Universitat Oberta de Catalunya

www.uoc.edu

Proyecto de despliegue de una red inalámbrica para el acceso gratuito a Internet

Autor: Carlos Ramos Gisbert

Director: Antoni Morell Pérez

Índice de contenido

Índice de ilustraciones

Índice de tablas

“A Marisol, por su infinita paciencia. A Celia, por su infinita alegría”.

1.Descripción del proyecto

Cartagena es ciudad costera que se encuentra ubicada en el Sureste peninsular. Poseedora de un beningo clima y un importante patrimonio cultural y arqueológico, ha venido desarrollando en los últimos años un sostenido incremento de visitantes año tras año.

La reciente construcción de una terminal de cruceros en la dársena del puerto, auspiciada por la creciente popularidad de este tipo de turismo, ha conseguido atraer a la ciudad a cerca de 120.000 visitantes[1] y más de 100 cruceros[2] a lo largo del 2013, generando unos ingresos de más de 570.000€. Estos datos representan un incremento respecto el año anterior del 21%.

Ante las buenas expectativas, el colectivo de empresas del sector se plantea ofrecer a los turistas servicios de valor añadido. Valorando el uso masivo de teléfonos inteligentes entre la población, se decide finalmente implantar un servicio de conexión a internet inalámbrico y gratuito en la playa de la ciudad, Cala Cortina.

Para llevar a cabo la implantación, se plantea un convenio de colaboración con el Ayuntamiento de la ciudad, mediante el cual éste asume el coste de implantación y mantenimiento a cambio de unos ingresos regulares en concepto de publicidad.

El Ayuntamiento, dada la ubicación de la Cala Cortina, se plantea el aprovechamiento de la nueva infraestructura para dotar también de acceso a internet a la cercana Diputación de Santa Lucía que cuenta con una población de 6544 habitantes.

Por otro lado, la Diputación de Santa Lucía está muy próxima a la terminal de contenedores del muelle de San Pedro. De aquí surge la posibilidad de utilizar la cobertura inalámbrica para un proyecto se seguimiento de contenedores por parte del Puerto de Cartagena, a cambio de una cuota de uso.

1 Información obtenida de http://noticias.lainformacion.com/arte-cultura-y-espectaculos/monumentos-y-patrimonio-nacional/cartagena-puerto-de-culturas-vive-su-mejor-verano-con-la-presencia-de-119-000-turistas_jd67weNGxU8uVoTPsBI1H/

2 Información obtenida de http://www.apc.es/conexiones.php?reg=10&ind=2

2.Objetivos del proyecto

A continuación se detallan los principales objetivos del proyecto.

- ✔ Dotar de un acceso inalámbrico y gratuito a Internet en el ámbito de la Diputación de Santa Lucía y Cala Cortina.
- ✔ Minimización de los costes de instalación y mantenimiento.
- ✔ Adecuación a la normativa vigente, evitando posibles quejas o denuncias de proveedores privados de acceso a Internet.
- ✔ Desarrollo de la Sociedad de la Información entre los ciudadanos de la zona.
- ✔ Aumento del atractivo turístico de la zona.
- ✔ Ofrecer al Puerto de Cartagena cobertura wifi en la plataforma de contenedores del muelle de San Pedro para arrancar un piloto de control logístico de containers mediante IoT[3].

3.Condiciones de servicio al usuario

Se plantea la necesidad de que los usarios se autentifiquen ante el sistema, por los siguientes motivos:

- ✔ Evitar el colapso del ancho de banda debido a una utilización indiscriminada.
- ✔ Poder limitar el ancho de banda por usuario a un máximo de 256 Kbps, conforme a la legislación vigente.
- ✔ Aumentar la seguridad del sistema, habida cuenta de que el acceso a internet es proporcionado por el CPD del Ayuntamiento de Cartagena.
- ✔ Poder aplicar políticas de control de acceso a determinadas páginas web, control sobre la descarga de archivos adjuntos, ...

Para ello se adopta el siguiente criterio:

- ✔ Los habitantes de la diputación deberán realizar la solicitud de usuario en las oficinas del Ayuntamiento, para comprobar que efectivamente están empadronados en la zona.
- ✔ Los turistas que visiten la zona pueden solicitar usuario en las oficinas de Turismo de la ciudad.

3 Internet of Things

4.Dimensionamiento del ancho de banda

Vamos a estimar a continuación los requerimientos de ancho de banda de los usuarios, necesarios para dimensionar la infraestructura inalámbrica y la conexión al ISP[4].

Inicialmente el dimensionamiento del sistema será conservador, por los siguientes motivos:

- ✔ Reducir el coste inicial del proyecto.
- ✔ En el criterio de selección de los sistemas inalámbricos se tendrá en cuenta su escalabilidad, para de este modo tener garantizado el crecimiento en caso necesario.
- ✔ El acceso a internet no es abierto, por lo que se reduce la necesidad de ancho de banda.
- ✔ La descarga de ficheros pesados (mp3, avi, mpg,...) está restringida desde el proxy.

A continuación, vamos a estimar la necesidad de ancho de banda del usuario medio de smartphone[5].

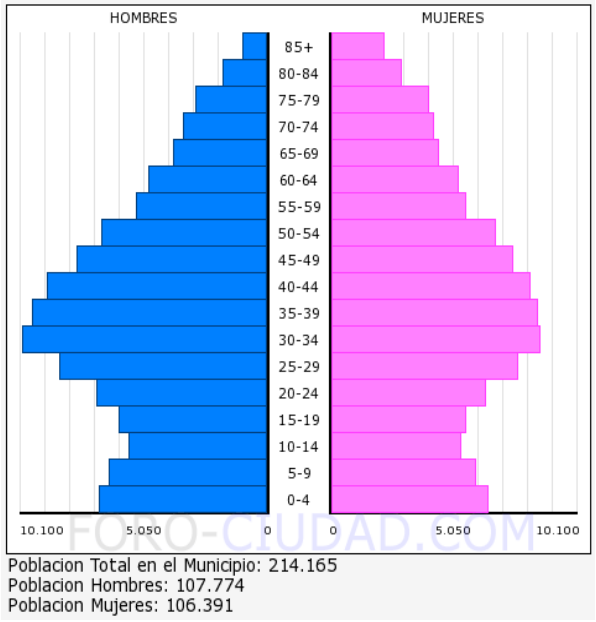
Sabemos que los usuarios utilizan principalmente su terminal para el acceso a las diferentes aplicaciones de mensajería instantánea, redes sociales y correo; siendo todas ellas poco intensivas en consumo de ancho de banda. De hecho, Si analizamos las tarifas planas de datos que ofrecen los operadores en España, veremos que son en general inferiores a 1Gb mensual lo que representaría un acceso continuado de 22,4 Kbps.

Para proporcionar al usuario una experiencia aceptable de uso vamos a considerar suficiente 64 Kbps de media por cada usuario.

Trajabamos ahora en el área de Santa Lucía. En primer lugar, nos centramos en el perfil de edad, estimando que en la franja de los 20 a los 40 años se encuentra la mayor proporción de usuarios. Descartamos los menores de 18 años ya que será requisito para la solicitud de acceso ser mayor de edad.

4 Internet Service Provider
5 Teléfono Inteligente

Si observamos la pirámide poblacional de Cartagena en 2010, vemos que dicha franja representa aproximadamente el 20% del total.



1. Ilustración: Pirámide poblacional Cartagena

Proyectando dicho porcentaje para los 6.544 habitantes de la diputación de Santa Lucía, obtendríamos 1.038 usuarios potenciales.

Si aplicamos un coeficiente de simultaneidad del 40%, tendríamos una estimación de 622 usuarios simultáneos.

En la zona turística de Cala Cortina, se estima que podrán existir un máximo de 100 usuarios simultáneos conectados dado que se trata de una cala de reducidas dimensiones.

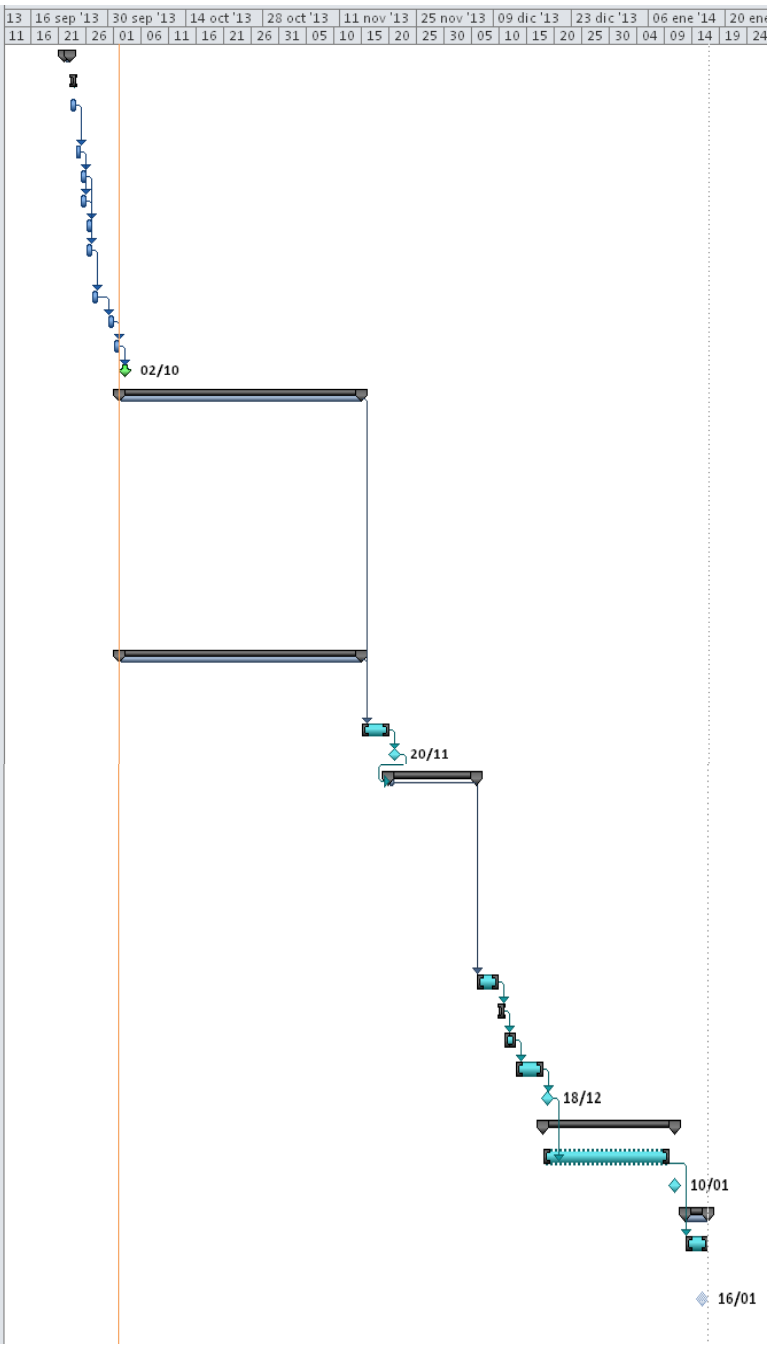
En la zona del muelle de contenedores del Muelle de San Pedro, la conexión será exclusivamente de los dispositivos IoT[6], cuyo requerimiento de ancho de banda es mínimo. Estimaremos que equivale al de un usuario conectado.

Por tanto obtenemos un total de 723 usuarios conectados, que a una media de 64 Kbps supondrá un ancho de banda agregado de 723x64Kbps=46,27Mbps.

6 Internet of Things

5.Planificación temporal del proyecto

Nombre de tarea	Duración	Comienzo	Fin
Justificación del proyecto	**1 día**	**dom 22/09/13**	**dom 22/09/13**
Objetivo y alcance	1 día	lun 23/09/13	lun 23/09/13
Busqueda software cobertura y enlaces	1 día	lun 23/09/13	lun 23/09/13
Selección del Municipio	1 día	mar 24/09/13	mar 24/09/13
Prospección tecnológica inicial	1 día	mié 25/09/13	mié 25/09/13
Búsqueda tarifas de precios	1 día	mié 25/09/13	mié 25/09/13
Estudio inicial de viabilidad	1 día	jue 26/09/13	jue 26/09/13
Título, descripción y objetivos del proyecto	1 día	jue 26/09/13	jue 26/09/13
Preparación índice preliminar	1 día	vie 27/09/13	vie 27/09/13
Elaboración planificación temporal	1 día	lun 30/09/13	lun 30/09/13
Elaboración documentación	1 día	mar 01/10/13	mar 01/10/13
Entrega PAC1	1 día	mié 02/10/13	mié 02/10/13
Diseño de red	**32 días**	**mié 02/10/13**	**jue 14/11/13**
Estimación necesidades de ancho de banda			
Nivel troncal y nivel acceso			
Estimación inicial ubicaciones equip			
Simulación cobertura inalámbrica y viabilidad enlaces			
Replanteo ubicaciónes físicas (en caso necesario)			
Validación cobertura inalámbrica y viabilidad enlaces			
Cierre prospección tecnológica	**32 días**	**mié 02/10/13**	**jue 14/11/13**
Selección de tecnologías			
Selección de fabricantes y modelos			
Elaboración documentación	3 días	vie 15/11/13	mar 19/11/13
Entrega PAC2	1 día	mié 20/11/13	mié 20/11/13
Configuración plataforma tecnológica	**12 días**	**mar 19/11/13**	**jue 05/12/13**
Troncal			
Acceso			
Protección equipamiento en exteric			
Elementos de soportación			
Electrónica de conmutación			
Seguridad			
Presupuesto económico	2 días	vie 06/12/13	lun 09/12/13
Mantenimiento y garantías	1 día	mar 10/12/13	mar 10/12/13
Estudio del ámbito legal	2 días	mié 11/12/13	jue 12/12/13
Elaboración documentación	3 días	vie 13/12/13	mar 17/12/13
Entrega PAC3	1 día	mié 18/12/13	mié 18/12/13
Memoria final	**18 días**	**mié 18/12/13**	**vie 10/01/14**
Maquetación y redacción definitiva	17 días	mié 18/12/13	jue 09/01/14
Entrega memoria final	1 día	vie 10/01/14	vie 10/01/14
Presentación	**4 días**	**lun 13/01/14**	**jue 16/01/14**
Síntesis y preparación de presentación	4 días	lun 13/01/14	jue 16/01/14
Entrega presentación		jue 16/01/14	



6.Marco legal

Para adaptar la Ley General de Comunicaciones a la normativa europea, entra en vigor la ley 32/2003[7] convirtiéndose en la ley marco del ámbito de las teleconicaciones.

En los años posteriores, el avance tecnológico ha echo posible que además de los operadores tradicionales surjan nuevos actores en terreno de los ISP. El desarrollo de tecnologías Wifi de ámbito metropolitano y bajo coste permitió a muchos Ayuntamientos plantearse la prestación de servicios de acceso a internet gratuito a sus ciudadados.

Sin embargo, surgieron quejas a la CMT[8] por parte de los operadores. Éstos, consideraron que proyectos pagados con dinero público vulneraba claramente el principio de libre competencia.

La CMT, con la voluntad de regular la prestación de servicios de telecomunicaciones por parte de las AAPP, publica la circular 1/2010[9].

A continuación se destacan los aspectos más importantes de dicha circular:

- ✔ Se recalca que, tal y como se indica en el artículo 6.2 de la Ley General de Telecomunicaciones, la AAPP deberá inscribirse en el registro de operadores. Este trámite es gratuito. El único caso en el que no será necesaria dicha inscripción es cuando se realice una autoprestación (centros educativos, servicios propios, control tráfico,...).

- ✔ Se debe actuar conforme a los principios de la economía de libre mercado:

  - Elaboración de un plan de negocio viable y coherente.

  - Generación de beneficios en un plazo razonable de tiempo.

  - Financiación a través de la publicidad o patrocinio, sin necesidad de recurrir a fondos públicos.

7 https://www.boe.es/buscar/doc.php?id=BOE-A-2003-20253
8 Comisión del Mercado de las Telecomunicaciones
9 http://www.cmt.es/c/document_library/get_file?uuid=f26dcedb-3cfc-429e-8629-303fc2c6de81&groupId=10138

- ✔ Gestión económica completamente independiente, mediante cuentas separadas, aplicando los principios de neutralidad, transparencia y no discriminación.
- ✔ Posibilidad de acometer proyectos con financiación exclusivamente pública si:
  - Se notifica a la CE[10], salvo que el importe de proyecto sea inferior a 200.000€.
  - La CMT confirma que no afecta negativamente al mercado, como por el ejemplo el caso de entornos rurales donde no están presentes los operadores privados.
- ✔ Las AAPP podrán prestar servicio gratuito e indefinido de los siguientes servicios sin afectar a la competencia:
  - Acceso a las páginas web de las AAPP.
  - Acceso a internet en Bibliotecas.
  - Acceso a internet inalámbrico basado en bandas sin licencia, con una velocidad máxima de descarga de 256 Kbps y cobertura en zonas exteriores y no en el interior de las viviendas.

Por tanto, podemos considerar que el presente proyecto cumple la normativa legal vigente.

10 Comisión Europea

7.Requerimientos tecnológicos

En este apartado vamos a describir los criterios de selección de tecnología, utilizando siempre que sea posible normativas estándar de ámbito internacional.

1.Tecnología inalámbrica

1.Wifi

El término Wifi hace referencia a una tecnología inalámbrica de interconexión de dispositivos, con una enorme implantación en la actualidad. Ello ha permitido el desarrollo de distintas tecnologías, todas ellas estandarizadas bajo la norma IEEE 802.11.

Los estándares 802.11 b/g/n, operan en la banda libre de 2,4 Ghz, obteniendo velocidades de hasta 11, 54 y 300 Mbits/s respectivamente.

El estandar 802.11 a opera en la banda libre de 5 Ghz, obteniendo una velocidad de hasta 54 Mbits/s.

El rango de alcance puede considerarse medio, del orden de 20 metros en interiores y algo superior en el exterior.

Puede obtenerse información detallada en apartado de Bibliografía.

2.Wimax

La tecnología Wimax[11], posterior a Wifi, se desarrolló para extender el alcance hasta el orden de decenas de kilómetros.

