK 1/2	-92 dBm	3,81 Mbps
QPSK 1/2	-89 dBm	7,62 Mbps
QPSK 3/4	-86,5 dBm	11,43 Mbps
16 QAM 1/2	-83,5 dBm	15,24 Mbps
16 QAM 3/4	-80 dBm	22,86 Mbps
64 QAM 2/3	-76 dBm	30,48 Mbps
64 QAM 3/4	-74 dBm	34,29 Mbps

Como se puede apreciar en la siguiente tabla y al tener que repartir el tráfico teniendo en cuenta los valores de recepción y la modulación utilizada cada estación base podrá suministrar como máximo unos 34 Mbps.

Como hemos indicado anteriormente BTS1 suministra acceso a dos CPEs, por lo tanto podrá dar 17 Mbps a cada uno. Sin embargo BTS2 que suministra acceso d tres CPEs solo podrá dar 11,3 Mbps a cada uno de los CPEs y APs.

Teniendo en cuenta que cada uno de los AP según se puede consultar en el anexo, puede soportar hasta 128 usuarios, tendríamos un tráfico por usuario de 132 Kbps para los CPEs que reciben 17 Mbps y 88 Kbps para los CPEs que pueden recibir 11,3 Mbps.

Del estudio demográfico realizado anteriormente se desprende que el número potencial de usuarios simultáneos es menor que el máximo que pueden soportar cada una de las APs, por lo que el ancho de banda real al que tengan acceso en cada momento es presumiblemente mayor al de estos cálculos (siempre con la limitación de los 256 Kbps según el marco legal)

4. Valoración económica y viabilidad.

4.1 Presupuesto.

Debemos considerar en primer lugar los equipamientos y costes mensuales de las líneas proporcionadas por el ISP. Considerando el operador con más presencia en el mercado y cuyo tipo de cobertura hemos comprobado en la localidad, Movistar, tenemos:

- Coste de instalación y equipamiento: gratuito.
- Coste mensual de las 4 líneas: 120 euros primer año. / 140 euros , siguientes.
- Coste anual mantenimiento de líneas: 1440 euros primer año / 1680 euros , siguientes.

Costes asociados al equipamiento de administración y seguridad:

CONCEPTO	UNIDADES/ HORAS	PRECIO UNIDAD	TOTAL
EQUIPAMIENTO	(En estos precios estarían incluidos el cableado y las antenas necesarias para cada unidad indicada.)		
BreezeMAX Extreme 5000	2	6000	12000
BreezeMAX PRO 5000	5	2000	10000
BreezeMax Wi2	5	1800	9000
Cisco ASA 5525-X Firewall Edition	1	4500	4500
Cisco SG300-28P	1	600	600
Dell PowerEdge T620	1	1420	1420
		Subtotal equipamientos	37520
MANO DE OBRA			
Estudio y realización del proyecto	100	40	4000
Instalación y configuración	50	40	2000
		Subtotal mano de obra	6000
		TOTAL	43520€

4.2- Escalabilidad del proyecto:

Tal como se ha planteado la arquitectura de esta red para el propósito específico de dar una red de acceso gratuita en exteriores, además de ser una red mixta WiFi/Wimax y teniendo en cuenta la inversión realizada que en principio no se recuperaría (dado que es una mejora para el municipio para atraer ingresos de forma indirecta), podemos realizar futuras ampliaciones con esta arquitectura:

- Se podría aumentar el ancho de banda y no limitarlo a los 256Kbps máximos, para dar más servicios, (claro que esto implicaría que el consistorio debería

darse de alta como operador según la legislación actual y cobrar por dicho servicio).

- Ampliarlo además el alcance a interiores de las dependencias municipales para el uso de los servicios municipales. (Esto al ser considerado régimen de autoprestación no implicaría darse de alta como operador).

- Otros servicios que se podrían ofrecer mediante la red Wimax, es la colocación de sensores, cámaras u otro tipo de dispositivos para la realización de distintos estudios (tráfico, vigilancia, clima, etc)

4.3- Viabilidad económica del proyecto.

Viendo los costes de dicho proyecto vemos que es asumible para el consistorio, aún siendo a fondo perdido como se indico en el anterior punto, ya que repercutiría en el comercio y el turismo.

No obstante, como se indicó en el anterior apartado, dado que la arquitectura permite ser ampliada o modificada, se podría financiar en un futuro ampliando el caudal de tráfico a los usuarios y cobrando el servicio prestado dándose de alta como operador. De esta forma se recuperaría en poco tiempo la inversión.

Por otra parte, actualmente desconozco si siguen existiendo ayudas o subvenciones por parte del gobierno central o autonómico para este tipo de proyecto, no obstante, creo que si se buscan patrocinios por parte de la empresa privada, como pueden ser los comercios de la región, no entra en conflicto con la legislación que he indicado. Y dado que este servicio se proporciona para fomentar el turismo y el comercio de la zona creo que puede ser una vía de financiación válida. Dentro de este mismo concepto se podría considerar la posibilidad de añadir publicidad en el portal cautivo, para la obtención de ingresos para su financiación.

