UNIVERSIDAD AUTÓNOMA DE MADRID
ESCUELA POLITÉCNICA SUPERIOR

PROYECTO FIN DE CARRERA

Análisis, diseño y despliegue de una red WiFi en Santillana del Mar

-Ingeniería de Telecomunicación-

Marta Moreno Martín
Enero 2015

Análisis, diseño y despliegue de una red WiFi en Santillana del Mar

AUTOR: Marta Moreno Martín

TUTOR: Eduardo Villanueva

PONENTE: Sergio López Buedo

Departamento de Tecnología Electrónica y de las Comunicaciones

Escuela Politécnica Superior

Universidad Autónoma de Madrid

Enero 2015

Agradecimientos

En primer lugar, me gustaría agradecer a toda mi familia el apoyo que he recibido por su parte durante los cinco años de la carrera así como durante la elaboración del Proyecto Fin de Carrera, en especial a mis padres, María José y Juan, que siempre me han animado y dado la fuerza necesaria para llegar hasta el final.

Gracias a todos mis amigos y compañeros que ante cualquier duda se han volcado en ayudarme, me han animado en todo momento a seguir adelante en circunstancias críticas y siempre han estado ahí cuando más les necesitaba.

Por último, no puedo dejar de agradecer a todos los profesores que he tenido en la carrera, los conocimientos que me han proporcionado, sin ellos hubiese sido más difícil llegar hasta aquí.

Resumen del proyecto

En este proyecto vamos a estudiar cómo implementar una red de comunicaciones haciendo uso de tecnologías inalámbricas que permitan ofrecer una cobertura WiFi total en un municipio de Cantabria, Santillana del Mar, así como interconectar las diferentes áreas con la finalidad de permitir un despliegue ordenado a lo largo del territorio.

En concreto, se analiza la tecnología inalámbrica WiFi que será la predominante en nuestra red de telecomunicaciones, así como la tecnología inalámbrica, WiMAX que también forma parte de la red a implementar.

Se realiza un caso de estudio en el que se define un escenario real. Se trata de un municipio rural en el que sería muy costoso económicamente llevar cableado. Basado en el análisis de requerimientos de la red y al estudio de las diferentes tecnologías se analiza el territorio y se define la solución para la implementación de la red así como su viabilidad: Arquitectura de red, estudios de cobertura, investigación sobre equipos disponibles en el mercado que cumplen los requerimientos del diseño y elección de los más adecuados.

Con el diseño realizado, se definen las fases a seguir para llevar a cabo el proyecto de ingeniería, instalación y configuración del caso estudiado.

Al final se analizan los plazos y la viabilidad económica del proyecto, para hacer una estimación lo más exacta posible de los precios finales, los que llegan al cliente.

Abstract of The Project

In this project we are going to study how to install a communication network by using wireless technology that provides a total coverage of WiFi in a specific town in Cantabria, Santillana del Mar, as well as to interconnect the different areas with the purpose of doing a structured deployment throughout the territory.

Specifically, we are going to analyze WiFi as the Wireless technology dominating our telecommunication network and WiMAX as part of the network to be installed.

A case study is made in which a real scenario is defined. It deals with a rural municipality which would be fairly costly to wire. Based on the analysis of network requirements and on the study of different technologies, the territory was analyzed and a solution defined for the implementation of the network and its viability: Network architecture, coverage studies, research into available equipment on the market that fulfills the design requirements and choosing the most appropriate.

With the design complete we outline the next stages to carry the project through to engineering, installation and configuration of the case study.

At the end we analyze the deadlines and the economic viability of the project, to make an estimate for the final prices that we will present to the clients.

LISTADO DE PALABRAS CLAVE:

- Tecnología inalámbrica
- Movilidad
- Banda de frecuencias
- WLAN (Red de área local inalámbrica)
- WiFi
- WMAN (Red inalámbrica de área metropolitana)
- WiMAX
- WiMAX Forum
- CNAF (Cuadro Nacional de Atribución de Frecuencias)
- IEEE (Instituto de Ingeniería Eléctrica y Electrónica)
- ETSI (Instituto Europeo de Normas de Telecomunicaciones)
- 802.11
- 802.16
- LOS (Línea de vista)
- NLOS (Sin línea de vista)
- OFDM (Multiplexación por División de Frecuencias Ortogonales)
- OFDMA (Acceso Múltiple por División de Frecuencia Ortogonal)
- MIMO (Múltiple entrada múltiple salida)
- 802.11 n
- Ancho de banda
- Modelo OSI
- Capa Física
- Capa MAC
- PLCP
- PMD
- Punto de acceso
- CPE (Equipo Local del Cliente)
- Antena
- QoS (Calidad de servicio)
- Punto a multipunto
- Topología mallada
- Usuario
- Arquitectura de red
- Red de Acceso Inalámbrica
- Red troncal
- L2TP
- EoIP
- NAT (Traducción de dirección de red)

KEYWORD LIST:

- Wireless Technology
- Mobility
- Frequencies Band
- WLAN (Wireless Local Area Network)
- WiFi
- WMAN (Wireless Metropolitan Access Network)
- WiMAX
- WiMAX Forum
- CNAF
- IEEE (Institute of Electrical and Electronics Engineers)
- ETSI (European Telecommunications Standards Institute)
- 802.11
- 802.16
- LOS (Line of Sight)
- NLOS (Non Line of Sight)
- OFDM (Orthogonal Frequency Division Multiplexing)
- OFDMA (Orthogonal Frequency Division Multiple Access)
- MIMO (Multiple Input Multiple Output)
- 802.11 n
- Bandwidth
- OSI Model (Open Systems Interconnection Model)
- Physical Layer
- MAC Layer
- PLCP (Physical Layer Convergence Procedure)
- PMD (Physical Medium Dependent)
- Access Point
- CPE (Customer Premises Equipment)
- Antenna
- QoS (Quality of Service)
- Point to multipoint
- Mesh topology
- User
- Network architecture
- Wireless Access Network
- Backbone
- L2TP
- EoIP
- NAT (Network Address Translation)

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

GLOSARIO

A

ACK: Confirmación de un paquete que ha sido recibido.

AAA: *Authentication, Authoritation and Accounting* (Autenticación, autorización y contabilización.

ADSL: *Asymmetric Digital Subscriber Line* (Línea de abonado digital asimétrica).

AES: Estándar de Encriptación Avanzado.

AP: *Access Point* (Punto de Acceso).

B

Beacon Frame: Contienen toda la información sobre la red inalámbrica y son transmitidos periódicamente para anunciar la presencia de la red WLAN.

Backbone: Red troncal.

BTS: Base Transceiver Station.

BWA: Broadband Wireless Access.

C

CSMA/CD: *Carrier Sense Multiple Access with Collision Detection* (Acceso múltiple con escucha de portadora y detección de colisiones), es un protocolo de acceso al medio compartido. Los dispositivos escuchan antes de transmitir.

CNAF: Cuadro Nacional de Atribución de Frecuencias.

CPE: *Customer Premises Equipment* (Equipo Local del Cliente).

Checksum: Suma de chequeo. Es una función que tiene como propósito detectar cambios accidentales en una secuencia de datos para proteger la identidad de estos, verificando que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra tras finalizar la transmisión.

CRC: Verificación por redundancia cíclica.

D

DHCP: Protocolo de Configuración Dinámica de Host. Protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

E

ETSI: Instituto Europeo de Estándares de Telecomunicaciones. Se trata de una organización de estandarización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial.

ESS: Conjunto de Servicios Extendidos.

EAP: Protocolo de Autenticación Extensible.

F

Frame Aggregation: Es una característica de los estándares IEEE 802.11e y 802.11n que incrementa el rendimiento enviando dos o más tramas de datos en una única transmisión.

Frame Relay: Es una red de conmutación de paquetes que envía paquetes de longitud variable sobre LANs o WANs.

FEC: *Forward Error Correction* (Corrección de Errores Hacia Adelante).

Firmware: Micro-código que controla al hardware.

H

HiperMAN: Es un estándar creado por el Instituto Europeo de Telecomunicaciones (ETSI) dirigido principalmente para proveer DSL inalámbrica de banda ancha, cubriendo una zona geográfica grande.

HiperLAN: LAN con alto rendimiento de radio.

Hacker: Atacante informático cuyo fin es obtener ilegalmente recursos de una red, para extraer información y sabotear el sistema.

Hotspot: Es una zona de cobertura WiFi, en el que el punto de acceso (Access Point) o varios proveen servicios de red a través de un Proveedor de Servicios de Internet Inalámbrico (WISP).

I

IP: *Internet Protocol* (Protocolo de Internet).

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos.

ISM: Banda de frecuencias para la Investigación Científica y Médica.

L

LAN: Red de área local.

LOS: *Line of Sight* (Línea de vista), se dice o aplica el término para un enlace de radio que debe tener visibilidad directa entre antenas.

M

Multiplexación: Combinación de dos o más flujos de información en un solo medio de transmisión.

MAC: *Media Access Control* (Control de Acceso al Medio).

MIMO: *Multiple Input Multiple Output* (Múltiple entrada múltiple salida), se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos.

N

NAT: *Network Address Translation* (Traducción de Dirección de Red), mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

NLOS: *Non Line of Sight* (Fuera de la línea de Visión), es un término utilizado en comunicaciones de radiofrecuencia, se usa para describir un trayecto parcialmente obstruido entre la ubicación del transmisor de la señal y la ubicación del receptor de la misma.

O

OFDM: *Orthogonal Frecuency Division Multiplexing* (Multiplexación por división de frecuencias ortogonales).

OFDMA: *Orthogonal Frecuency Division Multiple Access.*

OSI: *Open System Interconnection* (Interconexión de Sistemas Abiertos), modelo de red descriptivo, que fue creado por la Organización Internacional para la Estandarización (ISO).

P

P2P: *Peer to peer*. Red de pares en el que cada nodo actúa simultáneamente como cliente y servidor.

PIRE: Potencia Isotrópica Radiada Equivalente.

PDU: Unidad de datos del Protocolo, se utilizan para el intercambio de datos entre unidades disparejas, dentro de una capa del modelo OSI.

PPP: Protocolo punto a punto.

PCI: *Peripheral Component Interconnect* (Interconexión de Componentes Periféricos).

PoE: *Power over Ethernet*. Tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar.

Q

QoS: *Quality of Service* (Calidad de servicio).

R

Roaming: Conectividad entre celdas en un área de cobertura. Particularidad de los equipos inalámbricos para desplazarse dentro de una red sin perder la conexión.

RSTP: *Rapid Spanning Tree Protocol*, es un protocolo de red de la segunda capa OSI, que gestiona enlaces redundantes. Reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología.

S

SNR: *Signal to noise*. La relación señal/ruido se define como el margen que hay entre la potencia de la señal que se transmite y la potencia del ruido que la corrompe.

Switch: Conmutador.

T

Telnet: Protocolo para acceso a máquinas remotas.

TCP: Protocolo de Control de Transmisión.

Throughput o rendimiento: Cantidad de datos por unidad de tiempo que fluyen por un sistema.

U

UDP: Protocolo de Datagramas de Usuario.

W

WiFi: *Wireless Fidelity* (Fidelidad Inalámbrica). Estándar de transmission de datos sin cable.

WiMAX: *Worldwide Interoperability for Microwave Access* (Interoperabilidad Mundial para enlaces por Microondas).

WECA: Alianza de Compatibilidad Inalámbrica con Ethernet**.**

1. Introducción

1.1 Motivación y objetivos

El desarrollo de las telecomunicaciones se está orientando en los últimos años, a un uso intensivo de sistemas de banda ancha con altos niveles de calidad, mediante el desarrollo de tecnologías de alta capacidad de transmisión, entre los cuales podemos destacar la fibra óptica o el cable coaxial hasta el domicilio del abonado. Los sistemas anteriormente mencionados, basados en cable, por lo general tienen un alto costo de instalación, representando además dificultades en su construcción, instalación y puesta en servicio. Adicionalmente a esto, el desarrollo de estos medios de transmisión en medios rurales y de preferente interés social, representan inversiones de muy difícil recuperación por las características propias de la demanda.

Frente a esta situación y otras limitaciones tecnológicas y topográficas se han buscado alternativas inalámbricas que permitan un despliegue rápido de la infraestructura, mayor predictibilidad de amortización de la inversión hacia los lugares donde se instalan, así como menores costos de operación y mantenimiento.

Las redes inalámbricas, en los últimos años, han logrado una rápida y gran acogida a nivel mundial y poco a poco están ocupando un lugar más destacado dentro del panorama de las posibilidades que tienen dos dispositivos de intercomunicarse. Está ocupando rápidamente las preferencias de todo tipo de usuarios, además de que están abriendo paso para dar soporte a nuevos servicios que la propia sociedad ha demandado.

Debido a la continua evolución de las tecnologías, los usuarios de las redes inalámbricas son cada vez más exigentes en cuanto a la calidad, la rapidez, el coste y la apariencia de los productos que contratan. De esta forma, además del diseño y la innovación que han pasado a tener una gran importancia en el mundo actual, proporcionar accesos de alta capacidad es algo muy importante, ya que Internet constituye una de las innovaciones más importantes de nuestra época, por los sustanciales beneficios que aporta a las economías y a las sociedades. La posibilidad de comunicar información a alta velocidad a través de diferentes plataformas es algo esencial para el desarrollo de nuevos bienes y servicios.

Dentro de las tecnologías inalámbricas existentes en la actualidad, una de las más extendidas es la tecnología WiFi, que ha pasado a formar parte de cada vez más hogares, oficinas, zonas públicas así como en ciudades y transporte.

Permitir una conexión inalámbrica entre dispositivos electrónicos de modo que los ciudadanos sean capaces de transmitir información a lugares lejanos en fracciones de minutos, y recibir información en el momento que se precisa de forma gratuita y en cualquier parte de la ciudad, supone un gran desarrollo para las ciudades.

Las ventajas que obtiene una ciudad al proveer este tipo de servicios es eminentemente comercial: La ciudad se promociona cara al turismo, a sus habitantes y

a habitantes de zonas cercanas. Se mejora el tejido empresarial del municipio ya que las empresas pueden estar siempre conectadas y con ello mejorar la comunicación y eficiencia.

En concreto, en este proyecto nos centraremos en una solución de telecomunicación inalámbrica en la que se desplegará una red WiFi de modo que se pueda dar un servicio de acceso a Internet en el municipio Cántabro de Santillana del Mar. Se implementará una red de telecomunicaciones para dar cobertura a las zonas del municipio que se especificarán más adelante.

Para lograr las metas fijadas en el desarrollo del proyecto se han planteado los siguientes objetivos de trabajo.

- Se requiere un cuidadoso estudio y análisis de las tecnologías de comunicación que se utilizarán para interconectar las diferentes áreas con la finalidad de permitir un despliegue ordenado a lo largo del territorio y a su vez ofrecer una cobertura WiFi total en el área requerida.

- Sobre planos, cubrir el 100% de las áreas en las que se desea proveer cobertura utilizando el software correspondiente.

- Optimizar el número de puntos de acceso necesarios para cubrir la totalidad de la zona.

- Elección del equipamiento más eficiente para garantizar la calidad de servicio.

1.2 Metodología y plan de trabajo

Para alcanzar el objetivo principal el proyecto se resumirá en los siguientes hitos:

Fase de documentación: Se realizará un estudio del arte, a través de la bibliografía, de las principales tecnologías de comunicación inalámbrica existentes en el mercado. Se hará un estudio más exhaustivo de las tecnologías WiFi y WiMAX que son las que se llevarán a cabo en la implementación de nuestra red de telecomunicaciones.

Fase de toma de requisitos: Ajustándonos a los requerimientos que transmite el cliente, a lo largo del proyecto se irá implementando la red teniendo en cuenta que se deben cumplir cada uno de los puntos que impone el cliente. Analizamos los diferentes requisitos para poder alcanzar el objetivo de la forma más eficiente.

Fase de análisis y diseño: En dicha fase se realizará el caso de estudio de nuestra red de telecomunicaciones.

1. Estudio del terreno sobre el que se va a implementar el servicio.
2. Estudio de la arquitectura de red general del sistema que se implementará en el municipio. Cómo se conectarán los puntos de acceso entre sí y con las plataformas centrales. Donde se ubicarán las líneas de comunicación.

3. Estimación de la cobertura a través de planos del municipio proporcionados por Google Earth así como los puntos de acceso necesarios para cubrir la zona requerida a través de mapas.
4. Realización de un replanteo final de los puntos de acceso y de los equipos centrales de la red para corroborar que lo estudiado hasta el momento es completamente viable.
5. Estudio del equipamiento a utilizar con el fin de obtener las mejores prestaciones.

Fase de ejecución: Dicha fase no se ejecutará realmente, se explicarán los pasos a seguir y la metodología que habría que emplear si se llevase a cabo el proyecto.

1. Compra del equipamiento necesario para la implementación de la red de telecomunicaciones.
2. Solicitud de las líneas de comunicaciones
3. Configuración de los puntos de acceso con el software proporcionado por el fabricante.
4. Configuración de las controladoras centrales.
5. Envío de los equipos al municipio de Santillana del Mar.
6. Instalación de la red de telecomunicaciones llevada a cabo por los técnicos.

Fase de Certificación y mantenimiento: Fase en la cual se garantiza la calidad del proyecto.

1. Comprobación in situ de la instalación realizada en el municipio.
2. Estudio del sistema que proporcione la monitorización de los puntos de acceso y el rendimiento de ellos.
3. Mantenimiento a través del programa que proporcione la monitorización.

Fase de Documentación y seguimiento.

4. Durante la vida del proyecto, para garantizar la correcta ejecución del mismo, se realiza una labor de seguimiento, momento en el que es posible la solución a diferentes problemas, así como estar disponibles sobre cualquier consulta que pueda surgir.
5. Desarrollo de la memoria a lo largo de todo el proyecto.

1.3 Organización de la memoria

La memoria está dividida en ocho capítulos:

CAPÍTULO 1. INTRODUCCIÓN: Tiene como objetivo proporcionar al lector una idea aproximada de los objetivos de este proyecto y los motivos que han llevado a la elaboración del mismo, así como los hitos principales que se llevarán a cabo durante el ciclo de vida del proyecto.

CAPÍTULO 2. ESTADO DEL ARTE: Se trata de una introducción a las tecnologías inalámbricas, realizando un estudio más exhaustivo acerca de las tecnologías WiFi y WiMAX, para comprender el funcionamiento de ambas.

CAPÍTULO 3. CASO DE ESTUDIO: Comenzará con las necesidades del cliente. Se desarrollará y diseñará la red de telecomunicaciones y se exhibirá una solución óptima para ofrecer cobertura en el municipio Cántabro.

CAPÍTULO 4. FASE DE EJECUCIÓN: En dicho capítulo se detallarán los pasos necesarios para que la red quede completamente implementada. Abarcará desde las compras hasta la configuración de los equipos y posterior instalación de la red de telecomunicaciones.

CAPÍTULO 5. CERTIFICACIÓN Y MANTENIMIENTO. Se indican cómo se realizarán pruebas de campo para verificar el funcionamiento de la red así como la definición de una herramienta de monitoreo que optimice la administración del sistema.

CAPÍTULO 6. PLAZOS Y PRESUPUESTO DEL PROYECTO: Se realizará una estimación de los plazos necesarios para la ejecución del proyecto, así como la viabilidad económica, haciendo una estimación lo más exacta posible de los precios finales que llegan al cliente.

CAPÍTULO 7. CONCLUSIONES Y TRABAJO FUTURO: Resume el trabajo realizado durante la elaboración del proyecto recogiendo las conclusiones obtenidas y las posibles líneas de investigación que se podrían realizar una vez implementada la red de comunicaciones.

CAPÍTULO 8. REFERENCIAS: En este capítulo se indicará tanto la bibliografía utilizada como algunos anexos importantes.

2. Estado del arte

2.1 Introducción a las redes inalámbricas

En los últimos años se han desarrollado con gran éxito diversos estándares de redes inalámbricas, en áreas en las que anteriormente solo existían algunos sistemas propietarios con baja implantación. El concepto de redes inalámbricas generalmente se asocia a redes surgidas en el ámbito de transmisión de datos, en las que tradicionalmente se utilizaban redes basadas en cables eléctricos o en fibra óptica.

Las redes inalámbricas son de carácter libre, están diseñadas para operar en bandas de frecuencia para las que no se necesita licencia de uso. Éste es el caso de la banda de 2.4 GHz y de 5GHz. Esto ha favorecido enormemente la implantación de la tecnología inalámbrica, ya que da lugar a unos costos de uso mucho menores que las redes basadas en sistemas celulares. No obstante, no se está exento de problemas ya que estas bandas de frecuencias son utilizadas por distintas tecnologías (WiFi, Bluetooth, etc) pudiendo aparecer problemas de interferencias.

Además, permiten crear redes en áreas complicadas donde se pueden conectar gran cantidad de dispositivos, en lugares donde resulta dificultoso o muy cara la conexión de cables.

Gracias a la aparición y al éxito de los protocolos de comunicación inalámbrica se ha producido una gran difusión en la utilización de dichas redes, debido fundamentalmente a la interoperabilidad del equipamiento producido por distintos fabricantes. Esto ha promovido que se desarrollen productos de manera veloz, haciendo que los precios se hayan visto disminuidos gracias al volumen de producción.

Las comunicaciones inalámbricas pueden clasificarse de distintas formas dependiendo del criterio al que se atienda. En este caso, vamos a clasificar los sistemas de comunicaciones inalámbricas de acuerdo con su alcance, definido como la distancia máxima a la que pueden situarse las dos partes de la comunicación inalámbrica.

- **Las redes inalámbricas de área personal o WPAN (Wireless Personal Area Network)** son aquellas que tienen un área de cobertura de unos pocos metros. La finalidad de estas redes es la comunicación entre cualquier dispositivo personal (por ejemplo, el ordenador con la impresora) con sus periféricos, así como permitir una comunicación directa a corta distancia entre estos dispositivos. Algunas tecnologías que se utilizan en este tipo de redes son Bluetooth, DECT y los infrarrojos.

- **Las redes inalámbricas de área local o WLAN (Wireless Local Area Network)** cubren distancias de unos cientos de metros. Estas redes están pensadas para crear un entorno de red local entre ordenadores o terminales situados en un mismo edificio o grupo de edificios. En el mercado existen distintas tecnologías que dan respuesta a esta necesidad, aunque la más frecuente es la tecnología

WiFi, existen otras como HomeRF, HiperLAN, OpenAir.

- **Las redes inalámbricas de área metropolitana o WMAN (Wireless Metropolitan Area Network)** pretenden cubrir el área de una ciudad o entorno metropolitano. Tienen una cobertura desde cientos de metros hasta varios Kilómetros. Los protocolos WiMax (Worldwide Interoperability for Microwave Access) o LMDS (Local Multipoint Distribution Service) ofrecen soluciones de este tipo.

- **Las redes inalámbricas de área global o WWAN (Wireless Wide Area Network)** son los sistemas basados en la tecnología celular y tienen la posibilidad de cubrir un país entero o un grupo de países. Se trata de un sistema para mantener la comunicación independientemente del lugar donde nos encontremos. Las tecnologías WWAN se conocen también como sistemas de segunda generación (2G), de tercera generación (3G) o los actuales sistemas (4G) definidos como un estándar de la norma 3GPP.

Como hemos visto, existen tecnologías distintas de comunicaciones inalámbricas. Muchas de ellas son complementarias, otras dan respuesta a una misma necesidad y por ello compiten entre ellas por ser las preferidas en el mercado.

A continuación se muestra una tabla comparativa de las principales tecnologías de las comunicaciones inalámbricas.

Tipo de red	**WWAN** (Wireless **Wide** Area Network)	**WMAN** (Wireless **Metropolitan** Area Network)	**WLAN** (Wireless **Local** Area Network)	**WPAN** (Wireless **Personal** Area Network)
Estándar	GSM/GPRS/UMTS	IEEE 802.16	IEEE 802.11	IEEE 802.15
Denominación/ Certificación	2G/3G	WiMAX	WiFi	Bluetooth, Zigbee
Velocidad	9.6/170/2000 Kb/s	15-134 Mb/s	1-2-11-54-300-Mb/s- 1 Gb/s	721 Kb/s
Frecuencia	0.9/1.8/2.1 GHz	2-66 GHz	2.4 y 5 GHz Infrarrojos	2.4 GHz
Rango	Limitado por células (máx. 35 Km por célula)	1.6-50 Km	30-150 m	10 m
Técnica radio	Varias	Varias	FHSS, DSSS, OFDM	FHSS
Itinerancia (Roaming)	Sí	Sí (802.16e)	Sí	No
Equivalente a:	Conex.telef. (modem)	ADSL,CATV	LAN	Cables de conexión

Tabla 1. Comparativa de tecnologías inalámbricas

Una vez conocidas las diferentes tecnologías inalámbricas, este proyecto se va a basar en la implantación de una red WiFi a lo largo del municipio de Santillana del Mar, donde se hará uso de la tecnología inalámbrica WiFi principalmente. No necesariamente la misma tecnología puede satisfacer todas las necesidades requeridas en cada punto, por lo que es posible que WiMAX sea otra de las tecnologías a utilizar.

En los apartados sucesivos se estudiarán en profundidad dichas tecnologías de comunicación inalámbrica.

2.2 Tecnología inalámbrica WIFI

Como se ha comentado anteriormente, una de las tecnologías más utilizadas en la actualidad para la creación de redes inalámbricas de área local es WiFi.

Inicialmente era muy habitual que las redes inalámbricas se llevasen a cabo utilizando soluciones particulares de cada fabricante, ya que los diferentes dispositivos que existían en el mercado eran incompatibles entre sí. Esto suponía estar sometido siempre a las limitadas soluciones que un solo fabricante puede ofrecer.

Para normalizar la situación, se desarrolló un sistema que fuese aceptado por todos los fabricantes como sistema común.

De esta forma, se creó la asociación WECA (Wireless Ethernet Compatibility Alliance), actualmente conocida como WiFi Alliance, cuyo objetivo fue designar una marca que permitiese fomentar la tecnología inalámbrica y asegurar la compatibilidad de equipos. Además WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello WiFi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos.

2.2.1 Estándares IEEE 802.11

La familia de estándares de redes WLAN IEEE 802.11 ha sido la causa de la incorporación y el desarrollo rápido de las redes WLAN en el mercado. Dentro del grupo de trabajo IEEE 802.11 se pueden encontrar diferentes estándares:

- **IEEE 802.11b**

Publicado en 1999, ganó una amplia aceptación en la industria. Tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el método de acceso definido en el estándar original CSMA/CA. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, la velocidad real de transmisión se reduce a 5.9 Mbps sobre TCP y 7.1 Mbps sobre UDP.

El estándar 802.11b funciona en la banda de frecuencia de 2.4 GHz, la cual, al no necesitar licencia de uso, puede ser utilizada por cualquier tecnología inalámbrica y producir interferencias.

- **IEEE 802.11a**

Estandarizado por el IEEE en julio de 1999 aunque no llega a comercializarse hasta 2002. Se consiguen velocidades de 54 Mbps e incluso es posible alcanzar los 72 y 108 Mbps con versiones propietarias de esta tecnología. Esto hace que sea un estándar con velocidades reales de hasta 20 Mbps.

Trabaja en la banda de 5GHz, y utiliza la técnica OFDM (Orthogonal Frequency-Division Multiplexing) con 52 subportadoras. El estándar 802.11 tiene doce canales sin solapa,

8 para red inalámbrica y 4 para conexiones punto a punto.

El hecho de que no pudiera interoperar con equipos del estándar 802.11b, salvo si se dispone de equipos que implementen ambos estándares y la limitación del radio de alcance debido a un mayor índice de absorción de sus ondas, supuso una desventaja que limitó su aceptación en la industria.

- **IEEE 802.11g**

En Junio de 2003 aparece el estándar 802.11g con la idea de aumentar la velocidad sin renunciar a las ventajas de la banda de los 2.4 GHz. Esta norma, permite transmitir datos a 54 Mbps que en promedio es de 22 Mbps de velocidad real de transferencia.

Es compatible con el protocolo 802.11b y puede trabajar con el protocolo 802.11a cambiando la configuración de los equipos. Esto es debido a que 802.11g, puede operar con las tecnologías OFDM y DSSS.

Pese a la compatibilidad, en redes bajo el estándar b, la presencia de nodos g reduce notablemente la velocidad de transmisión, debido a que los clientes 802.11b no comprenden los mecanismos de envío de OFDM.

- **IEEE 802.11n**

El estándar 802.11n fue ratificado en Septiembre de 2009 por la organización IEEE. La base de su funcionamiento es la incorporación de varias antenas, que permiten utilizar varios canales para enviar y recibir datos simultáneamente, mejorando de forma sustancial la señal recibida por el receptor y multiplicándose de esta forma el ancho de banda utilizado. Esto es lo que se conoce como la tecnología MIMO (Multiple Input Multiple Output).

El 802.11n incluye grandes mejoras en el uso del entorno radio con el fin de mejorar el caudal neto de la WLAN. Algunos de los cambios más relevantes son:

- **Incremento del canal de transmisión**: A diferencia de los estándares 802.11a/b/g que utilizan un canal con un ancho de banda de 20 MHz, el 802.11n usa canales con un ancho de banda de 20 MHz y 40 MHz. Un canal de 40 MHz está formado por una combinación de dos canales de 20 MHz adyacentes. La unión de canales aumenta la velocidad de transmisión de datos debido a que la velocidad de transmisión de datos es directamente proporcional al ancho de banda. La idea de este solapamiento es aprovechar el ancho de banda de las cabeceras de inicio del canal y las cabeceras de la cola del canal para enviar datos. Al unir dos canales adyacentes la cola del primer canal que se usa para reducir la interferencia entre canales adyacentes y la cabecera del segundo canal ya no tienen ninguna utilidad y el ancho de banda que ocupan pasa a ser usado para la transmisión de datos.

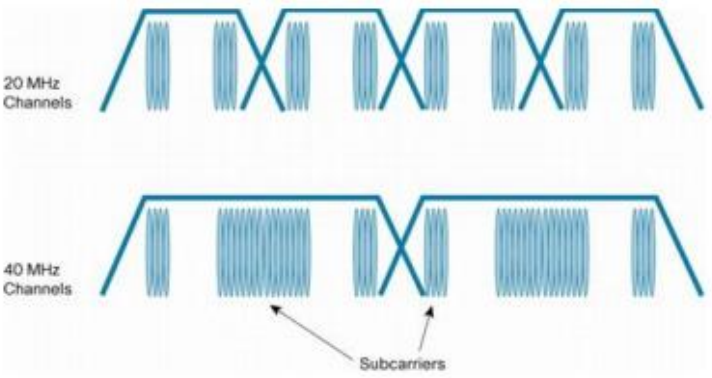


Ilustración 1. **Canales de 20 MHz y 40 MHz**

Fuente. Yaagoubi, M. Universidad Carlos III

- **Alta tasa de modulación**: El estándar 802.11n usa la modulación OFDM (Ortogonal Frequency Division Multiplexing) que divide un canal de transmisión en varios subcanales, teniendo cada subcanal su propia subportadora que transporta información independientemente de las otras portadoras. El aumento de ancho de banda de los canales de 802.11n a 40 MHz proporciona más portadoras, traduciéndose en un aumento de la velocidad de transmisión de hasta 600 Mbps.

- **Reducción de cabeceras (Intervalo de guarda)**: El intervalo de guarda se utiliza para asegurarse de que no interfieren las diferentes transmisiones entre ellas. El 802.11a/g utilizan un intervalo de guarda de 0.8 microsegundos al igual que el estándar 802.11n en su modo por defecto, pero para aumentar la velocidad de los datos, dicha norma añadió un soporte opcional para un intervalo de guarda de 0.4 microsegundos que proporciona un aumento de 11% en la velocidad de transferencia de datos.

Además, la versión 802.11n introduce cambios en la trama MAC. Se añade lo que se llama Frame Aggregation que consiste en el envío de dos o más fragmentos en una sola transmisión.

A diferencia de las otras versiones de WiFi, 802.11n puede trabajar tanto en la banda de frecuencia de 2.4 GHz como en la de 5 GHz, lo que hace que sea compatible con las tres tecnologías anteriores (a, b y g).

Es muy útil que pueda trabajar en la banda de frecuencias de 5GHz, ya que esta menos congestionada y permite un mejor rendimiento de dicho estándar.

❖ **IEEE 802.11ac**

Es una mejora de la norma 802.11n que se ha desarrollado entre 2012 y 2013. La industria ya trabaja en nuevos protocolos y dispositivos basados en el protocolo 802.11ac. El sistema permite unas tasas de transferencia de 1Gbps en la banda de 5GHz, un ancho de banda hasta 160 MHz, hasta ocho flujos MIMO y modulación de

alta densidad.

Otra de las ventajas con respecto a las versiones anteriores, es el alcance de cobertura, que llega hasta un máximo de 90-100 metros mediante el uso de tres antenas internas.

Protocolo	Año de publicación	Frecuencia	Ancho de banda	Velocidad de datos (típica)	Velocidad máxima	Alcance interior	Alcance exterior
802.11b	1999	2.4 GHz	20 MHz	6.5 Mbps	11 Mbps	~100 m	~200 m
802.11a	1999	5 GHz	20 MHz	25 Mbps	54 Mbps	~ 70 m	~ 70 m
802.11g	2003	2.4 GHz	20 MHz	25 Mbps	54 Mbps	~ 38 m	~ 140 m
802.11n	2009	2.4 GHz 5 GHz	20 MHz a 40 MHz	200 Mbps	600 Mbps	~ 70 m	~ 250 m
802.11ac	2012	5 GHz	20, 40, 50 y 160 MHz	-	>1 Gbps	~70 m	~ 250 m

Tabla 2. Estándares IEEE 802.11

Es necesario aclarar la diferencia entre velocidad de transmisión en el aire y velocidad real (comúnmente conocida como throughput). Cuando se habla de velocidad de transmisión en el aire se incluye la información de usuario así como toda aquella información adicional para asegurar el intercambio fiable de información (protocolos, verificación errores, etc.), mientras que cuando hablamos de velocidad real es la velocidad en cuanto a transferencia de datos que observa el usuario. Una manera de medir este último es monitorizando la velocidad de transmisión en el puerto Ethernet de los equipos mientras se está usando alguna aplicación que consuma todo el ancho de banda (como puede ser una transferencia de archivos mediante FTP). Es importante realizar todo el diseño, en cuanto a ancho de banda se refiere, basándose siempre en la velocidad real.

Otro parámetro a tener en cuenta a la hora de diseñar una red WiFi es el alcance de su cobertura inalámbrica. Algunos de los motivos por los que puede variar el alcance de la señal son los siguientes:

- Las obstrucciones en el trayecto que recorre la señal como pueden ser árboles, edificios, paredes, accidentes geográficos, etc.
- Tipo de material con que está construida la locación donde se desea recibir la señal WiFi
- Potencia de emisión de la estación base o Punto de Acceso
- Posición y ubicación de la antena receptora
- Ganancia de la antena receptora
- Interferencias que puedan provenir de otros sistemas radioeléctricos
- Longitud del cable que une la antena receptora con la placa WiFi

Por lo que el alcance especificado en la tabla anterior es una medida aproximada.

❖ **Otros estándares**

802.11 c- Estándar que define las características que necesitan los APs para actuar como puentes (bridges). Utilizado para la comunicación de dos redes distintas a través de una conexión inalámbrica.

802.11 d- Está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo móvil.

802.11 e- Estándar inalámbrico que permite interoperar entre entornos públicos, de negocios y usuarios residenciales. Añade características QoS y de soporte multimedia, manteniendo la compatibilidad con el estándar 802.11b y 802.11a. El sistema de gestión centralizado integrado en QoS evita la colisión y cuellos de botella, mejorando la capacidad de entrega en tiempo crítico de las cargas.

802.11 f- Es una recomendación para los proveedores de puntos de acceso que permite que los productos sean compatibles. Este estándar permite a un usuario itinerante cambiarse de un punto de acceso a otro mientras está en movimiento sin importar qué fabricantes de puntos de acceso se usen en la infraestructura de red. También se conoce a esta propiedad simplemente como itinerancia. La adopción de esta práctica es lo que permitirá el Roaming entre diferentes redes.

802.11 h- Estándar que proporciona al 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia como la potencia de transmisión.

802.11 i – Define el cifrado y la autentificación para complementar, completar y mejorar WEP. Es un estándar que mejora la seguridad de las comunicaciones mediante el uso de WPA con su técnica llamada Temporal Key Integrity Protocol (TKlP), aplicable a redes 802.11a, 802.11b y 802.11g.

802.11 k- Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN, para hacer las redes inalámbricas más eficientes. Está diseñado para ser implementado en software, para soportarlo el equipamiento WLAN sólo requiere ser actualizado. Y, como es lógico, para que el estándar sea efectivo, han de ser compatibles tanto los clientes (adaptadores y tarjetas WLAN) como la infraestructura (puntos de acceso y conmutadores WLAN).

802.11 m: Estándar Propuesto para el mantenimiento de redes inalámbricas.

802.11 r- También conocido como *Fast Basic Service Set Transition*, su principal característica es permitir a la red que establezca los protocolos de seguridad que identifiquen a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él. Esta función permite transferencias rápidas, de forma que se mantenga una comunicación sin que haya cortes perceptibles.

802.11s: Es la especificación desarrollada por el IEEE Task Group (TGs) para redes

WiFi malladas. También son conocidas como redes Mesh. Se trata de una topología de red donde cada nodo está conectado a uno o varios nodos dando lugar a diferentes caminos para transmitir la información de un nodo a otro. En el caso que un punto de acceso sufra un desperfecto y provoque un fallo, la red no se caería, si no que los demás puntos de acceso buscarían un camino alternativo para transmitir la información.

Las infraestructuras de una arquitectura de malla inalámbrica es en efecto un router de la red menos el cableado entre los nodos. Esta construido por pares de dispositivos de radio que no tienen que estar cableados a un puerto como los puntos de acceso WLAN tradicionales lo hacen. La arquitectura de malla sostiene la intensidad de la señal mediante las largas rupturas a distancias, en una serie de saltos más cortos. Los nodos intermedios no sólo aumentan la señal, también hacen cooperativamente decisiones de envío en base a su conocimiento de la red, es decir, realizan enrutamiento. Tal arquitectura con un diseño cuidadoso puede proporcionar un gran ancho de banda, eficiencia espectral y una ventaja económica sobre el área de cobertura.

Las redes Mesh facilitan la comunicación inalámbrica brindando así soluciones a las necesidades que afrontan las comunicaciones. En los últimos años ha tenido bastante demanda la idea de implantar sistemas de redes WiFi Mesh. En una parte del presente proyecto se implementará una red mallada WiFi.

802.11 v- Permite la configuración remota de los dispositivos, pudiendo realizar una gestión de las estaciones de forma centralizada o distribuida, a través de un mecanismo de la capa 2.

2.2.2 Bandas de frecuencias de las redes WIFI

Se ha hablado de que las redes WiFi funcionan en dos bandas de frecuencias:

- Banda de 2.4 GHz
- Banda de 5GHz

Ninguna de las dos bandas requiere licencia para su utilización, pero se encuentran sujetas a la regulación fijada por la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) en el Cuadro Nacional de Frecuencias (CNAF). Ambas bandas están designadas para aplicaciones ISM (Industry, Science and Medical) ó ICM (Industrial, Científica y Médica).

- **Banda 2.4GHz**:

La banda de 2.4GHz para uso en redes WiFi consta del siguiente rango de frecuencias 2.4 – 2.4835 GHz. En España, la utilización de dicha banda de frecuencias para el establecimiento de una red inalámbrica WLAN fue aprobada en el 2002 bajo las Notas de utilización nacional UN-85 del CNAF para sistemas de telecomunicaciones de baja

potencia en redes de interiores o de exteriores de corto alcance.

En la UN-85 se establece que dicha banda de frecuencias podrá ser utilizada también para los siguientes usos de radiocomunicaciones bajo la consideración de uso común:

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

  Estos dispositivos pueden funcionar con una potencia isotrópica radiada equivalente (PIRE) máxima de 100mW (20 dBm) conforme a la Decisión de la Comisión 2011/829/UE y la Recomendación CEPT ERC/REC 70-03.

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

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

- Dispositivos genéricos de baja potencia en recintos cerrados y exteriores de corto alcance. Siendo la potencia isotrópica radiada equivalente máxima inferior a 10 mW.

Existen un total de 14 canales, aunque cada país y zona geográfica aplica sus propias restricciones al número de canales disponibles. En Europa disponemos de los trece primeros canales. El ancho de banda por canal en la banda de 2.4GHz es de 22MHz y la separación entre ellos es de 5MHz. Esto hace que se produzca un solapamiento de todos los canales con sus adyacentes como se puede observar en la Ilustración 2**.**

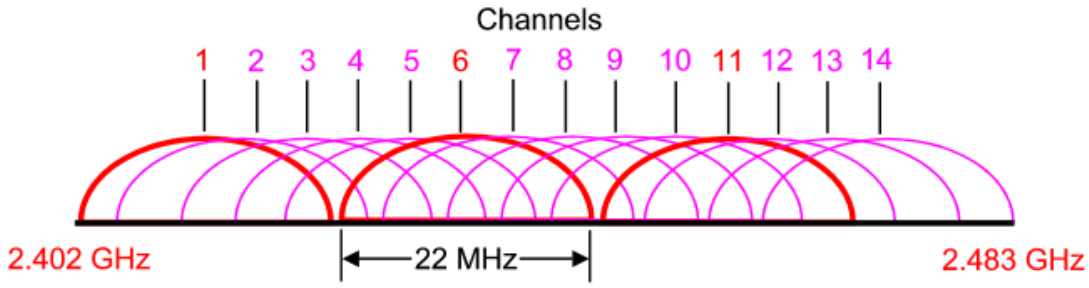


Ilustración 2. Canales en la banda de 2.4 GHz

Aparece un concepto importante a tener en cuenta a la hora de asignar las frecuencias: el solapamiento. Como puede observarse en la figura, el canal 1 se superpone con los canales 2, 3 ,4 y 5, y por lo tanto los dispositivos que emitan en ese rango de frecuencias pueden generar interferencias. Lo mismo ocurre con el canal 6 y los canales 7, 8, 9 y 10, y con el canal 11 y los canales 12, 13 y 14. Por lo tanto, para obtener un rendimiento óptimo de la red inalámbrica WiFi, nuestros equipos Access Point (AP) se deben configurar en los canales que están más separados, bien sea el canal 1, el canal 6 o el canal 11, dependiendo del nivel de saturación de nuestra zona de cobertura.

❖ **Banda 5GHz**

La banda de 5GHz dispone de un mayor ancho de banda que la de 2.4 GHz y presenta un menor nivel de interferencias ya que en la banda de 5 GHz existen menos servicios que los que se pueden encontrar en la banda ICM. Aun así, presenta otros problemas como que el uso de mayores frecuencias implica mayor atenuación en las transmisiones y la poca armonía que existe a nivel internacional en cuanto a las bandas. Los canales tienen un ancho de banda de 16.6 MHz y están separados 20 MHz. En este caso, el espectro de ningún canal solapa con algún otro colindante, por lo que pueden ser utilizados todos al mismo tiempo para planificar una red inalámbrica. La banda fue aprobada para uso común en el año 2003 y adaptada en España en la norma UN-128 del CNAF. Las bandas de frecuencia indicadas seguidamente podrán ser utilizadas por el servicio móvil en sistemas y redes de área local de altas prestaciones. Los equipos utilizados deberán disponer del correspondiente certificado de conformidad de cumplimiento con la norma EN 301 893 o especificación técnica equivalente.

La banda de 5GHz para uso en redes WLAN consta del siguiente rango de frecuencias: 5.150GHz – 5.725GHz en España. Su utilización es el siguiente:

- **Rango de frecuencias 5150 – 5350 MHz**: La potencia isotrópica radiada equivalente máxima será de 200mW, siendo la densidad máxima de PIRE media de 10 mW/MHz en cualquier banda de 1 MHz. Este valor se refiere a la potencia promediada sobre una ráfaga de transmisión ajustada a la máxima potencia. Adicionalmente, en la banda 5250-5350 MHz el transmisor deberá emplear técnicas de control de potencia (TPC) que permitan como mínimo un factor de reducción de 3dB de la potencia de salida. En caso de no usar estas técnicas, la potencia isotrópica radiada equivalente máxima deberá ser de 100 mW (PIRE).

- **Rango de frecuencias 5470-5725 MHz**: Esta banda puede ser utilizada para redes de área local en el interior o exterior de recintos con potencia inferior o igual a 1W (PIRE).

  Estos sistemas deberán disponer de técnicas de control de potencia (TPC) y selección dinámica de frecuencia (DFS) de acuerdo a las especificaciones de la Recomendación UIT-R M.1652 sobre sistemas de acceso radio en la banda de 5GHz.

Banda de frecuencia (MHz)	Número canal	Frecuencia central	CNAF
5150-5250	36	**5180**	Sí
	40	**5200**	Sí
	44	**5220**	Sí
	48	**5240**	Sí
5250-5350	52	**5260**	Sí
	56	**5280**	Sí
	60	**5300**	Sí
	64	**5320**	Sí
5470-5725	100	**5500**	Sí
	104	**5520**	Sí
	108	**5540**	Sí
	112	**5560**	Sí
	116	**5580**	Sí
	120	**5600**	Sí
	124	**5620**	Sí
	128	**5640**	Sí
	132	**5660**	Sí
	136	**5680**	Sí
	140	**5700**	Sí
5725-5825	149	**5745**	Sí
	153	**5765**	Sí
	157	**5785**	Sí
	161	**5805**	Sí

Tabla 3. Banda de frecuencias 5GHz

2.2.3 Fundamentos: capa física y capa de enlace

El comité IEEE, encargado de la tecnología de red de área local desarrolló el primer estándar para redes LAN inalámbricas (IEEE 802.11). Se diseñó para que pudiera sustituir a las capas física y MAC de la norma IEEE 802.3 (Ethernet). Dichas normas sólo se diferencian en la forma en que los ordenadores y terminales acceden a la red, el resto es similar.

MODELO OSI			PROTOCOLOS
7	Aplicación	Común	HTTP, FTP, POP3, etc.
6	Presentación		DNS, LDAP, XML, etc.
5	Sesión		
4	Transporte		UDP, TCP, etc.
3	Red		IP, ICMP, RSVP, etc.
2	Enlace	IEEE 802	LLC, MAC, etc.
1	Físico		Coaxial, FO, radio, etc.

Tabla 4. Protocolos de red local en el modelo OSI

Los diferentes estándares, permiten que aparezcan nuevas versiones de ese mismo estándar simplemente modificando una de las capas. Esto facilita no sólo la evolución de los estándares, sino que un mismo equipo pueda ser compatible con distintas versiones de un estándar. Por ejemplo, IEEE 802.11b sólo se diferencia de IEEE 802.11 en que su capa física permite transmitir datos a alta velocidad.

IEEE 802.11 cumple con la arquitectura IEEE 802 establecida para redes LAN. La norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas del sistema OSI: La capa física, que se corresponde totalmente con la capa física del modelo OSI y la capa de enlace, que en el estándar 802.11 al igual que en todos los protocolos 802 se divide en dos subcapas. Por lo tanto el resultado queda de la siguiente manera:

- **PHY** (Physical Layer, 'Capa física')
- **MAC** (Medium Access Control, 'Control de acceso al medio')
- **LLC (**Logical Link Control, 'Control de enlace lógico')

El resto de capas son idénticas a las empleadas en las redes locales cableadas e Internet y se conoce con el nombre de conjuntos de protocolos IP (Internet Protocol).

2.2.3.1. La capa física

La capa física es la que se encarga de definir las características mecánicas, eléctricas y funcionales del canal de comunicación. Intercambia tramas entre PHY y MAC, utiliza portador de señal y modulación de espectro ensanchado para transmitir tramas a través del medio y proveer al MAC de un indicador de detección de portadora para señalizar actividad en el medio.

La capa física se ocupa de definir los métodos por los que se difunde la señal. Para hacer esto, la capa física de IEEE 802.11 se divide en dos subcapas conocidas como PLCP (Physical Layer Convergence Procedure, 'Procedimiento de convergencia de la capa física') la cual se encarga de convertir los datos a un formato compatible con el medio físico y PMD (Physical Medium Dependent, 'Dependiente del Medio físico') se encarga de la difusión de la señal.

2.2.3.1.1. Subcapa PMD

La subcapa PMD (Physical Medium Dependent) gestiona las características particulares del medio inalámbrico y define los métodos para transmitir y recibir datos en el medio.

La tecnología básica en la que se basa el funcionamiento de los sistemas inalámbricos es el sistema conocido como espectro expandido. Se trata de una técnica de modulación empleada en telecomunicaciones para la transmisión de datos digitales y por radiofrecuencia. Este sistema consiste en que el ancho de banda real utilizado en la transmisión es superior al estrictamente necesario. Lo que se consigue con esto es

un sistema muy resistente a las interferencias de otras fuentes de radio, lo que permite coexistir con otros sistemas de radiofrecuencia sin verse afectado.

IEEE 802.11 utiliza una de las siguientes técnicas de transmisión que posibilitan el envío de tramas MAC de una estación a otra, dependiendo de la velocidad a la que se vayan a transmitir los datos.

En la siguiente tabla se muestran las técnicas de difusión utilizadas por los diferentes estándares 802.11.

Estándar	Técnicas de difusión
802.11	IR, FHSS, DSSS
802.11ª	OFDM
802.11b	DSSS
802.11g	DSSS Y OFDM
802.11n	MIMO-OFDM

Tabla 5. Técnicas de difusión estándares 802.11

- **IR** (Infrarrojos) es un medio de transmisión que fue definido y utilizado en las primeras versiones del 802.11. La luz infrarroja es un tipo de radiación electromagnética invisible para el ojo humano. Los sistemas de comunicaciones con infrarrojo se basan en la emisión y recepción de haces de luz infrarroja. Dichos sistemas de comunicaciones pueden ser divididos en dos categorías:

  - **Infrarrojo de haz directo:** Esta comunicación necesita una visibilidad directa sin obstáculos entre ambos terminales.

  - **Infrarrojo de haz difuso:** En este caso el haz tiene suficiente potencia como para alcanzar el destino mediante múltiples reflexiones en los obstáculos intermedios. No se necesita visibilidad directa entre terminales.

  Su espectro está comprendido entre los 850 y 950 nm, con velocidades de 1 y 2 Mbps, usando modulación PMM.

  Las ventajas que ofrecen las comunicaciones de infrarrojo es que no están reguladas, son de bajo coste e inmunes a las interferencias de los sistemas de radio de alta frecuencia. Sus principales inconvenientes son su corto alcance (máximas típicas 9 centímetros a 1 metro), el hecho de que no puedan traspasar objetos y que no son utilizables en el exterior debido a que agentes naturales como la lluvia o la niebla les producen grandes interferencias. Por lo que su funcionalidad se ve reducida drásticamente, siendo inviables para usuarios móviles.

  No obstante, no cabe duda de que los sistemas infrarrojos son de los más eficaces sistemas de comunicaciones punto a punto para corta distancia.

- **FHHS** (Frequency Hopping Spread Spectrum, 'Espectro expandido por salto de frecuencia') consiste en dividir la banda de frecuencias en una serie de canales

e ir transmitiendo la información saltando de un canal a otro de acuerdo con un patrón de saltos (Hopping code). El orden en los saltos en frecuencia se determina según una secuencia pseudoaleatoria almacenada en unas tablas que tiene que ser conocido tanto por el emisor como por el receptor. El máximo tiempo que se debe permanecer en cada frecuencia es de 400 ms, es decir, pasado ese tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. Esta técnica utiliza la zona de los 2.4 GHz, organizada en 79 canales con un ancho de banda de 1 MHz cada uno.

La técnica FHHS sería equivalente a una multiplexación en frecuencia.

A continuación se muestra gráficamente como se transmite parte de la información en una determinada frecuencia durante un intervalo de tiempo (llamado dwell time)

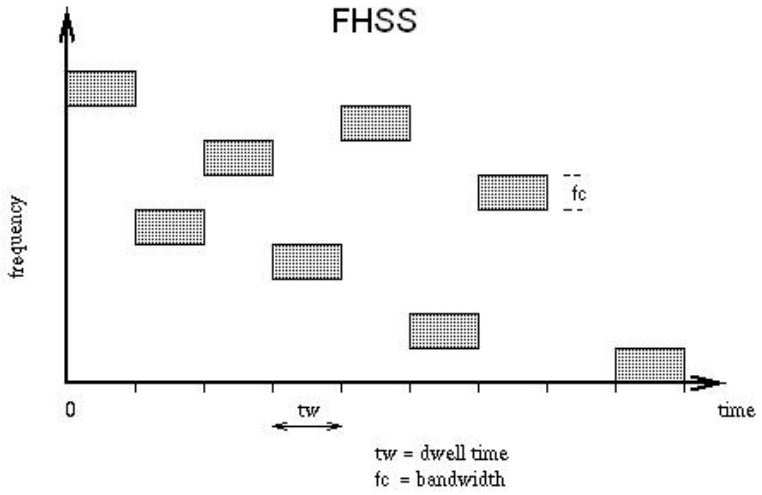


Ilustración 3. Transmisión de información durante un Dwell Time

- **DSSS** (Direct-Sequence Spread Spectrum, 'Espectro ensanchado por secuencia directa') es una técnica en la que se genera un patrón de bits redundante para cada uno de los bits que componen la señal. Se basa en sustituir cada bit de información por una secuencia de bits conocida como código de chips (chipping code). Estos códigos de chips permiten a los receptores eliminar por filtrado las señales que no utilizan la misma secuencia de bits, como el ruido y las interferencias.

  Cuanto mayor sea este patrón de bits, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100. Aunque parte de la señal de transmisión se vea afectada por las interferencias, en recepción es necesario realizar el proceso inverso para obtener la información original.

  La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barker. Dicha secuencia está diseñada para que aparezcan

aproximadamente el mismo número de 0 y de 1. Solo los receptores a los que el emisor haya enviado previamente la secuencia, pueden descifrar los datos y reconstruir la señal original.

Siendo la señal de datos *d(t)*, donde cada a_k puede tomar $M=2^k$ valores distintos que multiplican a un punto básico *g(t)* cada periodo de símbolo T (Régimen binario R_b =k/T)

$$d(t) = \sum_{-\infty}^{\infty} \mathrm{ak}\, g(t - KT)$$

La señal código *c (t)* que toma valores ±1 cada cierto periodo de chip $T_c = T / L_c$ *(L_c entero >>1)*

$$c(t) = \sum_{-\infty}^{\infty} cn\, p(t - nTc)$$

La señal *v(t)* se forma multiplicando la señal de datos con la señal código y después *se transmite* (previamente se hace una modulación de canal)

$$v(t) = d(t)c(t)$$

En recepción (quizás después de una demodulación de canal) se multiplica la señal recibida de nuevo por una réplica sincronizada de la señal código, obteniendo como resultado la señal original.

$$yr(t) = v(t)c(t) = d(t)c(t)c(t) = \boldsymbol{d(t)}$$

En las siguientes imágenes se muestra de forma gráfica la formación de la señal de espectro ensanchado y la recuperación de la señal de datos para un mejor entendimiento.

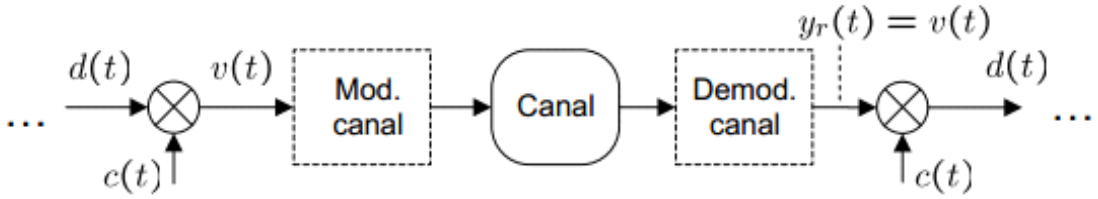


Ilustración 4. Formación de la señal de espectro ensanchado

Fuente. Temas Avanzados en Comunicaciones, Univ. Autónoma de Madrid

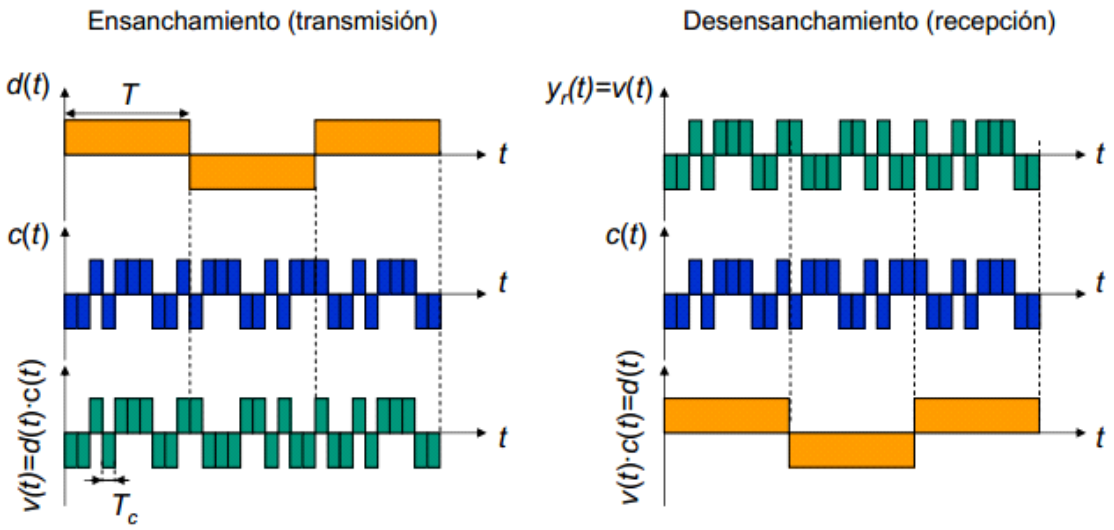


Ilustración 5. Recuperación de la señal de datos

Fuente. Temas Avanzados en Comunicaciones, Univ. Autónoma de Madrid

- **OFDM** (Orthogonal Frequency Division Multiplexing, 'Multiplexación por división de frecuencias ortogonales') es una combinación de dos o más canales de información en un solo medio de transmisión el cual envía un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información.

  Divide el ancho de banda en subcanales más pequeños que operan en paralelo consiguiendo velocidades de transmisión de hasta 54 Mbps. La técnica OFDM está basada en la FFT (Fast Fourier Transform, 'Transformada rápida de Fourier') y divide la frecuencia portadora en 52 subportadoras solapadas, 48 de estas subportadoras son utilizadas para transmitir datos y las otras cuatro para poder alinear las frecuencias en el receptor. Este sistema consigue un uso muy eficiente del espectro radioeléctrico.

  El principal concepto de las señales OFDM es la ortogonalidad de las portadoras, ya que nos permite la transmisión simultánea en un estrecho rango de frecuencias, reduciendo notablemente el ancho de banda y sin que se produzcan interferencias entre ellas.

  En el siguiente esquema se muestra el ahorro de ancho de banda que supone la técnica OFDM con respecto a una técnica multiportadora convencional.

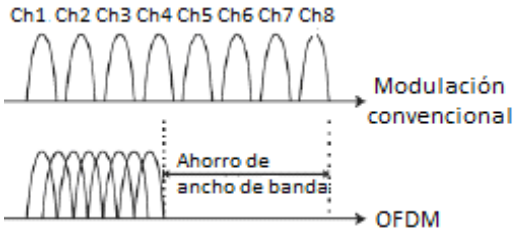


Ilustración 6. Ahorro de ancho de banda- Técnica OFDM

Fuente. Estudio sistema CDMA-OFDM, Capitulo 2.

OFDM puede transmitir datos a distintas velocidades, utilizando distintas técnicas de modulación en cada una de ellas. Las velocidades normalizadas que admite son 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. La siguiente tabla muestra de forma más precisa las modulaciones utilizadas en OFDM.

Tasa de transferencia de datos (Mbps)	Tipo de modulación
6	BPSK
9	BPSK
12	QPSK
18	QPSK
24	16-QAM
36	16-QAM
48	64-QAM
54	64-QAM

Tabla 6. Modulaciones OFDM

- **MIMO** (Multiple Input Multiple Output, 'Múltiple entrada múltiple salida') es una tecnología que usa múltiples antenas transmisoras y receptoras para mejorar el desempeño del sistema, permitiendo manejar más información que al utilizar una sola antena. Dicha tecnología se consigue gracias al desfase de la señal, de tal forma que los rebotes de la señal (reflexiones) en lugar de ser destructivos (como en algunas otras tecnologías) sean constructivos y nos proporcionen mayor velocidad. Esto se debe a que al haber menor pérdida de datos, se necesitan menos retransmisiones y por lo tanto proporciona velocidades mayores. En otras palabras, MIMO aprovecha fenómenos físicos como la propagación multitrayecto para incrementar la tasa de transmisión y reducir la tasa de error.

  Otra habilidad que provee MIMO es el Multiplexado de División Espacial (SDM). SDM multiplexa espacialmente flujos de datos independientes, transferidos simultáneamente con un canal espectral de ancho de banda. Gracias a la utilización de SDM se aumenta la eficiencia espectral de un sistema de comunicación inalámbrica.

Durante los últimos años, MIMO ha sido aclamada en las comunicaciones inalámbricas ya que aumenta significativamente la tasa de transferencia de información utilizando diferentes canales en la transmisión de datos o la multiplexación espacial por tener las antenas físicamente separadas.

El estándar 802.11n utiliza esta tecnología para lograr un rendimiento de aproximadamente unos 300 Mbps. Según las compañías que promueven esta tecnología, MIMO incrementa significativamente el área de cobertura y hasta más de seis veces la velocidad de las actuales redes IEEE 802.11g. Además, viene a ser la primera tecnología de comunicaciones inalámbricas que trata la propagación multidireccional como una característica inherente a los ambientes inalámbricos.

2.2.3.1.2. Subcapa PLPC

La subcapa de convergencia de la capa física, PLCP, se encarga de convertir los datos a un formato compatible con el medio físico. Es la subcapa superior de la capa física y tiene como misión básica la aplicación de un procedimiento de convergencia que permite convertir MPDUs en PPDUs y viceversa. Durante la transmisión, a la MPDU se le adicionará un preámbulo y una cabecera para crear la PPDU. En el receptor, se procesarán el preámbulo y la cabecera y se despachará la MPDU. En la Ilustración 7 se muestra la composición de un segmento PLCP.

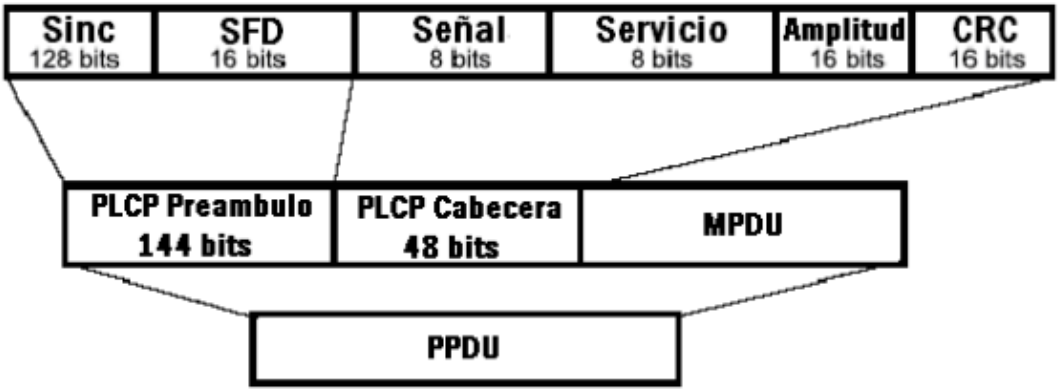


Ilustración 7. Trama PLCP

Fuente. López Ortiz, F. Wireless LAN

Como se puede observar en la figura, la trama PLCP consta de tres campos:

- **Preámbulo**: Se utiliza por el receptor para adquirir la señal entrante y sincronizar con el demodulador. Indica el inicio de una trama. contiene los campos de Sincronización (SINC) y Delimitador del Inicio de Trama (SFD).

