Arquitectura para el despliegue de redes *wireless* sobre redes *wired*

Architecture for Wireless Networks Development over Wired Environments

M. Griera, M. Jiménez y J. A. Martínez

Resumen

Desde sus inicios, las tecnologías *wireless* han tenido un éxito imparable. Su evolución ha sido constante y los estándares actuales ya proporcionan velocidades que permiten trabajar en entornos Ethernet con cierta comodidad.

Quizás este es el motivo por el cual, últimamente el despliegue de los entornos inalámbricos en paralelo con los entornos cableados ha sido espectacular. Su simplicidad de instalación –basta poco menos que colocar un punto de acceso *wireless* pinchado a la red *wired*– ha permitido este despliegue masivo.

Sin embargo, y desde el punto de vista del administrador de red, no deben pasarse por alto muchos efectos colaterales de este despliegue. El punto más criticado de estos entornos es quizás la facilidad de desencriptación, pero no cabe duda de que hay otras fuentes de problemas. A modo de ejemplo podemos citar el acceso no controlado a la red, la validación de usuarios y la asignación de direcciones –con lo que esto comporta– a estos nuevos usuarios.

El presente artículo intenta abordar cómo debe hacerse un despliegue de una red wireless sobre una red wired, manteniendo la seguridad y controlando los accesos. A nivel práctico, el artículo expone también los resultados concretos que han llevado a la creación de un *wireless-gateway* implementado con IPtables y Linux.

Palabras clave: Wireless, ingeniería de red, diseño de red, redes inalámbricas.

Summary

Wireless technology has been a successful story from its beginning. It has been in continuous development and current standards can provide user-speed that allows Ethernet users to work seamlessly.

This is maybe the key point that can explain the spectacular development of wireless environments connected to wired networks. Its simplicity to install –a wireless access-point is almost all you need– has permitted this massive deployment.

Nevertheless, looking at it from the network manager's perspective, some aspects must be pointed out, due to collateral effects. The most criticised point is, maybe, the weakness of the encryption protocol these networks use, but there are many others. For example, uncontrolled access to network resources, no user validation or the problem of assigning IP addresses –with all this involves–.

This article explains how a wireless network development over wired environments should be made, keeping good security levels and providing adequate access-control means. As a practical result, we provide also our wireless-gateway implementation based on a Linux box.

Keywords: Wireless, network engineering, network design.

Las tecnologías wireless han tenido un éxito imparable. Su evolución ha sido constante y los estándares actuales ya proporcionan velocidades que permiten trabajar en entornos Ethernet con cierta comodidad

1.- Introducción

Las tecnologías *wireless* están entrando en el mundo de la redes de datos con tanta fuerza como hace unos años irrumpiera la telefonía móvil en el mundo de la voz. La movilidad en sistemas de voz ya está asumida, y quizás por ello el usuario espera obtener funcionalidades análogas para las nuevas redes de datos inalámbricas.

Uno de los problemas de las redes *wireless* es que el punto de acceso se convierte en un punto potencial de entrada de usuarios no autorizados a la red

De todas formas, y pese al paralelismo, la problemática no es la misma. Simplificando el problema, encontramos, al menos dos frentes. Desde el punto de vista del usuario, queremos darle siempre las mismas funcionalidades, con independencia de su ubicación o punto de acceso. Desde el punto de vista del gestor de red, es necesario un control de los accesos que se están realizando, ya que, en último término, serán accesos conectados directamente a la red cableada.

El presente artículo analiza la problemática y expone una solución para el caso más habitual: el despliegue de redes *wireless* asentadas sobre una red existente ya cableada.

2.- La problemática de las redes *wireless*

Tal y como ya hemos comentado, el despliegue de las redes *wireless* suele ir asociado a su implantación en la red cableada presentando los siguientes problemas:

- La configuración de los puntos de acceso es sumamente sencilla, muchas veces con cómodas interfaces web. Esto permite que, en el límite, se puede llegar a situaciones en las que cada punto de acceso mantiene su propia política y ésta es sólo responsabilidad de la persona que lo ha configurado.
- El punto de acceso se convierte en un punto potencial de entrada de usuarios no autorizados a la red. No hay un estándar para el control de acceso a través del access-point (y en muchos casos tampoco se soporta esta funcionalidad).
- Es muy difícil desplegar una política común a toda la red wireless. Si la red es multifabricante, no existe una forma trivial de hacerlo (y en ocasiones es imposible). Si es monofabricante, estamos ligados a una marca concreta.
- El despliegue de políticas en función del punto de acceso hace altamente probable que el usuario tenga funcionalidades diferentes según el punto de conexión, cosa que va contra el principio de 'acceso basado en usuario'.
- La configuración segura más allá de WEP no es estándar, no suele venir activada por defecto y en muchos casos implica que el fabricante sea el mismo para el punto de acceso y la tarjeta del cliente.