Según la norma IEEE 802.16, la banda de operación es de 2,3 a 3,5 Ghz. Sin embargo, el elevado coste de licencia de estas bandas impulsó el desarrollo de equipos que pudieran operar en la banda libre de 5,4 Ghz.

Existen dos variantes del estandar: 802.16d para el acceso fijo y 802.16 para movilidad.

Puede obtenerse información detallada en apartado de Bibliografía.

11 Worlwide Interoperatibility for Microware Access

2.Resistencia de los equipos al ambiente

En un proyecto inalámbrico es importante tener en cuenta la exposición de los equipos al medioambiente. Esto es especialmente importante en una zona costera, donde el salitre y la elevada humedad existente pueden deteriorar rápidamente los equipos.

El estándar IEC 60529 define los diferentes grados de protección disponibles.

La nomenclatura estándar que se utiliza viene definida según la norma ICE 941.

2. Ilustración: Nomenclatura protección medioambiental

A continuación se indica el significado de cada una de las cifras:

			2º CIFRA - Protección contra la entrada perjudicial de agua								
			IP_0	IP_1	IP_2	IP_3	IP_4	IP_5	IP_6	IP_7	IP_8
											
1ª CIFRA - Proteccion contra cuerpos solidos de diametro mayor a:			No Protegido	Goteo vertical de agua	Goteo hasta 15º de la vertical	Rociado hasta 60º de la vertical	Rociado en todas direcciones (360º)	Lanzamiento en todas direcciones (360º)	Golpes de mar (olas)	Protegido contra inmersión	Protegido contra submersión
IP0_		Sin Protección	IP 00								
IP1_		50mm	IP 10	IP 11	IP 12						
IP2_		12mm	IP 20	IP 21	IP 22	IP 23					
IP3_		2,5mm	IP 30	IP 31	IP 32	IP 33	IP 34				
IP4_		1,0mm	IP 40	IP 41	IP 42	IP 43	IP 44	IP 45	IP 46		
IP5_		Protegido contra el polvo	IP 50				IP 54	IP 55	IP 56		
IP6_		Libre contra el polvo	IP 60					IP 65	IP 66	IP 67	IP 68

3. Ilustración: Grados de protección medioambiental

Para el presente proyecto vamos a exigir a los equipos que queden ubicados en el exterior un grado de protección mínimo IP66. En el caso de que algún equipo no ofrezca dicha protección, se colocará dentro de un armario de exteriores con la debida certificación.

Puede obtenerse información detallada en apartado de Bibliografía.

3.Alimentación sobre ethernet

PoE[12] es una tecnología desarrollada para transportar sobre el mismo cable de datos LAN que llega al equipo tanto datos como alimentación eléctrica, aprovechando para ello los dos pares de hilos que no son utilizados.

Esta tecnología simplifica el despliegue de equipos al no necesitar disponer de un punto de alimentación eléctrico, algo especialmente útil en equipos como puntos de acceso inalámbricos.

La alimentación sobre Ethernet se rige mediante la norma IEEE 802.3af.

Puede obtenerse información detallada en apartado de Bibliografía.

12 Power Over Ethernet

8.Estructura de red

1.CPD

1.Conexión al ISP

La conexión al ISP se realiza desde el CPD[13] del Ayuntamiento de Cartagena, donde se garantiza el espacio necesario en armarios estándar de 19” debidamente climatizados así como la administración de los nuevos sistemas.

Sin embargo, por cuestiones de seguridad el SI[14] del Ayuntamiento exige que la nueva infraestructura sea lógica y físicamente independiente de la existente.

El SI se encargará de la contratación de la conexión a internet con Movistar. Dado que el ancho de banda necesario se estima en 18 Mbps, no es posible utilizar una conexión ADSL por lo que se contratará una conexión FTTH[15] con 100 Mbps de bajada y 10 Mbps de subida con su correspondiente router.

2.Servicio de directorio

A la hora de seleccionar un servicio de directorio de usuarios, vamos a tener en cuenta que:

- ✔ El número de usuarios previsto no debe ser muy grande, estimando unos 500 en una primera fase.
- ✔ No se plantea interacción de estos usuarios con las unidades organizativas existentes.
- ✔ Deberá ser sencillo de administrar y con un coste reducido.

Optaremos por tanto por un servicio de autentificación basado en usuarios locales de Linux. Dado que se almacenan datos personales, el SI se encargará de actualizar la política de ficheros de la LOPD[16].

13 Centro de Proceso de Datos
14 Servicio de Informática
15 Fiber To The Home
16 Ley Orgánica de Protección de Datos

3.Firewall

Aunque la nueva infraestructura va a estar completamente aislada del resto del entorno de producción del Ayuntamiento, sigue siendo necesaria la implantación de un firewall.

De esta forma, se podrá controlar el acceso de los usuarios a determinadas páginas así como reducir el riesgo de infección por virus y malware.

Vamos a optar por el fabricante Fortinet, ya que dispone de una gama de productos amplia, robusta y sencilla de configurar.

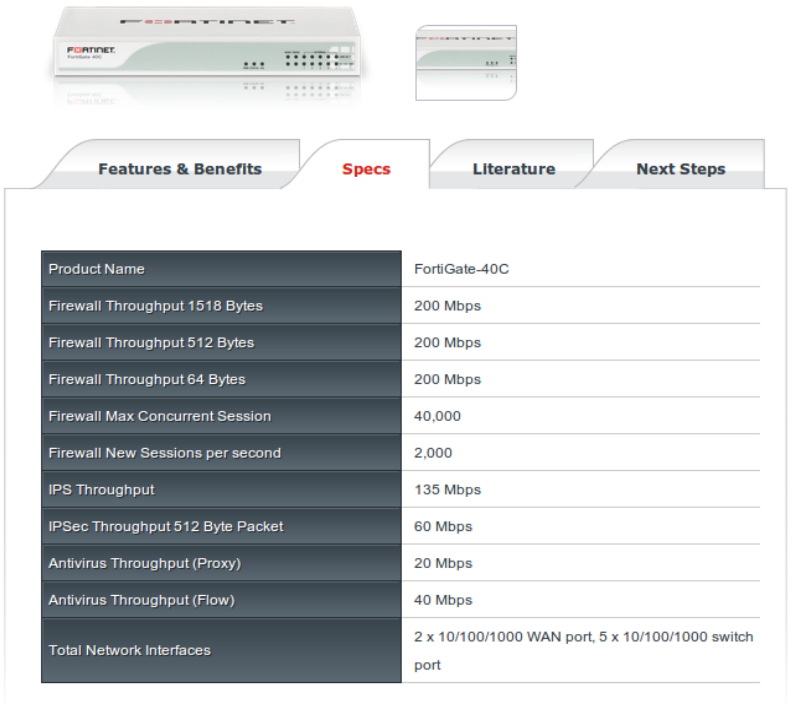
Fortinet posiciona sus productos en tres niveles: High-End, Mid-Range y Desktop. Vamos a centrarnos en la gama inferior.

El fabricante facilita la elección del modelo adecuado dimensionándolos por su throughput[17]. Recordemos que la estimación de ancho de banda inicial prevista es de 18 Mbps.

El Fortigate 20C tiene un throughput de 20 Mbps, lo cual nos deja sin capacidad de crecimiento.

17 Capacidad de proceso

Pasamos al modelo inmediatamente superior, Fortinet 40C.



Features & Benefits | Specs | Literature | Next Steps

Product Name	FortiGate-40C
Firewall Throughput 1518 Bytes	200 Mbps
Firewall Throughput 512 Bytes	200 Mbps
Firewall Throughput 64 Bytes	200 Mbps
Firewall Max Concurrent Session	40,000
Firewall New Sessions per second	2,000
IPS Throughput	135 Mbps
IPSec Throughput 512 Byte Packet	60 Mbps
Antivirus Throughput (Proxy)	20 Mbps
Antivirus Throughput (Flow)	40 Mbps
Total Network Interfaces	2 x 10/100/1000 WAN port, 5 x 10/100/1000 switch port

4. Ilustración: Especificaciones Firewall Fortinet 40C

Como vemos, el throughput excede sustancialmente nuestros requerimientos. Sin embargo, siempre es recomendable que el equipo tenga margen de rendimiento. Esto es debido a que los sistemas UTM[18] disponen de múltiples funcionalidades (antivirus, control malware, IPS[19], VPN[20],...) que si son habilitadas pueden generar una elevada carga de trabajo que llegue a saturar la CPU.

Vamos a configurar ahora la política de seguridad. Inicialmente, los servicios que vamos a permitir utilizar a los usuarios son los siguientes:

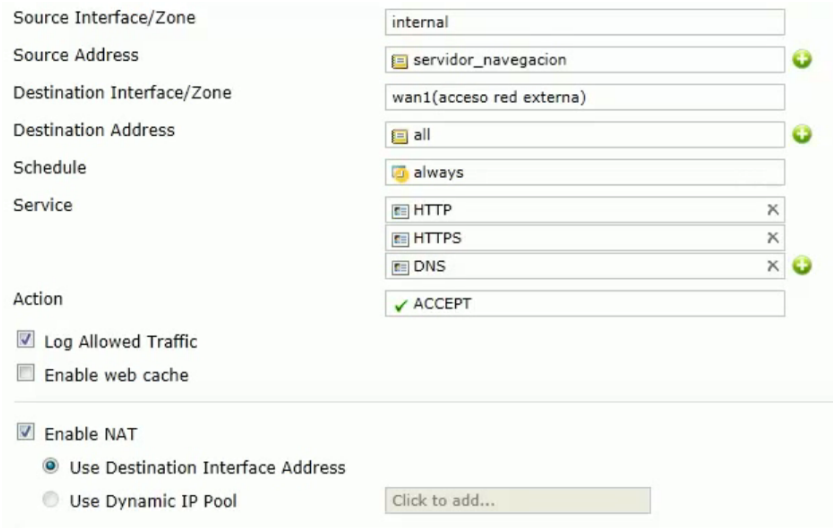
- ✔ DNS.
- ✔ POP3 e IMAP.
- ✔ Navegación web (http).
- ✔ Navegación web segura (https)

18 Unified Threat Manegement
19 Intrusion Prevention System
20 Virtual Private Network

El resto de servicios serán explicitamente denegados.

Para ello iremos al menú Policy, donde por defecto existe ya una regla que deniega todo independientemente de su origen y destino.

Dicha regla, que llamaremos “Regla navegación”, tendrá como interfaz de origen la pata LAN[21] del firewall y como destino la pata WAN[22] que está conectada al router.



5. Ilustración: Configuración política seguridad Fortinet

En el apartado “Source Address”, podríamos dejar que todas las direcciones IP de la red interna accedieran a internet. Sin embargo, en el diseño se ha previsto la utilización de un proxy para que todos los usuarios se autentifiquen. Por tanto, sólo vamos a permitir a dicho equipo “Servidor_navegacion” que pueda pasar por el firewall.

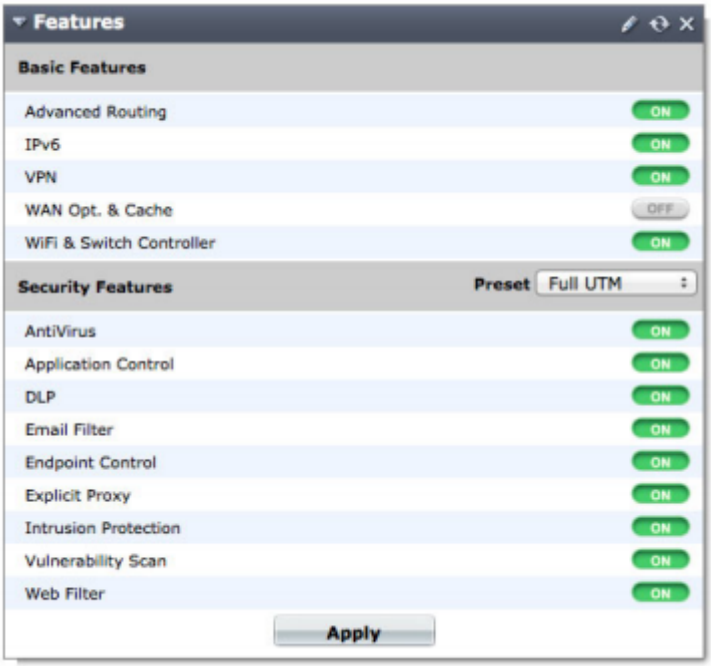
Habilitaremos el logeado de tráfico, que permitiría un posterior análisis en caso de ser necesario, así como el NAT[23].

Finalmente activaremos el checkbox de UTM, que nos permitirá posteriormente seleccionar el tratamiento que queremos realizar sobre el flujo de datos.

21 Local Area Network
22 Wide Area Network
23 Network Address Translation

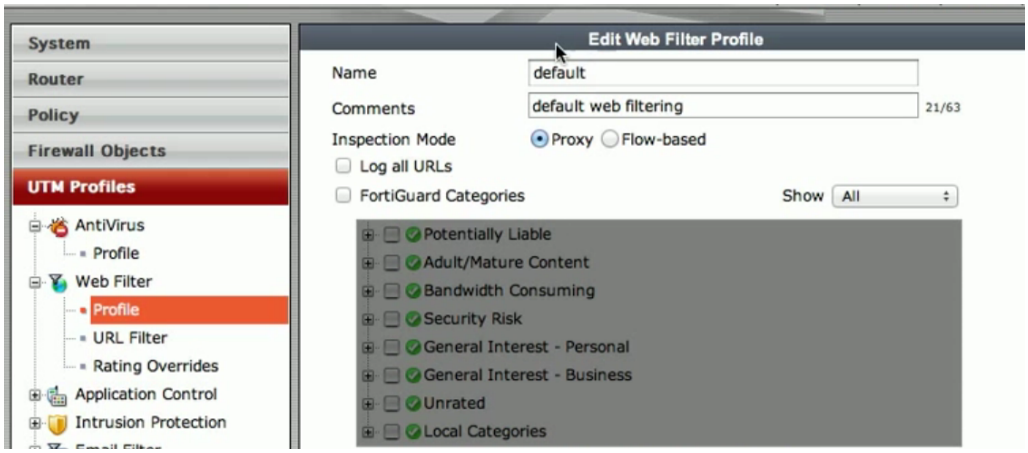
Resulta trivial la activación de los diferentes servicios UTM que aplican en el escenario propuesto,Accediendo al menú desde System > Config > Features.:

- ✔ Wan Optimization & Caché.
- ✔ Antivirus.
- ✔ Intrusion Protection Web Filter.



6. Ilustración: Selección funcionalidades UTM

Una vez activada la funcionalidad de filtrado web, podemos definir desde el siguiente menú el tipo de páginas cuyo acceso se va a restringir.



7. Ilustración: Configuración del filtrado web

4.Proxy/DHCP

El Ayuntamiento solicita que los usuarios se autentifiquen antes de acceder a internet. Para cubrir este requisito, vamos a implementar un proxy mediante SQUID corriendo sobre un servidor Linux.

Cuando el usuario solicita su login, se le proporcionará también la dirección del servidor proxy que debe utilizar y la forma de configurarlo en los diferentes navegadores.

En el propio servidor correrá el servicio DHCP[24], de modo que la dirección IP será asignada automáticamente al dispositivo del usuario.

Los usuarios serán dados de alta localmente en el servidor, utilizando para la autentificación el módulo NCSA[25]. Para ello creamos el fichero de usuarios mediante el siguiente comando:

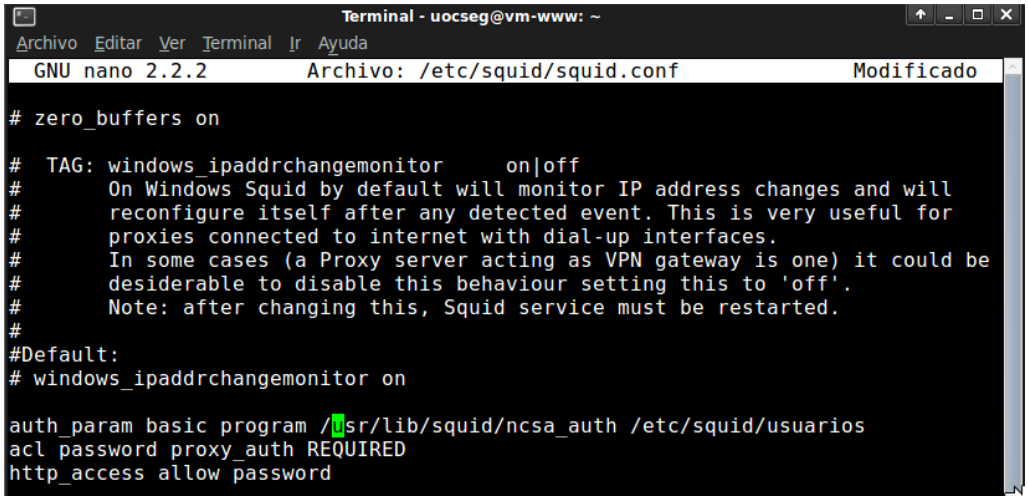
```
uocseg@vm-www:~$ sudo htpasswd -c /etc/squid/usuarios usuario1
Adding password for usuario1.
New password:
Re-type new password:
```

8. Ilustración: Creación del fichero de usuarios del proxy

24 Dynamic Host Configuration Protocol
25 National Center for Supercomputing Applications

Siendo necesario crear el primer usuario.

A continuación editamos el fichero de configuración de squid.



9. Ilustración: Edición del fichero de configuración de squid

De este modo los usuarios deberán introducir su usuario y contraseña para poder acceder a Internet, una vez reiniciado el servicio squid para que tomen efecto los cambios.