- **Cabecera PLCP**: Contiene información acerca del paquete MAC transmitido, tal como la duración o la velocidad de transmisión utilizada. Contiene los campos de *Señalización* IEEE 802.11 (SEÑAL), que indicará la modulación que será usada

para transmisión y recepción, *Servicio* IEEE 802.11 (SERVICIO), *Longitud* (AMPLITUD) que indica el número de microsegundos requeridos para transmitir la MPDU, y *CRC* que protege a los campos SEÑAL, SERVICIO y AMPLITUD.

- **Payload**: PDU-PLCP son los datos o la trama entregada por la MAC.

El conjunto de estos tres campos dan el formato general de una trama PLCP y conforman lo que se llama PHY Protocol Data Unit (PPDU).

2.2.3.2. La capa de enlace

Respetando el modelo OSI, son dos, los niveles que conforman la capa de enlace (MAC: Medium Access Control, 'Control de Acceso al Medio' y LLC: Logical Link Control, 'Control del enlace lógico'). Desde el punto de vista de 802.11, solo interesa hacer referencia al subnivel MAC.

La capa MAC define los procedimientos que hacen posible que los distintos dispositivos compartan el uso del espectro radioeléctrico. Mientras que las distintas versiones del estándar 802.11 utilizan distintos sistemas para difundir su señal (la capa física es distinta), la capa MAC es la misma para todas ellas.

Las funciones principales de la capa MAC son las siguientes:

- **Exploración**: Es el proceso por el cual una determinada estación logra identificar la existencia de una determinada red. En dicho proceso se envían señales que identifican la estación, estás incluyen los SSID (Service Set Identifiers), y los ESSID (Extended SSID) con una longitud máxima de 32 caracteres.

- **Autenticación**: Establece la identidad de las estaciones y autoriza la asociación. En el caso inalámbrico, la posibilidad de un acceso más libre origina el uso en el estándar 802.11 de dos formas de autenticación: Autenticación de sistema abierto y Autenticación de Clave compartida.

  - **Autenticación de Sistema Abierto**: Esta es la única autenticación obligatoria en 802.11. Se suele asociar con el filtrado MAC. El cliente envía una solicitud de autenticación con su SSID a un AP (Access Point, 'Punto de Acceso'), el cual autorizará o no. Se envía una primera trama por parte de la estación que requiere el acceso, donde se especifica el identificador del algoritmo de autenticación, y el número de secuencia de transacción de la autenticación.

    La identificación de una estación en 802.11 se hace por medio de la transmisión de la dirección MAC de esa estación. La respuesta al requerimiento de autenticación la realiza el AP y lo hace enviando en una trama el identificador del algoritmo de autenticación, el número de

secuencia de transacción de autenticación y el código de estado indicando el resultado del requerimiento.

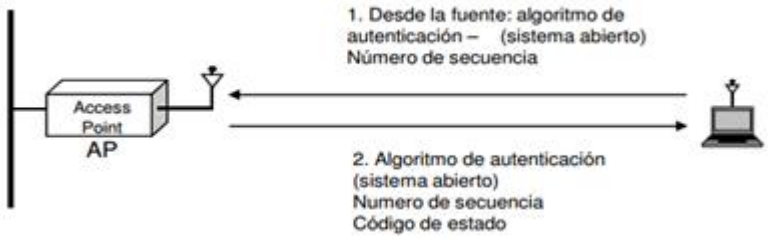


Ilustración 8. Autenticación Sistema Abierto

- **Autenticación de Clave compartida:** Requiere que ambas partes del proceso tengan implementado el algoritmo WEP. (Proceso hoy totalmente desacreditado). El proceso inicia exactamente igual que en el caso anterior y a continuación la estación envía el identificador de algoritmo de autenticación, el número de secuencia de transacción de autenticación, y un texto de 128 bytes denominado texto de desafío (interrogatorio del AP al cliente) . El AP recibe la información, la desencripta y controla la integridad del mismo. Si tuvo éxito envía un código de estado de aceptación.

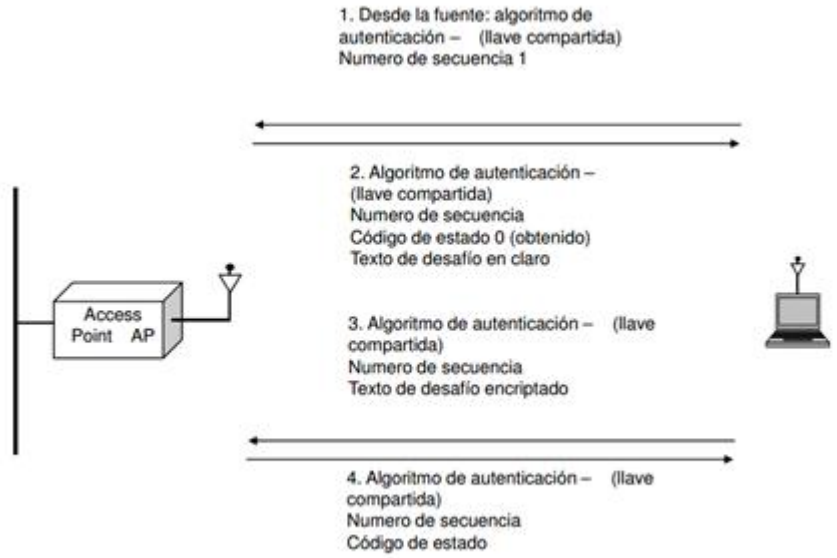


Ilustración 9. Autenticación Clave Compartida

- **Asociación:** Este proceso es el que dará acceso a la red y solo puede ser llevado a cabo una vez realizada la autenticación.

- **Seguridad:** Mediante WEP, con este protocolo se cifran solo los datos, no los encabezados. Hoy en día se prefieren protocolos como WPA y WPA2, que se

especificaran más adelante.

- **Señales de control RTS/CTS:** Intercambio de señales que permiten la administración del canal, definen el tamaño de trama (En 802.11 entre 256 y 2312 bytes)

- **Gestión de potencia:** El ahorro de potencia es una necesidad importante en comunicaciones, debido a la cantidad de potencia necesaria para transmitir y el consiguiente consumo de baterías. Los APs conocen que la estación está en modo de ahorro de energía y colocan en su buffer las tramas de dichas estaciones.

- **Fragmentación:** Es la capacidad que tiene un AP de dividir la información en tramas más pequeñas y así garantizar su recepción.

- Sincronización, direccionamiento, comprobación de errores y los servicios de gestión para permitir Roaming dentro de un ESS son otras de las funciones principales del nivel MAC.

Un aspecto interesante es el hecho de que la capa MAC sea muy similar a la utilizada por la red Ethernet. Ambas utilizan la técnica conocida como CSMA (Carrier Sense Multiple Access, 'Acceso múltiple por detección de portadora'). No obstante, la versión cableada (Ethernet) utiliza la tecnología CD (Collision Detection, 'Detección de Colisión'), mientras que la versión inalámbrica utiliza la tecnología CA (Collision Avoidance, 'Evitación de la Colisión'). Una colisión se produce cuando dos terminales intentan hacer uso del medio físico simultáneamente. La tecnología CD detecta que se ha producido una colisión y retransmite los datos, mientras que la tecnología CA dispone de procedimientos para evitar que se produzcan colisiones.

En el medio radioeléctrico un terminal no puede transmitir y recibir al mismo tiempo por el mismo canal (la transmisión dejaría opaca a la recepción), por lo que, al no poder detectar las posibles colisiones, se dispone de una técnica que las evite.

Entre la capa MAC y la capa física se intercambian tres tipos de paquetes de datos: de control, de gestión y de información. Para coordinar la transferencia de datos, la arquitectura MAC del estándar 802.11 se compone de dos funciones de coordinación que determinan, dentro de un conjunto básico de servicios (BSS), cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico. Dichas funciones son:

- **DCF** (Distributed Coordination Function, 'Función de coordinación distribuida') se encuentra en el nivel inferior del subnivel MAC. Su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio. El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles ni tolerados por los servicios síncronos. En DCF todas las estaciones compiten por

el acceso al canal simultáneamente y para ello facilita un sistema que permite compartir el medio físico entre todas las estaciones de la red. CSMA/CA y MACA (CSMA/CA con RTS/CTS), son mecanismos que le permiten a las estaciones negociar el acceso al medio físico, así como asegurar la entrega de los datos a las estaciones.

El algoritmo CSMA/CA consiste en testear el medio, o canal inalámbrico antes de transmitir para determinar su estado (libre u ocupado). La función DCF contempla un mecanismo físico conocido como CCA (Clear Channel Assessment, 'Valoración de la disponibilidad del canal' que comprueba si el medio esta en uso antes de transmitir: Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos. De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto llamado espaciado entre tramas (IFS) y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión. Este mecanismo es muy eficiente, pero no es eficaz cuando dos estaciones de una misma red que no se ven entre ellas emiten al mismo tiempo. Esto se conoce con el nombre del problema del nodo oculto. Para evitar estos casos, se dispone del sistema lógico de detección de colisión que consiste en intercambiar la información del uso del medio a través de tramas de control.

Para enviar una trama, el equipo origen primero envía una trama corta de control de solicitud de transmisión RTS (Request To Send, 'Solicitud para enviar'). Este mensaje de control RTS contiene las direcciones de MAC del equipo origen y destino. Si el equipo destino recibe esta trama significa que está preparado para recibir una trama. Este equipo devolverá una trama de contestación: preparado para transmitir CTS (Clear To Send, 'Listo para enviar') o receptor ocupado (RxBUSY). Si la respuesta es afirmativa el equipo origen transmite la trama en espera (DATA). Si el equipo destino recibe correctamente el mensaje contesta con la trama de confirmación positiva ACK (Acknowledgment, 'Confirmación') y si no la recibe correctamente contesta con la trama de confirmación negativa NAK (Naknowledged) y el equipo origen tratará de volver a enviarlo. Este procedimiento se repite un número predefinido de veces hasta conseguirse una transmisión correcta de la trama DATA.

- **PCF** (Point Coordination Function, 'Función de coordinación del punto') situada por encima de la funcionalidad DCF. Asociada a las transmisiones libres de contienda que utilizan técnicas de acceso deterministas para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio. A la estación que hace uso de esta función se le llama coordinadora del punto, PC (Point Coordinator) y generalmente se trata de un AP. El PC emite una señal guía con

la duración del periodo de tiempo que necesita disponer del medio. Las estaciones que reciben esta señal no emiten durante ese tiempo.

PCF es totalmente compatible con DCF, pueden operar conjuntamente dentro de una misma celda o un conjunto básico de servicios dentro de una estructura llamada supertrama. Una parte de esta supertrama se asigna al periodo de contienda permitiendo al subconjunto de estaciones que lo requieran transmitir bajo mecanismos aleatorios. Una vez finaliza este periodo el punto de acceso toma el medio y se inicia un periodo libre de contienda en el que pueden transmitir el resto de estaciones de la celda que utilizan técnicas deterministas.

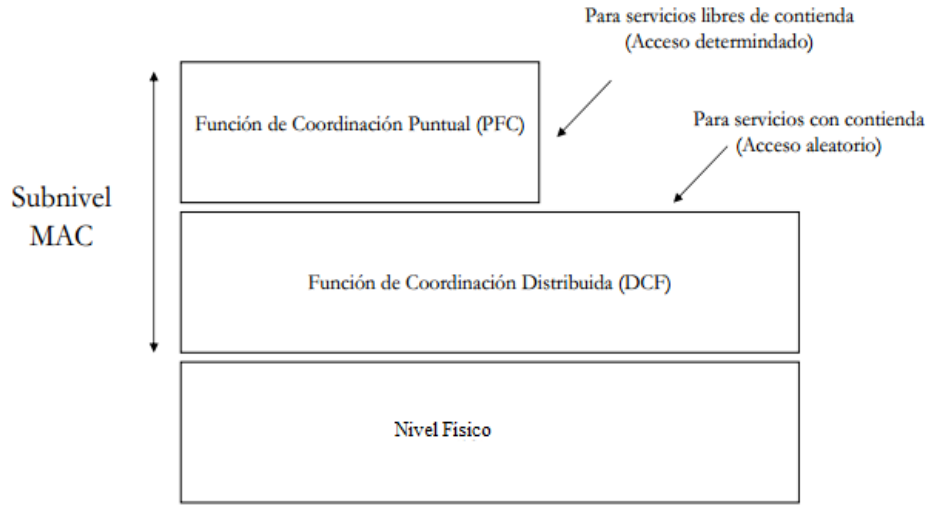


Ilustración 10. Funciones de coordinación MAC

Fuente. Oliver, M. / Escudero, A. Redes de área local inalámbricas según estándar 802.11

Las tramas MAC contienen tres componentes básicos: Una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia; Un cuerpo de trama de longitud variable, que contiene información específica de la trama; Y una secuencia Checksum (FCS) que contiene un código de redundancia CRC de 32 bits para el chequeo de errores.

El estándar 802.11 puede clasificar las tramas MAC según tres tipos: Las tramas de datos, las tramas de control que sirven para el intercambio y reconocimiento de datos como los ACKs, RTS, CTS y las tramas libres de contienda, y por último las tramas de gestión utilizadas para los diferentes servicios de distribución como el servicio de asociación, para sincronismo y tareas de autenticación.

A continuación se muestra una trama MAC genérica de datos con sus nueve campos, donde los siete primeros forman parte del encabezado de la trama MAC, y los dos siguientes se corresponden con el cuerpo de trama y el checksum.

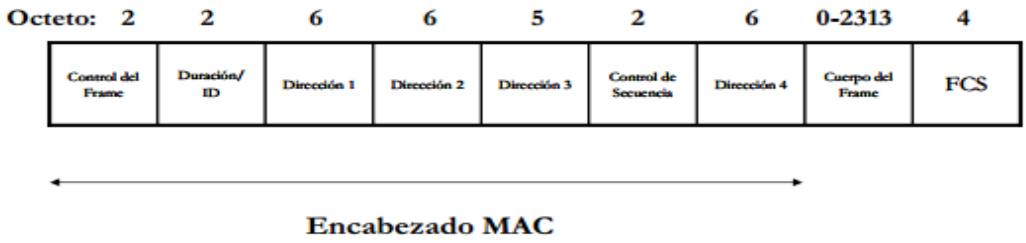


Ilustración 11. Trama MAC

Los campos que definen esta trama son:

- El campo de control de trama definido a través del siguiente formato.

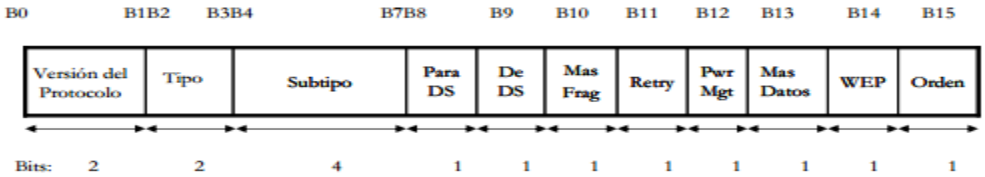


Ilustración 12. Campo de control de trama MAC

Como se puede comprobar, dicho campo de control está compuesto por once subcampos: La *versión del protocolo*, que permite que los dispositivos conozcan la versión; la parte de *tipo* que identifica si la trama es de datos, de control o de gestión; El subcampo *subtipo*, identifica cada uno de los tipos de tramas de cada uno de esos tipos, es decir, si la trama es de control indicará si se trata de un CTS, RTS, etc; *Para DS* indica si la trama se envía al sistema de distribución DS*; De DS* que identifica si la trama viene o se recibe del sistema de distribución DS; *Más fragmentos* se activa si se usa fragmentación; *Retry* se activa si se realiza una retransmisión de una trama que se envió anteriormente; *Power Management* es utilizado por la estación base cuando se quiere activar el modo de economía de potencia; *Más Datos* se activa cuando la estación tiene tramas pendientes para transmitir en un punto de acceso; *WEP* se utiliza si se usa el mecanismo de autenticación y encriptación; *Orden* indica que una secuencia de tramas debe procesarse con el servicio de ordenamiento estricto.

- **Duration/ID** indica la duración del periodo que se ha reservado una estación para la transmisión de una trama y su confirmación de recepción.

- **Campos Dirección 1-4** contiene direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.

- **Campo de control de secuencia** contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.

- **Cuerpo de la trama,** varía según el tipo de trama que se quiere enviar.

- **FCS** contiene el checksum, que es una función que tiene como propósito principal detectar cambios accidentales en una secuencia de datos para proteger la integridad de estos, verificando que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra final tras la transmisión.

2.2.4 Elementos básicos de una red

A la hora de diseñar una red es importante conocer los elementos básicos que la componen, es cierto, que no existe un diseño de red modelo, si no que cada red está formada por un equipamiento y una topología diferente. Sin embargo, en las redes inalámbricas existen una serie de elementos básicos que son indispensables.

El **punto de acceso** (Access Point, 'AP') Es el centro de las comunicaciones de la mayoría de las redes inalámbricas. Por medio de ondas de radio frecuencia (RF) recibe información de diferentes dispositivos y la transmite a través del cable al servidor de la red cableada o viceversa. El punto de acceso no sólo es el medio de intercomunicación de todos los terminales inalámbricos, sino que también es el puente de interconexión con la red fija e Internet. Desde este punto de vista, es importante tener en cuenta aspectos como:

- Comprobar las características del router del punto de acceso. DHCP, NAT o propiedades firewall son facilidades que ayudan en la configuración y manejo de las comunicaciones con Internet o con otras redes.

- Conviene comprobar que el AP que se va a comprar sea compatible con el protocolo de red cableada con el que se va a conectar.

- Los puntos de acceso WiFi funcionan sin problema con los adaptadores de red de cualquier fabricante. No obstante, existe cierta incompatibilidad cuando se desea crear una red con varios puntos de acceso de distintos fabricantes. El estándar 802.11 es bastante ambiguo y no define con claridad todas las funciones que debería realizar un Punto de Acceso. Esto dio lugar a que cada fabricante los diseñara según su criterio y, por lo tanto existen en el mercado decenas de Puntos de Acceso con características y funcionalidades muy dispares.

  La falta de entendimiento aparece a la hora de mantener en servicio una comunicación cuando un usuario pasa del área de cobertura de un punto de acceso a otro (a esto se le llama itinerancia o roaming). Es recomendable que los puntos de acceso vecinos sean del mismo fabricante para evitar cortes de comunicación al pasar de un AP a otro.

En cualquier caso, un Punto de Acceso está compuesto por un equipo radio, antenas exteriores o interiores, un software de gestión de comunicaciones y puertos para conectar el punto de acceso a Internet o a la red cableada.

Los **adaptadores inalámbricos** de red son fundamentalmente unas estaciones de radio que se encargan de comunicarse con otros adaptadores (modo ad hoc) o con un punto de acceso (modo infraestructura) para mantener a los dispositivos que están conectados dentro de la red inalámbrica a la que se asocie.

Estos equipos pueden recibir el nombre de tarjetas de red, interfaces de red o NIC (Network Interface Cards) y cumplen con el estándar 802.11 que permite a un equipo conectarse a una red inalámbrica. Hay diversos tipos de adaptadores en función del tipo de cableado o arquitectura que se utilice en la red.

En la actualidad, la mayoría de los dispositivos y ordenadores tienen integrado el adaptador de red inalámbrico. Es importante que el adaptador WiFi sea compatible con el router. La elección de un adaptador u otro dependerá de nuestras necesidades y de las características de nuestro equipo.

También existen **amplificadores y antenas** que se pueden agregar, según las necesidades, a instalaciones WiFi y sirven para direccionar y mejorar las señales de RF (Radio Frecuencia) transmitidas.

2.2.5 Configuraciones de red

Las redes inalámbricas WiFi admiten dos tipos de configuraciones desde el punto de vista del tipo de equipamiento:

- **Modo Ad hoc**. Se trata de una configuración en la cual sólo se necesita disponer de tarjetas o dispositivos inalámbricos WiFi en cualquier equipo susceptible de ser conectado a la red. La red es *ad hoc* porque no depende de una infraestructura pre-existente, como routers (en redes cableadas) o de puntos de accesos en redes inalámbricas administradas. En lugar de ello, cada nodo participa en el encaminamiento mediante el reenvío de datos hacia otros nodos, de modo que la determinación de estos nodos hacia la información se hace dinámicamente sobre la base de conectividad de la red.

  Este tipo de red permite la adhesión de nuevos dispositivos, con el solo hecho de estar en el rango de alcance de un nodo ya perteneciente a la red establecida. El principal inconveniente de este tipo de redes radica en el número de saltos que debe recorrer la información antes de llegar a su destino. Cada nodo que retransmite la información implica un salto, cuantos más saltos, mayor es el tiempo que tarda en llegar la información a su destino y aumenta la probabilidad de que la información se corrompa con cada salto.

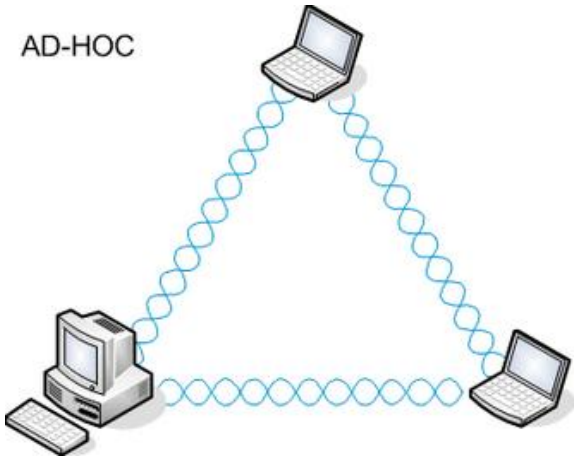


Ilustración 13. Modo AD-HOC

- **Modo infraestructura.** En esta configuración, además de las tarjetas WiFi se necesita disponer de un equipo conocido como Punto de Acceso (AP). Cada estación informática (EST) se conecta a un punto de acceso a través de un enlace inalámbrico. La configuración formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico o BSS. Estos forman una célula. Cada BSS se identifica a través de un BSSID que en modo infraestructura corresponde al punto de acceso de la dirección MAC.

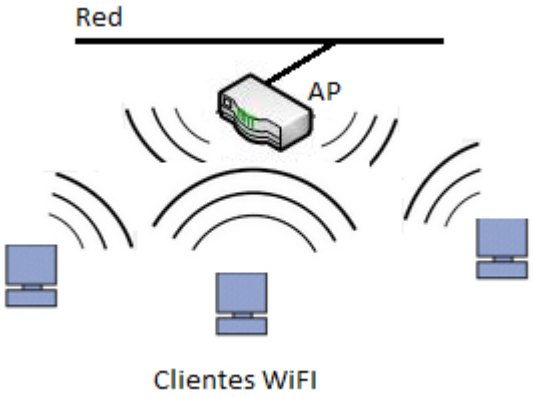


Ilustración 14. Modo infraestructura

Es posible vincular varios puntos de acceso juntos (o con más exactitud, varios BSS) con una conexión llamada sistema de distribución (SD) para formar un conjunto de servicio extendido o ESS.

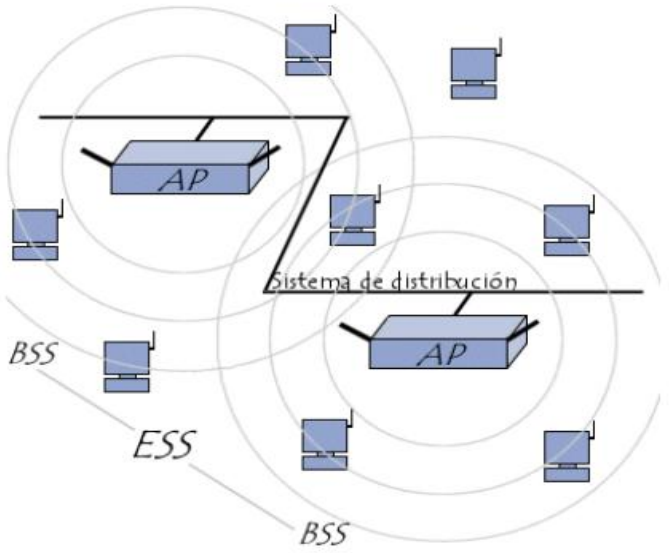


Ilustración 15. Modo infraestructura- Varios APs

Un ESS se identifica a través de un ESSID (identificador del conjunto de servicio extendido), a menudo abreviado como SSID, que muestra el nombre de la red y de alguna manera representa una medida de seguridad de primer nivel ya que una estación debe saber el SSID para conectarse a la red extendida.

Las comunicaciones *ad hoc* son muy fáciles de configurar y resultan muy interesantes cuando se necesita establecer una comunicación temporal entre dos equipos. Por otro lado, el modo infraestructura es el más adecuado para crear redes permanentes. Las razones que nos llevan a esta conclusión son varias:

- El modo infraestructura ofrece un mayor alcance que la modalidad *ad hoc*. Los terminales no tienen por qué estar dentro del área de cobertura el uno del otro; al tener un punto de acceso intermedio pueden, al menos, duplicar su distancia.

- El punto de acceso permite compartir el acceso a Internet entre todos sus terminales. Esto permite compartir un acceso de banda ancha (ADSL o cable) entre todos los terminales que forman la red, sean dos o cientos de ellos.

- El punto de acceso permite crear redes con un mayor número de terminales.

- El punto de acceso ofrece características de gestión de la comunicación que no ofrece el modo *ad hoc.*

- El punto de acceso, al igual que cualquier red local, permite compartir los recursos de los terminales que forman la red (archivos, impresoras, etc.

2.2.6 Seguridad en redes de telecomunicaciones

La seguridad es un aspecto crítico a tener en cuenta a la hora de diseñar cualquier infraestructura de comunicaciones basada en tecnologías de la información.

Esto es debido, por una parte, a que se requieren importantes inversiones y desarrollos para la implantación de la tecnología, por lo que es necesario evitar su uso no autorizado por parte de elementos externos que puedan degradar la calidad del servicio ofrecido por las mismas.

Por otro lado, en la mayoría de los casos se hace necesario que la comunicación se realice de manera fiable y confidencial, ya que la inspección o modificación de la información transmitida por parte de terceras personas no autorizadas puede comprometer de manera muy importante la seguridad de las personas u organizaciones que hacen uso de las tecnologías de información implantadas.

En las redes inalámbricas, la utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado importantes riesgos de seguridad. Dichas redes carecen de barreras físicas lo que supone que cualquier persona con unos conocimientos sobre seguridad puedan acceder desde fuera de los límites físicos de una organización, haciéndolas susceptibles a múltiples tipos de ataques.

Para que un sistema de seguridad en las redes de comunicaciones, y más específicamente en los entornos de red inalámbricos, sea completo y eficiente debe ser capaz de proveer cinco premisas básicas de seguridad.

- **Confidencialidad:** Consiste en garantizar la privacidad de la información y asegurar que la información no pueda ser divulgada a personas, procesos o dispositivos no autorizados (protección contra divulgación no autorizada).

- **Integridad:** Consiste en las medidas de seguridad diseñadas para garantizar que la información transmitida al usuario final no pueda ser alterada en su forma ni en su contenido en su camino desde el emisor hasta el receptor.

- **Autenticación:** Consiste en las medidas de seguridad diseñadas para establecer la validez de una transmisión, mensaje o remitente, o un medio para verificar la autorización de un individuo para recibir categorías específicas de información (verificación de emisor).

- **Disponibilidad:** Consiste en garantizar el acceso oportuno y confiable a datos y servicios de información para usuarios autorizados. Se trata de la resistencia del sistema de ataques y su capacidad de recuperarse rápida y completamente

después de estos. Estas medidas están desarrolladas en la política de seguridad de la compañía, especificando procedimientos y responsables de las mismas.

- **No repudio:** Consiste en asegurar que el remitente de información es provisto de una prueba de envío y que el receptor es provisto de una prueba de la identidad del remitente, de manera que ninguna de las partes puede negar el proceso de dicha información.

Para enfrentar los problemas de seguridad en redes inalámbricas existen métodos de protección, el objetivo fundamental de éstos consiste en utilizar tanto estándares como protocolos de seguridad que complementado por herramientas adicionales referentes al funcionamiento de las WLANs refuerzan la protección y la seguridad frente a los hackers.

El primer paso para asegurar una red WiFi es conocer cuáles son las amenazas y ataques que puede sufrir. Existen diferentes métodos para interceptar, atacar y descubrir una red inalámbrica. Estas amenazas pueden ser divididas en dos grandes grupos: Ataques Pasivos y Ataques Activos.

2.2.6.1. Ataques pasivos

El principal objetivo del atacante es obtener información. Se trata de un método en el que no se altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener la información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico.

- **Espionaje (Surveillance)**: El espionaje es la técnica más simple a la que se puede someter una red inalámbrica. Consiste en observar el entorno para recopilar información relacionada con la topología de red. Esta información se puede emplear en posteriores ataques. No es necesario ningún tipo de hardware o software especial, sólo tener acceso a la instalación.

Mediante el espionaje, un atacante puede encontrar mucha información para utilizar a su favor. Información sensible en este caso sería la localización de antenas, puntos de acceso, etc…

-**Escuchas (Sniffing)**: Las escuchas son un ataque pasivo que tienen como objetivo final monitorizar la red para capturar información sensible como, por ejemplo, la dirección MAC o IP origen y destino, identificadores de usuario, contraseñas, clave WEP, etc..

Las escuchas se consideran un paso previo a los ataques posteriores que suponen una importante fisura en cuanto a seguridad.

Para que un dispositivo tenga la capacidad de llevar a cabo escuchas en una red WiFi, debe tener instalada o integrada una tarjeta WLAN que actúa en ‘modo monitor’ o en ‘modo promiscuo’. Estos modos de operación permiten recibir todo el tráfico que

circula por la red. Adicionalmente es necesario un software especial que monitorice toda la información que viaja a través de la red.

-Wardriving: Es un caso particular del ataque anterior donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos de acceso inalámbricos.

-**Warchalking**: Es un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que cualquier transeúnte con un dispositivo con conectividad WiFi pueda hacer uso de la red gracias a la información ofrecida por los símbolos.

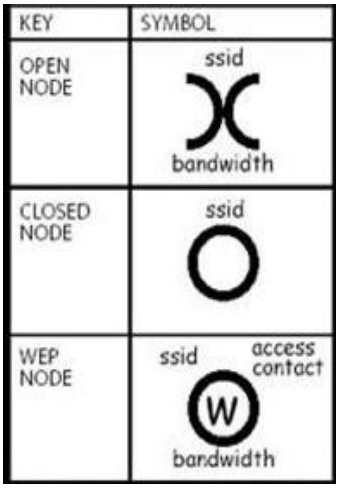


Ilustración 16. Símbolos utilizados para el Warchalking

Fuente. Andreu/Pellejero/Lesta Fundamentos y aplicaciones de seguridad en redes WLAN

-Ataques de descubrimiento de contraseña: Este tipo de ataques tratan de descubrir la contraseña que un usuario utiliza para acceder al sistema o descubrir claves de cifrado de la información, generalmente, tras llevar a cabo una escucha y recopilación del tráfico cifrado durante cierto tiempo. Para elegir las posibles contraseñas se utilizan principalmente dos métodos:

- Ataques de fuerza bruta
- Ataques de diccionario

Estos tipos de ataque son la base para el descubrimiento de claves WEP (Wired Equivalen Privacy, 'Protocolo de equivalencia con red cableada') de una red WiFi.

- **Ataques de fuerza bruta**: Los ataques por fuerza bruta son aquellos que intentan romper un cifrado mediante la prueba de todas las combinaciones posibles. Normalmente un cifrado se considera seguro si sólo es capaz de ser descifrado por medio de ataques de fuerza bruta. Mediante estos ataques, se puede descifrar tanto las claves de los algoritmos de cifrado como el nombre de usuario y la contraseña de autenticación del usuario.

Este método, por definición, siempre consigue su meta, si bien el problema que tiene es de recursos y tiempo. Si una contraseña es suficientemente larga, el número de combinaciones posibles se dispara exponencialmente.

- **Ataques de diccionario**: Son muy similares a los de fuerza bruta. La única diferencia es que para descubrir una clave de cifrado o conseguir una contraseña se utilizan una serie de palabras probables, generalmente tomadas de un glosario de palabras y nombres, en lugar de todas las combinaciones posibles. Si la clave utilizada está en el diccionario se consigue reducir sustancialmente el tiempo necesario para encontrarla.

-**Descubrimiento de ESSID ocultos:** En general en una red WiFi el proceso de conexión de un usuario consiste en la autenticación y asociación del mismo a un punto de acceso. Para ello, es necesario que el usuario conozca previamente la existencia de una red LAN.

El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. Dependiendo de si la red inalámbrica funciona en modo ad-hoc o en modo Infraestructura, el SSID se denomina BSSID (Basic Service Set Identifier) o ESSID (Extended Service Set IDentifier). El BSSID suele ser la dirección MAC del equipo. El ESSID es el parámetro clave para llevar a cabo el descubrimiento de una red WiFi por parte de un usuario. Existen dos procesos mediante los cuales el usuario puede identificar la existencia de una o varias redes:

- **Escaneo Pasivo**: El dispositivo de usuario espera recibir la señal del punto de acceso. Los usuarios escuchan los Beacon Frames que emiten los puntos de acceso y lo identifican pudiendo en ese momento iniciarse el proceso de asociación y autenticación.

- **Escaneo Activo**: La estación lanza tramas a un punto de acceso determinado y espera una respuesta. El usuario puede enviar una trama Prove Request con un determinado ESSID para ver si algún punto de acceso inalámbrico responde.

2.2.6.2. Ataques activos

Los ataques activos suponen una modificación en el flujo de datos o la creación de falsos flujos en la transmisión de datos. Pueden tener dos objetivos diferentes: pretender ser alguien que en realidad no es para obtener información o colapsar los servicios que puede prestar la red.

-Puntos de acceso no autorizados/Rogue APs: Son aquellos puntos de acceso que se conectan sin autorización a una red existente. Estos puntos de acceso no son gestionados por los administradores de la red y es posible que no se ajuste a las políticas de seguridad de la red. De esta forma se abre una puerta a todo tipo de

ataques indeseados, puesto que permite a cualquiera con un terminal WiFi conectarse a la red, y vulnera todos los mecanismos que se basan en el cifrado de información entre extremos (WEP, WEP2, WPA, etc…)

-Spoofing: Un ataque de Spoofing consiste en el uso de técnicas de suplantación de validadores, credenciales o identificadores estáticos. Los identificadores que se pueden suplantar mediante un ataque de Spoofing son los mostrados en la *Figura 17*.

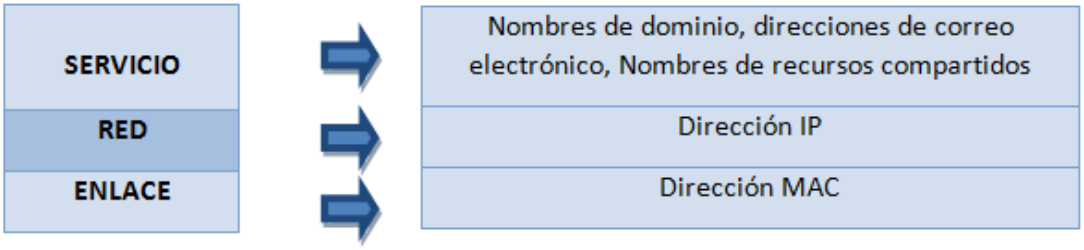


Ilustración 17. Identificadores de ataque de Spoofing

-Man In The Middle: Es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

-Secuestro de sesiones/ Hijacking: Consiste en tomar una conexión existente entre dos dispositivos de usuario. Tras monitorizar la red el atacante puede generar tráfico que parezca venir de una de las partes envueltas en la comunicación, robando la sesión de los individuos envueltos.

-Denegación de servicio: La denegación de servicio no tiene como objetivo escuchar los paquetes ni acceder a la red, sino simplemente inutilizarla para que otros usuarios no puedan acceder a ella.

La denegación de servicio se produce cuando un atacante intenta ocupar la mayoría de los recursos disponibles de una red inalámbrica, impidiendo a los usuarios legítimos de esta, disponer de dichos servicios o recursos. Para ello, se suelen modificar parámetros estándar que permitan enviar mensajes sin ni siquiera esperar los intervalos de guarda necesarios. No importa que no se procesen en el destino, el ataque consiste en bombardear la red y hacerla inaccesible.

Las formas de ataque DoS más comunes son los siguientes:

- **Radio jamming:** Interferir el espectro con una señal de alta potencia inhabilitando que el usuario legítimo acceda al servicio.
- **Wireless DoS:** Es inherente al protocolo IEEE 802.11. Como las tramas de gestión no están protegidas por privacidad, autenticación e integridad, cualquier atacante puede realizar un ataque Wireless DoS sin más que mandando tramas de disociación a cualquier usuario de la red WiFi.

Seguridad de las redes WiFi

La seguridad de cualquier red, incluidas las redes WiFi, puede ser comprometida en dos aspectos: autenticación y cifrado. Los mecanismos de autenticación se emplean para identificar un usuario inalámbrico ante un punto de acceso y viceversa, mientras que los mecanismos de cifrado aseguran que no sea posible decodificar el tráfico de usuario.

Los protocolos de seguridad para redes Wifi, deben, por lo tanto, proteger estos dos puntos vulnerables ante posibles ataques. Con ese objetivo, desde la aparición de dichas redes los protocolos del nivel de enlace desarrollados específicamente para dotarlas de seguridad han sido WEP, WPA, WPA2.

La evolución de la seguridad en el estándar IEEE 802.11 y la WiFi Alliance, se muestra en la *Tabla 7*.

Fecha	Hitos
Septiembre 1997	Estándar IEEE 802.11 ratificado, incluyendo WEP.
Abril 2000	Lanzamiento del programa de certificación (WiFi CERTIFIED), con soporte para WEP.
Mayo 2001	Se crea el grupo de trabajo IEEE 802.11i
Abril 2003	Se introduce WPA con: • Autenticación IEEE 802.11X • Encriptación *Temporal Key Integrity Protocol* (TKIP) • Compatible con *EAP-Transport Layer Security* (EAP-TLS)
Septiembre 2003	Obligatorio WPA para todos los equipos WiFi CERTIFIED
Junio 2004	Rectificación IEEE 802.11i ratificada
Septiembre 2004	Se introduce WPA2 con: • Autenticación IEEE 802.11X • Encriptación AES • Compatible con EAP-TLS
Abril 2005	Apoyo a cuatro tipos EAP adicionales: • *EAP Tunneled TLS Microsoft Challenge Handshake Authentication Protocol Version 2* (EAP-TTLS/MSCHAPv2) • *Protected EAP Version 0* (PEAPv0)/EAP-MSCHAPv2 • *Protected EAP Version 1* (PEAPv1)/EAP *Generic Token Card* (EAP-GTC) • *EAP-Subscriber Identity Module* (EAP-SIM)
Marzo 2006	Obligatorio WPA2 para todos los equipos WiFi CERTIFIED
Enero 2007	Lanzamiento *WiFi Protected Setup (*WP S*)*
Noviembre 2007	Se crea el grupo de trabajo IEEE 802.11w
Mayo 2009	Apoyo para EAP-AKA y EAP-FAST añadido

Tabla 7. Evolución de la seguridad en el IEEE 802.11 y la WiFi Alliance

Por otro lado, otros mecanismos de seguridad del nivel de enlace utilizables en este tipo de redes son PPTP y P2TP. No obstante, estos mecanismos de seguridad no son específicos de redes WiFi, sino que son aplicables también en otro tipo de redes. Estas tecnologías tienen la capacidad de crear una Red Privada Virtual o VPN.

Una Red Privada Virtual (VPN) es una tecnología de red que permite una extensión segura de la red LAN sobre una red pública o no controlada como Internet. Con este propósito se emplea una técnica llamada entunelamiento (tunneling): los paquetes de datos son enrutados por la red pública, Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura.

Desde el punto de vista del modelo OSI, se puede crear una VPN usando tecnologías de la capa 2 (enlace de datos) y de capa 3 (red). Dentro de la primera categoría están PPTP y L2TP, y en la segunda IPsec que se verá en el siguiente apartado.

Es importante tener en cuenta que un ataque que ha sido realizado a nivel de enlace con éxito tiene control sobre todas las capas superiores. Por lo que hay que tener especial atención en la seguridad de estas capas.

Los fundamentos de funcionamiento de todos los mecanismos anteriores se describen a continuación.

-PPTP: El protocolo PPTP (Point to Point Tunnelling Protocol) es una extensión de PPP (Point to Point protocol) que fue desarrollado por Microsoft como protocolo de comunicaciones para permitir el tráfico seguro de datos desde un cliente a un servidor estableciéndose así una red privada virtual o VPN basada en TCP/IP.

Para asegurar la privacidad de la conexión, los datos transmitidos entre ambos dispositivos son encriptados por el PPP, un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa por un dispositivo PPTP.

PPTP soporta múltiples protocolos de red (IP, IPX…) y puede ser utilizado para establecer dichas redes virtuales a través de otras redes públicas o privadas como líneas telefónicas, redes de área local e Internet u otras redes públicas basadas en TCP/IP.

La principal ventaja de PPTP es que es fácil y no muy costoso de implementar.

-**L2TP:** Layer Two Tunneling Protocol es una extensión del protocolo PPP que permite la creación de tuneles VPNs a nivel de enlace de datos. L2TP reúne las mejores características de otros dos protocolos de tunelización, PPTP de Microsoft y L2F de Cisco Systems.

Como PPTP, L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado que puede ser tunelizado a través de Internet a un sitio destino. Sin embargo, la principal diferencia es que, como el establecimiento de túneles de L2F no depende del protocolo IP (Internet Protocol), es capaz de trabajar directamente con otros medios, como Frame Relay o ATM.

Al contrario que PPTP, L2TP no depende de las tecnologías de cifrado específicas del fabricante para ofrecer una implementación completamente segura y correcta.

-**WEP**: (Wired Equivalency Protocol, 'Protocolo de equivalencia con red cableada') es el sistema de cifrado incluido en el estándar 802.11 como protocolo que permite cifrar la información que se transmite entre los usuarios y el punto de acceso utilizando el algoritmo de cifrado RC4.

RC4 fue diseñado en 1987 por Ron Rivest. Este algoritmo se basa en generar claves de cifrado arbitrarias empleando la función lógica XOR. La longitud de RC4 no es fija, puede ser de 64 bits (40 bits de clave con un vector de inicialización (IV) de 24 bits), o de 128 (104 bits con un vector de inicialización de 24 bits). El vector de inicialización es una parte variable de la clave para impedir que un posible atacante recopile suficiente información cifrada con una misma clave. Además, se utiliza un checksum basado en CRC32 para prevenir que se inyecten paquetes en el flujo de datos.

A continuación se resume el proceso de cifrado/descifrado de WEP:

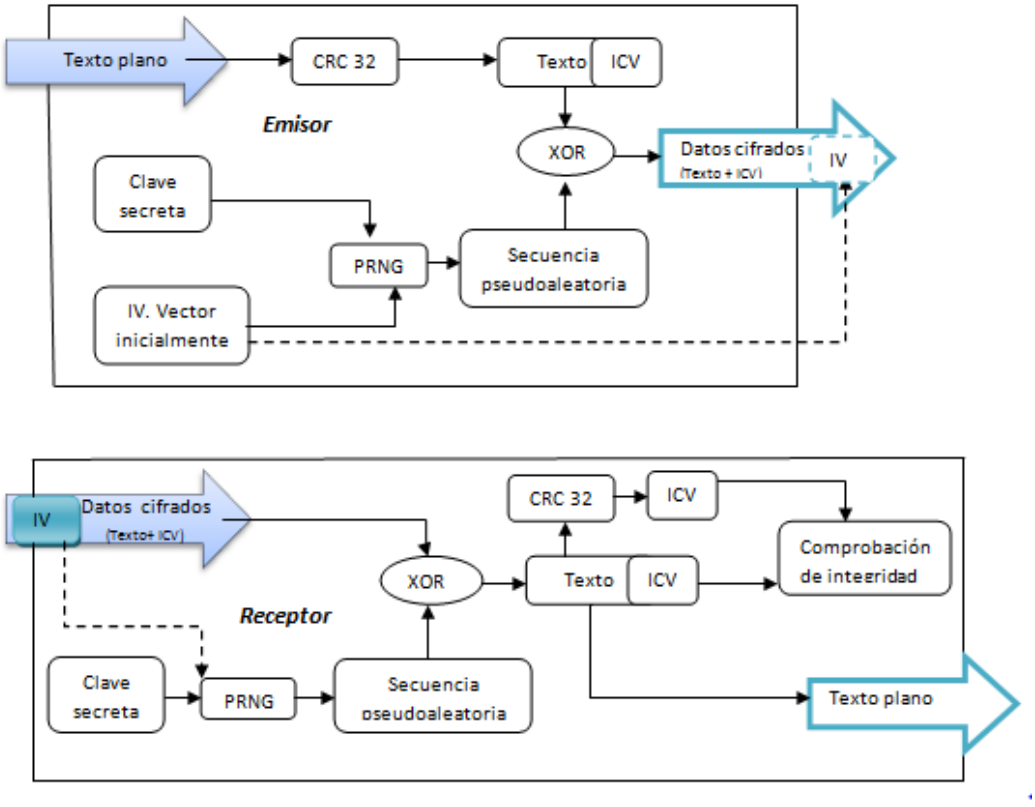


Ilustración 18. Proceso de cifrado y descifrado WEP

Fuente. Carballar, José A. WiFi- Instalación Seguridad y Aplicaciones.

Se calcula el CRC32 del payload (información útil) de la trama que se quiere enviar. Se añade a la trama como Valor de Chequeo de Integridad (ICV) y se escoge una clave secreta. A la trama se concatena la clave secreta con un número aleatorio llamado Vector de inicialización (IV) de 24 bits al principio de la clave seleccionada. A este conjunto se le conoce como Keystream. La clave será común para todos los paquetes cifrados y el vector de inicialización variará con cada paquete.

Se utiliza el Keystream para cifrar la trama; Este cifrado se lleva a cabo mediante la utilización de la función XOR. El resultado obtenido de este cifrado junto con el vector de inicialización usado durante el proceso y sin cifrar, conforman la trama cifrada que se enviará a través del medio.

Los pasos realizados en el proceso de descifrado son:

- Se utiliza el vector de inicialización y la llave para descifrar Payload e ICV.
- Se vuelve a calcular el ICV y se compara con el original. Si no coincide indica que el texto ha sido modificado por el camino.

Este proceso de cifrado y descifrado tiene lugar para todo el tráfico intercambiado entre el punto de acceso y el dispositivo del usuario de la red WLAN. Aparentemente el algoritmo WEB resuelve el problema de la seguridad en las redes WiFi, pero dicho mecanismo presenta debilidades como las que se muestran a continuación:

- Únicamente protege el medio radio, sin añadir ningún tipo de seguridad al tráfico más allá del AP.
- Al tener una clave común a todos los usuarios y puntos de acceso de la red, es decir, una clave compartida, no protege de intrusión de usuarios internos y cualquier usuario que posea la clave es capaz de comprometer la integridad de los datos transmitidos.
- Los problemas se incrementan cuando se utiliza la misma clave para el cifrado como para la autenticación, lo que provoca que un atacante que conozca la clave pueda ingresar y descifrar los mensajes transmitidos en la red.
- Adicionalmente, el vector de inicialización de WEP es enviado en texto plano sin ningún tipo de cifrado. Cuando se tiene una red muy ocupada, debido a la corta longitud del IV éste se repite cada cierto tiempo. Al capturar varios paquetes que contienen el mismo IV, un atacante puede descubrir la contraseña que le permita averiguar la clave WEP y lograr acceso a la red.

Como primera solución de seguridad, WEP resultó vulnerable debido a las limitaciones en el tamaño de las claves, a la facilidad para obtenerlas espiando el tráfico y a la falta de detección de réplicas maliciosas. A pesar de las múltiples vulnerabilidades, los usuarios solían completar la seguridad WEP generalmente de forma conjunta con otras soluciones de seguridad como por ejemplo soluciones VPN, facilidades IEEE 802.11X y soluciones propietarias de los fabricantes.

En cualquier caso, para neutralizar los problemas se ofrecieron alternativas con mayores niveles de seguridad como WPA, WPA2.

En 2003 la Alianza WiFi promovió la seguridad WPA con un subconjunto de las facilidades que se estaban diseñando en el 802.11i.

-**WPA:** WiFi Protected Access fue creado para corregir las deficiencias del sistema previo, WEP, incorporando un método de autenticación y mejoras en el nivel de codificación existente. Cuando IEEE se puso a trabajar en su nueva recomendación 802.11i, buscaba una solución rápida a los inconvenientes WEP y además una solución que fuese compatible con el hardware existente. Por este motivo, se decidió desarrollar dos soluciones. Una rápida y temporal que se denominó WPA y otra más definitiva para aplicar en nuevos puntos de acceso, no siendo compatible con el hardware anterior, que se denominó WPA2.

WPA es un estándar que opera a nivel MAC y está basado en un borrador del estándar IEEE 802.11i. Aunque WPA tiene algunas carencias que el definitivo IEEE 802.11i no tiene.

WPA consigue paliar las debilidades conocidas de WEP introduciendo una extensión del vector de inicialización que pasa a ser de 24 a 48 bits, minimizando así la reutilización de claves. Se proponen mecanismos nuevos de derivación y distribución de claves y un nuevo protocolo conocido como TKIP (Temporal Key Integrity Protocol) para la generación de claves por paquete. Este protocolo emplea el algoritmo de cifrado RC4, al igual que WEP, pero elimina el problema de las claves estáticas compartidas. Se encarga de cambiar dicha clave cada cierto tiempo, ampliando la longitud de la clave de 40 a 128 bits, y pasa de ser única y estática a ser generada de forma dinámica para cada usuario y para cada paquete.

TKIP cifra el vector de inicialización, que suponía un problema de privacidad en WEP ya que el IV se enviaba por el aire sin cifrado alguno, para evitar ataques que permitan revelar la clave.

Además, se incluye el Control de la Integridad del Mensaje (Message Integrity Check, MIC), llamado Michael, que verifica la integridad de los datos de las tramas diseñado para prevenir que intrusos capturen paquetes, los alteren y los reenvíen. La función MIC, reemplaza el Checksum CRC32 utilizado en WEP. Michael provee una función matemática de alta fortaleza en la cual el transmisor y el receptor deben computar y comparar si coinciden o no los datos; Si no coinciden los datos se consideran corruptos y se desecha el paquete. De este modo, TKIP impide que un atacante pueda alterar los datos que se transmiten dentro de un paquete.

En cuanto a la autenticación, el mecanismo usado emplea 802.X y EAP. En función del entorno de aplicación, en WPA es posible operar en dos modalidades:

- **Modalidad de red doméstica o WPA-PSK (Pre-Shared Key)**: En estos entornos no es posible contar con un servidor de autenticación centralizado o un marco EAP. Se requiere introducir una contraseña compartida en el punto de acceso o modem ADSL, así como en cada uno de los dispositivos que desean conectarse a la red WiFi. Solamente podrán acceder al punto de acceso los dispositivos

cuya contraseña coincida con la del punto de acceso. Esto evita ataques basados en escuchas así como acceso de usuarios no autorizados. La contraseña provee una relación de acuerdo único para generar el cifrado TKIP en la red. Por lo tanto, aunque la contraseña inicial es compartida por todos los dispositivos de la red, no lo son las claves de cifrado que son diferentes para cada dispositivo.

- **Modalidad de entorno empresarial**: En este entorno WPA utiliza el estándar IEEE 802.11x y EAP. EAP se emplea como transporte extremo a extremo para los métodos de autenticación entre el dispositivo de usuario y los puntos de acceso. Mientras que IEEE 802.1x se emplea como marco para encapsular los mensajes EAP en el enlace radio. El conjunto de estos dos mecanismos junto con el esquema de cifrado forman una fuerte estructura de autenticación que utiliza un servidor de autenticación centralizado, como por ejemplo, un servidor RADIUS.

-**WPA2**: Es la versión certificada interoperable de la especificación completa del estándar IEEE 802.11i. La seguridad es mucho más robusta que la que ofrece WPA. WPA2 refuerza el algoritmo de cifrado utilizando como protocolos de cifrado CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) basado en el algoritmo de encriptación AES (Advanced Encryptation Standard) de 128 bits. Este brinda un alto nivel en la autenticación de usuarios, pero tiene como desventaja que no es compatible con versiones anteriores de software.

El elemento estándar que negocia dinámicamente los algoritmos de autentificación y de cifrado que se utilizarán para las comunicaciones entre los puntos de acceso y los usuarios inalámbricos es conocido como RSN (Robust Security Network). RSN utiliza AES, junto con IEEE 802.1x y EAP. El protocolo de seguridad que RSN construye sobre AES es el CCMP.

Otra mejora respecto a WPA es que incluye soporte no sólo para el modo infraestructura BSS sino también para redes ad-hoc y permite la de-autenticación y disociación segura de la red.

-**Autenticación y gestión de claves WPA, WPA2: EAP e IEEE 802.1X**

- **IEEE 802.1X:** Es un estándar para el control de acceso a red de nivel 2 que contempla un marco para la autenticación y la distribución de claves. El estándar traduce las tramas enviadas por un algoritmo de autenticación en el formato necesario para que estas sean entendidas por el sistema de autenticación que utilice la red. Por lo tanto, IEEE 802.1x, no es por sí mismo un método de autenticación y debe emplearse de forma conjunta con protocolos de autenticación para llevar a cabo la verificación de las credenciales de usuario, así como la generación de las claves de cifrado.

802.1x involucra la existencia de tres actores:

- **Solicitante**: Usuario inalámbrico que desea acceder a la red
- **Autenticador**: Generalmente es un punto de acceso que recibe la conexión del solicitante, su función es forzar el proceso de autenticación y enrutar el tráfico a las entidades adecuadas de la red.
- **Servidor de autenticación**: Se trata del servidor que verifica las credenciales del solicitante. Generalmente se suele emplear como servidor de autenticación remota de usuarios servidores RADIUS (Remote Authentication Dial In User Service)

Cuando el equipo del usuario va a acceder a la red, el punto de acceso le envía una petición de identificación. El usuario le envía su identificación, que el punto de acceso reenvía al servidor. Tras comprobar el derecho de acceso del usuario, el servidor envía su autorización para permitir su acceso a la red.

La autenticación del cliente se lleva a cabo mediante el protocolo EAP y generalmente un servidor RADIUS; Existen algunas variantes del protocolo EAP, según la modalidad de autenticación que se emplee.

-**EAP**: Un punto de acceso 802.1x sólo se comunica con los usuarios autentificados. Antes de su autenticación sólo admite las comunicaciones con el protocolo EAP (Extensible Authentication Protocol) para verificar su identidad.

EAP es un protocolo de autenticación definido para llevar a cabo tareas de AAA y fue diseñado originalmente como una extensión del protocolo PPP (Point to Point Protocol). Cuando una red inalámbrica utiliza EAP, el usuario solicita conectividad a la red WiFi a través de un punto de acceso. El punto de acceso solicita al dispositivo que se identifique y envía los datos de identificación que éste le envía a un servidor de autenticación. Una vez el servidor ha comprobado la veracidad del nuevo dispositivo, envía su respuesta al punto de acceso, y este concluye la autenticación del nuevo dispositivo si la respuesta por parte del servidor de autenticación ha sido satisfactoria.

Existen diferentes versiones de EAP, siendo las más comunes:

- **EAP-MD5 (Message Digest 5)**: Para la autenticación emplea un nombre de usuario y contraseña. La contraseña se cifra mediante el algoritmo MD5, mientras que el nombre de usuario se envía sin ningún tipo de protección. Este sistema es vulnerable a los ataques del tipo Man-In-The-Middle y ataques diccionario. Además, no utiliza ningún mecanismo de seguridad para autenticar el servidor y la estrategia para autenticar al usuario es por medio de contraseñas. Proporciona un nivel de seguridad muy bajo por lo que no es recomendable utilizarlo como protocolo en redes inalámbricas.
- **EAP-LEAP (Lightweight EAP)**: Protocolo propietario de Cisco en el que se utilizan las contraseñas como método de autenticación del servidor. Las credenciales de usuario se envían sin cifrar. LEAP no soporta la utilización de One Time Password (OTP) y requiere de infraestructura CISCO para poder ser utilizado. Esta autenticación, aunque ligera, previene de ataques Man-in-

The-middle y de secuestro de la sesión, pero sigue manteniendo el riesgo de exposición de la identidad y de ataques diccionario.

- **EAP-TLS (Transport Layer Security)**: Está considerado como el protocolo más seguro. Ofrece una autenticación mutua entre el cliente y el servidor. Utiliza certificados digitales para garantizar la identidad del cliente y del servido. Esto obliga a disponer de una infraestructura de clave pública para gestionar estos certificados, lo que lo hace aconsejable sólo cuando se necesitan altos niveles de seguridad.

- **EAP-TTLS (Tunnelled TLS)**: Está orientado a trabajar con servidores RADIUS. Está integrado con una gran variedad de formatos de almacenamiento de contraseñas y sistemas de autenticación basados en contraseñas así como con múltiples bases de datos de seguridad. TTLS ofrece autenticación fuerte mutua y sólo requiere certificados en el servidor. Con EAP-TTLS se elimina la necesidad de configurar certificados para cada usuario de la red inalámbrica. Se autentica al usuario en el sistema con las credenciales basadas en nombre de usuario y contraseñas, y se cifran las credenciales de usuario para garantizar la protección de la comunicación inalámbrica.

- **PEAP (Protected EAP)**: Desarrollado por Microsoft, Cisco y RSA Security, es muy similar a EAP-TTLS, en el sentido de que solamente requiere certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP mediante el establecimiento de un túnel seguro TLS entre cliente y el autenticador.

- **EAP-FAST (Flexible Authentication via Secure Tunnelling)**: Protocolo creado por Cisco para reemplazar a LEAP. Ofrece una autenticación mutua tunelada y no es imprescindible que el servidor se identifique con un certificado digital. En su lugar ofrece utilizar una clave secreta compartida conocida como PAC (Protected Access Credential, 'Credencial de acceso protegido').

- **EAP-SIM (Subscriber Identity Module)**: Ofrece una autenticación mutua mediante la utilización de tarjetas SIM insertadas en el propio dispositivo inalámbrico o conectada a través del puerto USB.

2.3 Tecnología inalámbrica WIMAX

La tecnología **WiMax** (Worldwide Interoperability for Microwave Access, 'Interoperabilidad Mundial para Acceso por Microondas) es una norma de transmisión por ondas de radio orientada a la última milla que permite la recepción de datos por microondas y retransmisión por ondas de radio. El propósito de WiMax es promover el despliegue de redes de acceso de banda ancha inalámbrica que usen el estándar mundial que define esta tecnología, IEEE 802.16. Se trata de una especificación diseñada para cubrir las necesidades de las WMANs (Wireless Metropolitan Area Networks, 'redes de acceso metropolitanas inalámbricas').

La nomenclatura WiMax fue presentada por WiMaX Forum, establecida en Junio de 2001 sin fines de lucro. Se trata de una organización formada por un consorcio de industrias fabricantes de equipos de telecomunicaciones, que impulsada por el sector fue creada con el objeto de promover y certificar la interoperabilidad de los productos inalámbricos de banda ancha de conformidad con los estándares 802.16 y ETSI HiperMAN (High permormance radio MAN).

Como sucedió con la tecnología WiFi, que garantiza la interoperabilidad entre distintos equipos, WiMax se asociará globalmente con el propio nombre del estándar para certificar el cumplimiento del estándar y la interoperabilidad entre equipamiento de distintos fabricantes: todo equipamiento que no cuente con esta certificación, no puede garantizar su interoperabilidad con otros productos.

Ilustración 19. WiMAX Forum

Fuente. WiMAX FORUM

El estándar inicial **IEEE 802.16** hace referencia a un sistema BWA (Broadband Wireless Access, 'Acceso Inalámbrico de ancho de banda'), publicado en Abril de 2002. Inicialmente tan solo abarcaba enlaces fijos de radio con visión directa LOS (Line of Sight) entre transmisor y receptor para última milla, en la banda de frecuencias de 10-66 GHz, con unas tasas de transferencia de hasta 70 Mbps y un alcance de cobertura de unos 50 Km.

La propagación de la línea de visión (LOS) se refiere a la radiación electromagnética. Se trata de un enlace de radio que debe tener visibilidad directa entre las antenas, por lo que no debe haber obstáculo entre transmisor y receptor, para garantizar la calidad del radio enlace.

El objetivo de dicho estándar se enfocaba en el uso eficiente del ancho de banda y

definía una capa de control de acceso al medio para soportar todas las especificaciones de las capas físicas que pudieran utilizar la banda de 10-66 GHz.

En el año 2003 fue ratificada la nueva versión **802.16a** y fue entonces cuando WiMax comenzó a cobrar relevancia como una tecnología de banda ancha inalámbrica. Debido a que es compleja la operación de dispositivos a frecuencias mayores de 11 GHz el grupo empezó a trabajar utilizando una banda del espectro mucho más estrecha y baja, de 2 GHz a 11 GHz, facilitando así su regulación. Además, se centraron esfuerzos en especificar enmiendas a los estándares anteriores para soportar las aplicaciones que no tienen visibilidad directa NLOS (Non LOS). Este subrango de frecuencias permite el desempeño de enlaces 'sin línea de vista', haciendo al estándar 802.16a la tecnología apropiada para aplicaciones de última milla donde los obstáculos como árboles, edificios, montañas y otras estructuras que están presentes en la vida real no sean un problema a la hora de establecer radioenlaces. No requiere, por tanto, de torres LOS sino únicamente del despliegue de estaciones base (BS) formadas por antenas emisoras/receptoras.

Se introduce la modulación basada en Multicanalización Ortgonal por División de Frecuencia (OFDM) y se utiliza tanto una portadora, como en la proposición inicial 802.16, como múltiples subportadoras. Se pueden seleccionar diferentes frecuencias y distintos anchos de banda de canal de forma dinámica. Se proporciona una calidad de servicio garantizada mediante la definición expresa de funciones QoS y mecanismos de control de errores en la capa MAC.

Se agregó soporte por Acceso Múltiple Ortogonal por División de Frecuencia (OFMDA) pudiéndose realizar también un acceso al medio TDMA (Time Division Multiple Access) de bajada.

El grupo empieza a trabajar en aportar al protocolo una fuerte calidad de servicio; Se estandarizó como **802.16b** a dicho protocolo que además daba prioridad a cierto tráfico pudiéndose utilizar para transmitir voz y datos. Utiliza la banda de frecuencia entre 5 GHz y 6 GHz.

Posteriormente, el estándar **IEEE 802.16c** se ocupó sobre todo del rango de 10 GHz a 66 GHz. Se desarrollaron aspectos como la evolución del funcionamiento y la prueba y ensayo de los posibles perfiles del sistema. Esto último, es un elemento crucial dentro de las herramientas de WiMax, ya que pasa a constituir un gran acuerdo de opciones disponibles en el estándar 802.16. La metodología de perfiles del sistema evoluciona para definir que características podrían ser obligatorias y cuáles opcionales. Con esto, los fabricantes tendrían un conocimiento mayor para fabricar sus dispositivos pudiendo distinguir sus productos por precio, funcionalidad y sector del mercado.

