

Trabajo Fin de Carrera

Proyecto UD-WIFI

Miguel Angel Castiella Lecuona

Índice de contenido

1. Descripción y objetivos del proyecto.....	5
2. Introducción a la tecnología Wireless.....	7
2.1. Estándar 802.11.....	7
2.2. Arquitectura estándar 802.11.....	10
2.3. Características radioeléctricas de un sistema WiFi.....	16
2.4. Esquemas de red.....	18
2.5. Elementos de una red Wireless.....	20
2.6. Seguridad en redes WiFi.....	21
2.7. Aspectos a tener en cuenta en una Wireless LAN.....	22
2.8. Estudio de impacto en la salud pública.....	24
3. Distribución temporal.....	27
4. Preparación del entorno.....	29
4.1. Situación al 1 de enero de 2006.....	29
5. Realización del pliego de condiciones.....	32
6. Valoración de productos presentados.....	33
7. Instalación de Hardware y Software.....	36
8. Instalación de un punto de acceso de pruebas	48
9. Instalación de los puntos de acceso del campus	57
10. Certificado de satisfacción de la instalación	58

11. Vista aérea del Campus.....	59
12. Glosario.....	60
13. Bibliografía.....	61

Índice de ilustraciones

Ilustración 1: Diferencias entre estándares inalámbricos.....	9
Ilustración 2: Distribución de canales, 2.4-2.4835 GHz.....	12
Ilustración 3: Condiciones técnicas de utilización en la banda de 5GHz.....	17
Ilustración 4: Conexión ad-hoc.....	18
Ilustración 5: Interconexión entre dispositivos a través de un punto de acceso	19
Ilustración 6: Conexión mediante antenas direccionales.....	20
Ilustración 7: Materiales y atenuación que producen.....	23
Ilustración 8: Velocidad de transmisión Vs Área de cobertura.....	24
Ilustración 9: Límites de radiación para distintas instituciones y bandas de frecuencia.....	25
Ilustración 10: Tabla de valoración de Empresas y Soluciones.....	34
Ilustración 11: Preparación de la instalación.....	37
Ilustración 12: Selección de la instalación. En nuestro caso seleccionamos 3WWM.....	38
Ilustración 13: Selección del directorio donde instalar.....	38
Ilustración 14: Selección del directorio donde se guardan las configuraciones	39

Ilustración 15: Confirmación para el comienzo de la instalación.....	39
Ilustración 16: Nueva confirmación de la instalación.....	40
Ilustración 17: Una vez instalado el software nos muestra un mensaje de que la instalación ha terminado. Ahora pasamos a configurar la instalación realizada.....	40
Ilustración 18: Selección del tipo de licencia. En nuestro caso no tenemos limitaciones.....	41
Ilustración 19: Introducción de la licencia que viene en el CD.....	41
Ilustración 20: Proceso de activación del software.....	42
Ilustración 21: Introducción de la clave de activación del producto.....	42
Ilustración 22: Introducción de la clave de la licencia de ampliación de puntos de acceso.....	43
Ilustración 23: Mensaje de la ampliación.....	43
Ilustración 24: Proceso de solicitud de la clave de activación I.....	43
Ilustración 25: Proceso de solicitud de la clave de activación II.....	44
Ilustración 26: Proceso de solicitud de la clave de activación IV.....	44
Ilustración 27: Proceso de solicitud de la clave de activación V.....	45
Ilustración 28: Proceso de solicitud de la clave de activación VI.....	45
Ilustración 29: Proceso de solicitud de la clave de activación VII.....	46
Ilustración 30: Proceso de solicitud de la clave de activación VIII.....	46
Ilustración 31: Proceso de solicitud de la clave de activación IX.....	47
Ilustración 32: Insertar perfil de radio.....	48

Ilustración 33: Nombre para el perfil de radio.....	49
Ilustración 34: Atributos 802.11.....	49
Ilustración 35: Selección de configuración automática de potencia de radio y canal de transmisión.....	50
Ilustración 36: Insertar Service Profile.....	51
Ilustración 37: Nombre del Perfil, SSID asociado y tipo de seguridad.....	51
Ilustración 38: Asociación de perfil de radio.....	52
Ilustración 39: Creación automática del SSID.....	52
Ilustración 40: Configuración del Servidor DHCP para las puntos de acceso...	53
Ilustración 41: Captura del número de serie.....	54
Ilustración 42: Inserción de un punto de acceso.....	54
Ilustración 43: Definición de datos del punto de acceso.....	55
Ilustración 44: Definición de radio. Importante marcar en Enabled.....	55
Ilustración 45: Aplicar cambios de configuración.....	56
Ilustración 46: Configuración de todas las antenas.....	57
Ilustración 47: Vista aérea del Campus.....	59

1. Descripción y objetivos del proyecto

Desde hace 5 años la Universidad de Deusto - campus de San Sebastián - en su apuesta por la innovación tecnológica, ha facilitado el uso de ordenadores portátiles como herramienta de trabajo para sus alumnos. Esta incorporación de equipos se ha ido realizando por cursos, empezando el primer año con los alumnos de primero, el segundo con los de primero y segundo y así hasta llegar a la totalidad del alumnado.

Para dar acceso a la red del campus e Internet, se tomó la decisión de utilizar la tecnología wireless, realizando la conectividad según se iba necesitando -el primer año las aulas de los alumnos de primero, el segundo las de segundo- así hasta llegar a dar conexión inalámbrica en todo el campus.

La no existencia de tecnología switching-wireless para su gestión provoca que si se desea realizar algún cambio en el acceso, por ejemplo incorporar una clave web o un cambio de SSID, se tenga que realizar antena por antena.

La Universidad de Deusto en su campus de San Sebastián pretende con este proyecto gestionar centralizadamente los espacios con cobertura WIFI correspondientes a ubicaciones concretas y localizadas. Para ello se va a acoger al programa "Acceso a Internet y movilidad con WI-FI" promovido por la SPRI (Sociedad para la Promoción y Reconversión Industrial), que ofrece subvenciones para la instalación de redes inalámbricas con tecnología WIFI ubicadas dentro de la Comunidad Autónoma del País Vasco.

Para poder recibir las ayudas que se contemplan en el programa de la SPRI, las instalaciones a dotar de cobertura WIFI deberán cumplir los siguientes requisitos:

1. La red inalámbrica WIFI debe permitir la conectividad a Internet de las personas que estén en tránsito por las instalaciones de la Universidad.

2. La Universidad debe garantizar la conectividad de los usuarios en condiciones de velocidad de banda ancha y de forma gratuita durante al menos un año a partir de la fecha de puesta en marcha de la instalación.

2. Introducción a la tecnología Wireless

El objetivo de este apartado es la presentación de la tecnología inalámbrica basada en el conjunto de estándares 802.11, y comúnmente conocida como tecnología Wi-Fi.

Una red de área local inalámbrica puede definirse como una red de alcance local que tiene como medio de transmisión el aire. Por red de área local se entiende una red que cubre un entorno geográfico limitado, con una velocidad de transferencia de datos relativamente alta (mayor o igual a 1 Mbps, tal y como especifica el IEEE), con baja tasa de errores y administrada de forma privada. Por red inalámbrica se entiende una red que utiliza ondas electromagnéticas como medio de transmisión de la información que viaja a través del canal inalámbrico, enlazando los diferentes equipos o terminales móviles asociados a la red.

Una red de área local inalámbrica, también llamada wireless LAN (WLAN), es un sistema flexible de comunicaciones que puede implementarse como una extensión, o directamente como una alternativa a una red cableada.

2.1. Estándar 802.11

En el año 1997 el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) ratificó el estándar 802.11, permitiendo una nueva forma de comunicación entre dispositivos utilizando los recursos radioeléctricos.

El estándar 802.11 es, en realidad, un conjunto de especificaciones que abarcan todos los aspectos de una red WLAN. Las especificaciones de nivel físico (802.11a, 802.11b y 802.11g) definen las técnicas de modulación y el procesamiento de la señal a bajo nivel. Por su parte, la calidad de servicio (QoS) es tratada por 802.11e y en 802.11i se describen robustos mecanismos de seguridad. Además, 802.11h y 802.11j procuran la interoperabilidad entre

los productos de diferentes continentes. Finalmente, 802.1X soporta la autenticación de usuarios.

- **802.11**

- Ancho de banda máximo de hasta 2 Mbps.
- Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
- Posible interferencia con hornos microondas y dispositivos bluetooth puesto que operan en el mismo espectro de frecuencias.
- Sistemas de modulación FHSS (Espectro Distribuido con Saltos de Frecuencias) y DSSS (Espectro Ensanchado de Secuencia Directa).

- **802.11b**

- Ancho de banda máximo de hasta 11Mbps.
- Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
- Las mismas interferencias que para 802.11.
- Conocido como WIFI.
- Modulación DSSS.
- Compatible con los equipos DSSS del estándar 802.11.

- **802.11g**

- Ancho de banda máximo de hasta 54 Mbps.

- Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
- Compatible con 802.11b.
- Modulación DSSS y OFDM.

- **802.11a**

- Ancho de banda máximo de hasta 54 Mbps.
- Opera en el espectro de 5 Ghz sin necesidad de licencia. Menos saturado.
- No es compatible con 802.11b y 802.11g.
- Modulación de OFDM.

	802.11	802.11a	802.11b	802.11g
Standard Approved	July 1997	September 1999	September 1999	Draft Stage. Completion Executed in 2002
Available Bandwidth	83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
Unlicensed Frequencies of Operation	2.4 - 2.4835 GHz	5.15 - 5.35 GHz & 5.725 - 5.825 GHz	2.4 - 2.4835 GHz	2.4 - 2.4835 GHz
Number of Non-Overlapping channels	3 (Indoor Or Outdoor)	4 Indoor UNII1, 4 Indoor/Outdoor UNII2, 4 Outdoor UNII3	3 (Indoor Or Outdoor)	3 (Indoor Or Outdoor)
Data Rate Per Channel	2,1 Mbps	54, 48, 36, 24, 18, 12, 9, 6 Mbps	11, 5.5, 2, 1 Mbps	54, 36, 33, 24, 22, 12, 11, 9, 6, 5.5, 2, 1 Mbps

Ilustración 1: Diferencias entre estándares inalámbricos

- **802.11e.** Su objetivo es proporcionar soporte de QoS (Calidad de Servicio) para aplicaciones de redes LAN. Se aplicará a los estándares físicos a, b y g de 802.11. La finalidad es proporcionar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y vídeo.

- **802.11i.** Se refiere al objetivo más frecuente del estándar 802.11, la seguridad. Se aplicará a los estándares físicos a, b y g de 802.11. Proporciona una alternativa a la Privacidad Equivalente Cableada (WEP) con nuevos métodos de encriptación y procedimientos de autenticación. IEEE 802.1x constituye una parte clave de 802.11i.

- **802.11d.** Constituye un complemento al nivel de Control de Acceso al Medio (MAC) en 802.11 para proporcionar el uso, a escala mundial, de las redes WLAN del estándar 802.11. Permitirá a los puntos de acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.

- **802.11f.** Su objetivo es lograr la interoperabilidad de Puntos de Acceso (AP) dentro de una red WLAN multiproveedor. El estándar define el registro de puntos de acceso dentro de una red y el intercambio de información entre los mismos, cuando un usuario se traslada desde un punto de acceso a otro.

- **802.11h.** El objetivo es cumplir los reglamentos europeos para redes WLAN a 5 GHz. Los reglamentos europeos para la banda de 5 GHz requieren que los productos tengan control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas, en particular el radar.

2.2. Arquitectura estándar 802.11

Una vez conocido el estándar en el que se va a basar el sistema, se deben poseer unos conocimientos previos sobre las técnicas de acceso y el tipo de modulaciones utilizadas. A continuación se introduce un apartado relativo a los

aspectos anteriormente mencionados con objeto de una mejor comprensión del funcionamiento del sistema.

En primer lugar se va a hablar sobre el método de acceso al medio, puesto que es una parte fundamental dentro del funcionamiento de cualquier tecnología que se sustenta en el entorno radio, ya que éste es un medio compartido por todos.

Atendiendo al modelo de capas OSI, antes de explicar la capa de enlace, se debe hacer referencia a la capa física, encargada de gestionar el tratamiento de la información a nivel de "bit físico". La capa física proporciona una serie de servicios a la capa MAC o capa de acceso al medio. El estándar 802.11 define dos posibles opciones para la elección de la capa física, FHSS o DSSS.

Estas dos posibles opciones se basan en la tecnología de espectro ensanchado. Esta tecnología consiste en difundir la señal de información a lo largo del ancho de banda disponible, es decir, en vez de concentrar la energía de las señales alrededor de una portadora concreta, lo que se hace es repartirla por toda la banda disponible. Este ancho de banda total se comparte con el resto de usuarios que trabajan en la misma banda frecuencial.

El método DSSS consiste en la generación de un patrón de bits redundante llamado señal de chip para cada uno de los bits que componen la señal de información. A continuación se efectúa una modulación de la señal resultante mediante una portadora de RF. En recepción es necesario realizar el proceso inverso para obtener la señal de información original.

En el caso de Estados Unidos y de Europa la tecnología de espectro ensanchado por secuencia directa, DSSS, opera en el rango que va desde los 2.4 GHz hasta los 2.4835 GHz. El ancho de banda total disponible es de 83.5 MHz. Este ancho de banda total se divide en un total de 14 canales con un ancho de banda por canal de 5 MHz.

En topologías de red que contengan varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias en el sistema si la separación entre las frecuencias centrales es como mínimo de 30 MHz. Esto significa que de los 83.5 MHz de ancho de banda total disponible se puede obtener un total de 3 canales independientes (canal 1, 6, 11), que pueden operar simultáneamente en una determinada zona geográfica sin que aparezcan interferencias en un canal procedentes de los otros dos canales. Esta independencia entre canales permite aumentar la capacidad del sistema de forma lineal, con el número de puntos de acceso operando en un canal que no se esté utilizando y hasta un máximo de tres canales.

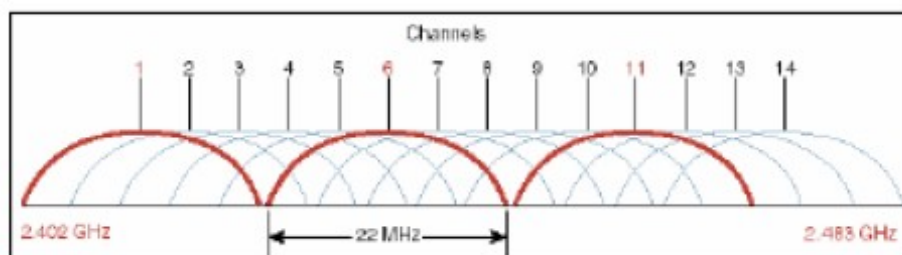


Ilustración 2: Distribución de canales, 2.4-2.4835 GHz.

El método FHSS consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada *dwell time*, inferior a 400ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se transmite en una frecuencia distinta durante un intervalo muy corto de tiempo.

Cada una de las transmisiones a una frecuencia concreta, se realiza utilizando una portadora de banda estrecha que va cambiando (saltando) a lo largo del tiempo. Este procedimiento equivale a realizar una partición de la información en el dominio temporal. El orden en los saltos en frecuencia que el emisor debe realizar viene determinado según una secuencia pseudoaleatoria que se encuentra definida en unas tablas, que tanto el emisor como el receptor deben conocer.

Existe una opción basada en infrarrojos, pero debido a su poca utilización en el ámbito comercial se omite cualquier explicación de la misma, puesto que se supone que carece de interés para la realización del presente proyecto.

Una vez tomado contacto con los métodos disponibles que están relacionados con la capa física, realizaré una breve explicación sobre los métodos de acceso al medio, utilizados por los dispositivos necesarios para la implantación de la tecnología basada en el estándar 802.11.

Los diferentes métodos de acceso de IEEE 802 están diseñados según el modelo OSI y se encuentran ubicados en el nivel físico, como se ha explicado anteriormente, y en la parte inferior del nivel de enlace o subnivel MAC. La capa de gestión MAC controlará aspectos como sincronización y los algoritmos del sistema de distribución, que se definen como el conjunto de servicios que precisa o propone el modo infraestructura.

El algoritmo básico de acceso al medio es relativamente conocido y se denomina CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance). A continuación se muestra el funcionamiento básico de dicho algoritmo. Cabe destacar que es necesario realizar unas modificaciones para poder tomar como válido el algoritmo en comunicaciones inalámbricas. Estas modificaciones son llevadas a cabo por el protocolo MACA.

- Antes de transmitir información una estación debe testear el medio, o canal inalámbrico, para determinar su estado (libre / ocupado).

- Si el medio no está ocupado por ninguna otra trama, la estación ejecuta una espera adicional llamada espaciado entre tramas.
- Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.
- Una vez finaliza esta espera debida a la ocupación del medio, la estación ejecuta el llamado algoritmo de Backoff, que determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado ventana de contienda. El algoritmo de Backoff da un número aleatorio y entero de ranuras temporales, y su función es la de reducir la probabilidad de colisión.
- Mientras se ejecuta la espera marcada por el algoritmo de Backoff se continúa escuchando el medio, de tal manera que si el medio se determina libre durante un tiempo de al menos un valor igual al espaciado entre tramas, esta espera va avanzando temporalmente hasta que la estación consume todas las ranuras temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior al de espaciado entre tramas, el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición.

Es el momento de analizar los diferentes problemas con los que se podría encontrar si se utilizara el anterior algoritmo en la implantación de sistemas inalámbricos.

Principalmente hay dos problemas: la aparición de nodos ocultos y de nodos expuestos.

El primero consiste en la situación en la que una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no oye. Por otro lado, el segundo problema se basa en que una estación cree que el canal

está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino. La solución que se implementa consiste en la utilización del protocolo MACA con CSMA/CA.

Para concluir con los datos técnicos del estándar 802.11, a continuación se presentan las diferentes modulaciones que utilizan los equipos WiFi.

- **CCK** Complementary Code Keying (Alternando Códigos Complementarios).
- **QAM** Quadrature Amplitude Modulation (Modulación De Amplitud En Cuadratura).
- **DSSS** Direct Sequence Spread Spectrum (Espectro Distribuido Consecuencia Directa).
- **FHSS** Frequency Hoping Spread Spectrum (Espectro Distribuido Con Saltos De Frecuencia).
- **BFSK** Binary Frequency Shift Keyed (Alternando Frecuencia Binaria).
- **BPSK** Binary Phase Shift Keyed (Alternando Cambio De Fase Binaria).
- **QPSK** Quadrature Phase Shift Keyed (Alternando Cambios De Fase En Cuadratura).
- **OFDM** Orthogonal Frequency Division Multiplexing (Multiplexando División De Frecuencia Ortogonal).
- **GFSK** Gaussian Frequency Shift Keyed (Alternando Cambios De Frecuencia Gausiana).
- **DQPSK** Differential Quadrature Phase Shift Keyed (Alternando Diferencia De Fase En Cuadratura).

- **DBPSK** Differential Binary Phase Shift Keyed (Alternando Diferencia Binaria De Fase).

2.3. Características radioeléctricas de un sistema WiFi

En este apartado se hace referencia a las características técnicas correspondientes de las bandas de frecuencias señaladas en el CNAF y que se corresponden con las bandas de trabajo de un sistema WiFi. Un sistema WiFi no deberá producir interferencias ni solicitar protección frente a otros servicios de radiocomunicaciones autorizados con categoría diferente.

- **UN – 85**
 - **Banda de frecuencias 2.400 a 2.483,5 MHz.** Estas frecuencias podrán ser utilizadas en redes de área local para la interconexión sin hilos entre ordenadores y dispositivos periféricos, para aplicaciones en interior de edificios. La potencia total será inferior a **100 mW** (PIRE). Otras condiciones de uso han de ser conformes a la Recomendación CEPT/ERC 70-03. Esta utilización se considera de uso común. Esta banda de frecuencias también podrá utilizarse para aplicaciones generales de baja potencia en recintos cerrados y exteriores de corto alcance. La potencia radiada máxima será inferior a **100 mW**. Esta utilización se considera de uso común. En ambos casos, las características radioeléctricas de estos equipos se ajustarán a las especificaciones ETSI ETS 300 328, ETS 300 440, o bien al estándar específico, si es el caso deberá realizarse la correspondiente evaluación de la conformidad.