5.Acceso del usuario al sistema

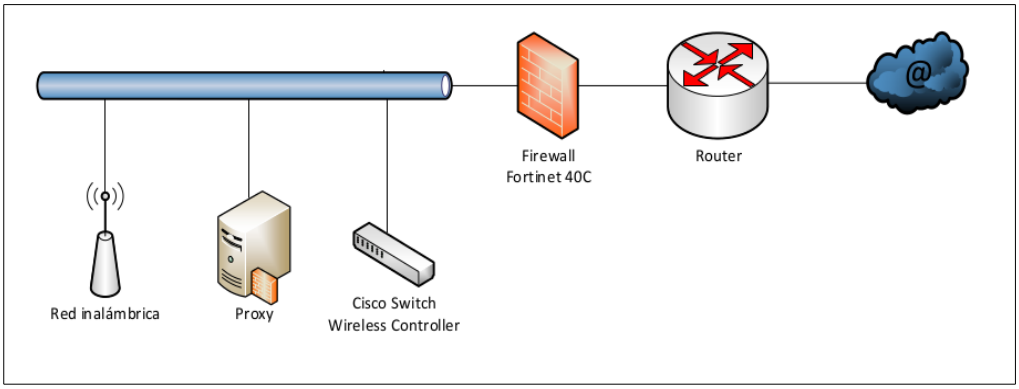
A continuación se resume el procedimiento que debe seguir el usuario para poder acceder a internet.

1. Solicitar en el Ayuntamiento el alta en el sistema.
2. Configuración de los datos de conexión proporcionados (DNS, proxy) así como el procedimiento para configurarlo en los diferentes navegadores.
3. Introducción del usuario y contraseña en el portal de entrada del proxy.

6.Esquema lógico

Como ya se ha mencionado anteriormente, el diseño de esta nueva red es totalmente independiente de la infraestructura existente a nivel de conexionado, si bien comparte infraestructura de CPD para el control de acceso, climatización y alimentación estabilizada.

A continuación, se muestra a continuación el esquema lógico de los equipos a instalar:



10. Ilustración: Esquema lógico del CPD

El router, proporcionado por el ISP, dispone de dos interfaces. Un interfaz de fibra óptica que se conecta a la red FTTH y un puerto Gigabit Ethernet que se conecta directamente al interfaz Gigagit Ethernet WAN del Firewall.

El resto de equipos se encuentran detrás del firewall, por tanto se conectarán a su interfaz LAN. Para concentrar todos los puertos de conexión físicos utilizaremos el Cisco Switch Wireless Controller.

Finalmente, conectaremos también a dicha red LAN el interfaz Ethernet del suscriptor Wifi que se encuentra en el tejado del CPD, y que da acceso a Internet a la red inalámbrica.

2.Estructura inalámbrica

1.Visión general

En primer lugar vamos a estudiar una vista general de la ciudad, con las tres áreas a las que se debe dar cobertura:

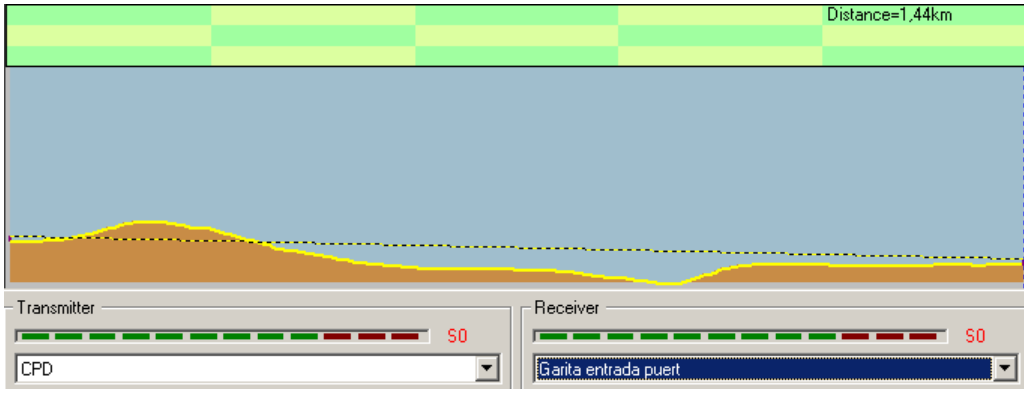
- ✓ Diputación de Santa Lucía.
- ✓ Terminal de contenedores del Muelle de San Pedro.
- ✓ Cala Cortina.

11. Ilustración: Vista general de la ciudad de Cartagena

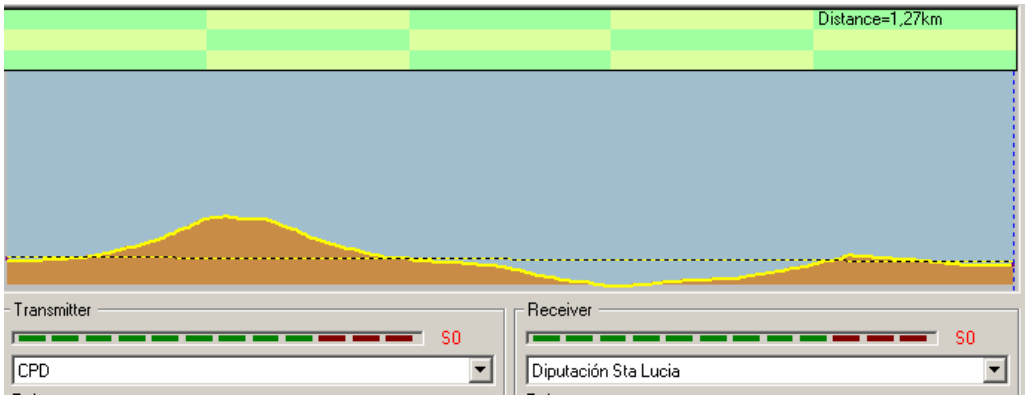
El CPD del Ayuntamiento de Cartagena, donde está disponible el acceso a internet, se encuentra situado en el centro de la ciudad.

En un primer análisis de la imagen aérea, podemos intuir que existirán problemas de visibilidad entre las diferentes áreas de cobertura, punto crítico en las tecnologías inalámbricas

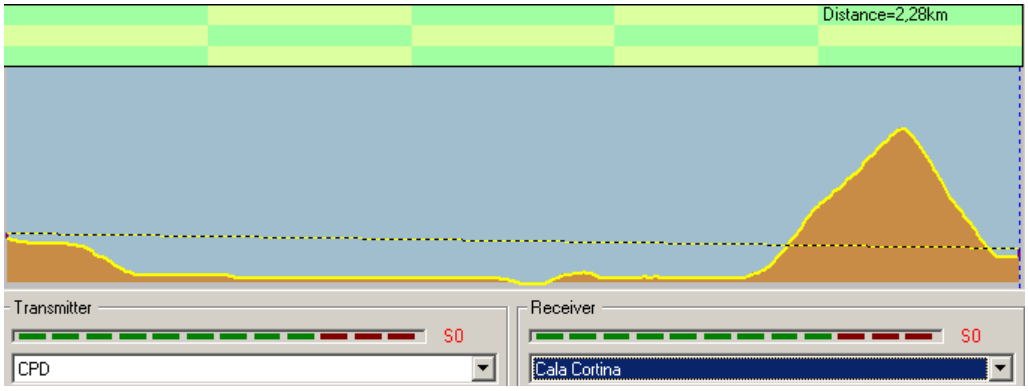
Efectivamente, el promontorio del Parque Torres se interpone en la linea de visión directa, tal y como nos muestra Radio Mobile.



12. Ilustración: Sección CPD-Muelle de San Pedro



13. Ilustración: Sección CPD-Santa Lucía



14. Ilustración: Sección CPD-Cala Cortina

Por tanto, hemos de localizar una elevación que nos permita salvar dichos obstáculos.

Existe un promontorio que cierra la dársena de Cartagena por su margen izquierda, donde se encuentra el castillo de Galeras. Dicha ubicación nos permitiría librar los obstáculos observados, sin embargo es zona militar por lo que no es posible ubicar antenas en él.

Sin embargo, en la margen derecha de la dársena se encuentra el castillo de San Julián. Con 274 metros de altitud, domina toda la ciudad y cuenta con la ventaja de disponer de alimentación eléctrica y estructuras de soportación, lo cual simplificaría las tareas de instalación.

Como puede observarse en la foto, actualmente están en servicio distintas antenas de radio, telefonía móvil y televisión.

15. Ilustración: Infraestructuras Castillo de San Julián

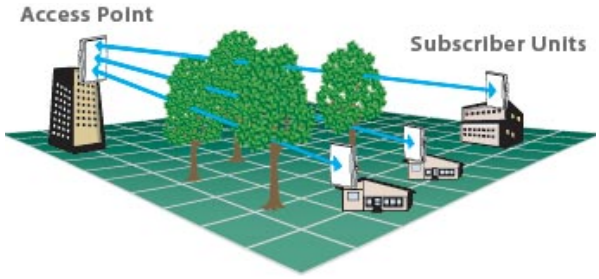
2.Espectro del espacio radioeléctrico utilizado

La selección de las frecuencias de trabajo utilizadas y por tanto los equipos a utilizar, viene condicionada por una serie de condicionantes de diseño.

- ✔ Hemos de interconectar diferentes áreas de cobertura Wifi, que se encuentran a distancias de hasta 2 Km.
- ✔ Existen obstáculos orográficos.
- ✔ Para simplificar los trámites burocráticos, se optará preferentemente por utilizar frecuencias de licencia libre.
- ✔ El coste total del proyecto.

Existen sistemas de enlaces inalámbricos para largas distancias y NLOS[26] trabajando en la banda de 900Mhz. Esta solución nos permitiría establecer directamente los enlaces de cada zona Wifi con el CPD, sin necesidad de utilizar el monte San Julián como punto intermedio.

Sin embargo, el elevado coste de estos equipos y la necesidad de licenciamiento hacen inviable esta solución.



16. Ilustración: Comunicación sin visión directa

Por tanto, para los enlaces entre zonas utilizaremos tecnología Wimax en su banda no licenciada aunque implique la utilización de más equipamiento para salvar los obstáculos naturales al necesitar una linea de visión más limpia.

Para el acceso inalámbrico de los terminales de usuario, utilizaremos la tecnología Wifi basada en los estándares 802.11 a/b/g/n.

26 No Line Of Ssight

Resumiendo utilizaremos las siguientes bandas de frecuencia:

- ✔ Wimax: 5,470-5,725 Ghz
- ✔ 802.11 b/g: 2,4-2,497 Ghz
- ✔ 802.11 a: 5,15-5,35 Ghz, 5,425-5,675 Ghz, 5,725-5,875 Ghz

Con respecto a la potencia de emisión de los equipos, al tratarse de una banda no licenciada se configurarán para no superar los límites de PIRE establecidos. En el caso de Wimax la potencia máxima no debe superar 1W y en el caso de Wifi 0,1W para la banda de 2,4 Ghz y 0,2W para la banda de 5 Ghz.

3.Topología red troncal Wimax

Selección de equipos

Hemos optado por el fabricante Alvarion en base a los siguientes criterios:

- Empresa pionera en el desarrollo de equipos Wimax.
- Elevado número de instalaciones en España, tanto para AA.PP como ISP´s privados.
- Elevada protección ante las inclemencias meteorológicas.
- Facilidad de instalación y administración.

Alvarion tiene un amplio catálogo de productos, nos vamos a centrar en la gama BreezeMAX Extreme. Dicha gama cuenta con tres modelos: 3600, 3650 y 5000. Los dos primeros están destinados a la banda de frecuencias de Wimax en Estados Unidos, por lo que el modelo elegido será el 5000.

Estos equipos permiten trabajar en topologías punto a punto o punto-multipunto, que en la que configuraremos en el presente proyecto.

A nivel de protección ambiental, están certificados IP67, por lo que exceden los requerimientos solicitados.

Disponemos de dos equipos diferentes:

- ✔ Base Station: Es el equipo que se coloca en el centro de la estrella. Incluye una antena integrada de sector y 14,5 dBi, así como un conector para añadir una antena externa. Va configurado en un único chasis preparado para exterior. El sistema de alimentación es mediante PoE[27].

- ✔ CPE: Es el equipo cliente o suscriptor. Incluye una antena integrada de sector y 16 dBi. Este equipo está separado en dos partes, llamadas IDU[28] y ODU[29] que se comunican entre sí mediante un cable Categoría 5E de hasta 90 metros.

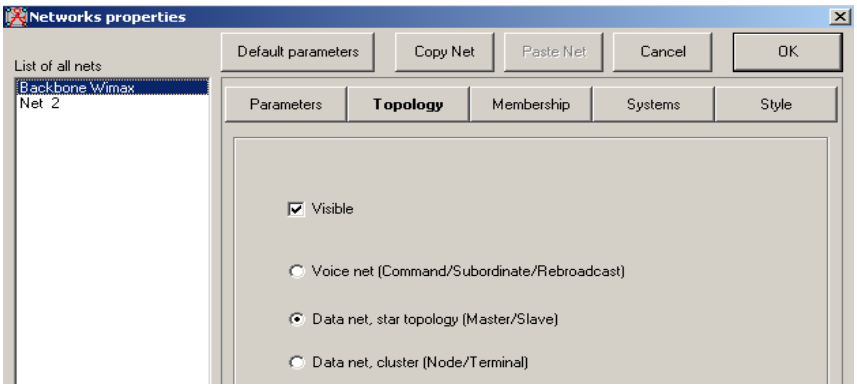
Dada la orografía de la zona, situaremos una Base Station en el castillo de San Julián, sirviendo como centro de la estrella.

En cada uno de los extremos de la estrella ubicaremos una unidad CPE.

Cálculo de viabilidad de los enlaces

En primer lugar, crearemos en Radio Mobile una nueva red que llamaremos “Backbone Wimax”.

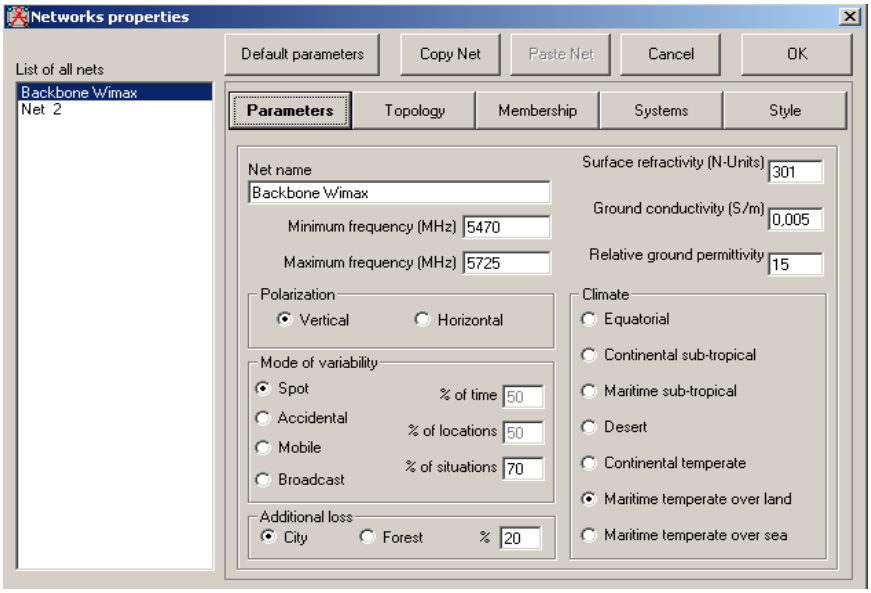
Dicha red la configuraremos con una topología de estrella.



17. Ilustración: Configuración topología red Wimax

27 Power Over Ethernet
28 Indoor Unit
29 Outdoor Unit

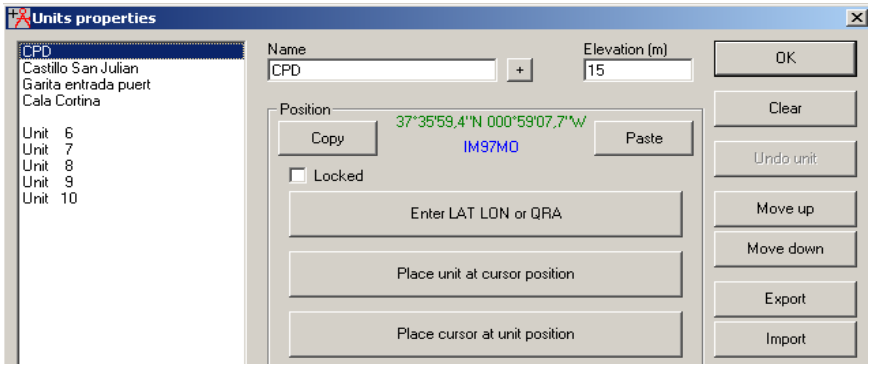
A continuación configuramos los parámetros generales:



18. Ilustración: Configuración parámetros generales red Wimax

Introducimos la banda de frecuencias, climatología, polarización,... Por la ubicación geográfica de cada zona vamos a estimar unas perdidas adicionales suponiendo que un 20% del recorrido es por ciudad.

A continuación introducimos las ubicaciones físicas. Una forma sencilla es crear la ubicación en Google Earth y copiarla en Radio Mobile.



19. Ilustración: Configuración ubicaciones red Wimax

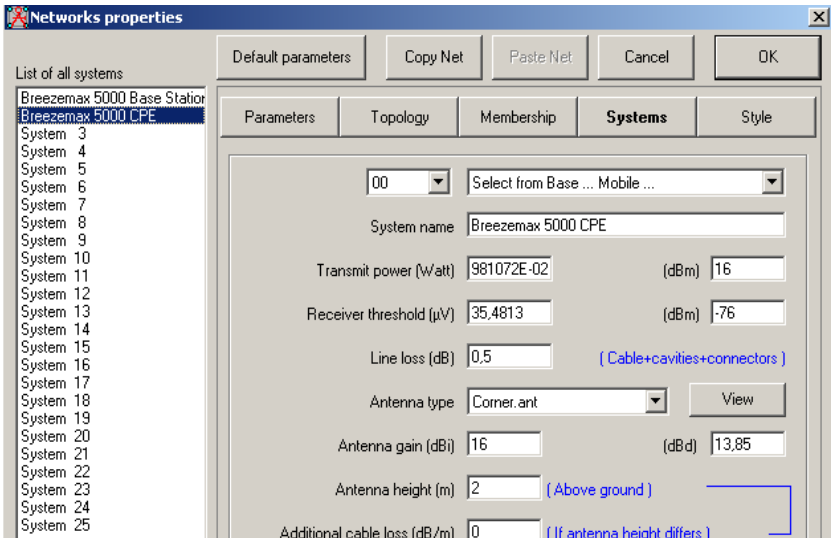
Hemos de tener en cuenta que la altitud que considera Radio Mobile en cada punto es a ras de suelo. Por tanto, como en el caso del CPD la antena estará instalada en lo alto de un edificio de 4 plantas, agregamos 15 mts de elevación.