Debe tenerse presente que para este estándar se tienen tres tipos de modulación para la capa física: modulación con una sola portadora, modulación con OFDM de 256 portadoras y de 2048 portadoras. El utilizado en este protocolo es OFDM de 256 portadoras, ya que el proceso de cálculo para la sincronización tiene menor complejidad que el esquema de 2048 portadoras.

En Octubre de 2004, fue publicado el estándar **IEEE 802.16d (802.16-2004**) con el fin de reemplazar el estándar IEEE 802.16a. IEEE 802.16d está diseñado para modelos de uso de acceso fijo. Mantiene la operación en las bandas 10-66 GHz y 2-11 GHz, consolida los protocolos anteriores e incorpora los perfiles indicados por el WiMaX Forum soportando numerosos elementos obligatorios y opcionales. Mejora la entrega de última milla es aspectos cruciales como la interferencia del multitrayecto, el retraso difundido y la robustez. Utiliza OFDM 256 FFT (Transformada rápida de Fourier) o OFDMA 2048 FFT.

Finalmente el estándar **802.16e (802.16-2005)** se trata de una revisión del 802.16d que apunta al mercado móvil añadiendo portabilidad y la capacidad para clientes móviles con adaptadores IEEE 802.16e para conectarse directamente a la red Wimax. Define un sistema combinado de acceso de banda ancha fijo y móvil. Las especificaciones anteriores para el acceso fijo se mantienen y para el soporte de movilidad se utilizan frecuencias de hasta 6 GHz, proporcionando servicios hasta velocidades de 120 Km/h.

IEEE 802.16m (IEEE 802.16m-2011) se trata de una extensión del 802.16 y define una interfaz aérea avanzada, conocida como IMT-Advanced, con velocidades de transferencia de hasta 100 Mbps en estaciones móviles y 1 Gbps en estaciones fijas.

El protocolo publicado en agosto de 2012, **IEEE 802.16-2012**, incluye las especificaciones del protocolo anterior y define la interfaz aérea (capas PHY y MAC) de los accesos inalámbricos de banda ancha, tanto fijos como móviles punto/multipunto. Permite la utilización de las bandas 10-66 GHz y las inferiores a 11 GHz.

Existen otros estándares IEEE 802.16f y 802.16g que se encargan de las interfaces de administración de la operación fija y móvil.

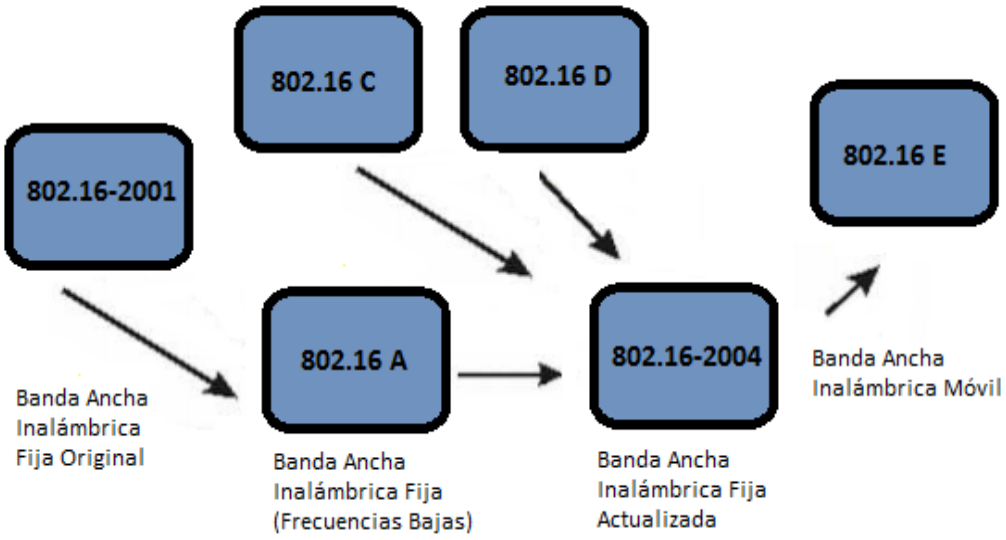


Ilustración 20. Familia de estándares IEEE 802.16

	802.16	802.16d	802.16e
Estado	Completado Diciembre 2001	Completado Junio 2004	Completado Diciembre 2005
Banda de frecuencia	10 GHz- 66 GHz	2 GHz-11GHz	2 GHz-11GHz para aplicaciones fijas 2 GHz-6GHz para aplicaciones móviles
Aplicaciones	LOS fijo	NLOS Fijo	NLOS fijo y móvil
Arquitectura MAC	Punto a multipunto, Mesh	Punto a multipunto, Mesh	Punto a multipunto, Mesh
Esquema de transmisión	Una única portadora	Una portadora, 256 ODFM o 2048 OFDM	Una portadora, 256 OFDM o Scalable OFDM con 128, 512, 1024 o 2048 subportadoras
Modulación	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM
Velocidad de trasnsmisión	32 Mbps – 134.4 Mbps	1 Mbps- 75 Mbps	1 Mbps- 75 Mbps
Multiplexación	Burst TDM/TDMA	Burst TDM/TDMA/OFDMA	Burst TDM/TDMA/OFDMA
Duplexación	TDD y FDD	TDD y FDD	TDD y FDD
Ancho de banda del canal	20 MHz, 25 MHz, 28 MHz	1.75 MHz, 3.5 MHz, 7 MHz,14 MHz, 1.25 MHz, 5 MHz, 10 MHz, 15 MHz, 8.75 MHz	1.75 MHz, 3.5 MHz, 7 MHz, 14 MHz, 1.25 MHz, 5 MHz, 10 MHz, 15 MHz, 8.75 MHz
Implementación Wimax	Ninguna	256- OFDM como WiMAX Fijo.	Scalable OFDMA como WiMAX Móvil.

Tabla 8. Características principales estándares IEEE 802.16

2.3.1 Características de WIMAX

WiMAX es una alternativa de red inalámbrica de banda ancha que ofrece características muy flexibles en términos de despliegue y posibles ofertas de servicios. A continuación, se enumeran algunos puntos a destacar acerca de la tecnología inalámbrica:

- **Capa física basada en OFDM**: La capa física está basada en multiplexado por división de frecuencias ortogonales (OFDM), un sistema que presenta gran cantidad de beneficios con respecto a otras modulaciones. OFDM se caracteriza por dividir la señal de banda ancha en un número de señales de banda reducida permitiendo transmitir eficientemente la información. Se trata de una modulación multiportadora, donde múltiples datos se envían paralelamente utilizando diferentes subportadoras con banda de frecuencias solapadas ortogonalmente. Una característica peculiar es que permite que WiMAX opere en modo NLOS, ofreciendo una fuerte resistencia al multitrayecto de la banda ancha inalámbrica.

  OFDM está bastante extendido en las comunicaciones inalámbricas gracias a su resistencia a las interferencias y a las degradaciones de señal. Esto se consigue debido a que las frecuencias, al ser ortogonales entre ellas, tratan de eliminar las interferencias entre canales. Por ello, utilizando OFDM se consigue alcanzar y garantizar una distancia mayor con menos interferencias.

- **Tasa de transmisión pico de datos:** El estándar 802.16 incluye técnicas MIMO (Multiple Input Multiple Output) junto con esquemas flexibles de sub-portadoras, codificación avanzada y modulación de hasta 64 QAM (Quadrature Amplitude Modulation). WiMAX es capaz de soportar elevados picos de tasa de datos. De hecho, las velocidades que puede alcanzar la capa física (PHY) llegan a ser de 74 Mbps cuando opera con un espectro de frecuencia de 20 MHz de ancho de canal. Estas velocidades de pico son alcanzadas cuando se utiliza una codificación 64QAM con un índice de corrección de error de 5/6. Típicamente, cuando se usa un espectro con un ancho de canal de 10 MHz y un esquema TDD (Time-Division Duplexing) con un radio 3:1 (3 tramas de bajada, 1 trama de subida), la tasa de pico en la capa física está cerca de los 25 Mbps para el enlace de bajada y de 6.7 Mbps para el enlace de subida. Bajo buenas condiciones para la señal se podrían alcanzar velocidades mayores, utilizando múltiples antenas y multiplexación espacial.

- **Ancho de banda escalable y soporte de tasa de datos:** La tecnología WiMAX está diseñada para poder trabajar con diferentes anchos de banda, esto conlleva a que puedan cumplir con gran variedad de requerimientos espectrales existentes. WiMAX tiene una arquitectura de capa física escalable que permite adecuar la transferencia de datos a los diferentes anchos de banda

del canal disponibles. Esta escalabilidad se soporta en el modo OFDMA, donde el tamaño de la FFT (Transformada Rápida de Fourier) debe estar basado en el ancho de banda disponible en el canal. Cuanto más grande sea el ancho de banda del canal, más grande será el tamaño de la FFT lo que implica un mayor número de subportadoras en el canal, facilitando de este modo un aumento en la tasa de datos o velocidades de transmisión.

- **Modulación y codificación adaptativa (AMC)**: Esta técnica es una de las características principales que hacen que WiMAX sea una tecnología capaz de adaptarse de una forma efectiva al usuario en función de un canal variable en el tiempo maximizando de este modo el caudal de información. Esta técnica soporta un número de esquemas de modulación y de mecanismos de corrección de errores (FEC) permitiendo que el esquema sea cambiado por usuario y estructura básica, teniendo en cuenta la SNR (Signal to Noise Ratio) instantánea que el receptor WiMAX recibe en un instante de tiempo. Se denomina adaptativa ya que utiliza la codificación o modulación más favorable para cada subtrama de usuario mejorando así la velocidad de transmisión.

- **Retransmisiones en la capa de enlace**: WiMAX requiere que las conexiones establecidas aseguren una alta fiabilidad y para ello soporta protocolos ARQ (Automatic Repeat reQuest) utilizados para el control de errores en la transmisión de datos, garantizando la integridad de los mismos. Esta técnica de control de errores se basa en el reenvío de los paquetes de información que se detecten como erróneos. Para controlar la correcta recepción de un paquete se utilizan ACKs y NACKs de forma que cuando el receptor recibe un paquete correctamente el receptor asiente con un ACK, mientras que si el paquete no se recibe correctamente se responde con un NACK. Si el emisor no recibe información sobre la recepción del paquete en un periodo de tiempo fijado éste se reenvía automáticamente.

- **Soporta multiplexaciones en el tiempo (TDD) y frecuencia (FDD)**: Este tipo de comunicaciones tiene una característica dúplex, es decir, existe una transmisión y recepción en los dos extremos. Las técnicas de transmisión que soporta WiMAX son TDD (Time Division Duplex) y FDD (Frequency Division Duplex). Además de dichos estándares, permite un modo Half Duplex FDD (HD-FFD) que permite una implementación de bajo coste del sistema.

  Normalmente, las soluciones para bandas licenciadas recurren a las técnicas FDD, mientras que las orientadas a bandas libres usa la técnica TDD. Aún así, dentro de las bandas existe una cierta flexibilidad a la hora de usar cada tipo de tecnología.

  La técnica FDD o duplexación por división en frecuencia, se basa en la utilización de dos bandas diferentes de frecuencia una para el canal

descendente y otra para el ascendente manteniendo una banda de separación entre dichas frecuencias con la finalidad de no solapar los canales. Esto hace que la eficiencia espectral de FDD no sea muy buena. Por otro lado, una de las ventajas más llamativas de este esquema de multiplexación es que no introduce retardos ni latencia adicional. FDD es la técnica que mejor se adapta al tráfico de voz, ya que permite tener un retardo mínimo, pero, por el contrario es la que requiere una implementación más costosa, principalmente por la adquisición de la licencia para operar en el espectro.

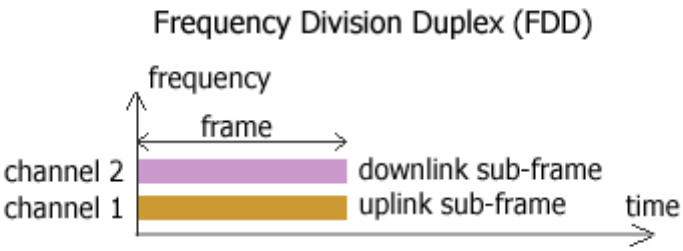


Ilustración 21. Duplexación por División en Frecuencia

La técnica TDD o duplexación por división en el tiempo utiliza una única banda de frecuencia para la transmisión de la información, es decir, en este caso la transmisión y la recepción se realiza por la misma frecuencia pero con diferencias de tiempo y una separación temporal entre los dos sentidos de la comunicación, haciendo mucho más eficiente el uso del espectro. La multiplexación TDD realiza una asignación temporal para los sentidos de la comunicación, además del tiempo de guarda, que hace que sea más sensible a los retardos y a la latencia. Esta técnica es muy eficiente para tráfico asimétrico, ya que se adapta al perfil del tráfico, por lo que se considera más adecuado para perfiles con descargas masivas de Internet, por ejemplo. Es muy utilizada en redes inalámbricas.

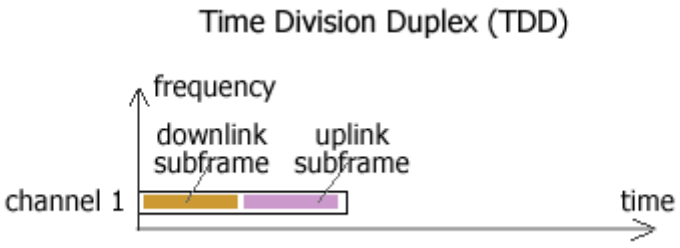


Ilustración 22. Duplexación por División en el Tiempo

Es cierto que en muchas de las implementaciones se utiliza TDD debido a sus características:

- Flexibilidad al elegir la razón entre las velocidades del enlace de subida y de bajada.
- Habilidad para explotar la reciprocidad del canal

- Habilidad para implementarse en un espectro no pareado.
- Diseño del transductor menos complejo

- **Uso de OFDMA**: OFDMA (Orthogonal Frequency Division Multiple Access) es la versión multiusuario de la conocida OFDM. Se utiliza para conseguir que un conjunto de usuarios de un sistema de telecomunicaciones puedan compartir el espectro de un cierto canal para aplicaciones de baja velocidad. El acceso múltiple se consigue dividiendo la señal en múltiples subportadoras como en OFDM. OFDMA, sin embargo, va un paso más allá agrupando subportadoras en subcanales. Una sola estación podría usar todos los subcanales dentro del periodo de transmisión, o los múltiples clientes podrían transmitir simultáneamente usando cada uno una porción del número total de subcanales. Para conseguir una mayor eficiencia, el sistema se realimenta con las condiciones del canal, adaptando continuamente el número de subportadoras asignadas al usuario en función de la velocidad que éste necesita y de las condiciones del canal. Si la asignación se hace rápidamente, se consigue cancelar de forma eficiente las interferencias co-canal y los desvanecimientos rápidos, proporcionando una mejor eficiencia espectral que OFDM.

- **Técnicas avanzadas de antenas**: Además de las técnicas descritas anteriormente para aumentar la tasa de transmisión, WiMAX permite incorporar antenas adicionales al transmisor o al receptor que mejoran la capacidad total del sistema y su eficiencia espectral. Concretamente, la velocidad se aumenta gracias a las técnicas de antenas avanzadas como: beamforming, codificación en espacio-tiempo y multiplexación espacial.

    - Beamforming: La conformación de haces o beamforming consiste en la formación de una onda de señal reforzada mediante el desfase en distintas antenas. Sus principales ventajas son una mayor ganancia de señal además de una menor atenuación con la distancia. Gracias a la ausencia de dispersión se consigue un patrón bien definido y direccional.

    - Multiplexación espacial: Consiste en la multiplexación de una señal de mayor ancho de banda en señales iguales de menor ancho de banda transmitidas desde distintas antenas. Si estas señales llegan con la suficiente separación en el tiempo al receptor este es capaz de procesarlas y distinguirlas creando así múltiples canales en anchos de banda mínimos. Esta técnica es eficaz para aumentar la tasa de transmisión, sobre todo en entornos difíciles en cuanto a la relación señal ruido. Únicamente está limitado por el número de antenas

disponibles tanto en receptor como en transmisor. Para este tipo de transmisiones es obligatoria una configuración de antenas MIMO.

- Codificación espacio-tiempo: Los denominados códigos espacio-temporales añaden redundancia a los bits de información de tal modo que los bits de código resultante permiten señalizar una forma de onda por cada antena transmisora. De este modo, la redundancia del codificador, se traduce no sólo en la habitual redundancia temporal, sino que, además se utiliza para la señalización en un sistema con diversidad espacial.

- **Calidad de servicio (QoS)**: En cuanto a la implementación propia de la QoS en WiMAX, a nivel MAC, se asocia cada transmisión a un flujo de servicio. Así, se obtiene un nivel de acceso a red orientado a conexión. La capa MAC de WiMAX está diseñada para soportar una gran variedad de aplicaciones, incluyendo servicios de voz y multimedia. Este sistema ofrece soporte para una tasa de bit constante (CBR), tasa de bit variable (VBR), flujo de tráfico en tiempo real y tiempo no real. WiMAX MAC está diseñado apra soportar una gran cantidad de usuarios con múltiples conexiones por terminal.

- **Seguridad robusta**: WiMAX basa su sistema de seguridad en los principios de autenticación y cifrado, los cuales hacen de ella una tecnología a día de hoy prácticamente invulnerable. WiMAx admite una fuerte encriptación usando AES (Advanced Encryption Standard) que es un esquema de cifrado por bloques y tiene un protocolo robusto de privacidad y de gestión de claves. Además, el sistema ofrece una arquitectura muy flexible de autenticación basado en el protocolo EAP (Extensible Authentification Protocol), el cual permite una variedad de credenciales de usuarios, incluyendo esquemas de usuario-contraseña, certificados digitales y tarjetas inteligentes.

  Los algoritmos empleados para garantizar la seguridad en la tecnología WiMAX son muy robustos. Independientemente de los mecanismos de cifrado o autenticación el propio diseño de la tecnología WiMAX implica un valor añadido en cuestiones de seguridad:

  - Dicha tecnología se diseñó como una tecnología MAN de operador que tiene que poder interconectar gran cantidad de usuarios. Al ser una red de gran escala, la propia tecnología se diseñó para poder velar por la seguridad con total garantía.

  - El acceso al medio no es aleatorio, sino completamente determinista, y regido por una estación base (BS, Base Station) que actúa en todo momento como árbitro controlando las transmisiones. Ningún terminal no autorizado puede transmitir datos hacia la BS o hacia otros SSs de

una celda, con lo que los ataques tipo DOS (Denial of Service) son más difíciles que en tecnologías de acceso aleatorio.

- **Arquitectura basada en IP**: WiMAX Forum ha definido una arquitectura de referencia de red que está basada en una plataforma all-IP (Todo IP) logrando diferentes opciones de QoS, gestión de sesiones, seguridad y movilidad.

2.3.2 WIMAX fijo y WIMAX móvil

Tal y como se ha descrito anteriormente, el estándar IEEE 802.16 ha sufrido diferentes versiones a lo largo de su creación y se basa principalmente en dos modelos de uso: el fijo y el móvil.

2.3.2.1. WIMAX fijo

El estándar 802.16-2004 o 802.16d puede ser conocido como 'Inalámbrico Fijo'. Fue publicado con el objetivo de armonizar las redes HiperMAN europeas especificadas por el ETSI (European Telecommunications Standards Institute) y las redes MAN inalámbricas especificadas en los estándares IEEE. Hay que mencionar que WiMax se basa principalmente en el estándar IEEE 802.16 cuando hablamos de LOS, mientras que cuando hablamos de NLOS se apoya en gran parte en la norma HiperMAN de ETSI.

El estándar es una solución inalámbrica para acceso a Internet de banda ancha fijo (también conocido como Internet Rural) y ofrece una alternativa al cable módem, a la línea Digital de Abonado de cualquier tipo (xDSL), circuitos de transmisión/intercambio (Tx/Ex) y circuitos a nivel de carrier óptico (OC-x). Está diseñado para proporcionar una gran capacidad tanto en el enlace descendente como en el ascendente. Dependiendo de la aplicación que se pretenda implementar en la red, la relación entre las tasas del enlace descendente como en el ascendente pueden ser variables o simétricas.

Normalmente, para lograr el acceso a Internet se establece un enlace radio entre la estación base y un equipo de usuario situado en un lugar estratégico como muestra la siguiente figura:

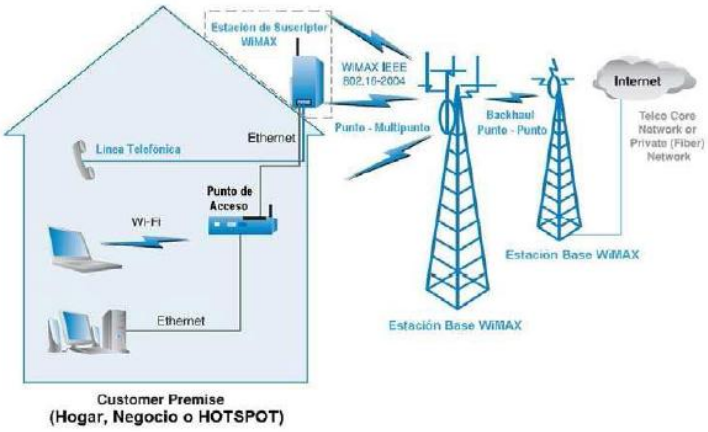


Ilustración 23. Topología WiMAX para Acceso Fijo

Fuente. Universidad Católica de Cuenca

2.3.2.2. WIMAX móvil

Es una solución inalámbrica de banda ancha que permite la convergencia de redes de banda ancha fija y móvil a través de una tecnología de acceso radio de banda ancha desplegada sobre un área extensa común y una arquitectura de red flexible. La interfaz aire de WiMAX móvil adopta OFDMA para reducir la interferencia multitrayecto en entornos en los que no hay visión directa entre antenas.

La capa física se basa en la tecnología OFDMA (Acceso Múltiple por División de Frecuencia Ortogonal), la cual es similar a OFDM en cuanto a que divide las portadoras en múltiples subportadoras, sin embargo, OFDMA va un paso más allá agrupando múltiples subportadoras en subcanales. Un cliente o una estación suscriptora podría transmitir utilizando todos los subcanales dentro del espacio de la portadora, o múltiples clientes podrían transmitir cada uno usando una fracción del número total de subcanales simultáneamente.

Se pretende que WiMAX sea la tecnología inalámbrica que unifique la telefonía móvil con las redes de datos. Se mejora y optimiza este soporte, la combinación de las capacidades de comunicación tanto fijas como móviles en frecuencias por debajo de los 6 GHz, se introduce una nueva modulación SOFDMA (OFDMA Escalable), que permite un número variable de ondas portadoras. Aparte ofrece un sistema mejorado de las tecnologías MiMO y ASS, además de incluir mejoras para el ahorro de energía.

Los perfiles de los sistemas WiMAX móvil están siendo desarrollados por el grupo MTG (Mobile Technical Group) de WiMAX Forum, con el propósito de definir las características obligatorias y opcionales del estándar IEEE que son necesarias para construir la interfaz aire conformada para los sistemas WiMAX móvil que pueden ser certificadas por WiMAX Forum. El perfil de los sistemas WiMAX móvil permite a los sistemas móviles ser configurados en base a un conjunto de características comunes, para que de esta manera se aseguren absolutamente las funcionalidades para terminales de usuario y estaciones base que sean completamente interoperables.

Algunos elementos de los perfiles de las estaciones base (BS) se especifican como opcionales para proporcionar flexibilidad adicional en despliegues basados en escenarios específicos que requieran diferentes configuraciones.

Un hecho de gran relevancia ocurrió en Octubre de 2007 cuando, el Sector de Radiocomunicación de la Unión Internacional de Telecomunicaciones (ITU/R) decidió la inclusión de la tecnología WiMAX dentro del conjunto de estándares del IMT 2000 (International Mobile Communications).

WiMAX tenía todas las condiciones para convertirse en la principal tecnología de banda ancha móvil, pero la gran alternativa LTE hizo que WiMAX perdiera fuerza en este ámbito.

2.3.3 Tipos de topología

La topología de red es la relación física y lógica entre los nodos de una red. El sistema WiMAX puede ser configurado como Punto-Punto (PTP), punto a multipunto (PMP) o como red mallada.

- **Topología Punto-Punto**: Las redes punto a punto son aquellas que responden a una arquitectura de red en la que se comunican únicamente dos nodos. Se trata de un proceso que consiste en transferir información de un dispositivo (o punto) a otro punto (solo punto receptor) y por lo general están formados por la estación base (BS- Base Station) y la Estación Suscriptora (SS- Suscriber Station). La BS es la entidad que controla toda la comunicación y establece vínculos con la SS como se muestra en la Ilustración 24

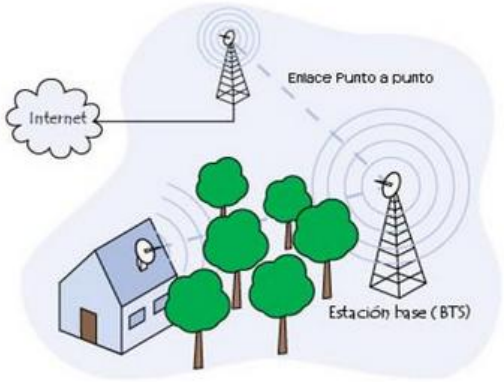


Ilustración 24. Topología punto a punto

- **Topología Punto-Multipunto**: La comunicación punto a multipunto se refiere a la comunicación que se logra ofreciendo varias rutas desde una única ubicación a múltiples puntos receptores. Está compuesta por una BS y múltiples SS. Esta topología es muy utilizada para el acceso de banda ancha de última milla para servicios inalámbricos de largo alcance, pudiendo ser utilizada tanto en medios LOS como en NLOS.

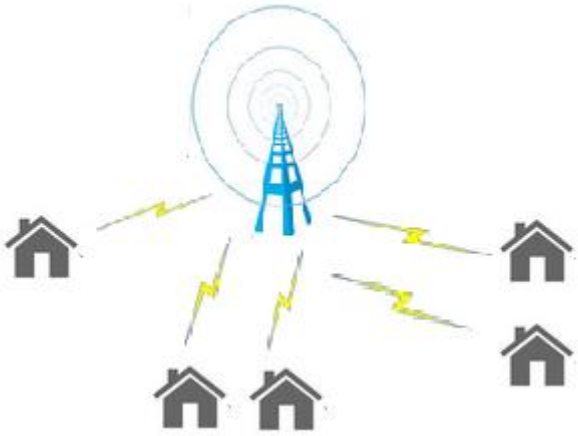


Ilustración 25. Topología punto a multipunto

- **Topología mallada**: Se puede considerar como una alternativa a la topología punto-multipunto en la cual una SS se puede conectar a una o más SS hasta alcanzar la BS de la red. Es una topología muy utilizada cuando se necesita expandir la cobertura de un área sin la necesidad de incrementar el número de estaciones base. Los paquetes de datos pueden viajar por caminos alternos para alcanzar su destino.

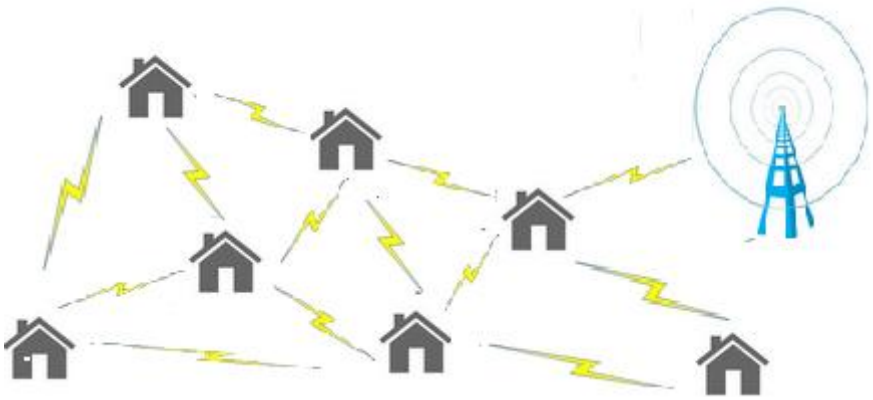


Ilustración 26. Topología malla

3. Caso de estudio

3.1 Análisis de los requisitos

El Ayuntamiento de Santillana del Mar está promoviendo el despliegue de una red inalámbrica a nivel municipal para proporcionar acceso a Internet tanto a sus ciudadanos como a los turistas que se acerquen a la localidad de Santillana del Mar. El proyecto persigue como objetivo estratégico impulsar la regeneración socioeconómica del municipio creando las condiciones necesarias para favorecer la atracción de visitantes y el fomento de la actividad ciudadana.

En la reunión con las personas encargadas se comentaron los diferentes requisitos que debía conformar la red.

Los requisitos transmitidos por el municipio serán:

- La red de acceso estará constituida por puntos de acceso y/o repetidores con tecnología Wifi 802.11 b/g/n que permitan itinerancia (roaming)
- Proporcionar a los usuarios de la red, movilidad y flexibilidad, garantizando anchos de banda, gran estabilidad, una alta disponibilidad y redundancia que permitan detectar un fallo en la red de la manera más rápida posible y que, sea capaz de recuperarse del problema de forma eficiente y efectiva, afectando lo menos posible al servicio.
- Intentar desarrollar en la medida de lo posible una red de telecomunicaciones mallada para que cuando una cantidad notable de usuarios utilicen la red siga teniendo un alto rendimiento y en caso de fallo de un punto de acceso, la dirección de la información cambie de sentido para que llegue a todos los puntos de acceso.
- Garantizar una calidad de servicio extremo a extremo. Además, de desarrollar un sistema de telecomunicaciones global y centralizado y garantizar la seguridad tanto de la red como de los usuarios de la misma.
- Los ciudadanos podrán disponer del servicio en cualquier momento del día, no habrá restricciones en el horario de conexión.
- Se estima que el número máximo de usuarios que accederán a la red de telecomunicaciones simultáneamente será de unos 300 usuarios.
- El equipamiento instalado debe cumplir con la normativa vigente en el país correspondiente.
- El capital que dispone el Ayuntamiento para la implementación del proyecto es de 35.000 € por lo que nos deberemos ajustar a dicho presupuesto en la

medida de lo posible para cumplir con los requerimientos que se nos imponen.

- Las zonas requeridas por el Ayuntamiento de Santillana para ofrecer servicio WiFi son las siguientes:

Calle Santo Domingo	Calle Juan Infante
Plaza de las Arenas	Calle la Carrera
Calle Cantón	Calle Río
Plaza Gándara	Avenida Dorat
Parking Avenida Dorat	Calle Sánchez Tagle

Ilustración 27. Zonas requeridas para ofrecer servicio WiFi

Todos estos requerimientos serán de gran importancia y se tendrán continuamente en mente a la hora de dimensionar e implementar nuestra red de telecomunicaciones, para cumplir con los objetivos que se nos proponen.

3.2 Análisis del terreno

Previo a la realización del diseño de red, es imprescindible conocer el terreno de implementación; Santillana del Mar es un municipio y una villa de la comunidad autónoma de Cantabria (España), que limita con el Mar Cantábrico al norte y con otros municipios al este, sur y oeste. La villa se localiza en una hondonada que la incomunica visualmente con el mar.

Ilustración 28. Ubicación de Santillana del Mar en España

El paisaje se caracteriza por alternar la franja litoral con extensas zonas de praderías y algunas colinas de no mucha elevación. Sus 4215 habitantes (2013) se distribuyen en 10 localidades. En nuestro caso de estudio nos centraremos en la capital del municipio, Santillana del Mar, que cuenta con un total de 1108 habitantes y está ubicada a 82 metros sobre el nivel del mar en el fondo de una cuenca rodeada por pequeñas colinas.

El casco histórico de Santillana del Mar, que es casi lo mismo que decir toda ella, se organiza en torno a dos calles principales que van a parar a sendas plazas. La primera de las calles toma diversos nombres (Carrera, Cantón y del Río) y va a dar a la plaza religiosa, que da acceso a la colegiata. Esta se divide a su vez en dos: frente a la colegiata la plaza del Abad Francisco Navarro y en su lado este la plaza de las Arenas. Otras construcciones como la Torre de Don Borja, sirve actualmente de Ayuntamiento. La calle que atraviesa la localidad hasta ella recibe el nombre de Juan Infante. Más allá de éste núcleo, separados de él por una carretera autonómica, se encuentra el convento de Regina Coeli, el de San Ildefonso y la casona de Sánchez Tagle.

Se trata de una de las localidades de mayor valor histórico-artístico de España y el principal foco de atención turística de Cantabria, lo que le convierte en uno de los lugares más visitados y atractivos de la región. El municipio está claramente volcado hacia el sector terciario, especialmente dependiente del turismo. Este sector ocupa el 55.2% de la economía municipal. Sus calles están adoquinadas y es considerado un espacio protegido, por lo que el despliegue de red debe ser respetuoso con el entorno, minimizando al máximo el impacto visual. Se pintará si es necesario el equipamiento a instalar y se estudiará la utilización de las farolas o edificios municipales, planteando una colaboración de los organismos públicos para el despliegue de esta red.

Ilustración 29. Santillana del Mar

3.3 Breve descripción técnica del proyecto

Cómo se ha comentado anteriormente, el objetivo es proponer a Santillana del Mar, la solución ideal para la implantación de un Sistema de Telecomunicaciones que abarque conexiones WiFi en las zonas bajo estudio, de modo que los servicios públicos, dispositivos inteligentes y cualquier usuario, pueda acceder a la red haciendo uso de cualquiera de los estándares actualmente definidos (802.11 b/g/n).

Para ello se pretende implantar un sistema que ofrezca un servicio de alta calidad a los ciudadanos, de modo que se posibilite el acceso a Internet a través de un portal personalizado, permitiendo las conexiones de correo electrónico, webs, servicios de VoIP mensajería instantánea y cualquier otro servicio multimedia que exista o pueda surgir.

Se pretende que el sistema proporcione a los usuarios de la red movilidad y flexibilidad, garantizando anchos de banda, calidad de servicio extremo a extremo, seguridad de acceso y gran capacidad de gestión y control del servicio.

La red diseñada se presenta como una alternativa inalámbrica para satisfacer no sólo las necesidades actuales, sino también las necesidades futuras del municipio. La infraestructura a desplegar permitirá futuras ampliaciones, de modo que se pueda seguir ampliando el área de cobertura sin necesidad de tener que cambiar la infraestructura inicial de la red.

Todos los puntos de acceso a instalar en los diferentes emplazamientos, contarán entre sus características con “Configuration Zero”, esta opción permite a los

dispositivos y usuarios finales conectarse a la red, sin preocuparse de complicadas configuraciones de equipos. Los equipos serán capaces de enmascarar las IP estáticas de los usuarios y asignar una nueva por DHCP, por lo que el usuario solamente tendrá que habilitar la tarjeta de red de su dispositivo inalámbrico. El resto de la configuración necesaria para establecer la conexión la realizará la propia red.

El sistema de telecomunicaciones a implantar, será un sistema de telecomunicaciones global y centralizado con cobertura total en las zonas ofertadas. La arquitectura centralizada de toda la estructura de la red permitirá una sencilla gestión. De este modo desde el centro de control de la red se podrán realizar las siguientes tareas:

- **Gestión de usuarios**: Todos los usuarios que acceden a la red quedarán validados en el centro de control. Esto permite una trazabilidad de uso para cada usuario además de permitir desplegar políticas de acceso por perfiles y bloquear malos usos. Se podrá localizar la ubicación de los usuarios asociados a un AP en tiempo real.

- **Gestión de la red**: Desde el centro de control se podrá configurar y administrar toda la infraestructura y los Puntos de Acceso. Además, se dispondrá del estado en tiempo real de cada elemento de red pudiendo realizar análisis del uso de canales RF, usuarios asociados, anchos de banda, análisis de las señales, ruidos y relación señal/ruido, etc.

- **Gestión de la seguridad**: La seguridad en las redes de acceso público es un factor clave. Desde el centro de control podrán establecerse las políticas de encriptación y acceso para garantizar la seguridad tanto de la red como de los usuarios de la misma. A modo de resumen se enumeran algunos de los mecanismos de seguridad que aplican los puntos de acceso, los controladores de red y la herramienta de gestión.
    - Puntos de acceso: como mecanismos más destacados de seguridad:
        - Claves WEP
        - Claves WPA utilizando TKIP y con EAP-MD5, EAP-TLS, EAP-PEAP.
        - Claves WPA2 utilizando AES y con EAP-MD5, EAP-TLS, EAP-PEAP.
        - Servidor RADIUS.
    - Controladores de red: Como mecanismos de seguridad a destacar:
        - Todos los contenidos en los puntos de acceso.
        - Definición de Portal Web AAA local y remoto
        - Autenticación por MAC

        - Autenticación por 802.11x
        - Firewall Stateful Inspection
    - Herramienta de gestión: la herramienta de gestión presenta multitud de mecanismos de seguridad tanto para evitar ataques, como para actuar frente a los mismos.
        - Detección de Rogue AP
        - Clientes de Rogue AP
        - Grupos de usuarios ad-hoc
        - Hackers
        - Denegación de servicios
        - Suplantación de MAC

- **Optimización de la escalabilidad**
- **Optimización de la disponibilidad del servicio**

Además, la arquitectura centralizada de la red estará compuesta por tres sistemas claramente diferenciados, que se explicarán posteriormente con mayor detalle.

- **Red de Acceso Inalámbrica**, cuyo objetivo es proveer conectividad a los usuarios que se encuentren en las zonas de influencia de la red.
- **Red troncal,** destinada a transportar el tráfico de datos generados desde cada uno de los puntos de acceso que componen la red de acceso inalámbrica, hasta el nodo central de la zona por medio de los distintos tipos de tecnologías disponibles en redes de comunicación.
- **Red troncal IP,** destinada a dar soporte a los distintos escenarios. Compuesta por todo el equipamiento necesario para transportar el tráfico de la red hasta las plataformas centrales.

3.4 Arquitectura de red

Para llevar a cabo los objetivos propuestos, la arquitectura de red estará compuesta de tres sistemas claramente diferenciados:

- **Red de Acceso Inalámbrica**: Hace mención a aquella parte de la red de comunicaciones que conecta a los usuarios finales con el proveedor de servicios. El principal objetivo de la red de acceso será el de ofrecer a los ciudadanos y turistas que se encuentren en las zonas de cobertura del servicio, la posibilidad de conectarse a la red inalámbrica haciendo uso de dispositivos portátiles que incorporen una tarjeta de red inalámbrica compatible con los estándares 802.11 b/g/n.

  La Red de Acceso Inalámbrica será capaz de transportar mediante protocolo IP el acceso a Internet desde las zonas WiFi; Estará compuesta por los puntos de acceso de última generación desplegados a lo largo del municipio. Dichos APs permitirán la gestión remota de todas sus características y minimizarán al máximo el impacto visual.

  Tras el estudio realizado anteriormente de los diferentes estándares 802.11, esta red se implementará con tecnología 802.11n por ser un estándar que mejora significativamente el rendimiento de la red más allá de los estándares anteriores, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión y soportando actualmente la capa física velocidades de 300 Mbps, con el uso de flujos espaciales en un canal de 40 MHz. Se utilizará la banda de 2.4 GHz, que a pesar de estar más congestionada y con más posibles interferencias, tienen una mejor tolerancia a obstáculos, es compatible totalmente con dispositivos WiFi y ofrece un mayor rango de cobertura que la banda de 5 GHz. Gracias a la tecnología 2x2 MIMO, se podrían obtener velocidades de hasta 300 Mbps a distancia de unos 150 metros. Con esta red se cubrirán las plazas y calles del municipio de Santillana del Mar.

- **Red troncal inalámbrica**: Una red troncal inalámbrica (o Backbone) es una red utilizada para interconectar otras redes, es decir, un medio que permite la comunicación de varios segmentos. Para interconectar varios segmentos de red a una troncal, son necesarios dispositivos adicionales. El Backbone existe principalmente como un conducto que permite a los segmentos comunicarse entre sí. Dicha red presenta un papel muy importante ya que se trata del sistema que interconectará todos los puntos de acceso desplegados a lo largo del municipio con el nodo central de la red, permitiendo realizar 'Roaming' entre las zonas. Esto permite que los usuarios registrados en una de las zonas con servicio puedan disfrutar de los mismos servicios con el mismo usuario y sin ninguna restricción en el resto de zonas.

  Dicha red troncal transportará mediante protocolo IP las comunicaciones

municipales de las dependencias que interconecte. Estará compuesta por la electrónica de red que permita la alimentación de los APs, la redundancia del sistema y la transmisión de la información a altas velocidades, evitando en todo caso ser un cuello de botella.

La topología que tendrá esta red troncal inalámbrica será tipo 'Mesh' y empleará el protocolo 802.11a/n en la banda libre de 5GHz. Dicha topología servirá para interconectar todos los puntos de acceso entre sí mediante radio enlaces, sin necesidad de cableado entre los diferentes puntos de acceso. Dicha red mejora la redundancia entre nodos, pues la caída de un solo nodo no implica la caída de toda la red, sino que es capaz de encontrar caminos alternativos para que los paquetes lleguen a su destino. Es importante tener en cuenta que los Puntos de Acceso deberán disponer de interfaces 802.11a/n y soportar tecnologías de red WiFi mallada. Además, desde el centro de control, para dar salida a Internet a la totalidad de la red utilizaremos como vía principal la tecnología WiMAX y una línea de Backup ADSL que servirá como vía secundaria. El operador que nos ofrece el servicio nos dejará el equipamiento en una torre de comunicación y se realizará un radioenlace hasta nuestro centro de control. En caso de que se necesite realizar simulaciones previas para comprobar la viabilidad de los enlaces, se utilizará el Software Radio Mobile.

- **Red troncal IP**: El principal objetivo de la red troncal IP es el de optimizar la eficiencia y seguridad de la red, para lo cual se separa el tráfico en diferentes túneles, en nuestro caso túneles EoIP y L2TP**.** Dicha red está destinada a comunicar todos los puntos de acceso con las plataformas centrales. Dentro de esta red queda englobada toda la electrónica necesaria para la gestión integral de la red como switches, servidores y controladoras instaladas ya sea localmente en el centro de control o en el resto de dependencias, que serán definidos con exactitud en los apartados siguientes. Para concentrar la conexión a Internet, se dispondrá de un centro de control en el Palacio de Peredo en el municipio de Santillana del Mar.

La siguiente imagen muestra un diagrama genérico de lo que sería la arquitectura de red de nuestra red de telecomunicaciones.

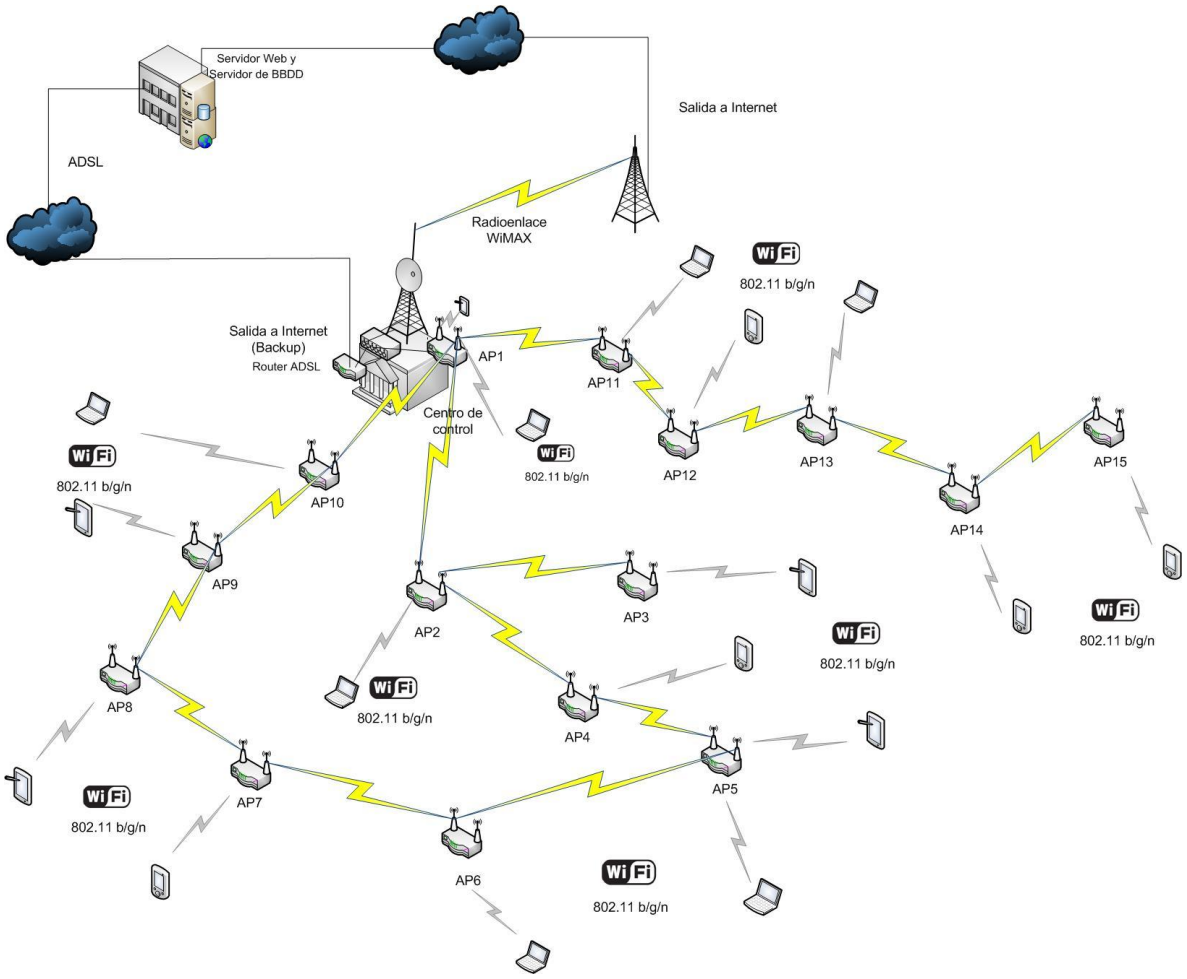


Ilustración 30. Arquitectura general del sistema

3.4.1. Características de la arquitectura de red

3.4.1.1. Escalabilidad del sistema

La red inalámbrica está diseñada de tal modo que en un futuro se puedan realizar ampliaciones sobre la misma sin necesidad de realizar costosas obras y permitiendo una ampliación gradual de la red.

El sistema presenta una arquitectura jerárquica que permite un alto grado de escalabilidad, y de este modo, poder dimensionar adecuadamente el sistema según los requerimientos, y posibilitar la ampliación del sistema según futuras necesidades y con el menor impacto.

Todos los sistemas centrales que utilizaremos tienen la capacidad de soportar el crecimiento de la red hasta cubrir todo el municipio completo.

La red troncal, posibilita el crecimiento mediante la inclusión de nuevos nodos a los que a su vez se enganche la red de acceso.

3.4.1.2. Capacidad del sistema

La red está dimensionada según las exigencias del Ayuntamiento de Santillana del Mar. Concretamente el municipio cuenta con 1108 habitantes y se duplica durante la temporada de verano, por lo que, el territorio puede llegar a contar con unas 2000 personas durante las fechas de temporada alta. Atendiendo a la premisa de dimensionamiento para el 15% de esa cantidad, el resultado obtenido es de un total de 300 usuarios que se conectarán simultáneamente como máximo.

Los APs que se propondrán soportarán como mínimo unos 30 usuarios simultáneamente de forma que se cumplan las premisas impuestas por los responsables del Ayuntamiento.

En cuanto a lo que concierne a las velocidades de acceso, la red se diseñará de modo que en el 100% de los entornos se consigan velocidades de acceso de hasta 54 Mbps para los usuarios que accedan a la red con dispositivos inalámbricos que emplean el estándar 802.11g, de hasta 11 Mbps para aquellos cuyos dispositivos estén basados en el estándar 802.11b y de hasta 300 Mbps para los usuarios conectados mediante 802.11n 2x2 MIMO.

3.5 Estudio de cobertura y viabilidad de los radioenlaces de la red troncal

Con la intención de dimensionar la red de comunicaciones descrita en los apartados anteriores, se han llevado a cabo una serie de cálculos y estudios de cobertura que ayuden a determinar la ubicación más idónea de los distintos equipos que la componen, así como a establecer los parámetros y especificaciones mínimas que han de reunir.

A lo largo del presente apartado se muestran las simulaciones realizadas para asegurar la cobertura y obtener una estimación de los puntos de acceso que serán necesarios para cubrir de forma eficiente las zonas objeto del presente estudio.

Los estudios realizados son los siguientes:

- El primero se trata del estudio de cobertura que proporciona la red Mesh; Esta interconecta los Puntos de Acceso WiFi y provee redundancia e inteligencia para la elección del mejor camino que deben seguir los paquetes para llegar a su destino. La simulación de la red Mesh se ha realizado con el Software Ekahau- Site Survey. Esta red permitirá seguir ampliando la red WiFi de una forma sencilla sin la realización de costosas obras civiles.

- Se ha realizado un segundo estudio, en el que se comprueba la cobertura para la red de Acceso. Esta red cubrirá las vías, plazas y parkings del municipio de Santillana del Mar. En las zonas en las que se proveerá cobertura, los usuarios de la red podrán acceder a la misma haciendo uso de las tecnologías

802.11b/g/n.

- En cuanto al servicio WiMAX se pensó primeramente en una alternativa que no tuvo éxito, no por no ser válida ni eficiente sino más bien por la existencia de otra posibilidad factible mucho más económica. Se detallarán, por lo tanto, ambas propuestas y se comprobará la viabilidad de cada una de ellas. Se utilizará el Software Radio Mobile para realizar simulaciones y comprobar la correcta comunicación de los radioenlaces que sean necesarios en cada una de las alternativas.

Para la realización de las simulaciones de la red WiFi Mesh y red de Acceso se ha empleado el software de simulación Ekahau Site Survey.

Ekahau Site Survey (ESS) es una herramienta software para profesionales desarrollada para la planificación y administración de redes inalámbricas (WLAN). Es la herramienta empleada por miles de administradores de TI, proveedores de servicios inalámbricos y proveedores de infraestructura de red. ESS ofrece a los usuarios una visión a nivel de suelo de cobertura y rendimiento, lo que permite crear rápida y fácilmente, mejorar y solucionar problemas de redes WiFi.

ESS está diseñado para proveer herramientas esenciales para el despliegue y la solución de problemas en redes WiFi. Sus características se muestran a continuación:

- 802.11a/b/g/n
- Planificación 3D para determinar el número óptimo y la ubicación de los puntos de acceso
- Sistema rápido y preciso para garantizar la cobertura de la red y el rendimiento
- Visualización, análisis y optimización de la red wireless.
- Informes automatizados
- Despliegue RTLS (Real Time Location System)
- Perfecta planificación de la expansión de las actuales redes WiFi.

Es muy importante la precisión y la exactitud con las que se realizan las medidas, ya que si no se hace correctamente, el número de puntos de acceso para cubrir la zona aumentará, incrementando los costes de la solución definitiva, o no cubrirá la zona de forma adecuada, repercutiendo en el rendimiento de la solución final. Hay que tener en cuenta que las simulaciones realizadas son una estimación, pero cuanto mejor se realicen todas las medidas, más se aproximará la simulación con la realidad.

Con los estudios de cobertura realizados, se ha pretendido identificar e inspeccionar visualmente las instalaciones para buscar los obstáculos potenciales a la señal RF: muros, arboles…etc; Determinar de una forma estimada el número y la ubicación de los puntos de acceso, así como la utilización de las posibles antenas que alcanzan los

niveles de señal mostrados en las imágenes que se muestran en los apartados siguientes.

3.5.1. Estudio del servicio WIMAX

3.5.1.1. Primera alternativa

En un primer momento se pensó en utilizar la tecnología WiMAX como red de transporte, para soportar el tráfico generado por los usuarios.

Para ello, se pretendía desplegar una red WiMAX compuesta por una estación base ubicada en el centro de control (Palacio de Peredo) y dos CPEs (Customer Premises Equipment) situados en ambos extremos de la red. La estación base se enlazaría con los dos suscriptores a través de radio enlaces punto a multipunto, mientras que estos estarían conectados cada uno al punto de acceso más cercano a través de un cable Ethernet.

Se realizó el presente estudio de radio propagación que tenía como finalidad validar el radio enlace punto a multipunto en la banda de 5.4 GHz, el cuál formaría la principal vía de transporte de datos de nuestra red. El nodo central que tendría la conexión a Internet sería la estación base.

Software de Cálculo

En este apartado se muestran los resultados de los cálculos realizados para comprobar la viabilidad de cada uno de los radioenlaces punto a multipunto. El primer radioenlace se creará entre la estación base y el CPE1 y el segundo radioenlace entre la estación base y el CPE2.

Se ha particularizado para cada radio enlace, realizándose un cálculo de las pérdidas básicas de propagación, y el correspondiente balance de potencias, ajustando en cada caso los parámetros de los equipos necesarios de forma que se asegure un nivel adecuado de señal en recepción.

El cálculo del balance de potencias es el procedimiento que se utiliza normalmente para estimar de una manera rápida si un radioenlace funcionará correctamente. Para llevar a cabo la realización de los cálculos teóricos, se ha hecho uso de una herramienta de software de planificación de radio que dispone de una base de datos de las cotas del terreno. El software en cuestión es el Radio Mobile.

Fue desarrollado por Roger Coudé para predecir el comportamiento de sistemas radio, simular radio enlaces y representar el área de cobertura de una red de radiocomunicaciones, entre otras funciones.

Para un enlace determinado, el programa calcula todas las pérdidas y realiza el balance de potencias, obteniendo la fiabilidad del enlace para diferentes probabilidades de error. El modelo de propagación en el cual se basa el programa para la realización de los cálculos es el conocido como 'Irregular Terrain Model (ITM)', basado en el

algoritmo de Longley-Rice.

Está basado en la teoría del electromagnetismo y en el análisis estadístico de las características del terreno y de los parámetros del radioenlace, prediciendo la atenuación media de una señal de radio que se propaga en un entorno troposférico sobre terreno irregular. Para ello, calcula la atenuación media de la misma, en función de la distancia y de la variabilidad de la señal en el espacio y en el tiempo, permitiendo estimar las características de recepción de la señal necesarias en un radio enlace determinado. Fue diseñado para frecuencias de trabajo entre 20 MHz y 20 GHz y para longitudes de trayecto entre 1Km y 2000 Km.

Para el cálculo de la propagación, el modelo Longley-Rice tiene los siguientes parámetros:

Parámetros del sistema	▪ **Frecuencia 20 MHz a 20 GHz** ▪ **Distancia de 1 a 2000 km** ▪ **Altura de las antenas 0.5 a 3000 m** ▪ **Polarización horizontal o vertical**
Parámetros del entorno	▪ 7 tipos de clima ▪ Constantes eléctricas del terreno ▪ Refractividad de la superficie 250 a 400 N-unidades ▪ Variable de terreno irregular Δh rugosidad promedio
Parámetros de instalación	▪ Criterio de posicionamiento random, careful o very careful.
Parámetros estadísticos	▪ Fiabilidad respecto a la variabilidad de tiempo, locación y situación 0.1% al 99.9%

Tabla 10. Principales parámetros de Radio Mobile

Los parámetros del sistema están asociados al conjunto de equipos de radio involucrados en el sistema y son independientes de las condiciones ambientales. Los parámetros del entorno describen estadísticamente las características del lugar donde operará el sistema.

Una vez definidos los valores para los parámetros de entrada, el modelo de terreno irregular realiza estimaciones geométricas sobre el camino de la propagación. Para

realizar los cálculos el modelo utiliza tratamientos teóricos de reflexión sobre terreno accidentado, refracción a través de una atmósfera estándar, difracción alrededor de la tierra y sobre obstáculos agudos y dispersión troposférica. Esta combinación de teoría elemental y datos experimentales por una parte, dan origen a un modelo semi-empírico acorde a la realidad física y a ciertos valores de referencia de los parámetros y por otra cumple con las leyes físicas lo suficientemente bien como para extrapolar éstos a partir de los valores de referencia con un buen grado de fiabilidad.

El procedimiento a seguir para comprobar la viabilidad de cada uno de los enlaces es el siguiente:

- Se sitúan los puntos que conforman la red sobre un plano de la zona de estudio mediante sus coordenadas geográficas.
- Para cada sistema de transmisión, se introducen en la ventana correspondiente los parámetros de configuración de los equipos, tales como la frecuencia de trabajo, potencia del transmisor, sensibilidad del receptor, ganancia de las antenas transmisora y receptora, altura de las antenas sobre el nivel del suelo, pérdidas en los cables y demás elementos de acoplamiento.
- Se generará un perfil de cada enlace en el que se muestran, además de dichos parámetros, los resultados de los cálculos realizados por el programa, pudiendo comprobar la viabilidad de cada uno de los radio enlaces generados. En todos los casos, el nivel de fiabilidad mínimo que se le ha exigido al radio enlace es del 99.999%.

Viabilidad del radio enlace

En este apartado se muestran los resultados de los cálculos realizados para comprobar la viabilidad de cada uno de los radio enlaces simulados.

Enlaces	
Palacio de Peredo (BS) →	**→ Edificio del municipio (CPE1)** **→ Edificio del municipio (CPE2)**

Tabla 11. Radioenlaces simulados

En primer lugar, como se comentaba, es necesario conocer dónde están ubicados los equipos. La estación base estará ubicada en el Palacio de Peredo de Santillana del Mar, mientras que las estaciones suscriptoras o CPEs se ubicarán en dos edificios del municipio. En la siguiente figura se muestran los puntos a interconectar.

Ilustración 31. Ubicación del equipamiento para realizar los radioenlaces

A continuación se indican las coordenadas geográficas de los puntos a interconectar, es decir, la ubicación de los equipos de los que a falta del replanteo in-situ se había pensado la instalación.

Equipo	Latitud	Longitud
Estación Base	43.389395°	-4.109111°
CPE1	43.391890°	-4.106340°
CPE2	43.387609°	-4.109214°

Tabla 12. Coordenadas geográficas de los puntos a interconectar

Para la simulación de los radio enlaces, en primer lugar, se crean las ubicaciones de los puntos con Google Earth y se importan en la herramienta de software Radio Mobile. Una vez tenemos las unidades, se introducen los parámetros de configuración de los equipos que serán utilizados para la implementación de la red WiMax con el objetivo de obtener un cálculo lo más aproximado posible. En este caso, se pensó en la utilización de equipos Radwin por ser un proveedor global líder de soluciones inalámbricas punto a punto y punto multipunto cuyas soluciones son altamente robustas, operando de modo impecable en todos los ambientes y son extremadamente sencillas de instalar y de mantener. Se utilizarán las especificaciones técnicas de la estación base RW-5200-2250 de una antena exterior RW-9402-5001 y CPEs RW-5550-2150, para la simulación de los radioenlaces. Dichas especificaciones se podrán comprobar en el Anexo D.

Los parámetros introducidos en el software son tales como:

- Frecuencia de trabajo: 5.475 – 5.720 MHz
- Potencia de transmisión: 25 dBm
- Umbral del receptor: -78 dBm
- Pérdida de la línea: 0.5 dB
- Tipo de antena: Omnidireccional 10 dBi (Estación Base), Omnidireccional 22.5 dBi (CPEs)
- Altura de la antena: 6 y 7 metros respecto el nivel del suelo
- Tipo de clima: Continental templado

Al pinchar sobre el enlace radio  se muestran los perfiles y resultados obtenidos para cada uno de los enlaces. Aparentemente ambos enlaces parecen ser efectivos y viables debido al color verde que marca la línea que los une.

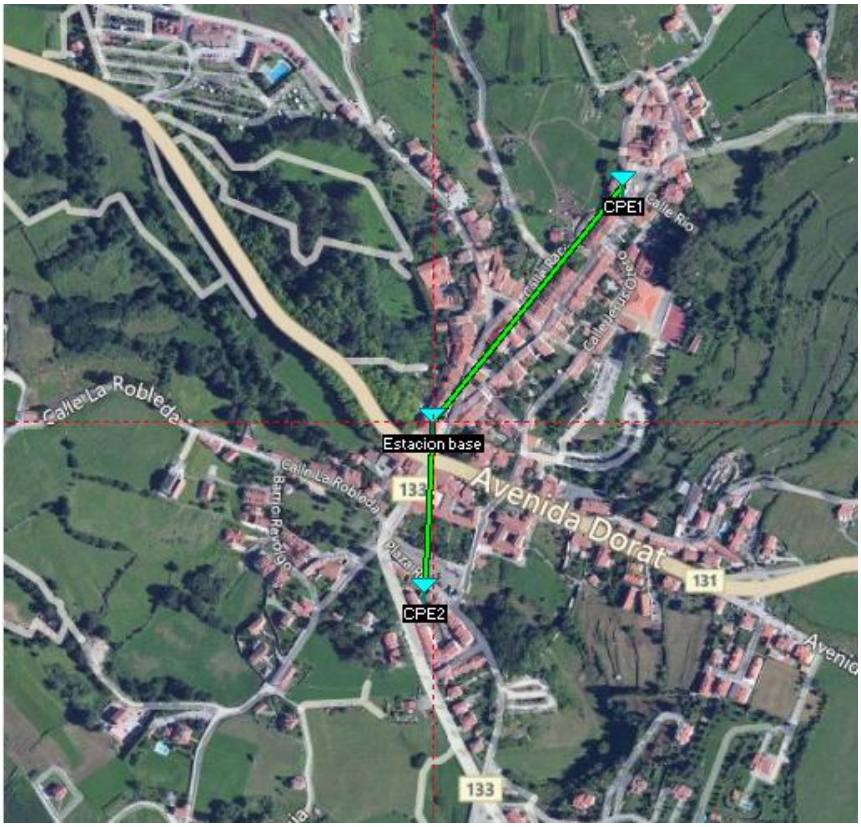


Ilustración 32. Radioenlaces simulados con Radio Mobile

Para corroborar esto, al introducir los parámetros anteriores, se genera un perfil de cada enlace en el que se muestran, además de dichos parámetros, los resultados de los cálculos realizados por el programa.