Se hacía mención en la escalabilidad del proyecto, a que la misma infraestructura se podía usar para realizar estudios mediante sensores, cámaras u otro tipo de dispositivos del tráfico, clima, vigilancia, etc. El consistorio también podría cobrar el uso de dicha infraestructura para estudios parecidos a la empresa privada, en caso de que se ampliara para estos fines.

Glosario:

VDSL. *Assymetric Digital Subscriber Line*. Protocolo de comunicaciones de banda amplia.

BTS. *Base Transceiver Station*. Estación base de transmisión Wimax

DSSS. *Direct Sequence Spread Spectrum*

CMT. Comisión del mercado de telecomunicaciones.

CNAF. Cuadro nacional de atribución de frecuencias

CPE. *Customer Premises Equipment.* Equipo local de cliente Wimax

CTC. Codigo de convolución *Turbo.*

FHSS. *Frequency hopping Spread Spectrum*.

ISP. Proveedor de servicios de internet.

LAN. *Local Area Network*; red de área local.

OFDMA. Acceso por multiplexación de división de frecuencia ortogonales.

PIRE. Potencia irradiada externa.

VLAN. Red local virtual. VoIP. Sobre IP.

WAN. *Wide Area Network.* Red de área global.

Bibliografía:

Definiciones técnicas:
Comunicaciones sin hilos. Sistemas telemáticos. Antonio Satué Villar. P07/89015/00419. UOC.
Redes locales y metropolitanas sin hilos. Sistemas telemáticos. Antonio Satué Villar. P07/89015/00421. UOC.
http://es.wikipedia.org
(WiMAX vs WiFi en enlaces PtP en banda libre, Enero 2010)

Legislación:
http://www.boe.es/buscar/doc.php?id=BOE-A-2003-20253
http://www.europapress.es/portaltic/sector/noticia-gobierno-aprueba-anteproyecto-nueva-ley-general-telecomunicaciones-20121228154545.html
http://www.lamoncloa.gob.es/ConsejodeMinistros/Enlaces/101210-enlaceteleco.htm
http://www.privacidadlogica.es/wp-content/uploads/downloads/2013/01/anteproyecto-ley-telecomunicaciones.pdf
http://www.boe.es/buscar/doc.php?id=BOE-A-2010-12831
http://www.minetur.gob.es/telecomunicaciones/espectro/paginas/cnaf.aspx
http://www.minetur.gob.es/telecomunicaciones/Espectro/CNAF/notasUN2013.pdf

Llança:
http://es.wikipedia.org/wiki/Llans%C3%A1
http://www.llanca.cat/
http://www.idescat.cat/emex/?id=170926&lang=es#h4

Datos estadísticos del uso de WiFi fuera del domicilio:
http://www.ine.es

ISP (Proveedor de acceso a Internet):
https://www.movistar.es
https://www.movistar.es/rpmm/estaticos/operadoras/acceso-y-transporte/servicios-de-transporte/servicio-de-transporte-metropolitano.pdf

Equipamientos, precios y datasheets:

http://www.albentia.com/documentacion.php
http://freeradius.org//
http://www.cisco.com

Anexo I (datasheets)

Dell PowerEdge T620

OPCIONES DE HARDWARE

Base	PowerEdge T620
Configuración de chasis	Chassis with up to 4, 3.5" Hard Drives, Software RAID, Tower Configuration
Procesador	Intel® Xeon® E5-2603 1.80GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W, DDR3-1066MHz
Procesador adicional	No Additional Processor
Tipo de configuración de memoria	Performance Optimized
Tipo y velocidad de los DIMM de memoria	1600 MHz UDIMMs
Capacidad de memoria	4GB UDIMM, 1600 MHz, Low Volt, Dual Rank
Sistema operativo instalado de fábrica	Red Hat Enterprise Linux 6.3, Factory Install, Requires Subscription and Media Selectio
Kits de medios del OS	Red Hat Enterprise Linux 6 Media Only X86_64, No Subscription,Factory Install
Microsoft System Center Essentials	No incluido
Sistema operativo de secondary	No incluido
Suscripciones y licencias de virtualización	No incluido
Módulo SD interno	No incluido
Software de virtualización	No incluido
Software de virtualización	No incluido
Particiones del SO	No incluido
Configuración RAID	C1 - No RAID for S110, Embedded SATA, 1 SATA/SATA SSD HDD
Controlador RAID	S110 Controller
Discos duros	500GB, SATA, 3.5-in, 7.2K RPM Hard Drive (Hot-Plug)
Discos duros (2.° grupo)	No incluido
Discos duros (3.er grupo)	No incluido
Discos duros (SSD PCIe)/discos duros (compartimento flexible)	No incluido
Configuración del BIOS (administración de energía)	Power Saving Dell Active Power Controller
Configuraciones del sistema avanzadas	No incluido
Fuente de alimentación	Single, Hot-plug Power Supply (1+0), 495W
Cables de alimentación	European - 220V Spare Power Cord

BreezeMAX® Extreme 5000

Benefit

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.