Ahora configuramos los equipos de comunicación.

En la documentación de la estación base se indica que trae una antena direccional integrada de 14,5 dBi con opción de conectar una antena externa. Dada la ubicación de las unidades suscriptoras, necesitamos agregar una antena omnidireccional de 9,5 dBi.

Consideraremos unas pérdidas en el cable de 0,5 dB.

Con respecto a la potencia de transmisión según se indica en el apartado de legislación la PIRE[30] máxima ha de ser de 1W. Este equipo puede ajustar su potencia de 1 a 21 dBm en pasos de un dBm.

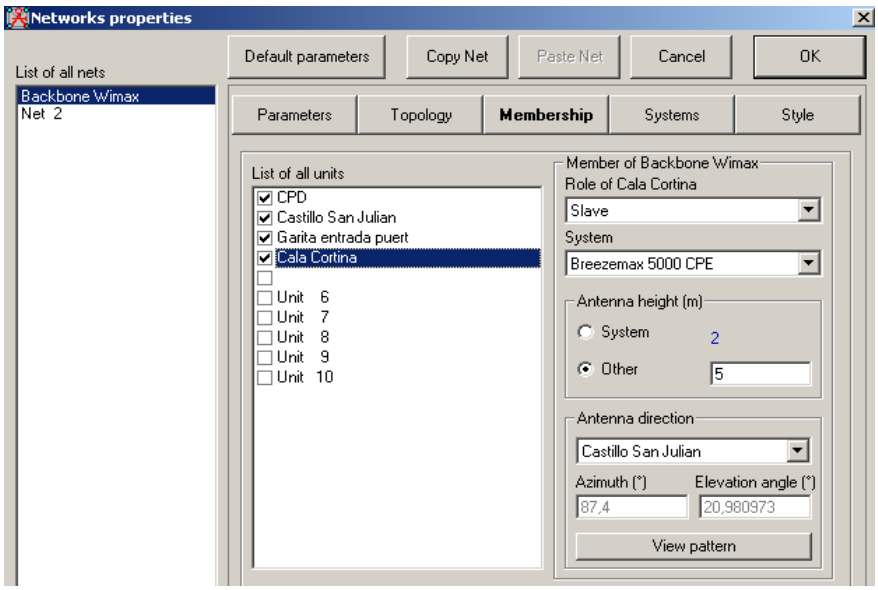


20. Ilustración: Configuración propiedades sistemas Wimax

A continuación configuramos la unidad suscriptora, que dispone de una antena directiva de 16 dBi.

30 Potencia isotrópica radiada equivalente

Por último, en la pestaña Membership realizamos la asociación entre las ubicaciones físicas y los equipos que se van a instalar en cada una de ellas.



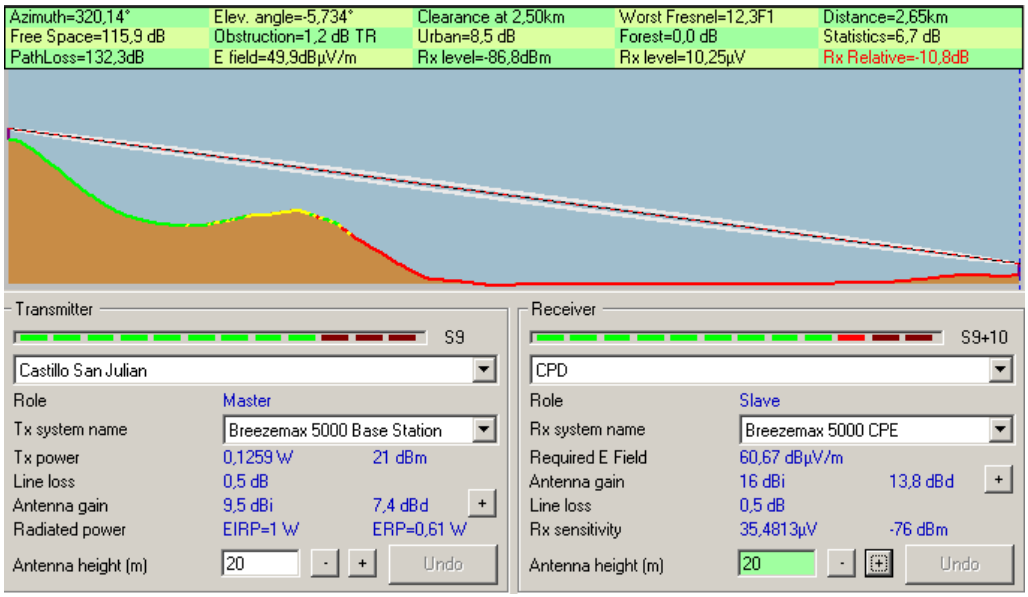
21. Ilustración: Configuración membership red Wimax

Para cada una de las ubicaciones se indica la altura a la que quedará ubicada la antena.

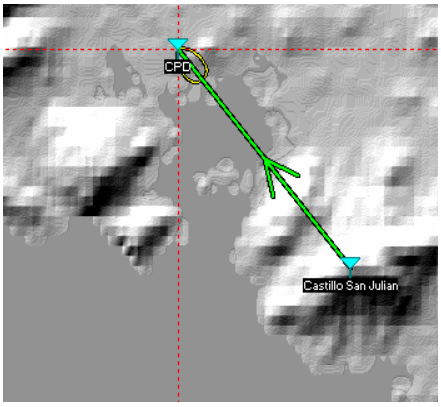
En el caso de los equipos suscriptores equipados con antenas directivas, es importante así mismo configurar el azimuth para que quede alineado con la dirección en que se encuentra la estación base. De este modo obtendremos el máximo rendimiento posible del enlace.

Ya podemos comenzar a comprobar la viabilidad de los enlaces.

Enlace Castillo de San Julián-CPD:

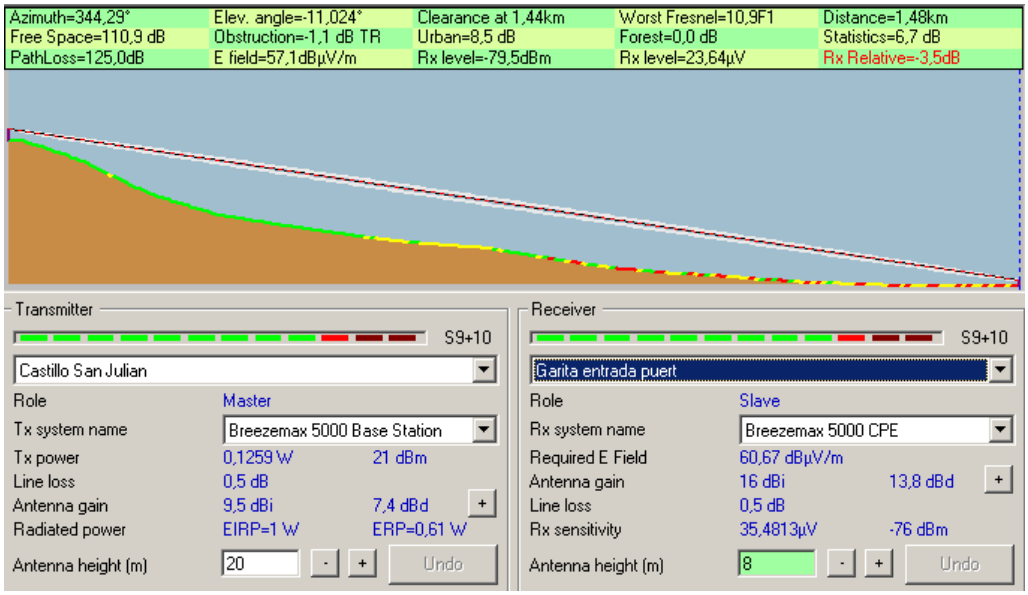


22. Ilustración: Viabilidad enlace Castillo San Julián-CPD



23. Ilustración: Orientación antena CPD

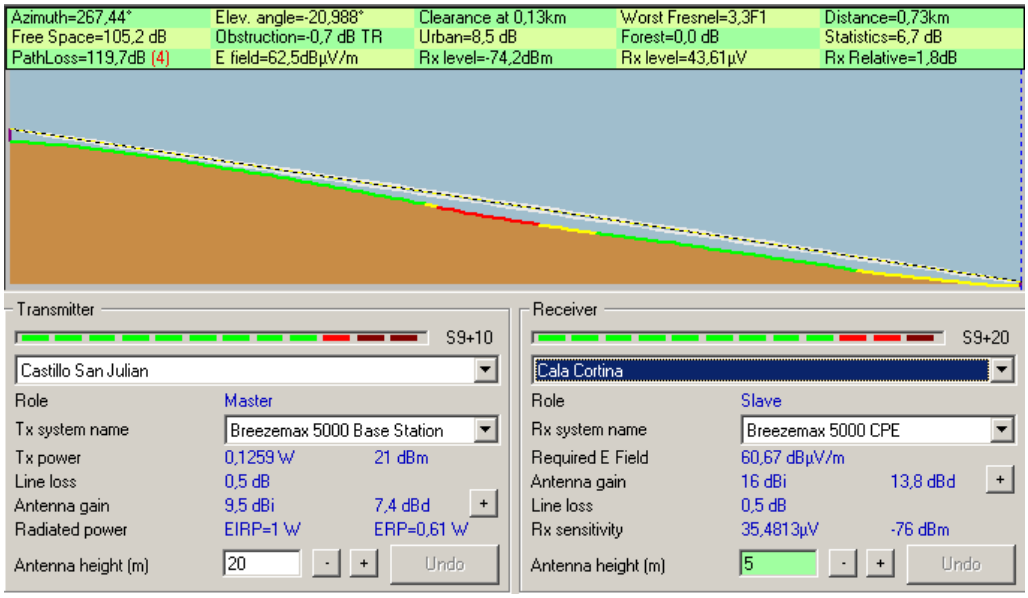
Enlace Castillo de San Julián-Garita de entrada muelle de San Pedro



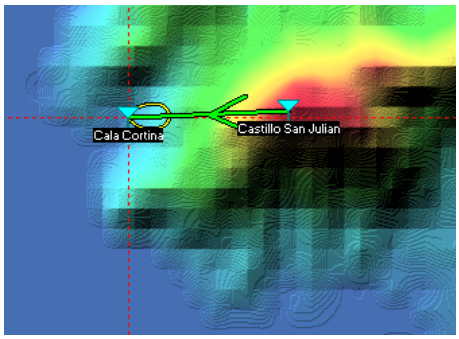
24. Ilustración: Viabilidad enlace Castillo San Julián-Garita

25. Ilustración: Orientación antena garita

Enlace Castillo de San Julián-Cala Cortina



26. Ilustración: Viabilidad enlace Castillo-Cala Cortina

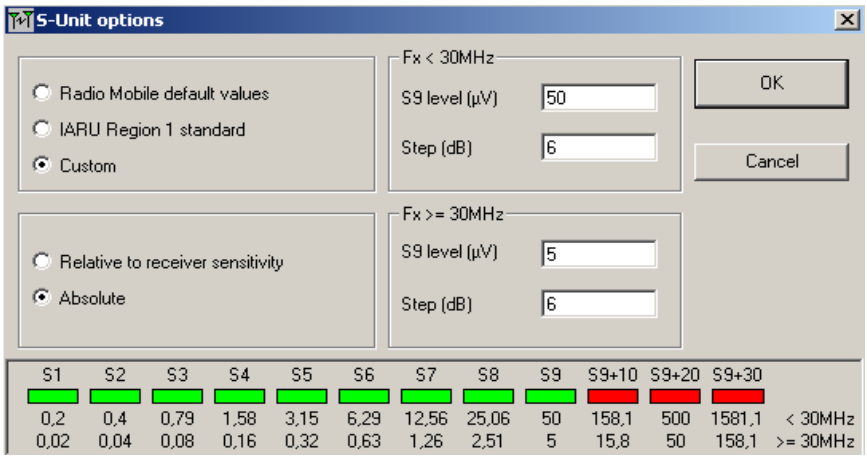


27. Ilustración: Orientación antena Cala Cortina

A primera vista, el color verde de la flecha nos indica que los enlaces son viables.

Podemos observar también que aparece una escala de color desde S1 a S9+30, llamadas S-Units.

En el programa podemos configurar los valores correspondientes a dicha escala.



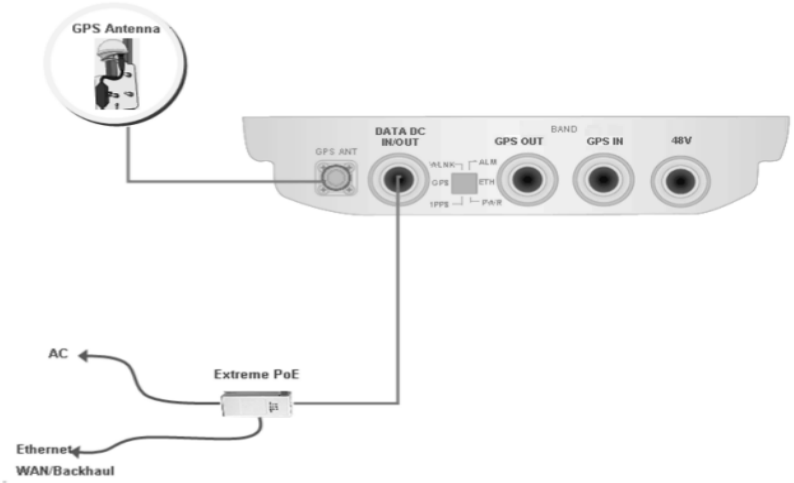
28. Ilustración: Configuración S-Units Radio Mobile

Para frecuencias superiores a 30 Mhz, como es el caso, S9 corresponde a 5µV. Este valor equivale a -93 dBm con una impedancia de 50 Ω.

Todos los enlaces alcanzan o mejoran el valor de S9, por tanto entran dentro de los valores de sensibilidad mínima de -76 dBm y alcanzarán un ancho de banda elevado.

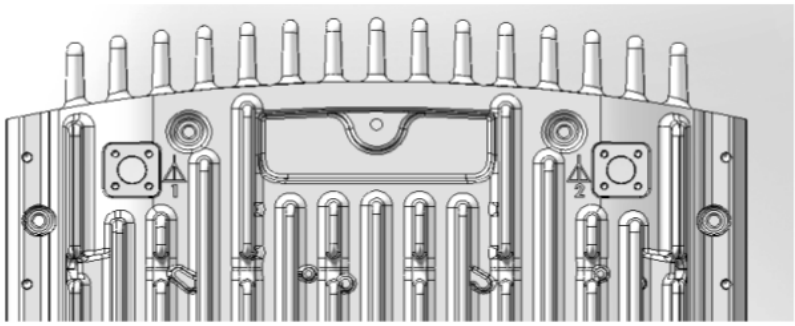
Configuración de los equipos

Dada la ubicación en exterior tanto de la Base Station como los suscriptores CPE, el fabricante ha minimizado el número de cables que llegan al equipo. Para ello, utiliza la tecnología PoE[31], que aprovechando los pares libres de un cable Categoría 5E hace llegar tanto alimentación como datos al equipo.



29. Ilustración: Alimentación PoE BreezeMax Base Station

En el caso de la Base Station, el diseño requiere una antena exterior omnidireccional, que se conecta a uno de los conectores cuadrados de la figura.

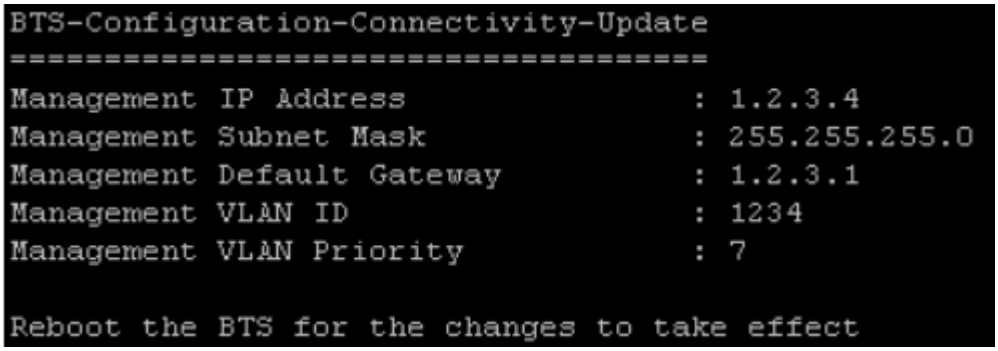


30. Ilustración: Conector antena externa BreezeMax Base Station

31 Power Over Ethernet

Procedemos a la configuración de la Base Station, que será el centro de la red de distribución de datos. Para ello nos conectamos via Telnet a la aplicación Monitor, embebida en el propio equipo.

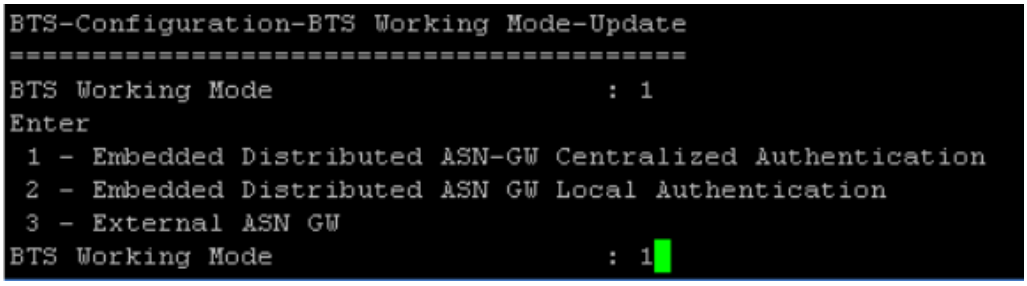
Mediante el menú 1.BTS > 4.Configuration > 3.Connectivity > 2.Update instroducimos la información de red. Es necesario reiniciar el equipo para que los cambios tengan efecto.