Enlace Estación Base – CPE1

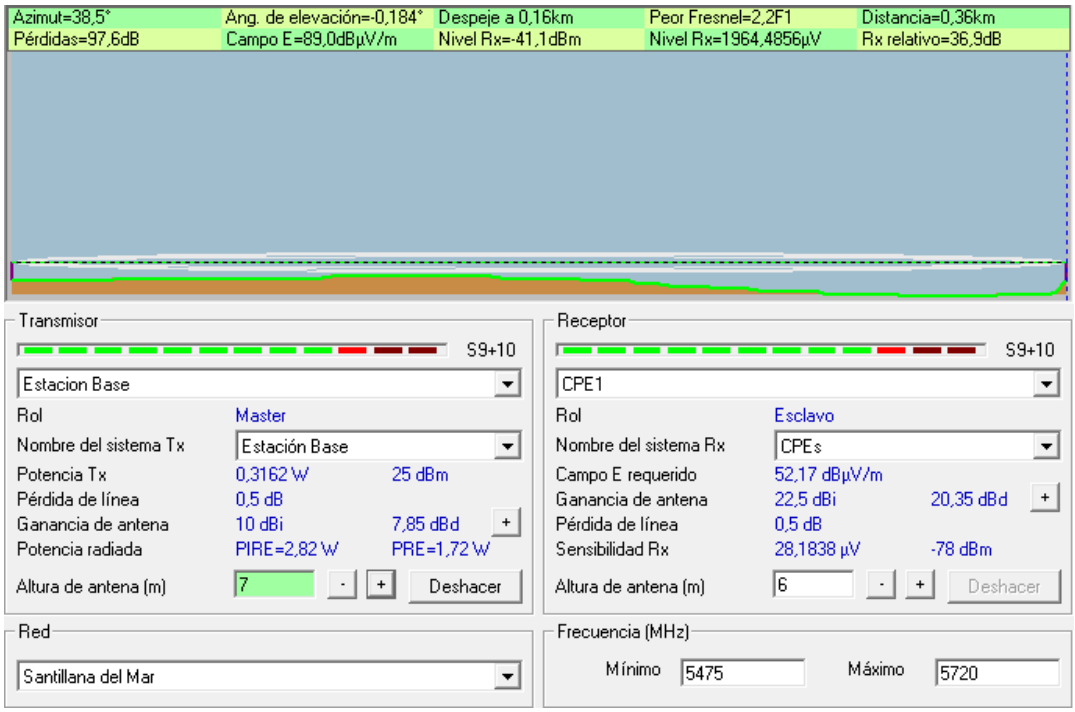


Ilustración 33. Perfil Radioenlace BTS → CPE1

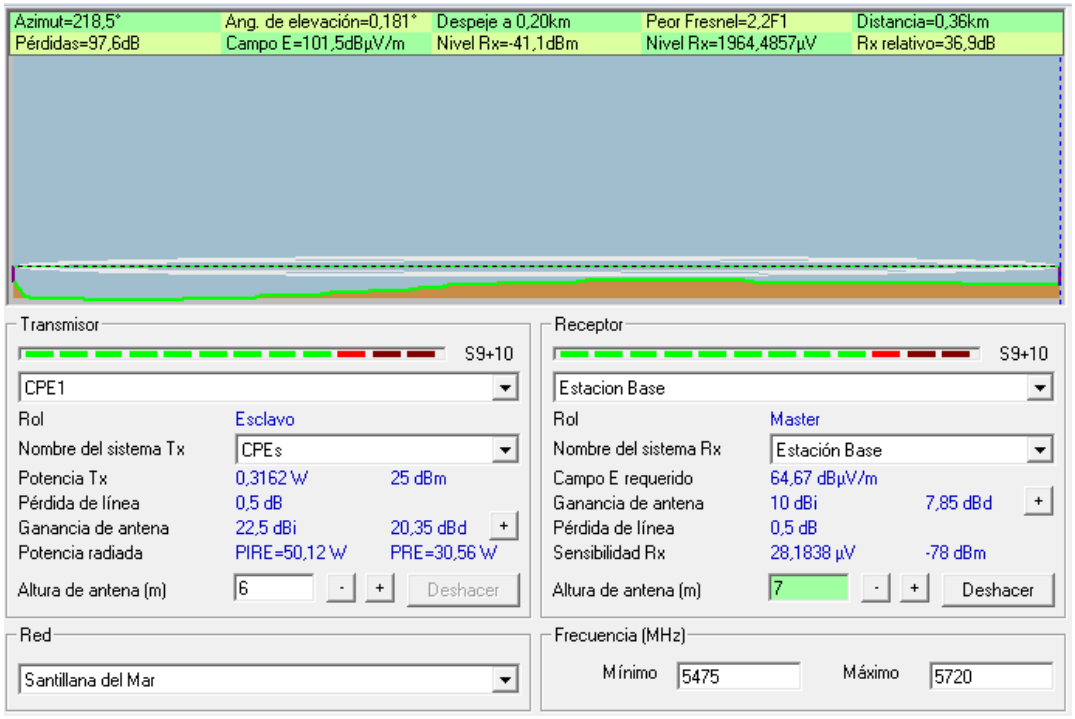


Ilustración 34. Perfil Radioenlace CPE1 → BTS

Como se puede observar en la Ilustración 33 se presentan todos los resultados relativos al enlace establecido. En la fila superior se muestran los resultados radioeléctricos de propagación:

- Azimut con el que está orientada la antena (38.5˚, 218.5˚)

- Angulo de elevación: Inclinación respecto al eje horizontal que ha de sufrir la antena (0.184˚, 0.181˚)
- Peor ángulo de Fresnel para este trayecto (2.2F1, 2.2F1)
- Distancia en línea recta entre dispositivos (0.36 km)
- Pérdidas del espacio libre entre el emisor y receptor (97.6 dB)
- Rx Relative: Señal relativa en dB con respecto a la sensibilidad del sistema receptor (36.9 dB)
- Nivel Rx: Nivel de potencia recibida (41.1 dB)

En la figura además se aprecia el perfil orográfico del enlace, así como la descripción de los sistemas y la topología de cada uno de los emplazamientos.

Según los datos que ofrece Radio Mobile, podemos concluir que dicho enlace es completamente viable. No obstante, en caso de que esta propuesta se llevará a cabo habría que realizar una visita in situ en el municipio para corroborar la viabilidad de dicho enlace.

Enlace Estación Base – CPE2

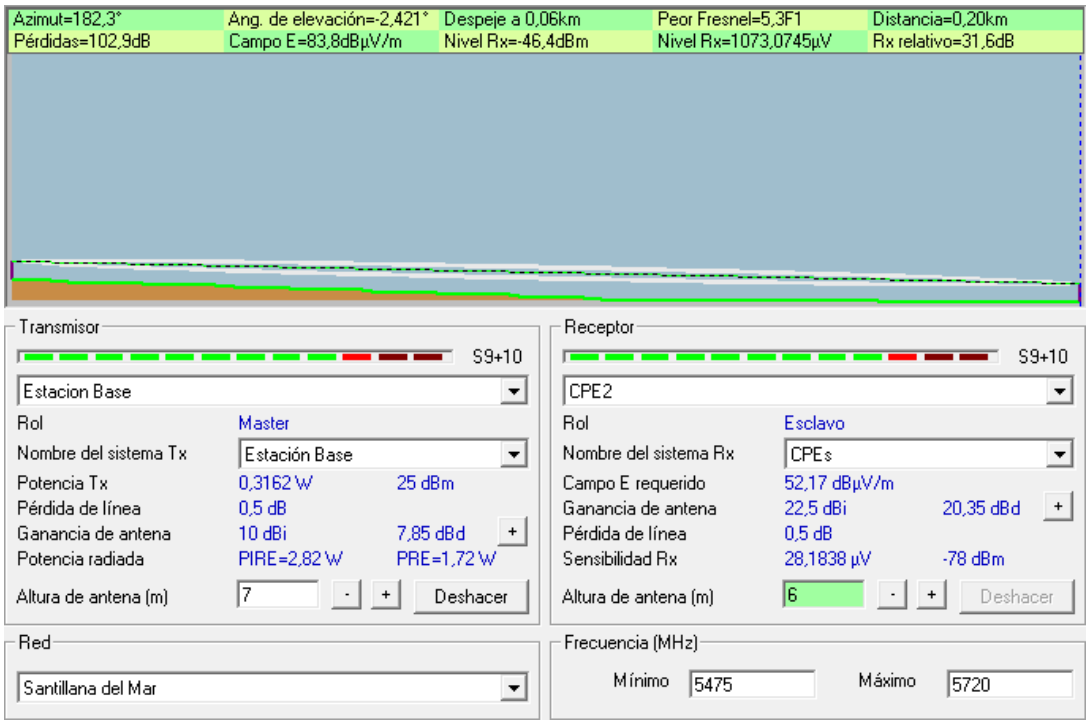


Ilustración 35. Perfil Radioenlace BTS → CPE2

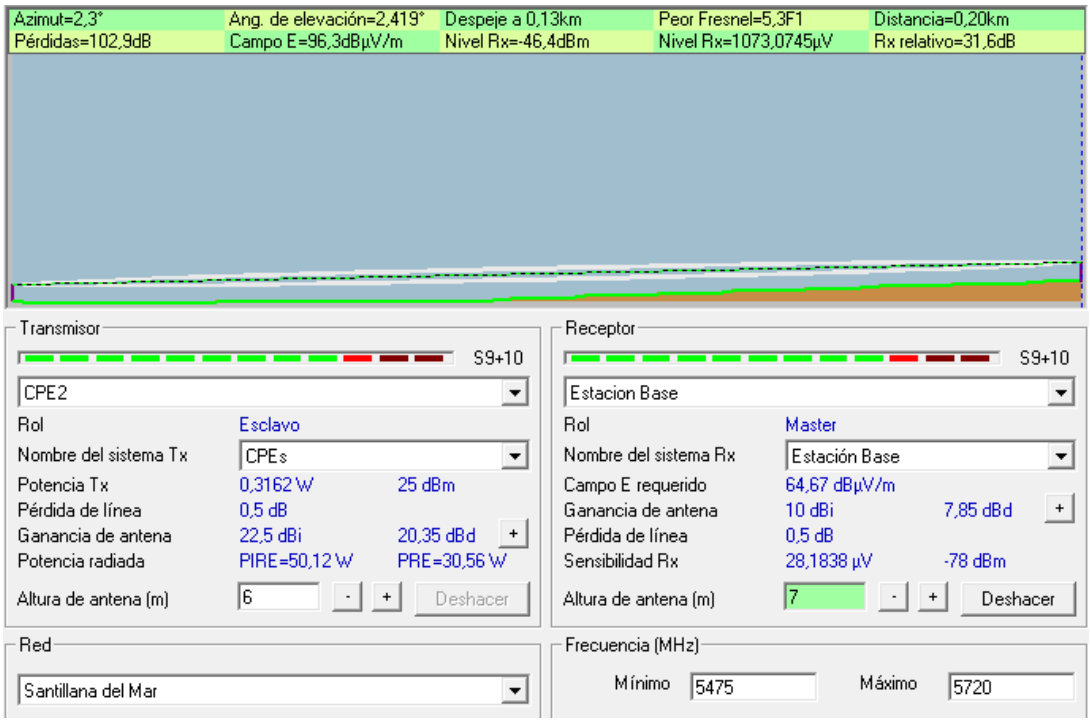


Ilustración 36. Perfil Radioenlace CPE2 → BTS

Según los datos que presenta Radio Mobile, al igual que en el caso anterior, dicho enlace es completamente viable. Aun así, debería corroborarse realizando una visita in situ en Santillana del Mar la viabilidad del enlace.

Lo comentado en el presente apartado resume aquello que se había contemplado en un primer momento. Sin embargo, al analizar los puntos de acceso que conformaban la red se comprobó que dichos equipos eran capaces de transportar el tráfico generado, sin necesidad de la instalación del equipamiento WiMAX. Además, la implantación del equipamiento Radwin suponía un elevado coste y el presupuesto se excedía, por ello se pensó la siguiente alternativa comentada en el siguiente apartado.

3.5.1.2. Alternativa que se ejecuta en el proyecto

A raíz del elevado coste que suponía la instalación del equipamiento Radwin en el municipio y comprobando que los puntos de acceso a instalar son capaces de transportar el tráfico generado por la red, se pensó otra alternativa en la que la tecnología WiMAX no se deja a un lado, sino que, en este caso se utiliza como salida a Internet proporcionando un acceso de alta velocidad además de un gran ancho de banda.

La tecnología WiMaX pretende junto con WiFi competir con las tecnologías de cable coaxial o ADSL en lo que es llevar Internet a los domicilios o lugares de interés de los usuarios. Este tipo de aplicación se llama de “última milla” dentro de la jerga propia del sector, ya que su función es llevar Internet desde los centros de conexión de las operadoras hasta el lugar de interés de los usuarios, que suelen estar a distancias relativamente cercanas pero que obligan a disponer de algún tipo de infraestructura.

Una de las alternativas es la de poder llegar a los domicilios o puntos de interés de los usuarios mediante ondas, haciéndolo posible la tecnología WiMAX.

Por lo tanto, para dar acceso a Internet, el operador Conexión Rural, cuyo objetivo marcado por el Gobierno regional, garantiza el acceso tecnológico en aquellas regiones que no resultan prioritarias para las grandes operadoras proporcionará Internet mediante WiMAX hasta una torre de comunicaciones ubicada a 6Km del Palacio de Peredo.

Desde la estación base se realizará un radioenlace hasta un CPE que será instalado en el centro de control y proporcionará Internet que servirá para que todos los usuarios puedan lograr navegar por la red. Para proporcionar una mejor calidad de servicio se instalará una segunda línea ADSL que servirá de Backup en el centro de control, para que en el caso de que se interrumpa el servicio a causa de la principal línea de comunicación, la red tenga una segunda vía.

Para comprobar la viabilidad del radioenlace desde la torre de comunicación hasta nuestro centro de control, utilizamos el Software RadioMobile. Tras ubicar los puntos e importarlos en la herramienta, introducimos los parámetros del equipamiento que utilizará el operador y calculamos el radioenlace.

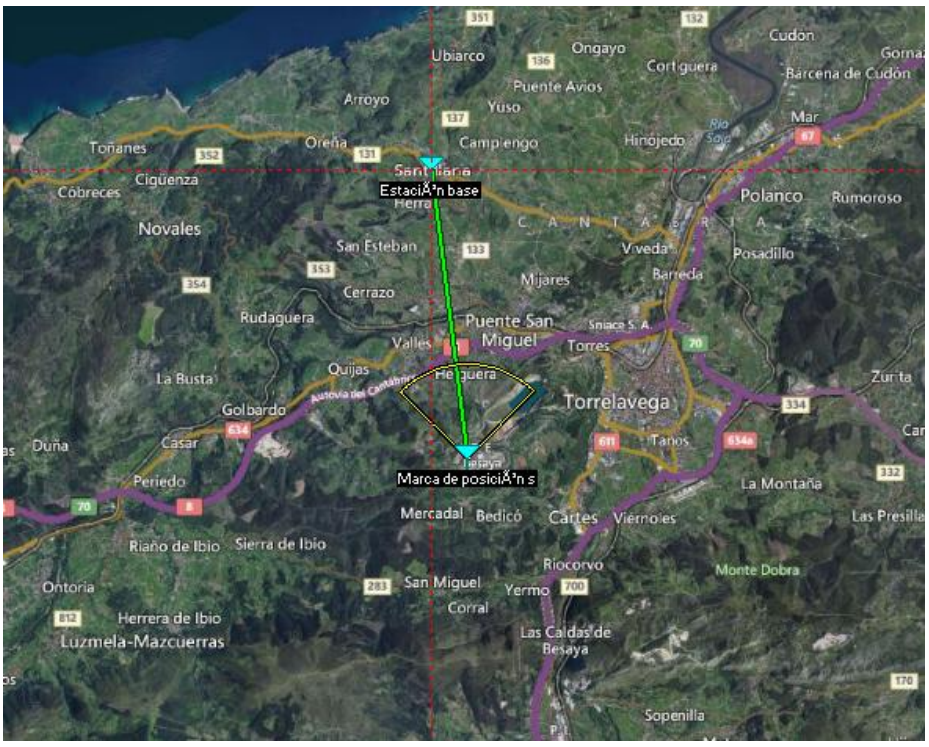


Ilustración 37. Radioenlace BTS del operador → CPE instalado en el Palacio de Peredo

Para corroborar la viabilidad del radioenlace, se genera el perfil del mismo donde se presentan todos los resultados relativos al enlace establecido como se puede observar en la Ilustración 38.

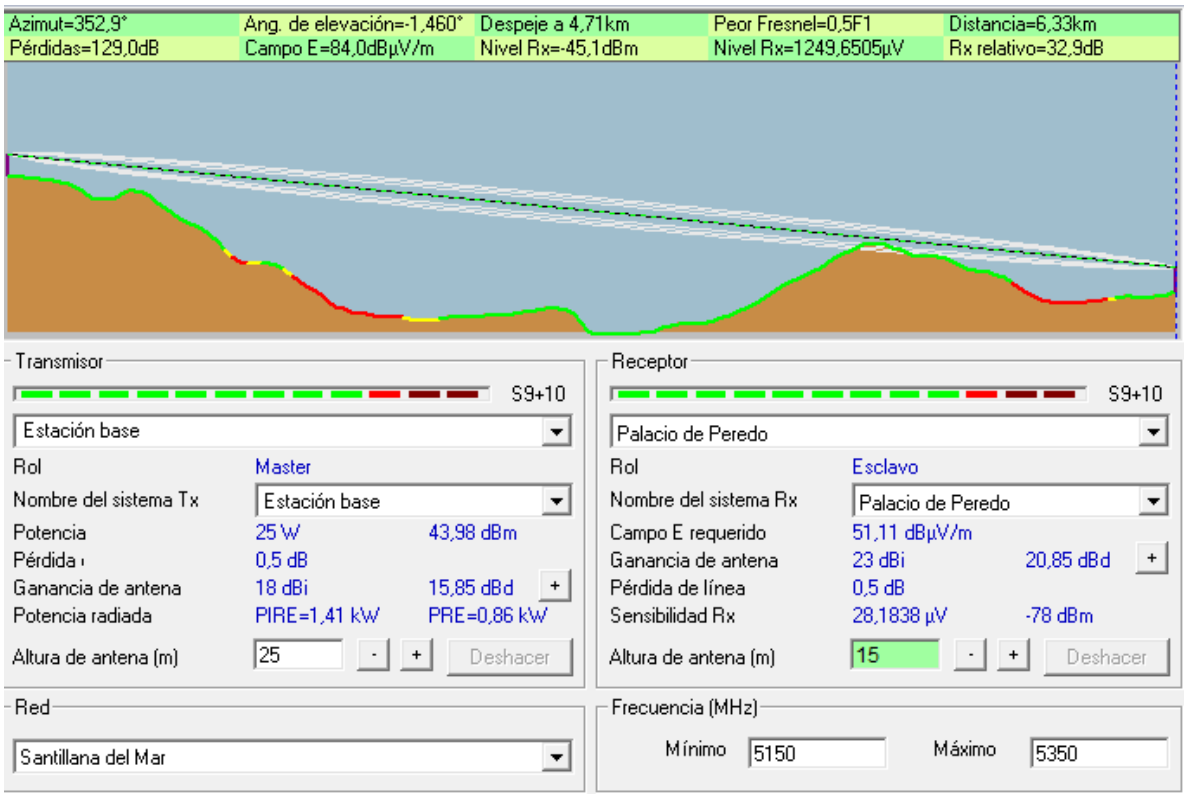


Ilustración 38. Perfil Radioenlace BTS del operador → Palacio de Peredo

- Angulo de elevación: Inclinación respecto al eje horizontal que ha de sufrir la antena (1.460°)
- Peor ángulo de Fresnel para este trayecto (0.5F1)
- Distancia en línea recta entre dispositivos (6.33 km)
- Pérdidas del espacio libre entre el emisor y receptor (129 dB)
- Rx Relative: Señal relativa en dB con respecto a la sensibilidad del sistema receptor (32.9 dB)
- Nivel Rx: Nivel de potencia recibida (45.1 dBm)

Según los datos que ofrece Radio Mobile, podemos concluir que dicho enlace es completamente viable. No obstante, en caso de que esta propuesta se llevara a cabo, en el momento en el que el técnico realizase la instalación del CPE en el Palacio de Control resultaría conveniente acudir al emplazamiento, para que una vez instalado se realicen las pruebas necesarias para corroborar la viabilidad de dicho enlace y por lo tanto el correcto funcionamiento y recepción de la señal que será nuestra vía principal de acceso a Internet. De esta forma, se podrá acceder a cada uno de los puntos de acceso que conforman la red pudiendo conectarse los usuarios con el fin de disfrutar del servicio ofrecido.

3.5.2. Estudio de cobertura de la red Mesh

Para cubrir la zona objeto del proyecto, a través de la red Mesh, se ha utilizado el software de simulación Ekahau Site Survey. Para la realización de la simulación Mesh, se ha tenido en cuenta el estándar 802.11n en la banda de 5 GHz, utilizando una antena omnidireccional con una ganancia de 4 dB. Esto es condicionante a la hora de elegir el equipamiento necesario para el proyecto, ya que las imágenes que se muestran a continuación nos dan una estimación del nivel de señal y los puntos de acceso a instalar con dichas características.

En cuanto a las simulaciones ofrecidas por este Software, representan las zonas de cobertura en las cuales el usuario podrá conectarse a la velocidad máxima permitida en función del estándar que implemente su tarjeta inalámbrica.

Para la simulación de la red Mesh, es deseable que exista un cierto grado de solapamiento entre las zonas de influencia de los diferentes puntos de acceso, de tal forma que los radioenlaces se establezcan de forma efectiva entre todos los APs permitiendo en caso de fallo de un punto encontrar caminos alternativos para que los paquetes lleguen a su destino.

A continuación se detalla el mapa de cobertura Mesh de las zonas incluidas en el despliegue. Para cubrir la zona y que todos los puntos de acceso queden enlazados a través de radio enlaces de una forma eficiente, se ha considerado la instalación de un total de quince puntos de acceso. En las siguientes imágenes se muestra el nivel de señal y los emplazamientos pensados para la instalación, siempre teniendo en cuenta que la ubicación definitiva se hará efectiva una vez se haga el replanteo in-situ.

Ilustración 39. Ubicación de los Puntos de Acceso-Red Mesh

A continuación se muestra el nivel de señal que se espera recibir en el municipio de Santillana del Mar.

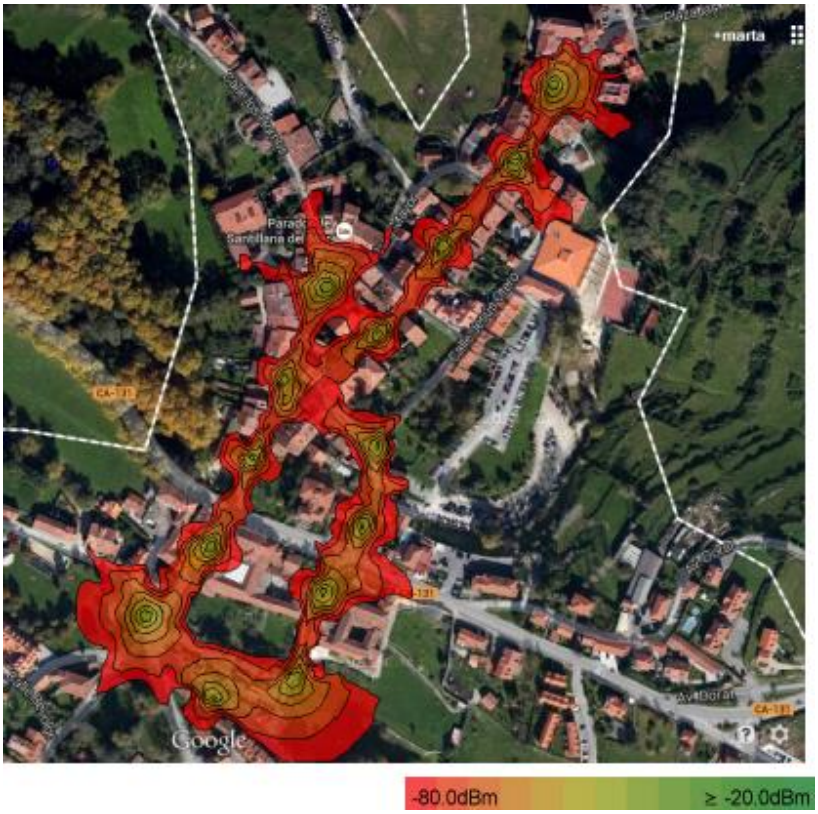


Ilustración 40. Nivel de señal esperado- Red Mesh

Para facilitar la visualización del nivel de señal y las ubicaciones de los puntos de acceso, se ha dividido en dos zonas el conjunto total del municipio.

Parte Norte

Ilustración 41. Ubicación APs Parte Norte- Red Mesh

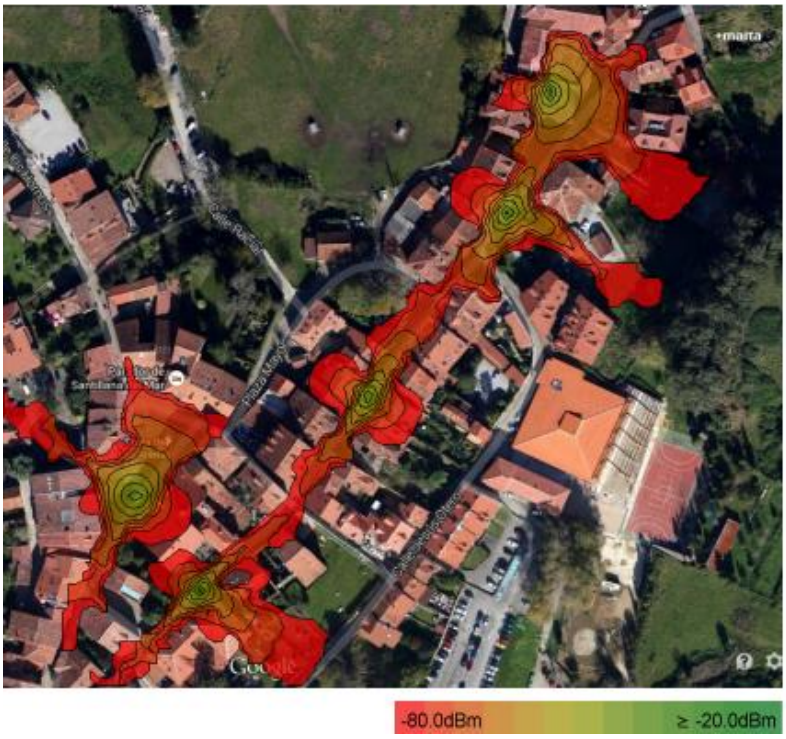


Ilustración 42. Nivel de señal esperado Parte Norte - Red Mesh

Parte sur

Ilustración 43. Ubicación APs en la Parte Sur – Red Mesh

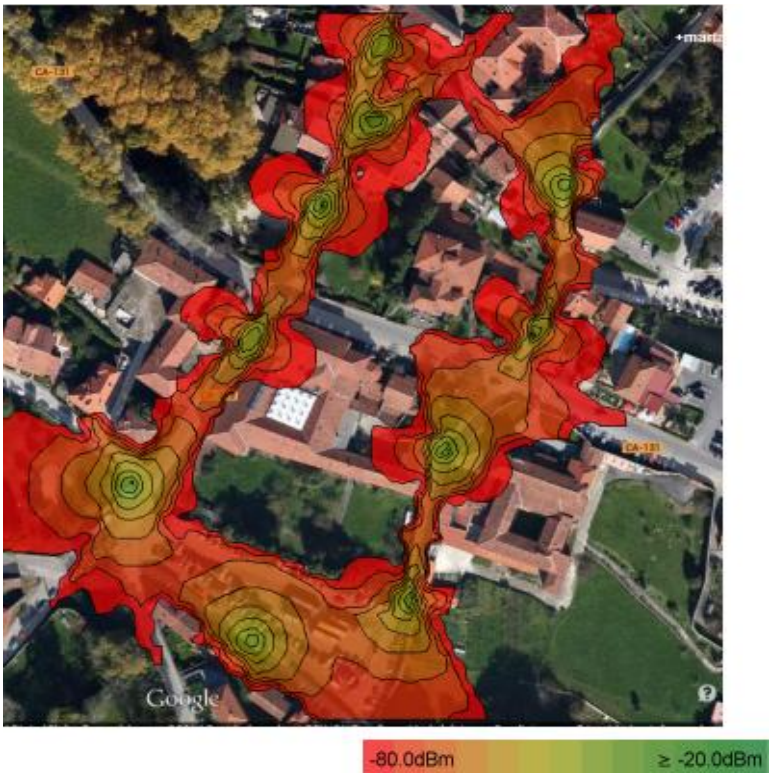


Ilustración 44. Nivel de señal esperado Parte Sur - Red Mesh

Como observamos, la planificación realizada con Ekahau indica que con los quince APs para la red troncal en 802.11n cubrimos la mayor parte del municipio de Santillana del Mar.

La totalidad de los puntos de acceso estarán colocados en las mismas posiciones que los APs utilizados para la Red WiFi de acceso detallada en el siguiente apartado. Esto nos permite un ahorro importante en los costes ya que se pueden utilizar APs duales en todos los emplazamientos. Esa 'doble banda' hace referencia a la capacidad de transmitir tanto en la banda de 2.4 GHz como en la de 5GHz, evitando la utilización de diferentes equipos para las distintas bandas de frecuencia inalámbrica.

La instalación de los puntos de acceso se realizará en las farolas o postes de luz existentes en el municipio o incluso en los tejados de las viviendas privadas. Además, será necesaria la alimentación continuada de los equipos para que puedan ofrecer el servicio. El proyecto de telecomunicaciones contemplará un apartado específico donde se detallarán los suministros eléctricos y las ubicaciones finales de los APs tras la visita in-situ a Santillana del Mar.

3.5.3. Estudio de cobertura de la red WIFI de acceso

Esta red permitirá el acceso a Internet a los ciudadanos y visitantes del municipio en las principales vías y plazas de Santillana. El estudio de cobertura se ha realizado con el software Ekahau Site Survey utilizando para las simulaciones el estándar 802.11n en la banda de 2.4 GHz y una antena omnidireccional de ganancia 4 dB. Estas características serán condicionantes a la hora de la elección del equipamiento, ya que si se realiza dicha simulación con la precisión y la exactitud requerida se ajustará lo máximo posible a la realidad siendo de tal forma un proyecto muy eficiente.

El estudio de ingeniería indica que con quince puntos de acceso es posible llegar al siguiente mapa de cobertura:

Ilustración 45. Nivel de señal esperado en Santillana del Mar- Red WiFi

Como en el caso anterior, se ha dividido en dos el conjunto total del proyecto para una

mejor interpretación.

Parte Norte

Ilustración 46. Ubicación de APs Parte Norte - Red WiFi

Ilustración 47. Nivel de señal esperado Parte Norte - Red WiFi

Parte Sur

Ilustración 48. Ubicación de APs Parte Sur- Red WiFi

Ilustración 49. Nivel de señal esperado Parte Sur- Red WiFi

Como se indicó en el apartado anterior y como se puede comprobar en las fotografías aéreas los puntos de acceso serán colocados en las mismas posiciones que los APs

utilizados para la red Mesh, reduciendo así notablemente el impacto visual además de los costes al utilizar los puntos de acceso con banda dual como se comentaba anteriormente.

3.5.4. Replanteo

Tras realizar el estudio de pre-ingeniería en el que se detalla la arquitectura de red y un mapa de cobertura de análisis teórico, se ve la necesidad de visitar todo el término municipal para la correcta planificación y dimensionamiento de la red a implantar. Durante la visita a Santillana del Mar, se identificaron los puntos de interés que podían ser utilizados para el despliegue de la red. Los requisitos básicos de las ubicaciones son que fuesen de propiedad municipal o, que en su defecto, fuese factible obtener el permiso para la instalación. Otro de los requisitos que se tuvieron en cuenta en la visita in-situ es que hubiera corriente eléctrica para alimentar a los equipos de forma ininterrumpida. Además, se hizo un estudio radioeléctrico a lo largo del municipio de Santillana, se comprobó cómo podía llevarse a cabo la instalación eléctrica (detallado en el apartado de instalación) y por último, se pactó con el Ayuntamiento una próxima visita para comenzar los trabajos de instalación de la red. Para una mejor coordinación del proyecto, es necesario elaborar un informe en el que se resuman la totalidad de los puntos analizados durante el replanteo. En el documento es recomendable, que entre otras cosas, se muestren las ubicaciones exactas del equipamiento, y la forma en la que se realizará la instalación eléctrica, para facilitar el trabajo, más adelante, a los técnicos que instalarán la red de comunicaciones.

3.5.5. Ubicación geográfica de los puntos de acceso

De todas las ubicaciones recogidas en el replanteo, se han seleccionado aquellas que eran más adecuadas para la realización de los enlaces necesarios. Para que los equipos se enlacen sin problema, se han elegido puntos estratégicos de modo que el enlace de radio tenga visibilidad directa entre antenas, no existiendo obstáculos entre ellas.

A continuación se detalla la ubicación geográfica de los puntos de acceso teniendo en cuenta la ubicación de cada una de las farolas del mobiliario urbano donde se van a instalar los puntos de acceso.

El primer punto de acceso se instalará en el balcón del Palacio de Peredo mientras que el resto se ubicarán en las diferentes farolas del municipio.

Punto de Acceso	Longitud	Latitud
AP1	-4.108943°	43.389382°
AP2	-4.108654°	43.389937°
AP3	-4.108313°	43.390361°
AP4	-4.108634°	43.389665°
AP5	-4.108021°	43.390046°
AP6	-4.107207°	43.390710°
AP7	-4.106670°	43.391224°
AP8	-4.106153°	43.391710°
AP9	-4.107827°	43.389316°
AP10	-4.107928°	43.388811°
AP11	-4.108328°	43.388444°
AP12	-4.108480°	43.387987°
AP13	-4.109060°	43.387583°
AP14	-4.109647°	43.388228°
AP15	-4.109294°	43.388838°

Tabla 13. Coordenadas geográficas de los puntos de acceso

El router ADSL, el CPE de WiMAX y la controladora se ubicarán en el armario Rack en el Palacio de Peredo.

3.5.6. Electricidad de los puntos de acceso

Se debe tener en cuenta que los puntos de acceso necesitan electricidad para poder operar y por lo tanto es necesario disponer de una toma eléctrica donde se coloquen los equipos. En nuestro caso, para el despliegue de los puntos de acceso se utilizarán las farolas del municipio donde se suministrará corriente continua para alimentar los APs. Para ello, se realizará la tirada de cable desde los armarios eléctricos hasta las farolas correspondientes.

Los equipos a utilizar serán equipos de exteriores preparados para soportar un suministro eléctrico exterior continuado y que cumplen con las exigencias recogidas en las leyes vigentes.

En el Palacio de Peredo existen tomas eléctricas, por lo que, para alimentar el primer punto de acceso no habría ninguna dificultad. La mejor opción es utilizar equipos que trabajen con POE.

3.5.7. Líneas de comunicación o salida a Internet

Las líneas de comunicación para dar la salida a Internet se ubicarán en el Centro de Control. Se debe pensar en la necesidad de contar con redundancia en la red en la parte de proveedores; La vía principal de salida a Internet será mediante la tecnología WiMAX que será encargada de ofrecer el servicio de Internet a través de un proveedor, por otro lado, se dispondrá de un router ADSL que servirá como backup y estará a cargo de un segundo proveedor, estando en todo momento atento en caso de que el maestro falle. El router backup se configurará para servir a la vía principal de comunicación en caso de que esta pierda conectividad. Esto se realizará de forma automática de forma que el router backup lo reemplazará y todo el tráfico pasará por dicho router hasta que el maestro recupere la conectividad, el cual cuando se

encuentre operativo volverá a ofrecer servicio.

Esto permitirá que ante la caída de una de las líneas los APs puedan salir por la otra línea, no perdiendo en ningún momento la conexión a Internet.

Se definirá la velocidad de salida básica presupuestada como un servicio dedicado de 10 Mbps simétricos.

3.5.8. Estudio radioeléctrico

El real decreto 1066/2001, establece la necesidad de realizar una medición previa de nivel radioeléctrico antes de la implementación de cualquier tipo de red. El propósito de este estudio consiste en verificar que no sobrepasa el nivel de emisión radioeléctrica, comprobar que no existen otros dispositivos que puedan causar interferencias al implementar nuestra red y establecer la idoneidad del emplazamiento en ese aspecto. Durante el replanteo se realizó un estudio de cobertura in situ así como un análisis de las señales existentes en las bandas de uso WiFI. Esto servirá para realizar un diseño radioeléctrico con el objetivo de usar de forma eficiente el espectro. Se utilizarán canales alternativos entre los diferentes puntos de acceso de forma que puedan existir solapes de cobertura sin interferencias permitiendo al usuario pasar de un punto de acceso a otro de forma transparente. En el apartado de configuración de los equipos se asignarán las frecuencias específicas para cada ubicación con los criterios mencionados. Se utilizarán los canales libres y no utilizados por otras infraestructuras detectadas.

Los APs escogidos no tienen sistemas de protección contra interferencias dinámicos. Por ello, es muy importante analizar bien si existen otras infraestructuras para que no interfieran con nuestra red. Al ser un municipio rural, que apenas cuenta con infraestructura desplegada a lo largo del municipio, no existirá posibilidad de que nuestra red sea interferida por otras.

3.5.9. Equipamiento

Existen una gran cantidad de alternativas a la hora de elegir el equipamiento para la implementación de una red inalámbrica WiFi; Para el despliegue de nuestra red se utilizarán APs de última generación, y para ellos se analizarán productos Ruckus y Mikrotik con el fin de determinar la mejor opción para nuestro diseño. Dicha elección se debe a que son marcas muy reconocidas y que ofrecen atractivas funcionalidades que se acoplan a los requerimientos de la red diseñada.

Los requerimientos del diseño hacen necesaria la adquisición de 15 Puntos de Acceso para cubrir los principales ejes comerciales de la ciudad.

3.5.9.1. Access Points

3.5.9.1.1. Access Points Mikrotik

Mikrotik es una compañía letona que vende principalmente productos para tecnología inalámbrica como RouterBoards o routers para la creación de redes. También es conocida por el Software que lo controla, RouterOS. Mikrotik RouterOS es el principal producto de esta compañía, está basado en Linux y funciona como un Sistema Operativo para convertir un PC o una placa Mikrotik RouterBoard en un router dedicado.

Las principales características que ofrece Mikrotik son las siguientes:

- Potente control de QoS
- Filtrado de tráfico P2P
- Alta disponibilidad con el protocolo VRRP (Virtual Router Redundancy Protocol)
- Vinculación de Interfaces
- Mejoras en las interfaces
- Consume menos recursos
- Avanzada calidad de servicio
- Cortafuegos, túneles
- Puentes STP con filtrado
- Alta velocidad en los estándares 802.11 a/b/g/n inalámbricos con WEP/WAP
- WDS y AP Virtual
- HotSpot para acceder Plug-and-Play
- Telnet/ mac-telnet /ssh/ consola de administración en tiempo real, configuración y monitorización
- Soporte 3G/LTE
- Soporte WPA2

Características técnicas de los puntos de acceso de exterior

Entre la gran variedad de productos de Mikrotik, el modelo de punto de Acceso que podría encajar en la implementación de nuestra red para proporcionar cobertura inalámbrica sería el Mikrotik RB433AH**.**

Ilustración 50. Mikrotik RB 433AH

A continuación se describen detalladamente todas las características y funcionalidades de este modelo de punto de acceso.

- **Características físicas y de alimentación**

Respecto a las tomas de corriente, este modelo de punto de acceso tiene una entrada de cable coaxial para la alimentación de corriente eléctrica, aunque soporta también la alimentación eléctrica por medio de "Power over Ethernet" a través de uno de los interfaces físicos RJ45. El consumo energético de este modelo de punto de acceso es de ~3W sin tarjetas, máximo 25W (18W de salida a tarjetas)

Presentan además indicadores luminosos LED, uno para comprobar si el routerboard está encendido y otro que puede ser programado a opción del usuario. Está iluminado por defecto cuando el routerboard se inicia, cuando se ejecuta el gestor de arranque se apaga.

Por último, tienen un botón de RESET para devolver el punto de acceso a sus valores de fábrica en caso de que resulte necesario.

Las características físicas del punto de acceso le permiten trabajar en unos márgenes de temperaturas de funcionamiento entre -20 y 60ºC. Soportando márgenes de humedad relativa hasta 70%.

- **Interfaces físicas**

Los puntos de acceso presentan hasta 3 radios capaces de trabajar de manera independiente. Soportan los protocolos de red inalámbrica 802.11a/b/g/n según los estándares correspondientes IEEE 802.11a/b/g/n en frecuencias 2.5Ghz y 5Ghz, indistintamente.

De esta manera, cada una de las radios puede ser configurada para trabajar según el protocolo 802.11a, o según los protocolos 802.11b/g/n, o todos ellos simultáneamente. Con respecto a los interfaces cableados, este modelo presenta tres bocas RJ45 para la conexión a redes LAN de 10/100 Mbps, soportando el

descubrimiento automático de la velocidad de la red a la que se encuentran conectados. La boca LAN principal da soporte al dispositivo para su alimentación eléctrica mediante “Power Over Ethernet”.

Según los estándares mencionados y la legislación vigente para la radiación de este tipo de dispositivos, los puntos de acceso trabajan en las siguientes frecuencias y canales de transmisión, con las velocidades indicadas en el siguiente apartado.

- **Modos de transmisión**

    - Modo 802.11a

Para la velocidad de transmisión máxima de 54 Mbps ofrece en las dos bandas de funcionamiento (5,3 y 5,7 GHz) un radio de cobertura máximo de 30 m, con una potencia de emisión de 30 dBm y una sensibilidad de recepción de -67 dBm.

    - Modo 802.11b

Para la velocidad de transmisión máxima de 11 Mbps ofrece un radio de cobertura máximo de 70 m, con una potencia de transmisión de 20 dBm y una sensibilidad de recepción de -87 dBm.

    - Modo 802.11g

Para la velocidad de transmisión máxima de 54 Mbps ofrece un radio de cobertura máximo de 100 m, con una potencia de transmisión de 20 dBm y una sensibilidad de recepción de -75 dBm.

    - Modo 802.11n

Para la velocidad de transmisión máxima de 108 Mbps ofrece un radio de cobertura máximo de 150 m, con una potencia de transmisión de 17 dBm y una sensibilidad de recepción de -90 dBm

Los puntos de acceso seleccionan automáticamente el canal de funcionamiento en el encendido y, posteriormente, tienen la opción de realizar de manera continua un escaneo de interferencias en segundo plano para automáticamente realizar una selección dinámica del canal de transmisión óptimo. También es posible configurar un canal concreto en el que radiará, e incluso permitir la selección dinámica del canal excluyendo de los seleccionables aquellos que se deseen. Es posible utilizar el escaneo continuo en segundo plano para la identificación de intrusos.

También para minimizar las interferencias, ajusta de manera automática la potencia de transmisión. Por otra parte, desactiva la radiación por los interfaces WLAN en caso de encontrar un fallo en las trasmisiones a través de interfaz LAN.

Este modelo de punto de acceso ofrece una capacidad de configuración altamente flexible, para adecuarlo a las necesidades de funcionalidad de la instalación. De esta manera, pueden ser configurados para utilizarse según los modos de operación que se

describen a continuación.

- **Modos de operación**

    - Modo de punto de acceso (infraestructura)

El punto de acceso funciona como tal para ofrecer cobertura inalámbrica a los usuarios finales. Soporta una densidad de hasta 80 usuarios por radio y modo de operación, de manera que puede ser configurado para soportar un máximo de hasta 240 usuarios asociados simultáneamente.

    - Modo Mesh (WDS – Wireless Distribution Systems)

El modo de operación Mesh, también llamado en ocasiones WDS, regula el establecimiento de enlaces inalámbricos entre puntos de acceso. Utilizando este mecanismo, los puntos de acceso son capaces de establecer redes locales inalámbricas en extensiones amplias sin la necesidad de conectar cada punto de acceso a las redes mediante cables, proporcionando además soporte de redundancia para mantener la cobertura y conectividad en caso de caída de algún punto de acceso de la red.

Este modo de operación está pensado para su utilización en entornos exteriores o difíciles de cablear. Por ello, en la instalación propuesta en el caso en el que se decida la utilización de este punto de acceso se utilizará este mecanismo en los APs instalados.

Cada una de las radios que presentan los puntos de acceso puede trabajar simultáneamente para dar soporte a usuarios y para establecer enlaces Mesh. No obstante, se puede mejorar en gran medida la calidad de transmisión en la instalación mediante el uso de una de las radios para el soporte de clientes y la otra para el soporte Mesh, seria de esta manera como se realizaría el despliegue de la red municipal.

    - Modo monitor WLAN

Los puntos de acceso ofertados aprovechan las funciones de escaneo continuo del entorno para proporcionar funcionalidades de monitorización de la red WAN. Mediante estas funcionalidades se proporciona un soporte adicional a la gestión de la seguridad en la red inalámbrica.

Se puede definir y utilizar una lista predefinida de puntos de acceso conocidos y autorizados. En su operación normal, los puntos de acceso son capaces de identificar a otros puntos de acceso que estén radiando en su área de cobertura. A partir de la comparación de la lista de puntos de acceso conocidos y autorizados con la lista de puntos de acceso que se genera con los dispositivos descubiertos, el equipo es capaz de encontrar discrepancias entre ambas listas, realizando así la identificación de puntos de acceso no autorizados (Rogues). Cuando un punto de acceso encuentra un Rogue no deniega directamente la conexión a la red del mismo, pero es capaz de generar TRAPS SNMP indicando la situación, enviándolos a la herramienta de gestión

para que desde esta se efectúen las acciones necesarias.

3.5.9.1.2. Access Points Ruckus

Ruckus Wireless es líder en el mercado de la infraestructura inalámbrica, lo cual permite tanto a prestadores de servicios como a empresas estar a la cabeza de la creciente demanda de aplicaciones y servicios de banda ancha. La tecnología Smart WiFi de Ruckus redefine lo que es posible en el desempeño de redes inalámbricas con flexibilidad, fiabilidad y buen precio. Ruckus define a sus productos como la combinación de características innovadoras necesarias para alcanzar el rendimiento inalámbrico más estable y de mayor velocidad. Los diferentes componentes que son absolutamente esenciales para lograr este nivel de desempeño son los siguientes:

- Control de señal adaptable
- Reducción de interferencia
- Asignación de canales basado en la capacidad
- Diversidad de polarización dinámica
- Intensidad de la señal mejorada
- Optimización de la capacidad de red

Esta tecnología brinda conexiones WiFi de mayor alcance y más confiables a los dispositivos de los clientes; Además, abre paso a las señales entre obstáculos y obstrucciones de forma permanente, reduce la interferencia y concentra la energía de Radiofrecuencia (RF) solamente cuando es necesario asegurar una cobertura sin precedentes y un rendimiento constante a grandes distancias.

Los puntos de acceso de dicha marca se utilizarán en la mayoría de los casos en entornos donde exista una alta densidad de usuarios y una alto grado de interferencias, en entornos donde todo el mundo este compitiendo por acceder a los recursos, entornos donde se necesite extender la cobertura y en entornos donde se necesite una gran escalabilidad en las redes.

Ruckus, como se ha comentado, permite mejorar las prestaciones en entornos de gran intensidad con un gran número de clientes pero también permite mejorar la capacidad de nuestras redes, aunque sea una red pequeña. No pretende competir a través del precio, sino que su base tecnológica es la que le dirige a la hora de fundamentar su negocio.

Entre la gran variedad de productos que ofrece Ruckus el modelo de punto de acceso que podría encajar en la implementación de nuestra red inalámbrica es ZoneFlex7762.

Ilustración 51. Ruckus ZoneFlex7762

Se trata del primer Punto de Acceso que trabaja tanto en la banda de 2.4 GHz como en la de 5 GHz, es decir, de banda dual 802.11n de exterior que integra tecnología de antena adaptativa; Esta tecnología permite habilitar señales de mayor alcance, una mejor penetración de la señal en el interior de los edificios, y conexiones malladas mucho más resistentes que se adaptan automáticamente a las interferencias y a las condiciones ambientales cambiantes del entorno.

Debido a que soporta redes de mallado inteligentes avanzadas, la serie ZoneFlex 7762 de Ruckus es perfecta para los proveedores de servicio que buscan extender rápidamente y de modo asequible los servicios de banda ancha de marca propia, descargar el tráfico de datos de redes 3G congestionadas, implementar zonas de concentración multimedia u ofrecer servicios de banda ancha inalámbrica a lugares donde el acceso de la línea fija es limitado. Tienen radios independientes para el acceso y para el tráfico de backhaul; Y son capaces de ofrecer un alto rendimiento a los clientes en toda la red de malla.

La serie Zoneflex 7762 se puede administrar de manera centralizada por medio del controlador WLAN inteligente ZoneDirector como parte de una LAN inalámbrica para interiores y exteriores, unificada e implementada como AP independiente y administrada de manera individual, o a través del sistema de administración de WiFi remoto FlexMaster.

Esta serie de Ruckus implementa la tecnología de antenas inteligentes BeamFlex patentadas por la propia marca que permiten una cobertura extendida consistente y de alto rendimiento y apoyo multimedia en los entornos RF más exigentes. La gestión dinámica de canales optimiza el rendimiento del cliente al seleccionar el mejor canal para operar en cada momento. Un asistente alojado en la web permite que cualquier usuario de computadora configure la serie ZoneFlex 7762 y cree una WLAN segura y sofisticada en cuestión de minutos.

Algunos de los beneficios que ofrece este producto se comentan a continuación:

- Rendimiento WiFi exterior sin precedentes: Avanzado diseño Wi-Fi con radios 802.11n concurrentes que ofrecen 150 Mbps de rendimiento sostenido entre puntos de acceso con topología mallada de hasta 300 m de distancia y 50 Mbps de rendimiento a clientes hasta 150 metros de distancia.

- La mejor tecnología de selección de canales: La administración de canales dinámica ChannelFly basada en la capacidad, predice y selecciona automáticamente el canal de mejor rendimiento en base a un análisis de capacidad en tiempo real y estadístico de todos los canales RF.

- Protegido contra las condiciones del entorno con energía de CA: Permite el montaje rápido y fácil en postes de alumbrado, control de tráfico y otro mobiliario urbano. Incluye gabinete reforzado para instalación en exterior con calificación de protección IP-67.

- La administración WiFi centralizada y unificada facilita la administración: Zone Director y FlexMaster proporcionan una vista detallada y control sobre los AP WiFi inteligentes tanto interiores como exteriores lo que permite la administración continua y de todo el sistema del entorno inalámbrico completo.

- Capacidad y confiabilidad de WiFi inigualables: La antena adaptativa BeamFlex junto con la tecnología para la mitigación de interferencias emite hasta 6 dB de ganancia de señal adicional y hasta 15 dB de mitigación de interferencia y soporte para 500 clientes

Además de contar con características físicas y de alimentación muy similares a las de otros puntos de acceso, así como las interfaces físicas y los modos de transmisión que soporta (802.11a, 802.11b, 802.11g y 802.11n, con velocidades máximas de transmisión de 54 Mbps, 11 Mbps, 54 Mbps y 130 Mbps (20MHz) y 300 Mbps (40 MHz), este modelo de punto de acceso destaca por otras muchas técnicas que se detallan a continuación y que hacen ser sobresaliente y muy eficaz a dicho punto de acceso para redes de comunicaciones inalámbricas.

Como se ha comentado anteriormente, ZoneFlex 7762 es un punto de acceso que cuenta con tecnología de antena adaptativa. A través de dichas antenas, el equipo es capaz de reforzar la señal en la dirección que se determine; Se necesita un conocimiento previo del canal para estimar como es ese canal y donde se encuentra el receptor y se dirige un ancho de haz en una dirección concreta de forma que se refuerza el nivel de potencia en la dirección que deseemos, haciendo mucho más óptimo el rendimiento de nuestra red.

Cuenta con antenas integradas para conseguirlo. A través de un algoritmo software el equipo controla que antenas se tienen que activar en cada momento para cada cliente con el objetivo de proporcionar el flujo óptimo para ese cliente en ese determinado momento. Esto tiene muchas ventajas pero también presenta inconvenientes. Inconvenientes: El algoritmo es muy complejo. Ventajas: Para cada cliente se personaliza un diagrama de cobertura para cada una de las transmisiones. Nos proporciona una mayor ganancia en determinadas direcciones, además de mejorar la relación señal/ruido nos permite aumentar la cobertura de nuestra red. Todo el ruido

que venga de la zona donde no está confinada nuestra energía se va a rechazar. Cuenta con 15 dB de rechazo de ruido.

El punto de acceso además, tiene en cuenta cual es la polarización óptima (vertical u horizontal) según la posición en la que se encuentre el dispositivo del cliente.

Otro método que utilizan los puntos de acceso Ruckus para mejorar las prestaciones es el balanceo de clientes. A través de estimaciones de medidas de canales el punto de acceso es capaz de hacer un equilibrio y los que tenían más capacidad libre acogen más clientes para que se queden todos por igual.

Band Steering es lo mismo que el balanceo de clientes pero entre bandas. Normalmente los clientes se van a asociar a los puntos de acceso de la banda de 2.4 asegurando que el cliente tenga una capacidad mínima de conexión sin perder prestaciones para cada cliente individual. Va a hacer que los clientes miren de una banda a otra en cada punto de acceso de tal forma que se igualen los canales que cada uno consumen y por tanto el rendimiento de la red será mucho mayor.

Otra característica que hace más efectivo a este modelo de punto de acceso es Airtime Fainess que se refiere a la igualdad en el tiempo de uso de la red. Si ponemos a los usuarios en la cola y vamos dando acceso al canal en función del tiempo de llegada se penaliza a los usuarios rápidos sin que los lentos estén viendo mejoras significativas en su rendimiento. Este método, intenta maximizar el rendimiento conjunto. Para ello, no penaliza a los usuarios rápidos asignándoles más tiempo en el canal y retrasa o controla a los usuarios lentos de forma que su rendimiento que es lento de por si no va a empeorar mucho más. Se prioriza a los usuarios rápidos, se mide la capacidad y rendimiento de cada uno y se asigna slot de canal en función de eso.

En entornos de alta interferencia utilizamos DFS (Dinamyc Frecuency Selection 'Selección Dinámica de Frecuencia'). Cuando hay un canal menos saturado hace que el dispositivo conmute y trabaje en esa frecuencia. ChannelFly es una función opcional del sistema Ruckus ZoneFlex que monitoriza desde arriba todos los canales en cada punto de acceso; Está viendo continuamente el tráfico que circula por cada punto y la capacidad real que hay en cada canal. Cada punto de acceso negocia con clientes para que en función de la capacidad que necesiten esos clientes de transmitir pasarlos de un canal a otro, mejorando el rendimiento no solo de los clientes si no el rendimiento conjunto de la red.

En entornos de alta cobertura también podemos aprovechar las prestaciones de Ruckus por lo que denominamos el Smart Mesh. Nos permiten conectar puntos de acceso a la red sin necesidad de cablearlos hasta un máximo de 8 saltos aunque como sabemos, al realizar cada salto perdemos ancho de banda. Nos permite ampliar la cobertura de nuestras redes de forma muy fácil. No hay que configurar nada, teniendo un Zone Director, sólo con encender un nuevo AP, automáticamente el sistema lo detectará y lo preconfigurará. En caso de caída de un AP, la red utilizará caminos óptimos con la finalidad de autoreparar la red en caso de un fallo en la misma.

3.5.9.2. Conclusión y selección

Una vez analizado y estudiado los dos modelos de punto de acceso que se han considerado oportunos para la implementación de nuestra red inalámbrica llega la hora de decidir cuál es el que mejor se adapta a las necesidades de nuestra red.

Los requisitos necesarios de los dispositivos para su uso en una zona rural como es Santillana del Mar son:

- Bajo consumo. Es importante que el hardware usado tenga un consumo reducido.
- Bajo coste. No se pueden implementar soluciones de un alto costo que no sean sostenibles por la localidad de Santillana del Mar.
- Reducido tamaño. De esta forma se asegura que el diseño final sea lo más compacto posible.
- Robusto ante condiciones meteorológicas adversas. Ya que los dispositivos se instalarán en el exterior es necesario que tengan una cierta robustez en cuanto a condiciones extremas de temperatura y humedad.
- Tipo de procesador. El punto de acceso debe contar con un procesador lo suficientemente potente para poder realizar las tareas que se le exijan.
- Rangos y tipos de alimentación. Por razones de flexibilidad es recomendable que el AP cuente con un rango variable de alimentación. Es recomendable que la placa seleccionada tenga la opción de poder ser alimentada a través de PoE (Power over Ethernet)
- Disponibilidad de watchdog. Se recomienda la existencia de un watchdog hardware que permita reiniciar la placa cuando ésta se bloquee.
- Disponibilidad de compra a medio/ largo plazo. Este requisito resulta especialmente importante, ya que es necesario asegurar de alguna manera que el hardware seleccionado va a seguir siendo distribuido a medio o largo plazo. Es más que recomendable tener posibles alternativas localizadas en caso de que sea necesario llegar a usarlas.

Tanto los equipos de Mikrotik como los de Ruckus se acoplan perfectamente a los requerimientos del diseño. Haciendo una comparación entre ellos para determinar cuál se adapta mejor a nuestra red obtenemos:

- El modelo de punto de acceso Mikrotik 433AH tiene un coste mucho menor que el modelo de punto de acceso Ruckus ZoneFlex 7762. El coste aproximado del AP Mikrotik es de 130,00 € mientras que el Ruckus tiene un coste

aproximado de 1500,00 €.

- El equipo 433AH ofrece una velocidad máxima de transmisión de hasta 108 Mbps, mientras que ZoneFlex 7762 ofrece una velocidad máxima de 130 Mbps para 20 MHz y 300 Mbps en 40 MHz.
- El modelo Ruckus además de contar con muchas de las características que ofrece el modelo Mikrotik añade otras características muy llamativas que harán de nuestra red una red eficiente, flexible, fiable y con un alto rendimiento.
- ZoneFlex 7762 tiene unas dimensiones mayores que los equipos Mikrotik.
- Ambos puntos de acceso tienen arquitectura MIPSBE basada en un procesador integrado con una CPU de 680 MHz.

Santillana del Mar es un municipio rural que no cuenta con una cantidad elevada de usuarios además que no se caracteriza por tener un alto grado de interferencias ya que apenas existe espectro ocupado en las vías, plazas y parques del municipio. El modelo Ruckus suele utilizarse más a menudo para redes donde exista una alta densidad de usuarios y un alto grado de interferencias. Debido al alto coste que supondría en el proyecto utilizar los productos Ruckus, además de que sus dimensiones son mayores que las del Mikrotik y que para nuestra red no es necesario que los equipos soporten tal cantidad de usuarios, optamos por elegir como puntos de acceso de nuestra red los equipos **433AH**. Dichos equipos cumplen perfectamente las expectativas y los requerimientos para nuestra red ofreciendo además una relación calidad-precio muy buena. Con estos puntos de acceso podemos implementar una red flexible, segura, eficiente y con un elevado rendimiento.

3.5.9.3. Características técnicas del equipamiento de la solución propuesta

A lo largo del presente apartado, se detallarán las características técnicas más relevantes de cada uno de los elementos claves que compondrán los puntos de acceso de nuestra red.

Los productos a analizar son los siguientes:

- Mikrotik RouterBoard RB433AH 128 MB
- Mikrotik MiniPCI Card R52N 802.11ABGN 100/200 mW 300 Mb/s MMCX
- Pigtail 2.4 a 5 GHz. MMCX-N Jack BulkHead 18 cm
- Antena omnidireccional WRL-MTO-247
- Antena omnidireccional WRL-MTO-5085

Se utilizarán por lo tanto 15 APs Mikrotik RouterBoard 433AH que se instalarán como se explica en el apartado 4.4.2 a lo largo del municipio de Santillana. Cada uno de los cuales soportará un promedio de 50 usuarios simultáneos; Se usarán los tres canales no solapados y por lo tanto pueden ocupar la misma área sin interferirse entre sí. Los canales a ocupar serán normalmente el 1, 6 y 11 y serán seleccionados en el momento de la configuración de los equipos.

Además de los RouterBoards, es necesaria la utilización de otro tipo de equipamiento para conformar nuestra red.

Como sabemos RB433AH dispone de tres ranuras miniPCI y tres puertos Ethernet que ofrecen suficientes opciones de conectividad como para utilizar dicho RB como parte central de nuestra red.

En nuestro caso, el modo de transmisión que utilizaremos será el modo 802.11n. Por lo tanto se ha pensado en la utilización de tarjetas radio mini PCI Mikrotik R52N-M

Ilustración 52. Mini PCI R52N-M

Dicho adaptador MiniPCI RouterBoard R52n ofrece el rendimiento líder en el estándar 802.11a/b/g/n tanto en la banda de 2.4 GHz como en 5GHz, soportando 300 Mbps de velocidad y hasta 200 Mbps de flujo real tanto en subida como en bajada. Cuenta con dos conectores de antena MMCX. Al añadir Wireless N a nuestro dispositivo Wireless, aumenta la eficiencia en las aplicaciones diarias como la transferencia de ficheros, navegación en Internet y media streaming. Las especificaciones de dicho producto se pueden encontrar en el Anexo B.

Según el diseño de nuestra red, para realizar los enlaces que interconectarán todos los puntos de acceso desplegados a lo largo del municipio, será necesario utilizar dos tarjetas R52n, mientras que para dar acceso WiFi será necesario una única tarjeta R52n. Por lo tanto, cada RB433AH llevará incorporado tres MiniPCI R52n**.**

Serán necesarios cuatro Pigtails MMCX que irán conectados a las tarjetas radio y que servirán para conectar las antenas que serán las encargadas de emitir y recibir ondas electromagnéticas hacia el espacio libre en la red.

Los pigtails tienen un tipo de conector MMCX a N hembra. Por lo que será necesario que las antenas dispongan de conector N- macho, o en caso contrario se necesitará un conector específico para que se conecten adecuadamente.

Ilustración 53. Pigtail MMCX - N

En la siguiente imagen se muestra el punto de acceso con los componentes necesarios

Ilustración 54. Punto de Acceso Mikrotik

3.5.9.4. Teoría básica de antenas

Debido a la diversidad de ambientes en los que habrá que proveer cobertura, así como los diferentes estándares que debe soportar la red, se hace necesario el empleo de diferentes antenas para dar la mejor cobertura posible y minimizar el impacto visual.

La elección de antenas tiene gran importancia en la configuración de la red inalámbrica ya que serán las encargadas de distribuir la señal en las áreas a cubrir.

El rendimiento de las antenas está determinado por una serie de parámetros como son la polarización, la orientación, el diagrama de radiación, ancho de banda, directividad, ganancia, el VSWR o ROE, etc.

Se denomina ROE o VSWR (Razón o Relación de ondas estacionarias) a una medida de la energía enviada por el transmisor que es reflejada por el sistema de transmisión y vuelve al transmisor. Un valor de VSWR de 1:1 es perfecto (no hay reflejo de la energía). Los valores típicos de ROE en las antenas suelen estar en torno a 1.5:1 - 2:1, lo cual indica que el VSWR tiene el doble de voltaje reflejado que el enviado; La pérdida real de la radiación es de un 10% lo que equivale una reducción de la señal de

0.5 dB. Para conseguir que la ROE sea lo más cercana posible a su valor ideal, hay que tratar de conseguir la adaptación de impedancias entre la antena y el conector.

Para conseguir que los usuarios reciban la máxima potencia de señal se emplearán antenas capaces de radiar con polarización tanto vertical como horizontal, aunque actualmente la mayoría de las tarjetas inalámbricas del mercado permiten trabajar con ambas polarizaciones.

La polarización de una antena describe la orientación de los campos electromagnéticos que irradia o recibe la antena. Además de la polarización vertical y horizontal que son las más comunes existen también la circular y la elíptica.

- Polarización vertical: Cuando el campo eléctrico generado por la antena es vertical con respecto al horizonte terrestre (Va de arriba a abajo)

- Polarización horizontal: Cuando el campo eléctrico generado por la antena es paralelo al horizonte terrestre.

- La polarización circular se representa cuando dos componentes ortogonales tienen exactamente la misma amplitud y están desfasadas exactamente 90°, el campo eléctrico generado por la antena va rotando de vertical a horizontal, y viceversa, creando movimientos circulares en todas direcciones.

- La polarización es elíptica cuando el campo eléctrico se mueve como en la polarización circular pero con desigual fuerza en las distintas direcciones. Generalmente, este tipo de polarización no suele ser intencionado.

Idealmente, la polarización de las antenas de ambos extremos de la comunicación debe ser la misma para minimizar la pérdida de ganancia.