● **UN-128** Redes de área local de altas prestaciones en la banda de 5 GHz. Las bandas de frecuencia indicadas seguidamente podrán ser utilizadas por el servicio móvil en redes de área local de altas prestaciones, de conformidad con las condiciones que se indican a continuación.

- **Banda 5.150 – 5.350 MHz:** En esta banda, el uso por el servicio móvil en redes de área local se restringe para su utilización únicamente en el interior de recintos, y las características técnicas deben ajustarse a las indicadas en la tabla adjunta, en el caso que sea de aplicación en función de la subbanda utilizada, y de las modalidades técnicas contempladas en la misma.

	POTENCIA (p.i.r.e.) (*)		
Banda (MHz)	Sistemas sin TPC	Sistemas con TPC	Sistemas con TPC y con DFS
5150-5250 (**)	30 mW	120 mW	200 mW
5250-5350 (**)	60 mW con DFS	200 mW con DFS	200 mW

Ilustración 3: Condiciones técnicas de utilización en la banda de 5GHz

(*) Se refiere a la potencia (P.I.R.E.) promediada sobre una ráfaga de transmisión ajustada a la máxima potencia

(**) En estas bandas, la densidad espectral de P.I.R.E. media no ha de exceder de 0,04 mW/4 Khz. medida en cualquier ancho de banda de 4 kHz.

TPC: se refiere a sistemas que dispongan de control de potencia transmitida.

DFS: se refiere a sistemas que dispongan de selección dinámica de frecuencia de acuerdo a la Recomendación UIT-R M.1652 sobre sistemas de acceso radio incluyendo RLAN en 5 GHz.

- **Banda 5.470 – 5.725 MHz.** Esta banda puede ser utilizada para redes de área local en el interior o exterior de recintos con potencia inferior o igual a **1 W** (P.I.R.E.). 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 incluyendo RLAN en la banda de 5 GHz.

2.4. Esquemas de red

Gracias a las diferentes configuraciones y posibilidades que ofrece el estándar IEEE 802, se pueden encontrar diferentes tipos de arquitecturas de red. Esto se debe, a que en función de las necesidades que se tengan, se puede encontrar una configuración determinada para obtener el resultado buscado. Dichas necesidades vienen impuestas por el tipo de servicio que se pretenda dar, así como por el tipo de equipos disponibles.

Existen dos modos de configuración de los equipos. El primero denominado "ad-hoc", comúnmente conocido como p2p (peer to peer). El segundo consiste en una red inalámbrica con infraestructura de red. El elemento clave de este modo de configuración es el punto de acceso.

- **Modo punto a punto.** La configuración más básica es la llamada de igual a igual o ad-hoc, que consiste en una red de dos terminales móviles equipados con la correspondiente tarjeta adaptadora para comunicaciones inalámbricas. Para que la comunicación entre estas dos estaciones sea posible, hace falta que exista una línea de visión directa, es decir, que cada una de ellas esté en el rango de cobertura radioeléctrica de la otra y no exista ningún tipo de obstáculo que pueda impedir la comunicación. Las redes de tipo ad-hoc son muy sencillas de implementar y no requieren ningún tipo de gestión administrativa.



Ilustración 4: Conexión ad-hoc

Modo Infraestructura. Este modo de configuración se caracteriza por aumentar el alcance del tipo de redes anteriormente mencionadas. El elemento

fundamental es el punto de acceso. En función de las prestaciones del equipo se puede conseguir una zona de cobertura relativamente amplia y que sea capaz de englobar un número amplio de usuarios. En esta nueva configuración se permite que dos equipos de usuarios puedan conectarse entre sí sin que sus respectivas zonas de cobertura se solapen. La comunicación se establece entre un usuario y el punto de acceso, y entre el punto de acceso y el usuario destino.

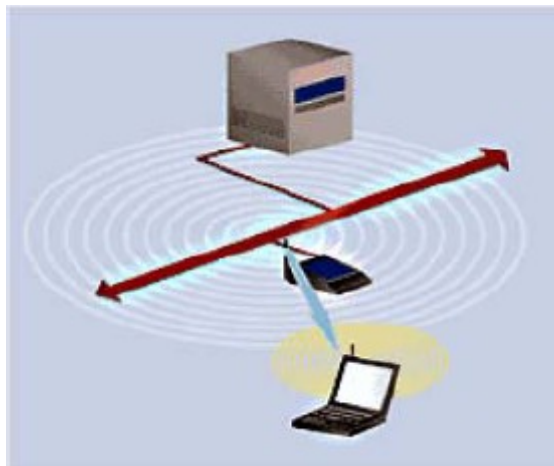


Ilustración 5: Interconexión entre dispositivos a través de un punto de acceso

En caso de ser necesaria una cobertura en una amplia zona geográfica, es posible conectar diferentes puntos de acceso entre sí. Las zonas de cobertura de los diferentes dispositivos deberán estar solapadas ligeramente para permitir el paso de una celda a otra. Se debe tener en cuenta los posibles problemas que pueden aparecer tras la instalación de los puntos de acceso, como pueden ser las interferencias entre canales o la aparición de zonas de sombra. Con objeto de aclarar conceptos, se puede ver este tipo de configuración como a un sistema celular de telefonía.

Otra posibilidad que ofrecen estos sistemas inalámbricos es la utilización de antenas directivas para interconectar puntos geográficos, físicamente separados una distancia considerable. El objetivo de estas antenas direccionales es el de enlazar redes que se encuentran situadas

geográficamente en sitios distintos, por ejemplo la conexión entre dos edificios con objeto de crear una red local.

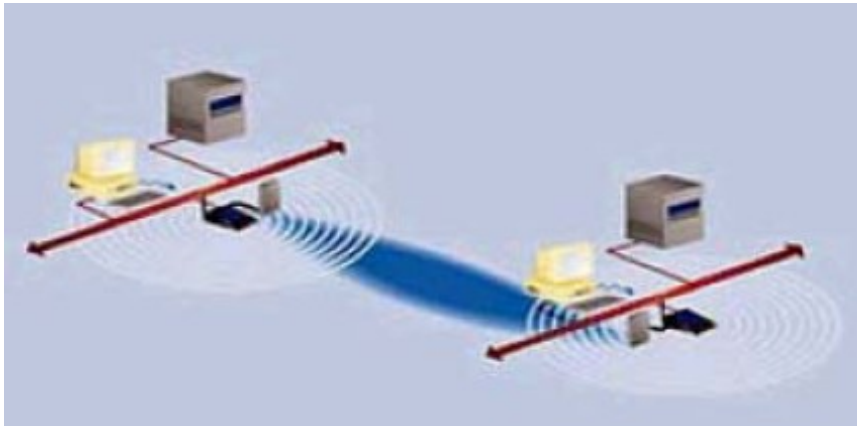


Ilustración 6: Conexión mediante antenas direccionales

2.5. Elementos de una red Wireless

A continuación se van a enunciar los diferentes elementos que se pueden encontrar en una red inalámbrica y su principal función.

- **Antena.** Es el elemento de transmisión básico. Puede estar integrada en el dispositivo o conectarse mediante cable coaxial al mismo. Tiene la función de enviar la información al espacio de una forma eficiente. Lo más usual es utilizar antenas omnidireccionales, ya que permiten una amplia zona de cobertura radial. En el caso de realizar conexiones punto a punto o conexiones a larga distancia, se deberá utilizar antenas directivas. Se deben tener en cuenta factores como el ancho de banda, potencia emitida y la directividad.

- **Puntos de acceso (AP).** Actúa como puente con dos tipos de interfaces, el inalámbrico hacia los terminales inalámbricos y el cableado hacia la red troncal (Ethernet). El AP es el encargado de coordinar la comunicación entre los terminales inalámbricos que están conectados a él. Posee funcionalidades para la asignación de recursos, mediante el uso de tramas sonda, asignando un canal a los usuarios que se asocian al AP.

- **Distribution System (DS).** Es la parte cableada de la red inalámbrica. Generalmente es una red Ethernet de la que cuelgan los AP. Pueden existir otros tipos de configuraciones del DS, ya que no existe un estándar que lo fije.

2.6. Seguridad en redes WiFi

Un aspecto de vital importancia en las redes inalámbricas es la seguridad de la información. Una red debe asegurar la integridad de los datos que transmite. En las redes WiFi la seguridad ha sido un aspecto más que cuestionable, puesto que se ha ido demostrando que se podía burlar la seguridad de las mismas.

Existen varios protocolos de seguridad desarrollados para el estándar WiFi. Estos protocolos serán comentados a continuación.

El protocolo básico utilizado en este tipo de redes es conocido como *WEP* que se encarga de proporcionar una transmisión relativamente segura. El funcionamiento de dicho protocolo se basa en la encriptación de la información mediante una clave de 128 o 64 bits. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave. Existen más posibilidades de cifrado WEP, como WEP 152, 256 y hasta 512 bits.

Uno de los mayores problemas del cifrado WEP, es que ya han sido demostradas múltiples vulnerabilidades que lo hacen débil frente a ataques. Para mejorar el cifrado WEP, se ha desarrollado otro protocolo de seguridad más eficiente, conocido como WPA. A nivel de cifrado WPA es WEP, pero cambiando constantemente de claves, aumentando el número de vectores de inicialización posibles y el tamaño de las claves de encriptación. Se ha demostrado que este protocolo, al igual que WEP, es inseguro.

Finalmente, tras los intentos fallidos de obtener un cifrado robusto para las redes WiFi, se ha desarrollado la segunda versión WPA, WPA2. Se distingue de la primera versión en que introduce el concepto de autenticación segura de los usuarios.

Existen otras formas de aumentar la seguridad de las redes WiFi atendiendo a las funcionalidades que permiten los puntos de acceso. Una de ellas es el filtrado de direcciones MAC. Esta solución es conocida con el nombre ACL. La habilitación del filtrado de direcciones MAC permite la inclusión o exclusión de usuarios sobre la base de sus direcciones MAC, que son únicas, puesto que hacen referencia al dispositivo de red utilizado por el usuario.

Otra posibilidad, es la desconexión de la difusión del identificador de la red SSID. Mediante la desconexión de la difusión SSID se añade otro nivel más de desconocimiento para acceder a la red, lo que hace más difícil para cualquier usuario no autorizado tener acceso a la misma. Este método es conocido con el nombre CNAC. Este mecanismo pretende controlar el acceso a la red inalámbrica, permitiéndolo únicamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID), actuando éste como contraseña.

Para concluir con el tema de la seguridad en este tipo de redes, se puede hacer uso de tecnologías como las redes privadas virtuales (VPN), o la implementación de dispositivos creados íntegramente para la seguridad como los corta fuegos (FireWalls).

2.7. Aspectos a tener en cuenta en una Wireless LAN

Una vez visto el concepto general de lo que significa una red inalámbrica, así como de su funcionamiento básico, diferentes arquitectura y equipos, hay que mencionar algunos aspectos que son de vital importancia para el buen funcionamiento de la red inalámbrica.

En primer lugar, se debe tener en cuenta la atenuación que puede sufrir la señal mientras se propaga por el medio de transmisión. Como se ha visto, se va a estar trabajando en torno a los 2.4GHz, por teoría de las ondas electromagnéticas se sabe que a mayor frecuencia, la señal es más sensible a las atenuaciones, cuanto mayor sea la frecuencia la línea de visión directa que necesitan es mayor. En un sistema inalámbrico, el entorno de trabajo será una zona interior con múltiples obstáculos, lo que acusará el fenómeno de las atenuaciones. A continuación se muestra una tabla en la que se relacionan los distintos materiales con la atenuación que produce.

Material	Ejemplo	Atenuación
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Arboles y plantas	Media
Agua	Lluvia, Niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos papel	Alta
Vidrio con alto contenido de plomo	Ventanas	Alta
Metal	Vigas, armarios	Muy Alta

Ilustración 7: Materiales y atenuación que producen

Otro tipo de problemas relacionados con el medio de transmisión, son las diferentes interferencias que puede haber provocando daños irreversibles en la señal útil. Hay que tener mucha precaución con los sistemas que operan en la misma banda frecuencial.

- Transformadores.
- Motores Eléctricos De Uso Industrial (Como Los Refrigeradores).
- Hornos Microondas.
- Otras redes WLAN.
- Otros Equipos De Radio (Bluetooth).

También se debe tener en cuenta que la velocidad de transmisión varía en función de la distancia. Los sistemas inalámbricos pueden trabajar en un rango de alcance variable. Es lógico pensar que cuanto mayor alcance se necesite, la tasa de información por unidad de tiempo será menor, puesto que será necesaria la implementación de técnicas referentes a la redundancia en la información, para garantizar su correcta recepción. En la siguiente figura se puede apreciar este efecto.

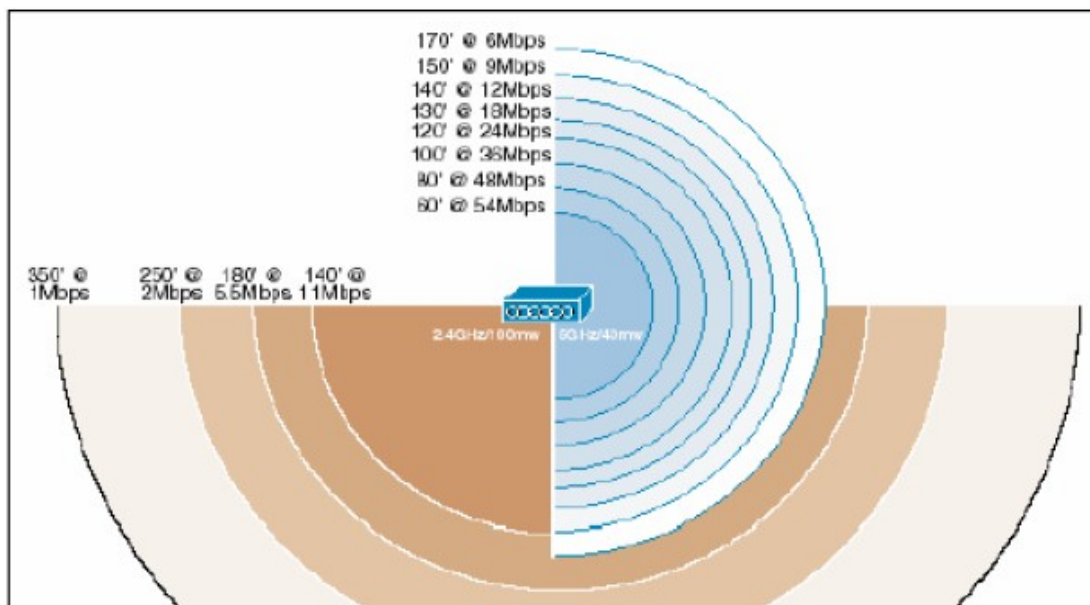


Ilustración 8: Velocidad de transmisión Vs Área de cobertura

2.8. Estudio de impacto en la salud pública

En este apartado se hace referencia al posible impacto de las tecnologías inalámbricas en la salud pública. La implantación rápida de estas tecnologías, así como de los aparatos necesarios para su propagación, ha provocado un riesgo, ya que ha sido imposible realizar un estudio previo de la influencia de las tecnologías inalámbricas en la salud de las personas.

Los efectos biológicos de las ondas RF dependen de la tasa de energía absorbida, denominada técnicamente tasa de absorción específica (SAR) y se mide en W/kg. Al ser difícil de medir este último parámetro, suele medirse la densidad de potencia de la onda. La SAR máxima que impone la Unión Europea es 1,6 W/kg, aunque la tasa media que se aconseja para toda la población es

de 0,008 W/kg con picos de 2 W/kg no más de 6 minutos. Actualmente existe una falta de consenso total entre los distintos países, que ya han establecido límites de radiación y normas de seguridad al respecto.

	TELEFONÍA MÓVIL		ACCESO FIJO INALÁMBRICO	
	900MHz	1800MHz	3.5GHz	26GHz
ICNIRP	4.5 W/m ²	9 W/m ²	10 W/m ²	10 W/m ²
CENELEC	4.5 W/m ²	9 W/m ²	--	--
FCC	6 W/m ²	10 W/m ²	10 W/m ²	10 W/m ²
ANSI/IEEE	6 W/m ²	12 W/m ²	23 W/m ²	10 W/m ²
CANADA	6 W/m ²	10 W/m ²	10 W/m ²	10 W/m ²

Ilustración 9: Límites de radiación para distintas instituciones y bandas de frecuencia.

La situación actual en España está regida por el Real Decreto 1066/2001 que fue publicado el 28 de febrero de 2001. Este decreto supone un desarrollo de la Ley General de las Telecomunicaciones en cuanto al establecimiento de límites de exposición y otras restricciones a las emisiones radioeléctricas. Surgió como respuesta a la preocupación social generada con la implantación en zonas urbanas de los nuevos sistemas inalámbricos. Ha sido elaborado conjuntamente por los Ministerios de Sanidad y Consumo y de Ciencia y Tecnología. Las líneas generales establecidas por este decreto son las siguientes.

- Convierte en obligatorios los límites de exposición a emisiones radioeléctricas fijadas en la Recomendación del Consejo de la Unión Europea (1999/519/CE), recogidos a su vez de la ICNIRP.

- Garantiza una continuidad en las limitaciones de los niveles, mediante la presentación de certificaciones por parte de los operadores de telefonía móvil y de los que establezcan redes soporte de servicios de radiodifusión sonora y TV.
- Obliga a una adecuación de las estaciones base de radiodifusión sonora y TV instaladas y en funcionamiento a los requisitos del Real Decreto, mediante la presentación de una certificación en un plazo de 9 meses.
- Obliga a la aprobación de proyectos técnicos, previos a la puesta en servicio de una instalación, con estudio de exposición a emisiones, que tenga en cuenta el entorno.
- Inspección previa a la puesta en servicio.
- Elaboración de informes anuales y de planes de inspección por parte del Ministerio de Ciencia y Tecnología.

Más tarde, concretamente el 11 de enero de 2002, se publicó la orden CTE/23/2002 que establecía las condiciones para la presentación de estudios y certificaciones por parte de los proveedores de servicios de telecomunicaciones. Las principales características fijadas por esta orden son:

- Regula las condiciones, contenido y formato de los estudios y certificaciones a los que hace referencia el Real Decreto anterior.
- Se fija la tipología de las estaciones radioeléctricas.
- Se fijan los procedimientos de realización de los estudios de los niveles de exposición y se establecen modelos para los documentos de certificación.

3. Distribución temporal

Preparación del entorno

- Objetivo: Recopilar información sobre la distribución de los puntos de acceso existentes, configuraciones,...
- Duración: 2 días.

Realización del pliego de condiciones

- Objetivo: Crear un documento con las condiciones mínimas requeridas de la instalación que será presentada a los proveedores.
- Duración: 1 día.

Valoración de los productos presentados

- Objetivo: Crear una tabla con las valoraciones de los diferentes productos para presentar a la dirección de la Universidad.
- Duración: 2 días.

Instalación de hardware y software

- Objetivo: Instalar el hardware del producto seleccionado y el software asociado al mismo, si fuera necesario.
- Duración: 1 día.

Instalación de un punto de acceso de pruebas

- Objetivo: Instalar un punto de acceso de pruebas para comprobar que todo funciona correctamente.

- Duración: 1 día.

Instalación de los puntos de acceso del campus

- Objetivo: Instalación de los puntos de acceso de la red inalámbrica WIFI.
- Duración: 2 días.

