

# **AirMonitor™ Monitorización de Redes Inalámbricas (WIFI)**

Oscar Cordero Saldaña (oscar.cordero@openwired.net) Coordinador de proyectos

David Moron Ruano (david.moron@openwired.net) Coordinador de proyectos

Antoni Barba Martí (telabm@entel.upc.edu) Director de proyectos

OpenWired SL (www.openwired.net)

1 junio del 2005

*Abstract. Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar ordenadores mediante tecnología inalámbrica. Las redes inalámbricas facilitan la operación en lugares donde los ordenadores no pueden permanecer en un solo lugar ó lugares donde no hay redes físicas.*

*El AirMonitor™ es un dispositivo desarrollado por la empresa OpenWired SL (www.openwired.net) conjuntamente con UPCNet que incorpora un completo grupo de herramientas orientadas a la monitorización y análisis de la red wireless, de los puntos de acceso (access point), de los usuarios, etc. Combina un sistema de administración remoto basado en web, que permite controlar una red inalámbrica, a administradores de red con poca experiencia.*

*El código fuente fue liberado y esta disponible a través de la Farga de la UPC (<http://lafarga.upc.es>).*

## **1 Introducción.**

El AirMonitor™ es un dispositivo que incorpora un completo grupo de herramientas orientadas a la monitorización de la red wireless. Dispone de un sistema de administración remoto a través de un sistema basado en web, que permite administrar una red inalámbrica, de manera sencilla e intuitiva. Está orientado a la detección de anomalías tales como fallos de hardware, interferencias en la red, bajas velocidades de conexión, malas configuraciones, baja calidad de señal, congestión de los puntos de acceso.

El colector de datos de alta velocidad del AirMonitor™ utiliza el protocolo de gestión SNMP [1] y el protocolo HTTP, y otros protocolos para recopilar datos en tiempo real, permitiéndole localizar rápidamente cada dispositivo en la red y a la vez visualizar la información de cada dispositivo y usuario inalámbrico conectado a la red.

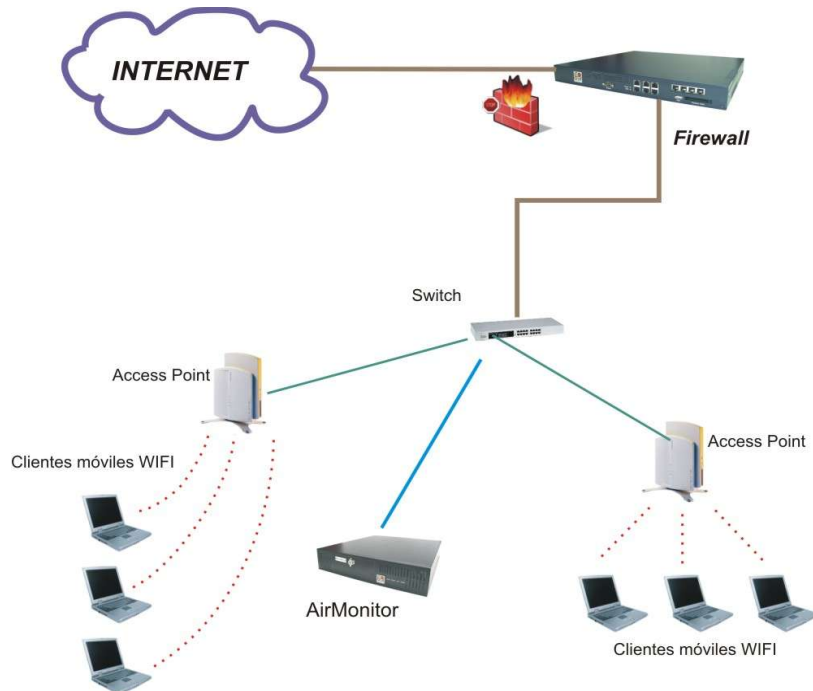


Figura 1: Esquema básico del AirMonitor™ para una monitorización en una red local.

En la anterior figura, se muestra la topología mas básica donde el AirMonitor™ esta conectado en la misma red LAN donde están los puntos de accesos a ser monitorizados.