Una característica importante en las antenas es su ganancia. La ganancia viene a ser el grado de amplificación de la señal. Representa la relación entre la intensidad de campo que produce dicha antena en un punto determinado y la intensidad de campo que produce una antena isotrópica en el mismo punto y en las mismas condiciones. Una antena tiene mejores prestaciones cuanto mayor sea su ganancia. En nuestro punto de acceso se incluirán antenas externas que conseguirán que la energía radioeléctrica llegue bastante más lejos.

A la hora de realizar el diseño de la red habrá que tener en cuenta las posibles fuentes de interferencia que provoquen la dispersión de la señal. Las principales fuentes de interferencia a tener en cuenta serán las superficies metálicas, muros de hormigón, escaleras,…. Este tipo de superficies provocan reflexiones de la señal, habrá veces que estas reflexiones favorezcan la difusión de la señal (reflexiones constructivas) y otras en las que provoquen la anulación de la señal (reflexiones destructivas).

Otro factor que influye en la calidad de recepción entre los terminales de usuario y los puntos de acceso será si existe o no línea de vista entre ambos dispositivos:

- **Línea de vista (LOS-Line Of Sight)**, en un canal de radio de un sistema de comunicaciones inalámbrico es descrito como la señal que viaja a través de un camino directo y sin obstrucciones desde el transmisor hasta el receptor. Un enlace LOS requiere la mayor parte de la primera zona de Fresnel esté libre de obstrucciones, como se observa en la Ilustración 55. Si no se cumple este requerimiento existirá una reducción significativa de la intensidad de la señal.

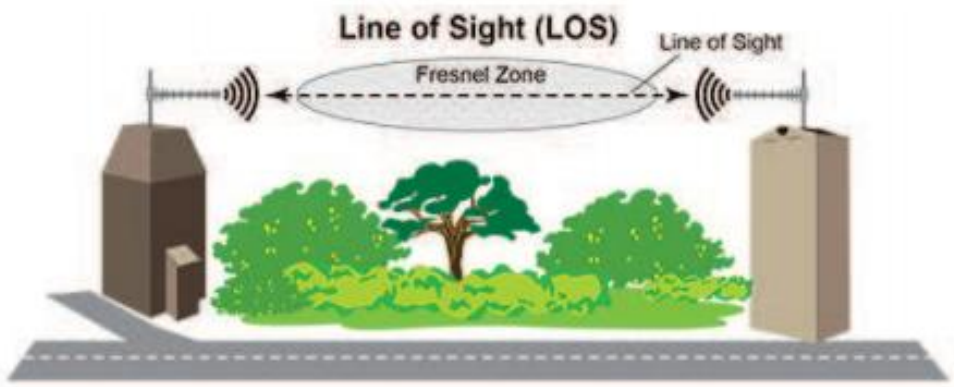


Ilustración 55. Línea de vista (LOS)

Fuente. Netkrom Group,2005.

- **Sin línea de vista (NLOS- Non Line of Sight),** las obstrucciones son completas entre las dos antenas, por lo cual la antena puede ser reflejada, refractada, absorbida, o dispersos como se observa en la figura. En consecuencia, los sistemas inalámbricos desarrollados para el entorno NLOS tienen que incorporar una serie de técnicas para superar este problema.

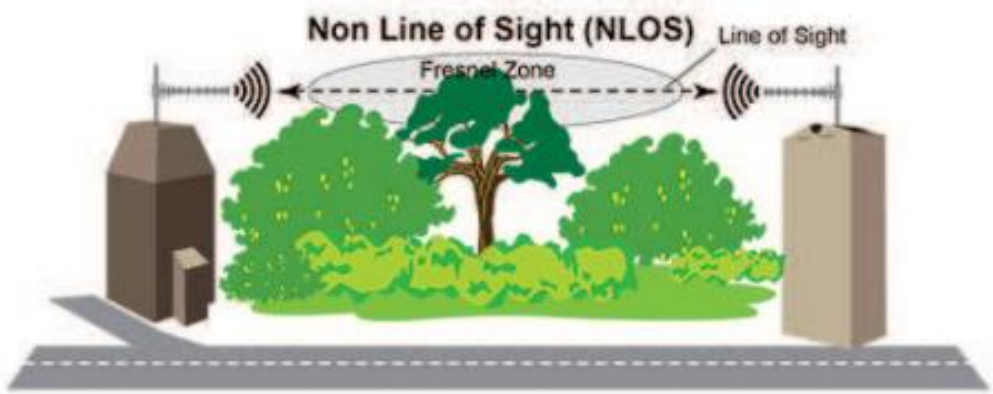


Ilustración 56. Sin línea de vista

Fuente. Netkrom Group,2005.

Zona de Fresnel

Se denomina zona o elipsoide de Fresnel a la propagación de la radiación, por donde viaja la mayor parte de la energía entre transmisor y receptor.

Las ondas de radio reflejadas por los objetos pueden llegar fuera de fase con la señal que viajó directamente a la antena de recepción reduciendo así la potencia de la señal recibida, como se observa en la Ilustración 57. Esta zona se extiende por encima y por debajo de la línea recta entre el emisor y el receptor, y para que se considere útil debe mantener alrededor del 60% de esa zona totalmente libre de obstáculos.

La constante establece lo siguiente:

$$r = 17.32\sqrt{\frac{D}{4f}}$$

- R= radio (M)
- D=distancia del enlace (Km)
- f= frecuencia del enlace (GHz)

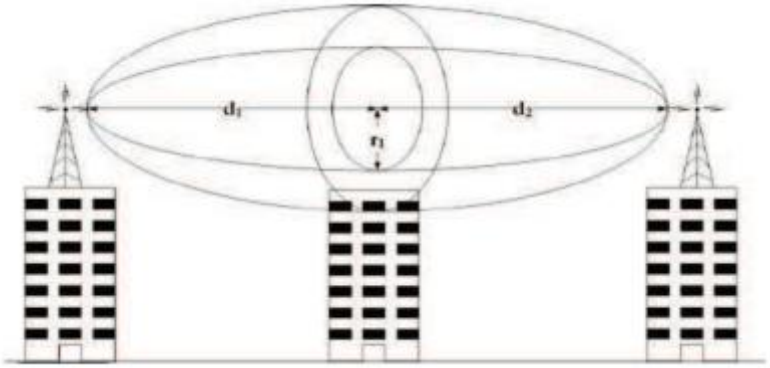


Ilustración 57. Zona de Fresnel

Fuente. Netkrom Group,2005.

3.5.9.4.1. Diversidad de antenas

Los puntos de acceso a instalar presentan 4 conectores de antena los cuales por medio de ellos podremos conectar antenas externas con gran ganancia que incrementarán el área de cobertura para interiores y exteriores. Existen dos tipos de antenas que se utilizan para redes inalámbricas, antenas omnidireccionales y antenas direccionales o sectoriales.

- **Antenas omnidireccionales**

Las antenas omnidireccionales son aquellas que radian en todas direcciones y también pueden captar la señal procedente de todas las direcciones. Proveen un área de cobertura de 360˚ en el plano horizontal y suelen cubrir unos 10 metros en el plano vertical. Están ideadas para cubrir superficies diáfanas. A continuación se muestra el

diagrama de radiación omnidireccional.

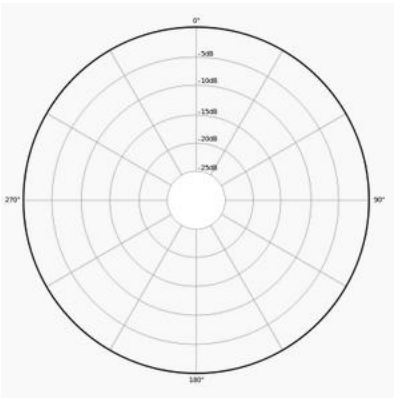


Ilustración 58. Diagrama de radiación de una antena omnidireccional

Las antenas más habituales son las conocidas como dipolo. Un dipolo emite su señal haciendo que la energía se propague paralela al dipolo y perpendicular al suelo (polarización vertical). Si se girase la antena 90 grados, se obtendría una antena de polarización horizontal. Ambos modelos son posibles aunque para cada caso particular un modelo puede funcionar mejor que el otro.

- **Antenas direccionales**

Las antenas direccionales concentran la mayor parte de la energía radiada en una sola dirección creando una estructura cónica y aumentando así la potencia emitida hacia el receptor o desde la fuente deseada y evitando interferencias introducidas por fuentes no deseadas. Las antenas direccionales son ideales para zonas alargadas, esquinas, etc. Cuanto más direccional es una antena, mayor es su alcance. Existen muy distintos modelos de antenas direccionales entre los que destacan las antenas Yagui, las antenas panel y las parabólicas.

Un ejemplo de diagrama de radiación de una antena direccional es el mostrado en la Ilustración 59.

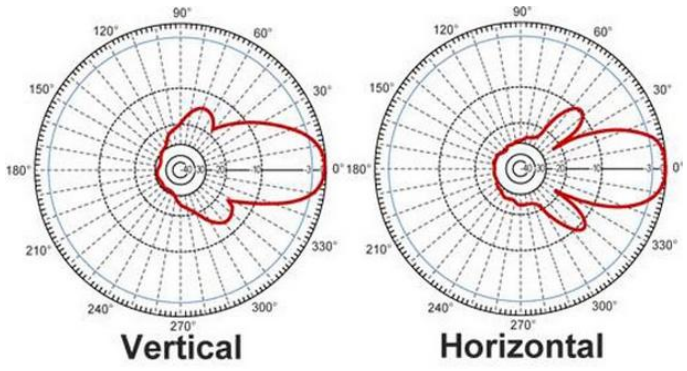


Ilustración 59. Diagrama de radiación de una antena direccional

3.5.9.4.2. Antenas a utilizar en el proyecto

El punto de acceso a instalar no presenta antenas omnidireccionales integradas por lo que para incrementar el área de cobertura se conectarán antenas externas que se encargarán de emitir y recibir las ondas electromagnéticas hacia el espacio libre.

En cada punto de acceso se instalarán cuatro antenas omnidireccionales:

- Dos antenas WRL-MTO-247 omnidireccionales de 7.5 dBi 2.4 GHz que se conectarán a una de las tarjetas radio que servirá de acceso.
- Para realizar los enlaces con los puntos de acceso vecinos y que queden interconectados se utilizarán dos de las tarjetas radio a las cuales se conectará una antena WRL-MTO-5085 de 8.5 dBi 5GHz por cada tarjeta radio.

La explicación de porqué utilizar dos antenas MTO-247 es la siguiente: Las miniPCI montadas en los equipos RB433 trabajan sobre el estándar 802.11n. Como sabemos dicho estándar trabaja con MIMO (Multiple Input Multiple Output), el cual se basa en la utilización de varias antenas para transportar múltiples flujos de datos de un lugar a otro, consiguiendo transmitir un volumen mayor de datos en el mismo período de tiempo. En nuestro caso se utiliza la tecnología MIMO 2x2 que indica la disponibilidad de dos antenas emisoras y otras dos en el extremo receptor. Por lo tanto, para aprovechar esta tecnología y crear una red mucho más eficiente, se usan dos antenas en cada radio que además aumentan la distancia a la que se puede mantener una determinada velocidad de datos.

Las antenas externas que se integrarán en el RB433AH se detallan a continuación.

- **Antena omnidireccional WRL-MTO-247 de 2.4 GHz y 7.5 dBi de ganancia.**

La antena omnidireccional MTO-247 es una antena de alto rendimiento fabricada por MTI Wireless Edge diseñada para puntos de acceso WiFi en la banda 2.4 GHz. Están preparadas completamente para funcionar en condiciones de intemperie extrema y proporcionar años de funcionamiento libre de errores.

Ilustración 60. Antena omnidireccional WRL-MTO-247

La antena es ligera y cumple los requisitos ETSI, es fácilmente instalable ya que se integra directamente en el equipo gracias a su conector N-macho. Es un producto muy estético y tiene una base de aluminio con protección.

Algunas especificaciones se muestran en la siguiente Tabla.

Rango de Frecuencia	**2.4 -2.5 GHz**
Ganancia	**7 dBi**
Espectro de cobertura horizontal	**360°**
Espectro de cobertura vertical	**21°**
Polarización	**Vertical**
Impedancia	**50 Ω**
Máxima entrada de potencia	**6 Watt**
VSWR	**< 1.5 : 1**
Peso	**0.5 Kg**
Tamaño	**28 x 337 mm**
Temperatura de operación	**-45 a +70 ° C**

Tabla 14. Especificaciones Antena WRL-MTO-247

- **Antena omnidireccional WRL-MTO-5085 de 5 GHz y 8.5 dBi de ganancia**

Las antenas omnidireccionales de 5 GHz fabricadas por MTI Wireless Edge ofrecen una excelente relación calidad-precio para aplicaciones de larga distancia. Estas antenas están preparadas completamente para funcionar en condiciones de intemperie extrema y proporcionar años de funcionamiento libre de errores.

Ilustración 61. Antena omnidireccional WRL-MTO-5085

La antena ofrece un alto rendimiento, mantiene una estética de calidad, es muy ligera y fácilmente instalable gracias a su conector N-macho. Las especificaciones eléctricas más destacables se muestran a continuación en la tabla.

Rango de frecuencia	5.470 – 5.875 GHz
Ganancia	8.5 dBi
Espectro de cobertura horizontal	360°
Espectro de cobertura vertical	10°
Polarización	Vertical
Impedancia	50 Ω
Máxima entrada de potencia	4 Watt
VSWR	< 1.7 : 1
Peso	0.5 kg
Tamaño	16 x 337 mm
Temperatura de operación	-45 a +70°C

Tabla 15. Especificaciones Antena WRL-MTO-5085

3.5.9.5. Características de los sistemas centrales

A continuación se muestra el esquema de red, con los elementos que formarán el centro de control de la red y que serán ubicados en el Palacio de Peredo en el municipio de Santillana del Mar.

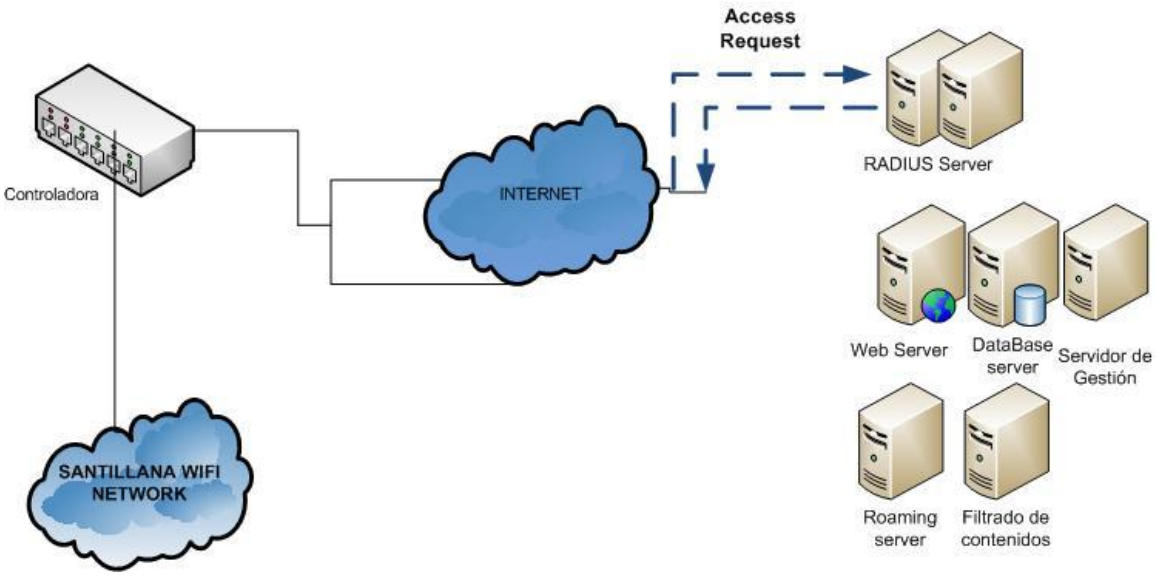


Ilustración 62. Esquema de red Sistemas Centrales

Los dispositivos que componen la red son los que se detallan a continuación.

❖ **Servidor RADIUS**

El servidor RADIUS, es una de las herramientas más completas del mercado, pues a diferencia de los convencionales que sólo ofrecen Autorización y Autentificación, este servidor incluye una tercera función, el Accounting (contabilización), por eso se denominan "AAA" o "Triple A". La descripción que ofrece el servidor RADIUS en cada una de las fases se describe a continuación.

Autentificación: En esta fase básicamente se responde a la pregunta ¿quién es el usuario? Es un proceso por el cual se determina si un usuario tiene permiso para acceder a la red. Antes de admitir el usuario a la red, se comunica con el servidor RADIUS para verificar la identidad que declara una persona o máquina. Esta autentificación puede realizarse mediante el clásico sistema de usuario/contraseña (que es lo que se utilizará en nuestro sistema para la validación pública estándar) o mediante otros sistemas como puede ser el uso de certificados digitales, contra servidores de Active Directory, o la dirección MAC de un equipo, entre otros.

Para permitir la autentificación de un usuario, se tiene en cuenta si ese usuario ya se ha dado de alta en el sistema y si está en ese momento conectado. Si el usuario está conectado vía WiFi, no se puede conectar de nuevo al sistema. Sólo se permite, con usuarios estándar una conexión simultánea por usuario.

Autorización: El proceso de autorización responde a la pregunta ¿A qué servicios puede acceder el usuario? Durante esta fase del funcionamiento del protocolo se decide qué puede hacer un usuario autentificado en el sistema. En los sistemas RADIUS como parte más importante le indica al servidor NAS (el controlador) el tiempo de conexión que tiene un cliente autentificado, sus fechas de caducidad, los privilegios que tiene, etc.

Contabilización: Durante este proceso se responde a la pregunta ¿qué uso hace el usuario de los servicios? Es una fase que se inicia justo después de que el cliente haya sido autorizado a usar un recurso de la red. Se refiere a realizar un registro del consumo de recursos que realizan los usuarios.

Para finalizar, dígase que en lo que respecta a seguridad WiFi, los servidores RADIUS, además de autenticar y autorizar el acceso de usuarios añaden otras ventajas muy relevantes:

- A diferencia de las VPN, protegen la capa 2 (capa de enlace), pues cifran el canal antes de que el usuario sea autenticado y reciba su IP; mientras que la VPN necesita una dirección IP para autenticar al usuario.
- El servidor RADIUS genera claves dinámicamente, lo que mitiga significativamente las deficiencias del protocolo de encriptación WEP.

La solución que se propondría en el caso en el que el proyecto se ejecutase sería la instalación de dos servidores RADIUS en modo activo-activo, que divide de la manera más equitativa posible el trabajo, para evitar así los denominados cuellos de botella y la indisponibilidad del servicio.

- **Base de datos y servidor Web**

Para poder utilizar de la manera más eficiente posible el servidor RADIUS, será necesario disponer una base de datos donde se almacene la información relativa a los accesos, que cumpla en todo momento con la ley de protección de datos. Esta base de datos está dada de alta en la Agencia de Protección de Datos según los protocolos de seguridad de la LOPD.

Además, con el propósito de alojar las páginas de validación o portal captivo para el servicio público de acceso a Internet se diseñará un servidor Web.

- **Controladora MIKROTIK ROUTERBOARD RB1200**

RB1200 dispone de 10 puertos individuales Gigabit Ethernet, cinco de ellos se pueden conectar en un mismo grupo de switch de 5 puertos. Dispone de una ranura DIMM con 512 MB de RAM. El corazón de éste sistema es lo último en procesadores de red PowerPC, lo que hace que dicho producto sea mucho más rápido que otros productos.

Cuenta con dos slots Compact Flash para caché de Web Proxy y backups de configuración.
RB1200 incluye el sistema operativo RouterOS, lo que le convierte en un sofisticado router/firewall/bandwidth manager.

La RB1200, es el elemento encargado de controlar los accesos de los usuarios a la red, gestión de tráfico, reservas de ancho banda, definición de políticas de seguridad, etc. Digamos que es el elemento "inteligente dentro de la red"; No obstante, los puntos de acceso que se instalarán a lo largo de la ciudad son capaces de hacer reservas de ancho de banda en función de los usuarios. Esto permitiría definir políticas de mayor rigidez en ciertas zonas de la ciudad en las que se prevea o se intuya que los usuarios de esas zonas puedan hacer un uso no deseado de la red.
Será necesario instalar la controladora en el Palacio de Peredo, puesto que será la responsable de toda la inteligencia de la red. La controladora tendrá un sistema de alimentación ininterrumpido con el fin de ofrecer un servicio continuado.

En cuanto al funcionamiento propio de la RB1200, además de lo comentado anteriormente, la controladora es capaz de definir los perfiles de acceso, de crear las listas blancas y negras de usuarios, páginas de navegación gratuitas, servidor de DHCP, firewall y otra de sus funciones principales es la comunicación con el servidor RADIUS para validación y control de usuarios.

En la siguiente tabla se indican las características técnicas del controlador RB1200

RB1200		
CPU	PPC460GT 1000MHz network processor RAM: 512MB	  Controlador RB1200
Boot Loader	RouterBOOT, 1Mbit Flash chip	
Almacenamiento	64 MB NAND	
Ethernet	Ten 10/100/1000 Mbit/s Gigabit Ethernet with Auto-MDI/X	
Puerto Serie	One DB9 RS232C asynchronous serial port	
Alimentación eléctrica	Standard connector 110/220V	
Caja	Caja metálica incluida. Carcasa 1U con dimensiones 144x176x442 mm	
Sistema Operativo	Mikrotik RouterOS, Level 6 license	

Tabla 16. Especificaciones Controladora RB1200

❖ Servidores

Un tipo de servidor que puede ser utilizado tanto para el servidor Web, como para el servidor de base de datos, el servidor de Roaming y el de gestión es el DELL R620 cuyas características técnicas se muestran a continuación.

Ilustración 63. Servidor DELL R620

Fuente. Web Dell

Feature	PowerEdge R620 technical specification
Form factor	1U rack
Processors	Intel® Xeon® processor E5-2600 product family
Processor sockets	2
Internal interconnect	2 x Intel QuickPath Interconnect (QPI) links: 6.4 GT/s, 7.2 GT/s, 8.0 GT/s
Cache	2.5MB per core; core options: 2, 4, 6, 8
Chipset	Intel C600
Memory[1]	Up to 768GB (24 DIMM slots): 2GB/4GB/8GB/16GB/32GB DDR3 up to 1600MT/s
I/O slots	**3 PCIe slots:** (10-drive-bay configuration is available only with the 3 PCIe slot option) Two x16 slots with x16 bandwidth, half-height, half-length One x16 slot with x8 bandwidth, half-height, half-length **or** **2 PCIe slots:** One x16 slot with x16 bandwidth, full-height, 3/4 length One x16 slot with x16 bandwidth (or x8 with one processor only), half-height, half-length
RAID controller	**Internal controllers:** PERC S110 (SW RAID) PERC H310 PERC H710 PERC H710P **External HBAs (RAID):** PERC H810 **External HBAs (non-RAID):** 6Gbps SAS HBA
Drive bays	Up to ten 2.5" hot-plug SAS, SATA, or SSD or up to four hot-plug 2.5" SAS, SATA, or SSD + two PCIe SSD
Maximum internal storage[1]	Up to 10TB
Hard drives	**Hot-plug hard drive options:** 2.5" PCIe SSD, SAS SSD, SATA SSD, SAS (15K, 10K), nearline SAS (7.2K), SATA (7.2K) Self-encrypting drives available
Embedded NIC	Broadcom® 5720 Quad Port 1GbE BASE-T (no TOE or iSCSI offload) Intel I350 Quad Port 1GbE BASE-T (no TOE or iSCSI offload) Intel X540 Dual Port 10GbE BASE-T with 2 x 1GbE (FCoE capability enabled on the 10GbE ports) Broadcom 57800S Dual Port 10GbE Base-T with 2 x 1GbE (TOE and iSCSI offload available on 10GbE ports Broadcom 57800S Dual Port 10GbE SFP+ with 2 x 1GbE (TOE and iSCSI offload available on 10GbE ports
Power supply	Auto-ranging Titanium efficiency, hot-plug redundant 750W AC power supply; Auto-ranging Platinum efficiency, hot-plug redundant 495W, 750W or 1100W AC power supply; 1100W DC power supply
Availability	High-efficiency, hot-plug, redundant power supplies; hot-plug hard drives; TPM; dual internal SD support; hot-plug, redundant fans; optional bezel; information tag; ECC memory; interactive LCD screen; extended thermal support; ENERGY STAR® compliant; switch independent partitioning
Remote management	iDRAC7 with Lifecycle Controller iDRAC7 Express (default), iDRAC7 Enterprise (upgrade option), 8GB vFlash media (upgrade option), 16GB vFlash media (upgrade option)
Systems management	IPMI 2.0 compliant Dell OpenManage™ Essentials and Dell Management Console Dell OpenManage Power Center Dell OpenManage Connections: • OpenManage Integration Suite for Microsoft® System Center • Dell plug-in for VMware® vCenter™ • HP Operations Manager, IBM Tivoli® Netcool®, and CA Network and Systems Management
Rack support	• ReadyRails™ II sliding rails for tool-less mounting in 4-post racks with square or unthreaded round holes or tooled mounting in 4-post threaded hole racks, with support for optional tool-less cable management arm • ReadyRails static rails for tool-less mounting in 4-post racks with square or unthreaded round holes or tooled mounting in 4-post threaded and 2-post (Telco) racks
Operating systems	Microsoft® Windows Server® 2012 Microsoft Windows Server 2012 Essentials Microsoft Windows Server 2008 R2 SP1, x64 (includes Hyper-V® v2) Microsoft Windows® Small Business Server 2011 Novell® SUSE® Linux Enterprise Server Red Hat® Enterprise Linux® **Virtualization options:** Citrix® XenServer® VMware vSphere® including ESX™ and ESXi™ Red Hat Enterprise Virtualization® For more information on the specific versions and additions, visit Dell.com/OSsupport.

[1] GB means 1 billion bytes and TB equals 1 trillion bytes; actual capacity varies with preloaded material and operating environment and will be less.

Tabla 17. Especificaciones Servidor Dell R620

Fuente. Web Dell

4. Fase de ejecución

Una vez realizado el diseño y elegido el equipamiento que conforma la red de telecomunicaciones se definen las fases a seguir para llevar a cabo el proyecto de ingeniería.

Dicho apartado no se ejecutará realmente, si no que se definirán los pasos a seguir y la metodología que habría que seguir en el supuesto en el que se llevase a cabo el proyecto en la realidad.

4.1 Compras

Para la realización de las compras se sigue el esquema que se muestra en la Ilustración 64

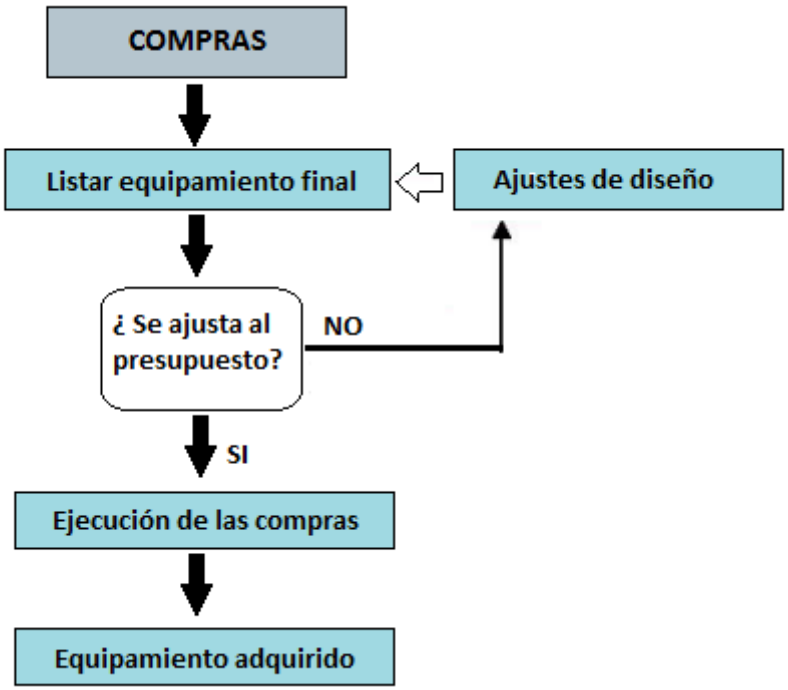


Ilustración 64. Esquema de compras

La primera actividad de este campo deberá ser la definición del listado del equipamiento final de acuerdo con el diseño.

Dispositivo	Modelo	Cantidad	Precio unidad
Punto de Acceso	Mikrotik RouterBoard 433AH	15	92.69 €
	Mikrotik R52N	45	24.53 €
	Pigtail PMN-HM20	60	6.09 €
	Cajas de aluminio exterior	15	25.90 €
Antenas	WRL-MTO247	30	55.91 €
	WRL-MTO-5085	30	53.45 €
Controladora	Mikrotik Router RB1200	1	244.61 €
Cableado	Cable Ethernet	10 m	5.09 €
Armario Rack	Rack	1	120 €
Alimentación	PoE	1	3.00 €
	Alimentador	15	10.33 €
	Cable eléctrico	80m/AP	1.20 € /m
	Diferencial	3	50 €

Tabla 18. Listado de Equipamiento final. Compras

Calculando el presupuesto en el Apartado 6.2 comprobamos que se ajusta a nuestro presupuesto por lo que el siguiente paso sería ejecutar las compras.

La empresa que proporciona el equipamiento será Landatel. Se trata de una empresa mayorista de valor añadido especializado en soluciones Wireless profesional. Distribuye productos inalámbricos de vanguardia a precios competitivos además de aportar soluciones al canal de distribución. El pedido se realiza a través de la web www.landashop.com indicando el equipo (marca y modelo) y las unidades necesarias que se deben comprar y desde el momento en que se ordena la compra hasta la recepción del equipamiento se podrá demorar de una a dos semanas aproximadamente; Si se trata de un producto importado o que no tienen en stock, hasta 30 días.

Los productos se recibirán en Madrid ya que habrá que configurar los equipos de comunicación, montar los puntos de acceso y acondicionar las cajas para después poder enviarlas a Santillana del Mar.

4.2 Solicitud e instalación de las líneas de comunicación

Se procederá a solicitar las líneas de comunicación que sean necesarias para la implementación de una red a los proveedores correspondientes.

En nuestro caso será necesaria la solicitud de un ADSL de 10 Mbps al operador Telefónica, así como un servicio dedicado WiMAX de 10 Mbps simétricos al operador conexión rural.

Para la instalación de las líneas se citará a ambos operadores el mismo día en Santillana del Mar para que procedan a realizar sus trabajos de instalación.

4.3 Fase de configuración de la red

Una vez recibido el pedido se comprobará si el equipamiento recibido es el que se solicitó y se seguirá el siguiente esquema con el fin de poder embalar el equipamiento en cajas, una vez configurado y simulado para finalmente enviarlo al municipio donde procederá la instalación.

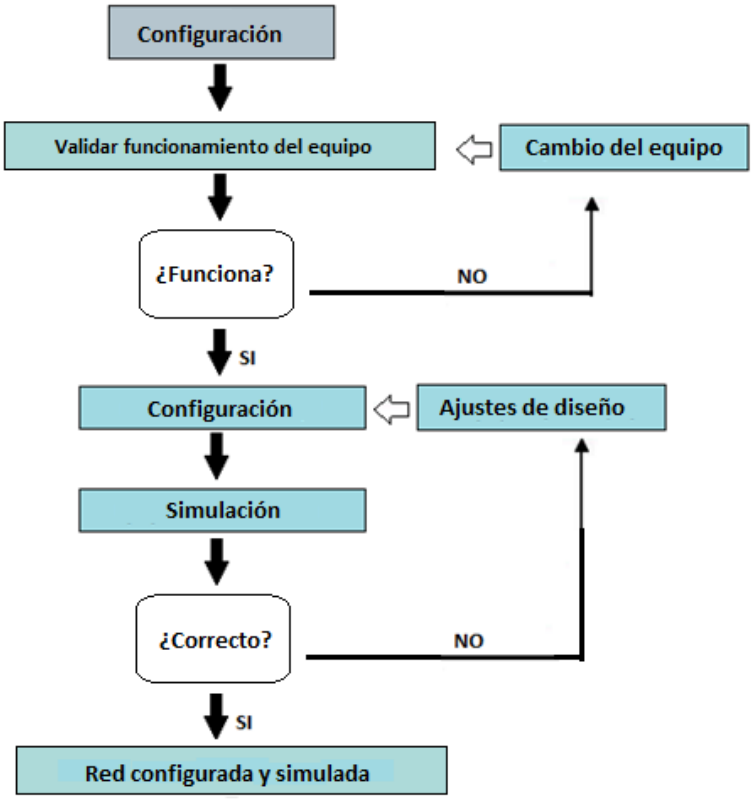


Ilustración 65. Esquema de configuración

Se deberá realizar la configuración de cada elemento del sistema de comunicaciones y para ello en los apartados sucesivos se mostrarán tanto diagramas que facilitan la configuración del direccionamiento IP, el enrutamiento, los túneles EoIP y L2TP, como la configuración detallada de los elementos que componen la red de telecomunicaciones.

4.3.1. Diagramas de red

Para tener un correcto control en la organización de nuestra red se ha diseñado un diagrama en el que se ha documentado cómo es la estructura de nuestra red;

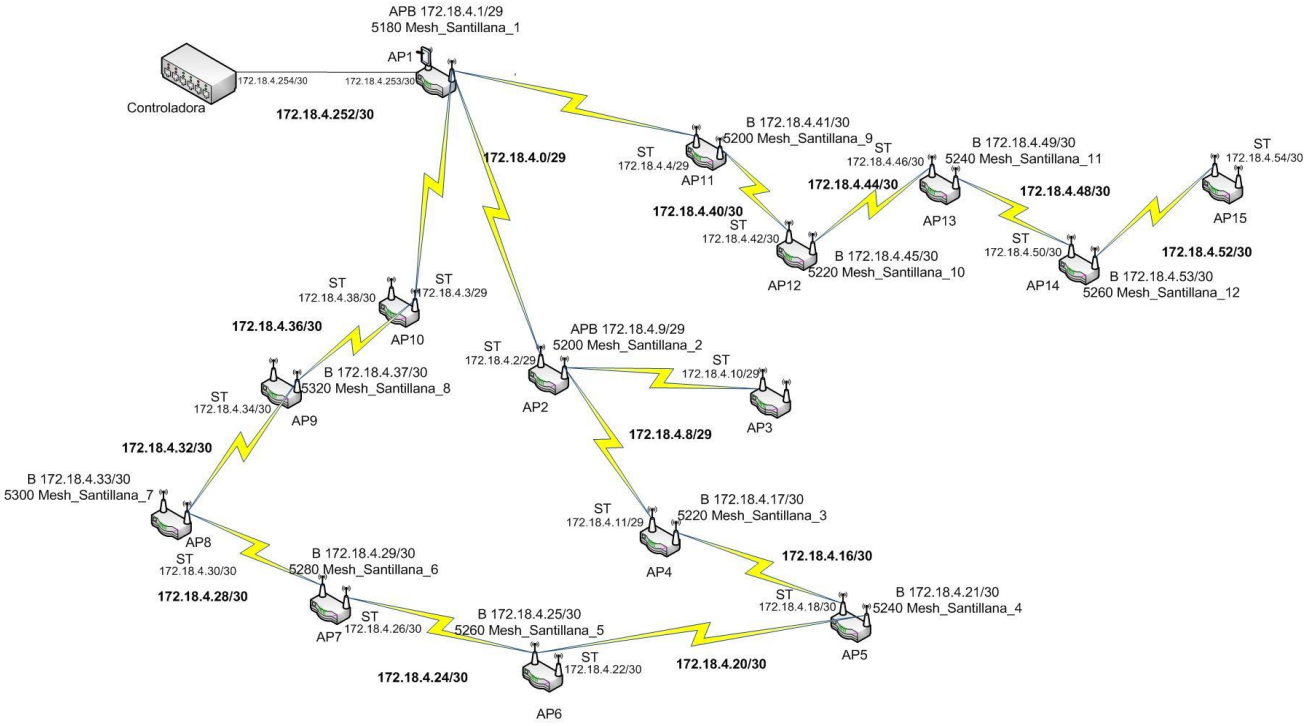


Ilustración 66. Diagrama de la estructura de red

Existen diferentes modos de configurar los enlaces de los Access Points:

AP Bridge (APB): Se utiliza para enlaces inalámbricos punto multipunto y permite la conexión de un equipo con varios.

Bridge (B): Se utiliza para enlaces inalámbricos punto a punto y permite la conexión con un solo equipo.

Por lo tanto, cuando enlazamos un equipo a otro lo configuraremos como Bridge (B)-Station (ST) como es el caso del AP4-AP5, mientras que si queremos enlazar un equipo con varios APs diferentes, lo configuramos como APBridge (APB)- Station (ST), como es el caso del AP2 con el AP3 y AP4.

Por otro lado, en el diagrama se han incluido las IPs privadas de cada equipo, la subred a la que pertenece cada equipo (marcado en negrita), el SSID de los enlaces, el enlace del primer AP con la controladora y la frecuencia en la que transmite cada equipo, evitando que puedan interferir con respecto al resto de los APs vecinos. Esto facilitará la posterior configuración de los Puntos de Acceso.

Además del diagrama de red, se ha diseñado un diagrama de configuración donde se documentan los datos necesarios para crear los túneles correspondientes.

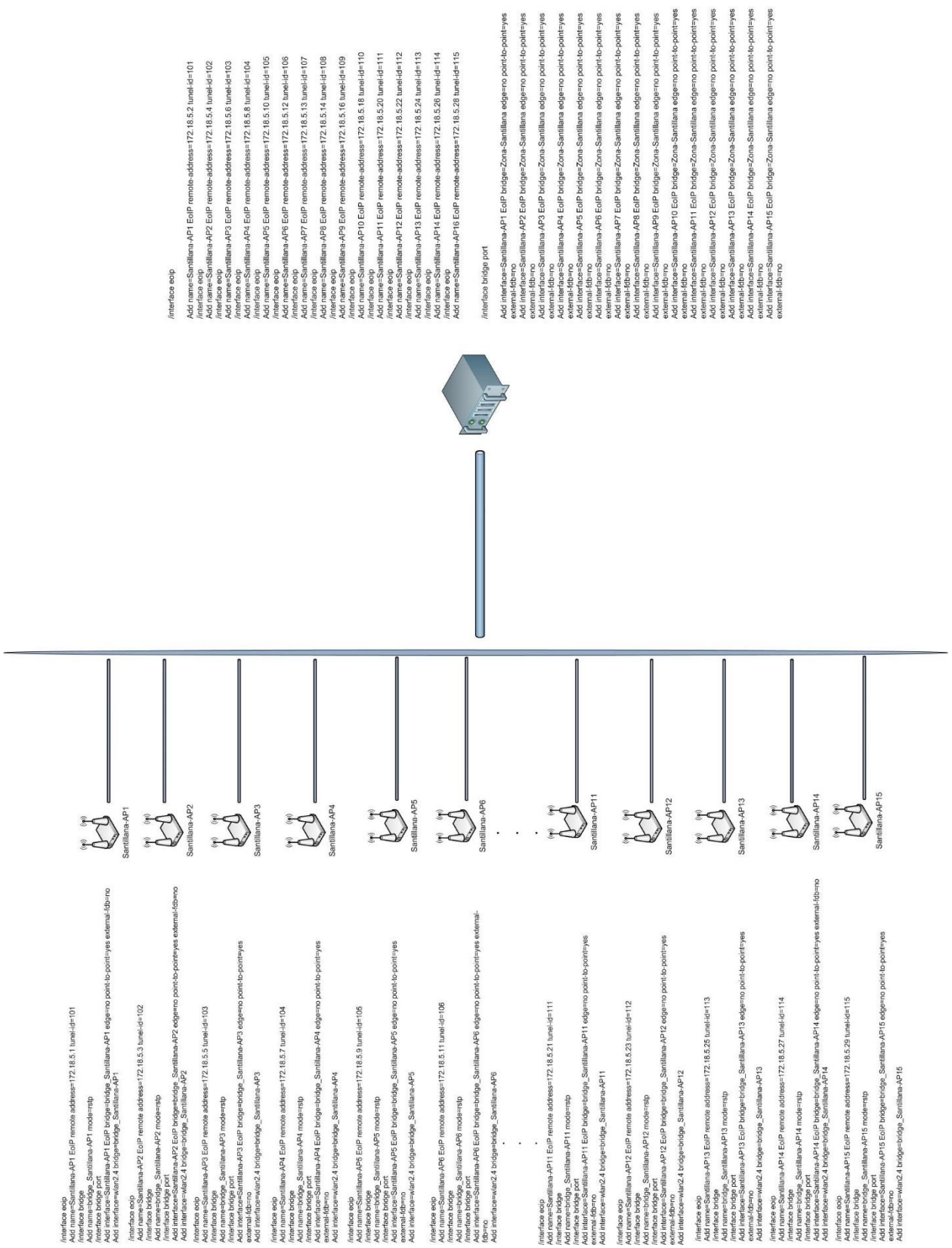


Ilustración 67. Diagrama de configuración

4.3.2. Configuración de los equipos

En el ANEXO A se detallarán los pasos a seguir para realizar la configuración de un Mikrotik RB433AH y los enlaces correspondientes para que todos los puntos de acceso vecinos queden interconectados a través de radioenlaces.

Además, se configurará la controladora, de forma que la red quede totalmente configurada y preparada para la instalación de la red.

4.4 Instalación de la red

4.4.1. Envío del equipamiento

Consiste en la preparación del equipamiento para ser enviado. Una vez montados, configurados y embalados los equipos, se mandan al municipio de Santillana del Mar junto con el material necesario para la instalación. En este caso, al ser únicamente dos cajas de dimensiones 50x50x70 cm, será el propio instalador el que trasladará el equipamiento. El medio de transporte a utilizar será una furgoneta de alquiler. El instalador comenzará con sus tareas el día después de su llegada a Santillana del Mar.

4.4.2. Instalación

Como se ha comentado anteriormente, con respecto a la instalación de los diferentes puntos de acceso se plantea la ubicación de los mismos en la parte superior de las farolas del municipio y otros sistemas de iluminación cercanos a las zonas de interés. Se plantea un proceso de instalación para cada uno de los emplazamientos.

Recepción de documentación específica

- Se procederá a realizar las solicitudes oportunas para que una persona del Ayuntamiento sea el que nos facilite la documentación relativa a las canalizaciones existentes a lo largo de las zonas de cobertura en las que se realizarán trabajos de instalación.

- Se solicitará igualmente el plan de riesgos, seguridad y salud del Ayuntamiento para trabajos tanto en edificios municipales como en áreas libres (instalaciones outdoor)

- Se solicitarán los protocolos de actuación ante incidencias, así como los de actuación de control de accesos.

Realización del estudio provisional

Con la documentación recibida relativa a las canalizaciones existentes se procederá a estudiar insitu cada uno de los emplazamientos de forma que se adecue la fijación de los equipos y el cableado de alimentación de cada AP.

- Confirmación de ubicación del AP

- Instalaciones outdoor: Adaptar la red de acceso inalámbrico a las condiciones meteorológicas para que estas no afecten al funcionamiento normal de la red.

- Replanteo para comprobar como se procederá a realizar la instalación del cableado eléctrico.

- Será necesario planificar la instalación y acordar las fechas de instalación

Realización de los documentos del replanteo

Una vez realizada la visita y el análisis para la instalación más idónea del equipamiento y las conexiones, se realizará un informe de replanteo con planos en detalle de la ubicación exacta de los equipos y antenas, tendidos del cableado, puntos de conexión…, que deberá ser aprobado por el personal designado por el Ayuntamiento antes de empezar los trabajos de instalación.

Acopio de materiales e Inicio de la instalación

El técnico se encargará de reagrupar el material necesario para la instalación. Se trasladará a los técnicos para comenzar con la instalación de la red de comunicaciones. Deberán cumplir con los plazos indicados en el cronograma.

Documentación de la instalación

- Una vez terminada la instalación de cada emplazamiento se llevará un proceso de toma de datos, incluyendo equipamiento instalado y conexiones.

- Se comprobará el etiquetado de los equipos y las conexiones en cada emplazamiento.

- Se incluirá un reportaje fotográfico y un plano con detalle de la estructura de la instalación.

Entrega de la instalación

- Se entregará al Ayuntamiento toda la documentación, incluyendo memoria, planos y estudio fotográfico.

- Con la documentación entregada se realizará una visita con el personal designado por el Ayuntamiento a cada emplazamiento de forma tal de obtener el visto bueno final desde el punto de vista de la instalación.

- En los casos en los que el personal designado por el Ayuntamiento considere que deben hacerse modificaciones de la instalación, se tomará nota y se procederá a gestionar los trabajos pertinentes para realizar dichas modificaciones.

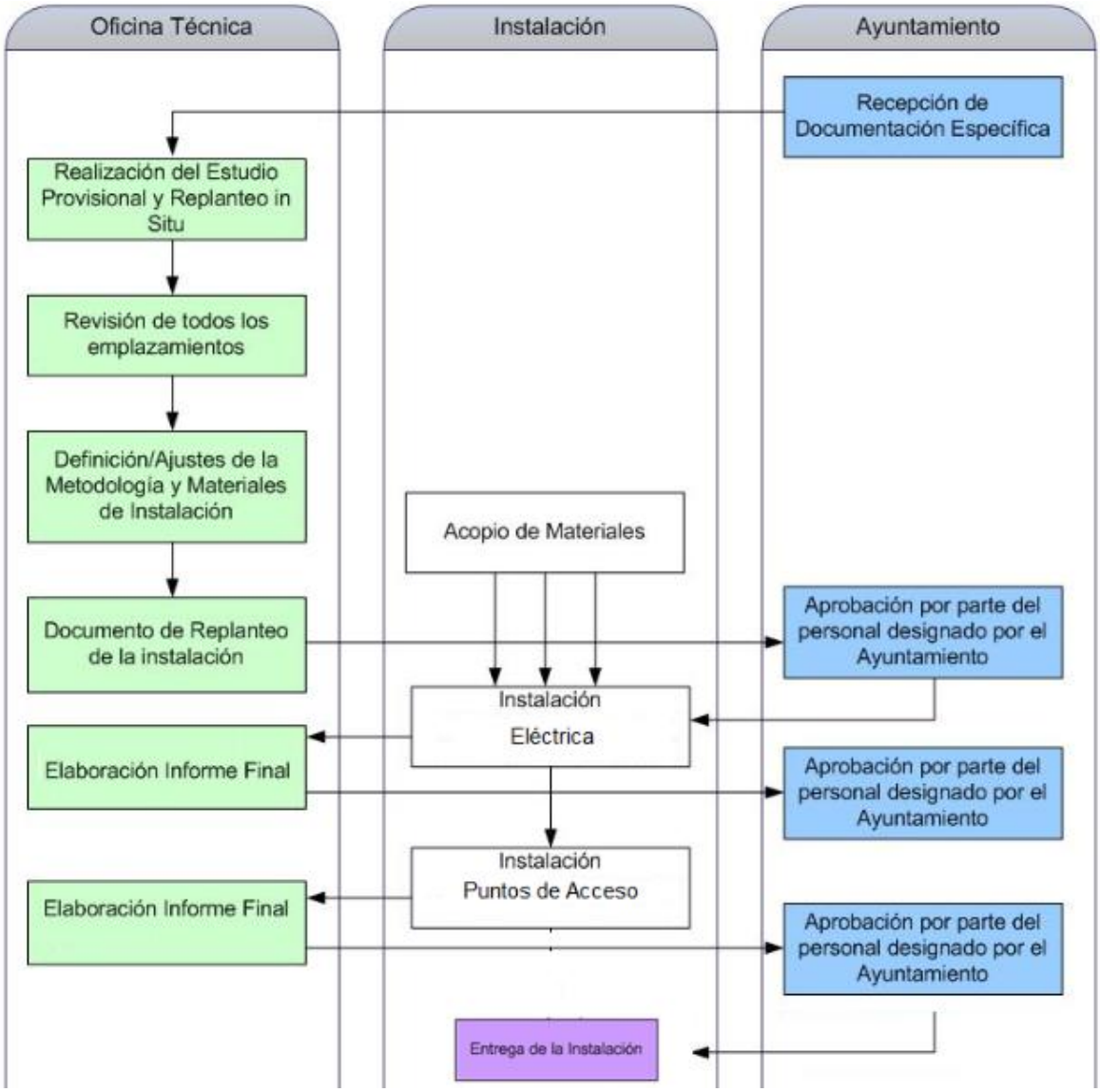


Ilustración 68. Plan de instalación. Red WiFi

El siguiente esquema corresponde a un diagrama tipo de instalación de puntos de acceso utilizando las farolas del municipio. Exceptuando el primer punto de acceso que se ubicará en la terraza del Palacio de Peredo, el resto de los equipos serán instalados en las farolas como se muestra en el siguiente diagrama.

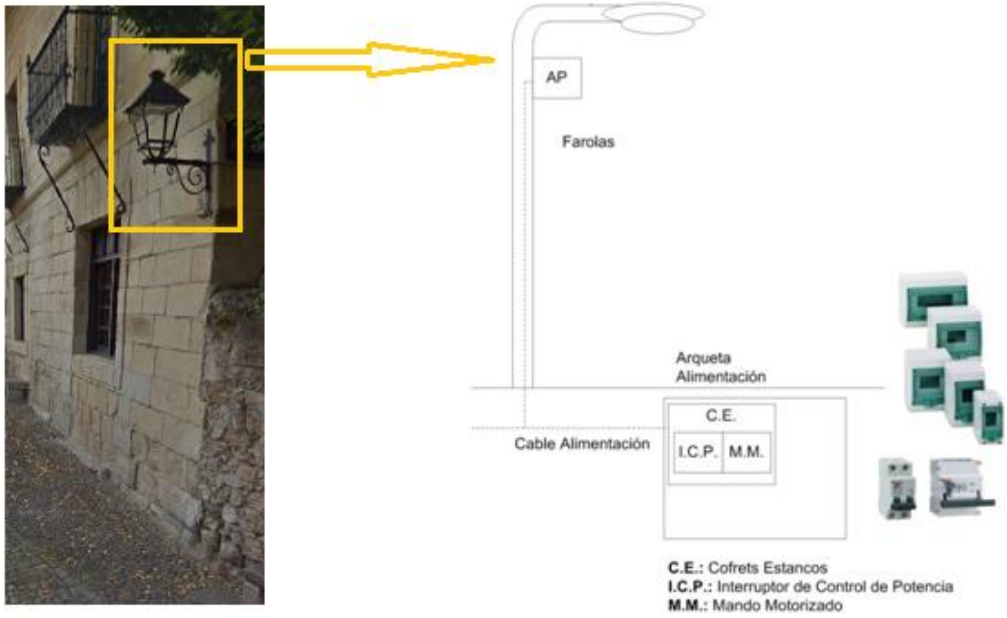


Ilustración 69. Instalación de los APs

Antes de comenzar con la instalación de los puntos de acceso, se debe realizar la instalación eléctrica completa. La alimentación necesaria para el equipo se hace llegar desde el cuadro del alumbrado público del que depende la farola. Para ello, se debe pasar el cableado eléctrico por el interior de la farola hasta el registro de la misma. A través de la canalización existente, que facilita notablemente la instalación, se va pasando el cable por las arquetas de alimentación que se encuentran a unos 50 metros de distancia a lo largo del municipio hasta alcanzar el cuadro de alumbrado eléctrico más cercano.

El cableado a utilizar para la instalación eléctrica será certificado de acuerdo a la normativa y metodología vigente. Se utilizará cableado libre de halógenos de 3x4 mm.

El tiempo de ejecución de la instalación eléctrica dependerá de los problemas que se presenten. Algunos de los problemas que pueden llevar más tiempo a la hora de realizar la instalación son:

- Arqueta sellada. Si la arqueta se encuentra sellada con hormigón o cemento se complica la instalación ya que se necesitan materiales especiales para poder acceder a la canalización.

- Si no se pudiera introducir el cableado por el canal que alimenta la farola, se tendría que realizar una canalización aparte que conlleva una costosa obra civil.

En este caso, según la información proporcionada por el responsable del Ayuntamiento se podrá acceder a la canalización existente que alimenta la farola y las arquetas estarían cubiertas por tierra.

Según el replanteo in situ que se realizó en el municipio, se redacta un documento indicando los pasos a seguir para realizar la instalación eléctrica, además de la ubicación exacta y la orientación de los puntos de acceso para facilitar el trabajo al técnico. No obstante, las personas encargadas de la instalación estarán acompañadas por el responsable asignado para el proyecto y comprobará que la instalación eléctrica se realiza correctamente y que los emplazamientos finales tanto de las antenas como de los puntos de acceso es el adecuado.

El personal necesario para dicho proceso será el responsable del proyecto junto con dos técnicos que realicen en primer lugar la instalación eléctrica y a continuación vayan instalando los puntos de acceso a lo largo del municipio, para lo cual se emplearán siempre las mayores medidas de seguridad, tanto a nivel de los técnicos instaladores como en los mecanismos que se usarán para fijar y asegurar los equipos.

La instalación del equipamiento, se realiza de tal modo que sea lo más discreto posible, minimizando al máximo el impacto visual. Se utilizarán anclajes para enganchar los puntos de acceso a las farolas municipales de Santillana del Mar.

Para alimentar el primer punto de acceso se ha pensado en la utilización de un inyector PoE (Power over Ethernet) específico para placas Mikrotik. Al instalar el punto de acceso en la terraza del Palacio de Peredo, no se dispone de una toma de corriente eléctrica cercana al AP. Además, el AP1 es el único que debe estar conectado a través de Ethernet a la controladora. Por ello, en vez de tirar un cable eléctrico desde el Mikrotik hasta la toma de corriente y por otro lado un cable Ethernet hasta la controladora, se ha considerado oportuno la utilización de un inyector PoE que sea capaz tanto de dejar que pasen los datos como de alimentar al equipo. El equipo será cableado con Ethernet categoría 6. A continuación se muestra como queda la instalación del primer punto de acceso.

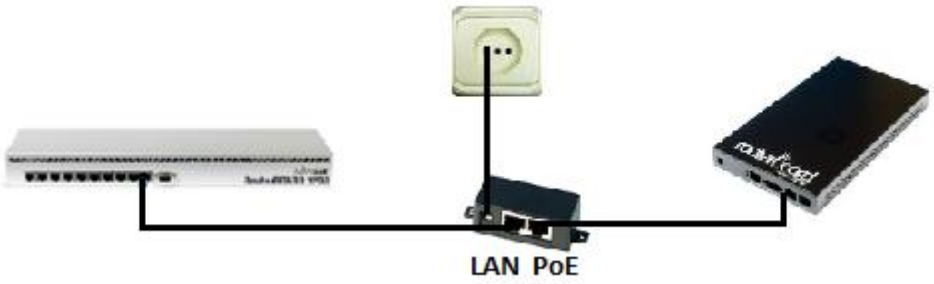


Ilustración 70. Instalación primer AP

Para garantizar la fiabilidad de los equipos centrales de la red, todos los elementos necesarios para la correcta prestación del servicio, quedarán alojados en el interior de un armario de comunicaciones. Se dispondrá, por lo tanto, de un rack con limitación de acceso, de 6 U de espacio con el fin de poder instalar los equipos de una manera segura. En el armario de comunicaciones se deberá alojar la controladora, el router ADSL y el CPE WiMAX.

5. Certificación y mantenimiento

En este capítulo se mencionará la metodología a seguir, pues en este caso, al no realizarse la instalación real del proyecto, no tendremos informe de instalación y pruebas, hoja de incidencias…

El objetivo de este apartado sería realizar la aceptación del emplazamiento instalado, la puesta en servicio y verificar la conformidad de la red.

Para la verificación de la red se necesita una visita in-situ en la cuál se realizarán tanto pruebas de cobertura como testeo de velocidades.

Para ello se utilizarán programas de software libre. Una de las herramientas que podría ser útil para analizar las señales de los puntos de acceso wiFi es WiFi Analyzer. Esta herramienta es capaz de generar gráficas de intensidad para cada señal disponible, medir intensidades concretas en tiempo real, conocer la banda en la que esta trabajando cada punto de acceso entre otras posibilidades.

Otra herramienta de localización de redes inalámbricas y control de la intensidad de las señales es el programa InSSIDer. Permite detectar todas las redes inalámbricas que ofrecen cobertura en tu zona y listar en pantalla detalles como: SSID, dirección MAC, tipo de red, canal…. InSSIDer permite monitorizar la calidad de la señal utilizando como parámetro de control el indicador que refleja la fuerza o intensidad de la señal radio recibida (RSSI).

Por otra parte, a través de Winbox se verificará que las antenas están emitiendo correctamente y que en cada punto de acceso se puede acceder y navegar por Internet con normalidad.

Certificada la red, se mostrará al personal del Ayuntamiento el resultado de la instalación para su aceptación final. Una vez desplegada la red de comunicaciones y puesta en servicio para que los usuarios puedan disfrutar de conexión a Internet a lo largo del municipio rural, sería recomendable poder monitorear la red durante 24 horas para ir detectando las incidencias que puedan surgir y resolverlas de la manera más eficaz posible.

El momento en el que la probabilidad de fallo es mayor, resultará ser inmediatamente posterior a la instalación. Después de un tiempo, el comportamiento de los equipos se estabilizará. En este periodo de pruebas, se someterá al equipamiento a estrés para determinar los posibles motivos de fallo y poder solucionarlos.

Mantenimiento y gestión de la red

Una aplicación interesante de monitoreo de redes es The Dude, fue diseñada por Mikrotik para mejorar la forma de gestionar un entorno de red. Se encarga de escanear automáticamente todos los dispositivos que se encuentran dentro de una subred específica, dibuja y diseña un mapa de nuestra red, controla los servicios de sus dispositivos y es capaz de avisar en caso de que un servicio tenga algún problema.

Además presenta un acceso directo a herramientas de control remoto para la gestión dedispositvos, se ejecuta en entornos Linux, Windows y Wine Darwine MacOS. Se trata de un producto gratuito y tiene una gran calidad en comparación con otros productos.

The Dude utiliza un diseño cliente/servidor, lo que significa que el software debe ser instalado en un servidor dedicado. Además, tiene que ser instalado en un PC para que pueda interactuar con el servidor. La gestión que realiza se enfoca en un ámbito SNMP (Simple Network Managment Protocol) donde pueden obtenerse datos de los dispositivos a través de este protocolo, basándose en una base de datos MIB (Managment Information Base) para saber que datos obtener.

Un entorno SNMP se puede clasificar los siguientes elementos:

- Dispositivo: Considerado como el punto o nodo que se desea evaluar o monitorear. Requiere poseer SNMP v 1, 2 o 4.
- Agente: Dispositivo intermedio, sirve para proveer datos de evaluación o monitoreo de otro segmento de red adyacente a este agente (generalmente se usan cuando la red posee un enrutamiento capa 3), también ayudan a reducir la carga de red producida por el sistema de Monitoreo.
- NMS (Network Managment system): Es el centro o servidor encargado de manejar y evaluar toda la información, en este punto se realizan los cálculos o funciones y búsquedas en la MIB.

El funcionamiento de SNMP se basa en un entorno de polling (sondeo, maestro – esclavo) basado en los siguientes pasos:

- El NMS (Network Managment system): pregunta al agente correspondiente sobre el dispositivo final datos o actualizaciones del estado de datos.
- Respuesta: la respuesta es recibida por el agente y este lo pasa al NMS en formato SNMP.
- Si existe un trap, el agente solo envía información puntual (caído o levantado), se usa para detectar anomalías.
- SNMP funciona con los puertos UDP 161 y 162 para el trap.

Dicho sistema de monitorización, proporciona una visión geo-localizada de cada controladora y hotspot de la red, informando de los cambios de estado de cada dispositivo en todo momento. Monitoriza de forma individual el tráfico consumido por cada uno de los puntos de acceso y de cada uno de los clientes.

The Dude posibilita a los administradores de red realizar un amplio abanico de funciones criticas para configurar, monitorizar y operar las redes. Esto incluye

configuraciones remotas en caliente, actualizaciones de software, monitorización de rendimiento en tiempo real y extremo a extremo de la red, procesado de históricos, análisis de tendencias y monitorización de conectividad del cliente.