4. Preparación del entorno

4.1. Situación al 1 de enero de 2006

El campus de la Universidad está repartido en varios edificios que tienen un armario de comunicación cada uno. Algunos de los edificios tienen uno por cada planta. Todos estos armarios están conectados por fibra óptica al edificio Matteo Ricci, en el que está el Servicio Informático. Los diferentes puntos de acceso se distribuyen por todo el campus, conectados a los switches de los armarios que les corresponde.

El acceso a la red WIFI del campus es libre, no está protegida con ningún tipo de seguridad. El usuario que se conecta a esta red entra en la VLAN de alumnos, VLAN 5, donde sólo pueden salir a Internet a través de un servidor proxy http no transparente.

Para poder acceder, los usuarios se tienen que conectar al SSID "101". A modo de anécdota contaremos que el nombre de SSID es debido a que el primer punto de acceso que se puso en el aula 101 hace ya 5 años.

Además del servidor proxy, los usuario de la red WIFI se pueden conectar a un servidor de archivos que está en la dirección IP 192.168.20.8. En este servidor los alumnos de la Facultad de Humanidades y Comunicación pueden acceder a una serie de carpetas, en la que pueden copiar sus trabajos y donde los profesores les pueden dejar diferentes tareas y ejemplos.

La biblioteca dispone de unas Bases de Datos en CD-Rom que están dispuestas para poder acceder a ellas a través de un cliente ICA-Citrix. El servidor de los CD-Rom de bases de datos se encuentra en el campus de Bilbao, por lo que tienen que tener acceso a las direcciones 130.206.100.170 a 130.206.100.175.

Aunque el acceso de la red WIFI está abierto, está pensado para uso de los alumnos, que siempre tienen que tener conexión disponible a la plataforma educativa ALUD, hospedada fuera de la Universidad y acceso a su cuenta de correo electrónico. Estas dos conexiones las hacen a través de clientes HTTP.

Además, los usuarios de esta red reciben una IP de un servidor DHCP situado en la IP 10.2.0.1. La IP que reciben es del rango 10.2.0.0/16 con puerta de enlace 10.2.0.254. El servidor DHCP les proporciona la dirección DNS, la IP 193.146.227.190, IP a la que tiene que tener acceso.

En total el campus de San Sebastián de la Universidad de Deusto dispone de 39 puntos de acceso a la red WIFI. Como están pensados para el acceso del alumnado, las diferentes antenas están dispuestas en aulas, biblioteca y Servicio Informático. A continuación detallamos una relación de las diferentes antenas, edificio en el que se encuentran, switch y boca del mismo al que están conectadas.

<i>Antena</i>	<i>Ubicación</i>	<i>Dirección IP</i>	<i>Switch</i>	<i>Boca</i>
<i>Antena-40</i>	Edificio Biblioteca	10.10.3.40	192.168.250.111	22
<i>Antena-41</i>	Edificio Biblioteca	10.10.3.41	192.168.250.111	23
<i>Antena-43</i>	Edificio Biblioteca	10.10.3.43	192.168.250.111	20
<i>Antena-57</i>	Edificio Biblioteca	10.10.3.57	192.168.250.119	12
<i>Antena-59</i>	Edificio Biblioteca	10.10.3.59	192.168.250.119	24
<i>Antena-5</i>	Edificio Matteo Ricci	10.10.3.5	192.168.250.131	48
<i>Antena-42</i>	Edificio Matteo Ricci -planta baja	10.10.3.42	192.168.250.126	33
<i>Antena-34</i>	Edificio Padre Arrupe – planta baja	10.10.3.34	192.168.250.107	15
<i>Antena-36</i>	Edificio Padre Arrupe – planta baja	10.10.3.36	192.168.250.116	1
<i>Antena-37</i>	Edificio Padre Arrupe – planta baja	10.10.3.37	192.168.250.107	17
<i>Antena-64</i>	Edificio Padre Arrupe – planta baja	10.10.3.64	192.168.250.107	16
<i>Antena-65</i>	Edificio Padre Arrupe – planta baja	10.10.3.65	192.168.250.107	18
<i>Antena-30</i>	Edificio Padre Arrupe – planta 1	10.10.3.30	192.168.250.118	22
<i>Antena-32</i>	Edificio Padre Arrupe – planta 2	10.10.3.32	192.168.250.118	24
<i>Antena-33</i>	Edificio Padre Arrupe – planta 2	10.10.3.33	192.168.250.118	21
<i>Antena-45</i>	Torre de Biblioteca	10.10.3.45	192.168.250.123	14
<i>Antena-46</i>	Torre de Biblioteca	10.10.3.46	192.168.250.123	15
<i>Antena-47</i>	Torre de Biblioteca	10.10.3.47	192.168.250.123	13
<i>Antena-48</i>	Torre de Biblioteca	10.10.3.48	192.168.250.123	5
<i>Antena-49</i>	Torre de Biblioteca	10.10.3.49	192.168.250.123	2
<i>Antena-51</i>	Torre de Biblioteca	10.10.3.51	192.168.250.123	1
<i>Antena-53</i>	Torre de Biblioteca	10.10.3.53	192.168.250.123	6
<i>Antena-70</i>	Edificio de Administración	10.10.3.70	192.168.250.114	21
<i>Antena-20</i>	Edificio Padre Errandonea	10.10.3.20	192.168.250.102	13

<i>Antena</i>	<i>Ubicación</i>	<i>Dirección IP</i>	<i>Switch</i>	<i>Boca</i>
<i>Antena-21</i>	Edificio Padre Errandonea	10.10.3.21	192.168.250.102	22
<i>Antena-22</i>	Edificio Padre Errandonea	10.10.3.22	192.168.250.102	15
<i>Antena-24</i>	Edificio Padre Errandonea	10.10.3.24	192.168.250.102	14
<i>Antena-25</i>	Edificio Padre Errandonea	10.10.3.25	192.168.250.102	21
<i>Antena-44</i>	Edificio Padre Errandonea	10.10.3.44	192.168.250.102	24
<i>Antena-52</i>	Edificio Padre Errandonea	10.10.3.52	192.168.250.102	16
<i>Antena-54</i>	Edificio Padre Errandonea	10.10.3.54	192.168.250.102	17
<i>Antena-62</i>	Edificio Padre Errandonea	10.10.3.62	192.168.250.102	23
<i>Antena-71</i>	Centro NewCon	10.10.3.71	192.168.250.134	24
<i>Antena-27</i>	Edificio Loiola Centrum	10.10.3.27	192.168.250.133	11
<i>Antena-28</i>	Edificio Loiola Centrum	10.10.3.28	192.168.250.133	12
<i>Antena-55</i>	Torre de la ESTE	10.10.3.55	192.168.250.105	17
<i>Antena-56</i>	Torre de la ESTE	10.10.3.56	192.168.250.105	14
<i>Antena-58</i>	Torre de la ESTE	10.10.3.58	192.168.250.105	16
<i>Antena-63</i>	Torre de la ESTE	10.10.3.63	192.168.250.105	15

5. Realización del pliego de condiciones

El pliego de condiciones consiste en un texto en el que recogemos las especificaciones mínimas que necesitamos para el proyecto. Este pliego será presentado a los diferentes proveedores para que realicen presupuestos y organicen presentaciones. Sobre estos presupuestos y presentaciones se realizará una valoración que será presentada a la dirección de la Universidad.

En el anexo 1 contiene el pliego de condiciones.

6. Valoración de productos presentados

Al proyecto se presentan una serie de empresas de las que preseleccionamos cinco con un total de 4 soluciones. Por motivos de privacidad se va a omitir los nombres de las empresas y se van a identificar a partir de ahora como Empresa1, Empresa2, Empresa3, Empresa4 y Empresa5.

Cada una de estas empresas realiza una demostración de sus productos. Durante esta demostración se les irán solicitando una serie de necesidades, con lo que podremos hacer una valoración del producto y del grado de conocimiento de la empresa sobre el mismo.

Sobre esta demostración y por los presupuestos presentados se realiza una tabla en la que se puntúa de 0 a 5 una serie de valores, que a su vez tienen un determinado peso sobre el global. De la suma de todas las puntuaciones dependiendo de su peso se obtiene una puntuación. Sobre esta puntuación se decidirá la solución seleccionada, que se presentará a la dirección de la Universidad.

Vamos a separar la solución en tres apartados:

1. Precio. Con un peso de 20 sobre 100 valoramos el precio de la solución. En este apartado tendremos en cuenta tres subapartados:

- Precio del punto de acceso. Peso de 3 sobre 100.
- Precio del equipo de gestión. Peso de 7 sobre 100.
- Precio del mantenimiento anual. Peso de 10 sobre 100.

2. Solución: Con un peso de 55 sobre 100 valoramos la solución en si misma. Dividimos este apartado en 7 subapartados:

- Funcionalidades del punto de acceso: Peso de 12 sobre 100.

- Funcionalidades del equipamiento de gestión. Peso de 12/100.
- Sencillez de uso: Peso de 5 sobre 100.
- Calidad de la presentación de la propuesta: Peso de 8 sobre 100.
- Documentación adjuntada: Peso de 5 sobre 100.
- Garantía del equipamiento: Peso de 5 sobre 100.
- Formación ofrecida a técnicos UD: Peso de 8 sobre 100.

3. Empresa: Con un peso de 25 sobre 100 valoramos la empresa presentadora de la solución. Dividimos este apartado en 3 subapartados:

- Confianza en la empresa: Peso de 7 sobre 100.
- Soporte técnico: Peso de 10 sobre 100.
- Antecedentes con la Universidad de Deusto: Peso de 8 sobre 100.

Sobre este patrón se crea la siguiente tabla:

(Evaluar de 0-5)	Peso	Empresa1-Alcatel	Empresa2 -3Com	Empresa3-Cisco	Empresa4-3om	Empresa5-Enterasys
PRECIO						
Precio del Punto de Acceso	3	2	5	1	5	2
Precio del Equipo de Gestión por AP	7	4	5	1	5	2
Precio del Mantenimiento anual	10	2	5	1	5	2
	20	2,70	5,00	1,00	5,00	2,00
SOLUCION						
Características del AP (funcionalidades)	12	4	4	5	4	5
Funcionalidades del equipamiento de gestión	12	4	3	4	3	3
Sencillez de uso	5	4	3	4	3	3
Calidad de la presentación de la propuesta	8	5	4	4	1	1
Documentación adjuntada	5	3	4	5	3	2
Garantía del equipamiento	5	3	3	5	3	3
Formación ofrecida a técnicos UD	8	3	3	3	3	3
	55	3,82	3,45	4,25	2,93	3,05
EMPRESA						
Confianza en la empresa	7	5	5	4	2	3
Soporte técnico	10	5	4	4	1	1
Antecedentes con la UD	8	5	3	3	3	1
	25	5,00	3,96	3,68	1,92	1,56
TOTALES	100	3,89	3,89	3,46	3,09	2,47

Ilustración 10: Tabla de valoración de Empresas y Soluciones

Como podemos ver en la tabla, aunque la empresa y solución más valorada es la Empresa1 y Alcatel, el apartado de precio va a hacer que nos decantemos por la solución de la Empresa2 y solución 3Com.

Esto es debido a que los equipamientos de gestión sólo funcionan con antenas de su propia marca. Así, Alcatel sólo funciona con puntos de acceso de su marca, no soportando las antenas de 3Com. Como hemos visto anteriormente, el campus dispone de 39 antenas inalámbricas instaladas, todas ellas de 3Com (5 puntos de acceso de 3Com deberán de ser sustituidas por nuevas ya que por su antigüedad no pueden ser actualizadas a un firmware que permita su gestión).

No tener que cambiar la mayoría de los puntos de acceso supone un ahorro de unos 9.000 euros sobre la factura final, lo que supone más o menos una rebaja del 40% sobre la solución de Alcatel.

En cuanto a la solución tenemos que destacar la de Cisco. Desgraciadamente su precio hace imposible la adquisición del producto.

7. Instalación de Hardware y Software

El 3com WX4400 es un equipo para colocar en rack y que ocupa 2U. Aunque dispone de una fuente de alimentación redundante, no hemos seleccionado esta opción. Además tiene 4 entradas ethernet para conectarlo a la red, en nuestro caso hemos utilizado la primera de las tomas para realizar la conectividad. El cable UTP debe estar cruzado. Mediante una entrada serie se puede conectar una consola para monitorizar y configurar tres aspectos básico del equipo:

- El país donde va a estar instalado. Este apartado es vital, ya que cada país legisla de manera deferentes su espacio de radio frecuencia. Así por ejemplo la distribución de canales dentro de la frecuencia de los 2.4 Ghz es distinto para Francia que para España.
- La dirección IP del equipo. Ésta es la IP con la que el equipo va a estar en la red, con la que se va a comunicar con el equipo donde está instalado el software de gestión.
- Nombre del equipo. Hay que identificar el equipamiento con un nombre.

Una vez está el hardware en funcionamiento, debemos de instalar el software de gestión. Desgraciadamente, éste es uno de los aspectos negativos del producto, sólo existe software para funcionar sobre máquinas con sistema operativo Microsoft Windows 2000 o Microsoft Windows 2003. Además como mínimo debe tener 1 Gb de memoria RAM.

Una vez cumplidos estos requerimientos, el proceso de instalación no tiene ningún tipo de problema. En una instalación típica de los productos de Microsoft, sólo debemos de ir pulsando en el botón de siguiente.

El producto viene por defecto para 24 licencias de cliente (puntos de acceso), así que una vez instalado el software lo primero que hacemos es

actualizar las 24 licencias extra que necesitamos para poder capturar todas las antenas del campus. Para realizar esto, debemos dar de alta el producto en la web de 3com. Desgraciadamente esta petición debe realizarse en un navegador Microsoft Internet Explorer, además la versión del sistema operativo del sistema y el navegador deben estar en Inglés. Para los que tenemos una inclinación por el software libre este tipo de actividades nos resultan como mínimo reprobables, y desde luego incompresible en una marca mundialmente extendida como 3com. Cuando el producto está registrado hay que pedir un código de activación. En el proceso de solicitud se nos pide un código que se llama licence-key, que obtenemos al comprar la aplicación. Este código de activación es introducido en el software de gestión.

A continuación presentamos unas imágenes con las capturas de pantalla de la instalación del software en la máquina:

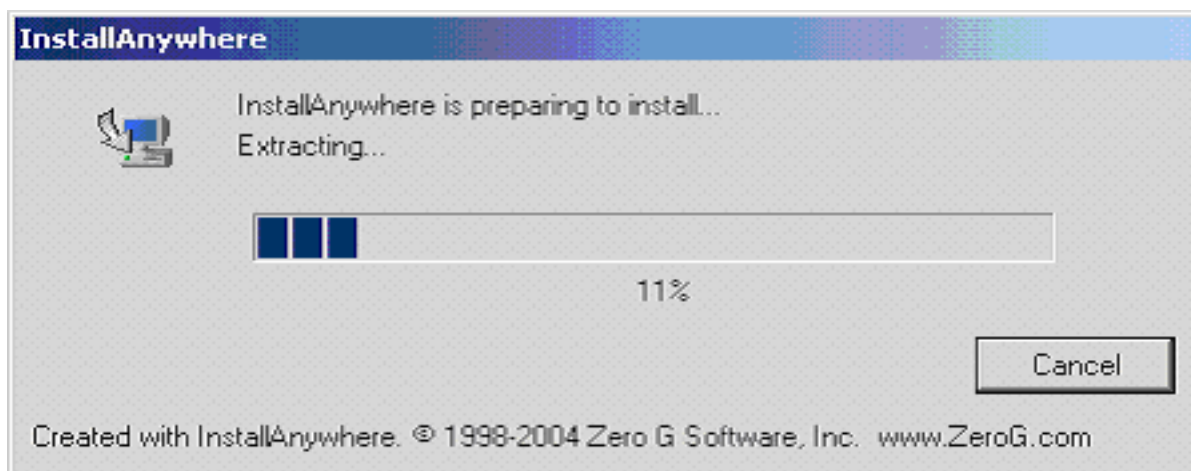


Ilustración 11: Preparación de la instalación



Ilustración 12: Selección de la instalación. En nuestro caso seleccionamos 3WXM

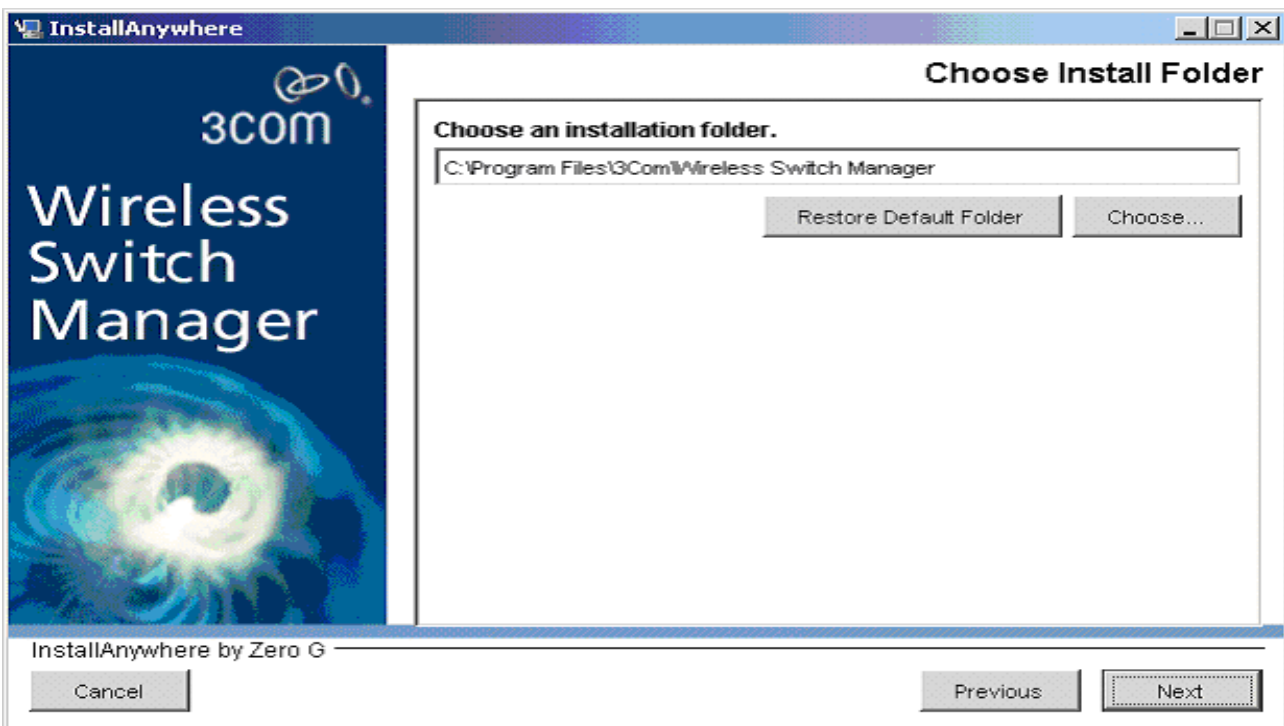


Ilustración 13: Selección del directorio donde instalar

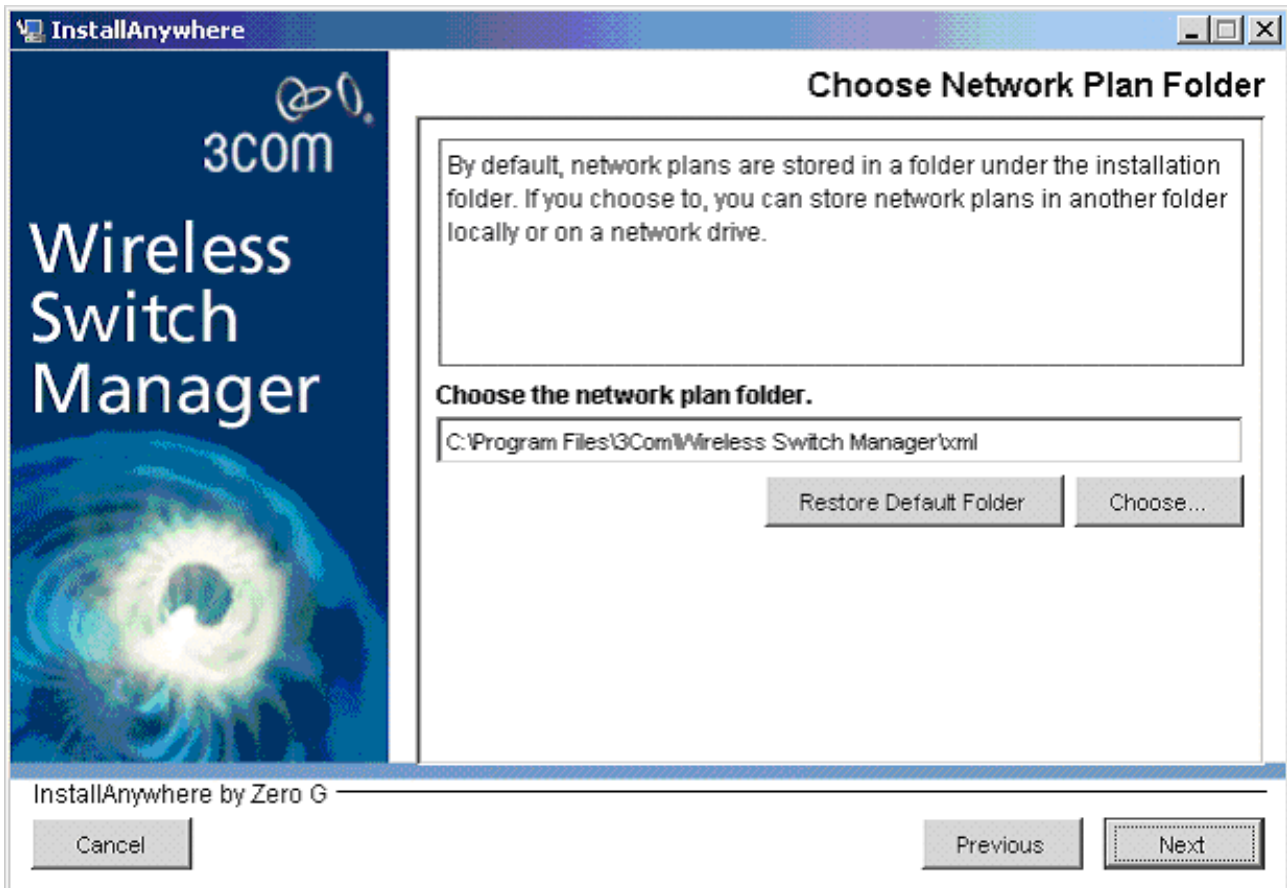


Ilustración 14: Selección del directorio donde se guardan las configuraciones

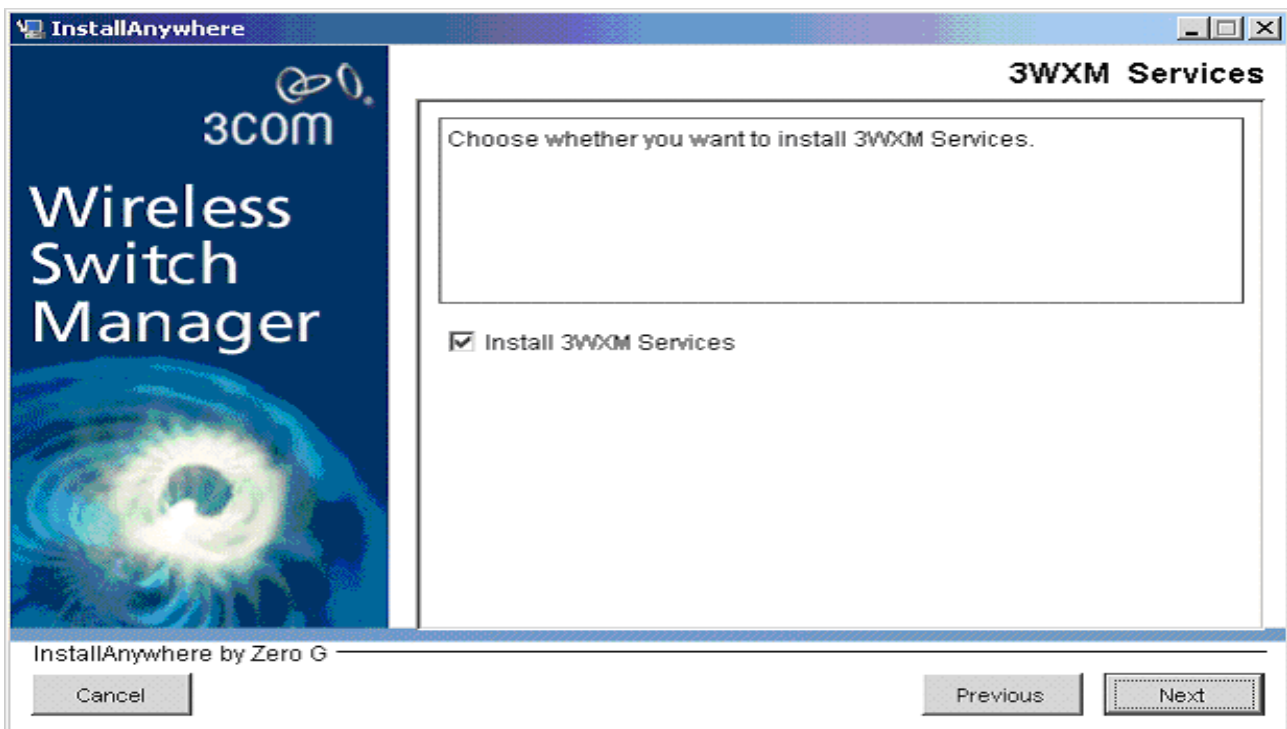


Ilustración 15: Confirmación para el comienzo de la instalación

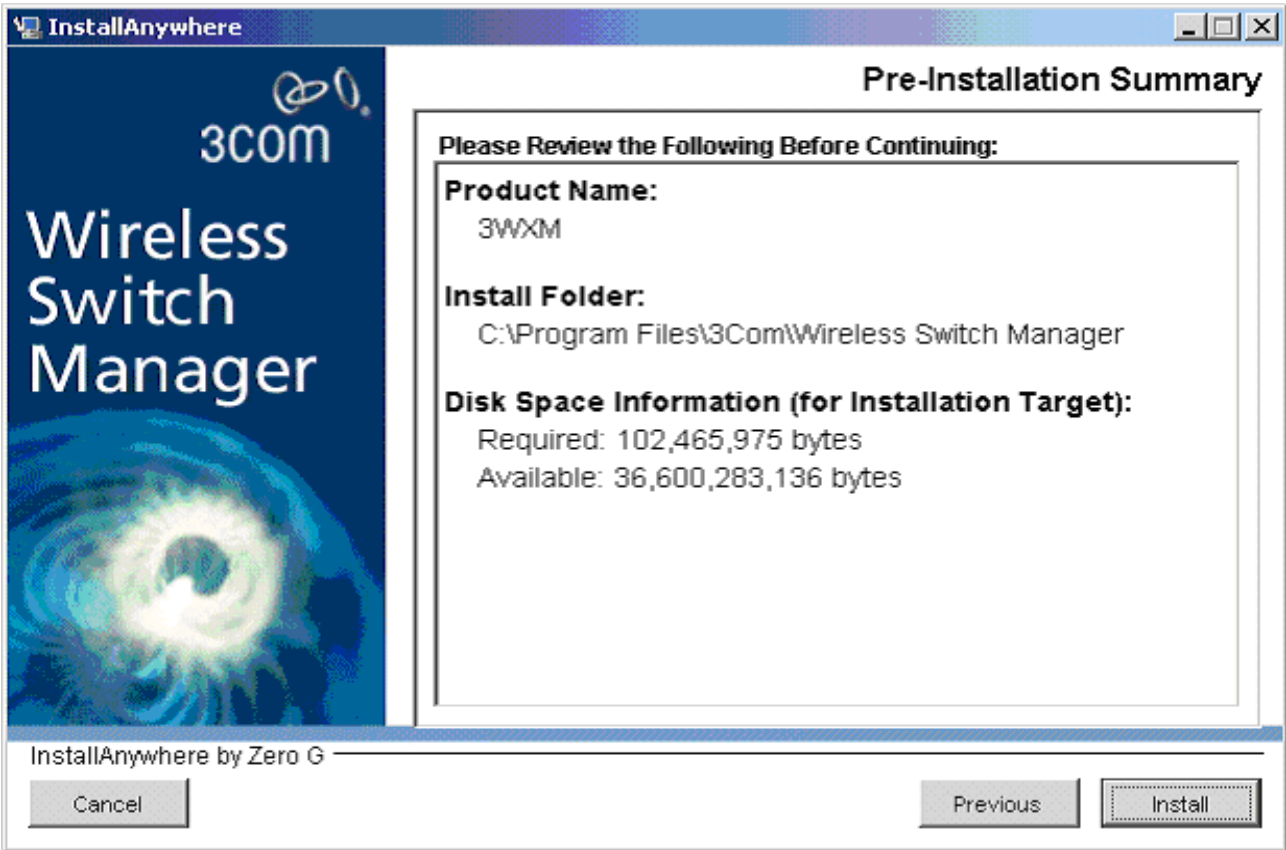


Ilustración 16: Nueva confirmación de la instalación



Ilustración 17: Una vez instalado el software nos muestra un mensaje de que la instalación ha terminado. Ahora pasamos a configurar la instalación realizada

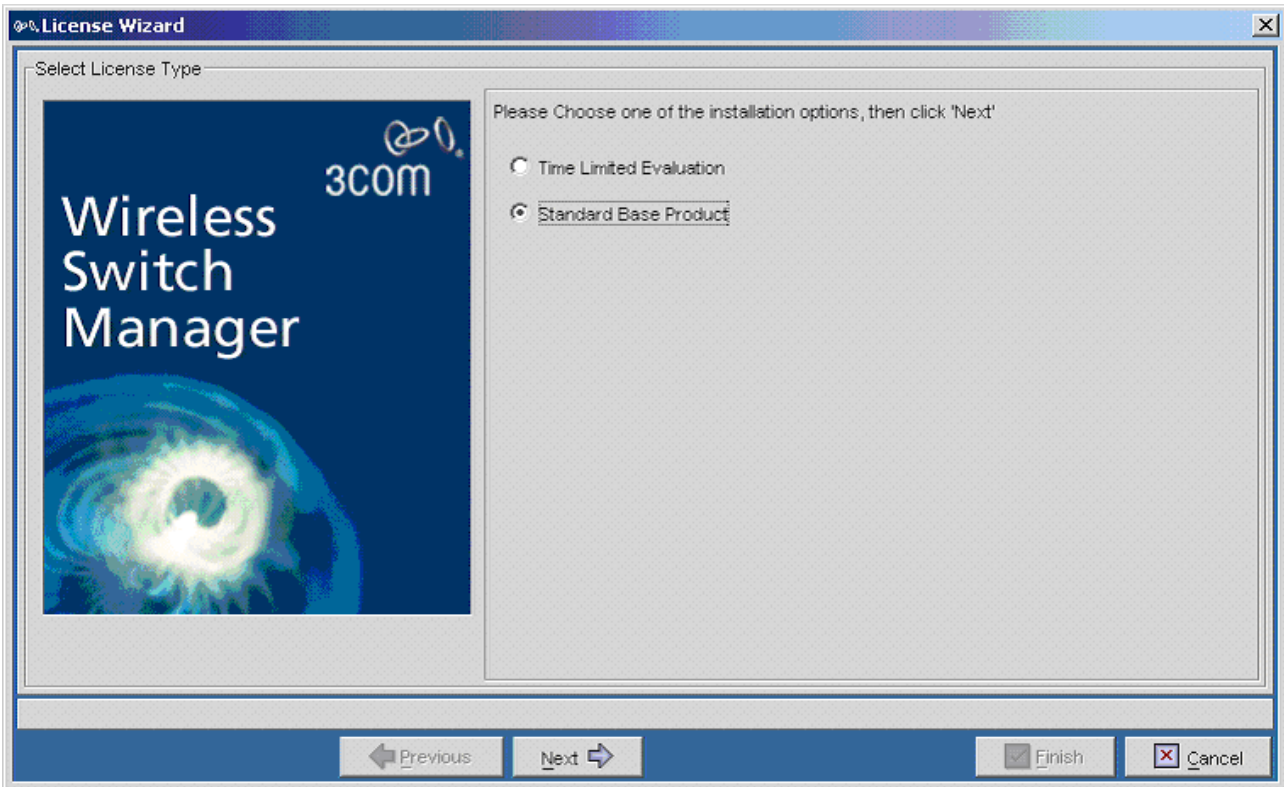


Ilustración 18: Selección del tipo de licencia. En nuestro caso no tenemos limitaciones