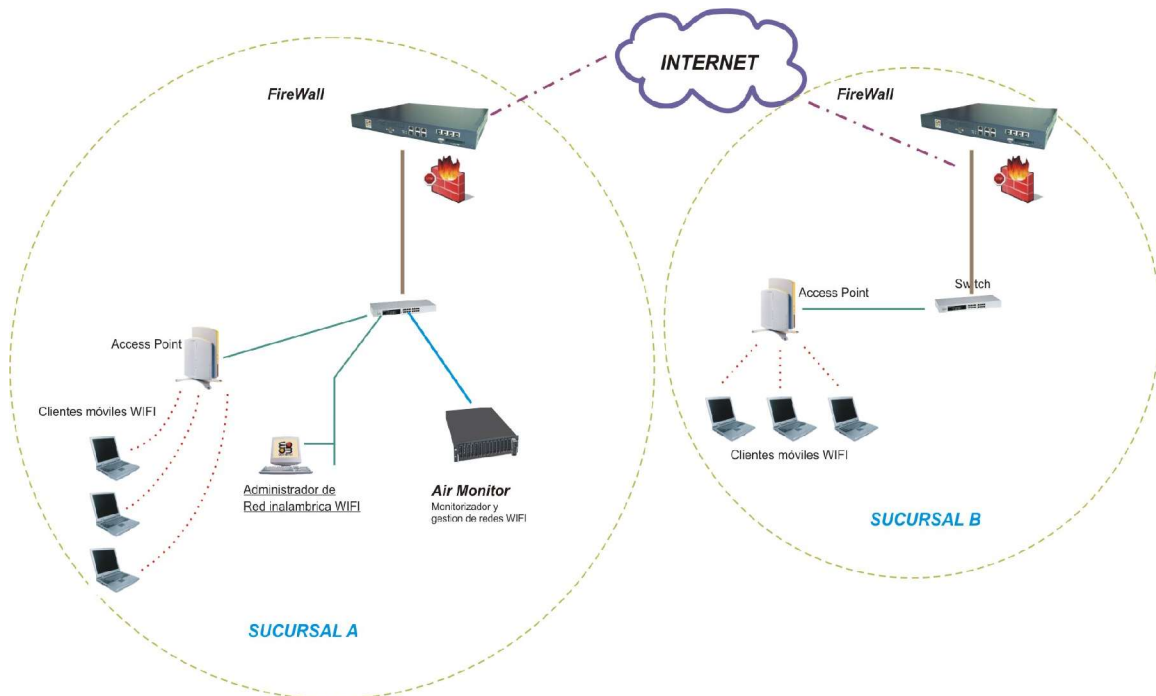


Figura 2: Esquema típico del AirMonitor™ para una monitorización remota a otras redes LAN.

En la anterior figura, se muestra el esquema más avanzado de la arquitectura del AirMonitor™ donde dos redes locales están conectadas a Internet a través de un enrutador. El AirMonitor™ puede colocarse en otra red LAN (Ej: empresa outsourcing) desde la cual se realizara la monitorización remota a los puntos de acceso. En este caso deberán hacerse configuraciones especiales en los firewall, informando a estos que deben dejar pasar los protocolos SNMP [1] y HTTP, desde una dirección IP destino a otra Origen.

## **2 Funcionalidades.**

Las funcionalidades mas importantes a destacar son:

- Monitorización en tiempo real 24x7 de la red WIFI [9]. Notificaciones vía e-mail.
- Soporte desde 1 hasta 1000 puntos de accesos.
- Interfaz segura basada en web.
- Informes detallados de todos los equipos y usuarios monitorizados

## **3 Descripción del AirMonitor.**

El AirMonitor cuenta con muchas funcionalidades completa de este menú se detalla en los siguientes apartados.

### **3.1 Grupos APs**

Grupos creados y puntos de acceso que pertenecen a cada grupo, como también los puntos de accesos que están funcionando y los que no, el ancho de banda utilizado, usuarios conectados al grupo de puntos de accesos y finalmente el intervalo de tiempo en segundos, en el cual todos los puntos de accesos son monitorizados.

### **3.2 Punto de Acceso.**

Monitorización en tiempo real del punto de acceso, mostrando gráficas de tráfico de entrada, tráfico de salida, usuarios conectados, memoria y cpu utilizada.