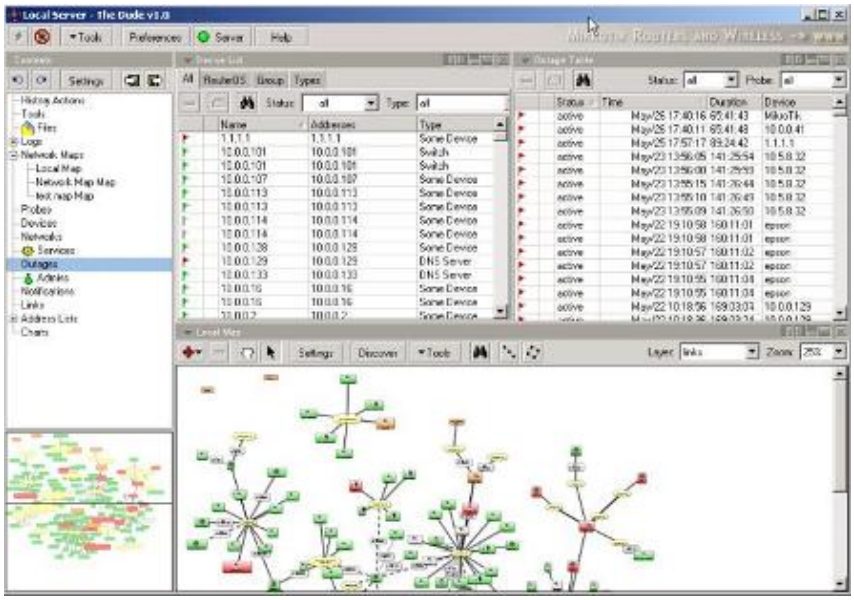


Ilustración 71. The Dude

Independientemente de la plataforma de gestión que se utilice para garantizar el correcto funcionamiento de la red y conseguir unos tiempos de disponibilidad de la red cercanos al 100% será necesario realizar actuaciones periódicas para comprobar que todos los equipos instalados están operativos y no hayan sufrido ningún desperfecto a lo largo del tiempo. Algunas de las tareas a realizar se muestran en la siguiente tabla:

Tareas
Revisión del estado de los puntos de acceso. Balanceo. Estanquidad de los APs de exteriores
Revisión de las controladoras de red. Análisis de trazas.
Supervisión de las antenas exteriores y de los pigtails y conectores que unen los Aps con las antenas.
Monitorización del volumen de usuarios
Medición de temperatura y humedad en el rack de comunicaciones
Revisión del estado de la estructura Mesh
Actualización del Software en puntos de acceso y controladoras
Revisión del espectro radioeléctrico
Ajuste de la configuración lógica de los equipos

Tabla 19. Tareas para comprobar el funcionamiento del equipamiento

6. Plazos del proyecto y presupuesto

6.1 Plazos

Las fases de caso de estudio y ejecución del proyecto conlleva los siguientes plazos:

- **Reunión de lanzamiento**: Definición y elaboración de los requisitos que se deben cumplir en la red que se va a implementar. **1 día**

- **Estudio de Ingeniería**: Se trata del estudio de ingeniería para la planificación y dimensionamiento de la red Radioeléctrica en el que se definirá la infraestructura, la arquitectura general y el estudio de coberturas y radio enlaces necesarios, así como el equipamiento de la red de radiocomunicaciones. **5 días**

- **Replanteo in situ.** Se determinarán las ubicaciones finales tanto de los puntos de acceso como de los servidores centrales. Se realizará un replanteo de cómo será la instalación eléctrica y se hará un pequeño documento en el que se mostrará como se debe tirar el cable desde cada punto hasta el cuadro de alumbrado público más cercano. **3 días**

- **Compra y Recepción del Equipamiento.** Una vez aprobada la red a implementar, se comprarán los equipos definitivos a través de Landatel. **10 días**

- **Solicitud e instalación de las líneas de comunicación.** Se solicitará a Télefonica un ADSL de 10 Megas y al operador conexión rural un servicio WiMaX de 10 Mb simétricos. **1 día**

- **Montaje y configuración de los equipos.** Se montarán los puntos de acceso y se configurarán los equipos que conforman la red. **4 días**

- **Congiguración de la controladora y de los servidores centrales. 1 día**

- **Instalación del cableado eléctrico.** Se llevarán a cabo las tareas asociadas para realizar la instalación eléctrica. Será necesaria la intervención de dos técnicos para realizar los trabajos. **8 días**

- **Instalación del equipamiento WiFi y la controladora.** Una vez que todas las estructuras necesarias estén instaladas y acondicionadas será el momento de la instalación final de los equipos junto con sus antenas en las plazas y calles del municipio. **3 días**

- **Pruebas funcionales WiFi y certificación de la red**. Una vez instalado todo el equipamiento de la red de acceso inalámbrica, se realizarán las pruebas y

reajustes necesarios y se certificará el correcto funcionamiento y ubicación de todo el equipamiento. **4 días**

- **Puesta en marcha del sistema de comunicaciones y monitorización de la red.** Una vez certificada la red, se pondrá en marcha el servicio y se iniciará la monitorización de todos los dispositivos que conforman la red. **1 día**

6.2 Presupuesto

A. EQUIPAMIENTO

A.1 Red WiFi Mesh

Artículo	Precio Unitario	Unidades	Coste
Tarjetas Radio Red Mesh R52N	24,53 €	30	735,90 €
Pigtail MMCX PMN-HM20	6,09 €	30	182,70 €
Antenas Omni 5 GHz WRL-MTO-5085	53,45 €	30	1.603,50 €
Total			**2.522,10 €**

Total equipamiento **2.522,10 €**

A. EQUIPAMIENTO

A.2 Red WiFi Acceso

Artículo	Precio Unitario	Unidades	Coste
Mikrotik RouterBOARD RB433AH	92,69 €	15	1.390,35 €
Tarjetas Radio Red Acceso R52N	24,53 €	15	367,95 €
Pigtail MMCX PMN-HM20	6,09 €	30	182,70 €
Antena Omni 2.4 GHz WRL-MTO-247	55,91 €	30	1.677,30 €
Caja estanca exterior- SNW-CAX	25,90 €	15	388,50 €
Total			**4.006,80 €**

Total equipamiento **4.006,80 €**

A. EQUIPAMIENTO INSTALACIÓN

A.3 Equipamiento instalación

Artículo	Precio Unitario	Unidades	Coste
Anclajes	25,00 €	15	375,00 €
Alquiler elevador	200,00 €	1	200,00 €
Inyector PoE- PoE-PAS	3,00 €	1	3,00 €
Cable Ethernet	5,09 €	1	5,09 €
Alimentadores	10,95 €	15	164,25 €
Cable eléctrico	1,20 €/m	80 m/AP	1.440,00 €
Diferencial	50,00 €	3	150,00 €
Total			**2.337,34 €**

Total **2.337,34 €**

B. SERVIDORES – ELECTRÓNICA CENTRAL

B.1 Servidores

Artículo	Precio Unitario	Unidades	Coste
Servidor DELL R620	2.500,00 €	0,2	500,00 €
Rack GSAP 6 U 19"	120,00 €	1	120,00 €
Total			**620,00 €**

B.2 Electrónica central

Artículo	Precio Unitario	Unidades	Coste
Mikrotik Router RB1200	244,61 €	1	244,61 €
Total			**244,61 €**

Total eléctronica central	**864,61 €**

Total equipamiento **864,61 €**

C. INGENIERIA Y DIRECCIÓN DE PROYECTO

C.1 Replanteo in situ y análisis radioeléctrico

Concepto	Días	Ingeniero día	Nº Personas	Coste
Replanteo	4	180,00 €	2	1.440,00 €
Dietas	3,5	40,00 €	2	280,00 €
Estancia	3	60,00 €	2	360,00 €
Viaje	1	200,00 €	2	400,00 €
Total				**2.480,00 €**

C.2 Montaje y Configuración de los puntos de acceso y la controladora

Concepto	Días	Técnico día	Nº Personas	Coste
Montaje de los puntos de acceso	0,5	70,00 €	1	35,00 €
Configuración de los APs y la controladora	4,5	100,00 €	1	450,00 €
Total				485,00 €

C.3 Configuración sistemas centrales

Concepto	Días	Técnico día	Nº Personas	Coste
Configuración sistemas centrales de validación	0,5	100,00 €	50,00 €	50,00 €
Total			**50,00 €**	**50,00 €**

C.4 **Instalación cableado eléctrico y equipamiento**

Concepto	Días	Técnico día	Nº Personas	Coste
Instalación cableado eléctrico	8	70,00 €	2	1.120,00 €
Instalación equipamiento WiFi	3	70,00 €	2	420,00 €
Dietas	7	40,00 €	2	560,00 €
Estancia	6	50,00 €	2	600,00 €
Viaje	2	200,00 €	2	400,00 €
Total				**3.100,00 €**

C.5 **Pruebas y Certificación**

Concepto	Días	Técnico día	Nº Personas	Coste
Pruebas y Certificación	3	100,00 €	1	300,00 €
Dietas	2,5	40,00 €	1	100,00 €
Estancia	2	60,00 €	1	120,00 €
Viaje	1	200,00 €	1	200,00 €
Total				**720,00 €**

C.6 **Estudio Ingeniería**

Concepto	Días	Ingeniero día	Nº Personas	Coste
Estudio Ingeniería	5		1	100,00 €
Total				**100,00 €**
		Total ingeniería		**6.935,00 €**

D. SERVIDORES – ELECTRÓNICA CENTRAL

D.1 **Comunicaciones**

Artículo	Precio Unitario	Unidades	Años	Meses	Coste
WiMAX 10 Mb simétricos	466,00 €	1	1	12	5.592,00 €
10 Mb ADSL	45,00 €	1	1	12	540,00 €
Total					**6.132,00 €**

Total **6.132,00 €**

E. MANTENIMIENTO Y SUSTICIÓN DE EQUIPAMIENTO

E.1 **Mantenimiento**

Concepto	Unidades	Coste unidad	Coste configuración	% sustituciones año	Años	Coste en años de contrato
RouterBoard 433AH	15	92,69 €	17,00 €	15,00%	1	246,80 €
Tarjetas Radio R52N	45	24,53 €	2,50 €	15,00%		182,45 €
Antena Omni 2.4 GHz WRL-MTO-247	30	55,91 €	3,98 €	5,00%		89,84 €
Pigtail MMCX PMN-HM20	60	6,09 €	3,98 €	10,00%		60,42 €
Antenas Omni 5 GHz WRL-MTO-5085	30	53,45 €	3,98 €	5,00%		86,15 €
Caja estanca exteriores	15	25,90 €	35,00 €	1,00%		9,14 €
Alimentadores	15	10,95 €	3,98 €	25,00%		55,99 €
Mástiles y anclajes	15	25,00 €	20,00 €	2,00%		13,50 €
Inyector PoE	1	3,00 €	0,00 €	2,00%		0,00 €
Cable Ethernet	1	5,09 €	0,00 €	2,00%		0,10 €
Cable eléctrico	80 m/AP	1,20€/m	0,00 €	1,00%		14,40 €
Servidor DEL R620	0,2	2.500,00 €	275,00 €	1,00%		5,55 €
Rack GSAP 6 U 19"	1	120,00 €	250,00 €	1,00%		3,70 €
Mikrotik Router RB1200	1	244,61 €	140,00 €	15,00%		57,69 €
Total						825,72 €

E.1 **Incidencias**

Concepto	Unidades	Coste unidad	Años	Visitas al mes	Meses	Coste en años de contrato
Servicio de atención de incidencias	1	150,00 €	1	-	12	1.800,00 €
Visitas in situ	1	45,00 €		1	12	540,00 €
Total					-	2.340,00 €
					Total	3.165,72 €

A. EQUIPAMIENTO		
A.1	Red WiFi Acceso	4.006,80 €
A.2	Red WiFi Mesh	2.522,10 €
A.3	Equipamiento instalación	2.337,34 €
	Coste total equipamiento	**8.866,24 €**
B. SISTEMAS CENTRALES		
B.1	Servidores	620,00 €
B.2	Electrónica central	244,61 €
	Coste total servidores y electrónica central	**864,61 €**
C. INGENIERIA Y DIRECCIÓN DE PROYECTO		
C.1	Replanteo in situ y análisis radioeléctrico	2.480,00 €
C.2	Montaje y Configuración de APs y controladora	485,00 €
C.3	Configuración sistemas centrales	50,00 €
C.4	Instalación cableado eléctrico y equipamiento	3.100,00 €
C.5	Pruebas y Certificación	720,00 €
C.6	Estudio de ingeniería	100,00 €
	Coste total Ingeniería y Dirección de proyecto	**6.935,00 €**
D. COMUNICACIONES		
D.1	Comunicaciones	6.132,00 €
	Coste total Comunicaciones	**6.132,00 €**
E. MANTENIMIENTO y SUSTICIÓN DE EQUIPAMIENTO		
E.1	Mantenimiento	825,72 €
E.2	Incidencias	2.340,00 €
	Coste total Mantenimiento	**3.165,72 €**

Coste total infraestructura	**25.963,57 €**
IVA 21%	5.452,35 €
Total	**31.415,92 €**

7. Conclusión y trabajo futuro

Existen diferentes formas de abordar despliegues municipales de redes de datos sobre las cuales implementar servicios para la propia administración pública y para los ciudadanos. Una de estas formas es el uso de equipamiento inalámbrico para la transmisión de datos, cuyo desarrollo ha recibido un gran impulso en los últimos tiempos debido a la estandarización de los protocolos para transmisiones inalámbricas.

Como se puede apreciar, gracias a estas tecnologías inalámbricas, WiFi y WiMAX, es posible realizar un despliegue de red en una zona rural, sin que ello suponga elevados costes de instalación debido a que no hace falta realizar costosas obras civiles como ocurre en otro tipo de despliegues cableados. Además, al usar frecuencias en las que no se necesita licencia alguna, nos ahorramos costes. De esta manera se puede llevar las redes de comunicación de banda ancha a lugares en los que solo hay disponibles servicios básicos.

Con el presente proyecto técnico sería posible implementar la red inalámbrica descrita, siendo solo necesario ocuparse de los detalles específicos de la configuración e instalación de los equipos en cada una de las zonas descritas.

Además, dicho proyecto muestra las fases que habría que seguir para realizar cualquier otro proyecto similar, pudiéndose utilizar como plantilla unicamente modificando los contenidos de los apartados correspondientes.

Como posible continuación al proyecto realizado, se podría ampliar la red de comunicaciones por el resto de las calles del municipio, sin tener que realizar apenas cambios en la red descrita. Simplemente con la configuración e instalación de nuevos equipos se podría ampliar la red a lo largo del territorio.

Además, sería posible cubrir no sólo el casco hístorico del municipio, si no cubrir el interior de los edificios municipales o incluso llegar a través de la combinación de dichas tecnologías hasta zonas alejadas.

Otra línea de investigación podría ser como desplegar torres de comunicación o repetidores para llevar internet hasta municipios cercanos que sólo cuentan con servicios básicos o incluso no tienen acceso a Internet.

8. Referencias

8.1 Referencias bibliográficas

Carballar, José A. (2007). *WiFi – Instalación, Seguridad y Aplicaciones*. RA-MA Editorial.

Andreu, F. / Pellejero, I. /Lesta, A. (2006). *Redes WLAN - Fundamentos y aplicaciones de seguridad en redes WLAN*. MARCOMBO Editorial. Páginas 31-106.

Gast, Matthew. (2005). *802.11 Wireless Networks*. O'Reilly Media Editorial.

López Ortiz, F. (2008) *El estándar IEEE 802.11 Wireless LAN.* Obtenido de *http://web.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf*

Universidad del Mar de la Plata (2011). *Estándar 802.11 – Función MAC*. Obtenido de http://www3.fi.mdp.edu.ar/electronica/catedras/redesdedatos/files/10Management802.11.pdf

Perú. Universidad Nacional del Callao (2008) *Blog de Artículos TICS*. *La capa física de 802.11.* Obtenido de http://proyredes.blogspot.com.es

Oliver, M. / Escudero, Ana. *Redes de área local inalámbricas según el estándar IEEE 802.11.*

Valle Islas, L. (2005) *Colección de Tesis Digitales Universidad de las Américas Puebla. Biblioteca.* Capítulo 1. WLAN Red Inalámbrica de Área Local. Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/valle_i_lf/capitulo1.pdf

Barajas, S. (2004). Publicaciones de investigación, *Protocolos de seguridad en redes inalámbricas. Obtenido de http://www.saulo.net/pub/inv.php*

México. WNI México. *Tecnología Inalámbrica, Entendiendo el 802.11n.* Obtenido de http://www.wni.mx/index.php?option=com_content&view=article&id=63:80211n&catid=31:general&Itemid=79

España. Ministerio de industria, energía y turismo. (2013). *Cuadro Nacional de atribución de Frecuencias (CNAF), Notas de Utilización Nacional (UN).*

Alonso Montes, José I. / Almorox González, P. / Rodriguez, José A. *WiFi: El diferente uso del espectro en EEUU y Europa.*

Etemad, K. / Lai, Ming-Yee. (2010). *WiMAX Technology and Network Evolution.* Wiley- IEEE Press Editorial.

Nuaymi, Loutfi. (2007). *WiMAX: Technology for Broadband Wireless Access*. Wiley Editorial.

Bonilla, Jonny F. / Gallardo, Antonio E. / Quinatoa, Carlos A. *Estándar 802.16 WiMAX.* Obtenido de www.academia.edu/5202908/Est%C3%A1ndar_802.16_y_WiMax

Eklund, C. / Marks, Roger B. / Wang Stanley. IEEE Standard 802.16: A technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access

Productos Ruckus. (2014) Obtenido de www.ruckuswireless.com

Productos Mikrotik (2014). Obtenido de www.mikrotik.com

Mikrotik (2014) Documentation and Tutorials. Obtenido de www.wiki.mikrotik.com

Mikrotik. *Download Mikrotik software products.* Obtenido de http://www.mikrotik.com/download

Productos Radwin. Obtenido de www.radwin.com

Landatel. *Equipamiento red WiFi*. Obtenido de http://www.landatel.com/index.php/es/

Network World. (2008). *Principios tecnológicos. En clave de MIMO.* Obtenido de http://www.networkworld.es/archive/principios-tecnologicos

Universidad de Buenos Aires. *L2TP-Layer Tunneling Protocol*. Obtenido de http://www.fiuba6662.com.ar/6648/presentaciones/tordillo/Informe-htm-Tordillo/L2TP.htm

(2012) *Historia de las redes inalámbricas*. Obtenido de http://histinf.blogs.upv.es/2010/12/02/historia-de-las-redes-inalambricas/

The Dude. Obtenido de http://www.mikrotik.com/thedude

Colegio Oficial de Ingenieros de Telecomunicación. *WiFi, WiMAX y otras redes inalámbricas. Tecnología y aplicaciones. Programa de innovación internacional.*

Netkrom Group. (2005). *Netkrom.* Obtenido de http://www.netkrom.com/es/about_line_of_sight.php?item=resources

8.2 ANEXOS

Anexo A- Configuración Equipamiento de la red.

La consola Winbox es una pequeña aplicación que nos permite la administración de Mikrotik RouterOS y es la que se utilizará para acceder a la configuración del router Mikrotik, mediante una interfaz gráfica de usuario (GUI) fácil y simple. Se utiliza normalmente con Win32, aunque puede ser ejecutado en Linux y Mac OSX utilizando Wine.

Los pasos a seguir para realizar la configuración básica de los equipos es la siguiente:

1. **Descargar** el programa **Winbox** de la página http://www.mikrotik.com/download

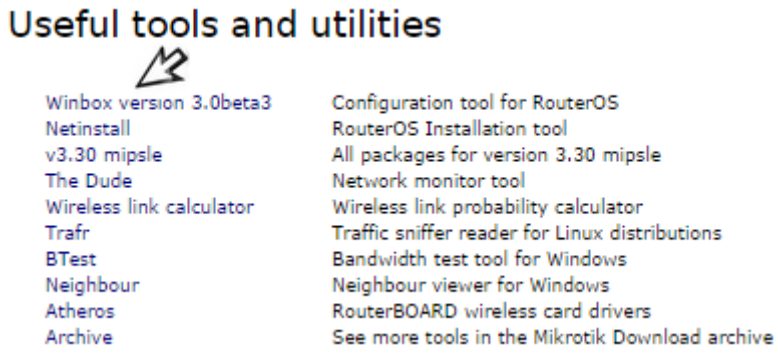


Ilustración 72. Descargar Winbox

2. En los equipos Mikrotik normalmente viene precargada la última versión del SO Mipsbe, en caso contrario, se procede a realizar la actualización de la última versión 6.18, que puede ser descargada desde la misma página que el programa Winbox. Una vez descargado el archivo, se arrastra a Winbox y para que coja los cambios de la nueva versión se digita el comando System→Reboot en la opción New Terminal.

3. Se reinicia el equipo y quedamos a la espera mientras el dispositivo arranca, una vez verificada la conexión y reconocido el Routerboard comienza su configuración.

4. Para que quede totalmente actualizado, es necesario actualizar el Firmware. El Firmware se trata de un software que maneja físicamente al hardware. Para ello se accede desde Winbox a System→Routerboard donde podemos encontrar el modelo de punto de acceso con la versión que tiene. En este caso el equipo tiene la versión 2.41 y la actualizamos a la versión 3.18.

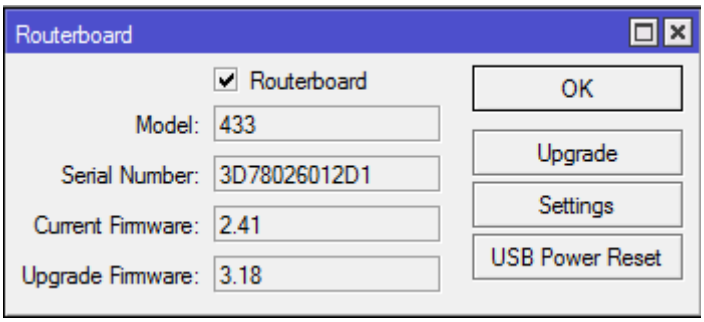


Ilustración 73. Firmware sin actualizar

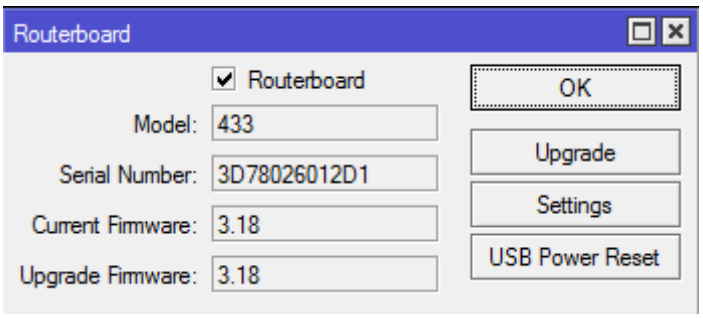


Ilustración 74. Firmware actualizado

5. Se crea un identificador para cada Punto de Acceso. Para ello se accede a System→Identity y se introduce el nombre asignado a cada punto de acceso.

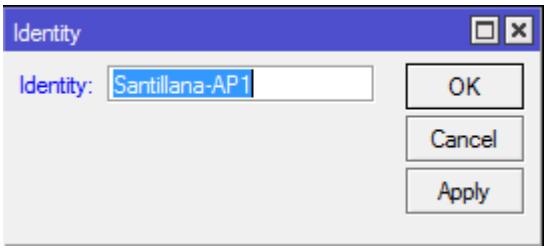


Ilustración 75. Nombre del equipo

Configuración de la seguridad

6. Para securizar el punto de acceso y que ningún hacker pueda acceder a él es necesario crear un nuevo usuario con contraseña y deshabilitar el usuario que viene por defecto para evitar posibles ataques. Para ello, accediendo a System→Users se crea el nuevo usuario.

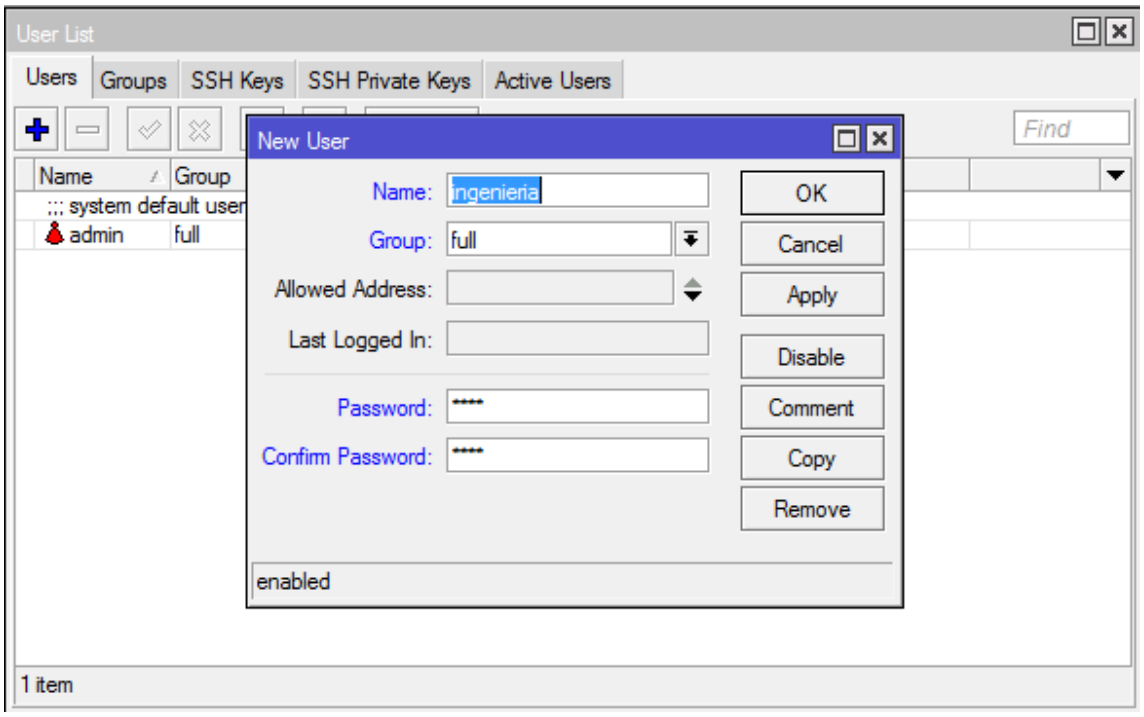


Ilustración 76. Creación de un nuevo usuario

7. Otra medida de prevención y de protección al equipo consiste en deshabilitar los servicios del AP, de forma que solo se pueda acceder a través de Winbox. Se digita el comando IP→Services donde aparecen todos los servicios desde los que se puede acceder al punto de acceso.

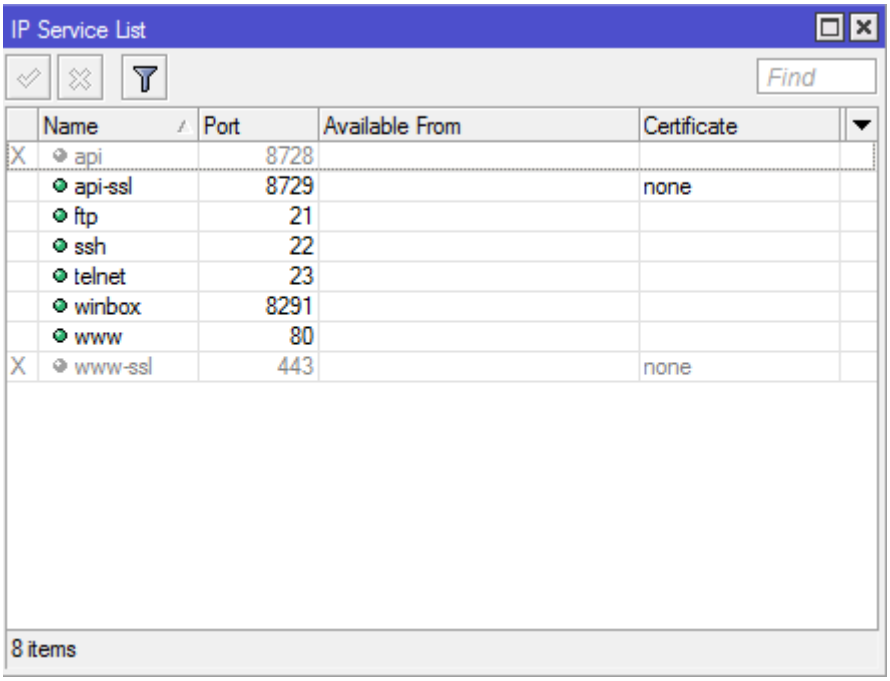


Ilustración 77. Servicios desde los que se puede acceder al AP

En este caso únicamente se deja habilitado el puerto 8291 (Winbox) como

único servicio desde el que se puede acceder al equipo como observamos en la Ilustración 78

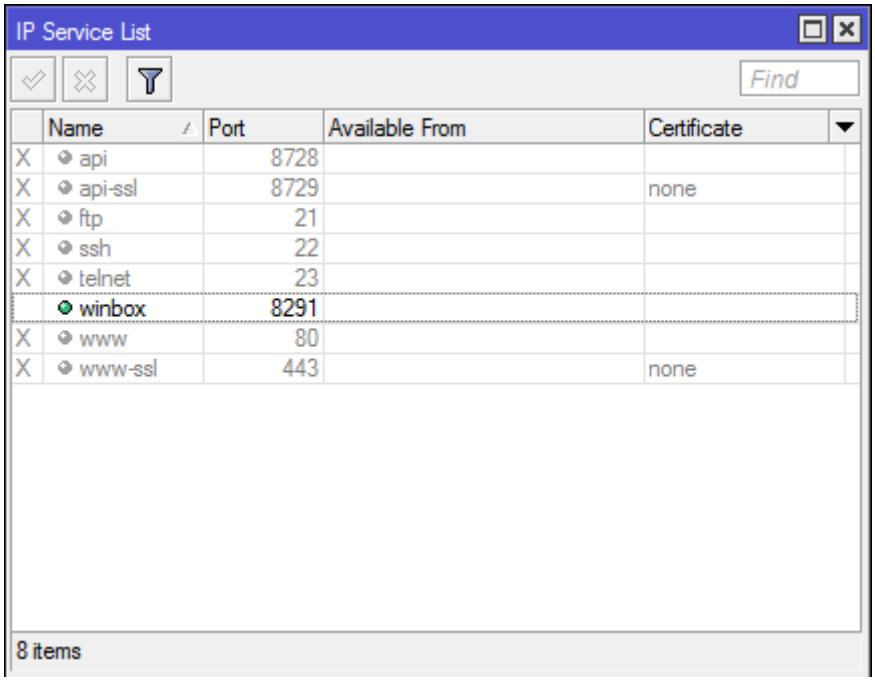


Ilustración 78. Habilitado el servicio Winbox

Configuración de interfaces

8. Se procede ir a la opción IP→Address para configurar el interfaz Ethernet en el AP1. Dicho punto de acceso será el único que esté conectado directamente a la controladora ubicada en el Ayuntamiento y por ello es el único que se conecta a la interfaz Ethernet. Para el resto de puntos de acceso no se efectúa el presente apartado ya que no estarán conectados a través de Ethernet si no que estarán enlazados por Mesh.

   Para configurar el enlace del AP1 con la controladora, se añade una dirección IP que ha sido asignada previamente como podemos observar en el diagrama de red de la Ilustración 66.

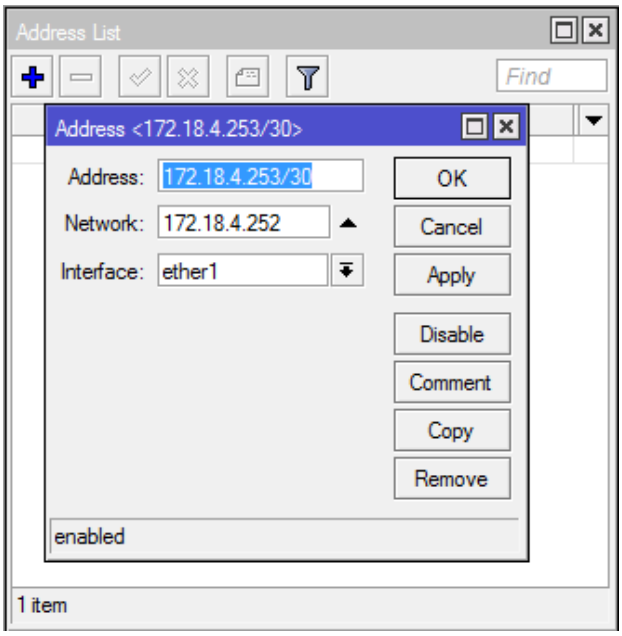


Ilustración 79. Configuración interfaz Ethernet AP1

9. Se configura una ruta de salida a Internet acceciendo a IP→Routes. Asignamos como dirección de destino la IP 0.0.0.0/0 que engloba todo Internet. Para que cada equipo logre tener Internet, se debe configurar el Gateway o Puerta de enlace, que se define normalmente como un equipo configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior.

   Al Punto de Acceso 1, le asignamos el Gateway o puerta de enlace 172.18.4.254 que es por donde le llega Internet. En este punto, a la hora de configurar los demás equipos, el Gateway se cambia por la dirección a través de la cual llega Internet. Por ejemplo, para el AP2 como podemos comprobar en el diagrama de red de la Ilustración 66 asignamos la puerta de enlace 172.18.4.1 que es la vía por donde llegará Internet. De esta forma, todos los equipos lograrán tener acceso a Internet.

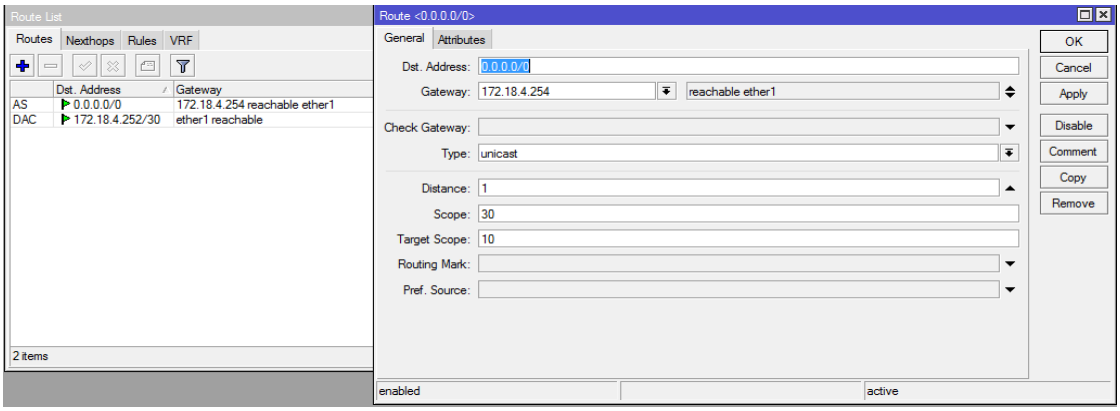


Ilustración 80. Configuración de ruta de salida a Internet

10. Se accede ahora a la opción Wireless para la configuración de la interfaz del equipo que enlazará los puntos de acceso de forma que queden interconectados, la tarjeta de 5GHz**.**

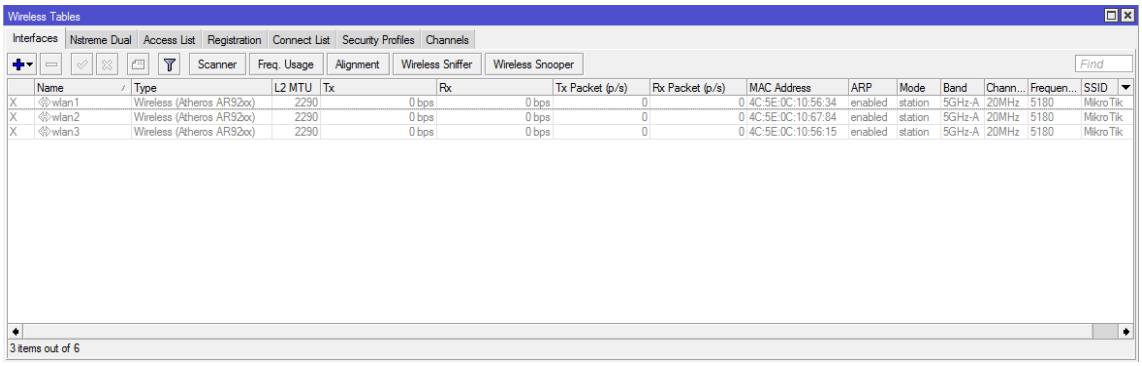


Ilustración 81. Configuración de las interfaces del equipo

En primer lugar, se da doble clic en el interfaz wlan 1 en donde se configura la tarjeta Wireless de 5 GHz para que se efectue el enlace entre los equipos vecinos. Dichas tarjetas se configurarán con los datos de configuración detallados en el diagrama de la estructura de red. En la pestaña General, se cambia el nombre de la interfaz para una mejor identificación.

La interfaz wlan 1→wlan5-1
La Interfaz wlan 2→wlan 2.4

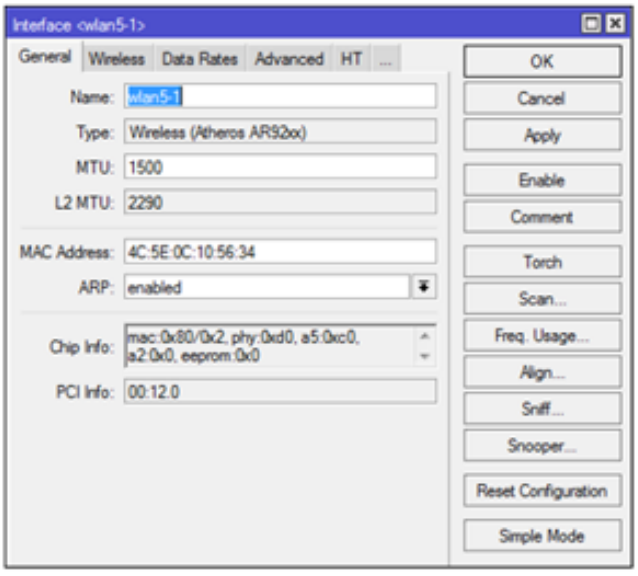


Ilustración 82. Cambio de nombre del interfaz 5GHz

En la pestaña Wireless se colocan los siguientes parámetros:

Mode: APB (AP Bridge)

Band: 5GHz- A/N

Channel Width: 20/40 MHz HT Above (Permite utilizar una extensión adicional

de canal de 20 MHz, la extensión de canal permite al estándar 11n usar 40 MHz de espectro, aumentando así el rendimiento máximo) Above significa que el canal adicional deberá estar por encima del canal principal.

Frequency: 5180 MHz

SSID: Mesh_Santillana_1

Radio Name: AP1

Wireless Protocol: NV2

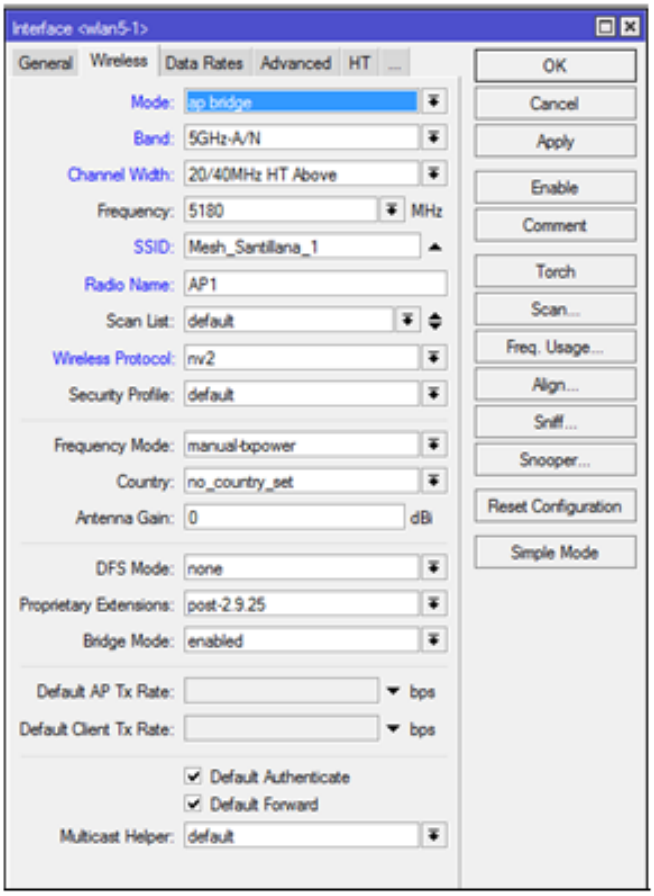


Ilustración 83. Parámetros de configuración tarjeta 5GHz

Para securizar el enlace accedemos a la pestaña NV2, habilitamos la seguridad y cambiamos la contraseña que viene por defecto.

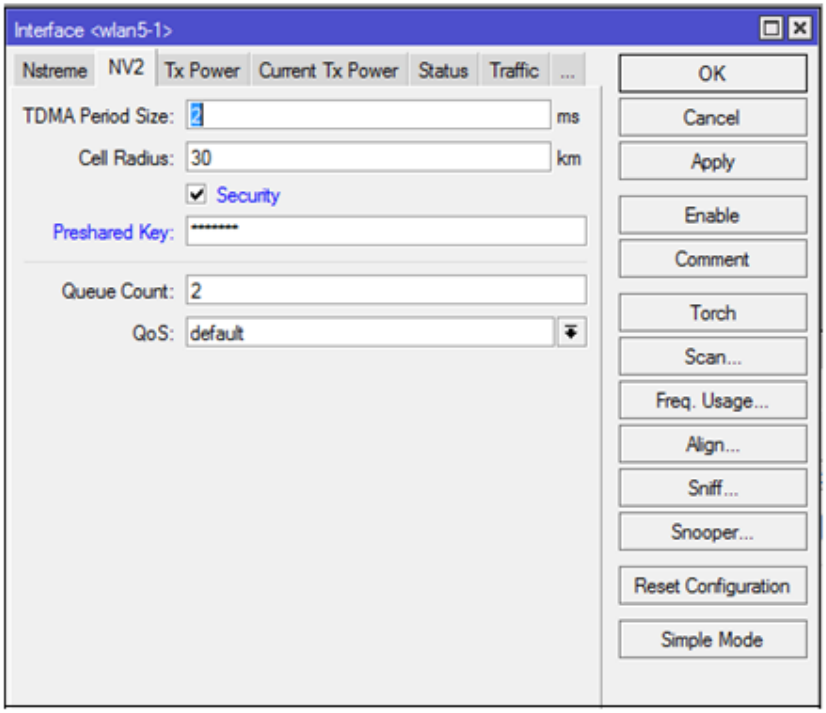


Ilustración 84. Securizar enlace

Una vez configurada la tarjeta Wireless, asignamos a la interfaz de 5GHz la dirección IP y la subred a la que pertenece con el objetivo de que se pueda enlazar con el equipo vecino. Dichos parámetros podemos obtenerlos del diagrama de red.

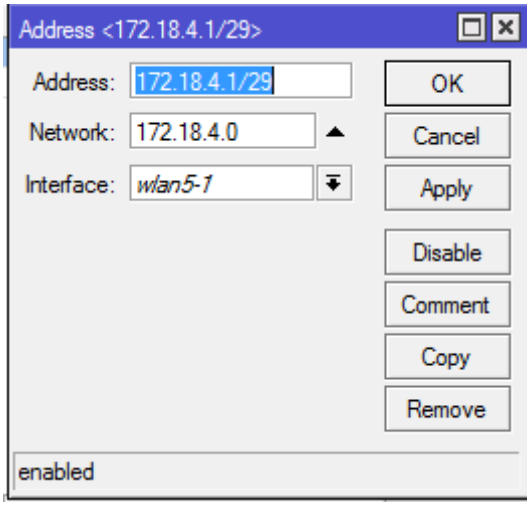


Ilustración 85. Asignar IP y subred

11. A continuación, se configurará la tarjeta de 2.4 GHz que servirá de acceso a la red por parte de los usuarios. Como en el caso anterior se cambia el nombre de la interfaz para una mejor identificación y se modifican los datos correspondientes.

    La Interfaz wlan 2→wlan 2.4

Mode: APB (AP Bridge)

Band: 2 GHz B/G/N

Channel Width: 20/40 MHz HT Above

Frequency: 2412 MHz

SSID: WiFiSantillanaDelMar

Radio Name: AP1

Deshabilitamos el campo Default Forward por seguridad para que solo se pueda ver la información de él mismo con el AP vecino y no se vean todos los APS con todos.

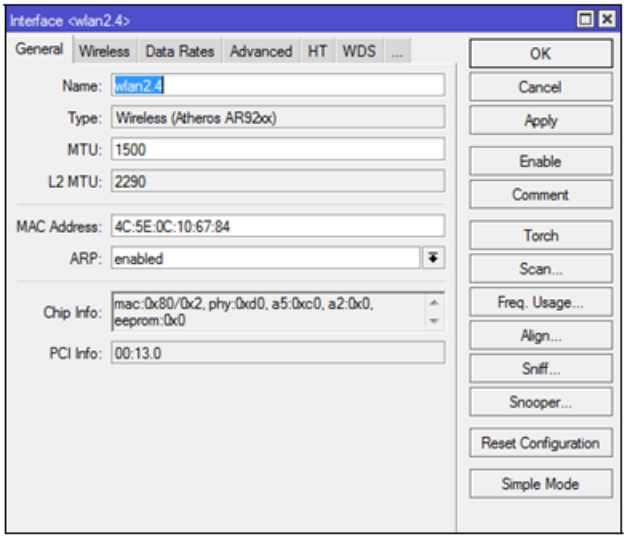


Ilustración 86. Cambio de nombre del interfaz 2.4 GHz

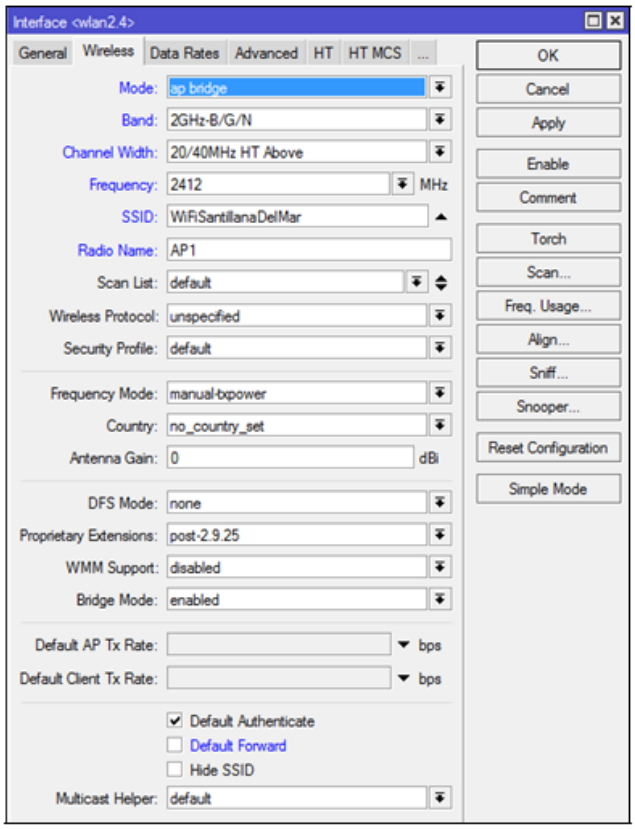


Ilustración 87. Parámetros de configuración tarjeta 2.4 GHz

Debido a que tenemos dos antenas de 2.4 GHz para dar cobertura N, será necesario activar los dos canales para que el tráfico salga por ambas antenas en igualdad de condiciones. Accedemos a la pestaña HT y activamos ambos canales: Chain 1 y Chain 2.

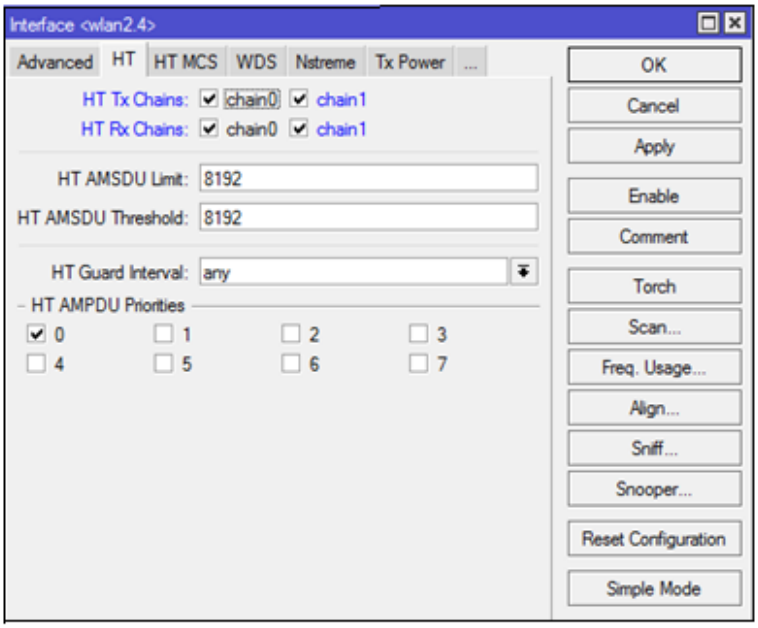
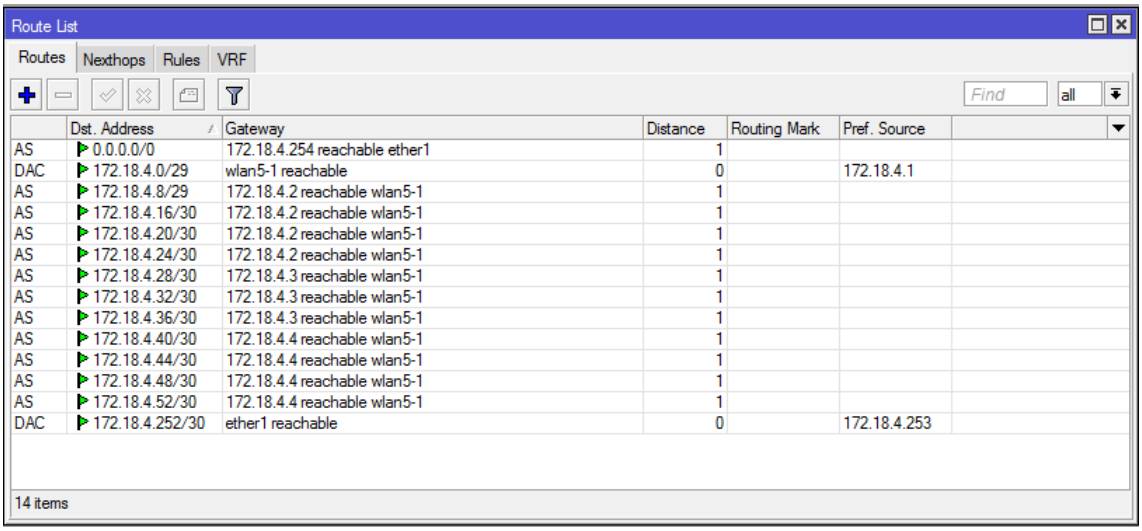


Ilustración 88. Habilitar los dos canales

12. **Configuración de las Rutas:** Para que todos los puntos de acceso sepan donde tienen que llevar el tráfico se deberán configurar las rutas de las subredes. Según el diagrama de la Ilustración 66, las rutas que se necesitan configurar para el punto de acceso uno (AP1) son las que se muestran a continuación:



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	172.18.4.254 reachable ether1	1		
DAC	172.18.4.0/29	wlan5-1 reachable	0		172.18.4.1
AS	172.18.4.8/29	172.18.4.2 reachable wlan5-1	1		
AS	172.18.4.16/30	172.18.4.2 reachable wlan5-1	1		
AS	172.18.4.20/30	172.18.4.2 reachable wlan5-1	1		
AS	172.18.4.24/30	172.18.4.2 reachable wlan5-1	1		
AS	172.18.4.28/30	172.18.4.3 reachable wlan5-1	1		
AS	172.18.4.32/30	172.18.4.3 reachable wlan5-1	1		
AS	172.18.4.36/30	172.18.4.3 reachable wlan5-1	1		
AS	172.18.4.40/30	172.18.4.4 reachable wlan5-1	1		
AS	172.18.4.44/30	172.18.4.4 reachable wlan5-1	1		
AS	172.18.4.48/30	172.18.4.4 reachable wlan5-1	1		
AS	172.18.4.52/30	172.18.4.4 reachable wlan5-1	1		
DAC	172.18.4.252/30	ether1 reachable	0		172.18.4.253

Ilustración 89. Configuración de rutas

Las rutas de los enlaces directos se añaden automáticamente

DAC	172.18.4.0/29	wlan5-1 reachable	0	172.18.4.1

Ilustración 90. Ruta de un enlace directo

Sin embargo, para configurar el resto de las rutas se debe añadir manualmente la subred del enlace e indicar el Gateway de conexión.

13. **Configuración del Firewall**- Un Firewall es un software o dispositivo de hardware que aplica las reglas, organizadas en cadenas, al tráfico que pasa para decidir si permitir o negar el paso. El firewall proporciona un límite de seguridad para la red en el borde de la red o en el host del extremo. La forma de funcionamiento del Firewall sigue una secuencia de estructura IF-THEN:

    IF <condition(s)> THEN <action>

    Si un paquete no coincide con la regla, continúa con la siguiente regla. Si un paquete coincide con alguna regla, entonces se ejecutará la acción definida en 'action' de la regla.

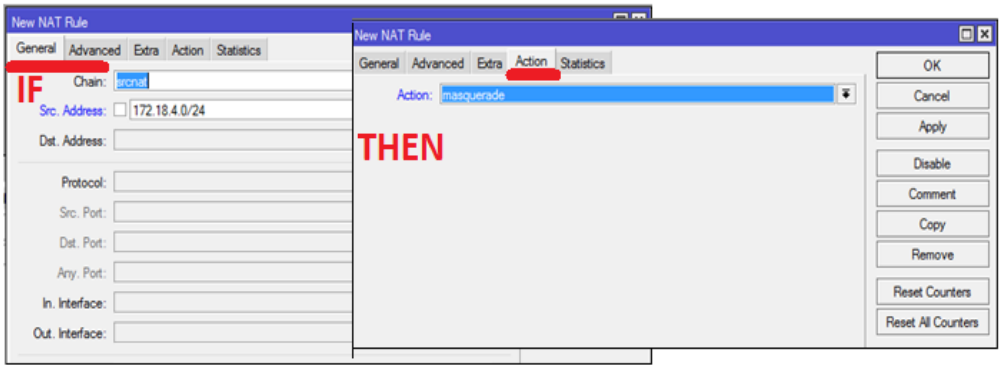


Ilustración 91. Configuración del Firewall

En el caso de nuestra red, se aplicará una regla de NAT y para entender el concepto se explicarán a continuación las ideas principales.

Network Address Translation es un estándar de Internet que permite a los 'hosts' en redes de área local usar un conjunto de direcciones IP para comunicaciones internas y otro conjunto de direcciones IP para comunicaciones externas. Para la explicación del concepto NAT, nos interesan dos tipos de direcciones IP: Direcciones públicas y direcciones privadas.

Las direcciones privadas son rangos especiales de direcciones IP que se reservan para ser utilizadas en redes locales, y se llaman privadas (o no-enrutables) porque no pueden ser utilizadas en Internet. Los routers intermedios que componen todo Internet, no 'entienden' este tipo de direcciones y no las encaminan.

Por lo tanto, se aplicará la regla de traducción de dirección de red o NAT logrando una conexión de pasarela a Internet para que los paquetes de la red inalámbrica lleguen a su destino.

En una configuración típica, como es el caso de esta red, una red local utiliza unas direcciones IP designadas privadas para subredes. Un router en esta red tiene una dirección privada en este espacio de direcciones. El router también está conectado a Internet por medio de una dirección pública asignada por un proveedor de servicios de Internet. Como el tráfico pasa desde la red local a Internet, la dirección de origen en cada paquete se traduce sobre la marcha, de una dirección privada a una dirección pública. El router sigue la pista de los datos básicos de cada conexión activa. Cuando una respuesta llega al routerr, utiliza los datos de seguimiento de la conexión almacenados en la fase de salida para determinar la dirección privada de la red interna a la que remitir la respuesta.

Todos los paquetes de Internet tienen una dirección IP de origen y una dirección IP de destino. En general, los paquetes que pasan de la red privada a la red pública tendrán su dirección de origen modificada, mientras que los paquetes que pasan a la red pública de regreso a la red privada tendrán su

dirección de destino modificada.

La función de la pasarela NAT es cambiar la dirección origen en cada paquete de salida. Estas traducciones de dirección se almacenan en una tabla para recordar qué dirección corresponde a cada dispositivo cliente y así saber dónde deben regresar los paquetes de respuesta.

Existen dos tipos principales de NAT: Uno el cual reescribe la dirección IP origen y/o el puerto origen (src-nat; El otro, que reescribe la dirección IP destino y/o puerto destino (dst-nat)

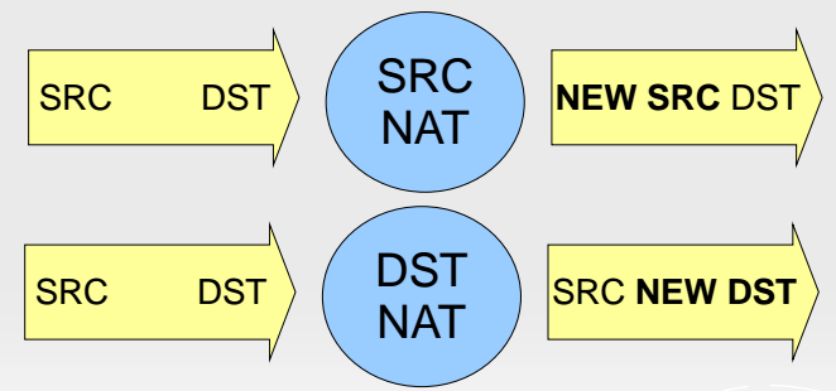


Ilustración 92. Tipos de NAT

En el caso de nuestra red se usará src-nat. El host remoto sabrá a qué IP pública tiene que enviar sus paquetes. Cuando una respuesta o un paquete pertenecientes a esa conexión llegue al router, éste traducirá la dirección IP de destino del paquete (que ahora es la IP del router) y la cambiará por la dirección privada del host que corresponde, para hacer la entrega del paquete a la red local. A continuación se muestra un ejemplo donde se observa lo comentado anteriormente.

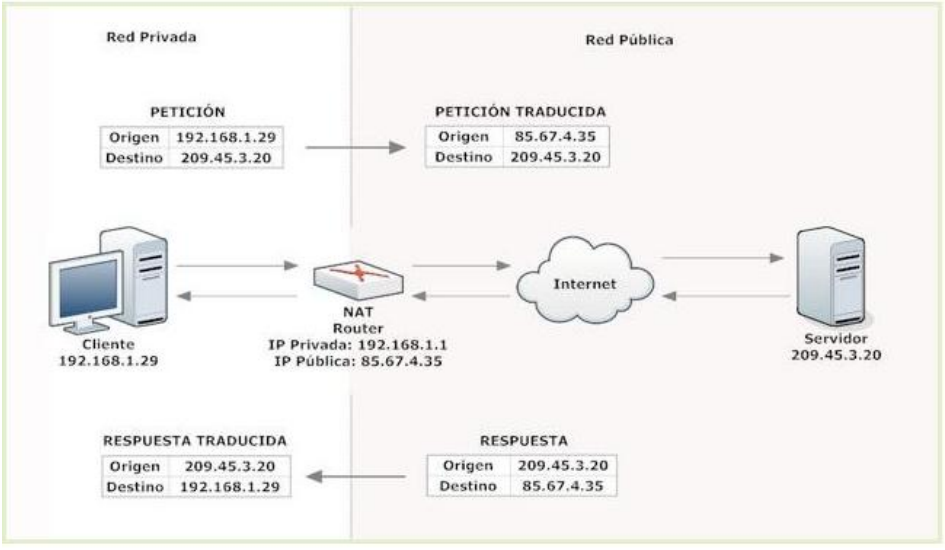


Ilustración 93. Ejemplo de NAT

La configuración de esta regla en los equipos Mikrotik Routerboard 433AH se realiza accediendo a IP→Firewall→NAT. Añadiremos como se ha dicho, en la pestaña General el tipo de NAT: src-nat y la dirección IP que engloba todas las IPs de nuestra red.

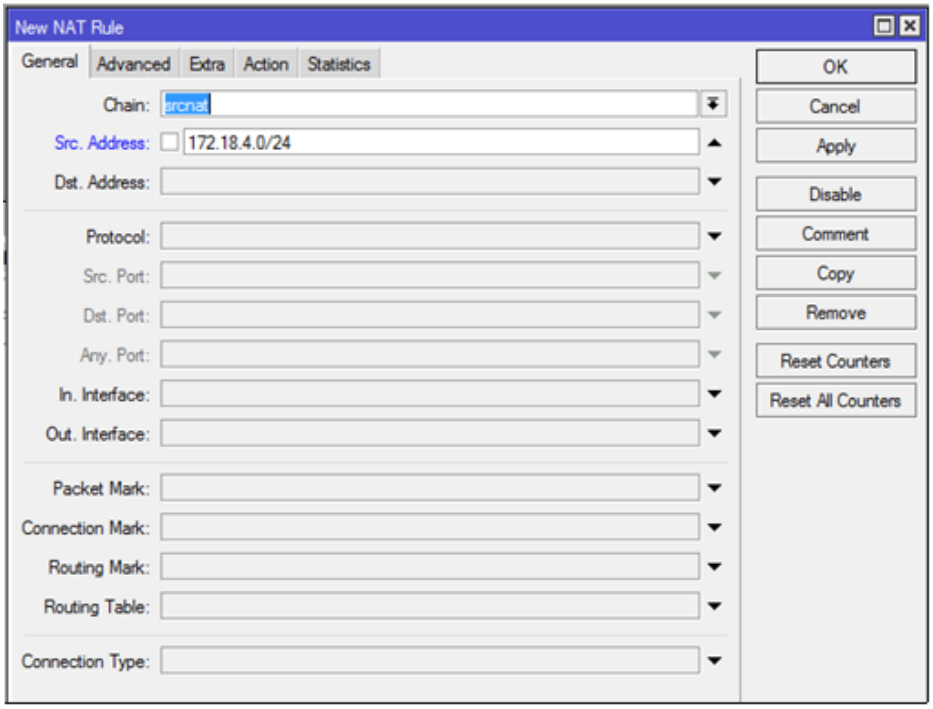


Ilustración 94. Configuración NAT- src-nat

Si esta regla se cumple, entonces se ejecutará la acción, que en nuestro caso utilizaremos, masquerade. Dicha acción enmascara el tráfico y reemplaza la dirección de origen de un paquete por la dirección de origen que determine el router de forma automática.

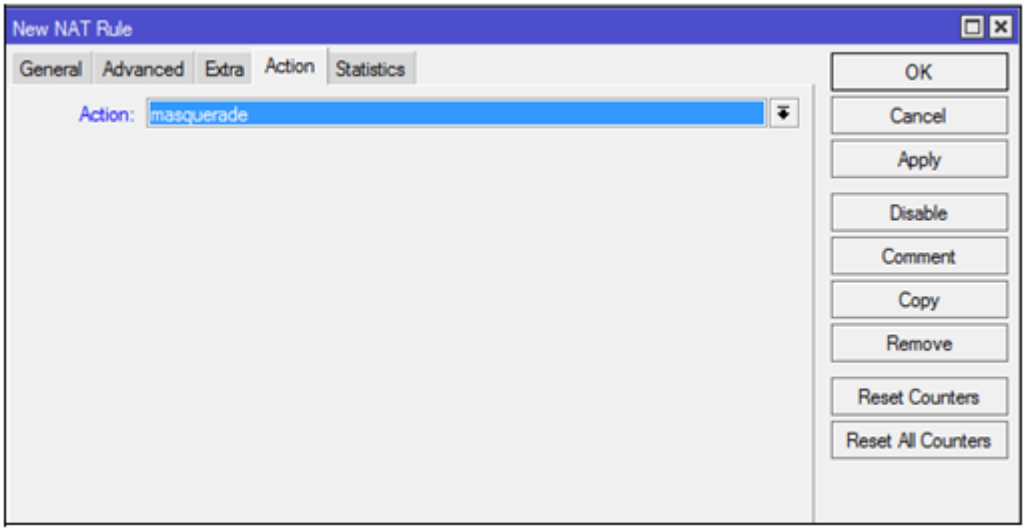


Ilustración 95. Configuración NAT- masquerade

14. **Configuración del tunel L2TP**: El Protocolo de Túnel de Capa 2 (L2TP, Layer Tunneling Protocol) es un protocolo estándar diseñado para transmitir datos y conectar de forma segura redes a través de Internet. L2TP es una extensión del Protocolo Túnel Punto a Punto (PPP, Point to Point Protocol) y emerge de la fusión de las mejores características de los protocolos PPTP de Microsoft y L2F de Cisco. L2TP encapsula las tramas PPP que van a enviarse a través de redes IP, Frame Relay, etc.

    L2TP facilita el "tunelizado" de paquetes PPP a través de una red interviniente, en forma lo más transparente posible a aplicaciones y usuarios finales.

    A su vez, el protocolo PPP, (Point to Point Protocol), provee un método estándar para el transporte de datagramas multiprotocolo sobre enlaces punto a punto.

    PPP está comprendido por tres conceptos principales:

    1. Metodo para el encapsulado de datagramas multiprotocolo
    2. Un protocolo de Control de Enlace (LCP), usado para establecer, confiturar y testear la conexión a nivel del enlace de datos
    3. Una familia de protocolos de control a nivel de red, (NCP), para establecer y configurar los diferentes protocolos de nivel de red.

    Este protocolo está diseñado para enlaces simples que transportan paquetes entre dos puertos. Estos enlaces proveen operación 'Full duplex' bidireccional simultánea y transportan los paquetes en orden.

    PPP encapsula paquetes de Nivel 2 en enlaces punto a punto. Los usuarios se conectan a las redes accediendo a un Network Access Server, (NAS). El extremo de la conexión PPP y la terminación L2 residen en el NAD. L2TP extiende el modelo PPP permitiendo que los extremos L2 y PPP residan en diferentes dispositivos interconectados por una red de conmitación de paquetes. Cpm L2TP, un usuario tienen una conexión L2 a un concetrador de acceso. El concentrador, tuneliza las tramas PPP hacia el NAS. Esto permite que el procesamiento actual de paquetes PP sea independiente de la terminación del circuito L2. La ventaja es que en lugar de terminar la conexión L2 en el NAS, la conexión termina en un circuito concentrador local, el que extiende la sesión PPP sobre una infraestructura compartida tal como Internet. Todo esto ocurre sin cambios visibles para el usuario.