Estos problemas no son nuevos, y de hecho ya existen soluciones en el mercado que intentan resolverlos de forma más o menos satisfactoria. Sin entrar en detalle, las alternativas son:

- Despliegue sin control: simple, pero no es seguro ni escalable ni homogéneo.
- Red monofabricante con control específico.
- Red paralela a la cableada de forma independiente: supone un elevado coste.
- Productos comerciales: como BlueSocket o AirWave, en general con funcionalidades más encaradas a la explotación comercial de hot-spots.

3.- Nuestra solución

A la hora de hacer el diseño de la solución, los puntos que nosotros consideramos fundamentales fueron los siguientes:

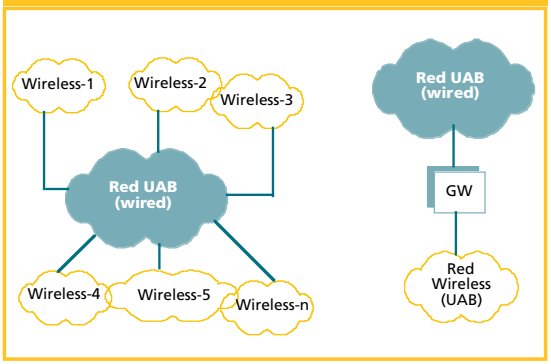
- El usuario debía obtener siempre idéntica funcionalidad, independientemente del punto de acceso que le diera cobertura.

- El dispositivo de acceso no debía requerir ninguna reconfiguración para acceder a la red. Los puntos de acceso se conectan a la red con la configuración "default".
- Deberiamos permitir el acceso a usuarios "anónimos", pero en tal caso, con una funcionalidad limitada (básicamente, acceso web y mail).
- No haría falta gestionar configuraciones complejas de seguridad ya que ésta se gestionaría a nivel de aplicación o mediante el servidor de VPN's corporativo.
- Debería ser una solución independiente de fabricante.
- La solución debería ser de bajo coste.

A grandes rasgos, el sistema que proponemos concentra todo el tráfico proveniente de los distintos puntos de acceso hacia un punto central *(wireless-gateway)*. Será en ese punto donde se implementen de forma centralizada las políticas de control de acceso. El resultado conceptual que obtenemos se muestra en la figura 1. La concentración del tráfico hacia el gateway se realiza mediante la conexión de todos los puntos de acceso en una misma VLAN.

A grandes rasgos, el sistema que proponemos concentra todo el tráfico proveniente de los distintos puntos de acceso hacia un punto central

FIGURA 1: VISTA CONCEPTUAL DE LA RED ANTES Y DESPUÉS DE LA IMPLANTACIÓN DEL GATEWAY



Queda por realizar la implementación del gateway. No se trata de un router convencional, ya que nuestro objetivo es definir perfiles y hacer un control del tráfico fino en función del perfil. La implementación concreta se hará con IPTables.

4.- Detalles de implementación

La idea central del proyecto era dotar a la red wireless de un funcionamiento completamente transparente para el usuario, garantizando a la vez el control en el acceso. Este control debía ser lo suficientemente granular como para dar accesos diferenciados a usuarios convenientemente autentificados. Seguidamente exponemos las funcionalidades concretas que buscamos y cómo se implementaron.

4.1.- Funcionalidades desde el punto de vista del usuario

Cuando pensamos cómo queríamos que operara el gateway desde el punto de vista funcional, nuestra idea era simple. Un usuario entra en la zona de cobertura de un access-point y desea navegar. Abre un navegador y, con independencia de su configuración, recibe un mensaje que le informa de que está accediendo a la red *wireless* de la Universidad y le obliga a aceptar las políticas de uso de la red de nuestra institución. Mientras no se dé esta aceptación el usuario no puede acceder más allá del gateway.