31. Ilustración: Configuración IP Base Station Alvarion

A continuación configuramos el modo de trabajo de la Base Station. En sistemas Wimax Punto-Multipunto, se crea una red de acceso formada por los BS y CPE, donde el nodo central ejerce el rol de ASN-GW[32]. Como mecanismo de seguridad, la BS registra las direcciones MAC de los suscriptores.

Para ello, en el menú 1.BTS > 4.Configuration > 2.BTS Working Mode > 2.Update seleccionamos la opción ASN-GW Centralized Authentication.

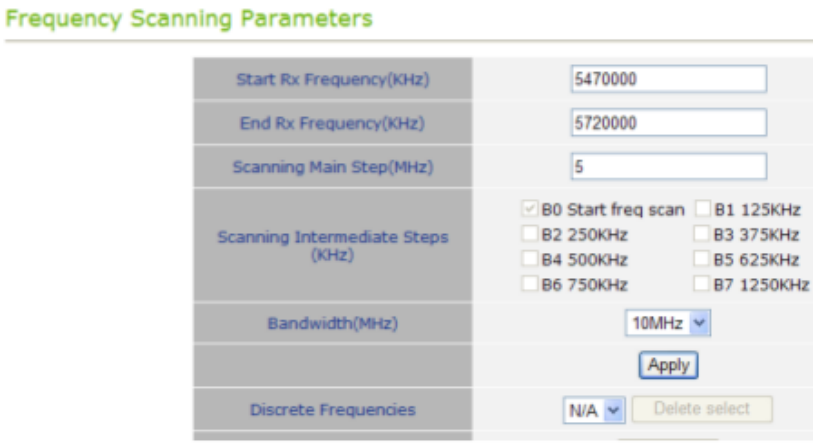


32. Ilustración: Configuración modo ASN-GW Base Station Alvarion

32 Access Service Network-Gateway

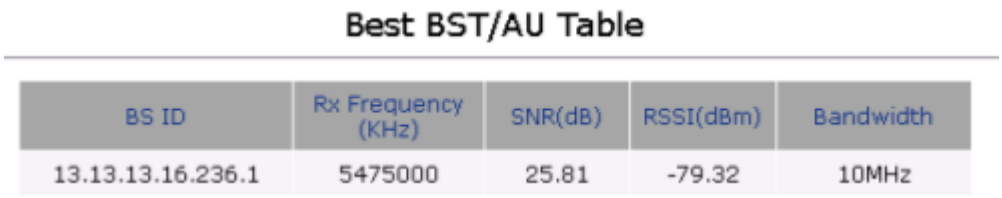
A continuación realizamos la configuración de los equipos CPE, mediante una aplicación web a la que accedemos introduciendo en el navegador la dirección IP por defecto 192.168.254.251 .

En primer lugar configuramos los parámetros de escaneo para detectar la Base Station.



33. Ilustración: Configuración frecuencias escaneo CPE Alvarion

Al realizar el escaneo se muestran las Base Station detectadas.



34. Ilustración: Estaciones Base detectadas en el escaneo

Ya podemos registrar el suscriptor en la BS. Es importante seleccionar el botón “EAP TTLS” para la encriptación de la contraseña.

35. Ilustración: Registro suscriptor Wimax en estación base

Ahora es necesario tomar nota de la dirección Air-MAC[33] del suscriptor para poder provisionarlo en la Base Station, que corresponde a MAC Ethernet del equipo incrementado su valor hexadecimal en uno.

Por ejemplo, el suscriptor con dirección MAC 00:12:CF:C8:DE:A4 tiene la Air-MAC 00:12:CF:C8:DE:A5 .

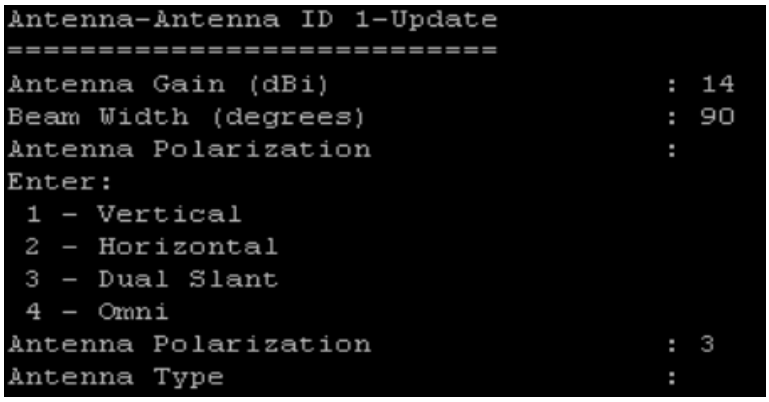
Con este valor, vamos al menú 8.MS > 6.Add de la Base Station y lo introducimos para poder provisionarlo.

```
ASN GW-Services-MSs Services-Add
================================
MS MAC Address                        : 00:12:CF:C8:DE:F9
Service Number                        :
Enter a decimal number in the range 1 to 3
Service Number                        : 1
Admin Status                          :
Enter 1 - Enable, 2 - Disable. Default value is  2 - Disable.
Admin Status                          : 1
Multiple Service Flow Name            : msf_ip_cs_mng
Service Profile Name                  :
Enter a string of 1 to 32 printable characters
Service Profile Name                  : sp_ip_cs_mng
```

36. Ilustración: Provisión suscriptor Wimax con dirección Air-MAC

33 Dirección MAC inalámbrica

Para el caso de los equipos suscriptores, vamos a utilizar la antena integrada por lo que no es necesaria configuración adicional. Sin embargo, la Base Station incorpora una antena externa que deberá ser configurada en el menú 6.Antenna > 2.Select > 1 > 2.Update

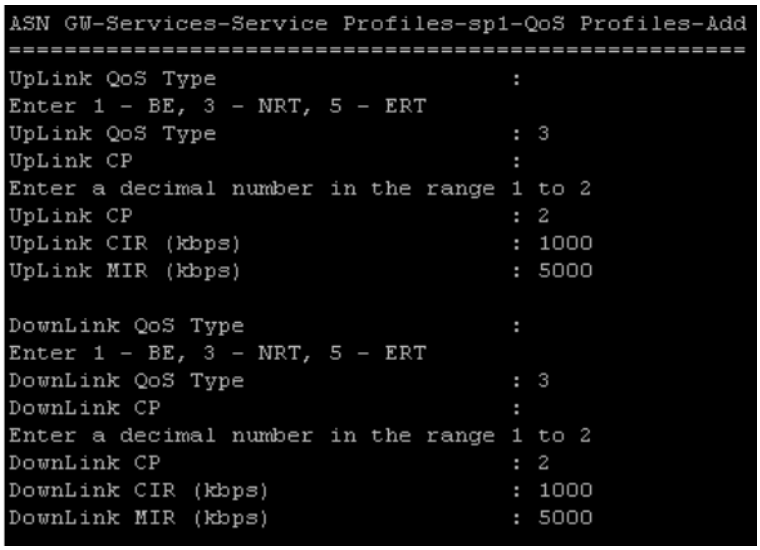


37. Ilustración: Configuración antena externa omnidireccional

En nuestro caso, la ganancia es 9,5 dBi, los grados de cobertura 360 y el tipo de antena Omni.

Asímismo, podemos establecer en la Base Station una política de priorización de tráfico mediante QoS, contemplando cinco colas: 1 - Data, 2 - VoIP, 3 - Management, 4 - PPPoE, 6 – Reliable Video .

De este modo, podemos asignar anchos de banda fijos a cada servicio, tanto de subida como de bajada.



38. Ilustración: Configuración QoS en la estación base Wimax

Finalmente, queda limitar la potencia de emisión de la Base Station a 21 dBm para cumplir los requerimientos de PIRE y limitar el umbral de saturación de los suscriptores a -16 dBm para no dañar los equipos.

4.Topología red acceso Wifi

Selección de equipos

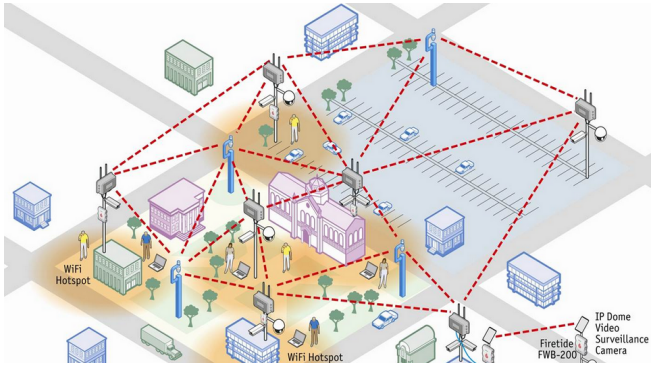
Hemos seleccionado al fabricante Cisco para proporcionar los equipos de acceso Wifi, dentro de la serie 1530.

Existe un modelo 1530E que ofrece la posibilidad de incorporar antenas externas. Sin embargo, consideramos suficiente el modelo 1530I que integra tres antenas omnidireccionales con una ganacia de 3 dBi para 2,4 Ghz y 5 dBi para 5 Ghz.

39. Ilustración:
Cisco Aironet 1530

Estos equipos ofrecen las siguientes características:

- ✔ Certificación IP67 contra inclemencias climatológicas.
- ✔ Alimentación mediante PoE.
- ✔ Soporte para tecnología mesh[34], que permite utilizar la banda de 2,4 Ghz para el acceso de los dispositivos y la banda de 5 Ghz para la transmisión de datos entre los distintos puntos de acceso.



40. Ilustración: Topología de red inalámbrica mallada

34 Mallada

A continuación se muestra la sensibilidad en recepción:

1530I 802.11b (Complementary Code Keying [CCK])	1530I 802.11g (non HT20)
-97 dBm @ 1 Mbps	-95 dBm @ 6 Mbps
-94 dBm @ 2 Mbps	-92 dBm @ 9 Mbps
-92 dBm @ 5.5 Mbps	-90 dBm @ 12 Mbps
-90 dBm @ 11 Mbps	-87 dBm @ 18 Mbps
	-84 dBm @ 24 Mbps
	-81 dBm @ 36 Mbps
	-78 dBm @ 48 Mbps
	-75 dBm @ 54 Mbps

41. Ilustración: Sensibilidad recepción Aironet 1530

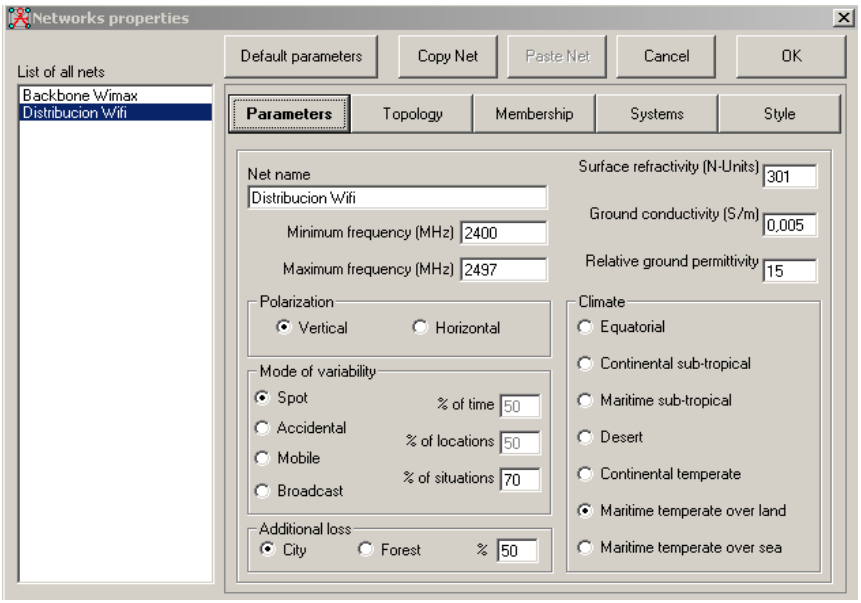
Así como la potencia de transmisión

2.4 GHz	5 GHz
• 802.11b (CCK) ▫ 27 dBm with 2 antennas ▫ 29 dBm with 3 antennas • 802.11g (non HT duplicate mode) ▫ 27 dBm with 2 antennas ▫ 29 dBm with 3 antennas • 802.11n (HT20) ▫ 27 dBm with 2 antennas ▫ 29 dBm with 3 antennas	• 802.11a ▫ 27 dBm with 2 antennas • 802.11n (HT20) ▫ 27 dBm with 2 antennas • 802.11n (HT40) ▫ 27 dBm with 2 antennas

42. Ilustración: Potencia transmisión Aironet 1530

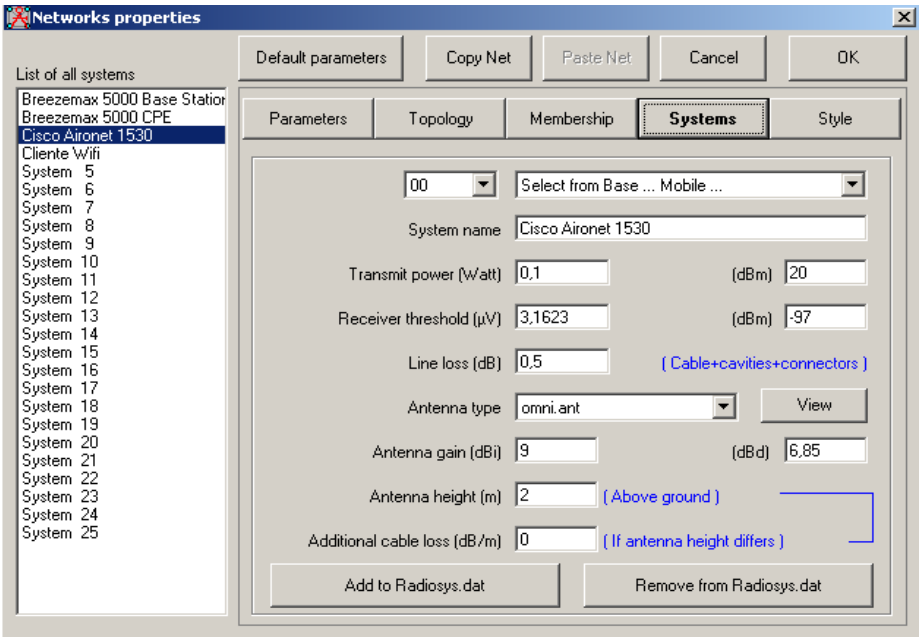
Cálculo de viabilidad de la cobertura

En primer lugar creamos una nueva red, llamada “Distribución Wifi” y configuramos la banda de frecuencia y el clima. Dado que nos encontramos en un entorno urbano, vamos a añadir una pérdida adicional provocada por los edificios.



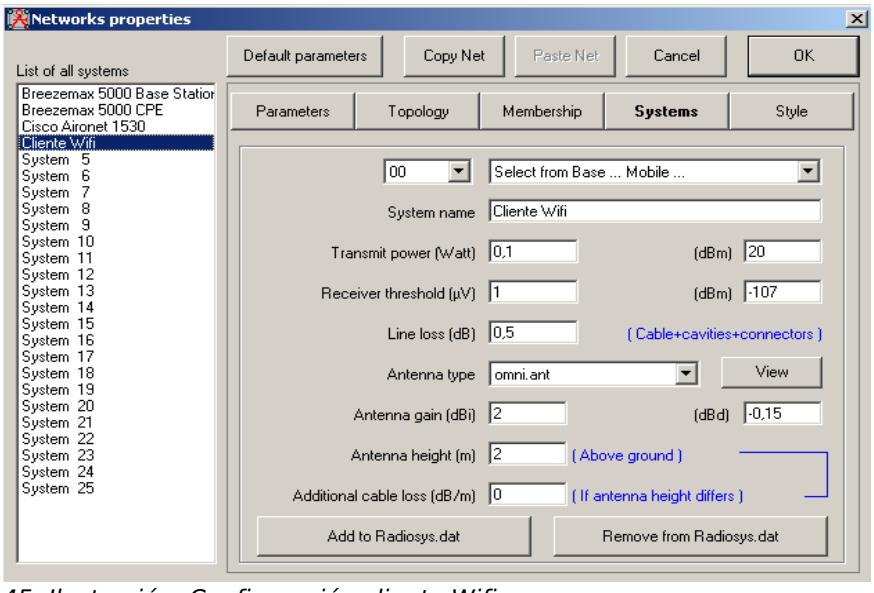
43. Ilustración: Configuración parámetros red Wifi

Configuramos las propiedades del punto de acceso, respetando el máximo PIRE que permite la legislación de 0,1 W.



44. Ilustración: Configuración punto de acceso Wifi

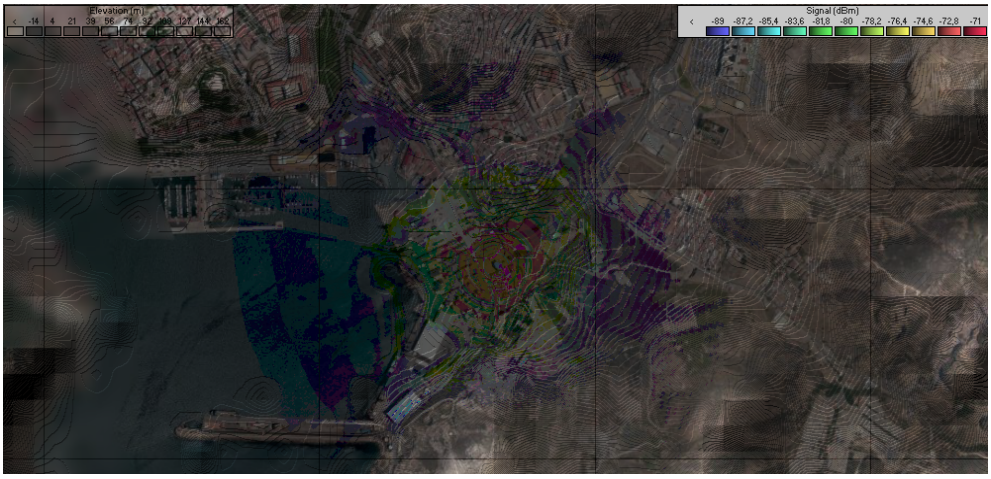
Añadimos también un cliente inalámbrico, que nos permitirá realizar la simulación de las coberturas.