    L2TP incluye autenticación PPP y la contabilidad de cada conexión L2TP. La autenticación y la cuenta de cada conexión se pueden realizar a través de un cliente de RADIUS o localmente.

    L2TP utiliza dos tipos de mensajes: Mensajes de contol y mensajes de datos; Los mensajes de control se utilizan para el establecimiento, mantenimiento y

despeje de túneles y llamadas, mientras que los mensajes de datos son utilizados para encapsular las tramas PPP que se transportan en el túnel.

El tráfico de L2TP utiliza el protocolo UDP para ambos tipos de paquetes. Usa el puerto UDP 1701 solamente para el establecimiento del enlace mientras que el tráfico utiliza cualquier puerto UDP disponible. Esto significa que L2TP puede ser utilizado con la mayoría de los Firewalls y routers permitiendo al tráfico UDP ser encaminado a través del firewall o router.

La configuración del túnel L2TP bajo RouterOS en nuestro caso se hace como se muestra a continuación:

Accediendo a PPP→Profiles creamos un perfil específico para el túnel L2TP

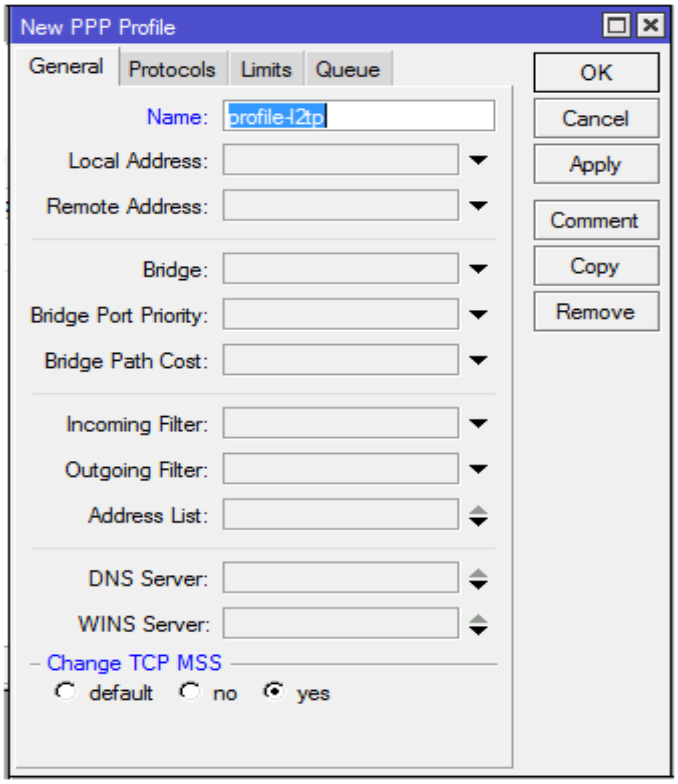


Ilustración 96. Configuración túnel L2TP- Creación de perfil

En la pestaña Protocols la única opción que cambiamos es Use Encryption: No

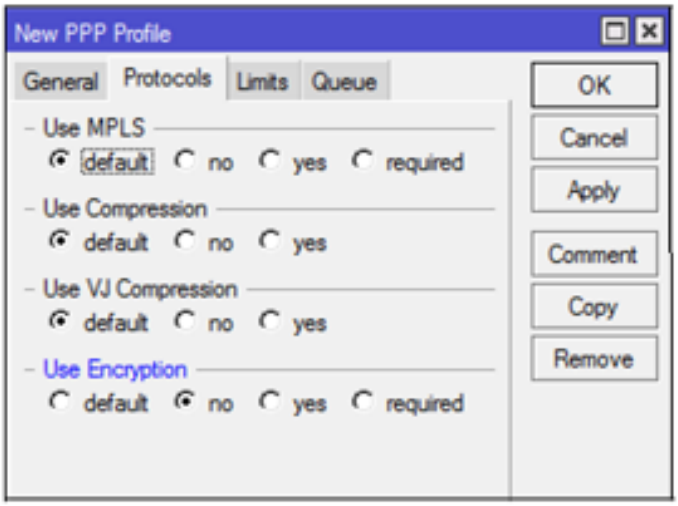


Ilustración 97. Configuración túnel L2TP- Protocolos

En PPP→Interface añadimos el nombre de un nuevo interfaz L2TP Client

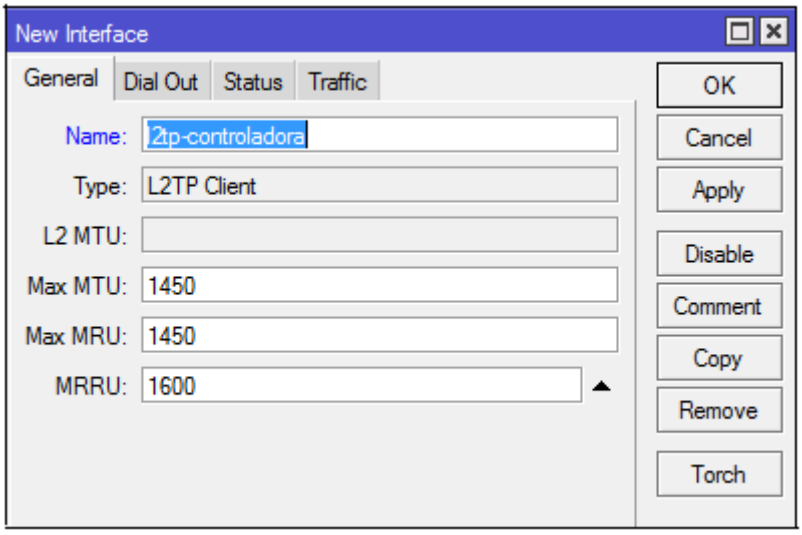


Ilustración 98. Configuración túnel L2TP - Interfaz L2TP Client

Se configuran los datos del túnel. Se añade la IP de la controladora, el usuario y la contraseña (tienen que coincidir con los datos de la controladora) y seleccionamos el perfil previamente configurado, l2tp.

En la pestaña Dial Out cambiamos los siguientes parámetros:

IP de la controladora: 172.18.4.254

Usuario: santillanaAP1-l2tp

Profile: profile-l2tp

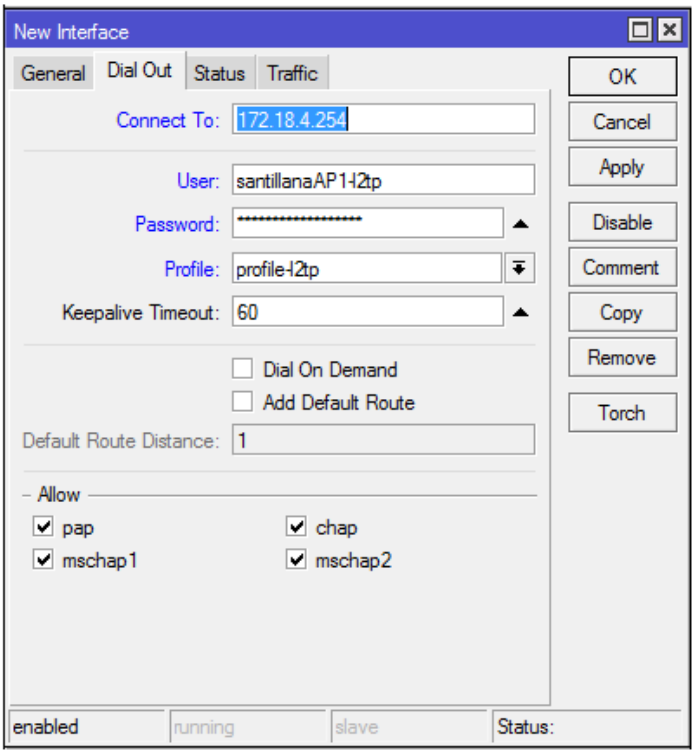


Ilustración 99. Parámetros de configuración

Una vez que se haya establecido la conexión del tunel, en IP Address aparecerá la IP que nos ha asignado la controladora al tunel L2TP.

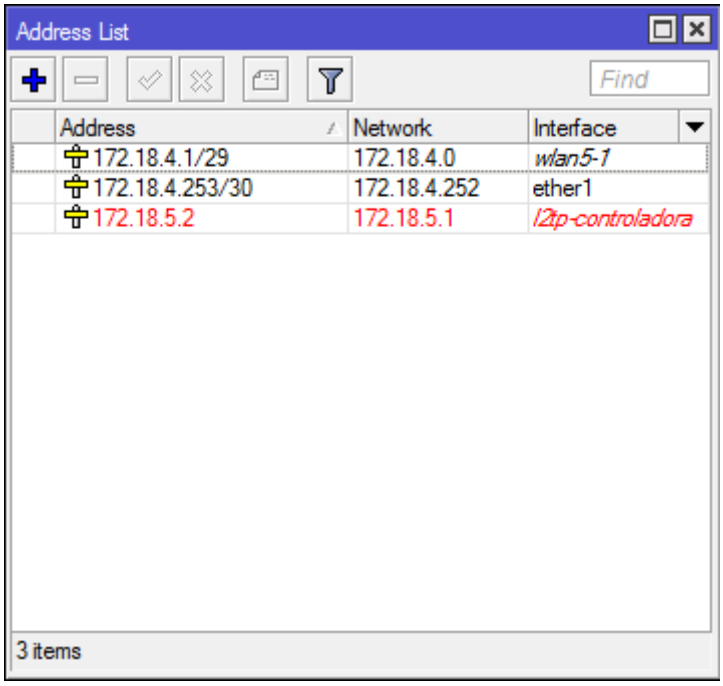


Ilustración 100. IP asignada por la controladora

15. **Configuración del tunel EoIP (Ethernet Over IP):** EoIP es un protocolo que crea un tunel Ethernet entre dos routers (on top of an IP connection). El túnel EoIP puede ejecutarse sobre PPTP o sobre cualquier otra conexión capaz de

transportar IPs. Cuando la función de puenteo del router está activada, todo el tráfico Ethernet se puenteará como si hubiese una interfaz física Ethernet y cable entre los dos routers.

Las configuraciones de red que se pueden realizar con EoIP son las siguientes:

- Posibilidad de puentear LANs sobre Internet

- Posibilidad de puentear LANs sobre túneles cifrados.

- Posibilidad de puentear LANs sobre redes inalámbricas 802.11b 'ad-hoc'.

El protocolo EoIP encapsula las tramas Ethernet en paquetes GRE (protocolo IP número 47 cuya función es establecer túneles a través de Internet) y las envía al extremo remoto del túnel EoIP.

La configuración del tunel EoIP en nuestro caso lo haremos de la siguiente manera: Accedemos a Interface→EoIP y añadimos los parámetros correspondientes que además tendrán que coincidir con los datos de la controladora para que se haga efectivo el túnel.

Name: Santillana-AP1 EoIP

Remote Address: 172.18.5.1 (Dirección IP del extremo remoto del túnel EoIP)

Tunel ID: 101 (Identificador de túnel único. Debe coincidir con el otro lado del túnel, la controladora)

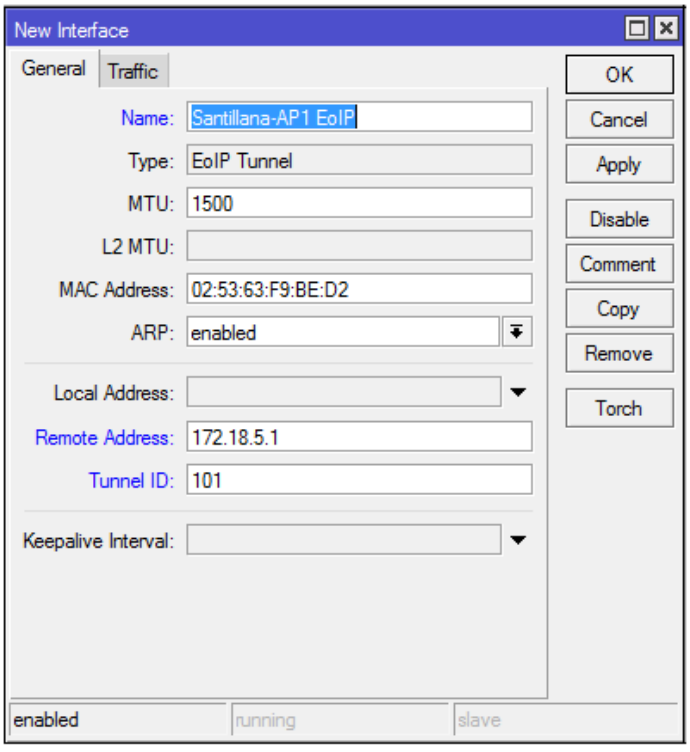


Ilustración 101. Configuración EoIP

16. **Configuración del Bridge:** Es necesario configurar un Bridge para la unión del interfaz Wireless 2.4 de acceso y el túnel EoIP que se encargará de pasar la información del usuario a la controladora y viceversa. Para ello, accediendo a Interface→Bridge añadimos el nombre de la interfaz: bridge_Santillana_AP1.

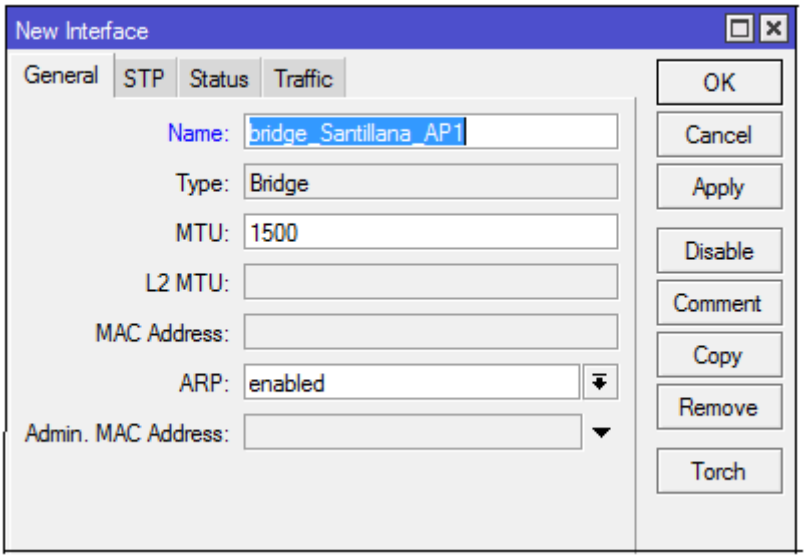


Ilustración 102. Configuración del Bridge

En la pestaña STP dejamos todo por defecto.

Una vez configurado el bridge se añade en Ports las interfaces que queremos unir: La tarjeta de acceso WLAN 2.4 y el tunel EoIP

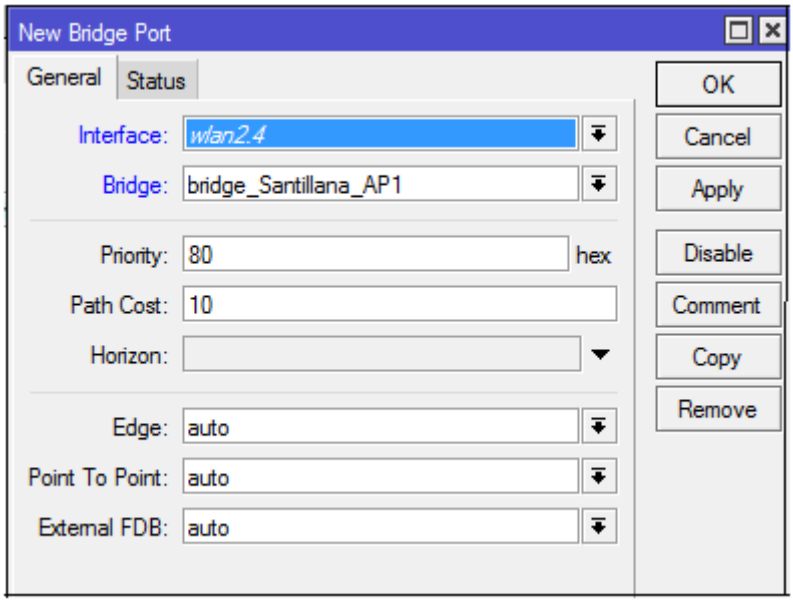


Ilustración 103. Configuración del Bridge- Interfaces a unir

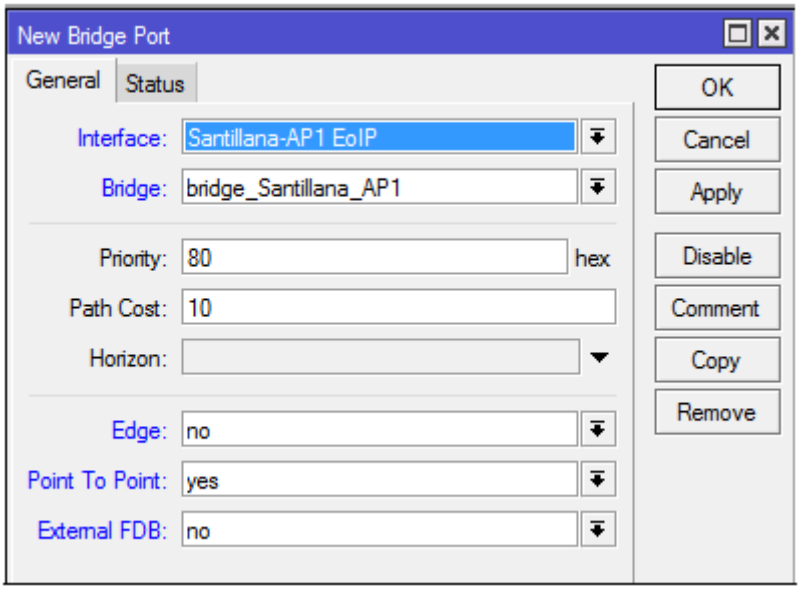


Ilustración 104. Configuración del Bridge

En la Ilustración 104 marcamos Yes en la pestaña Point to Point ya que de esta forma no se pueden ver el resto de túneles entre sí, sino que sólo se verá el tunel creado entre un equipo y la controladora.

17. **Comprobación de la configuración**: Para comprobar si los equipos se han enlazado correctamente se accede a Wireless→Registration. Se comprueba como vemos en la Ilustración 105 que el AP1 ha quedado enlazado con el AP2 correctamente.

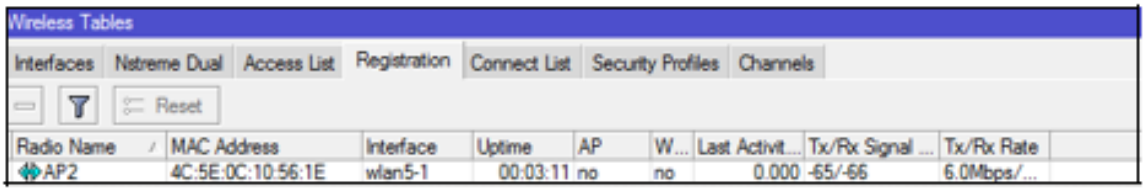


Ilustración 105. Comprobación enlace correcto

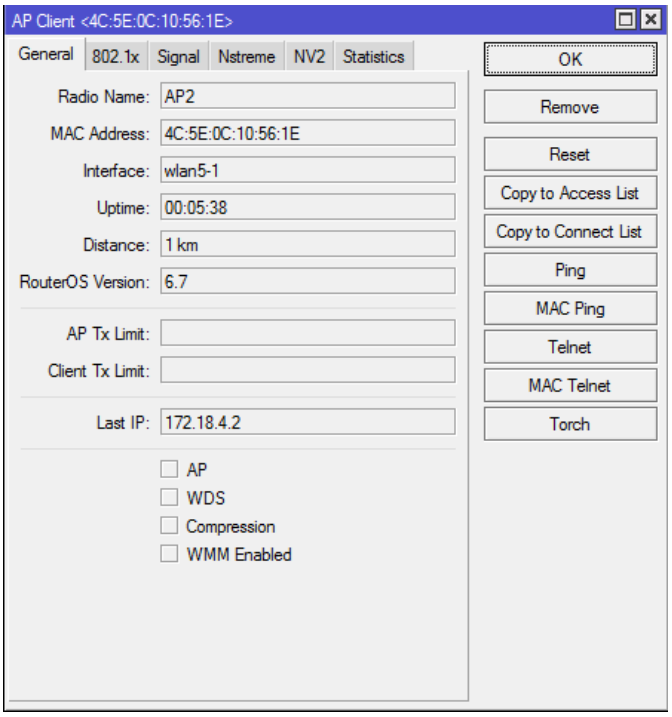


Ilustración 106. Comprobación de la configuración

Se puede realizar un Bandwith Test para comprobar el enlace

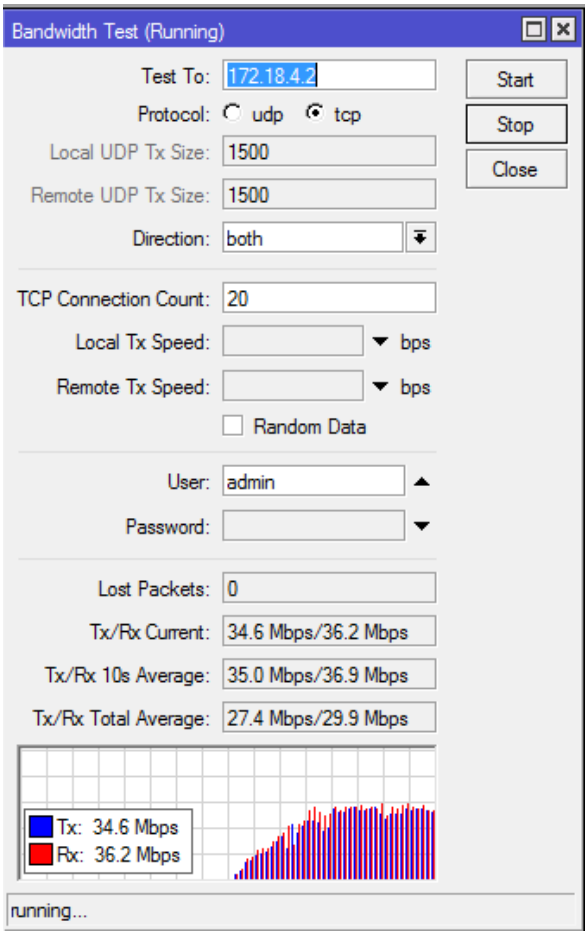


Ilustración 107. Bandwith Test

Configuración de la controladora

Este apartado trata de resumir los pasos necesarios para la correcta configuración de nuestra controladora. Se configurará a través del programa Winbox, de igual manera que los puntos de acceso.

Para comenzar con la configuración, accediendo a IP→Addresses se elimina la IP que viene por defecto y se crea otra nueva. Se cambia la IP fija del ordenador y nos conectamos a la controladora por IP, de forma que se realice una conexión punto a punto entre la controladora y nuestro computador.

Configuración Hotspot

En primer lugar, se configurará nuestro hotspot. Los pasos a seguir se muestran a continuación.

Creación del Interfaz Bridge

Lo primero de todo es crear un interfaz Bridge. Para ello, se accede al menú Bridge y se añade uno. El nombre del bridge no influye en nada. Como referencia usaremos el nombre que le vayamos a dar al hotspot: **Zona-Santillana**. Es importante fijar la MAC del interfaz usando el Admin MAC Address, de otra forma la MAC del bridge podría variar y haría que los clientes asociados a la red no pudieran navegar. También es necesario activar la opción ARP "reply-only", de esta manera evitaremos que los usuarios se intenten conectar con una IP estática al hotspot.

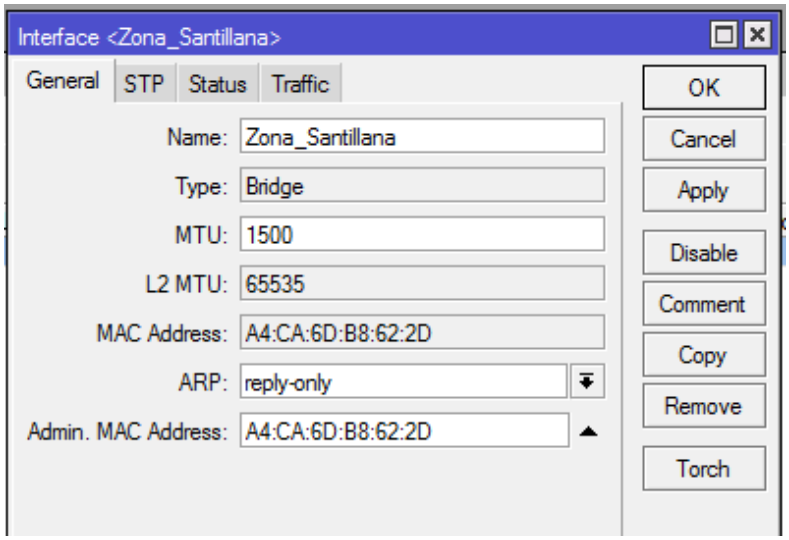


Ilustración 108. Configuración del interfaz Bridge

Para terminar la configuración del interfaz es necesario activar el protocolo RSTP para garantizar una topología sin bucles para nuestra LAN puenteada. Para asegurarse que el bridge del hotspot sea el bridge-root bajamos la prioridad a 1000.

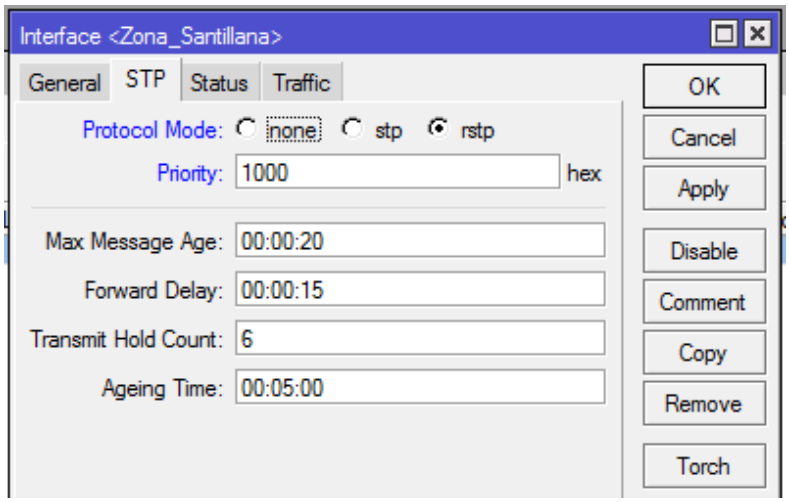


Ilustración 109. Protocolo RSTP

Dentro de la ventana Bridge es necesario ajustar el Settings para activar el Firewall del Bridge. También para las VLANs. De lo contrario no se mostraría el bridge-port de los clientes del hotspot.

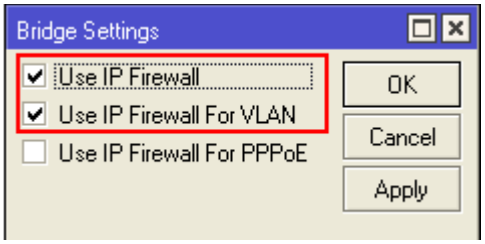
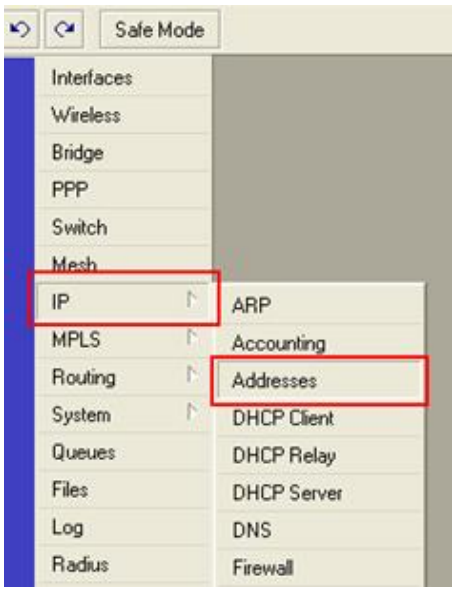


Ilustración 110. Activar Firewall del Bridge

Asignar direccionamiento

Una vez creado el Bridge, pasamos a configurar el direccionamiento en el menú IP→Addresses.



Asignamos la dirección IP en nomenclatura CIDR (Enrutamiento entre dominios sin clases). Esta IP es la que se va a dar a los usuarios DHCP

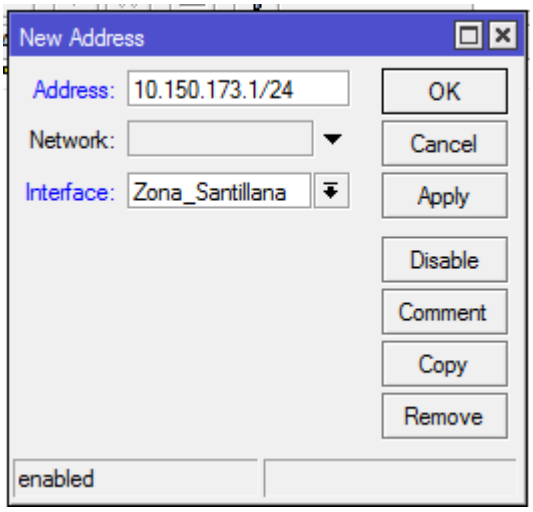


Ilustración 111. Asignación de dirección IP

Configuración del DHCP-Server

Se configura en el Menú IP→ DHCP Server.

Lo más sencillo es utilizar el asistente que tiene disponible el RouterOS. Para ello hay que seleccionar DHCP Setup, seleccionar el interfaz sobre el que queremos configurar el DHCP e ir siguiendo los pasos que indica el configurador.

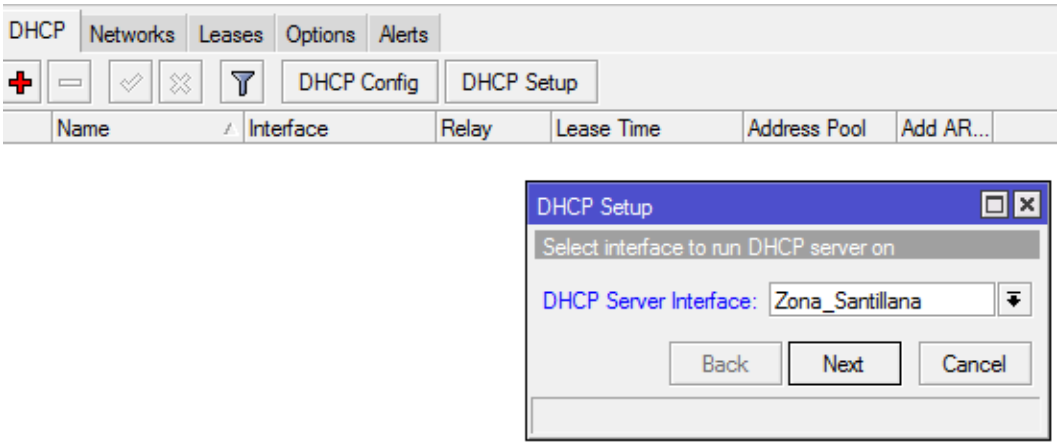


Ilustración 112. Configuración del DHCP server

Nos pregunta por el espacio del direccionamiento (coincide con la dirección del red del interfaz en el que queremos configurar el DHCP)

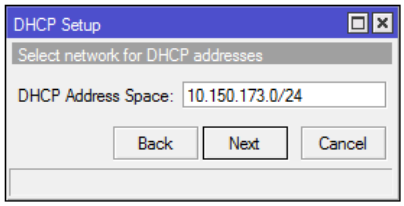


Ilustración 113. Espacio del direccionamiento

El Gateway (coincide con la IP del interfaz)

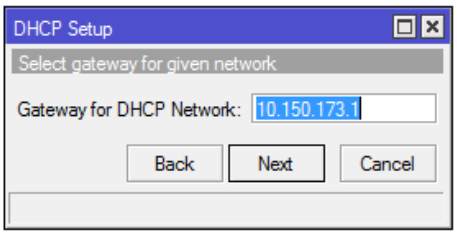


Ilustración 114. Gateway

El pool de direcciones. Podemos reservar algunas direcciones por si es necesario conectar equipos que no se conecten por DHCP. En este caso no dejaremos ninguna dirección libre porque todos los equipos se conectarán por DHCP.

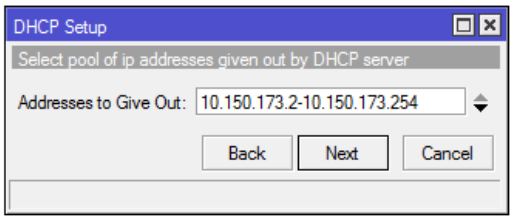


Ilustración 115. Pool de direcciones

Nos preguntará por los DNS. Por defecto nos asignará los que tenga configurados la controladora. Estas son las DNS que seleccionarán los clientes para navegar.

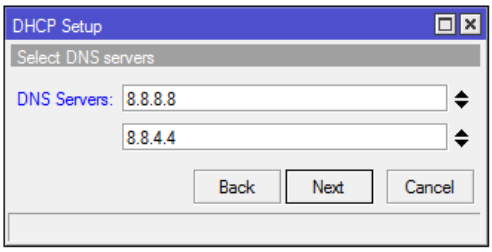


Ilustración 116. DNS

El Lease Time. Si estamos usando direcciones públicas, lo mejor es que no se superen los 5 min, de esta forma se hará un uso más eficiente de las mismas. Si por lo contrario usamos IPs privadas, podemos dejarlo en 20, 30 minutos o incluso 1 hora.

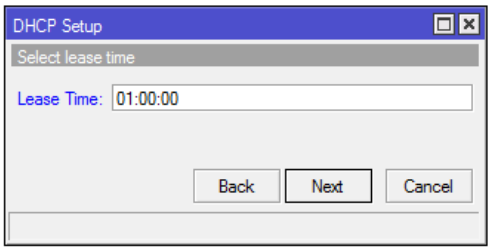


Ilustración 117. Lease Time

Una vez hecho esto, nos aparece una pantalla indicando que el DHCP ha sido configurado con éxito.

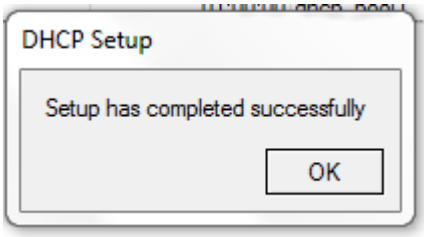


Ilustración 118. Configurado con éxito

Para evitar que los usuarios se intenten conectar con IP manual en el hotspot, configuramos la opción "Add ARP for leases", ya que el interfaz bridge tiene la opción "reply-only" para el ARP.

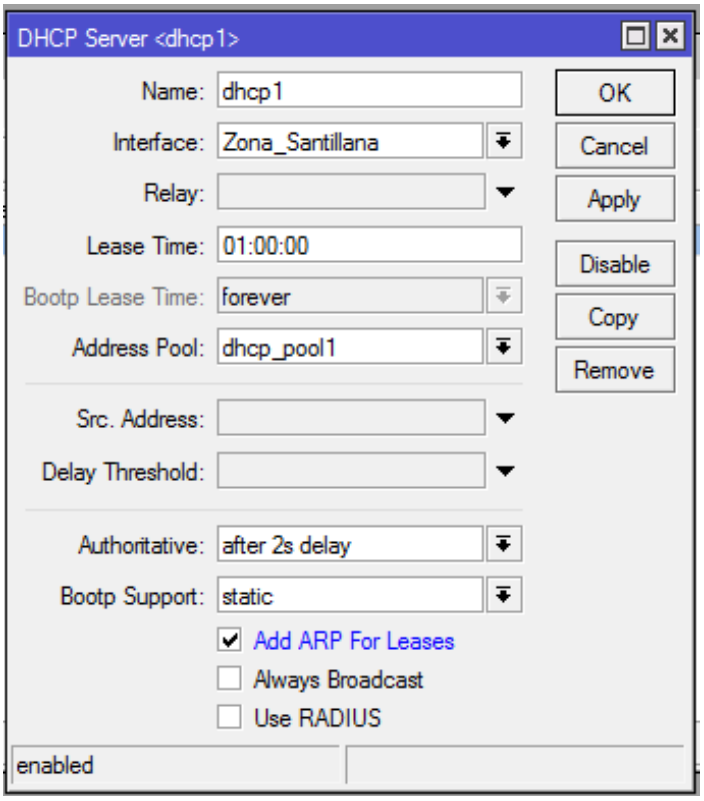


Ilustración 119. Configuración Add ARP for leases

Importación de los certificados SSL

Todos los hotspot deben tener un certificado SSL que permite la comunicación segura para el intercambio de contraseñas entre los dispositivos y la controladora. El certificado que utilizamos se trata de un CA.crt de VeriSign. Al igual que el certificado roaming1.santillana.com.

Lo primero es arrastrar los archivos hasta el Files de la controladora

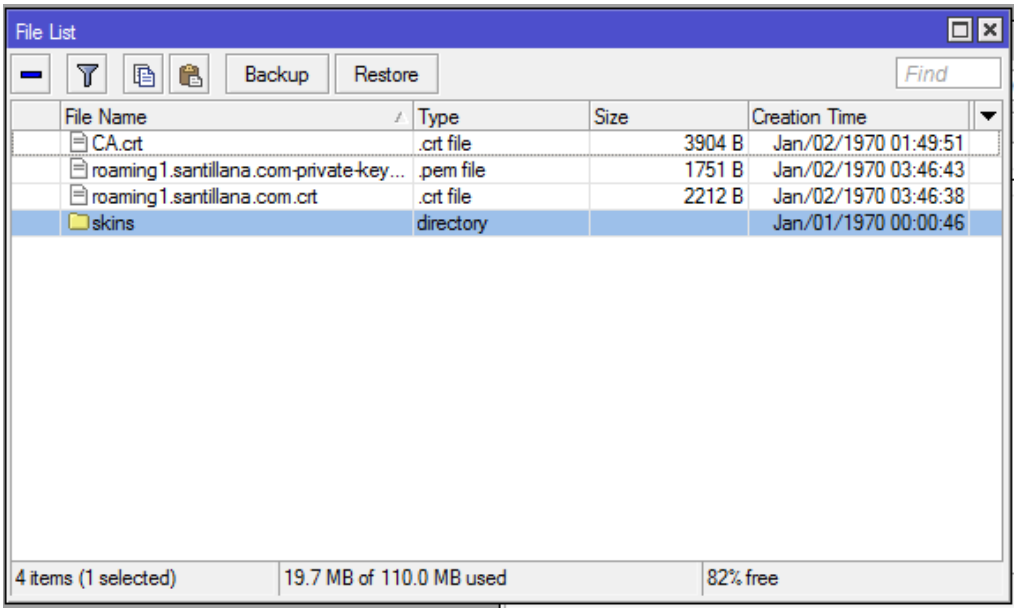


Ilustración 120. Importación de los certificados

Para importarlos, vamos al menú System→Certificates e importamos el CA.crt. Aparecerán 2 certificados, el primero el certificado primario y el segundo el G3. Si no importáramos el certificado raíz y sólo importásemos el de roaming, aparecería un error en los navegadores de seguridad.

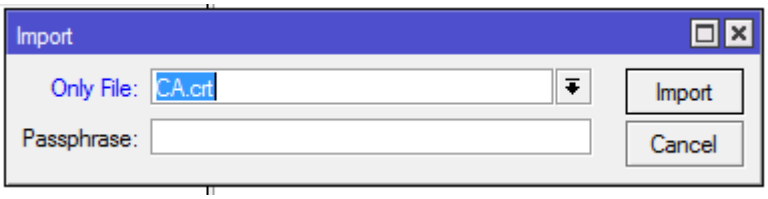


Ilustración 121. Importación de los certificados

A continuación, importamos el certificado roaming1.santillana.crt y por último la key que es necesaria para firmar el certificado. El passphrase es confidencial.

La estructura de certificados debería quedar de la siguiente manera:

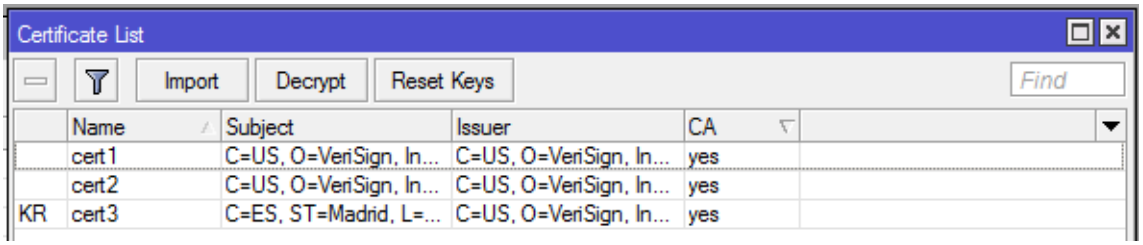


Ilustración 122. Certificados importados

Configuración del hotspot

Nos dirigimos al menú IP→ hotspot.

Al igual que para configurar el DHCP, lo más sencillo es utilizar el asistente del que dispone el RouterOS seleccionando Hotspot Setup y el interfaz sobre el que queremos configurar el Servicio. Después se realizarán las modificaciones oportunas en los perfiles creados.

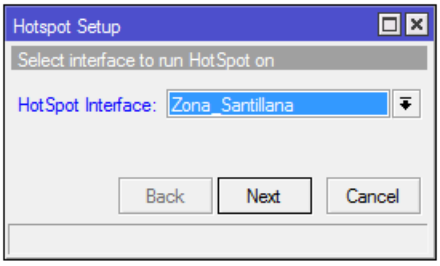


Ilustración 123. Configuración Hotspot

Lo primero es la dirección local del hotspot, siempre va a coincidir con la IP del Interfaz Bridge.

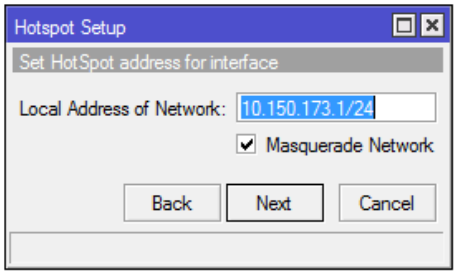


Ilustración 124. Dirección local del hotspot

El pool de direcciones coincide con el mismo que se había configurado en el DHCP.

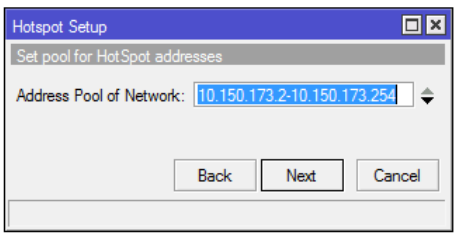


Ilustración 125. Pool de direcciones

Seleccionamos el certificado firmado que hemos importado

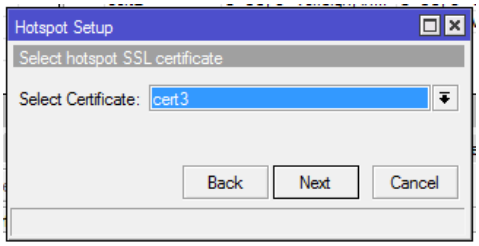


Ilustración 126. Certificado

El SMTP no lo utilizamos

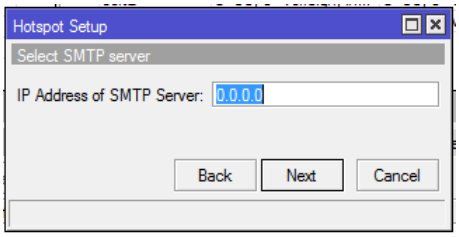


Ilustración 127. SMTP

Configuramos los DNS. Por defecto aparecen los que están configurados en la controladora

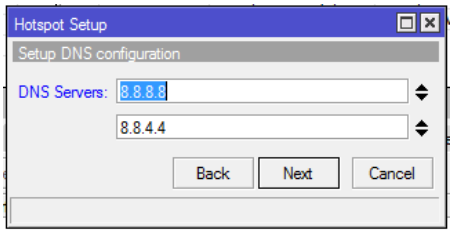


Ilustración 128. Configuración DNS

El DNS Name es el nombre contra el que va a resolver el hotspot. Siempre tiene que coincidir con el nombre del dominio que aparece en el certificado, de lo contrario aparecería un error de certificado

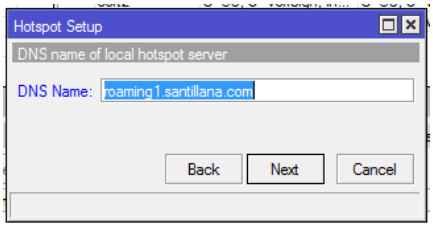


Ilustración 129. DNS Name

Al terminar la configuración aparecerá un mensaje indicando que la configuración se ha ejecutado correctamente

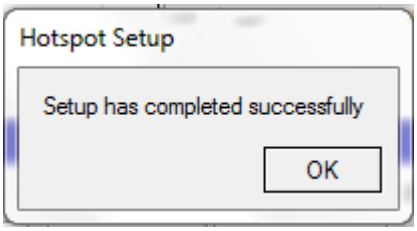


Ilustración 130. Configuración ejecutada con éxito

Pasamos a editar los "Profiles" que se han generado al configurar el Hotspot. El primero es el **Server Profile**. Le asignamos un nombre que haga referencia a la red a la que se va a dar servicio. El Hotspot Address es la IP donde el hotspot escuchará las peticiones de logueo y deslogueo. Siempre tiene que coincidir con la resolución del certificado. El último parámetro de la pestaña general que hay que configurar es el directorio donde se alojarán los archivos asociados al hotspot (rlogin.html, login.html, status.html…) Al igual que el nombre, que le asignamos uno que haga referencia a la red.

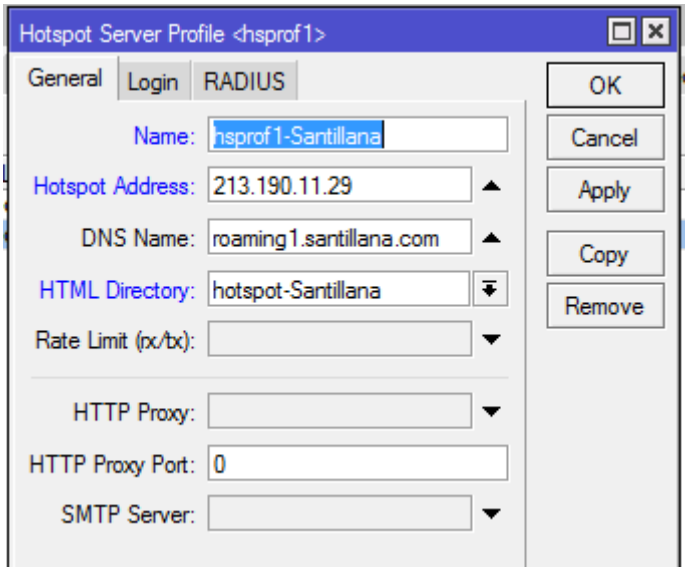


Ilustración 131. Server Profile

La siguiente pestaña es la del Login. La validación en nuestra controladora se hace mediante los siguientes métodos: HTTP PAP, HTTPS y Trial. Todas las demás opciones deben estar deshabilitadas.

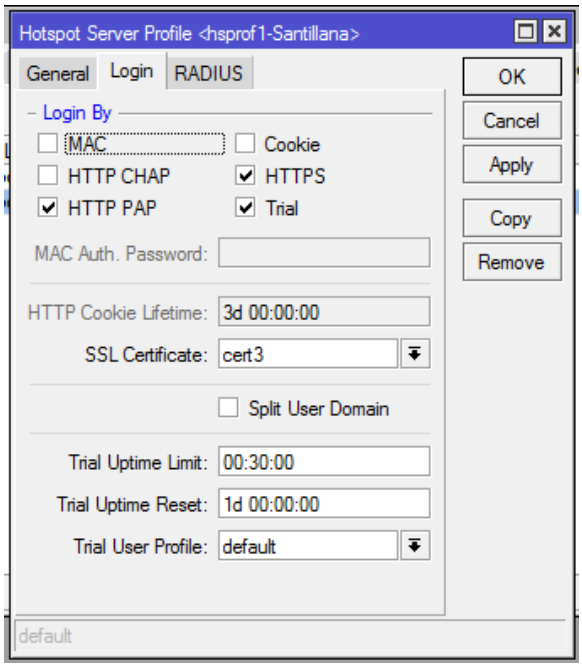


Ilustración 132. Configuración Login

En la pestaña de RADIUS debemos activar la opción Use RADIUS, el Accounting y fijar el Update cada 3 minutos. Por otro lado hay que configurar el Location ID y el Location Name con un nombre identificativo de la red.

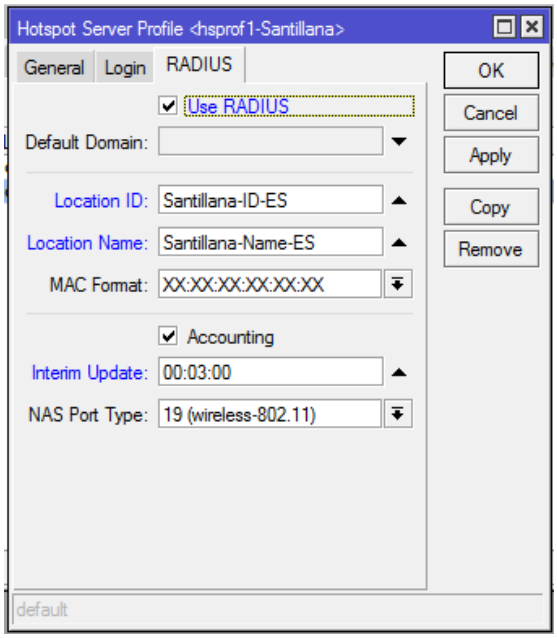


Ilustración 133. Configuración Radius

A continuación, procedemos a la Configuración del **Hotspot-Server** (Called-Station-Id). Se cambia el nombre del hotspot. Este parámetro es muy sensible ya que se envía al RADIUS. También hay que comprobar la IP del DNS Name que coincida con la IP local del hotspot y que el HTTPS está funcionando

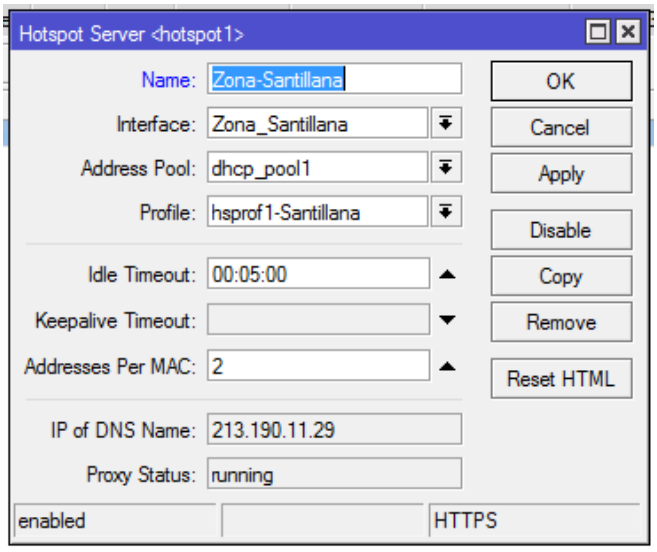


Ilustración 134. Configuración del Hotspot-Server

Por último hay que configurar el Walled-Garden (Listado de URLs permitidas a los usuarios para la navegación sin necesidad de estar validados).

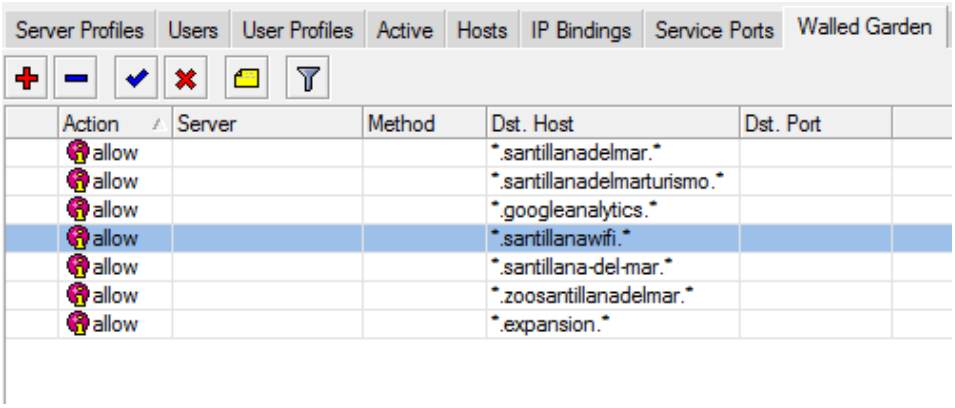


Ilustración 135. Configuración Walled-Garden

Modificación de los archivos del hotspot

El hotspot creado tiene los archivos por defecto, es decir, aparecería un portal captivo genérico de Mikrotik. En el caso de querer personalizar un portal captivo habría que añadir un archivo html en el Files de la controladora.

Una vez configurado el hotspot, se procede a configurar los túneles L2TP y EoIP que transportarán el tráfico IP desde la controladora hasta los Puntos de Acceso.

Configuración túnel L2TP

Para crear el túnel L2TP accedemos a PPP y creamos el "profile". Se hace de manera similar a como lo hicimos con los Puntos de Acceso.

En PPP Interface accedemos a L2TP server, lo habilitamos y añadimos el perfil que hemos creado anteriormente, para que todos los túneles L2TP tengan el mismo perfil.

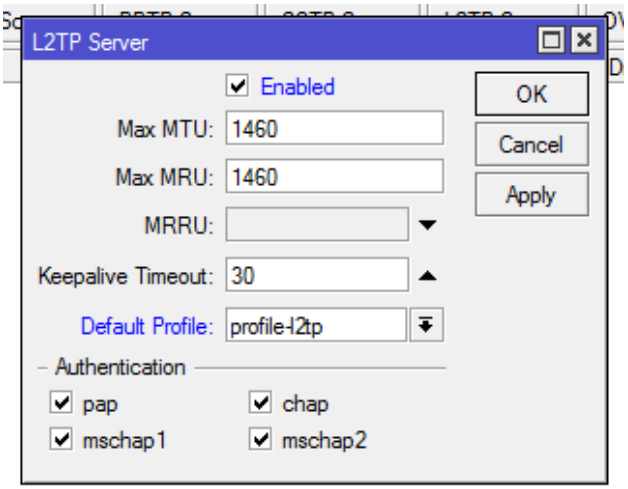


Ilustración 136. Configuración túnel L2TP

A continuación, en PPP accedemos a la pestaña Secret y creamos los túneles entre la controladora y cada uno de los Puntos de Acceso. En la siguiente imagen se muestra la configuración del túnel L2TP entre el primer Punto de Acceso y la controladora. Los datos de la configuración de los túneles podemos encontrarlos en la Ilustración 67

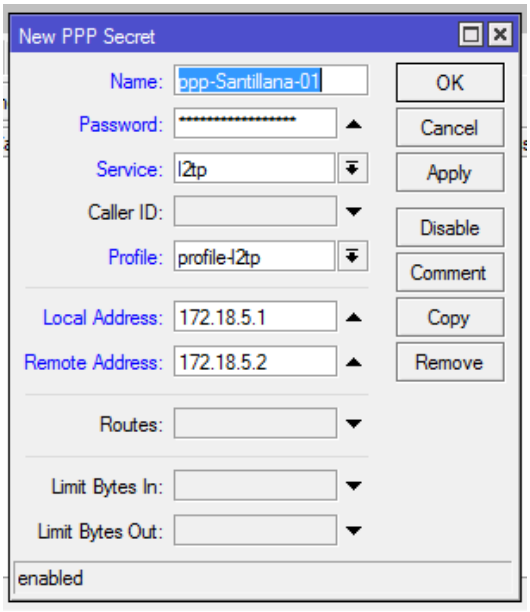
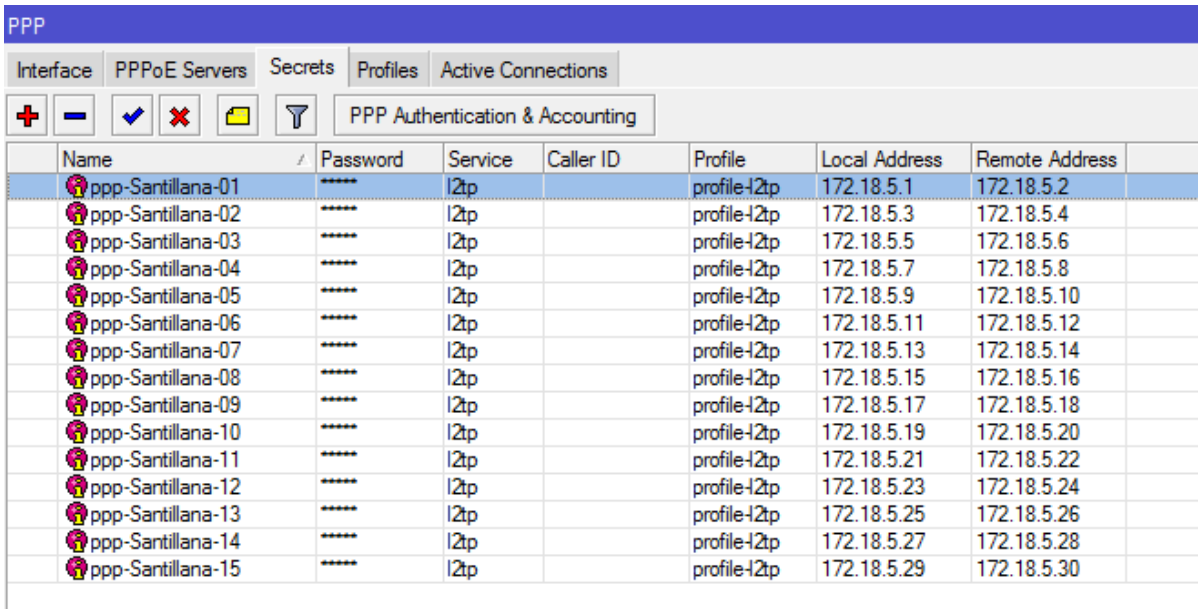


Ilustración 137. Túnel L2TP entre AP1 y la controladora

Se debe configurar el parámetro “Local Address” que es la IP del extremo de la controladora y “Remote Address“que es la IP del extremo del túnel del AP, de forma que quede creado el túnel.

Se realiza lo mismo con el resto de los Puntos de Acceso quedando, de este modo, configurado los túneles L2TP.



Name	Password	Service	Caller ID	Profile	Local Address	Remote Address
ppp-Santillana-01	*****	l2tp		profile-l2tp	172.18.5.1	172.18.5.2
ppp-Santillana-02	*****	l2tp		profile-l2tp	172.18.5.3	172.18.5.4
ppp-Santillana-03	*****	l2tp		profile-l2tp	172.18.5.5	172.18.5.6
ppp-Santillana-04	*****	l2tp		profile-l2tp	172.18.5.7	172.18.5.8
ppp-Santillana-05	*****	l2tp		profile-l2tp	172.18.5.9	172.18.5.10
ppp-Santillana-06	*****	l2tp		profile-l2tp	172.18.5.11	172.18.5.12
ppp-Santillana-07	*****	l2tp		profile-l2tp	172.18.5.13	172.18.5.14
ppp-Santillana-08	*****	l2tp		profile-l2tp	172.18.5.15	172.18.5.16
ppp-Santillana-09	*****	l2tp		profile-l2tp	172.18.5.17	172.18.5.18
ppp-Santillana-10	*****	l2tp		profile-l2tp	172.18.5.19	172.18.5.20
ppp-Santillana-11	*****	l2tp		profile-l2tp	172.18.5.21	172.18.5.22
ppp-Santillana-12	*****	l2tp		profile-l2tp	172.18.5.23	172.18.5.24
ppp-Santillana-13	*****	l2tp		profile-l2tp	172.18.5.25	172.18.5.26
ppp-Santillana-14	*****	l2tp		profile-l2tp	172.18.5.27	172.18.5.28
ppp-Santillana-15	*****	l2tp		profile-l2tp	172.18.5.29	172.18.5.30

Ilustración 138. Configuración túneles L2TP

Configuración túnel EoIP

Para configurar los túneles EoIP, tomamos como referencia los datos que se muestran en el diagrama de configuración de red en la Ilustración 67. En la imagen que se muestra a continuación aparecen los parámetros que hay que modificar para la configuración el túnel EoIP entre el primer punto de acceso y la controladora.

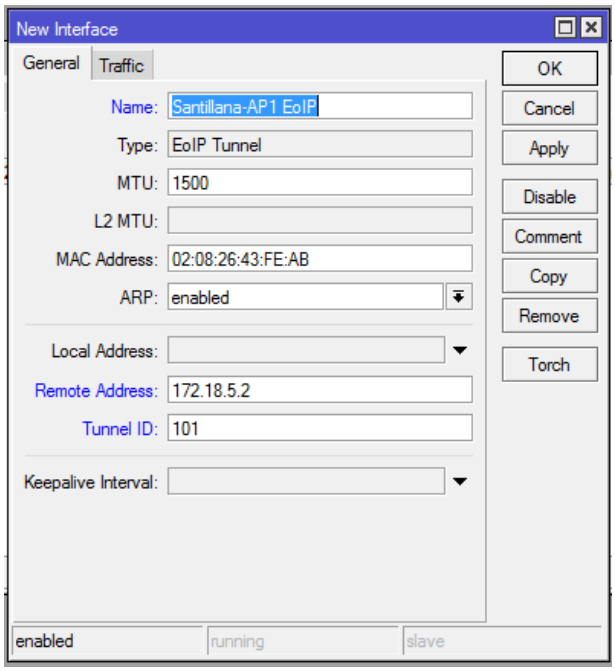
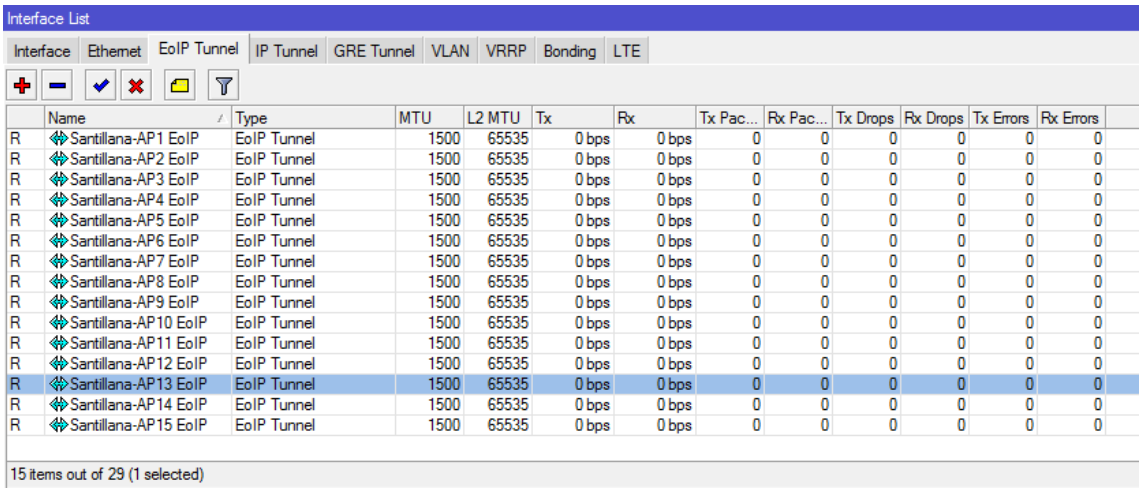


Ilustración 139. Configuración túnel EoIP entre AP1 y controladora

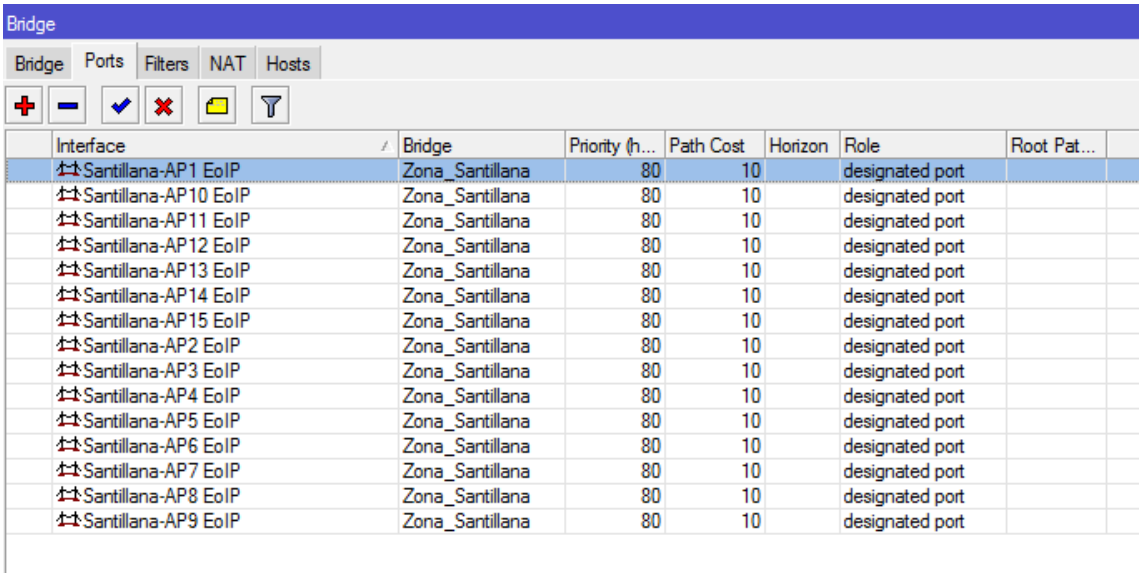
Dicho proceso deberá realizarse con el resto de los puntos de acceso, de forma que queden creados los túneles entre cada AP y la controladora.