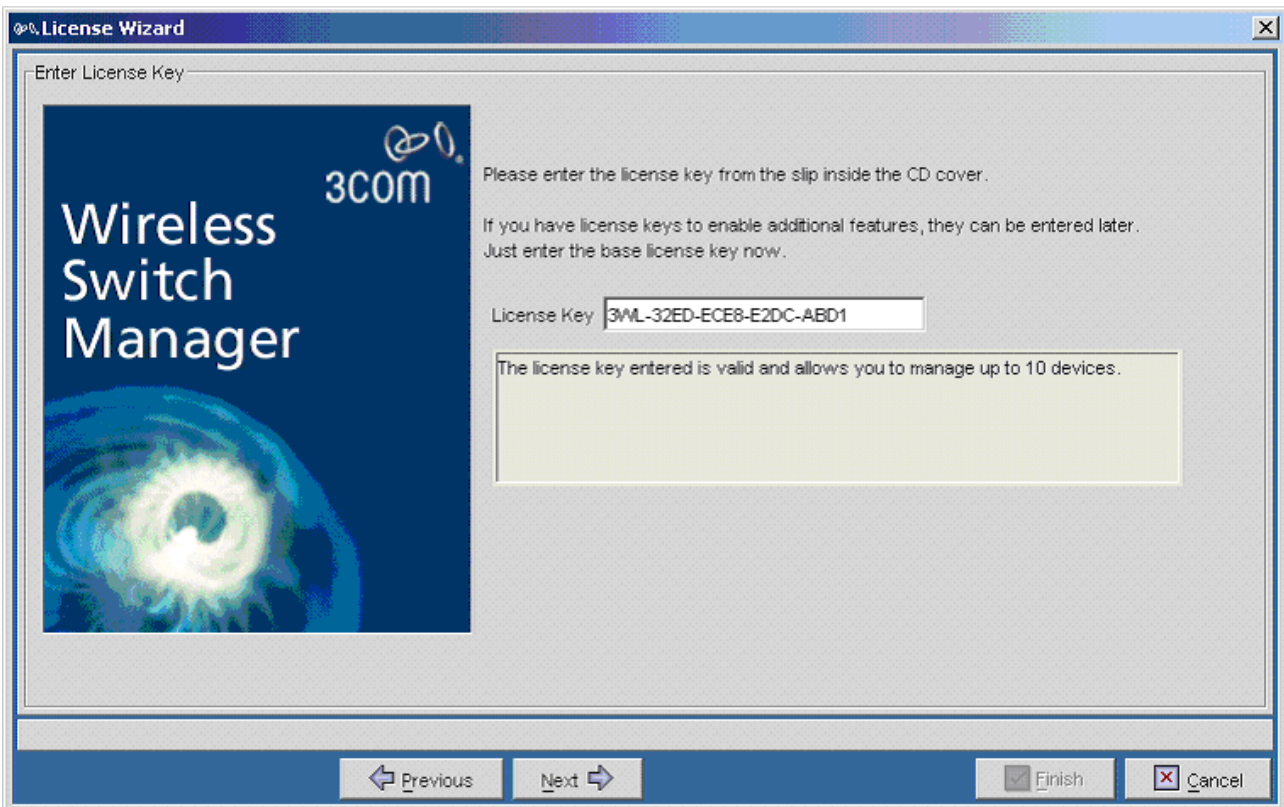


Ilustración 19: Introducción de la licencia que viene en el CD

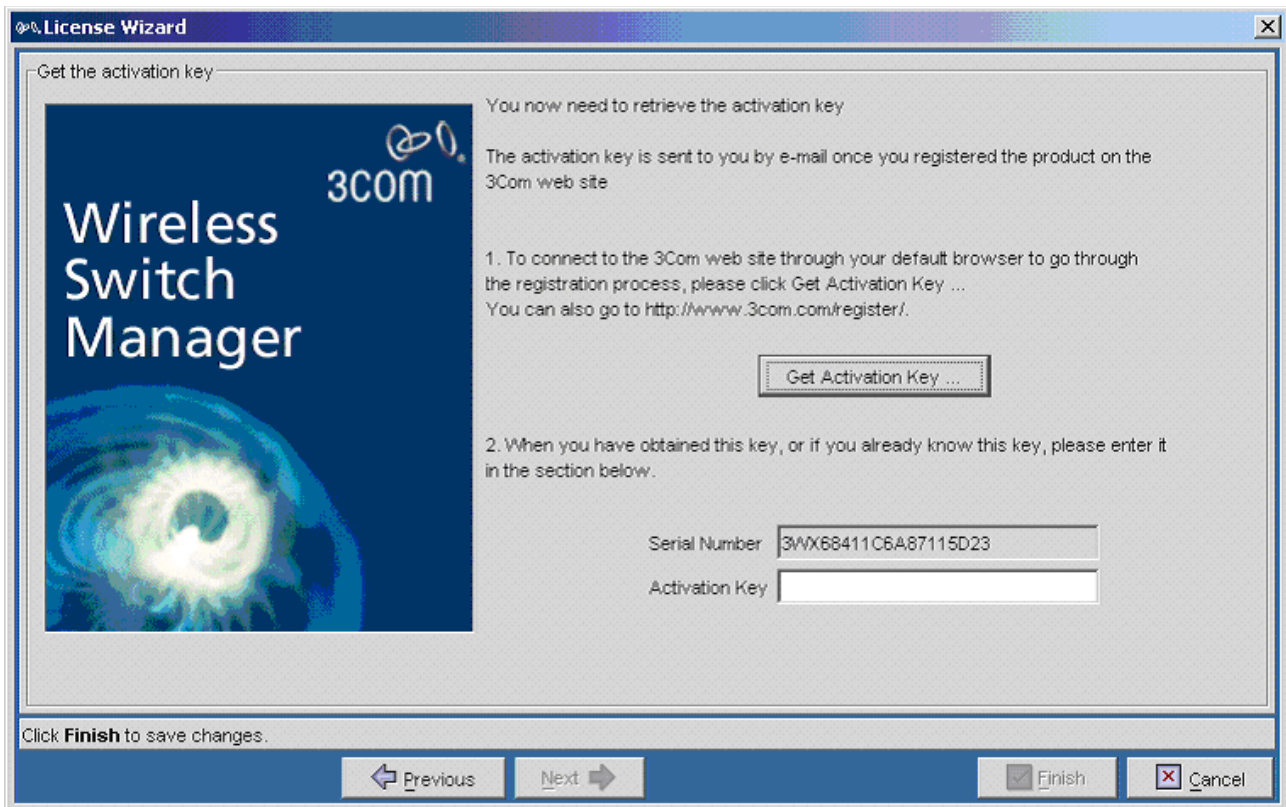


Ilustración 20: Proceso de activación del software

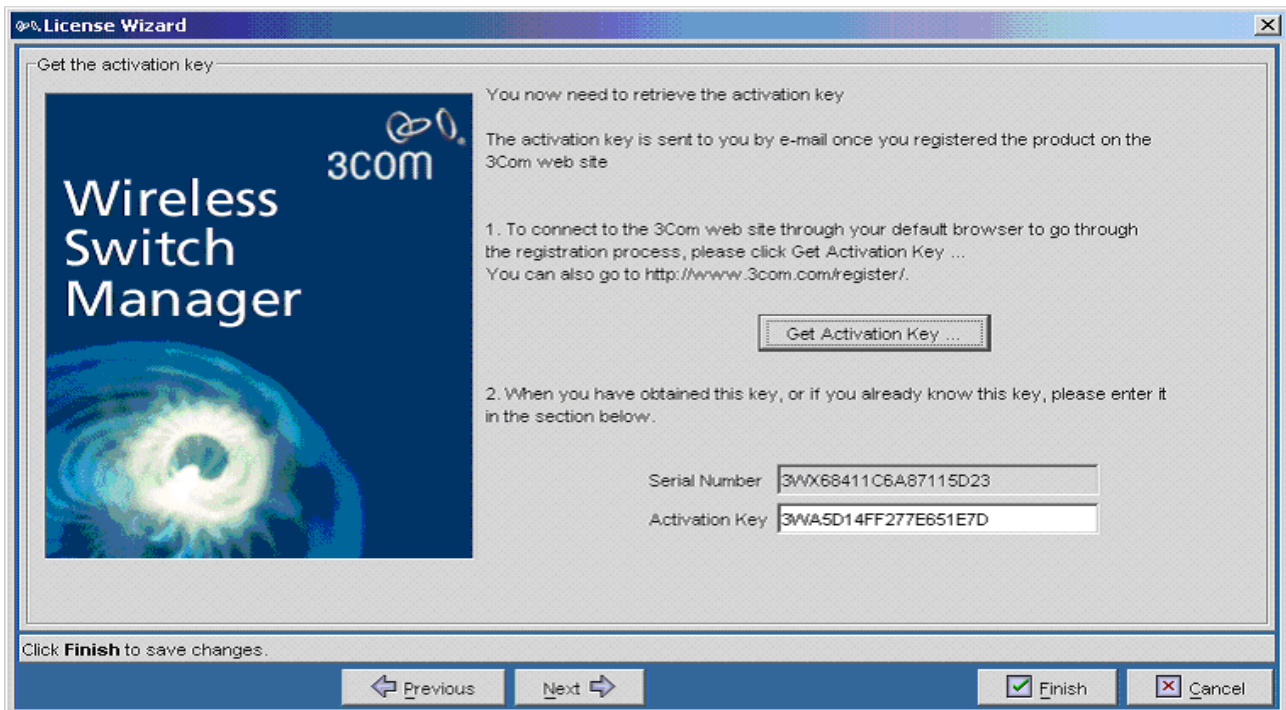


Ilustración 21: Introducción de la clave de activación del producto

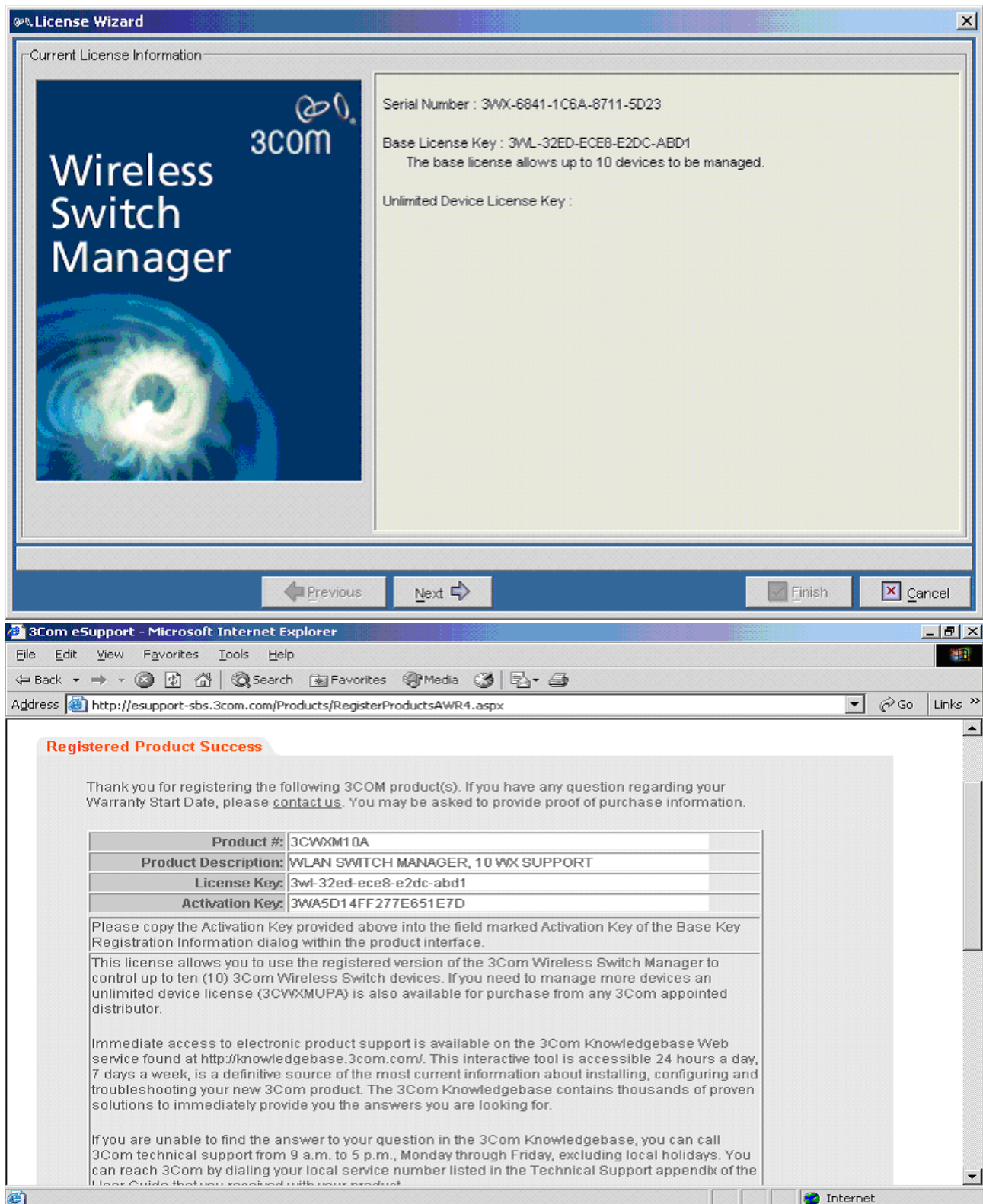


Ilustración 24: Proceso de solicitud de la clave de activación I

Ilustración 22: Introducción de la clave de la licencia de ampliación de puntos de acceso