BreezeMAX Extreme 5000

WiMAX™ 16e for the 5 Ghz license-exempt market

WiMAX 16e for the License-exempt Market

Overview

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).

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.

Specifications

International Corporate HQ
Alvarion Ltd.
21a HaBarzel Street
P.O. Box 13139
Tel Aviv, Israel 69710

Contact us at:
sales@alvarion.com

For local contact information
in your area, please visit
www.alvarion.com

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**	**CPE**
	4900-5350 MHz 5470-5875 MHz	4900-5875 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**	**CPE**
	0-21 dBm, 1dB resolution	QAM64: 18 dBm QAM16: 20 dBm QPSK: 21 dBm ATPC of 20 dB, 1 dB resolution
Integrated antenna gain	14.5 dBi	16 dBi

Security

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

Interfaces

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

Mechanical

	Base Station	**CPE**
Dimensions (H x D x W)	51 x 28 x 14.7 cm	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
Humidity	ETSI 300 019-2-4 Class T4.1E (IEC-60068-2-56)
Regulatory compliance	ROHS

+ Not available in North America

About Alvarion
Alvarion Ltd. (NASDAQ:ALVR) provides optimized wireless broadband solutions addressing the connectivity, coverage and capacity 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)

alvarion®

www.alvarion.com

215373 rev.f

The advanced application-layer security and content security defenses provided by these firewalls can be extended by deploying the high-performance intrusion prevention and worm mitigation capabilities of the Advanced Inspection and Prevention Security Services Module (AIP SSM) or the comprehensive malware protection of the Content Security and Control Security Services Module (CSC SSM). Using these optional security context capabilities, businesses can deploy up to 100 virtual firewalls within a physical appliance to enable compartmentalized control of security policies on a departmental level. This virtualization strengthens security and reduces overall management and support costs while consolidating multiple security devices into a single appliance.

Table 1 compares the features and capacities of the Cisco ASA 5500 and ASA 5500-X Series Next-Generation Firewalls for the Internet Edge.

Table 1. Cisco ASA 5500 and ASA 5500-X Series Next-Generation Firewalls for the Internet Edge

Feature	Cisco ASA 5520	Cisco ASA 5525-X	Cisco ASA 5540	Cisco ASA 5545-X	Cisco ASA 5550	Cisco ASA 5555-X
						
Stateful Inspection Throughput (Maximum[2])	Up to 450 Mbps	2 Gbps	Up to 650 Mbps	3 Gbps	Up to 1.2 Gbps	4 Gbps
Stateful Inspection Throughput (Multiprotocol[3])	-	1 Gbps	-	1.5 Gbps	-	2 Gbps
IPS Throughput[4]	• Up to 225 Mbps with AIP-SSM-10 • Up to 375 Mbps with AIP-SSM-20 • Up to 450 Mbps with AIP-SSM-40	• 600 Mbps	• Up to 500 Mbps with AIP-SSM-20 • Up to 650 Mbps with AIP-SSM-40	• 900 Mbps (extra hardware not required)	• Not available	• 1.3 Gbps (extra hardware not required)
Next-Generation Throughput[5] (Multiprotocol)	-	650 Mbps	-	1 Gbps	-	1.4 Gbps
3DES/AES VPN Throughput[6]	Up to 225 Mbps	300 Mbps	Up to 325 Mbps	400 Mbps	Up to 425 Mbps	700 Mbps
Users/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Cisco Cloud Web Security Users	300	500	1000	1500	2000	3000
IPsec VPN Peers	750	750	5000	2500	5000	5000
Premium AnyConnect VPN Peers	2/750	2/750	2/2500	2/2500	2/5000	2/5000
Concurrent Connections	280,000	500,000	400,000	750,000	650,000	1,000,000

[2] Maximum throughput measured with UDP traffic under ideal conditions.
[3] Multiprotocol: Traffic profile consisting primarily of TCP-based protocols/applications, such as HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.
[4] Firewall traffic that does not go through the IPS service can have higher throughput.
[5] Throughput was measured using ASA CX Software Release 9.1.1 with multiprotocol traffic profile with both AVC and WSE. Traffic logging was enabled as well.
[6] VPN throughput and sessions count depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