### **3.3 Usuarios.**

En esta pantalla se muestran todos los usuarios que actualmente están conectados . Para cada uno de ellos podemos observar el nombre del usuario, dirección MAC, dirección IP, punto de acceso al cual está conectado, fecha de inicio de conexión, duración, el tipo de autorización conseguida en la red WIFI [9] , calidad de señal y ancho de banda.

### **3.4 Informes.**

Se visualizan los diferentes informes que se pueden realizar, para tener un registro de toda la actividad de la red inalámbrica, y poder analizar y detectar futuros y presentes problemas de la red. Los informes disponibles son por grupo, AP, usuario, todos los usuarios y historial de alertas.

### **3.5 Administración.**

La administración de la red WLAN, se realiza en grupos de puntos de accesos, los usuarios que administran la red tienen privilegios y restricciones dependiendo del tipo de usuario y grupo. El AirMonitor viene con dos usuarios predefinidos los cuales no se pueden eliminar y únicamente se puede modificar su contraseña, lo cual se recomienda, durante la instalación, por motivos de seguridad, el super-administrador y el super-monitorizador. Además se pueden crear nuevos usuarios que administren los diferentes grupos y que tendrán una serie de restricciones en función de su tipo (administrador o monitorizador).

### **3.6 Servicios.**

Los servicios son básicamente la monitorización de los dispositivos físicos (switchs, enrutadores) y servicios (servicio de autenticación RADIUS [2], datos de autenticación del directorio LDAP [3]), además de servidores críticos para la funcionalidad de la red inalámbrica.

### **3.7 Alertas.**

El AirMonitor gestiona las alertas categorizándolas en tres estados:

- Activa y no reconocida: Este estado es cuando aparece una alerta nueva, la cual el administrador de la red no ha reconocido, es decir gestionado el inicio de la atención de la alerta.
- Activa reconocida: Estado cuando el administrador ha reconocido la alerta, pero aún no se ha solucionado, es decir que la alerta todavía esta presente.
- Superada no reconocida: Estado cuando la alerta ha sido superada, pero el administrador no se ha dado por enterado, es decir no la ha reconocido.

### **3.8 Tareas.**

Las tareas son acciones que se realizan sobre un punto de acceso a una determinada fecha, esta fecha puede ser programada cada semana, día, hora o minuto según las necesidades. Las acciones disponibles a realizar son las siguientes:

- Reiniciar AP: esta acción reinicia el punto de acceso, cada vez que se cumpla las fechas programadas.
- Enlace radio: esta acción habilita o deshabilita el enlace radio del punto de acceso, es decir no deja que ningún usuario se conecte a la red inalámbrica por medio de él.
- Actualizar firmware: actualiza la versión del firmware del punto de acceso.
- Configurar la potencia de la antena.

## **4 Diseño del AirMonitor.**

El AirMonitor está diseñado para trabajar sobre las siguientes herramientas:

- Servidor WEB APACHE [5] modo seguro (SSL-Secure Socket Layer).
- Servidor Tomcat [6].
- Base de Datos Postgres [7].
- Plataforma Linux [8].
- Servidor Radius [2].

La siguiente figura muestra el diagrama de bloques que forman el proyecto AirMonitor:

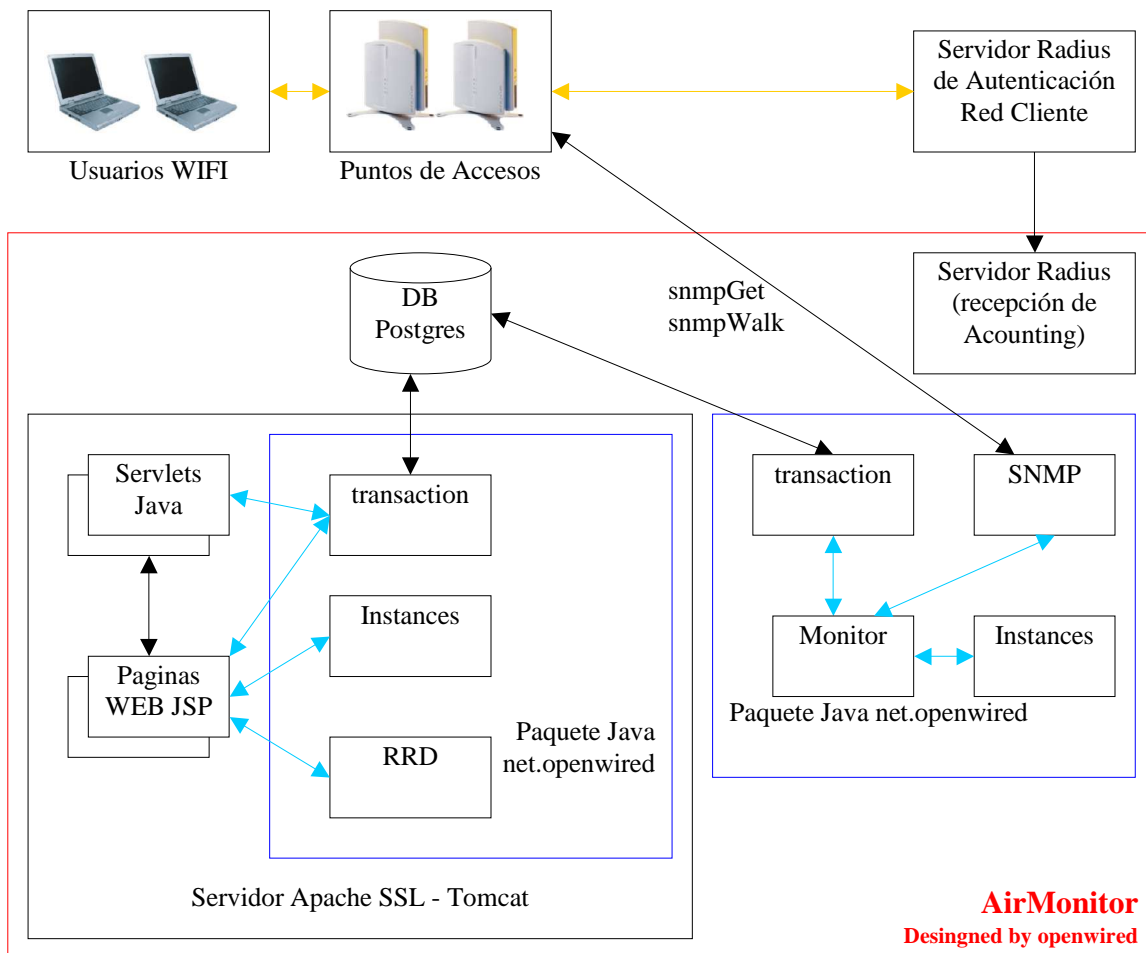


Figura 3: Diseño en bloques del AirMonitor

## Conclusiones

- El AirMonitor facilita la labor de los administradores de red, dándole una herramienta capaz de mostrar los datos necesarios para tomar decisiones en la ampliación de redes, modificaciones de la configuración de los puntos de acceso, reubicación de los puntos de acceso para mejorar la cobertura, etc.
- Es un sistema de monitorización y gestión de la infraestructuras wireless en tiempo real.
- Integración en una sola plataforma de gestión. Diferentes marcas y series de puntos de accesos.
- El tiempo de respuesta para la resolución de problemas en la red WIFI [9], mejora al tener alertas que avisan de problemas en los puntos de accesos y empezar a tomar acciones correctivas.
- Es una herramienta desarrollada en conjunto con UPCNet y que desde el día 3 de junio de 2005 está disponible en la Farga de la UPC para que toda la comunidad pueda disponer de ella.

## Referencias

- [1] SNMP ([www.simpleweb.org/ietf/rfc/complete/rfc3413.txt](http://www.simpleweb.org/ietf/rfc/complete/rfc3413.txt)).
- [2] Radius ([www.simpleweb.org/ietf/rfc/complete/rfc3580.txt](http://www.simpleweb.org/ietf/rfc/complete/rfc3580.txt)).
- [3] LDAP ([www.openldap.org](http://www.openldap.org)).
- [4] OID ([www.mibdepot.com](http://www.mibdepot.com)).
- [5] Servidor WEB APACHE modo seguro ([www.apache.org](http://www.apache.org)).
- [6] Servidor Tomcat (<http://jakarta.apache.org/tomcat>).
- [7] Base de Datos Postgres ([www.postgresql.cl](http://www.postgresql.cl)).
- [8] Plataforma Linux ([www.linux.org](http://www.linux.org)).
- [9] red inalambrica WIFI (<http://standards.ieee.org/wireless>).