45. Ilustración: Configuración cliente Wifi

Mediante la herramienta Cobertura Radio\Polar Simple vamos a realizar una primera simulación de cobertura.

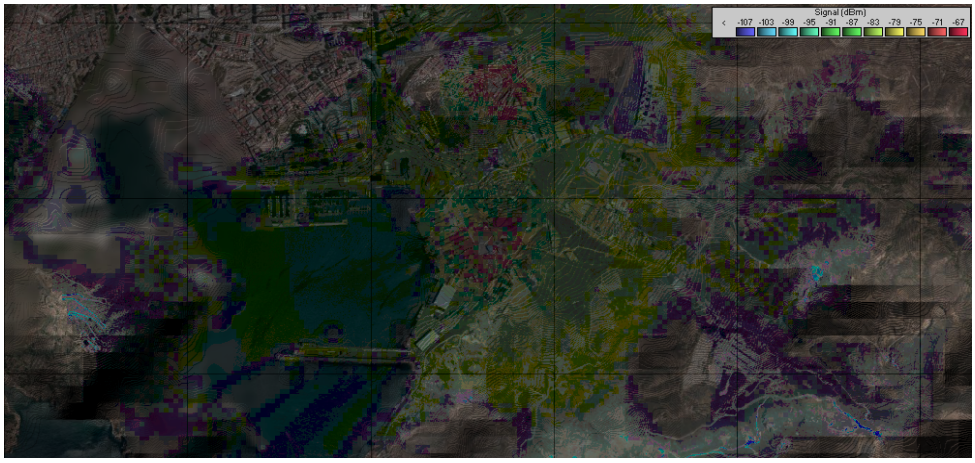
Como vemos, conseguimos un nivel de recepción de señal aceptable en el muelle de contenedores de Santa Lucía,



46. Ilustración: Cobertura Wifi Santa Lucía un punto de acceso

Sin embargo, en la Diputación de Santa Lucía la mitad superior queda en sombra, apreciándose la influencia del castillo de los Moros que domina la zona.

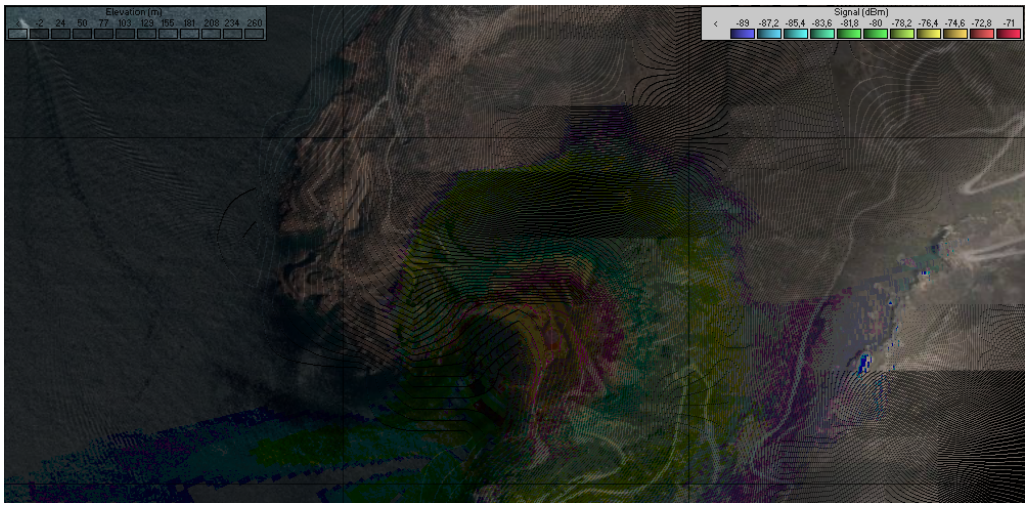
Colocando un segundo punto de acceso en la zona superior de la diputación, se obtiene un nivel de recepción aceptable en todas las áreas incluidas en el alcance de proyecto.Para esta vista hemos utilizado la herramienta Radio Coverage\Combined Cartesian.



47. Ilustración: Cobertura Wifi Santa Lucía dos puntos de acceso

A continuación vamos a calcular la cobertura en el área de Cala Cortina.

Como vemos, ubicando un punto de acceso junto al suscriptor Wimax, obtenemos un nivel de recepción en la zona de restaurante, playa, aparcamiento y buena parte de los restos de fortaleza defensiva.

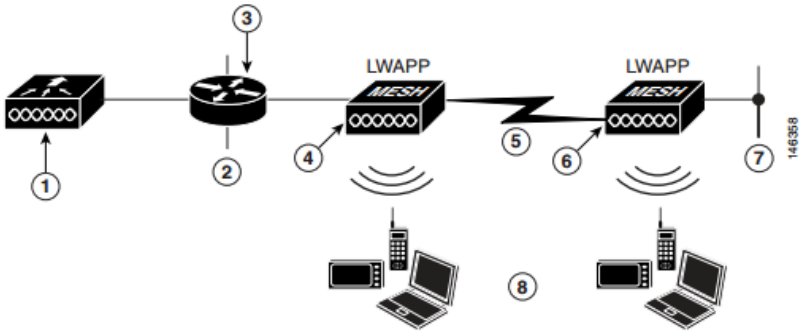


48. Ilustración: Cobertura Wifi Cala Cortina un punto de acceso

Por tanto, podemos considerar que este área queda inicialmente bien cubierta con un único punto de acceso.

Configuración de los equipos

Vamos a comenzar por la ubicación de Santa Lucía, donde existen dos puntos de acceso con la siguiente topología.



1	Cisco wireless LAN controller	**2**	LAN 1
3	Router or Switch -- Required when network is used for bridging LAN at Point **2** and LAN at Point **7**	**4**	Roof-top access point: Cisco Aironet 1030 remote edge lightweight access point or Cisco Aironet 1500 series lightweight outdoor access point
5	Wireless Backhaul	**6**	Pole-top access point Cisco Aironet 1030 remote edge lightweight access point or Cisco Aironet 1500 series lightweight outdoor access point (Note)
7	Optional wired connection to Ethernet termination device (such as a camera) or LAN 2; requires a Router or Switch at Point **3**	**8**	Wireless clients

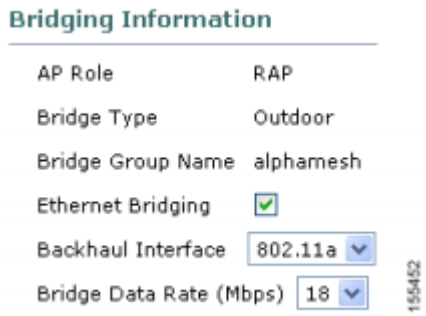
49. Ilustración: Jerarquía red en topología mallada

En este escenario, la banda de 2.4 Ghz se utiliza para dar acceso a los clientes y la banda de 5 Ghz se utiliza para backhaul.

Existen dos tipos de equipos en la terminología de Cisco. El RAP[35] es un equipo que dispone de interfaz Ethernet, para conectar con el controlador wireless. El PAP[36], no dispone de interfaz internet, ya que su comunicación es totalmente inalámbrica tanto hacia los clientes como al backhaul.

35 Roof Access Point
36 Pole Access Point

Mediante el WCS[37], podemos configurar el comportamiento de la red mallada.



50. Ilustración: Configuración de rol del punto de acceso en la red

Para terminar la configuración de la red mallada habilitaremos en el WCS la funcionalidad Zero Touch Configuration.

Al instalar el primer punto de acceso, trata de descubrir su rol automáticamente. Dado que tiene conexión cableada con el WCS, asume el rol de RAP.

A continuación se determina el canal de backhaul. Para ello el segundo equipo, con el rol de PAP, escanea los canales en busca de puntos de acceso mesh cercanos. Cuando encuentra a uno a través del cual tiene acceso al WCS, lo establece como padre dentro de la topología mallada.

Para garantizar la seguridad de la red mallada, el WCS mantiene una lista de direcciones MAC[38], así como una clave pública y otra compartida.

Para el interfaz de acceso al cliente, se seleccionará en cada uno de ellos una de los canales ortogonales (1, 6 u 11) para evitar interferencias.

37 Wireless Controller Switch
38 Media Access Control

Finalmente, configuramos el SSID y la seguridad WPA mediante la linea de comandos:

configure terminal

dot11 ssid ayto_ct

authentication key-management

end

copy running-config startup-config

A nivel de conectividad, el punto de acceso RAP estará conectado física mente mediante un cable Ethernet al suscriptor Wimax, para garantizar la conectividad hacia el CPD.

5.Interconexión Wimax-Wifi

A la hora de interconectar ambos niveles de red existen dos posibilidades.

- ✔ Backhauling: Esta técnica consiste en integrar en un único equipo la funcionalidad de suscriptor Wimax y de punto de acceso Wifi, de modo que el propio equipo gestiona los flujos de comunicación en uno u otro sentido.

- ✔ Bridging Ethernet: En este caso se trata de un suscriptor Wimax y un punto de acceso Wifi totalmente autónomos, incluso de distintos fabricantes. Para poder unirlos entre sí utilizamos los puertos Ethernet disponibles en ambos equipos.

Generalmente los equipos de backhauling suelen ser caros, por lo que vamos a optar por la segunda alternativa. Para ello utilizaremos un switch Fast Ethernet 10/100 Mbps. Se presenta este caso en dos ubicaciones:

- ✔ Garita de acceso del muelle de San Pedro: El switch se instalará dentro de el armario de comunicaciones de 19” ya existente, junto con la parte IDU del suscriptor Wimax.

- ✔ Cala Cortina: Se instalará un armario estanco con grado de protección IP66, para albergar los dos componentes anteriormente citados.

6.Seguridad y encriptación de la información

Se plantea la necesidad de que la navegación de los usuarios del servicio esté protegida hasta su salida por el router hacia internet, habida cuenta de que puede contener información sensible (correo, banca virtual, ...)

Para ello estableceremos diferentes medidas de protección.

Protección en el aire

Los paquetes que viajan entre los diferentes equipos pueden ser capturados por cualquiera, por lo que estarán encriptados mediante AES[39]. Dicha tecnología presenta las siguientes características:

- ✔ Algoritmo de encriptación simétrica, de substitución-permutación basado en el algoritmo Rijndael.
- ✔ Utiliza bloques de 128 bits y llaves de 128, 192 ó 256 bits.
- ✔ Adoptado por el NIST en 2001.

La principal ventaja de AES reside en su naturaleza simétrica. Es decir, que se utiliza la misma clave para cifrar y descifrar. Esto representa una ventaja en tiempo de procesamiento.

Adicionalmente, es es relativamente sencillo de implementar tanto mediante software como hardware en equipos relativamente poco potentes.

Esto hace que se haya convertido en el algoritmo de referencia para la encriptación de datos masivos, ofreciendo un buen balance entre protección y coste de procesamiento.

39 Advanced Encryption Standard

Protección de login y password

Los nombres de usuario y sus correspondientes contraseñas deben ser protegidos, de modo que un atacante no pueda obtener fácil acceso mediante un ataque de fuerza bruta.

En los inicios del estándar Wifi, se utilizaba habitualmente el sistema WEP[40]. Sin embargo, el desarrollo de diferentes técnicas de ataque han demostrado su elevada vulnerabilidad[41], basada en el hecho de la clave secreta es fija y debe ser introducida en ambos extremos de la comunicación.

Para protejer el acceso de los usuarios a los puntos de acceso WiFi Cisco, implementaremos el sistema WPA2[42]. Su principal característica es que las claves se generan y distribuyen dinamicamente para cada trama mediante TKIP[43].

Existen dos implementaciones distintas del protocolo, en función del tamaño y los requerimientos de seguridad:

- ✔ WPA-Personal: También llamado modo pre-shared key, cada dispositivo se autentifica ante el AP utilizando la misma clave de 256 bits.
- ✔ WPA-Enterprise: La autentificación del usuario se realiza a través del protocolo RADIUS 802.1x.

Adicionalmente, se cambiarán las contraseñas de administrador por defecto en todos los equipos.

Otra medida habitual de seguridad consiste en desactivar la difusión del SSID[44] de los equipos. Sin embargo, se considera que esto puede dificultar la conexión de los equipos para usuarios no expertos, por lo que no se va a implementar.

En el apartado de bibliografía se pueden encontrar enlaces con información adicional sobre los diferentes protocolos de seguridad en entornos inalámbricos.

40 Wired Equivalent Privacy
41 http://thehackerway.com/2012/04/16/wireless-hacking-ataques-contra-wep-korek-chopchop-parte-ix/
42 Wifi Protected Access
43 Temporal Key Integrity Protocol
44 Service Set Identifier

7.Ubicaciones físicas

En este apartado, vamos a desarrollar la forma de ubicar físicamente los equipos. Es importante mencionar la necesidad de instalar en cada equipo inalámbrico instalar un supresor de descargas para evitar daños en caso de ser alcanzados por un rayo.

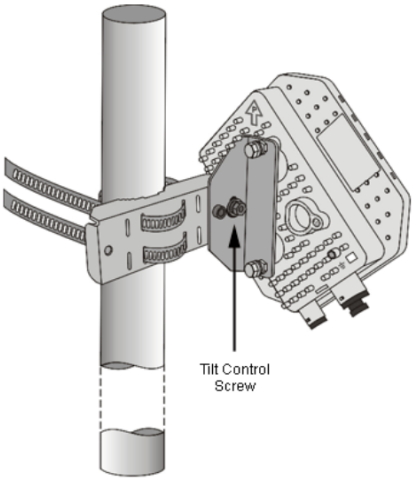
CPD

En el edificio donde está instalado es posible el acceso al techo del edificio, existiendo además una canalización traqueal que comunica con el mismo CPD. Por tanto, instalaremos una soportación de tipo brazo que se ancla al murete que remata el edificio tal y como se muestra en la fotografía.

51. Ilustración: Soportación de equipo inalámbrico para muro

No es necesario utilizar un sistema de soportación más robusto, dada la escasa resistencia al viento que presenta el equipo. Adicionalmente, este tipo de soportación presenta la ventaja de que no es necesario perforar la cubierta del edificio para su instalación, evitando el riesgo de filtraciones.

Como vemos, el sistema de fijación que incluye el equipo ODU[45] permite regular el ángulo de inclinación para poder lograr la orientación óptima. El propio equipo dispone de un sistema de LED´s que permite ajustar visualmente la orientación sin necesidad de tener el ordenador conectado.



52. Ilustración: Regulación inclinación equipo inalámbrico

El IDU[46], que no tiene protección para exteriores, se ubica en el rack del CPD donde están ubicados el resto de los equipos. La comunicación entre ODU e IDU se lleva a cabo mediante un cable de red Categoría 5E de un máximo de 90 metros, a través del cual viaja la alimentación y datos mediante PoE.

45 Outdoor Unit
46 Indoor Unit

Monte San Julian

Como ya hemos comentado anteriormente, por su ubicación dominante existen ya múltiples servicios de comunicaciones instalados sobre una torre de celosía de 10 metros de altura.

53. Ilustración: Ubicación física estación base en Monte San Julián

Por tanto vamos a utilizar dos brazos similares al utilizado en el CPD, uno para la Base Station de Alvarion y otro para la antena omnidireccional externa.

El edificio que se muestra a la izquierda en la foto ya dispone de alimentación eléctrica y climaticación, por lo que será dentro donde ubicaremos el equipo de PoE.

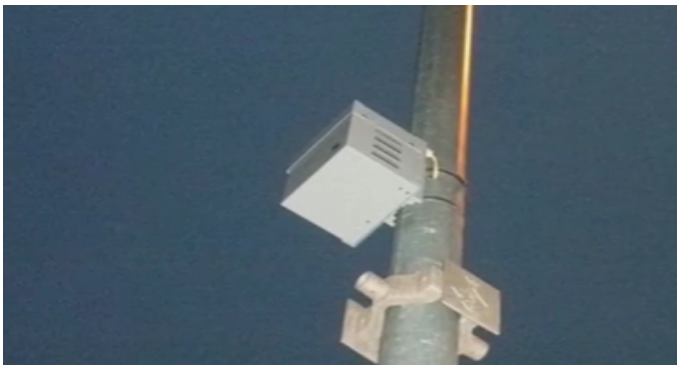
Para proteger el cable Categoría 5E de enlace entre la Base Station y el equipo PoE dentro del edificio, se utilizará un tubo corrugado de exteriores métrica 40.

Cala Cortina

En la siguiente imagen se muestra una panorámica de la Cala, con el Restaurante en primer término. Recuadrado en rojo se muestra un poste de sección circular donde actualmente está montada una cámara de videovigilancia con lo que ya dispone de alimentación eléctrica.

54. Ilustración: Ubicación física equipos Cala Cortina

A dicho poste fijaremos el suscriptor Wimax con su antena integrada y el punto de acceso wifi. La unión entre ambos equipos se realiza mediante un pequeño switch a través de sus respectivos interfaces Ethernet. Para proteger dicho switch, lo instalaremos dentro de un armario de exteriores IP66 como el que se muestra en la fotografía.