Feature	Cisco ASA 5520	Cisco ASA 5525-X	Cisco ASA 5540	Cisco ASA 5545-X	Cisco ASA 5550	Cisco ASA 5555-X
New Connections/ Second	12,000	20,000	25,000	30,000	33,000	50,000
Virtual Interfaces (VLANs)	150	200	200	300	400	500
Security Contexts (Included/ Maximum)[7]	2/20	2/20	2/50	2/50	2/50	2/100
High Availability	Active/Active and Active/Standby	Active/Active and Active/Standby	Active/Active and Active/Standby	Active/Active and Active/Standby	Active/Active and Active/Standby	Active/Active and Active/Standby
Expansion Slot	1 SSM	1 interface card	1 SSM	1 interface card	0	1 interface card
Number of User-Accessible Flash Slots	1	0	1	-	1	0
USB 2.0 Ports	2	2	2	2	2	2[2]
Integrated I/O	4 GE + 1 Fast Ethernet	8 GE copper	4 GE + 1 Fast Ethernet	8 GE copper	8 GE + 1 Fast Ethernet	8 GE copper
Expansion I/O	4 GE copper or 4 GE SFP	6 GE copper or 6 GE SFP	4 GE copper or 4 GE SFP	6 GE copper or 6 GE SFP	None	6 GE copper or 6 GE SFP
Dedicated Management Port	None	Yes (1 GE)	None	Yes (1 GE)	None	Yes (1 GE)
Serial Ports	2 RJ-45, console and auxiliary	1 RJ-45	2 RJ-45, console and auxiliary	1 RJ-45	2 RJ-45, console and auxiliary	1 RJ-45
Solid State Drive	-	1 slot 120 GB MLC SED	-	2 slots, RAID 1 120 GB MLC SED	-	2 slots, RAID 1 120 GB MLC SED
Memory	2 GB	8 GB	2 GB	12 GB	4 GB	16 GB
Minimum System Flash	256 MB	8 GB	256 MB	8 GB	256 MB	8 GB
System Bus	Multibus architecture	Multibus architecture	Multibus architecture	Multibus architecture	Multibus architecture	Multibus architecture
Environmental Operating Ranges						
Operating						
Temperature	32 to 104ºF (0 to 40ºC)	23 to 104℉ (-5 to 40℃)	32 to 104ºF (0 to 40ºC)	23 to 104℉ (-5 to 40℃)	32 to 104ºF (0 to 40ºC)	23 to 104℉ (-5 to 40℃)
Relative Humidity	5 to 95 percent noncondensing	90 percent	5 to 95 percent noncondensing	90 percent	5 to 95 percent noncondensing	90 percent
Altitude	Designed and tested for 0 to 9840 ft (3000m); agency approved for 2000m	Designed and tested for 0 to 10,000 ft (3050m)	Designed and tested for 0 to 9840 ft (3000m); agency approved for 2000m	Designed and tested for 0 to 10,000 ft (3050m)	Designed and tested for 0 to 9840 ft (3000m); agency approved for 2000m	Designed and tested for 0 to 10,000 ft (3050m)
Shock	1.14 m/sec (45 in./sec) 1/2 sine input	50G, 2 m/sec	1.14 m/sec (45 in./sec) 1/2 sine input	50G, 2 m/sec	1.14 m/sec (45 in./sec) 1/2 sine input	50G, 2 m/sec
Vibration	0.41 Grms2 (3 to 500 Hz) random input	0.41 Grms (3 to 500Hz) random input	0.41 Grms2 (3 to 500 Hz) random input	0.41 Grms (3 to 500Hz) random input	0.41 Grms2 (3 to 500 Hz) random input	0.41 Grms (3 to 500Hz) random input
Acoustic Noise	60 dBa max	64.2 dBa max	60 dBa max	67.9 dBa max	60 dBa max	67.9 dBa max

[7] Separately licensed feature; includes two SSL licenses with base system.