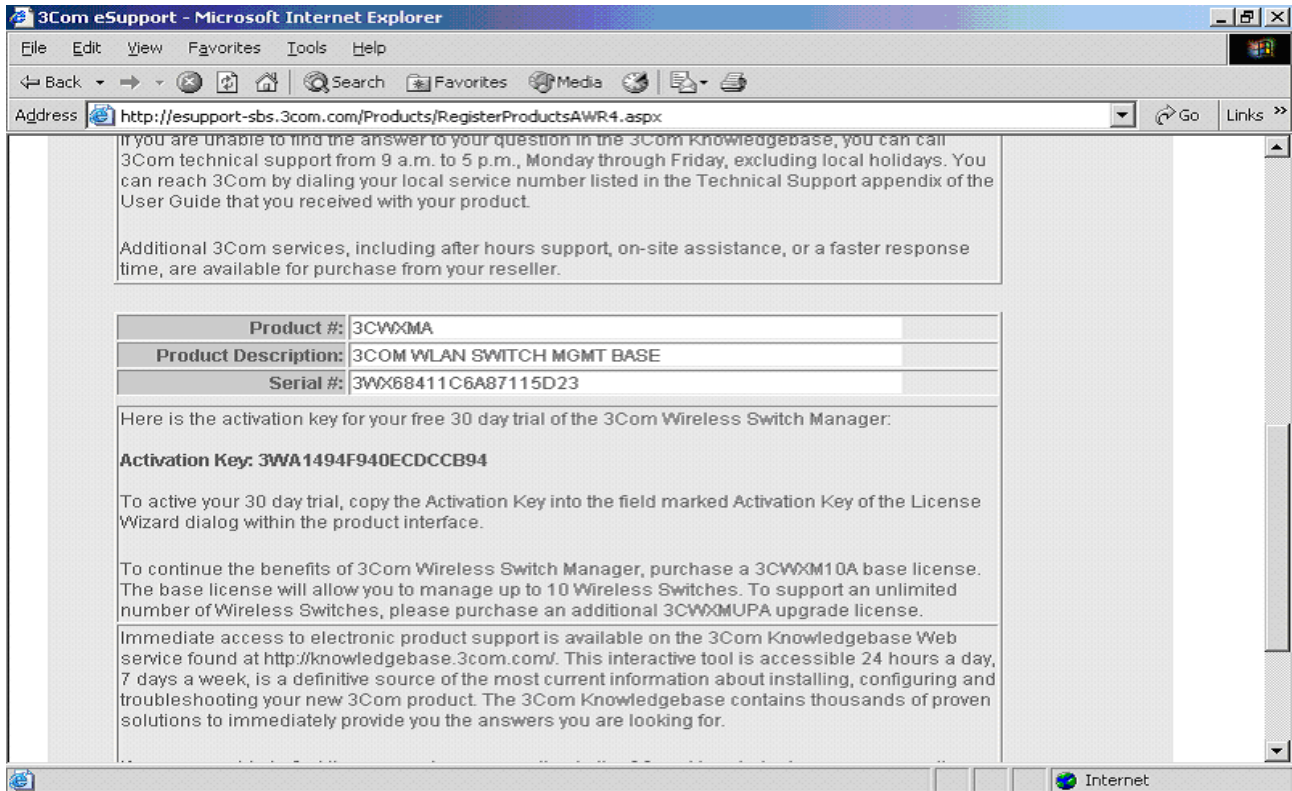


Ilustración 25: Proceso de solicitud de la clave de activación II

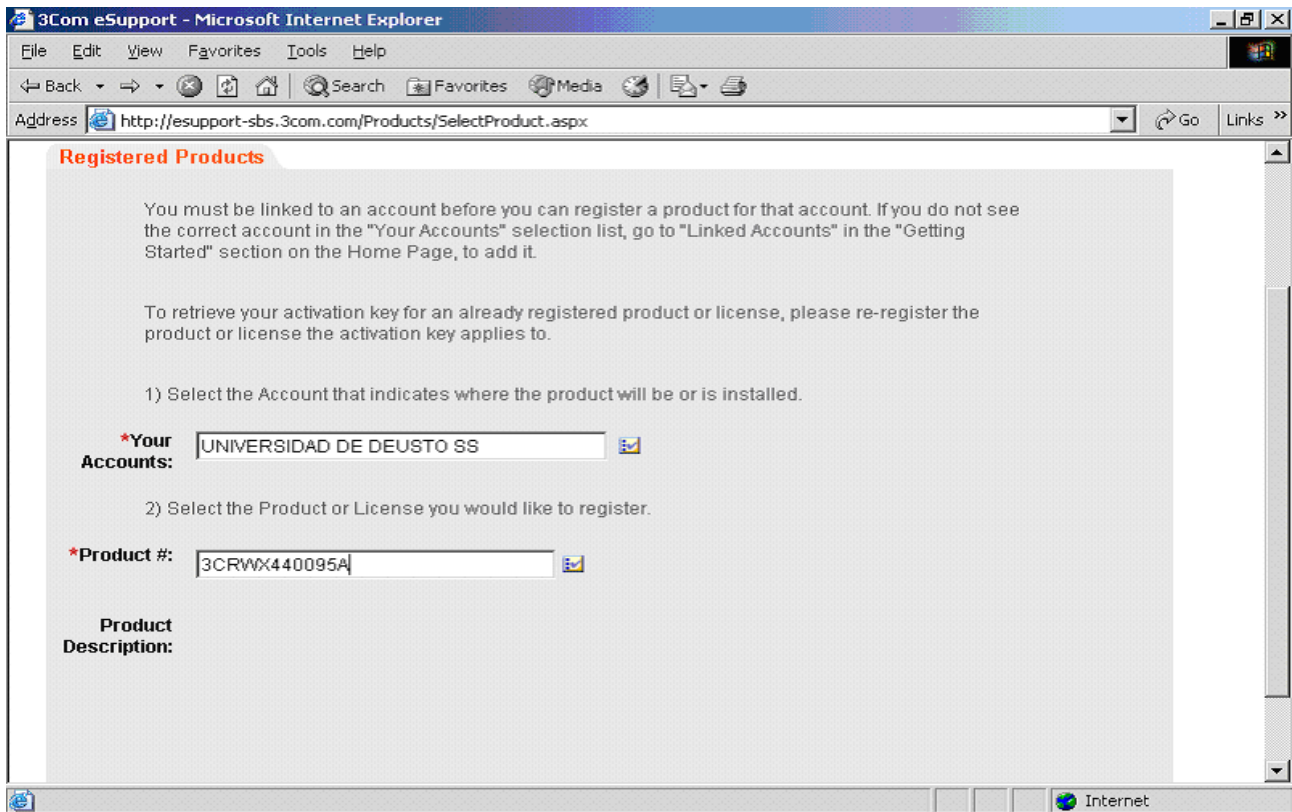


Ilustración 26: Proceso de solicitud de la clave de activación IV

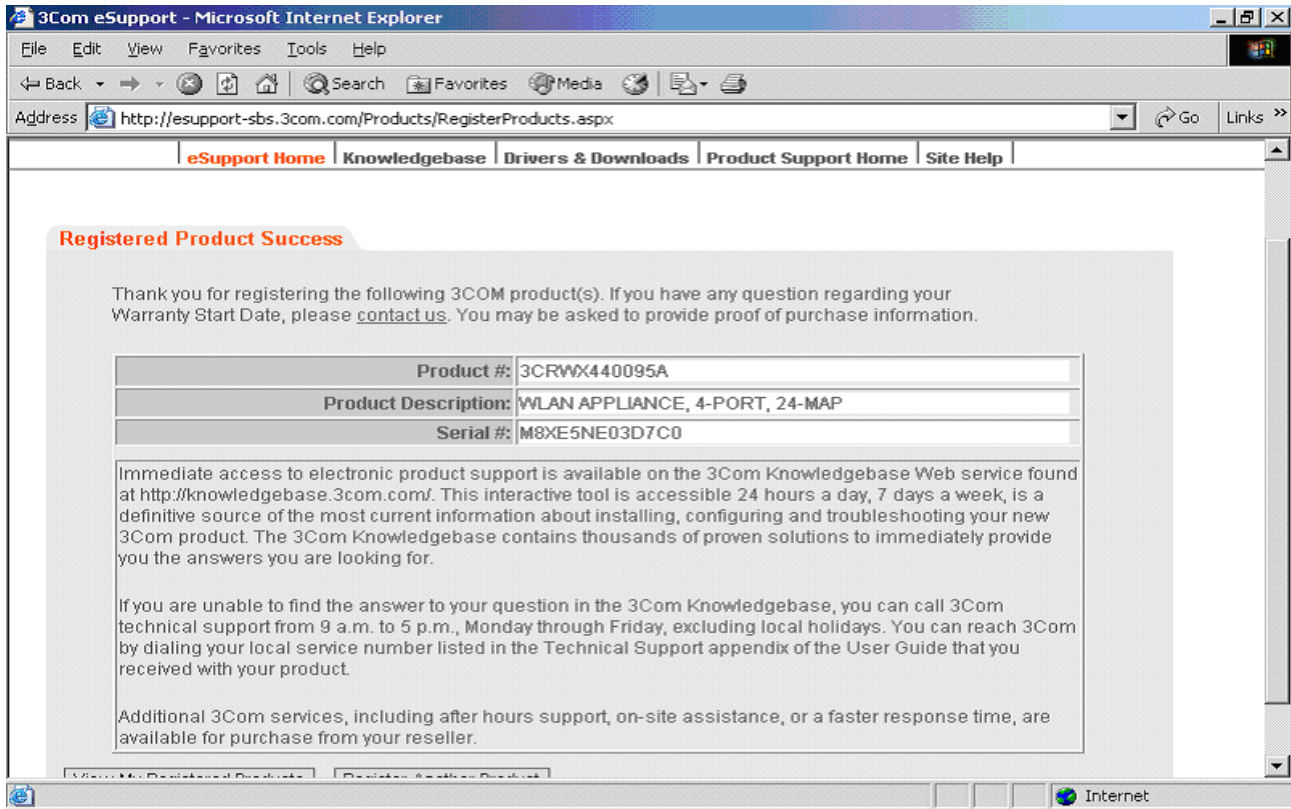


Ilustración 27: Proceso de solicitud de la clave de activación V

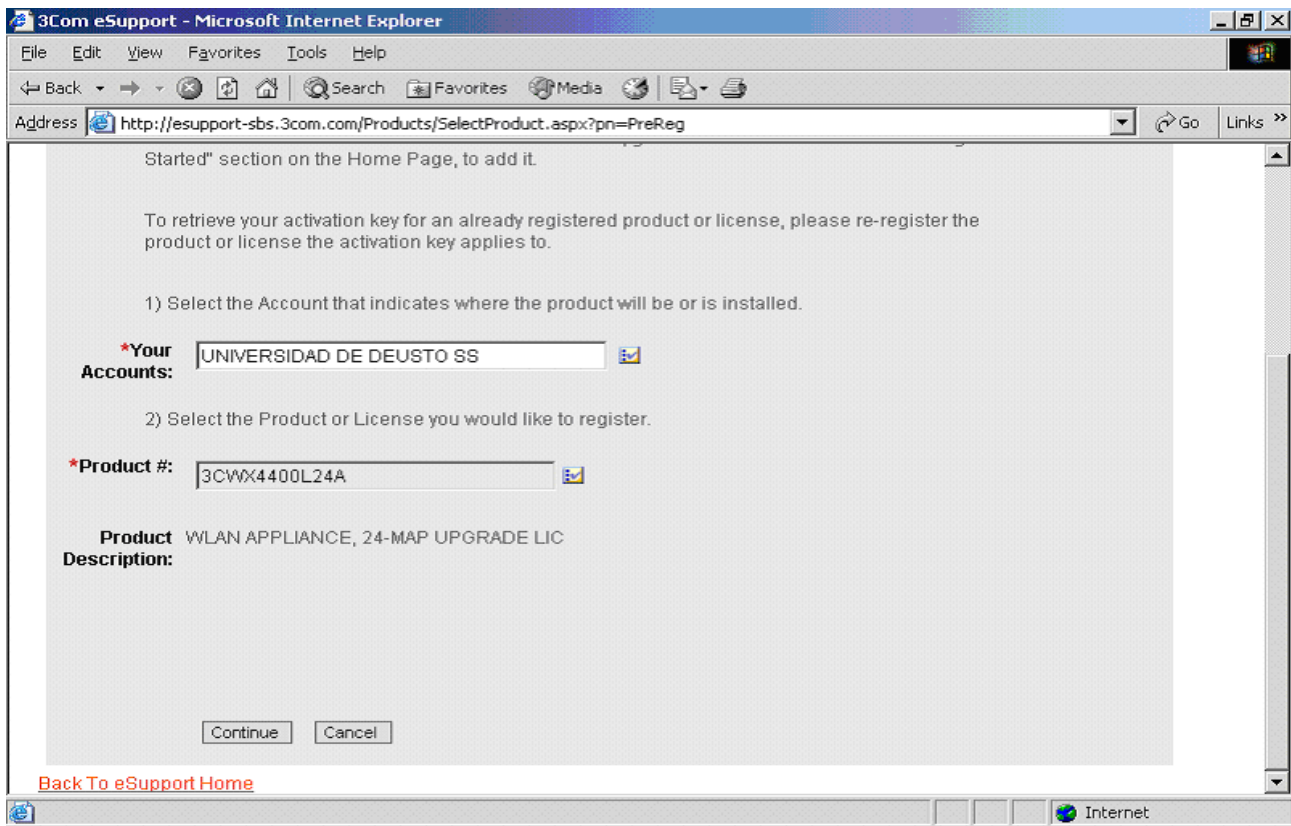


Ilustración 28: Proceso de solicitud de la clave de activación VI

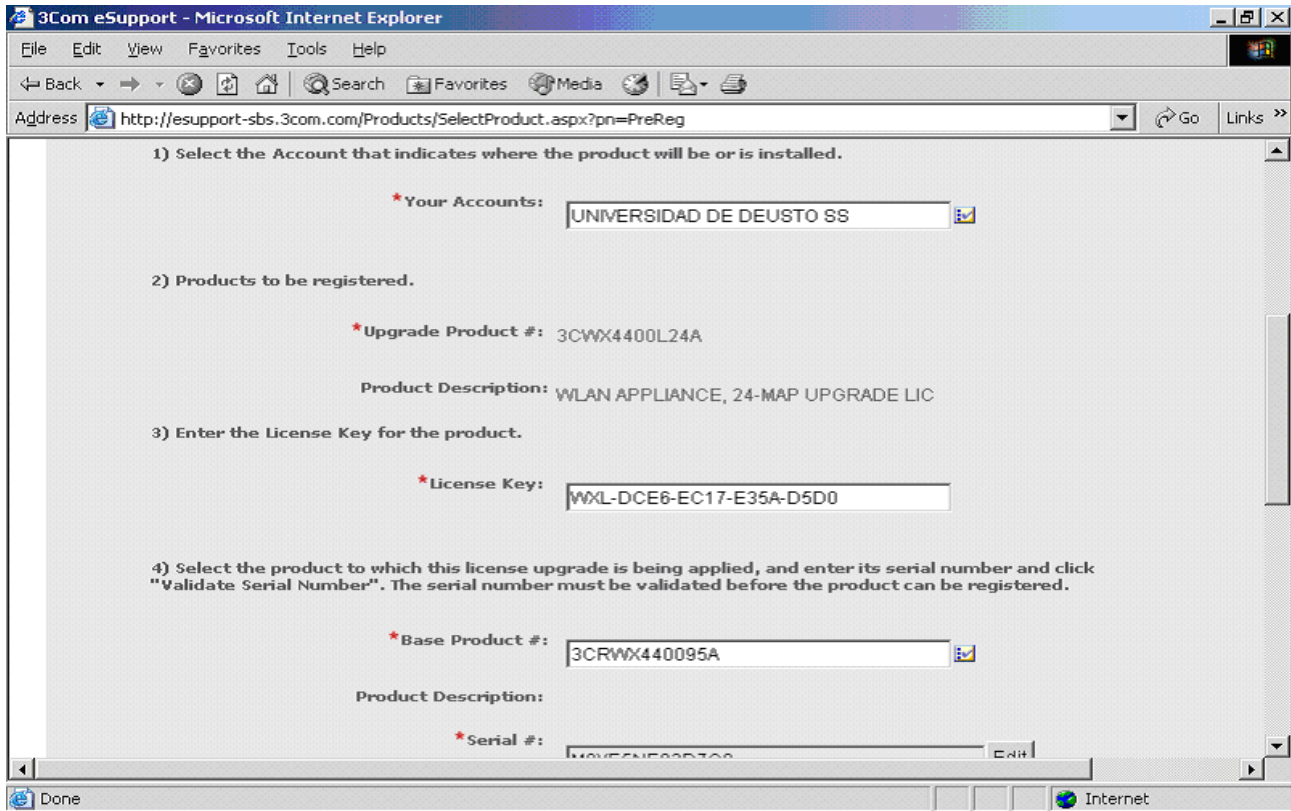


Ilustración 29: Proceso de solicitud de la clave de activación VII

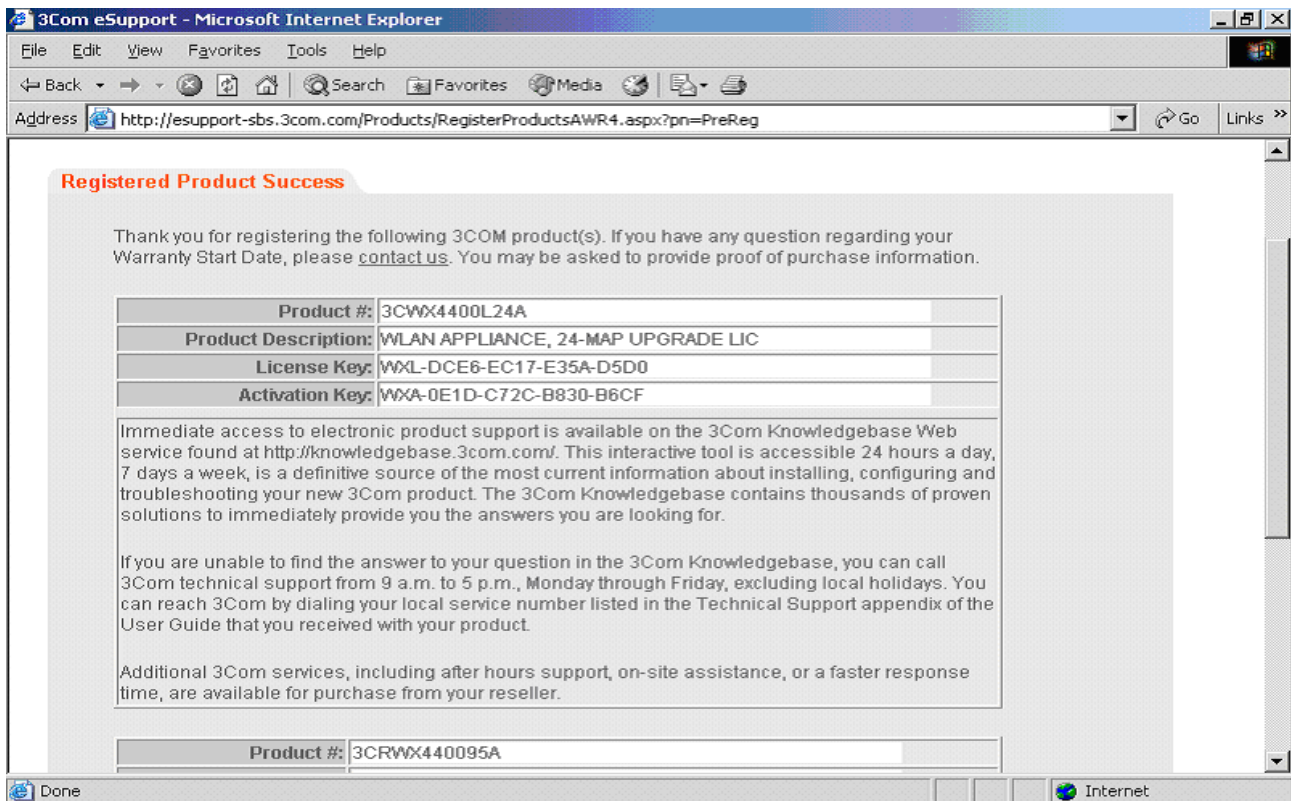


Ilustración 30: Proceso de solicitud de la clave de activación VIII

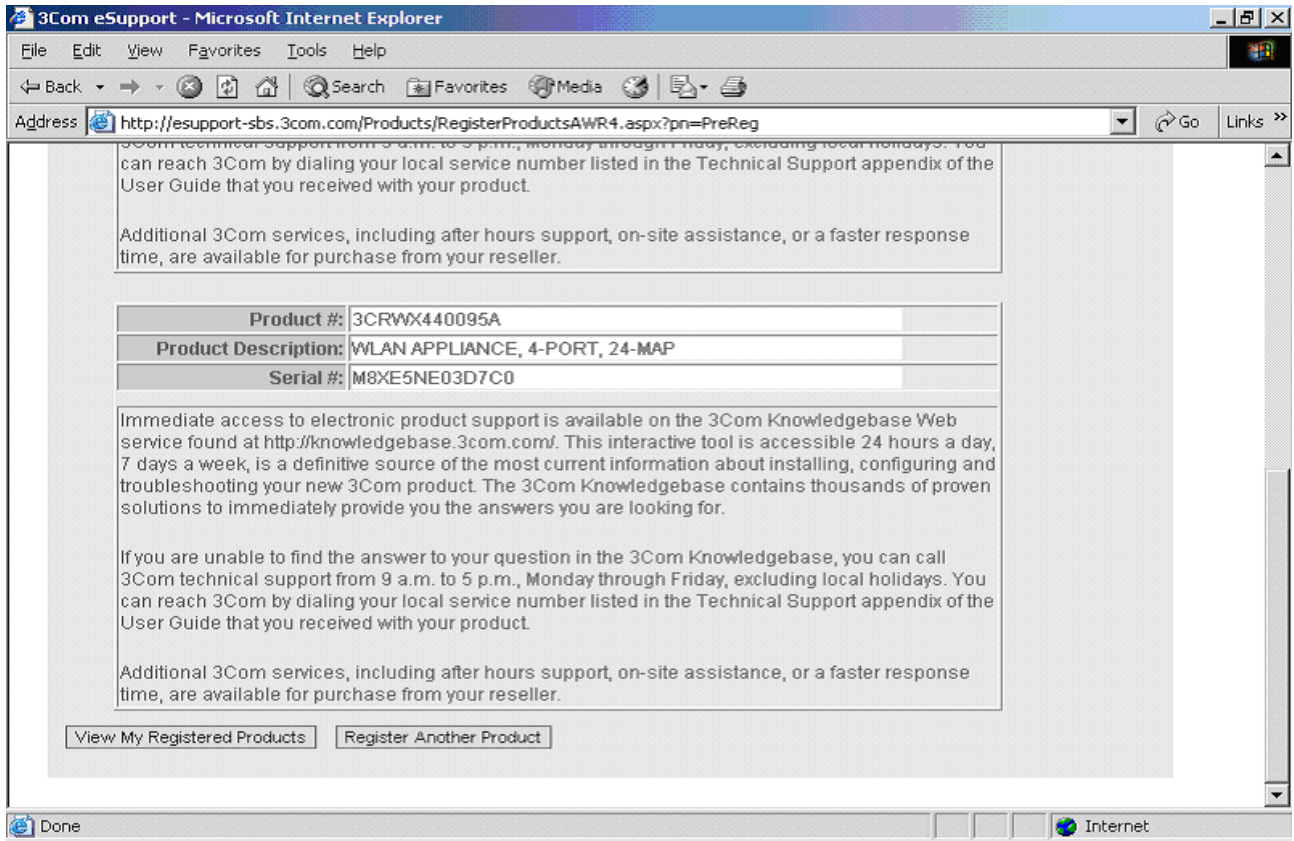


Ilustración 31: Proceso de solicitud de la clave de activación IX

8. Instalación de un punto de acceso de pruebas

En este proceso vamos a configurar el primer punto de acceso, para comprobar que el equipamiento funciona correctamente. Para la configuración de una antena hay que seguir dos pasos previos. Estos pasos servirán para la instalación del resto de antenas:

- Configuración de un perfil de radio (Radio profile): Aquí guardaremos los diferentes aspectos físicos de la radio frecuencia, los atributos 802.11. Mostramos las pantallas de configuración del perfil de radio.