	Name	Type	MTU	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx Drops	Tx Errors	Rx Errors
R	Santillana-AP1 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP2 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP3 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP4 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP5 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP6 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP7 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP8 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP9 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP10 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP11 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP12 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP13 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP14 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0
R	Santillana-AP15 EoIP	EoIP Tunnel	1500	65535	0 bps	0 bps	0	0	0	0	0	0

Ilustración 140. Configuración túneles EoIP

Se añaden todos los túneles EoIPs en el Bridge- Ports



	Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root Pat...
	Santillana-AP1 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP10 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP11 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP12 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP13 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP14 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP15 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP2 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP3 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP4 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP5 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP6 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP7 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP8 EoIP	Zona_Santillana	80	10		designated port	
	Santillana-AP9 EoIP	Zona_Santillana	80	10		designated port	

Ilustración 141. Configuración Bridge

Configuración de los puertos Ethernet de la controladora

En el presente apartado, se procederá a configurar los puertos Ethernet de la controladora. En este caso será necesaria la configuración de tres puertos Ethernet:

- El puerto Ethernet 1, será configurado como la vía principal de salida a internet, es decir, la tecnología WiMAX.
- El puerto Ethernet 2, será configurado como la vía secundaria de salida a internet en caso de que la vía principal falle. Se configurará en este puerto la tecnología ADSL.
- Por último, el puerto Ethernet 3, se configurará como el puerto que servirá de enlace entre la controladora y el primer punto de acceso (AP1).

Ilustración 142. Configuración puertos Ethernet de la controladora

Como se ha comentado, en el puerto Ethernet 1 se configurará la salida a Internet WiMAX. Para ello, se accede a IP→Addresses y se añade la dirección IP además de especificar la interfaz que va asociada a esa IP.

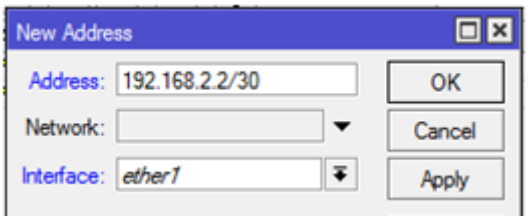


Ilustración 143. Configuración puerto Ethernet 1

En el puerto Ethernet 2 se configurará el Ethernet que irá al router ADSL

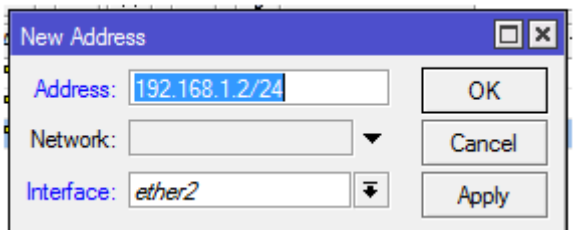


Ilustración 144. Configuración puerto Ethernet 2

Por último se configurará el tercer puerto Ethernet que será el que conectará el primer punto de acceso con la controladora.

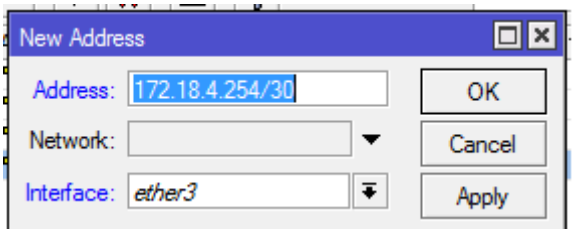


Ilustración 145. Configuración puerto Ethernet 3

Rutas de los equipos

Para que la controladora sepa por donde tiene que sacar el tráfico y hacia donde tiene que encaminarlo, es necesario configurar las rutas de los equipos. Accediendo a IP→Routes y observando la Ilustración 66, creamos las rutas indicando la dirección de destino y el Gateway de cada una de las subredes de la red.

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	172.18.4.0/29	172.18.4.253 reachable ether3	1		
AS	172.18.4.8/29	172.18.4.253 reachable ether3	1		
AS	172.18.4.16/30	172.18.4.253 reachable ether3	1		
AS	172.18.4.20/30	172.18.4.253 reachable ether3	1		
AS	172.18.4.24/30	172.18.4.253 reachable ether3	1		
AS	172.18.4.28/30	172.18.4.253 reachable ether3	1		
AS	172.18.4.32/30	172.18.4.253 reachable ether3	1		
AS	172.18.4.36/30	172.18.4.253 reachable ether3	1		
AS	172.18.4.40/30	172.18.4.253 reachable ether3	1		
AS	172.18.4.44/30	172.18.4.253 reachable ether3	1		
AS	172.18.4.48/30	172.18.4.253 reachable ether3	1		
AS	172.18.4.52/30	172.18.4.253 reachable ether3	1		

Ilustración 146. Configuración de las rutas

Rutas de salida a Internet

Las rutas de salida a Internet son creadas para saber porque línea de comunicación deben salir los paquetes. Para ello se hace una configuración del Firewall realizando la implementación que se muestra a continuación con el fin de marcar las conexiones de las salidas de internet, para que en el caso de que falle la principal línea de comunicación salgan por la línea de backup.

Se accede a IP →Firewall→Mangle y se genera el marcado.

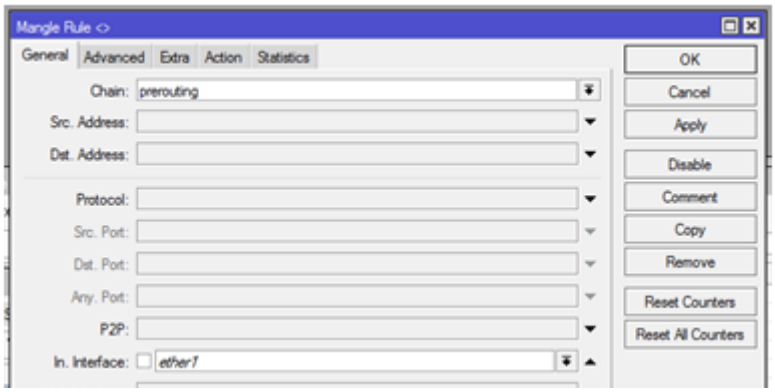


Ilustración 147. Configuración Rutas Salida a Internet I

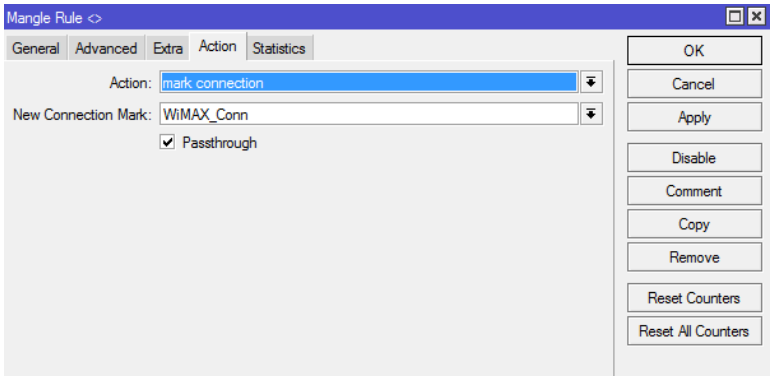


Ilustración 148. Configuración Rutas Salida a Internet II

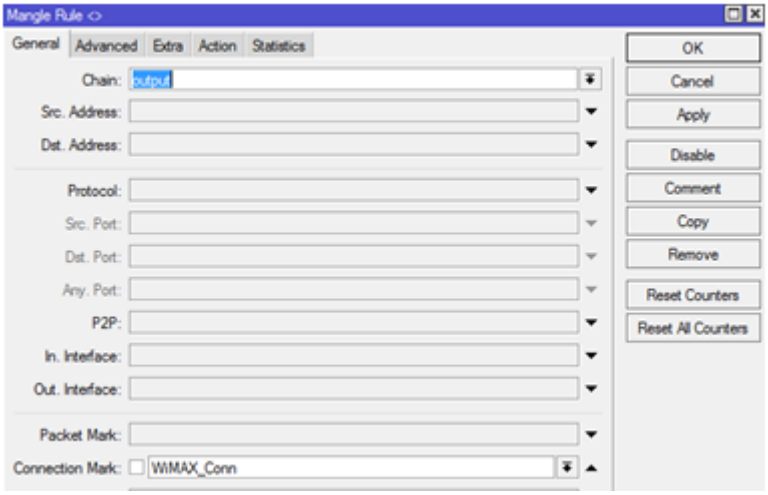


Ilustración 149. Configuración Rutas Salida a Internet III

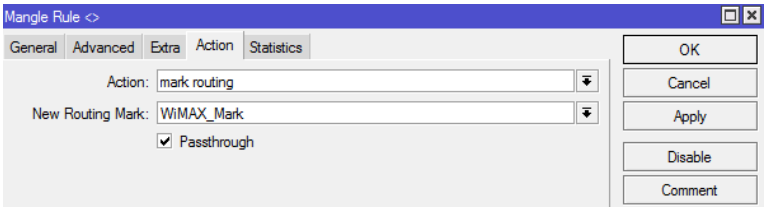


Ilustración 150. Configuración Rutas Salida a Internet IV

Para el puerto Ethernet 2 se hace exactamente igual, cambiando la marca de conexión.

Por último se accede a IP→Route y se marca como prioridad uno la salida a Internet a través de WiMAX y como prioridad segunda a la salida ADSL.

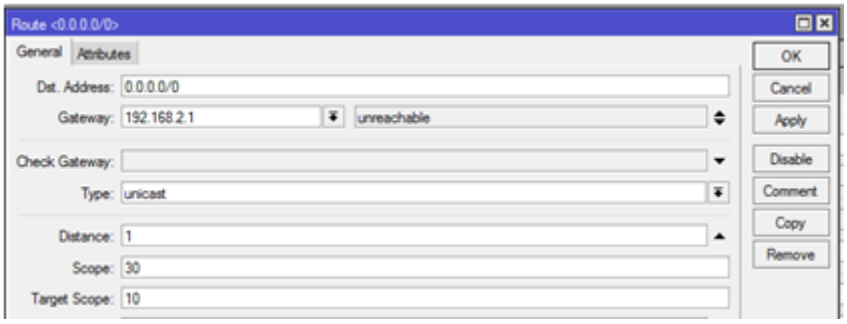


Ilustración 151. Prioridad I WiMAX

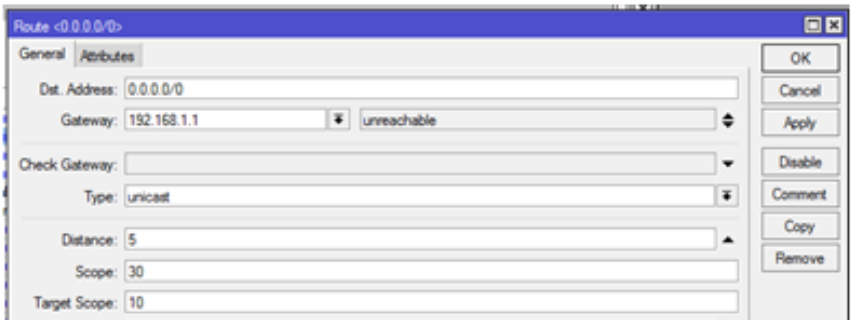


Ilustración 152. Prioridad II ADSL

Y se asigna a cada vía el marcado de conexiones creado anteriormente.

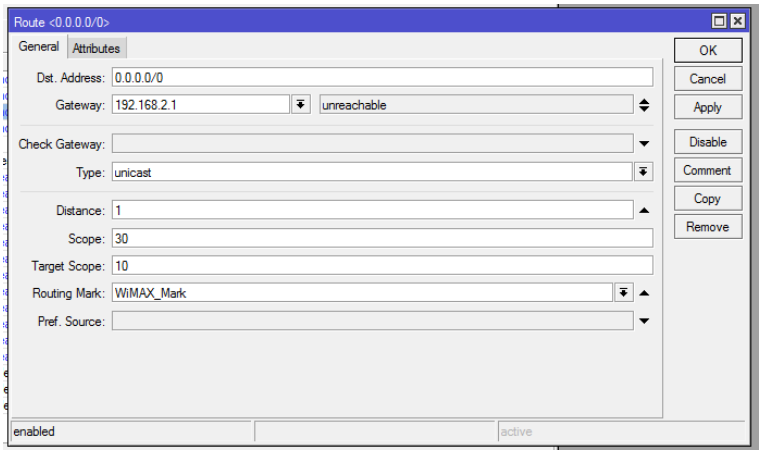


Ilustración 153. Configuración Rutas Salida a Internet V

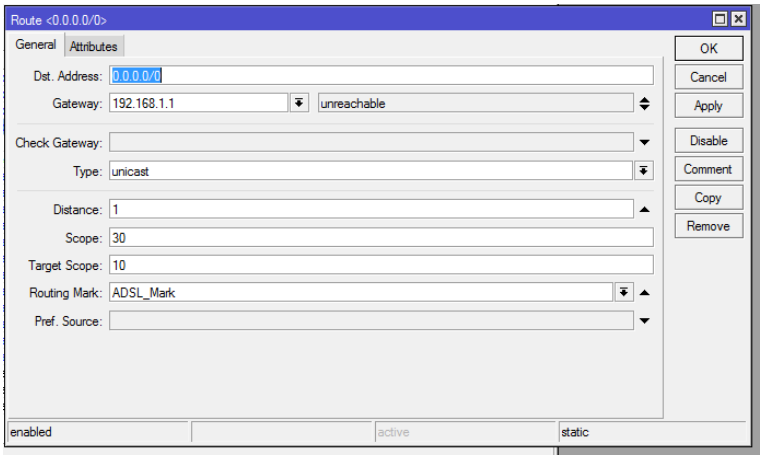


Ilustración 154.Configuración Rutas Salida a Internet VI

Para finalizar la configuración se muestra una imagen en la que se observan todas las rutas que han sido creadas para la implementación del proyecto.

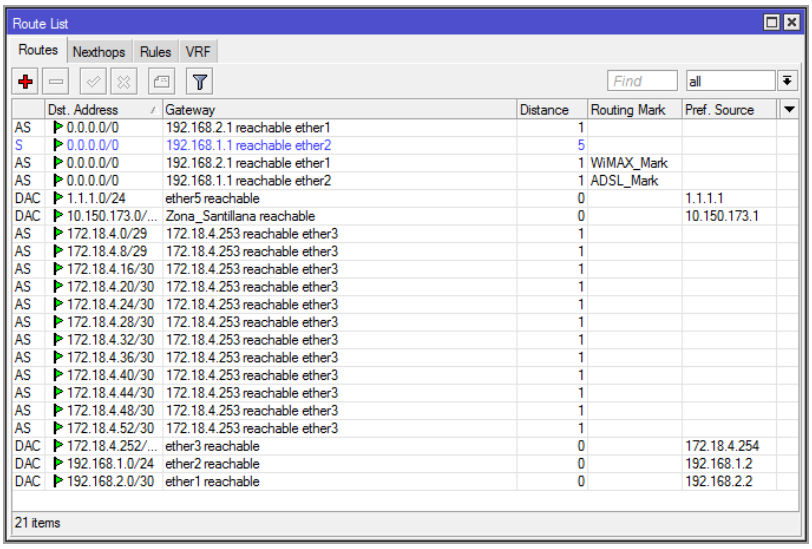


Ilustración 155. Totalidad de Rutas

Anexo B- Especificaciones equipamiento

RouterBOARD 433AH

The RB433AH is a more powerful version of the standard RB433. The 128MB DDR will be capable of supporting new RouterOS features coming. The microSD slot supports an additional memory card that can be used for a Dude database and other features.

The 680MHz Atheros MIPs 24K CPU with a 64KB/32KB instruction/data cache is probably the fastest CPU used in low cost wireless access points.

The three Ethernets and mpci slots give you ample data interfaces to put the big CPU power to work.

routerboard.com

CPU	Atheros AR7161 680MHz network processor
Memory	128MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip and microSD
Ethernet	Three 10/100 Mbit/s Ethernet ports with Auto-MDI/X
miniPCI	Three MiniPCI Type IIIA/IIIB slots
Extras	Reset switch, Beeper
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, NAND activity, 5 user LEDs
Power options	Power over Ethernet: 10..28V DC (except power over datalines). Power jack: 10..28V DC. Voltage monitor.
Dimensions	10.5 cm x 15 cm, 137 grams
Power consumption	~3W without extension cards, maximum ~ 25 W, 16W output to cards
Operating System	MikroTik RouterOS v3, Level5 license

RouterBOARD R52n-M

802.11a/b/g/n dual band miniPCI card

Key Features and Benefits

- Dual band IEEE 802.11a/b/g/n standard
- Output Power of up to **23dBm**
- Support for up to 2x2 MIMO with spatial multiplexing
- Four times the throughput of 802.11a/g
- Atheros AR9220, chipset
- High Performance (up to 300Mbps physical data rates and 200Mbps of actual user throughput) with Low Power Consumption
- Two MMCX antenna connectors
- Modulations:
  OFDM: BPSK, QPSK, 16 QAM, 64QAM
  DSSS: DBPSK, DQPSK, CCK
- Operating temperatures: -50°C to 60°C
- Power consumption MAX 1.95W
- ESD protection +/- 12kV

The RouterBOARD R52n-M miniPCI network adapter provides leading 802.11a/b/g/n performance in both 2GHz and 5GHz bands, supporting up to 300Mbps physical data rates and up to 200Mbps of actual user throughput on both the uplink and downlink. This card features the sturdy MMCX connectors for higher durability. Adding Wireless N to your Wireless device, it provides higher efficiency for everyday activities such as local network file transfers, Internet browsing, and media streaming.

802.11b	RX Sensitivity	Composite TX Power
1Mbit	-95	20
11Mbit	-91	21
802.11g		
6Mbit	-95	23
54Mbit	-81	19
802.11n 2.4GHz		
MCS0 20MHz	-95	21
MCS0 40MHz	-90	21
MCS7 20MHz	-78	17
MCS7 40MHz	-75	16

802.11a	RX Sensitivity	Composite TX Power
6Mbit	-95	21
54Mbit	-80	17
802.11n 5GHz		
MCS0 20MHz	-95	21
MCS0 40MHz	-92	19
MCS7 20MHz	-77	16
MCS7 40MHz	-74	13

Data Rates

802.11b	
	11Mbps; 5.5Mbps; 2Mbps; 1Mbps
802.11a/g	
	54Mbps; 48Mbps; 36Mbps; 24Mbps; 18Mbps; 12Mbps; 9Mbps; 6Mbps
802.11n	
20MHz	1Nss: 65Mbps @ 800GI, 72.2Mbps @ 400GI (Max.) 2Nss: 130Mbps @ 800GI, 144.4Mbps @ 400GI (Max.)
40MHz	1Nss: 135Mbps @ 800GI, 150Mbps @ 400GI (Max.) 2Nss: 270Mbps @ 800GI, 300Mbps @ 400GI (Max.)

RB1200

The new and affordable rackmount router.

It has ten individual gigabit Ethernet ports, five of them can be connected together in one 5-port switch group.

RB1200 has a SODIMM slot with bundled 512MB of RAM, a beeper and a serial port.

It has no moving parts and it's operation is completely silent. The RB1200 comes in a 1U aluminium rackmount case.

CPU	PowerPC PPC460GT
Memory	SODIMM DDR Slot, 512MB RAM
Boot loader	RouterBOOT, 1Mbit Flash chip
Ethernet	Ten 10/100/1000 Mbit/s Gigabit Ethernet with Auto-MDI/X
miniPCI	none
Storage	64MB NAND
Serial port	One DB9 RS232C asynchronous serial port
Extras	Reset switch, Beeper
Power options	IEC C14 standard connector 110/220V
Fan	no cooling fan
Dimensions	1U case: 44 x 176 x 442 mm, 1200g, Board only: 365g
Operating System	MikroTik RouterOS, Level 6 license

Pigtail MMCX a N Bulkhead RG-316 18 cm.

ESPECIFICACIONES

Tipo de conector: MMCX a N Hembra (Bulkhead)

Longitud del cable: 18 cm (Special length available upon request)

Impedancia: 50 Ohms nominal

Capacidad: 32 pF/ft

Frecuencia de corte: 65 GHz

ESTRUCTURA

Conductor: OD .060

Malla: 38 AWG SPC, OD 0.078" Nom.

Cubierta: OD 0.098"

ATENUACIÓN

1dBi a 30cm con 2 conectores

1GHz: 0,78 dB/m

2GHz: 1,11 dB/m

3GHz: 1,38 dB/m

4GHz: 1,61 dB/m

5GHz: 1,82 dB/m

6GHz: 2,02 dB/m

DATOS FÍSICOS

Peso por 1000 pies: 6,1 kg max

Máximo radio de curvatura: 0.5"

Temperatura de operación: -55 a +200 grados Centígrados

MTO-247

Antena Omnidireccional MESH 7.5 dBi 2.4 GHz - MT-341017/N/A

Las antenas omnidireccionales de 2.4 GHz fabricadas por MTI Wireless Edge ofrecen una excelente relación calidad-precio para aplicaciones de larga distancia. Estas antenas están preparadas completamente para funcionar en condiciones de intemperie extrema y proporcionar años de funcionamiento libre de errores.

Claves

Alta calidad y bajo coste
Ligera y fácilmente instalable
Perfil bajo
Respetuosa con el medioambiente
Integrable directamente en el equipo (gracia a su conector N-Macho)
Banda ancha
Cumple los requisitos ETSI
Muy estética

Beneficios

Alto rendimiento a bajo coste
Reduce el coste de instalación
Maintiene una estética de calidad
Baja carga al viento

Especificaciones

Modelo MT-341017/N/A
Rango de frecuencias 2.4 - 2.5 GHz
Ganancia 7.25 dbi +/- 0.75 db
VSWR < 1.5:1
Ancho de haz 360º / 21º
Polarización Vertical
Impedancia 50 ohms
Potencia entrada (Max) 6 Watt
Tamaño 28x337 mm
Peso 0.5 kg.
Conector N-Macho
Radome Plástico
Base Aluminio con protección

Medioambiente

Rango de Temperaturaa: -45 a +70ºC per IEC 68
Vibración: : Random 4M3 per IEC 60721
Shock Mecánico: 4M3 per IEC 60721
Humedad: 95% per ETSI EN300
Resistencia al agua: Per IEC 529 IP67
Spray de Sal: 500 horas per IEC 68
Radiación Solar: 1000 hours per ASTM G53
Hielo y nieve: 25mm Radial
Velocidad del viento: 160 Kmph Operation/220 Kmph Survival
Inflamabilidad: UL-94HB (excluding MT-485028/N)

MTO-5085 (MT-482016/N/A)

Antena Omnidireccional MESH 8.5 dBi 5.4-5.8 GHz

Las antenas omnidireccionales de 5 GHz fabricadas por MTI Wireless Edge ofrecen una excelente relación calidad-precio para aplicaciones de larga distancia. >Estas antenas están preparadas completamente para funcionar en condiciones de intemperie extrema y proporcionar años de funcionamiento libre de errores.

Claves

Alta calidad y bajo coste
Ligera y fácilmente instalable
Perfil bajo
Respetuosa con el medioambiente
Integrable directamente en el equipo (gracia a su conector N-Macho)
Banda ancha
Cumple los requisitos ETSI
Muy estética

Beneficios

Alto rendimiento a bajo coste
Reduce el coste de instalación
Maintiene una estética de calidad
Baja carga al viento

Especificaciones

Modelo	MT-482016/N/A
Rangod e frecuencias	5.470 - 5.875 GHz
Ganancia	8.5 dbi +/- 0.6 db
VSWR	< 1.7:1
Ancho de haz	360º / 10º
Polarización	Vertical
Impedancia	50 ohms
Potencia entrada (Max)	4 Watt
Tamaño	16x337 mm
Peso	0.5 kg.
Conector	N-Macho
Radome	Plástico
Base	Aluminio con protección

Medioambiente

Rango de Temperaturaa: -45 a +70ºC per IEC 68
Vibración: : Random 4M3 per IEC 60721
Shock Mecánico: 4M3 per IEC 60721
Humedad: 95% per ETSI EN300
Resistencia al agua: Per IEC 529 IP67
Spray de Sal: 500 horas per IEC 68
Radiación Solar: 1000 hours per ASTM G53
Hielo y nieve: 25mm Radial
Velocidad del viento: 160 Kmph Operation/220 Kmph Survival
Inflamabilidad: UL-94HB (excluding MT-485028/N)

ANEXO C- Especificaciones Ruckus

Ruckus
Simply Better Wireless.

data sheet

BENEFITS

Best in class channel selection technology
ChannelFly dynamic channel management, based on throughput measurements, not just interference, chooses the best channel to give users the highest throughput

Environmentally hardened with AC power
Enables fast and easy mounting to street lights, traffic controls and other street furniture. Includes hardened enclosures for outdoor deployment with IP-67 rated enclosure

Unified, centralized Wi-Fi management eases administration
ZoneDirector and/or FlexMaster provide a detailed view into and control over both indoor and outdoor Smart Wi-Fi APs enabling seamless and system-wide administration of the entire wireless environment including carrier grade 3GPP, I-WLAN core networks and future 4G/LTE core

Unmatched Wi-Fi range and reliability
Adaptive antenna technology combined with unique interference mitigation technology delivers up to 6 dB of added signal gain and up to 15 dB of interference mitigation and support for up to 500 clients in the AC

Enables a myriad of new services and service opportunities
Smart Wi-Fi applied outdoors now enables new revenue-generating services such as community Wi-Fi, IP-video applications, multimedia hotspots, extended WLAN services outdoors and wireless backhaul for small cell cluster, and mobile data offload

ZoneFlex™ 7762 Series

DUAL-BAND 802.11N SMART WI-FI OUTDOOR AP

World's First Concurrent 2.4/5GHz 802.11n Access Point with Adaptive Antenna Technology and Smart Wi-Fi Meshing

The ZoneFlex 7762 Series is the first dual-band 802.11n outdoor access point (AP) to integrate adaptive antenna technology to enable much longer range signals, better signal penetration inside buildings, and more resilient mesh connections that automatically adapt to interference and changing environmental conditions.

Supporting advanced Smart Mesh Networking, the Ruckus ZoneFlex 7762 Series is perfect for service providers looking to quickly and economically expand branded broadband services, offload data traffic from congested 3G networks, deploy multimedia hotspots or offer wireless broadband services where fixed line access is limited. Separate radios for access and backhaul traffic deliver high-throughput to clients throughout the mesh network.

The ZoneFlex 7762 Series is also ideal for hotels, resorts, multi-dwelling units, schools, warehouses and other enterprises needing to deliver broadband access from the outside in or to extend managed wireless LANs (WLANs) outdoors where Ethernet cabling is not possible.

The ZoneFlex 7762 Series can be centrally managed by the ZoneDirector Smart WLAN controller as part of a unified indoor/outdoor wireless LAN or deployed as a standalone AP and managed individually or through the FlexMaster remote Wi-Fi management system.

The ZoneFlex 7762 Series implements Ruckus-patented BeamFlex™ smart antenna technology that enables consistent, high-performance, extended coverage and multimedia support. Ruckus ChannelFly dynamic channel management optimizes client throughput by selecting the best channel to operate on. A Web-based wizard allows any computer user to configure ZoneFlex 7762 Series through the ZoneDirector™ — creating a secure and sophisticated WLAN in a matter of minutes.

ZoneFlex™ 7762 Series

DUAL-BAND 802.11N SMART WI-FI OUTDOOR AP

ZoneFlex 7762

Dual-band 802.11n
3:3x2, 600 Mbps

Smart antenna for 2.4/5 GHz
19 elements, +4000 patterns
360° coverage, optional
external 5 GHz antennas

- Optimized for enterprise apps
- Ideal for dual-band environments (e.g., most clients are laptops)

ZoneFlex 7762-S

Dual-band 802.11n
3:3x2, 600 Mbps

Smart antenna for 2.4 GHz
12 elements, 24 patterns,
120° coverage, 5 GHz
external antennas

- Optimized for 3G offload
- Best 2.4 GHz coverage and capacity at 120°
- Ideal for poles, exterior walls

ZoneFlex 7762-T

Dual-band 802.11n
3:3x2, 600 Mbps

Smart antenna for 2.4 GHz
12 elements, +4000
patterns, 360° coverage,
5 GHz external antennas

- Optimized for 3G offload
- Ideal for poles, street corners, areas where 3 APs cannot be mounted

ZoneFlex 7762-AC, ZoneFlex 7762-S-AC

Dual-band 802.11n
3:3x2, 600 Mbps

Smart antenna for 2.4 GHz
12 elements, +4000
patterns, 360° coverage,
5 GHz external antennas

- Optimized for 3G offload
- Ideal for poles, street corners, areas where 3 APs cannot be mounted
- AC power for flexible deployment

- Concurrent dual-band (5 GHz/2.4 GHz) support
- Adaptive antenna technology and advanced RF management
- Up to 6 dB signal gain / 15 dB interference mitigation
- Automatic interference avoidance, optimized for high-density environments
- Integrated smart antenna array with up to 4,000 unique patterns for ultra reliability
- Standard 802.3at/af Power over Ethernet (PoE)
- Ruckus custom high power PoE injector available
- Standard 802.3af output for surveillance cameras
- Wall, pole or ceiling mountable
- Built-in heater for cold climate (-40° C)
- Multicast IP video streaming
- 600 Mbps of user throughput (300 Mbps/radio)

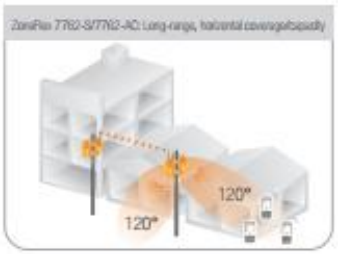
- 16 BSSIDs with unique QoS and security policies
- Advanced QoS packet classification and automatic priority for latency-sensitive traffic
- Dynamic, per-user rate-limiting for hotspot WLANs
- WEP, WPA-PSK (AES), 802.1X support for RADIUS and Active Directory*
- Smart Mesh Networking*
- Zero-IT and Dynamic PSK*
- Admission control/load balancing*
- Band steering and airtime fairness support
- Captive portal and guest accounts *

*when used with Ruckus ZoneDirector controller

ZoneFlex™ 7762 Series

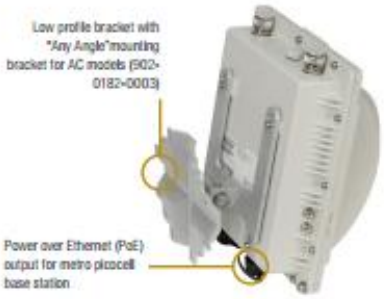
DUAL-BAND 802.11N SMART WI-FI OUTDOOR AP

- First dual-band 802.11n smart outdoor AP with adaptive antenna array
- Designed for extreme conditions
- Smart channel selection
- Concurrent dual-band 802.11n
- 360° coverage
- 19 elements, +4000 patterns
- IP-67 rated, -40°C – 65°C
- Standalone or centrally managed by ZoneDirector or FlexMaster



- First smart sector 802.11n AP
- Optimized for horizontal, long-range coverage and high-density user environments
- Smart channel selection
- Concurrent dual-band 802.11n
- 120° smart sector 2.4GHz antenna for longer range
- External 5GHz antennas
- IP-67 rated, -40°C – 65°C
- Standalone or centrally managed by ZoneDirector or FlexMaster

- Smart antenna optimized for 2.4GHz
- 360° coverage
- 12 elements, +4000 patterns
- Smart channel selection
- 5GHz external antennas
- Concurrent dual-band 802.11n
- IP-67 rated, -40°C – 65°C
- Managed by ZoneDirector and FlexMaster



Specifications (7762, 7762-S, 7762-T)

PHYSICAL CHARACTERISTICS	
POWER	• Power over Ethernet and 12V DC
PHYSICAL SIZE	• 23.9 cm (L), 19.5 cm (W), 14.1 cm (H)
WEIGHT	• 1900 grams (4.19 lbs.)
ANTENNA	• ZF 7762: Internal software-configurable dual band antenna array with directional and omni high-gain elements that provide over 4,000 unique antenna patterns • ZF 7762-S: Internal software-configurable 2.4GHz antenna array with directional high-gain elements that provide over 24 unique antenna patterns (requires external antenna for 5 GHz operations) • ZF 7762-T: Internal software-configurable 2.4GHz antenna array with directional and omni high-gain elements that provide over 4,096 unique antenna patterns (requires external antenna for 5 GHz operations)
ETHERNET PORTS	• 2 ports, auto MDX, auto-sensing RJ-45 • 10/100/1000 Mbps Power over Ethernet (802.3af) input • 10/100 Mbps Power over Ethernet (802.3af) output
ENVIRONMENTAL CONDITIONS	• IP-67 rated • Operating air temperature: -40°C – 65° C (-40°F – 149°F), -20°C when heater disabled • Operating humidity: 5% to 100% condensing
POWER DRAW	• 12.95W (PoE) • 15W (12V DC)

RF (7762, 7762-S)	
ANTENNA	• Adaptive antenna array that provides 4,000+ unique antenna patterns (24 for the sectorized version)
PHYSICAL ANTENNA GAIN	• 7762: 3 dBi (2.4 GHz) • 7762: 5 dBi (5 GHz) • 7762-S: 7 dBi (2.4 GHz) • 7762-S: 5 dBi (5 GHz)
RF POWER OUTPUT**	• 28 dBm (2.4 GHz) • 28 dBm (5 GHz)
BEAMFLEX* SINR TX GAIN	• Up to 6 dB
BEAMFLEX* SINR RX GAIN	• Up to 4 dB
INTERFERENCE MITIGATION	• Up to 15 dB
MINIMUM RX SENSITIVITY	• Up to -95 dBm

*BeamFlex gains are statistical system level effects translated to enhanced SINR here, and based on observations over time in real-world conditions with multiple APs and many clients
** Maximum power varies by country

RF (7762-T)	
ANTENNA	• Adaptive antenna array that provides 4,000+ unique antenna patterns
PHYSICAL ANTENNA GAIN	• 5 dBi (2.4 GHz) • 5 dBi (5 GHz)
RF POWER OUTPUT**	• 28 dBm (2.4 GHz) • 28 dBm (5 GHz)
BEAMFLEX* SINR TX GAIN	• Up to 6 dB
BEAMFLEX* SINR RX GAIN	• Up to 4 dB
INTERFERENCE MITIGATION	• Up to 15 dB
MINIMUM RX SENSITIVITY	• Up to -95 dBm

*BeamFlex gains are statistical system level effects translated to enhanced SINR here, and based on observations over time in real-world conditions with multiple APs and many clients
** Maximum power varies by country

CAPACITY	
CONCURRENT STATIONS	• 256
SIMULTANEOUS VoIP CLIENTS	• Up to 20

MANAGEMENT	
DEPLOYMENT OPTIONS	• Standalone (individually managed) • Managed by ZoneDirector • Managed by FlexMaster
CONFIGURATION	• Web User Interface (HTTP/S) • CLI (Telnet/SSH), SNMP v1, 2, 3 • TR-069 via FlexMaster

WI-FI	
STANDARDS	• IEEE 802.11a/b/g/n • 2.4GHz and 5GHz concurrent operation
SUPPORTED DATA RATES	• 802.11n: 6.5Mbps – 130Mbps (20MHz) 6.5Mbps – 300Mbps (40MHz) • 802.11a: 54, 48, 36, 24, 18, 12, 9 and 6 Mbps • 802.11b: 11, 5.5, 2 and 1 Mbps • 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6 Mbps
RADIO CHAINS	• 3 x 3: 2
FREQUENCY BAND	• IEEE 802.11n: 2.4 – 2.484 GHz and 5.15 – 5.85 GHz • IEEE 802.11a: 5.15 – 5.875 GHz • IEEE 802.11b: 2.4 – 2.484 GHz
BSSID	• Up to eight per radio (16 total)
WIRELESS SECURITY	• WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i • Authentication via 802.1X, local authentication database, support for RADIUS and ActiveDirectory
CERTIFICATIONS	• U.S., Europe, Australia, Brazil, Canada, China, Egypt, Hong Kong, India, Japan, Korea, Malaysia, Mexico, New Zealand, Philippines, Singapore, South Africa, Taiwan, Thailand, UAE, Vietnam • WEEE/RoHS compliance • Wi-Fi Alliance Certification (Wi-Fi Certified®)

Product Ordering Information

MODEL	DESCRIPTION
ZoneFlex 7762 Series 802.11n Outdoor Access Points	
901-7762-XX01	7762: Centrally managed concurrent dual band 802.11n outdoor access point, includes universal pole/wall/ceiling mounting bracket (902-0165-0000) and power injector.
901-7762-XX91	7762-T: Centrally managed concurrent dual band 802.11n outdoor access point, includes universal pole/wall/ceiling mounting bracket (902-0165-0000) and power injector.
901-7762-XX51	7762-S: Centrally managed concurrent dual band 802.11n outdoor access point, includes universal pole/wall/ceiling mounting bracket (902-0165-0000) and power injector.
Optional Accessories	
911-1212-DP01	5 GHz directional antenna, dual-polarized 12.5 dBi gain and 120 degrees 3 dBm beam width*
911-0536-VP01	5 GHz Omni-directional antenna, vertically polarized, 5.5 dBi
911-0536-HP01	5 GHz Omni-directional antenna, horizontally polarized, 5 dBi
911-0536-VH01	Bundle of one 911-0536-VP01 and one 911-0536-HP01
902-0165-0000	Universal pole/wall/ceiling mounting bracket, spare (sold in quantities of 10)
902-0166-0000	Flat mounting bracket
902-0180-XX00	PoE injector, spare (sold in quantities of 10 or 100)

PLEASE NOTE: When ordering you must specify the destination region by indicating -US, -WW, or -IL

Ruckus Wireless, Inc.
350 West Java Drive

Ruckus
Simply Better Wireless.

www.ruckuswireless.com

ANEXO D- Especificaciones Radwin

RADWIN 5000 – HPMP

Sector Base Station RW-5200-2250

Data Sheet

HBS 5200 SERIES

Sector Base Station - RW-5200-2250

RADWIN RW-5200-2250 is a Sector Base Station Radio unit, providing up to 250Mbps net aggregate throughput and delivering access connectivity up to 32 Subscriber Units (HSUs).
RW-5200-2250 supports 5.X GHz and complies with ETSI regulation.
RADWIN RW-5200-2250 is connectorized for use with external antenna.

Product Highlights

- High Capacity sector Base Station
- Up to 250 Mbps aggregated throughput
- Guaranteed Service level Agreement (SLA) per HSU
- Outstanding short and constant latency
- Support up to 32 HSUs
- Long range – up to 40 km/25 miles
- Single radio supporting multiple bands
- Advanced MIMO, OFDM and Diversity technologies
- Excellent operation in nLOS and NLOS scenarios
- Robust and reliable to operate in tough conditions, extreme temperatures
- Ease of operation and maintenance

Corporate Headquarters, T. +972.3.766.2900, E. sales@radwin.com, www.radwin.com

RADWIN

HBS 5200-2250 - Product Specifications

CONFIGURATION	
Architecture	Outdoor Unit Connectorized for External Antenna
PoE to ODU Interface	Outdoor CAT-5e; Maximum cable length: 100m for 10/100BaseT and 75m for 1000BaseT
RADIO	
Capacity	250 Mbps net aggregate throughput @ 40MHz 100 Mbps net aggregate throughput @ 20MHz
Subscriber Units (SUs) support	Up to 32 HSUs
Range	Up to 40 km / 25 miles
Channel Bandwidth	Configurable: 5, 10 , 20 and 40MHz (*)
Modulation	2x2 MIMO-OFDM (BPSK/QPSK/16QAM/64QAM)
Adaptive Modulation & Coding	Supported
Bandwidth allocation	Symmetric and Asymmetric
DFS	Supported
End to End Latency	Typical: 3.5msec @ 2 HSUs; 20msec @ 32 HSUs
Diversity	Supported
Spectrum Viewer	Supported
Max Tx Power	25 dBm (*)
Duplex Technology	TDD
Error Correction	FEC k = 1/2, 2/3, 3/4, 5/6
Encryption	AES 128
Ethernet Interface	10/100BaseT, 1000BaseT (supported via Indoor PoE device RW-9924-101X)
Layer 2	Bridging learning of 5K MAC addresses
QoS	Supported Packet classification to 4 queues according to 802.1p and Diffserv
VLAN	Supported 802.1Q, 802.1P, QinQ
TDD Intra Site Synchronization	Supported
TDD Inter Site Synchronization	Supported through common GPS receiver per site

Note (*) –Subject to regulation in each country

SUPPORTED BANDS RW-5200-2250		
5.4 GHz ETSI*	**5.475 - 5.720 GHz**	**ETSI EN 301 893**
5.8 GHz ETSI	5.725 - 5.875 GHz	ETSI EN 302 502
5.3 GHz ETSI	5.150 - 5.350 GHz	ETSI EN 301 893
***Default Band**		
MECHANICAL		
ODU Dimensions	19.5(w) x 27.0(h) x 8.0(d) cm	
ODU Weight	1.8 kg / 3.6 lbs	
POWER		
Power Feeding	Power provided over ODU-IDU cable using PoE	
Power Consumption	<25W	
ENVIRONMENTAL		
Operating Temperatures	-35°C to 60°C / -31°F to 140°F	
Humidity	100% condensing, IP67 (totally protected against dust and against immersion up to 1m)	
SAFETY		
FCC/IC (cTUVus)	UL 60950-1, UL 60950-22, CAN/CSA C22.2 60950-1, CAN/CSA C22.2 60950-22	
ETSI	EN/IEC 60950-1, EN/IEC 60950-22	
EMC		
FCC	47 CFR Class B, Part15, Subpart B	
ETSI	EN 300 386, EN 301 489-1, EN 301 489-4	
CAN/CSA-CEI/IEC	CISPR 22-04 Class B	
AS/NZS	CISPR 22-2004 Class B	

Ordering Info
Part Number: RW-5200-2250
Description: RADWIN HBS 5200 Series, Base Station Radio Connectorized for external antenna (2xN-type), supporting multi frequency bands at 5.x GHz, factory default 5.4 GHz ETSI

RADWIN

RADWIN 5000 – HPMP

RW-5550-2150 Subscriber Unit – Data Sheet

HSU 550 SERIES

Subscriber Units - RW-5550-2150

RADWIN RW-5550-2150 Subscriber Unit (HSU) provides high capacity access connectivity of up to 50Mbps net aggregate throughput. RW-5550-2150 works with HBS-5200 base station.

RW-5550-2150 supports 5.X GHz and complies with ETSI regulations.

Product Highlights

- Up to 50 Mbps net aggregate throughput
- Guaranteed Service level Agreement (SLA) per HSU
- Outstanding short and constant latency
- Long range – up to 40 km/25 miles
- Advanced MIMO, OFDM and Diversity technologies
- Excellent operation in nLOS and NLOS scenarios
- Ease of operation and maintenance

RADWIN

RW-5550-2150 - Product Specifications

CONFIGURATION	
Architecture	Outdoor Unit with Integrated Antenna
PoE to ODU Interface	Outdoor CAT-5e cable; Maximum cable length: 100 m
RADIO	
Capacity net aggregate throughput	50 Mbps
Range	Up to 40 km / 25 miles
Channel Bandwidth	Configurable: 10, 20 and 40 MHz (*)
Modulation	2x2 MIMO-OFDM (BPSK/QPSK/16QAM/64QAM)
Bandwidth allocation	Symmetric and Asymmetric
Adaptive Modulation & Coding	Supported
DFS	Supported
Diversity	Supported
Spectrum Viewer	Supported
Max Tx Power	25 dBm (*)
Duplex Technology	TDD
Error Correction	FEC k = 1/2, 2/3, 3/4, 5/6
Encryption	AES 128
Supported Indoor Units	RADWIN PoE device (RW-9021-001X)
Ethernet Interface	10/100 BaseT
Layer 2	Hub Mode
QoS	Supported Packet classification to 4 queues according to 802.1p and Diffserv
VLAN	Supported 802.1Q, 8021.P, QinQ

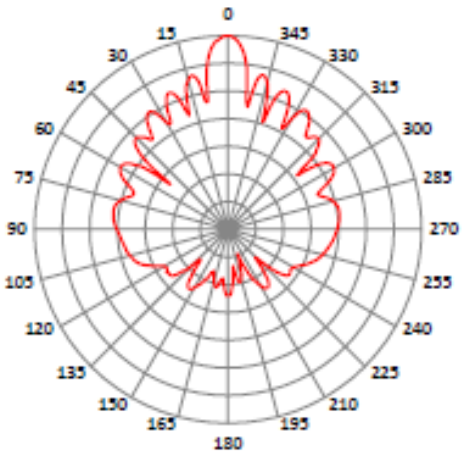
Note (*) - Subject to regulation in each country

SUPPORTED BANDS RW-5550-2150		
5.4 GHz ETSI*	5.475 - 5.720 GHz	ETSI EN 301 893
5.8 GHz ETSI	5.725 - 5.875 GHz	ETSI EN 302 502
5.3 GHz ETSI	5.150 - 5.350 GHz	ETSI EN 301 893
*Default Band		
MECHANICAL		
ODU Dimensions	37.1(w) x 37.1(h) x 11.0(d) cm	
ODU Weight	3.5 kg / 7 lbs	
POWER		
Power Feeding	Power provided over ODU-IDU cable using PoE	
Power Consumption	<20W	
ENVIRONMENTAL		
Operating Temperatures	-35°C to 60°C / -31°F to 140°F	
Humidity	100% condensing, IP67 (totally protected against dust and against immersion up to 1m)	
SAFETY		
FCC/IC (cTUVus)	UL 60950-1, UL 60950-22, CAN/CSA C22.2 60950-1, CAN/CSA C22.2 60950-22	
ETSI	EN/IEC 60950-1, EN/IEC 60950-22	
EMC		
FCC	47 CFR Class B, Part15, Subpart B	
ETSI	EN 300 386, EN 301 489-1, EN 301 489-4	
CAN/CSA-CEI/IEC	CISPR 22-04 Class B	
AS/NZS	CISPR 22-2004 Class B	

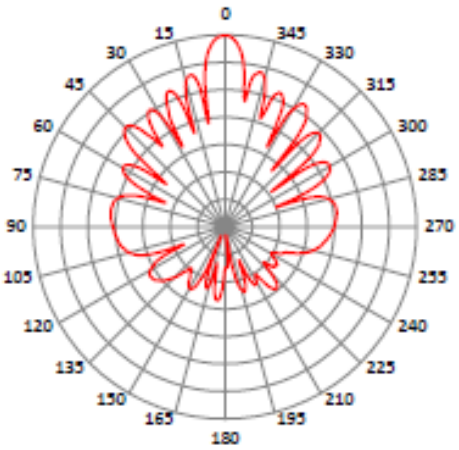
RADWIN

Integrated Antenna	
Gain	22.5 dBi @ 5.15-5.875 GHz
VSWR	1.5 : 1 (typ)
3 dB Beamwidth	9° (typ)
AZ & EL Beam Squint	±2° Port V & Port H
Polarization	Dual Linear (Vertical and Horizontal)
Sidelobes Level	ETSI EN 302 085 V1.1.2, TS1-TS3
Cross Polarization	ETSI EN 302 085 V1.1.2, TS1-TS3
F/B Ratio	-35 dB (max)
Port To Port Isolation	40 dB (min)
Lightning Protection	DC grounded
Antenna Pattern	

Azimuth @ 5.8GHz



Elevation @ 5.8GHz



Ordering Info

Part Number: RW-5550-2150

Description: RADWIN HSU 550 Series Subscriber Unit Radio with high gain integrated antenna, supporting multi frequency bands at 5.x GHz, factory default 5.4 GHz ETSI

Corporate Headquarters, T. +972.3.766.2900, E. sales@radwin.com, www.radwin.com

RADWIN

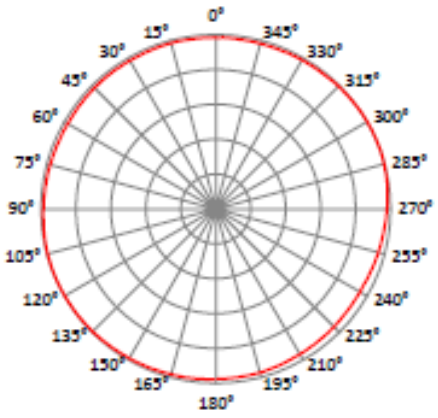
RW-9402-5001

Product Data Sheet

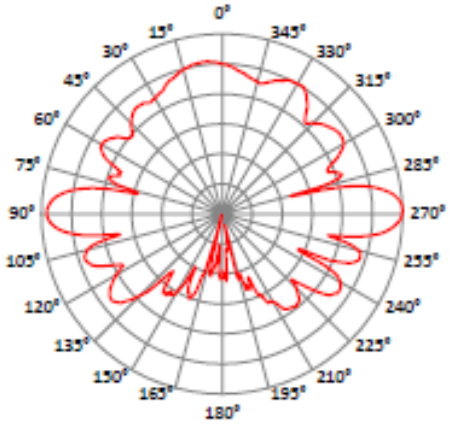
RADWIN ANTENNAS

RW-9402-5001 is an external Mobile Unit antenna part of the RADWIN 5000 Mobility-Series. RW-9402-5001 is a single polarization Omni-directional antenna with 10dBi Gain, supporting 4.900 – 5.875 GHz frequency range and complies with ETSI regulations

Antenna Pattern



H-Plane at 5.5 GHz



E-Plane at 5.5 GHz

RADWIN

RW-9402-5001 - Product Specifications

ELECTRICAL	
Frequency Range	4.90 – 5.875 GHz
Minimum Peak Gain	10 dBi
VSWR	2:1@4.9-5.15GHz; 1.8:1@5.15-5.875GHz.
3 dB Beam-width, H-Plane	360°
3 dB Beam-width, E-Plane	10°
Polarization	Linear Vertical
Input Impedance	50 Ohm
Input Power	10 Watt (max)
MECHANICAL	
Dimensions (L x D)	315 x 40mm
Weight	0.21kg
Connector	N-type female
Radome	UV protected, Plastic
Mounting Kit	Supplied
ENVIRONMENTAL	
Temperature	-40°C to +65°C
Humidity	ETS 300 019-1-4, EN 302 085
Water Tightness	IP67
Flammability	UL 94
Salt Fog	IEC 68-2-11
Ice and Snow	25mm
Wind Load (Survival)	200 km/h
Regulatory Compliance	
	EN 302 085 v1.2.3

Ordering Info

Part Number: RW-9402-5001

Description: Omni-directional antenna, gain 10dBi, 4.9-5.875GHz

Corporate Headquarters, T. +972.3.766.2900, E. sales@radwin.com, www.radwin.com

RADWIN

PRESUPUESTO

El presupuesto queda detallado en el apartado 6.2 del presente documento.
Realizado en Madrid, Enero de 2015

El Ingeniero Jefe de Proyecto

Fdo.: Marta Moreno Martín

Ingeniero de Telecomunicación

DOCUMENTACIÓN ACREDITATIVA

D. Christian García, con DNI 53400583B, como Director del Departamento de Operaciones de la empresa Gowex Wireless, S.L CERTIFICO que:

Dña. Marta Moreno Martín, con DNI 47296273Q, es trabajadora Gowex Wireless y ha desarrollado el proyecto "Análisis, diseño y despliegue de una red WiFi en Santillana del Mar", que fue presentado al cliente Ayuntamiento de Santillana del Mar (Cantabria) para su implantación en la ciudad. La contribución de Marta en dicho proyecto fue ejercer como jefe de proyecto realizando las siguientes tareas:

- Reunión con el cliente y toma de requisitos.
- Planificación y seguimiento del proyecto.
- Diseño y análisis de la arquitectura de red y toma de decisión del equipamiento a instalar.
- Planificación de cobertura y análisis de campo.
- Presentación y elaboración de documentación e informes del proyecto.
- Coordinación con los diferentes departamentos y el cliente durante el ciclo de vida del proyecto.

Por lo que firmo la presente, en Madrid, a 12 de Diciembre de 2014

Firmado:

Christian García

Director de Operaciones

PLIEGO DE CONDICIONES

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de un análisis, diseño y despliegue de una red WiFi en Santillana del Mar. En lo que sigue, se supondrá que el proyecto ha sido encargado por una empresa cliente a una empresa consultora con la finalidad de realizar dicho sistema. Dicha empresa ha debido desarrollar una línea de investigación con objeto de elaborar el proyecto. Esta línea de investigación, junto con el posterior desarrollo de los programas está amparada por las condiciones particulares del siguiente pliego.

Supuesto que la utilización industrial de los métodos recogidos en el presente proyecto ha sido decidida por parte de la empresa cliente o de otras, la obra a realizar se regulará por las siguientes:

Condiciones generales

1. La modalidad de contratación será el concurso. La adjudicación se hará, por tanto, a la proposición más favorable sin atender exclusivamente al valor económico, dependiendo de las mayores garantías ofrecidas. La empresa que somete el proyecto a concurso se reserva el derecho a declararlo desierto.

2. El montaje y mecanización completa de los equipos que intervengan será realizado totalmente por la empresa licitadora.

3. En la oferta, se hará constar el precio total por el que se compromete a realizar la obra y el tanto por ciento de baja que supone este precio en relación con un importe límite si este se hubiera fijado.

4. La obra se realizará bajo la dirección técnica de un Ingeniero Superior de Telecomunicación, auxiliado por el número de Ingenieros Técnicos y Programadores que se estime preciso para el desarrollo de la misma.

5. Aparte del Ingeniero Director, el contratista tendrá derecho a contratar al resto del personal, pudiendo ceder esta prerrogativa a favor del Ingeniero Director, quien no estará obligado a aceptarla.

6. El contratista tiene derecho a sacar copias a su costa de los planos, pliego de condiciones y presupuestos. El Ingeniero autor del proyecto autorizará con su firma las copias solicitadas por el contratista después de confrontarlas.

7. Se abonará al contratista la obra que realmente ejecute con sujeción al proyecto que sirvió de base para la contratación, a las modificaciones autorizadas por la superioridad o a las órdenes que con arreglo a sus facultades le hayan comunicado por escrito al Ingeniero Director de obras siempre que dicha obra se haya ajustado a los preceptos de los pliegos de condiciones, con arreglo a los cuales, se harán las modificaciones y la valoración de las diversas unidades sin que el importe total pueda exceder de los presupuestos aprobados. Por consiguiente, el número de unidades que se consignan en el proyecto o en el presupuesto, no podrá servirle de fundamento para entablar reclamaciones de ninguna clase, salvo en los casos de rescisión.

8. Tanto en las certificaciones de obras como en la liquidación final, se abonarán los trabajos realizados por el contratista a los precios de ejecución material que figuran en el presupuesto para cada unidad de la obra.

9. Si excepcionalmente se hubiera ejecutado algún trabajo que no se ajustase a las condiciones de la contrata pero que sin embargo es admisible a juicio del Ingeniero Director de obras, se dará conocimiento a la Dirección, proponiendo a la vez la rebaja de precios que el Ingeniero estime justa y si la Dirección resolviera aceptar la obra, quedará el contratista obligado a conformarse con la rebaja acordada.

10. Cuando se juzgue necesario emplear materiales o ejecutar obras que no figuren en el presupuesto de la contrata, se evaluará su importe a los precios asignados a otras obras o materiales análogos si los hubiere y cuando no, se discutirán entre el Ingeniero Director y el contratista, sometiéndolos a la aprobación de la Dirección. Los nuevos precios convenidos por uno u otro procedimiento, se sujetarán siempre al establecido en el punto anterior.

11. Cuando el contratista, con autorización del Ingeniero Director de obras, emplee materiales de calidad más elevada o de mayores dimensiones de lo estipulado en el proyecto, o sustituya una clase de fabricación por otra que tenga asignado mayor precio o ejecute con mayores dimensiones cualquier otra parte de las obras, o en general, introduzca en ellas cualquier modificación que sea beneficiosa a juicio del Ingeniero Director de obras, no tendrá derecho sin embargo, sino a lo que le correspondería si hubiera realizado la obra con estricta sujeción a lo proyectado y contratado.

12. Las cantidades calculadas para obras accesorias, aunque figuren por partida alzada en el presupuesto final (general), no serán abonadas sino a los precios de la contrata, según las condiciones de la misma y los proyectos particulares que para ellas se formen, o en su defecto, por lo que resulte de su medición final.

13. El contratista queda obligado a abonar al Ingeniero autor del proyecto y director de obras así como a los Ingenieros Técnicos, el importe de sus respectivos honorarios facultativos por formación del proyecto, dirección técnica y administración en su caso, con arreglo a las tarifas y honorarios vigentes.

14. Concluida la ejecución de la obra, será reconocida por el Ingeniero Director que a tal efecto designe la empresa.

15. La garantía definitiva será del 4% del presupuesto y la provisional del 2%.

16. La forma de pago será por certificaciones mensuales de la obra ejecutada, de acuerdo con los precios del presupuesto, deducida la baja si la hubiera.

17. La fecha de comienzo de las obras será a partir de los 15 días naturales del replanteo oficial de las mismas y la definitiva, al año de haber ejecutado la provisional, procediéndose si no existe reclamación alguna, a la reclamación de la fianza.

18. Si el contratista al efectuar el replanteo, observase algún error en el proyecto, deberá comunicarlo en el plazo de quince días al Ingeniero Director de obras, pues transcurrido ese plazo será responsable de la exactitud del proyecto.

19. El contratista está obligado a designar una persona responsable que se entenderá con el Ingeniero Director de obras, o con el delegado que éste designe, para todo relacionado con ella. Al ser el Ingeniero Director de obras el que interpreta el proyecto, el contratista deberá consultarle cualquier duda que surja en su realización.

20. Durante la realización de la obra, se girarán visitas de inspección por personal facultativo de la empresa cliente, para hacer las comprobaciones que se crean oportunas. Es obligación del contratista, la conservación de la obra ya ejecutada hasta la recepción de la misma, por lo que el deterioro parcial o total de ella, aunque sea por agentes atmosféricos u otras causas, deberá ser reparado o reconstruido por su cuenta.

21. El contratista, deberá realizar la obra en el plazo mencionado a partir de la fecha del contrato, incurriendo en multa, por retraso de la ejecución siempre que éste no sea debido a causas de fuerza mayor. A la terminación de la obra, se hará una recepción provisional previo reconocimiento y examen por la dirección técnica, el depositario de efectos, el interventor y el jefe de servicio o un representante, estampando su conformidad el contratista.

22. Hecha la recepción provisional, se certificará al contratista el resto de la obra, reservándose la administración el importe de los gastos de conservación de la misma hasta su recepción definitiva y la fianza durante el tiempo señalado como plazo de garantía. La recepción definitiva se hará en las mismas condiciones que la provisional, extendiéndose el acta correspondiente. El Director Técnico propondrá a la Junta Económica la devolución de la fianza al contratista de acuerdo con las condiciones económicas legales establecidas.

23. Las tarifas para la determinación de honorarios, reguladas por orden de la Presidencia del Gobierno el 19 de Octubre de 1961, se aplicarán sobre el denominado en la actualidad “Presupuesto de Ejecución de Contrata” y anteriormente llamado ”Presupuesto de Ejecución Material” que hoy designa otro concepto.

Condiciones particulares

La empresa consultora, que ha desarrollado el presente proyecto, lo entregará a la empresa cliente bajo las condiciones generales ya formuladas, debiendo añadirse las siguientes condiciones particulares:

1. La propiedad intelectual de los procesos descritos y analizados en el presente trabajo, pertenece por entero a la empresa consultora representada por el Ingeniero Director del Proyecto.

2. La empresa consultora se reserva el derecho a la utilización total o parcial de los resultados de la investigación realizada para desarrollar el siguiente proyecto, bien para su publicación o bien para su uso en trabajos o proyectos posteriores, para la misma empresa cliente o para otra.

3. Cualquier tipo de reproducción aparte de las reseñadas en las condiciones generales, bien sea para uso particular de la empresa cliente, o para cualquier otra aplicación, contará con autorización expresa y por escrito del Ingeniero Director del Proyecto, que actuará en representación de la empresa consultora.

4. En la autorización se ha de hacer constar la aplicación a que se destinan sus reproducciones así como su cantidad.

5. En todas las reproducciones se indicará su procedencia, explicitando el nombre del proyecto, nombre del Ingeniero Director y de la empresa consultora.

6. Si el proyecto pasa la etapa de desarrollo, cualquier modificación que se realice sobre él, deberá ser notificada al Ingeniero Director del Proyecto y a criterio de éste, la empresa consultora decidirá aceptar o no la modificación propuesta.

7. Si la modificación se acepta, la empresa consultora se hará responsable al mismo nivel que el proyecto inicial del que resulta el añadirla.

8. Si la modificación no es aceptada, por el contrario, la empresa consultora declinará toda responsabilidad que se derive de la aplicación o influencia de la misma.

9. Si la empresa cliente decide desarrollar industrialmente uno o varios productos en los que resulte parcial o totalmente aplicable el estudio de este proyecto, deberá comunicarlo a la empresa consultora.

10. La empresa consultora no se responsabiliza de los efectos laterales que se puedan producir en el momento en que se utilice la herramienta objeto del presente proyecto para la realización de otras aplicaciones.

11. La empresa consultora tendrá prioridad respecto a otras en la elaboración de los proyectos auxiliares que fuese necesario desarrollar para dicha aplicación industrial, siempre que no haga explícita renuncia a este hecho. En este caso, deberá autorizar expresamente los proyectos presentados por otros.

12. El Ingeniero Director del presente proyecto, será el responsable de la dirección de la aplicación industrial siempre que la empresa consultora lo estime oportuno. En caso contrario, la persona designada deberá contar con la autorización del mismo, quien delegará en él las responsabilidades que ostente.