Feature	Cisco ASA 5520	Cisco ASA 5525-X	Cisco ASA 5540	Cisco ASA 5545-X	Cisco ASA 5550	Cisco ASA 5555-X
Nonoperating						
Temperature	-13 to 158°F (-25 to 70°C)	-13 to 158°F (-25 to 70°C)	-13 to 158°F (-25 to 70°C)	-13 to 158°F (-25 to 70°C)	-13 to 158°F (-25 to 70°C)	-13 to 158°F (-25 to 70°C)
Relative Humidity	5 to 95 percent noncondensing	10 to 90 percent	5 to 95 percent noncondensing	10 to 90 percent	5 to 95 percent noncondensing	10 to 90 percent
Altitude	0 to 15,000 ft (4570m)	Designed and tested for 0 to 15,000 ft (4572m)	0 to 15,000 ft (4570m)	Designed and tested for 0 to 15,000 ft (4572m)	0 to 15,000 ft (4570m)	Designed and tested for 0 to 15,000 ft (4572m)
Shock	30G	70G, 4.22 m/sec	30G	70G,4.22 m/sec	30G	70G, 4.22 m/sec
Vibration	0.41 Grms2 (3 to 500 Hz) random input	1.12 Grms (3 to 500Hz) random input	0.41 Grms2 (3 to 500 Hz) random input	1.12 Grms (3 to 500Hz) random input	0.41 Grms2 (3 to 500 Hz) random input	1.12 Grms (3 to 500Hz) random input
Power						
Input (per Power Supply)						
AC Range Line Voltage	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
AC Normal Line Voltage	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
AC Current	3A	4.85A	3A	5A, 100 to 120V 2.5A, 200 to 240V	3A	5A, 100 to 120V 2.5A, 200 to 240V
AC Frequency	47/63 Hz, single-phase	50/60 Hz	47/63 Hz, single-phase	50/60 Hz	47/63 Hz, single-phase	50/60 Hz
Dual Power Supplies	None	None	None	Yes	None	Yes
DC Domestic Line Voltage	See the ASA 5500 Series Hardware Installation Guide	-40.5 to 56 VDC (-48 VDC nominal)	See the ASA 5500 Series Hardware Installation Guide	-40.5 to 56 VDC (-48 VDC nominal)	See the ASA 5500 Series Hardware Installation Guide	-40.5 to 56 VDC (-48 VDC nominal)
DC International Line Voltage	See the ASA 5500 Series Hardware Installation Guide	-55 to -72 VDC (-60 VDC nominal)	See the ASA 5500 Series Hardware Installation Guide	-55 to -72 VDC (-60 VDC nominal)	See the ASA 5500 Series Hardware Installation Guide	-55 to -72 VDC (-60 VDC nominal)
DC Current	See the ASA 5500 Series Hardware Installation Guide	15A (maximum input)	See the ASA 5500 Series Hardware Installation Guide	15A (maximum input)	See the ASA 5500 Series Hardware Installation Guide	15A (maximum input)
Output						
Steady State	150W	75W	150W	86W	150W	90W
Maximum Peak	190W	108W	190W	125W	190W	134W
Maximum Heat Dissipation	648 BTU/hr	369 BTU/hr	648 BTU/hr	427 BTU/hr	648 BTU/hr	458 BTU/hr
Physical Specifications						
Form Factor	1 RU, 19-in. rack-mountable	1 RU, 19-in. rack-mountable	1 RU, 19-in. rack-mountable	1 RU, 19-in. rack-mountable	1 RU, 19-in. rack-mountable	1 RU, 19-in. rack-mountable
Dimensions (H x W x D)	1.75 x 17.5 x 14.25 in. (4.45 x 20.04 x 36.20 cm)	1.67 x 16.7 x 15.6 in. (4.24 x 42.9 x 39.5 cm)	1.75 x 17.5 x 14.25 in. (4.45 x 20.04 x 36.20 cm)	1.67 x 16.7 x 19.1 in. (4.24 x 42.9 x 48.4 cm)	1.75 x 17.5 x 14.25 in. (4.45 x 20.04 x 36.20 cm)	1.67 x 16.7 x 19.1 in. (4.24 x 42.9 x 48.4 cm)
Weight (with Power Supply)	20.0 lb (9.07 kg)	14.92 lb (6.77 kg)	22.0 lb (10 kg)	16.82 lb (7.63 kg) with single power supply 18.86 lb (8.61 kg) with dual power supply	22.0 lb (10 kg)	16.82 lb (7.63 kg) with single power supply 18.86 lb (8.61 kg) with dual power supply

Product Specifications

Table 1 gives the product specifications for the Cisco 300 Series Switches.

Table 1. Product Specifications

Feature	Description		
Performance			
Switching capacity and forwarding rate All switches are wire-speed and non-blocking	**Model Name**	**Capacity in Millions of Packets per Second (mpps) (64-byte packets)**	**Switching Capacity in Gigabits per Second (Gbps)**
	SF300-08	1.19	1.6
	SF302-08	4.17	5.6
	SF302-08P	4.17	5.6
	SF302-08MP	4.17	5.6
	SF300-24	9.52	12.8
	SF300-24P	9.52	12.8
	SF300-48	13.10	17.6
	SF300-48P	13.10	17.6
	SG300-10	14.88	20.0
	SG300-10P	14.88	20.0
	SG300-10MP	14.88	20.0
	SG300-20	29.76	40.0
	SG300-28	41.67	56.0
	SG300-28P	41.67	56.0
	SG300-52	77.38	104.0
	SG300-52P	77.38	104
	SG300-52MP	77.38	104
	SG300-10SFP	14.88	20
	SF300-24MP	9.52	12.8
	SG300-28MP	41.67	56
Layer 2 Switching			
Spanning Tree Protocol (STP)	Standard 802.1d Spanning Tree support Fast convergence using 802.1w (Rapid Spanning Tree [RSTP]), enabled by default 8 instances are supported Multiple Spanning Tree instances using 802.1s (MSTP)		
Port grouping	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP) • Up to 8 groups • Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad link aggregation		
VLAN	Support for up to 4096 VLANs simultaneously Port-based and 802.1Q tag-based VLANs MAC-based VLAN Management VLAN Private VLAN Edge (PVE), also known as protected ports, with multiple uplinks Guest VLAN Unauthenticated VLAN Dynamic VLAN assignment via Radius server along with 802.1x client authentication CPE VLAN		
Voice VLAN	Voice traffic is automatically assigned to a voice-specific VLAN and treated with appropriate levels of QoS. Auto voice capabilities deliver network-wide zero touch deployment of voice endpoints and call control devices.		