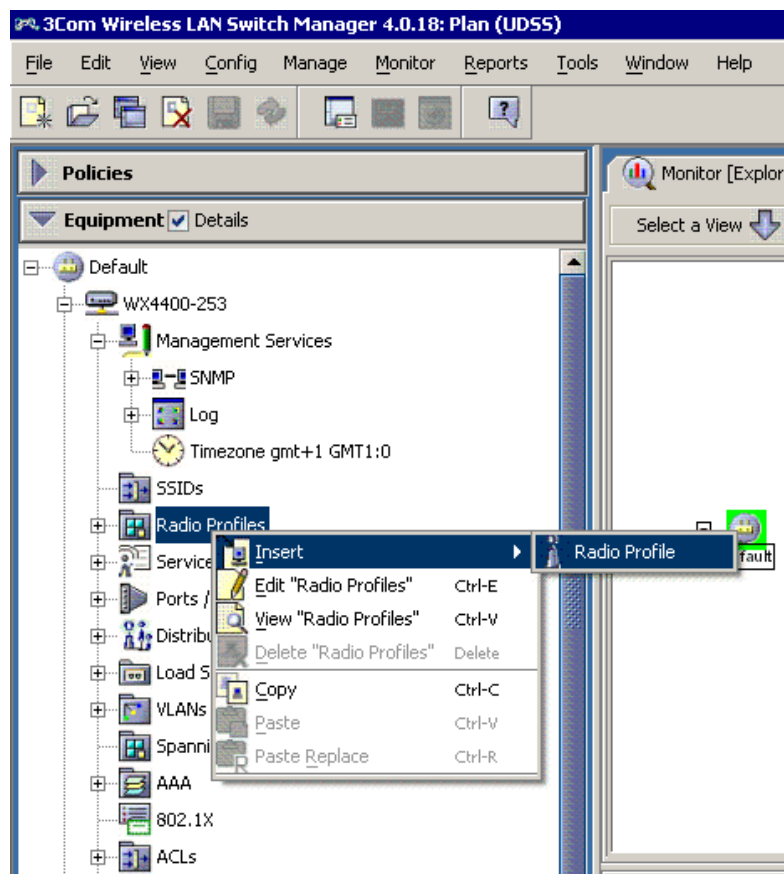


Ilustración 32: Insertar perfil de radio

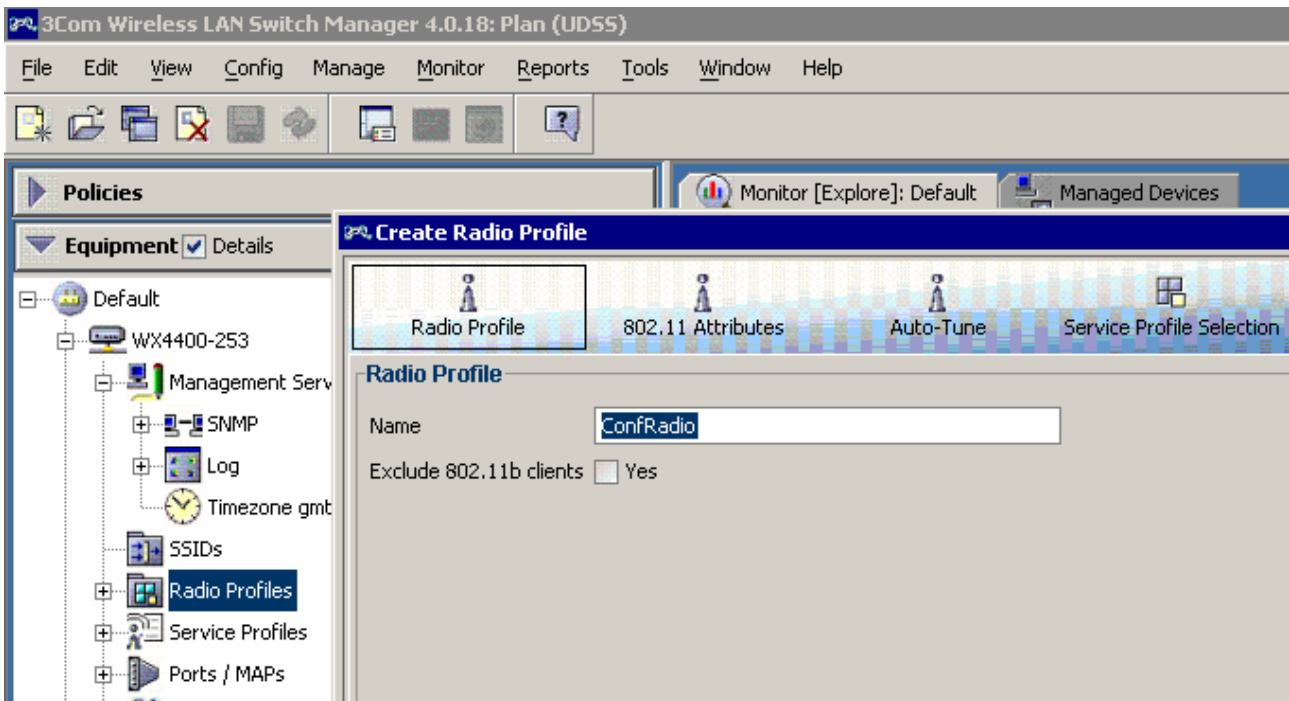


Ilustración 33: Nombre para el perfil de radio

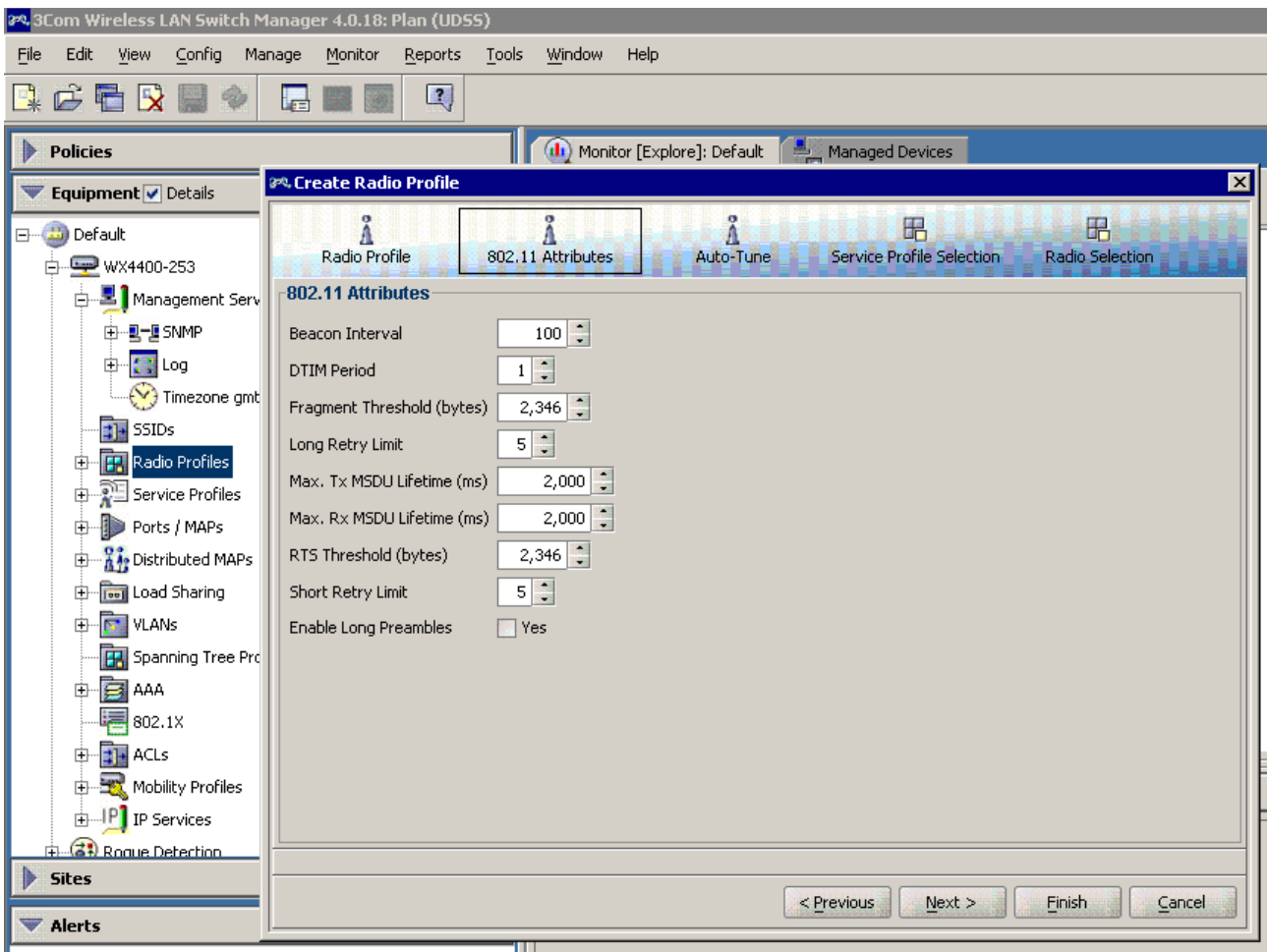


Ilustración 34: Atributos 802.11

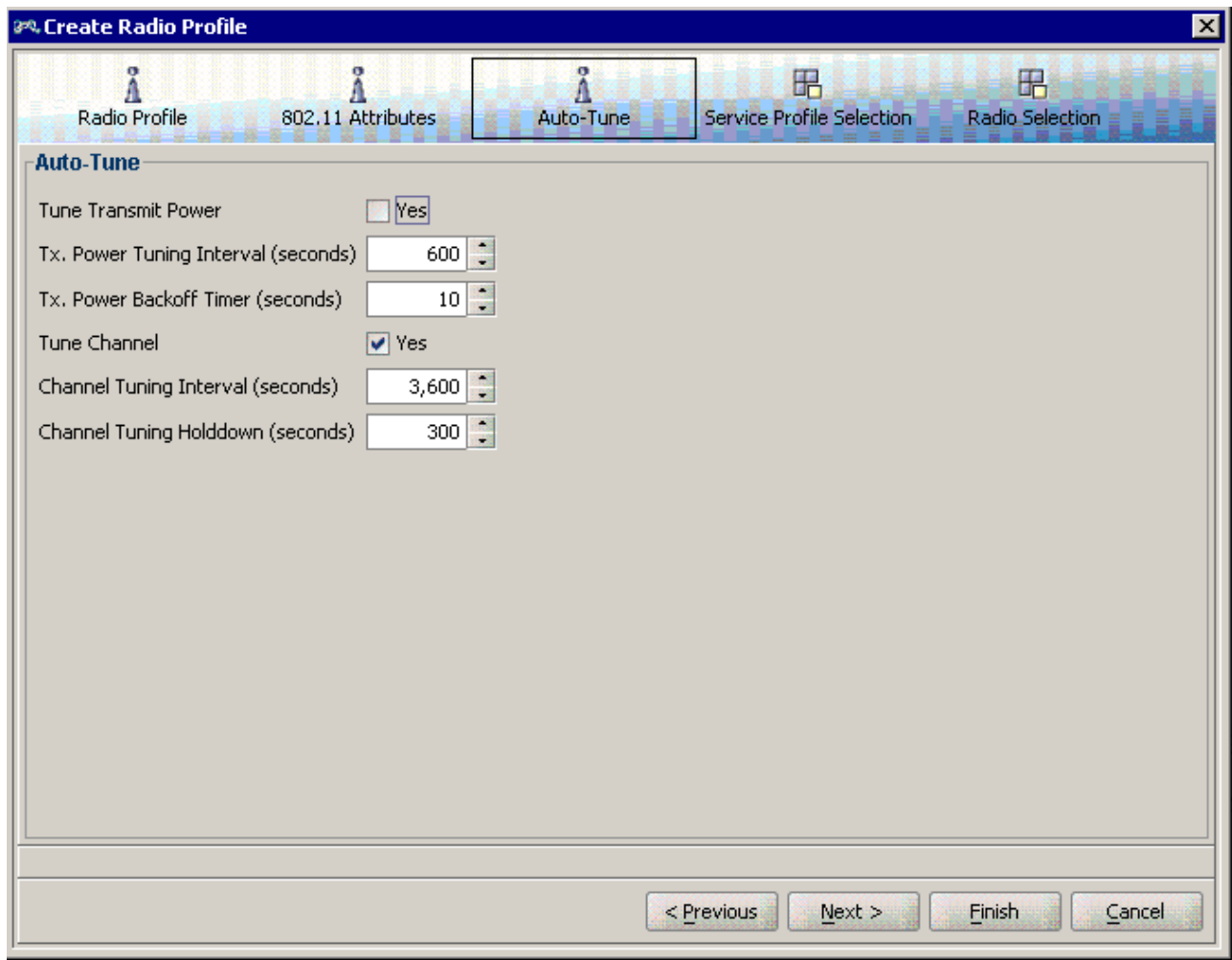


Ilustración 35: Selección de configuración automática de potencia de radio y canal de transmisión

- Configuración del perfil de encriptación (Service Profile): Desde el Servicio Informático del campus hemos defendido la libertad de conexión al protocolo HTTP dentro de su recinto, ya que consideramos este servicio como una divulgación del conocimiento. Es por esto que no hemos querido nunca poner impedimentos a este tipo de conexiones por lo que no usamos ningún tipo de seguridad en la conexión. En este apartado configuraremos una encriptación abierta. Para poder realizarlo , el wireless switch crea un usuario llamado *last-resort* que es la forma de identificarse automáticamente (como si de un usuario anónimo se trata). Además este perfil debe de tener asociado un perfil de radio y un SSID. El perfil de radio debe estar creado antes, no así el SSID que de

no estar creado lo crea automáticamente. Mostramos capturas de la configuración.

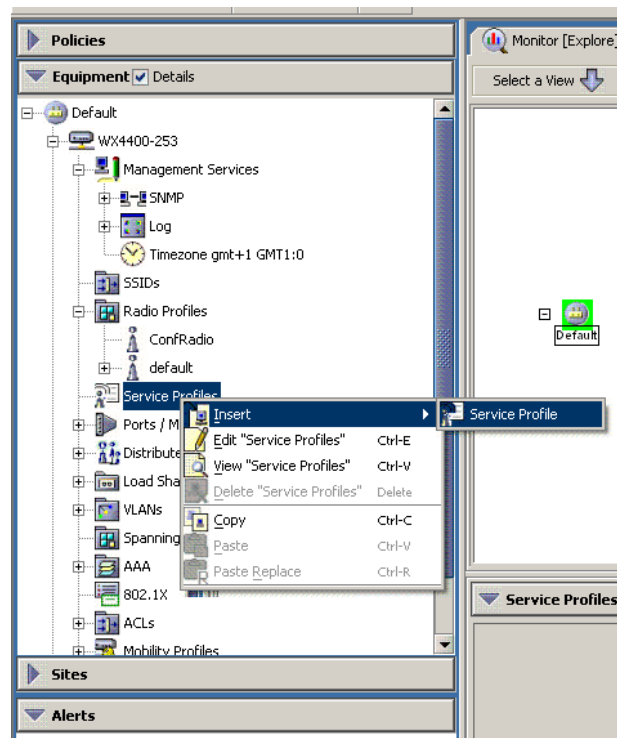


Ilustración 36: Insertar Service Profile

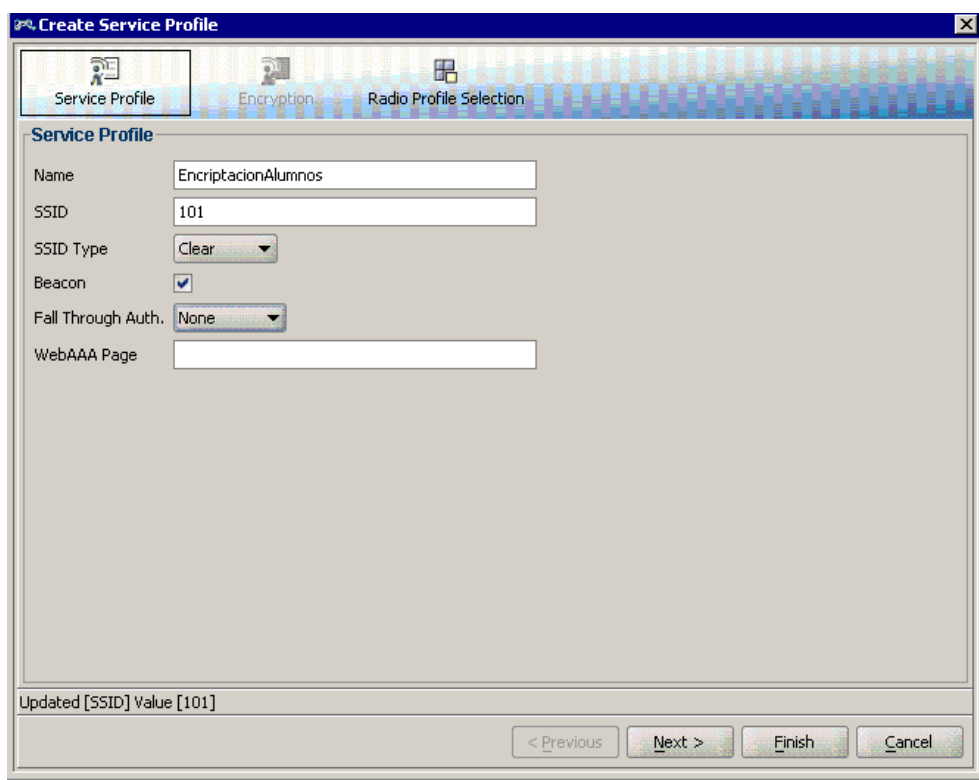


Ilustración 37: Nombre del Perfil, SSID asociado y tipo de seguridad

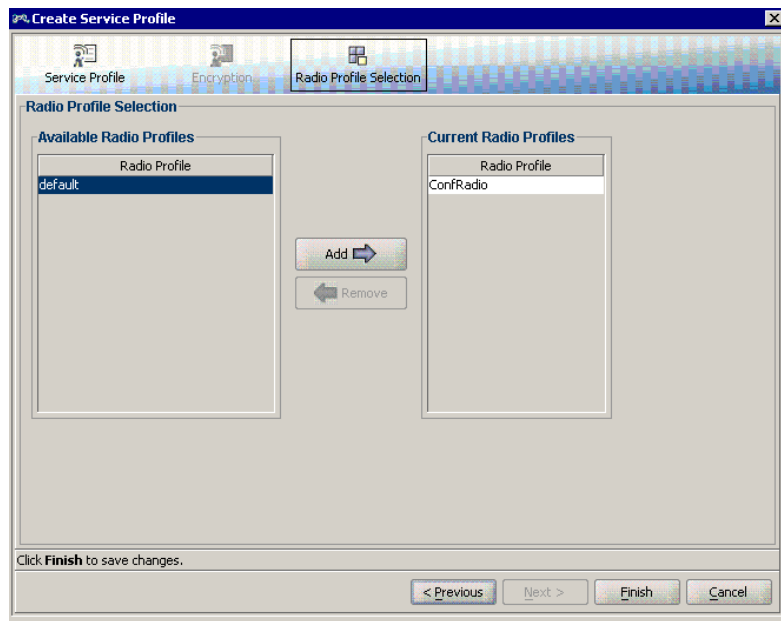


Ilustración 38: Asociación de perfil de radio

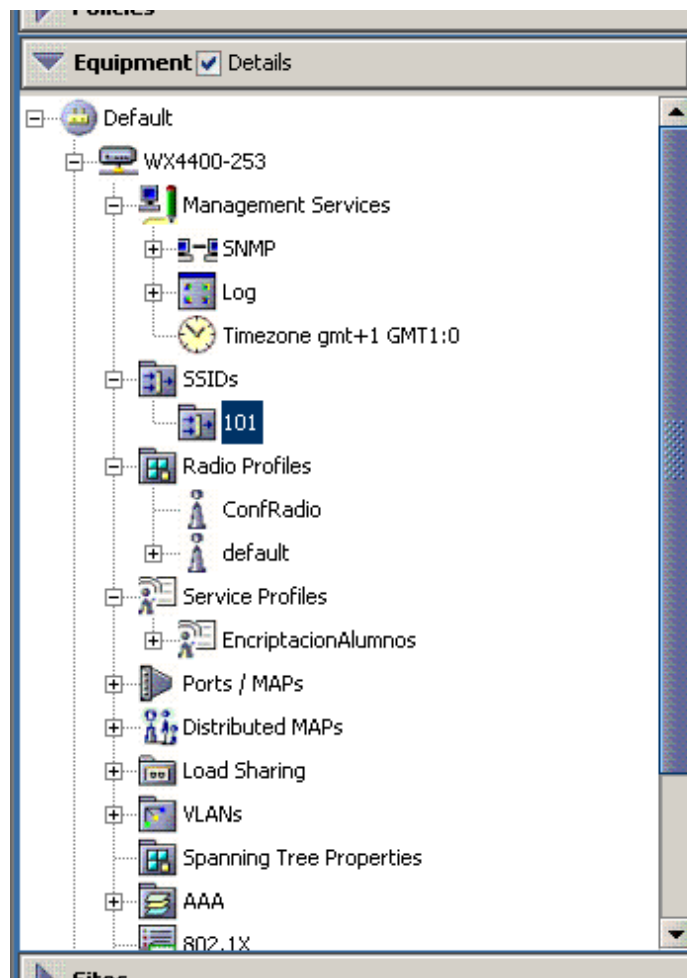
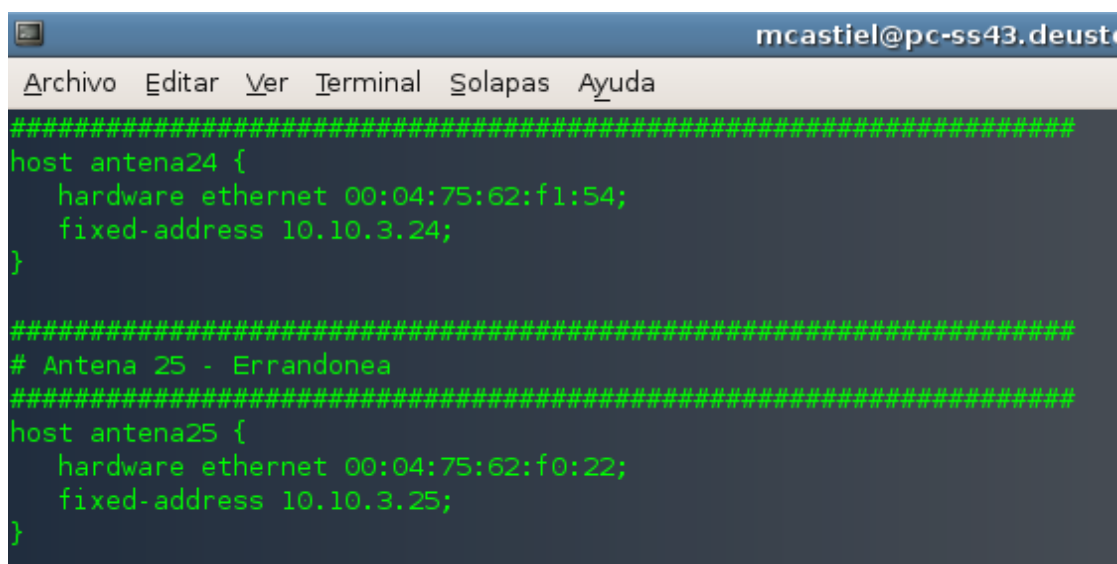


Ilustración 39: Creación automática del SSID

Una vez que tenemos el perfil de radio y el perfil de encriptación, ya podemos configurar nuestro primer punto de acceso. En nuestro caso lo primero que debemos hacer es cambiar el firmware de punto de acceso, ya que en la actualidad tenemos las antenas gestionadas individualmente. Con esto conseguimos que la antena se vuelva gestionable desde el switch. Para cambiar el firmware del punto de acceso nos conectaremos con un navegador a su dirección IP y entraremos en la opción de cambio de firmware.

Una vez cambiada la versión, en el servidor DHCP hemos configurado una entrada para asignar una dirección IP a la dirección MAC de la antena. Al reiniciar la antena coge esta dirección IP.

A screenshot of a terminal window with a blue title bar containing the text 'mcastiel@pc-ss43.deust'. The terminal has a menu bar with 'Archivo', 'Editar', 'Ver', 'Terminal', 'Solapas', and 'Ayuda'. The main content shows DHCP configuration for two hosts. The first host is 'antena24' with hardware ethernet '00:04:75:62:f1:54' and fixed-address '10.10.3.24'. The second host is 'antena25' with hardware ethernet '00:04:75:62:f0:22' and fixed-address '10.10.3.25'. There is a comment '# Antena 25 - Errandonea' above the second host configuration. Green lines of asterisks separate the two configurations.

```
mcastiel@pc-ss43.deust
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#####
host antena24 {
    hardware ethernet 00:04:75:62:f1:54;
    fixed-address 10.10.3.24;
}
#####
# Antena 25 - Errandonea
#####
host antena25 {
    hardware ethernet 00:04:75:62:f0:22;
    fixed-address 10.10.3.25;
}
```

Ilustración 40: Configuración del Servidor DHCP para las puntos de acceso

Además intenta conectarse al wireless switch, momento que aprovecharemos para capturar el número de serie del punto de acceso. Este número será necesario a la hora de definir la antena en la configuración. Para capturar el número de serie nos conectamos por telnet al wireless switch, y ejecutaremos en la consola el comando *show dap unconfigured*. Aquí nos mostrará las antenas que están intentando conectarse y no pueden al no estar definidas, mostrándonos entre otros datos el número de serie.

```
C:\WINNT\system32\CMD.exe - telnet 192.168.5.253

Copyright (c) 2004, 2005, 2006 3Com Corporation. All rights reserved.

Username: admin
Password:

WX4400-253> ena

Enter password:

WX4400-253# show dap unconfigured

Unrecognized command: show dap unconfigured
WX4400-253# display dap unconfigured
Serial Id: 75vf349a1ee4d Model: ap8250 IP Address: 10.2.35.216
Port: 2 Ulan: vlan5
WX4400-253#
```

Ilustración 41: Captura del número de serie

Ahora debemos configurar el punto de acceso capturado en la configuración. Esto lo haremos en el apartado Distributed MAPs.

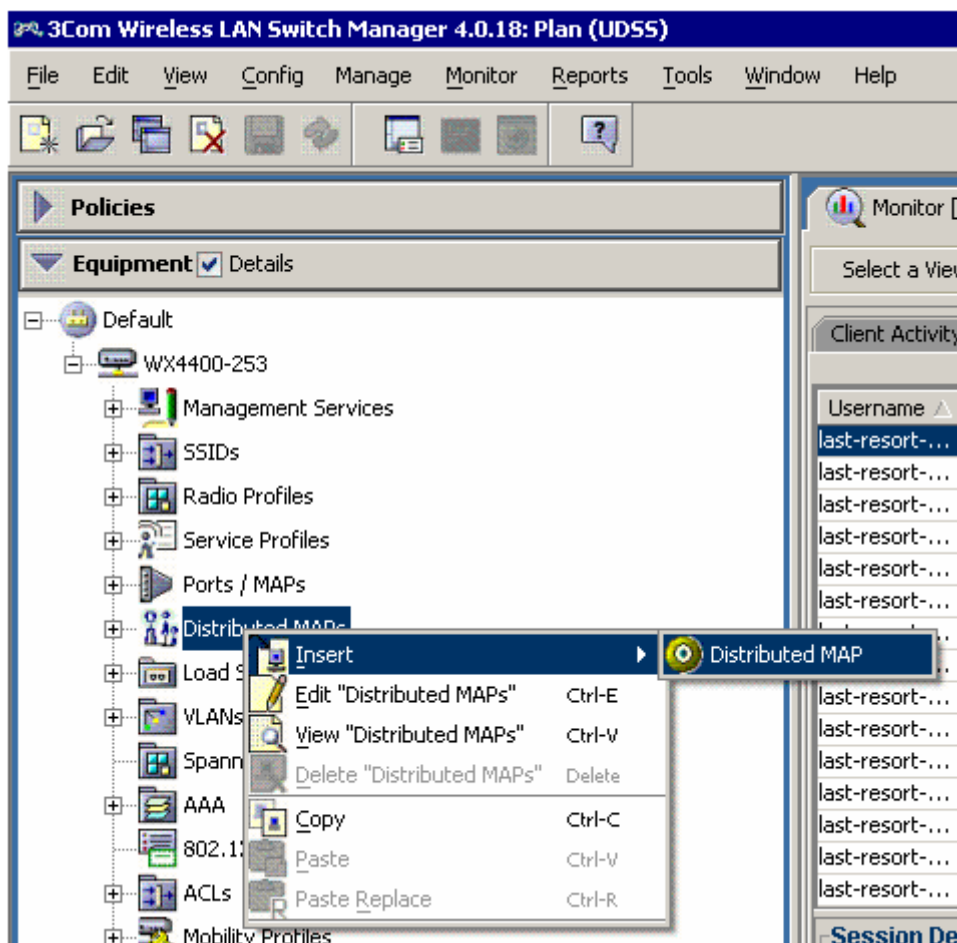


Ilustración 42: Inserción de un punto de acceso

Nos solicitará una serie de campos, como por ejemplo el número identificativo del MAP, el modelo, el tipo de radio y el número de serie antes citado.