55. Ilustración: Soportación sobre poste de sección circular

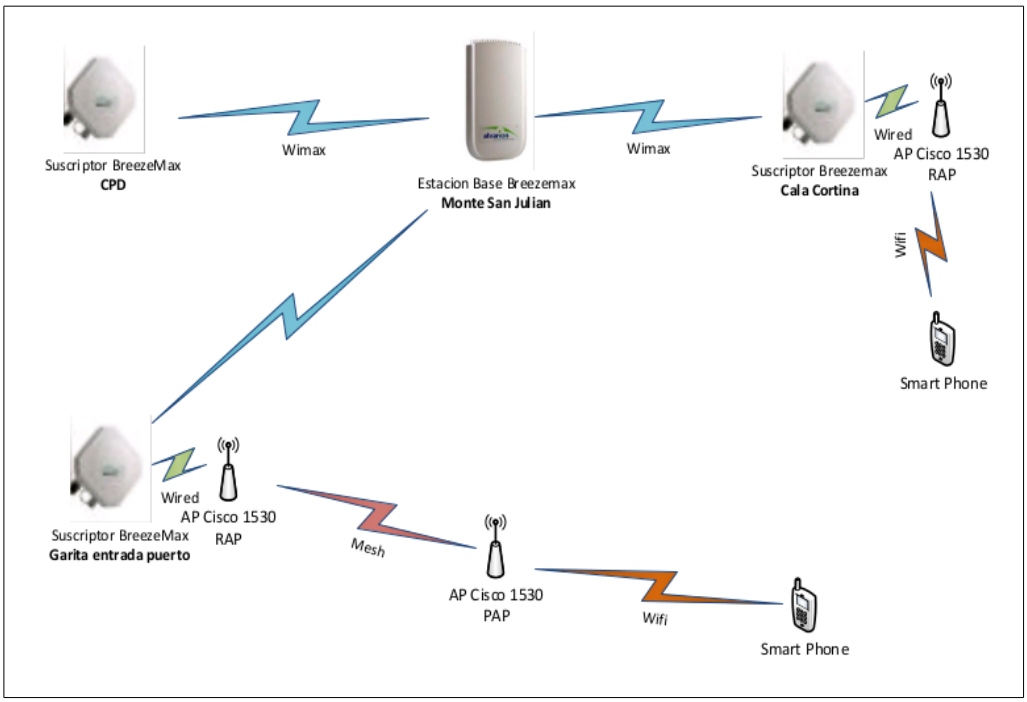
Como podemos observar en la fotografía, la forma correcta de montar equipos en postes de sección circular es mediante bridas de acero inoxidable. De este modo evitamos realizar orificios que pueden comprometer la resistencia estructural del poste.

Garita entrada Muelle

La instalación en este área es completamente análoga a la anterior, aprovechando así mismo un poste de soportación de cámaras de videovigilancia.

8.Esquema lógico

Finalmente, a modo de resumen se muestra el esquema lógico con todos los equipos a implantar.



56. Ilustración: Esquema lógico infraestructura inalámbrica

9.Presupuesto económico

A continuación se desglosa el presupuesto económico del proyecto.

Cantidad	Descripción	Precio Unitario	Precio Total
	Hardware		
1	Base Station Alvarion BreezeMax Extreme 5000	6.123,00 €	6.123,00 €
1	Antena Alvarion omnidireccional 9,5 dBi	355,00 €	355,00 €
3	CPE Alvarion BreezeMax Extreme 5000 (suscriptor)	2.067,00 €	6.201,00 €
3	Punto de Acceso Cisco Aironet	1.259,00 €	3.777,00 €
1	Cisco Wireless LAN Controller 2500	695,00 €	695,00 €
1	Soportaciones y material de instalación (vientos, tornillería,...)	500,00 €	500,00 €
1	Firewall Fortinet 40C	693,00 €	693,00 €
2	Switch 3Com 8 puertos 10/100 Mbps	49,00 €	98,00 €
1	Servidor IBM x3100 M4 Quad Core 4Gb RAM	732,00 €	732,00 €
		Subtotal HW.	19.174,00 €
	Servicios profesionales		
20	Director de proyecto	80,00 €	1.600,00 €
50	Administrador de Sistemas	60,00 €	3.000,00 €
60	Instalador	30,00 €	1.800,00 €
		Subtotal Servicios	6.400,00 €
		TOTAL IVA INCL.	25.574,00 €

1. Tabla: Presupuesto económico del proyecto

10.Estudio de viabilidad

Vamos a realizar un estudio de viabilidad estudiando los costos e ingresos del proyecto en un horizonte de cinco años. Se utiliza este plazo concreto ya que coincide con el ciclo de vida habitual de los equipos actuales. Obtener renovaciones de mantenimiento que cubran posibles averías más allá de los cinco años tiene una fuerte penalización económica. En algunos casos, el fabricante no contempla dicha opción y obliga a la renovación del equipo.

1.Gastos

A continuación se enumeran los gastos del proyecto:

- ✔ Inversión inicial.
- ✔ Conexión al ISP, con un importe mensual de 64€ iva incluido.
- ✔ Ampliación de la garantía de los equipos, estimando un coste del 5% del importe de compra para el tercer año, un 7% para el cuarto y un 10% para el quinto.
- ✔ Se estiman necesarias para la gestión del nuevo entorno 200 horas anuales de un perfil de administrador de sistemas, con un coste interno de 20€

2.Ingresos

La principal fuente de ingresos del proyecto es la publicidad, habida cuenta de los 120.000 turistas que visitaron la ciudad, con una fuerte perspectiva de crecimiento.

Vamos a tomar como referencia[47] el coste de alquiler mensual de un cartel monoposte de 12x5 mts en la Región de Murcia, que se sitúa en 870€ con un coste de impresión de 1.400€.

Consideramos razonable estimar que el impacto de la colocación de publicidad en el portal de acceso al servicio de conexión a internet será al menos igual de efectiva que si estuviera colocada en un monoposte, por lo que tendremos unos ingresos anuales de 10.720€.

Por otro lado, la ubicación de los puntos de acceso ofrece cobertura a la cercana explanada de contenedores del Muelle de San Pedro, por lo que se acuerda un convenio de utilización de dicha red por parte de la Autoridad Portuaria para el desarrollo de un prototipo de monitorización del transito de contenedores mediante tecnología inalámbrica IoT[48]. El coste anual de dicho convenio será de 600€.

Adicionalmente, podemos considerar otros beneficios de orden no económico:

- ✔ El desarrollo de la Sociedad de la Información en el área de Santa Lucía.
- ✔ Posibilidad de utilización de la nueva infraestructura para servicios ya existentes (Policía, Bomberos,...), pudiendo suponer un ahorro de costes.

47 Información obtenida de http://www.monopostes.biz/monopostes/monopostes-alquiler.html

48 Internet of Things

A continuación se muestra un cuadro resumen de ingresos y gastos:

Cantidad	Descripción	Precio Unitario	Precio Total
	Ingresos		
5	Ingresos directos por publicidad	10.720,00 €	53.600,00 €
5	Alquiler anual red inalámbrica al Puerto de Cartagena	600,00 €	3.000,00 €
		Subtotal ingresos	**56.600,00 €**
	Gastos		
1	Inversión inicial	25.574,00 €	25.574,00 €
1	Renovación del mantenimiento HW del 2º al 5º año	4.218,28 €	4.218,28 €
60	Coste mensual de la conexión a internet Movistar FTTH 100Mb	62,00 €	3.720,00 €
1000	Horas de administración del sistema	20,00 €	20.000,00 €
		Subtotal costos	**53.512,28 €**
		TOTAL BENEFICIO	3.087,72 €

2. Tabla: Previsión Ingresos y Gastos del proyecto

Finalmente, obtenemos que al final de la vida útil del proyecto resulta un beneficio total de 3.087,72€; siendo por tanto totalmente factible su puesta en marcha.

11.Conclusión

En el contexto económico actual, la búsqueda de financiación se convierte habitualmente en el aspecto más complejo en el desarrollo de un proyecto tecnológico.

Recordemos que la mayor parte de la financiación económica proviene del sector turístico, que obtiene un poderoso medio de difusión con el coste equivalente al de un poste de publicidad estática convencional.

A cambio, el Ayuntamiento puede desarrollar un proyecto de calado social, como es un servicio de conexión a Internet gratuito que permita reducir la brecha digital.

El presente proyecto representa pues una importante sinergia entre la iniciativa privada y la gestión pública, ofreciendo claras ventajas para todas las partes.

El aspecto económico ha tenido reflejo en la mayoría de las decisiones de diseño, para aumentar al máximo las posibilidades de viabilidad del hipotético proyecto:

- ✔ Ancho de banda disponible para el usuario. Se ha optado por estimar 64 Kbps por usuario, por debajo de los 256 Kbps que permite la legislación. Sin embargo, el sistema se ha diseñado de forma que sea altamente escalable ante un aumento de los requerimientos según el modelo “pay as you grow”. De este modo futuras inversiones se justifican en base a un incremento de los ingresos producidos por el turismo.

- ✔ Utilización de bandas de frecuencia no licenciadas.

- ✔ Elección de tecnología basada en estándares, garantizando de este modo la interoperabilidad de la base instalada con equipos de otros fabricantes en posibles ampliaciones.

Finalmente, cabe destacar la madurez de las tecnologías inalámbricas, que permiten realizar despliegues en zonas de orografía compleja sin linea de visión directa.

12.Bibliografía

Imágenes satélite, coordenadas GPS de las localizaciones del proyecto: http://www.google.com/earth/

Cálculo de la viabilidad de los enlaces:

Software: http://www.cplus.org/rmw/english1.html

Tutorial:http://www3.fi.mdp.edu.ar/electronica/catedras/mediosdetransmision/files/ManualRadioMobile.pdf

Legislación

Ley General de Telecomunicaciones: https://www.boe.es/buscar/doc.php?id=BOE-A-2003-20253

Ley que regula la prestación de servicios de telecomunicaciones por parte de AAPP: http://www.cmt.es/c/document_library/get_file?uuid=f26dcedb-3cfc-429e-8629-303fc2c6de81&groupId=10138

Artículo sobre el alcance de los servicios: http://cnmcblog.es/2011/09/15/wifi-en-los-ayuntamientos-nada-cambia/

Sanciones Ayuntamiento Málaga:http://cnmcblog.es/2010/02/23/wifi-en-malaga-la-importancia-de-inscribirse-como-operador/

Protocolos y estándares:

Protección IP: http://es.wikipedia.org/wiki/Grado_de_protecci%C3%B3n_IP

Alimentación sobre Ethernet: http://es.wikipedia.org/wiki/Power_over_Ethernet

Wifi: http://es.wikipedia.org/wiki/Wi-Fi

Wimax: http://es.wikipedia.org/wiki/WiMAX

Características WEP: http://es.wikipedia.org/wiki/Wired_Equivalent_Privacy

Características WPA2: http://es.wikipedia.org/wiki/WPA

Criptografía simétrica: http://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica

Cortafuegos Fortinet

Hoja de producto:

https://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-40C.pdf

Configuración firewall Fortinet: http://docs-legacy.fortinet.com/cookbook.html

Perfil de youtube con ejemplos de configuración: http://www.youtube.com/user/SecureNetworks?feature=watch

Proxy

Software: http://www.squid-cache.org/

Configuración:http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy_squid.html

Cisco

Hoja de producto Wireless LAN Controller: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6307/product_data_sheet0900aecd802570b0.pdf

Configuración Wireless LAN Controller: https://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ContCG40-Oct.pdf

Hoja de producto AP 1530: http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps12831/data_sheet_c78-728356.pdf

Configuración AP 1530:

http://www.cisco.com/en/US/docs/wireless/access_point/1530/quick/guide/ap1532qsg.html

Alvarion

Manual configuración BreezeMax: http://www.alvarion.com/addons/support/ics/product_support_form/BreezeMAX%20PRO%205000%20CPE_Ver.1.2_Product%20Manual_091110.pdf

Seguridad

Ataques contra WEP: http://thehackerway.com/2012/04/16/wireless-hacking-ataques-contra-wep-korek-chopchop-parte-ix/:

Ataques contra WPA: http://www.elladodelmal.com/2008/08/atacar-wpawpa2-psk-parte-i-de-iv.html

13.Hojas de producto

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 4900-5350 MHz 5470-5875 MHz	CPE 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 0-21 dBm, 1dB resolution	CPE 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

FORTINET

DATASHEET

FortiGate/FortiWiFi®-40C

Secure Connectivity and Compliance for the Small Office

The FortiGate-40C and FortiWiFi-40C are ideal for small businesses, small branch offices and retail outlets requiring the consolidated security functions of larger FortiGate devices in a small form factor. The appliances deliver enterprise-grade network security and performance to smaller locations at an entry-level price.

The Power of Unified Threat Management

The FortiGate-40C and FortiWiFi-40C appliances combine the purpose-built FortiOS™ operating system with the Fortinet System on a Chip (SoC) purpose-built processor to deliver unmatched security and performance advantages. These devices feature all of Fortinet's unified threat management (UTM) inspection capabilities: firewall, IPS, application control, VPN, and web filtering - all managed from a 'single pane of glass' console. They also include other security technologies such as data leakage prevention and vulnerability management. You can deploy security technologies as needed for your unique requirements.

The FortiGate-40C and FortiWiFi-40C provide you with a strategic and cost-effective solution that you can provision and manage from anywhere in the world. The appliances capitalize on multiple security enforcement technologies to protect your remote networks in today's sophisticated threat landscape, helping you maintain compliance with PCI, HIPAA, and GLBA regulations for data protection.

By consolidating multiple security technologies into a single appliance, the FortiGate-40C and FortiWiFi-40C eliminate multiple hardware devices and software solutions, greatly simplifying security at small offices, branch offices and retail locations while substantially reducing total cost of ownership. Installation and configuration is made easy with FortiExplorer setup wizard. The wizard provides an easy, inexpensive way to configure the initial settings for the FortiGate unit, enabling non-IT staff to set up the device for remote management in a few minutes.

The Fortinet System-on-a-Chip

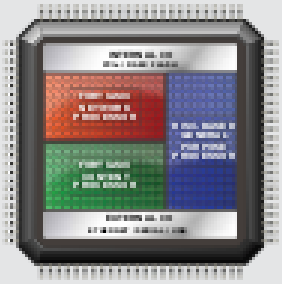
The FortiGate-40C and FortiWiFi-40C devices include the Fortinet System-on-a-chip (SoC). Designed by Fortinet to provide real-time network protection, the SoC integrates FortiASIC security acceleration logic with a RISC-based main processor and other system components. This simplifies appliance design and delivers breakthrough performance for smaller networks. The FortiGate/FortiWiFi-40C series appliances enable large distributed enterprises to provide integrated, multi-threat protection across all points on their network without sacrificing performance.

FortiOS The World's Most Advanced Security Operating System

FortiOS provides high performance, ultra low latency multi-threat security by leveraging the hardware acceleration provided by purpose-built FortiASIC processors. This combination of custom hardware and software gives you the best security and performance possible from a single device. FortiOS allows greater traffic visibility and more consistent, granular control over users, applications and sensitive data.

The FortiASIC Advantage

FortiASIC processors power FortiGate platforms. With exclusive hardware, the purpose-built, high performance Network, Security, and Content processors use intelligent and proprietary digital engines to accelerate security services.



Feature	Benefit
Unified Security Architecture	Multi-threat protection from a single device increases security and lowers costs.
Simple Licensing	Hassle-free unlimited user licensing increases ease of deployment and maintenance.
Multi-Port Wired / Wireless Interfaces	Multiple physical network interfaces and optional wireless connectivity allow flexible deployment and better security through multiple security zones.
Small Form-Factor	Compact, lightweight and designed for small offices.

FortiGate Consolidated Security Solutions

Fortinet's consolidated security solutions provide an integrated set of core security and networking services in a single, easy-to-manage, high-performance appliance that is capable of supporting a wide range of deployment scenarios. Consolidating stand-alone security products into a single device allows you to improve your network visibility and increase control over users, applications, and data.

Technical Specifications	FortiGate-40C	FortiWiFi-40C
HARDWARE SPECIFICATIONS		
LAN Ports 10/100/1000 Interfaces (Switched)	5	
WAN Ports 10/100/1000 Interfaces	2	
Wireless Interface	N/A	802.11 a/b/g/n
USB (Client/Server)	1 / 1	
RJ-45 Serial Console	1	
SYSTEM PERFORMANCE		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	200 / 200 / 200 Mbps	
Firewall Latency (64 byte UDP packets)	3 µs	
Firewall Throughput (Packets Per Second)	300 Kpps	
Concurrent Sessions (TCP)	40,000	
New Sessions/Sec (TCP)	2,000	
Firewall Policies	5,000	
IPSec VPN Throughput (512 byte packet)	60 Mbps	
Gateway-to-Gateway IPSec VPN Tunnels	20	
Client-to-Gateway IPSec VPN Tunnels	250	
SSL-VPN Throughput	17 Mbps	
Concurrent SSL-VPN Users (Recommended Max)	80	
IPS Throughput	135 Mbps	
Antivirus Throughput (Proxy Based / Flow Based)	20 / 40 Mbps	
Max Number of FortiAPs (Total / Tunnel Mode)	10 / 5	
Max Number of FortiTokens	100	
Max Number of Registered FortiClients	10	
High Availability Configurations	Active/Active, Active/Passive, Clustering	
Unlimited User Licenses	Yes	

Technical Specifications	FortiGate-40C	FortiWiFi-40C
DIMENSIONS & POWER		
Height	1.3 in (3.3 cm)	1.3 in (3.3 cm)
Width	8.5 in (21.6 cm)	8.5 in (21.6 cm)
Length	5.3 in (13.4 cm)	5.8 in (14.3 cm)
Weight	1.7 lb (0.8 kg)	
Wall Mountable	Yes	
AC Power	100-240 VAC, 60-50 Hz	
Current (Max)	110V / 0.38A, 220V / 0.19A	
Power Consumption (Avg / Max)	12.3 / 14.8 W	13.8 / 16.8 W
Heat Dissipation	50.5 BTU/h	56.6 BTU/h
Redundant Power Supply	No	
ENVIRONMENT		
Operating temperature	32 - 104 °F (0 - 40 °C)	
Storage temperature	-31 - 158 °F (-35 - 70 °C)	
Humidity	20 to 90% non-condensing	
Compliance	FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN	

All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 KB ptt HTTP files. IPS performance is measured using 1 Mbyte HTTP files.

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability and compliance management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with "return and replace" hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560 Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road #20-01, The Concourse
Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015

FST-PROD-DS-40C

FGFWF-40C-DAT-R9-201309

Data Sheet

Cisco Wireless LAN Controllers

The Cisco® 4400 Series Wireless LAN Controller provides systemwide wireless LAN functions for medium to large-sized facilities. By automating WLAN configuration and management functions, network managers have the control, security, redundancy, and reliability needed to cost-effectively scale and manage their wireless networks as easily as they scale and manage their traditional wired networks.

The Cisco 4400 Series Wireless LAN Controller (Figure 1) works in conjunction with Cisco Aironet® access points, the Cisco Wireless Control System (WCS), and the Cisco Wireless Location Appliance to support business-critical wireless data, voice, and video applications. It provides real-time communication between access points and other wireless LAN controllers to deliver centralized security policies, wireless intrusion prevention system (IPS) capabilities, award-winning RF management, quality of service (QoS), and mobility.