Feature	Description
Multicast TV VLAN	Multicast TV VLAN allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs (Also known as MVR)
Q-in-Q VLAN	VLANs transparently cross a service provider network while isolating traffic among customers
Generic VLAN Registration Protocol (GVRP)/Generic Attribute Registration Protocol (GARP)	Protocols for automatically propagating and configuring VLANs in a bridged domain
Dynamic Host Configuration Protocol (DHCP) Relay at Layer 2	Relay of DHCP traffic to DHCP server in different VLAN. Works with DHCP Option 82
Internet Group Management Protocol (IGMP) versions 1, 2, and 3 snooping	IGMP limits bandwidth-intensive multicast traffic to only the requesters; supports 1K multicast groups (source-specific multicasting is also supported)
IGMP Querier	IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router
Head-of-line (HOL) blocking	HOL blocking prevention
Jumbo Frames	Up to 9K (9216) bytes
Layer 3	
IPv4 routing	Wirespeed routing of IPv4 packets Up to 512 static routes and up to 128 IP interfaces
Classless Inter-Domain Routing (CIDR)	Support for CIDR
DHCP relay at Layer 3	Relay of DHCP traffic across IP domains
User Datagram Protocol (UDP) relay	Relay of broadcast information across Layer 3 domains for application discovery or relaying of BootP/DHCP packets
DHCP Server	Switch functions as an IPv4 DHCP Server serving IP addresses for multiple DHCP pools/scopes
Security	
Secure Shell (SSH) Protocol	SSH is a secure replacement for Telnet traffic. SCP also uses SSH. SSH v1 and v2 are supported
Secure Sockets Layer (SSL)	SSL support: Encrypts all HTTPS traffic, allowing highly secure access to the browser-based management GUI in the switch
IEEE 802.1X (Authenticator role)	802.1X: RADIUS authentication and accounting, MD5 hash; guest VLAN; unauthenticated VLAN, single/multiple host mode and single/multiple sessions Supports time-based 802.1X Dynamic VLAN assignment
STP Bridge Protocol Data Unit (BPDU) Guard	A security mechanism to protect the network from invalid configurations. A port enabled for BPDU Guard is shut down if a BPDU message is received on that port.
STP Root Guard	This prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
DHCP snooping	Filters out DHCP messages with unregistered IP addresses and/or from unexpected or untrusted interfaces. This prevents rogue devices from behaving as a DHCP Server.
IP Source Guard (IPSG)	When IP Source Guard is enabled at a port, the switch filters out IP packets received from the port if the source IP addresses of the packets have not been statically configured or dynamically learned from DHCP snooping. This prevents IP Address Spoofing.
Dynamic ARP Inspection (DAI)	The switch discards ARP packets from a port if there is no static or dynamic IP/MAC bindings or if there is a discrepancy between the source or destination address in the ARP packet. This prevents man-in-the-middle attacks.
IP/Mac/Port Binding (IPMB)	The features (DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection) above work together to prevent DOS attacks in the network, thereby increasing network availability.
Secure Core Technology (SCT)	Ensures that the switch will receive and process management and protocol traffic no matter how much traffic is received.
Secure Sensitive Data (SSD)	A mechanism to manage sensitive data (such as passwords, keys, etc) securely on the switch, populating this data to other devices, and secure autoconfig. Access to view the sensitive data as plaintext or encrypted is provided according to the user configured access level and the access method of the user.
Layer 2 isolation Private VLAN Edge (PVE) with community VLAN	PVE (also known as protected ports) provides Layer 2 isolation between devices in the same VLAN, supports multiple uplinks.
Port security	The ability to lock Source MAC addresses to ports, and limits the number of learned MAC addresses.