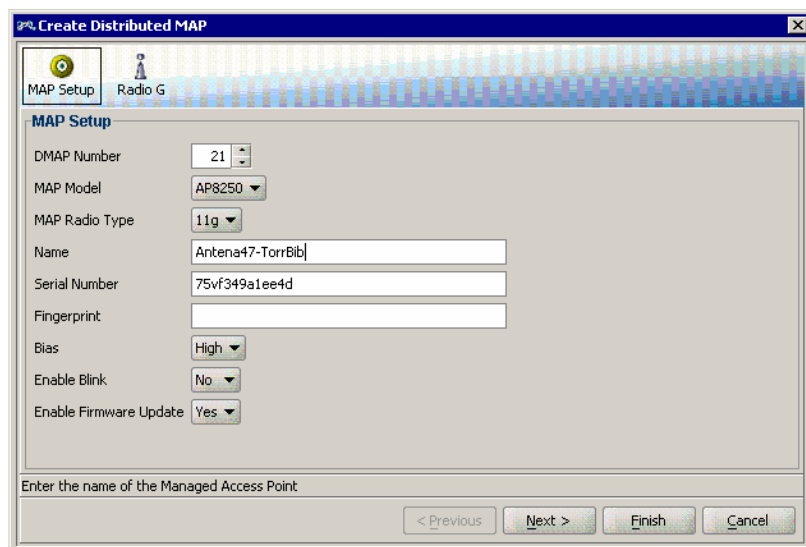


Ilustración 43: Definición de datos del punto de acceso

En la pestaña de configuración de radio, además de seleccionar el perfil de radio que hemos creado anteriormente, es importante que pinchemos en la opción de *Enabled*, ya que ésta aparece desmarcada, dejandola inutilizada para la conexión de los clientes.

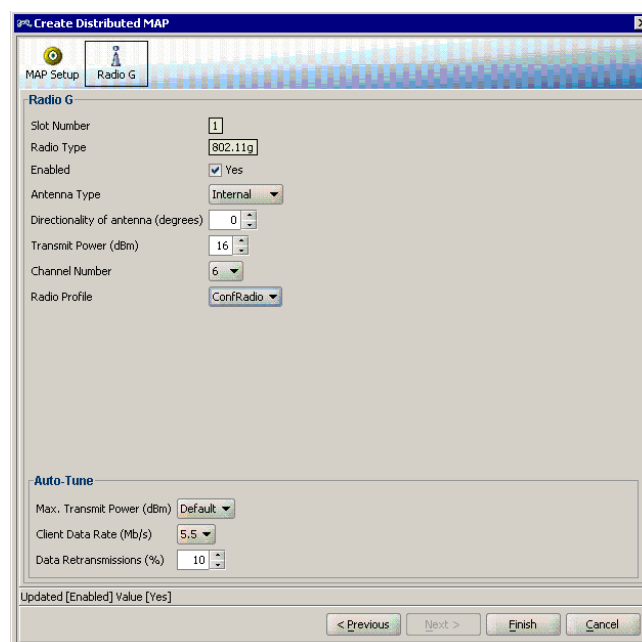


Ilustración 44: Definición de radio. Importante marcar en Enabled

Una vez definida, debemos instalar los cambios en el wireless switch, pinchando en el botón de *deploy* de la pestaña *Managed Devices*.

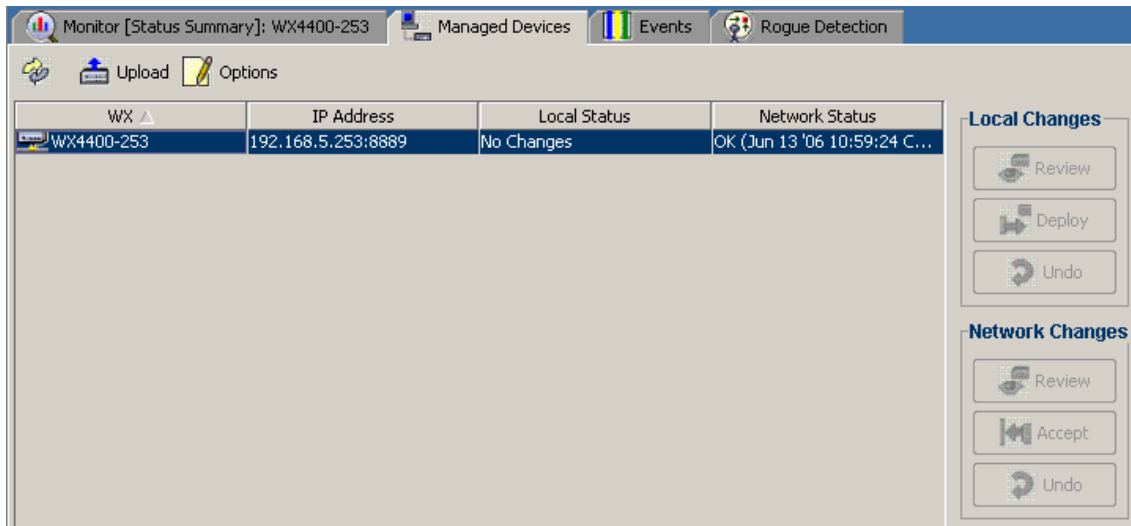


Ilustración 45: Aplicar cambios de configuración

9. Instalación de los puntos de acceso del campus

Una vez finalizadas las clases y un periodo de prueba del punto de acceso instalado, entre el martes 30 de mayo y martes 6 de junio de 2006 se procede a la instalación de los puntos de acceso. El proceso consiste en ir realizando los pasos anteriores sobre cada una de las antenas.

Desgraciadamente no se puede implementar la solución en todos los puntos de acceso, ya que algunas antenas no disponen de firmware adecuado. Se acuerda realizar en una segunda fase la sustitución de estos puntos de acceso, por unos nuevos gestionables, pero tenemos que esperar al curso siguiente para poder acometer el gasto.

Mostramos a continuación una captura con los puntos de acceso configurados.

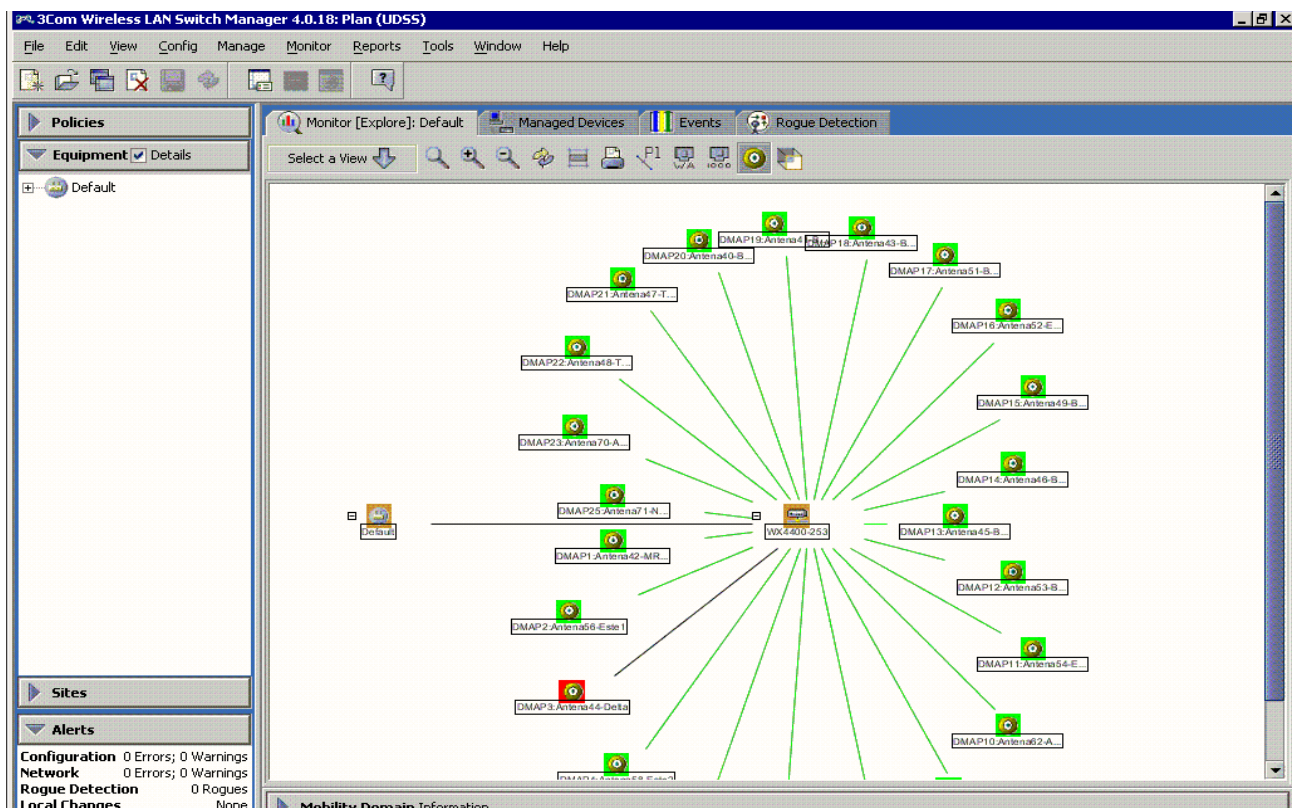


Ilustración 46: Configuración de todas las antenas

10. Certificado de satisfacción de la instalación

El 6 de junio de 2006 el Director del Servicio Informático de la Universidad de Deusto del Campus de San Sebastián certifica que la instalación se ha realizado satisfactoriamente.



Universidad de
Deusto
San Sebastián

Deustuko
Unibertsitatea
Donostia

Servicio
Informático

Informatika
Zerbitzua

Quien suscribe, Don Josué Mendivil Caldentey, Director del Servicio Informático de la Universidad de Deusto del campus de San Sebastián.

CERTIFICO QUE:

Don Miguel Castiella ha realizado satisfactoriamente la implantación del “switch wireless” para la gestión de las antenas inalámbricas en el campus que la Universidad de Deusto tiene en la ciudad de San Sebastián.

Y para que conste, expido la presente certificación en San Sebastián, a 6 de junio de 2006

Fdo. Josué Mendivil Caldentey



11. Vista aérea del Campus



Ilustración 47: Vista aérea del Campus

- 1.- Edificio Padre Arrupe
- 2.- Edificio Biblioteca
- 3.- Torre de Biblioteca
- 4.- Centro NewCon
- 5.- Loiola Centrum
- 6.- Edificio Mateo Ricci
- 7.- Edificio Administración
- 8.- Edificio Padre Errandonea
- 9.- Torre de la ESTE

12. Glosario

Mostramos a continuación un listado de acrónimos que han aparecido a lo largo del trabajo, ordenados alfabéticamente:

<i>Acrónimo</i>	<i>Significado</i>
<i>AP</i>	Punto de acceso
<i>CNAF</i>	Cuadro Nacional de Atribución de Frecuencias
<i>CSMA/CA</i>	Carrier Sense Multiple Access / Collision Avoidance
<i>DFS</i>	Selección de frecuencia dinámica
<i>DFS</i>	Selección dinámica de frecuencia
<i>DSSS</i>	Espectro ensanchado de secuencia directa
<i>FHSS</i>	Espectro distribuido con saltos de frecuencia
<i>IEEE</i>	Instituto de Ingenieros Eléctricos y Electrónicos.
<i>MAC</i>	Media Access control
<i>MACA</i>	Multiple Access with Collision Avoidance
<i>OFDM</i>	Multiplexado división de frecuencia ortogonal
<i>OSI</i>	Open Systems Interconnection
<i>PIRE</i>	Potencia isótropa radiada equivalente
<i>QoS</i>	Calidad de servicio
<i>TCP</i>	Transport control protocol
<i>WEP</i>	Wired equivalent privacy
<i>WIFI</i>	Wireless fidelity
<i>WLAN</i>	Red de área local inalámbrica

13. Bibliografía

"Redes wireless 802.11" Matthew S. Gast. 2005. Anaya multimedia.

"Wireless Lan (WIFI) Tutorial". <http://www.tutorial-reports.com>

"IEEE Wireless Lan 802.11". <http://standards.ieee.org>

"Wireless LAN Mobility System. Wireless LAN Switch and Controller Command Reference". <http://3com.com>

"Real Decreto 1066/2001". <http://www.boe.es>

"orden CTE/23/2002" <http://www.boe.es>

También se ha usado frecuentemente la página web de la wikipedia,
<http://www.wikipedia.org>

Anexo 1



Universidad de Deusto
Deusto Unibertsitatea

.

SERVICIO INFORMATICO INFORMATIKA
ZERBITZUA

PROYECTO UD-WIFI

AUTOR:	Servicio Informático de la UD
ASUNTO:	Ampliación de la cobertura WIFI en el Campus de San Sebastián de la UD
Fecha	16-01-2006



INDICE

<u>Descripción del proyecto.....</u>	<u>3</u>
<u>Alcance.....</u>	<u>3</u>
<u>Requisitos técnicos.....</u>	<u>4</u>
<u>Requisitos formales.....</u>	<u>6</u>



1

Descripción del proyecto

La **Universidad de Deusto** pretende con este proyecto gestionar centralizadamente el número de espacios con cobertura WIFI correspondientes a ubicaciones concretas y localizadas en su Campus de San Sebastián. Para ello se va a acoger al programa “Acceso a Internet y movilidad con WI-FI” promovido por la SPRI (Sociedad para la Promoción y Reconversión Industrial), que ofrece subvenciones para la instalación de redes inalámbricas con tecnología WIFI ubicadas dentro de la CAPV.

Para poder recibir las ayudas que se contemplan en el programa de la SPRI, las instalaciones a dotar de cobertura WIFI deberán cumplir los siguientes requisitos:

1. La red inalámbrica WIFI desplegada debe permitir la conectividad a Internet de las personas que estén en tránsito por las instalaciones de la Universidad.
2. La Universidad debe garantizar la conectividad de los usuarios en condiciones de velocidad de banda ancha y de forma gratuita durante al menos un año a partir de la fecha de puesta en marcha de la instalación.

2

Alcance

El Servicio Informático de la Universidad de Deusto en colaboración con el Vicerrectorado de Innovación ha identificado un total de 39 dispositivos en los que existe cobertura WIFI.

Actualmente disponen de cobertura WIFI con puntos de acceso 3Com. En caso de ser necesario serán sustituidos su equipamiento actual por el nuevo, facilitando así su gestión.



3

Requisitos técnicos

El equipamiento wireless propuesto deberá cumplir los siguientes requisitos:

REQUISITOS BASICOS

- Los Puntos de Acceso deben de ser compatibles con los estándares **802.11b y 802.11g**, y a nivel de seguridad seguirán el estándar **WPA** y se valorará que en un futuro puedan cumplir con el estándar **WPA 2 vs. 802.11i**. Además deberán ser **actualizables** en firmware a nuevas versiones.
- Se hará especial hincapié en la capacidad de gestión del equipamiento Wi-fi, ya que se trata de **39 o más puntos de Acceso** y por tanto se quiere una plataforma de gestión centralizada para todos ellos.
- Se quiere que esta solución sea **ampliable y escalable**, que permita añadir nuevos AP's en el futuro sin necesidad de controlar las frecuencias de trabajo de cada uno de los AP's, sino que la plataforma de gestión se encargue de decirle a cada AP en qué frecuencia debe trabajar.
- Deberá ser **tolerante a fallos**, en el sentido de que ante el fallo de un AP, los AP's vecinos deberán tratar de suplir ese fallo ampliando su radio de acción, y la plataforma de gestión deberá avisar de dicho fallo mediante correo electrónico o cualquier otro medio.
- El equipamiento de gestión deberá **permitir 802.1x** para las conexiones wireless y así poder autenticar a los clientes **preferiblemente contra un LDAP**, aunque también se admite el hecho de usar un RADIUS como pasarela intermedia. Se valorará especialmente poder autenticar directamente contra el Active Directory de Microsoft.
- Este equipamiento de gestión también deberá permitir la ubicación de los diferentes **clientes wireless en diferentes VLAN's** para poder gestionar y separar mejor el tráfico de red que genera cada uno, o permitir separar diferentes perfiles de usuario en diferentes redes.
- Los AP's deberán permitir alimentación a través del cable de red con el fin de que la acometida eléctrica se realice a través de inyector (PoE-Power over ethernet).

Hay que tener en cuenta que los AP pueden estar distribuidos por los armarios de red de la universidad y el equipo de gestión deberá de estar en las instalaciones del CPD.



REQUISITOS ADICIONALES

- Se valorará que la **solución sea segura**, permitiendo localizar “Rogue AP’s”, en las instalaciones, y ubicarlos de una forma más o menos certera en un plano.
- Se valorará que el propio **AP pueda ser ampliado** para dar soporte a más clientes con el simple hecho de añadir una segunda tarjeta.
- Se valorará que la electrónica de gestión sea capaz de **convivir con AP’s de otros fabricantes, en especial los de 3Com** y gestionarlos, aunque sea de una forma simple.
- Se valorará el **coste de mantenimiento anual** de la instalación y el coste de las futuras ampliaciones así como la garantía de los equipos instalados.
- Se valorará que la solución vaya acompañada de algún **software de gestión** que ayude a la gestión y mantenimiento del parque de AP’s instalados.
- Se valorará la capacidad de gestión de tráfico (**QoS**) en la solución propuesta.
- Se valorará la posibilidad de realizar diferentes tipo de filtrados (puertos, protocolos, filtrado de tormentas multicast,) directamente en el AP.
- Se valorará la presentación de referencias de experiencias recientes en proyectos de similares características al solicitado por la UD.



4

Requisitos formales

El próximo **viernes día 27 de enero a las 16:00h** se convocará a todas las empresas invitadas para visitar las instalaciones de la UD a dotar de cobertura inalámbrica. Además, se mostrarán las ubicaciones de los armarios de red desde los que se deben realizar las acometidas hasta cada uno de los AP's identificados.

El **martes día 31 de enero** se atenderá a las empresas interesadas (esta vez de forma individualizada) para aclarar las dudas que hayan podido surgir. Cada empresa interesada en esta reunión tendrá que solicitar cita por e-mail a la dirección mcastiel@ud-ss.deusto.es (**antes de las 18:00 h. del lunes día 30 de enero de 2006**).

La **fecha límite para la entrega de propuestas** será el **martes día 10 de febrero de 2006 a las 14:00 h.** (pudiéndose entregar por correo electrónico).

El día **17 de febrero** se decidirá qué propuestas serán finalistas en este proyecto, notificándose la resolución tanto a favor como en contra a todos los participantes. Aquellos que resulten finalistas, deberán preparar una presentación con una maqueta real en la que puedan demostrar qué funcionalidades ofrece el equipamiento de gestión propuesto y los AP's ofertados.

Estas presentaciones deberán tener lugar entre el 23 y 24 de febrero. El día 28 de febrero será notificada la empresa a la que se adjudica finalmente este concurso.

Una vez realizada la adjudicación del proyecto, será posible comenzar su ejecución de forma inmediata, siendo el plazo final de entrega el **15 de septiembre de 2006**.