Figure 1. Cisco 4400 Series Wireless LAN Controller

Because the Cisco 4400 Series Wireless LAN Controller supports 802.11a/b/g and the IEEE 802.11n draft 2.0 standard, organizations can deploy the solution that best meets their individual requirements. Organizations can offer robust coverage with 802.11 a/b/g or deliver greater performance with 5x the throughput and unprecedented reliability using 802.11n and Cisco's Next-Generation Wireless Solutions and Cisco Enterprise Wireless Mesh.

The Cisco 4400 Series Wireless LAN Controller is available in two models. The Cisco 4402 Wireless LAN Controller with two 1 GB Ethernet ports comes in configurations that support 12, 25, and 50 access points. The Cisco 4404 Wireless LAN Controller with four 1 GB Ethernet ports supports 100 access points. The Cisco 4402 controller provides one expansion slot. The Cisco 4404 controller provides two expansion slots that can be used to add VPN termination today, as well as enhanced functionality in the future. In addition, each Cisco 4400 WLAN Controller supports an optional redundant power supply to ensure maximum availability.

Product Specifications

Table 1 lists the product specification for Cisco 4400 Series wireless LAN controllers.

Table 1. Product Specifications for Cisco 4400 Series Wireless LAN Controllers

Item	Specification
Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11h, 802.11n
Wired/Switching/Routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, IEEE 802.1Q VLAN tagging, and IEEE 802.1D Spanning Tree Protocol
Data Request For Comments (RFC)	• RFC 768 UDP • RFC 791 IP • RFC 792 ICMP • RFC 793 TCP • RFC 826 ARP • RFC 1122 Requirements for Internet Hosts • RFC 1519 CIDR • RFC 1542 BOOTP • RFC 2131 DHCP
Security Standards	• WPA • IEEE 802.11i (WPA2, RSN) • RFC 1321 MD5 Message-Digest Algorithm • RFC 1851 The ESP Triple DES Transform • RFC 2104 HMAC: Keyed Hashing for Message Authentication • RFC 2246 TLS Protocol Version 1.0 • RFC 2401 Security Architecture for the Internet Protocol • RFC 2403 HMAC-MD5-96 within ESP and AH • RFC 2404 HMAC-SHA-1-96 within ESP and AH • RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV • RFC 2406 IPsec • RFC 2407 Interpretation for ISAKMP • RFC 2408 ISAKMP • RFC 2409 IKE • RFC 2451 ESP CBC-Mode Cipher Algorithms • RFC 3280 Internet X.509 PKI Certificate and CRL Profile • RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec • RFC 3686 Using AES Counter Mode with IPsec ESP
Encryption	• WEP and TKIP-MIC: RC4 40, 104 and 128 bits (both static and shared keys) • SSL and TLS: RC4 128-bit and RSA 1024- and 2048-bit • AES: CCM, CCMP • IPSec: DES-CBC, 3DES, AES-CBC
Authentication, Authorization, and Accounting (AAA)	• IEEE 802.1X • RFC 2548 Microsoft Vendor-Specific RADIUS Attributes • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS Authentication • RFC 2866 RADIUS Accounting • RFC 2867 RADIUS Tunnel Accounting • RFC 2869 RADIUS Extensions • RFC 3576 Dynamic Authorization Extensions to RADIUS • RFC 3579 RADIUS Support for EAP • RFC 3580 IEEE 802.1X RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol • Web-based authentication

Item	Specification
Management	• SNMP v1, v2c, v3 • RFC 854 Telnet • RFC 1155 Management Information for TCP/IP-Based Internets • RFC 1156 MIB • RFC 1157 SNMP • RFC 1213 SNMP MIB II • RFC 1350 TFTP • RFC 1643 Ethernet MIB • RFC 2030 SNTP • RFC 2616 HTTP • RFC 2665 Ethernet-Like Interface types MIB • RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions • RFC 2819 RMON MIB • RFC 2863 Interfaces Group MIB • RFC 3164 Syslog • RFC 3414 User-Based Security Model (USM) for SNMPv3 • RFC 3418 MIB for SNMP • RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs • Cisco private MIBs
Management Interfaces	• Web-based: HTTP/HTTPS • Command-line interface: Telnet, SSH, serial port
Interfaces and Indicators	• Uplink: 2 (4402) or 4 (4404) 1000Base-X transceiver slots • LED indicators: link, activity • Service Port: 10/100 Mbps Ethernet (RJ45) • LED indicators: link, activity • Utility Port: 10/100/1000 Mbps Ethernet (RJ45) • LED indicators: link, activity • Expansion Slots: 1 (4402) or 2 (4404) • Console Port: RS232 (DB-9 male, DTE interface) • Other Indicators: Status, Alarm, Power Supply 1, Power Supply 2
Physical and Environmental	• Dimensions (WxDxH): 17.45 x 15.75 x 1.75 in. (443 x 400 x 44.5 mm) • Weight: 15.3 lbs (6.95 kg) with 2 power supplies • Temperature: • Operating: 32 to 104 F (0 to 40C) • Storage: -13 to 158F (-25 to 70C) • Humidity: • Operating humidity: 10 95%, non-condensing • Storage humidity: up to 95% • Input power: 100 240 VAC; 50/60 Hz; 0.43 A at 110 VAC, 0.23 A at 220 VAC; 50W. Redundant power option available. • Heat Dissipation: 171 BTU/hour
Regulatory Compliance	• CE Mark • Safety: • UL 60950-1:2003 • EN 60950:2000 • EMI and susceptibility (Class A): • U.S.: FCC Part 15.107 and 15.109 • Canada: ICES-003 • Japan: VCCI • Europe: EN 55022, EN 55024

Ordering Information

Table 2 provides ordering information for the Cisco 4400 Series. To place an order, visit the Cisco Ordering Website: http://www.cisco.com/en/US/ordering/index.shtml

Table 2. Ordering Information for Cisco 4400 Series Wireless LAN Controllers

Part Number	Product Name
AIR-WLC4402-12-K9	4400 Series WLAN Controller for up to 12 Cisco access points
AIR-WLC4402-25-K9	4400 Series WLAN Controller for up to 25 Cisco access points
AIR-WLC4402-50-K9	4400 Series WLAN Controller for up to 50 Cisco access points
AIR-WLC4404-100-K9	4400 Series WLAN Controller for up to 100 Cisco access points
AIR-PWR-4400-AC=	4400 Series WLAN Controller AC Power Supply (redundant)

Summary

The Cisco 4400 Series Wireless LAN Controller is ideal for enterprise and service provider wireless LAN deployments. It simplifies deployment and operation of wireless networks, helping to ensure smooth performance, enhance security, and maximize network availability. The Cisco 4400 Series Wireless LAN Controller manages all of the Cisco access points within campus environments and branch locations, eliminating complexity and providing network administrators with visibility and control of their wireless LANs.

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, visit Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about Cisco wireless LAN controllers, contact your local account representative or visit: http://www.cisco.com/en/US/products/ps6366/index.html

For more information about the Cisco Unified Wireless Network framework, visit: http://www.cisco.com/go/unifiedwireless

Data Sheet

Cisco Aironet 1530 Series Outdoor Access Point

Compact Outdoor Wireless

- Most compact carrier-grade outdoor access point/mesh/bridge: 186 cubic in (3.0 liter), 5 lb (2.3 kg)
- 2.4- and 5-GHz radios: (802.11b/g/n, 802.11a/n)
- 802.11n range and performance with MIMO technology
- Gigabit Ethernet 10/100/1000 WAN and LAN ports
- Controller-based or autonomous operation
- Powered via PoE or separate DC input
- IP67 enclosure with operating temperature range of 22°F to 149°F (-30°C to +65°C)

Cisco Aironet 1530I

- Integrated antennas
- 2.4 GHz: 3x3 MIMO, 3 spatial streams
- 5 GHz: 2x3 MIMO, 2 spatial streams
- Ultra low profile

Cisco Aironet 1530E

- External antennas
- 2.4 and 5 GHz: 2x2 MIMO, 2 spatial streams
- Supports dual-band or single-band antennas
- Versatile RF coverage with external antennas

Sleek, Innovative, Flexible, Proven

As carrier-grade Wi-Fi becomes a critical small-cell element in next-generation mobile networks, operators are requesting new access point designs that can pack a punch in a small form factor. The Cisco® Aironet® 1530 Series Outdoor Access Points incorporate a low-profile design that is esthetically pleasing, yet they can withstand the most rugged outdoor conditions. Cisco brings engineering innovation to the platform with unique Cisco Flexible Antenna Port technology that allows the same antenna ports to be used either for dual-band antennas to reduce the antenna footprint or for single-band antennas to optimize radio coverage. This flexibility allows antenna changes to be made on the fly, and saves on sparing costs. And the Cisco Aironet 1530 Series brings all the same robust Wi-Fi features that operators have come to expect from Cisco, including radio resource management, BandSelect to automatically take advantage of the 5-GHz band, and VideoStream for high-quality video performance over Wi-Fi. Only Cisco delivers all of these features in a hardened outdoor access point that is ideal for any urban setting.

Compact, Place-Anywhere Design

The Cisco Aironet 1530 Series Outdoor Access Points are small enough and light enough to be unobtrusively mounted on street light poles or building facades. The integrated antenna version is just 9 x 7 x 4 inches (23 x 17 x 10 cm) and weighs 5 pounds (2.3 kg). A solar shield/cover option is also available, and can be painted to match its surroundings to allow the access point to be even less noticeable (Figure 1).

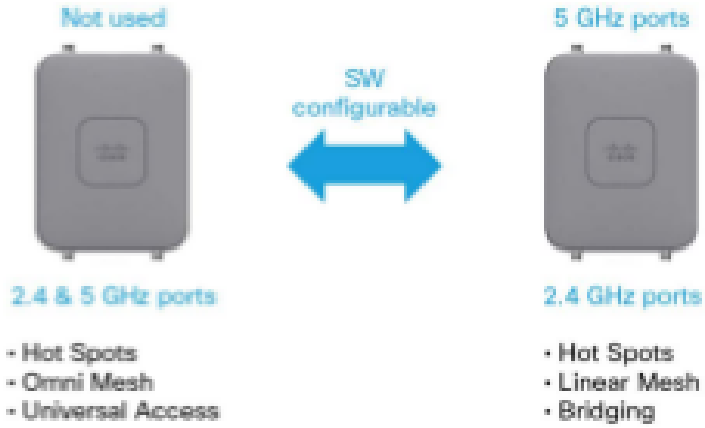
Figure 1. Cisco Aironet 1530 Series with Solar Shield/Cover

Innovative, Integrated, and External Antenna Options

The Cisco Aironet 1530I Outdoor Access Point includes a dual-band, integrated antenna radome. This antenna has three omnidirectional antenna elements with antenna gains of 3 dBi (2.4 GHz) and 5 dBi (5 GHz). More information, including antenna patterns, can be found in the Cisco Aironet Antennas and Accessories Guide: http://www.cisco.com/en/US/products/hw/wireless/ps469/index.html.

The innovatively designed Cisco Aironet 1530E Outdoor Access Point is designed with antenna Cisco Flexible Antenna Port technology, which can support either dual-band or single-band antennas on the same platform and is configurable via software. When configured for dual-band ports, the Aironet 1530E uses the bottom two antenna ports to connect to dual-band omnidirectional or directional antennas. Alternatively, and for additional radio coverage flexibility, the Aironet 1530E can be software-configured, enabling two separate 2.4-GHz and two 5-GHz antenna ports (Figure 2). This flexibility allows customers to use high-gain directional antennas for backhaul on 5 GHz while deploying omnidirectional antennas for access on 2.4 GHz. Refer to the Cisco Aironet 1530 Series Ordering Guide for the latest information on supported antennas.

Figure 2. Cisco Aironet 1530E with Flexible Antenna Port Antenna Technology

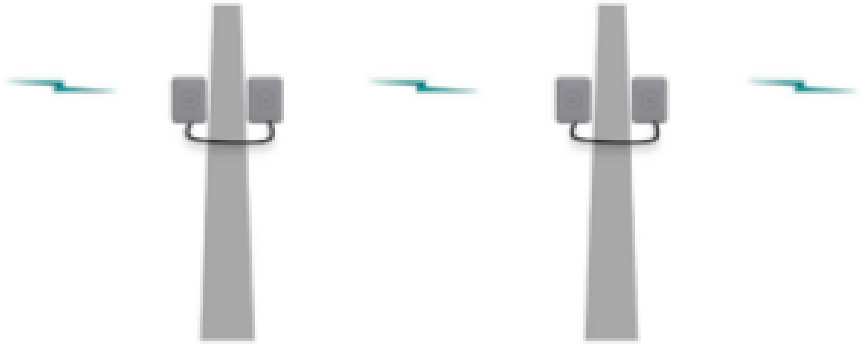


Flexible, High-Performance

The Cisco Aironet 1530 Series Outdoor Access Points offer a flexible, highly secure, and scalable platform that is part of the Cisco Unified Wireless Network and the Cisco Service Provider Wi-Fi solution. The Cisco Aironet 1530 Series provides high-performance device access through improved radio sensitivity and range with 802.11a/b/g/n multiple-input multiple-output (MIMO) technology, with two or three spatial streams and up to 300-Mbps data rates. Carrier-grade design allows service providers to take advantage of Wi-Fi for next-generation mobile data offloads. The Aironet 1530 Series can be deployed in the following configurations:

- Access point: Either in controller-based or standalone operation, provides Wi-Fi connectivity concurrently to clients on both 2.4-GHz and 5-GHz radios.
- Mesh network: as dedicated backhaul or universal access, the 5-GHz radio is used for wireless network connections to adjacent mesh nodes.
- Bridging: Provides point-to-point, high-capacity data links, as well as point-to-multipoint bridging for campuses.
- Workgroup bridge: Enables LAN mobility, such as on a vehicle.
- Serial backhaul: Extends linear mesh with two colocated Aironet 1530 Series access points connected via the LAN port (Figure 3).

Figure 3. Serial Backhaul Using Two Cisco Aironet 1530 Series Access Points



Centrally Managed Network

Central management and troubleshooting of the Cisco outdoor wireless access points help prevent costly maintenance service calls to outdoor locations. Cisco Prime™ Infrastructure works in conjunction with the Cisco Aironet access points and Cisco wireless LAN controllers to configure and manage the wireless networks. With Cisco Prime Infrastructure, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, security monitoring, and wireless LAN system management. Wireless network security is also a part of a unified wired and wireless solution. Cisco wireless network security offers the highest level of network security, helping ensure that data remains private and secure and that the network is protected from unauthorized access.

Product Specifications

Table 1 lists the specifications for the Cisco Aironet 1530 Series.

Table 1. Cisco Aironet 1530 Series Product Specifications

Item	Specification
Part Numbers	**Cisco Aironet 1530I (internal antennas) and 1530E (external antennas) Outdoor Access Points** • AIR-CAP1532I-A-K9 AIR-CAP1532E-A-K9 • AIR-CAP1532I-C-K9 AIR-CAP1532E-C-K9 • AIR-CAP1532I-D-K9 AIR-CAP1532E-D-K9 • AIR-CAP1532I-E-K9 AIR-CAP1532E-E-K9 • AIR-CAP1532I-F-K9 AIR-CAP1532E-F-K9 • AIR-CAP1532I-H-K9 AIR-CAP1532E-H-K9 • AIR-CAP1532I-K-K9 AIR-CAP1532E-K-K9 • AIR-CAP1532I-M-K9 AIR-CAP1532E-M-K9 • AIR-CAP1532I-N-K9 AIR-CAP1532E-N-K9 • AIR-CAP1532I-Q-K9 AIR-CAP1532E-Q-K9 • AIR-CAP1532I-R-K9 AIR-CAP1532E-R-K9 • AIR-CAP1532I-S-K9 AIR-CAP1532E-S-K9 • AIR-CAP1532I-T-K9 AIR-CAP1532E-T-K9 • AIR-CAP1532I-Z-K9 AIR-CAP1532E-Z-K9 **Cisco SMARTnet® Service for the Cisco Aironet 1530 Series Access Points** • CON-SNT-CAP1532x - SMARTnet 8x5xNBD 1532I integrated antenna access point • CON-SNT-CAP1532Ex - SMARTnet 8x5xNBD 1532E access point Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.

Item	Specification			
802.11n and Related Capabilities	• 1530X: 3x3 MIMO with 3 spatial streams (2.4 GHz) and 2x3 MIMO with 2 spatial streams (5 GHz) • 1530E: 2x2 MIMO with 2 spatial streams (2.4 GHz) and 2x2 MIMO with 2 spatial streams (5 GHz) • 20-MHz (2.4 and 5 GHz) and 40-MHz (5 GHz only) channels • PHY data rates up to 300 Mbps • Packet aggregation: A-MPDU (TxRx) • 802.11 dynamic frequency selection (DFS) • Cyclic shift diversity (CSD) support			
Data Rates Supported	802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps 802.11b/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps 802.11n data rates (2.4 and 5 GHz):			
	MCS Index[1]	GI[2] = 800 ns		GI = 400 ns	
		20-MHz Rate (Mbps)	40-MHz Rate (Mbps)	20-MHz Rate (Mbps)	40-MHz Rate (Mbps)
	0	6.5	13.5	7.2	15
	1	13	27	14.4	30
	2	19.5	40.5	21.7	45
	3	26	54	28.9	60
	4	39	81	43.3	90
	5	52	108	57.8	120
	6	58.5	121.5	65	135
	7	65	135	72.2	150
	8	13	27	14.4	30
	9	26	54	28.9	60
	10	39	81	43.3	90
	11	52	108	57.8	120
	12	78	162	86.7	180
	13	104	216	115.6	240
	14	117	243	130	270
	15	130	270	144.4	300
	16	19.5		21.7	
	17	39		43.3	
	18	58.5		65	
	19	78		86.7	
	20	117		130	
	21	156		173.3	
	22	175.5		195	
	23	195		216.7	
	MCS 16-23 available on 1530X on 2.4 GHz only				