Feature	Description
RADIUS/TACACS+	Supports RADIUS and TACACS authentication. Switch functions as a client.
Storm control	Broadcast, multicast, and unknown unicast
RADIUS accounting	The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session.
DoS prevention	Denial-of-Service (DOS) attack prevention
Congestion avoidance	A TCP congestion avoidance algorithm is required to minimize and prevent global TCP loss synchronization.
ACLs	Support for up to 512 rules Drop or rate limit based on source and destination MAC, VLAN ID or IP address, protocol, port, differentiated services code point (DSCP)/IP precedence, TCP/ UDP source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, IGMP packets, TCP flag, Time-based ACLs supported.
Quality of Service	
Priority levels	4 hardware queues
Scheduling	Strict priority and weighted round-robin (WRR) Queue assignment based on DSCP and class of service (802.1p/CoS)
Class of service	Port based; 802.1p VLAN priority based; IPv4/v6 IP precedence/type of service (ToS)/DSCP based; Differentiated Services (DiffServ); classification and re-marking ACLs, trusted QoS.
Rate limiting	Ingress policer; egress shaping and rate control; per VLAN, per port, and flow based.
Standards	
Standards	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad LACP, IEEE 802.3z Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP),IEEE 802.1Q/p VLAN, IEEE 802.1w RSTP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 879, RFC 896, RFC 826, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 922, RFC 920, RFC 950, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1350, RFC 1533, RFC 1541, RFC 1624, RFC 1700, RFC 1867, RFC 2030, RFC 2616, RFC 2131, RFC 2132, RFC 3164, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 2576, RFC 4330, RFC 1213, RFC 1215, RFC 1286, RFC 1442, RFC 1451, RFC 1493, RFC 1573, RFC 1643, RFC 1757, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2233, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 1157, RFC 1493, RFC 1215, RFC 3416
IPv6	
IPv6	IPv6 host mode IPv6 over Ethernet Dual IPv6/IPv4 stack IPv6 neighbor and router discovery (ND) IPv6 stateless address auto-configuration Path maximum transmission unit (MTU) discovery Duplicate address detection (DAD) ICMP version 6 IPv6 over IPv4 network with Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) support USGv6 and IPv6 Gold Logo certified
IPv6 QoS	Prioritize IPv6 packets in hardware
IPv6 ACL	Drop or rate limit IPv6 packets in hardware
Multicast Listener Discovery (MLD v1/2) snooping	Deliver IPv6 multicast packets only to the required receivers
IPv6 applications	Web/SSL, Telnet server/SSH, ping, traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, DNS client, Telnet Client, DHCP Client, DHCP Autoconfig, IPv6 DHCP Relay, TACACS

Specifications

Headquarters

International Corporate Headquarters
Tel: +972.3.645.6262
Email: corporate-sales@alvarion.com

North America Headquarters
Tel: +1.650.314.2500
Email: n.america-sales@alvarion.com

Sales Contacts

Australia
Email: australia-sales@alvarion.com

Brazil
Email: brazil-sales@alvarion.com

Canada
Email: canada-sales@alvarion.com

China
Email: china-sales@alvarion.com

Czech Republic
Email: czech-sales@alvarion.com

France
Email: france-sales@alvarion.com

Germany
Email: germany-sales@alvarion.com

Hong Kong
Email: hongkong-sales@alvarion.com

Italy
Email: italy-sales@alvarion.com

Ireland
Email: uk-sales@alvarion.com

Japan
Email: japan-sales@alvarion.com

Latin America
Email: lasales@alvarion.com

Mexico
Email: mexico-sales@alvarion.com

Nigeria
Email: nigeria-sales@alvarion.com

Philippines
Email: far.east-sales@alvarion.com

Poland
Email: poland-sales@alvarion.com

Romania
Email: romania-sales@alvarion.com

Russia
Email: info@alvarion.ru

Singapore
Email: far.east-sales@alvarion.com

South Africa
Email: africa-sales@alvarion.com

Spain
Email: spain-sales@alvarion.com

U.K.
Email: uk-sales@alvarion.com

Uruguay
Email: uruguay-sales@alvarion.com

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

alvarion®
Your Open WiMAX Choice

www.alvarion.com

214513 rev.c

Wi-Fi Access Point Specifications

Data Rates
802.11g: 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel
802.11b: 1, 2, 5.5, 11 Mbps per channel

Maximum Channels
FCC/IC: 1-11
ETSI: 1-13
Japan: 1-14

Maximum Clients
128 for the radio interface set to access point mode

Modulation Types
802.11g: CCK, BPSK, QPSK, OFDM
802.11b: CCK, BPSK, QPSK

Operating Frequency
802.11b/g:
2.4~2.4835 GHz (US, Canada, ETSI)
2.4~2.497 GHz (Japan)

Network Management
Web-management, Telnet, SNMP

Radio Signal Certification
FCC Part 15.247 (2.4 GHz)
EN 300.328, EN 302.893, EN 300 826, EN 301.489-1, EN 301.489-17
ETSI 300.328; ETS 300 826 (802.11b)

Safety
UL/CUL (CSA60950-1, UL60950-1)
CB (IEC 60950-1)
UL/GS (EN60950-1)

Wireless Radio/Regulatory Certification
ETSI 300 328 (11b/g), 301 489 (DC power)
FCC Part 15C 15.247/15.207 (11b/g), Wi-Fi, DGT, TELEC, RSS210 (Canada)