La puesta en funcionamiento del sistema demostró que ciertos usuarios de la red no estaban dispuestos a navegar con tanta restricción y a tener que aceptar las normas cada vez. Por ello, permitimos también que el sistema diera de alta ciertas direcciones MAC –debidamente autenticadas–

Todo el entorno se basa exclusivamente en el uso de software abierto

que se asociaban a un determinado rol y ya no requerían validación. Para el resto de usuarios 'anónimos' sencillamente les damos acceso a la navegación web y al correo (las funcionalidades son configurables).

Creemos importante destacar también que el sistema guarda logs de los accesos que se han realizado para su posterior análisis, así como la posibilidad de crear listas negras si se detecta un uso inadecuado de la red.

Si el usuario requiere un alto grado de seguridad en su conexión, la universidad dispone de un servidor de VPNs que le brinda esta facilidad. El servicio de VPNs se podía haber integrado en el gateway pero vimos que era un problema más general que podía resolverse mejor con una solución hardware específica.

4.2.- Aspectos del desarrollo

Todo el entorno se basa exclusivamente en el uso de software abierto. Los componentes requeridos son una distribución de Linux (en nuestro caso SuSe, pero no es obligado), una base de datos (nuestra implementación ha sido probada con Postgres y MySQL), un servidor Web (Apache) y PHP. El *core* del gateway se implementa con IPTables.

El diseño ha sido realizado de forma completamente modular y se han separado las capas correspondientes a interficie, interacción con la base de datos y plataforma de administración de forma que puedan cambiarse de forma sencilla.

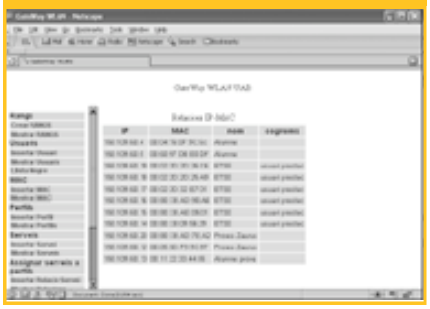
Para todos aquellos interesados en su instalación, la distribución puede descargarse desde el repositorio de SourceForge (http://sourceforge.net/projects/gatewaywlanuab/).

4.3.- Aspectos administrativos

Para simplificar la administración del sistema, todas las tareas de administración pueden hacerse vía web. Deseábamos que la máquina fuera un dispositivo del tipo 'caja negra', y de hecho, el administrador del sistema nunca tiene que entrar a tocar el entorno Linux si no quiere.

En nuestro caso, esto nos proporciona la ventaja de que, una vez hecho el desarrollo y puesto en marcha el sistema, la gestión puede hacerla una persona no técnica. A modo de ejemplo, si el sistema opera en una biblioteca, es esa persona la que puede dar de alta o de baja roles o añadir un usuario a la lista negra.

FIGURA 2: PANTALLA DE ADMINISTRACIÓN DEL SISTEMA



En la figura 2 pueden verse las tareas habituales de administración. Vemos cómo pueden añadirse usuarios, rangos de IPs que se asignarán, nuevos perfiles,... e incluso sin conocimiento técnico reconfigurar coherentemente las funciones de firewalling.

5.- Conclusiones

El sistema diseñado permite una solución de bajo coste para el despliegue controlado de redes wireless. Desde el punto de vista del usuario, el funcionamiento es completamente transparente. Desde el punto de vista del administrador de red, aporta control de acceso y seguridad a la red inalámbrica.

Cabe destacar también que, aun cuando inicialmente el desarrollo se pensó para redes inalámbricas, puede usarse también para el control de puntos de acceso libre (como por ejemplo puntos de Bibliotecas), obteniendo una funcionalidad similar a la que se consigue con 802.1x, pero sin requisitos especiales para la electrónica de red.

Aun cuando inicialmente el desarrollo se pensó para redes inalámbricas, puede usarse también para el control de puntos de acceso libre

Agradecimientos

Queremos agradecer a Jordi Salichs Magem la programación de todo el sistema como parte de su Proyecto Final de Carrera y a José Antonio Lorenzo y José Manuel Castillo por el mantenimiento del sistema y los desarrollos de nuevas funcionalidades.

Martí Griera
(marti.griera@uab.es)
Maribel Jiménez
(maribel.jimenez@uab.es)
Juanan Martínez
(juanan.martinez@uab.es)
Servei d'Informática
UAB