Electromagnetic Compatibility
CE Class B (EN55022)
CE EN55024
IEC61000-3-2, IEC61000-3-3, IEC61000-4-2, IEC61000-4-3, IEC61000-4-4, IEC61000-4-5, IEC61000-4-6, IEC61000-4-8, IEC61000-4-11
FCC Class B Part 15
VCCI Class B
ICES-003 (Canada)

Standards
IEEE 802.3 10BASE-T
IEEE 802.3u 100BASE-TX
IEEE 802.11 b, g

Antenna Specifications
2 x 8 dBi Omni directional (2.4-2.5 GHz)

TX Power and RX Sensitivity

802.11g	6 Mbps	9 Mbps	12 Mbps	18 Mbps	24 Mbps	36 Mbps	48 Mbps	54 Mbps
TX power (dbm)	20	20	20	20	20	19	19	18
RX sensitivity (dbm)	-95	-93	-87	-84	-80	-77	-73	-70

802.11b	1 Mbps	2 Mbps	5.5 Mbps	11 Mbps
TX power (dbm)	20	20	20	20
RX sensitivity (dbm)	-111	-102	-92	-91

Software Features

Access Control
Integrated HTML login/captive portal
Integrated RADIUS authentication
Configurable min./max. connect speed
Scalable to thousands of users

Centralized Management
Full plug and play AP configuration, upgrade and control
Centralized system monitor for thousands of APs
Full, secure GUI configuration and monitoring

Management
SNMP, CLI, web-based
Selectable RF channel and transmit power
Packet capture on WLAN or LAN interface (diagnostics)

Multiservice
Support for 16 virtual networks, hidden and broadcast SSIDs
Unique SSID, Mac address, authentication, encryption, VLANs and QoS
Per-user bandwidth management
User account profiles using embedded/external AAA
Full virtual AP configuration, including authentication, DTIM, QoS

Mobility
Full voice quality L2 and L3 mobility for clients roaming between APs
Service transparency through fast roaming and handovers

QoS and Other
Support for 802.11i, WMM, RADIUS, 802.1q, 802.1p, IP TOS/DSCP
Mesh (DWDS), self-healing, self-optimizing

Security
802.1x, AES, WPA2, Radius, WEP, Firewall
SSH/SSL, IPSec encapsulated SNMP, XML
Wireless MAC/IP filter, NAT, CIDR
Layer-2 wireless client isolation
DHCP: Server; Client; Relay, Option 82, Rogue AP detection and prevention

Physical Dimensions

Size (H x W x D)
32.9 x 27.8 x 21.1 cm
(13.0 x 11.0 x 8.3 in)

Weight
7.0 kg (49.37 lbs)

Temperature
Operating: -40 to 60°C (-40 to 140°F)
Storage: -55 to 80°C (-67 to 176°F)

Humidity
5 to 95% (non-condensing)

EMC Compliance (Class B)
FCC Class B (US)
RTTED 1999/5/EC
DGT (Taiwan)

* For backhaul specifications, please see BreezeMAX or BreezeACCESS VL documentation, as appropriate
* For further information, please contact your local Alvarion sales representative

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	• 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 metholds: 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

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

Configuration and Management

Management Options	• Web based (HTTP/HTTPS) • TR-069 • TFTP
Management access	From Wired LAN, Wireless Link
Management access protection	Access password
Allocation of IP parameters	• 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

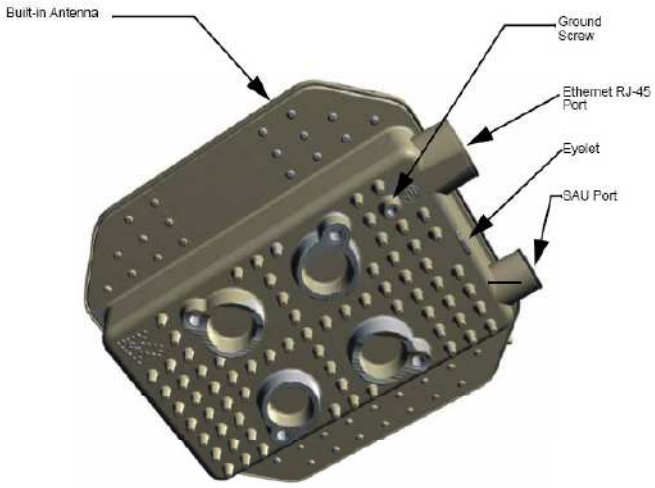
LAN interface	IEEE 802.3, 802.1Q, 802.1P IP CS bridge mode with transparent DHCP traffic Selective Proxy ARP
Air Interface	IEEE 802.16e IP CS with traffic classifier DSCP. Eth. CS (future release)

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

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

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/m3
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