Implantación de un sistema multiproveedor para redes wireless

PONENCIAS

Implementation of an Open Access System for Wireless Networks

J. Barceló, M. Oliver y M. Vives

Resumen

La Universitat Pompeu Fabra dispone desde enero de 2004 de un sistema de acceso a su red inalámbrica wifi basado en la arquitectura de redes abiertas (OAN [1]). Este sistema le ha permitido crear una red inalámbrica abierta, disponible para toda la comunidad universitaria, extensible a usuarios de organizaciones cercanas a la universidad, con una política de seguridad razonable y fácilmente escalable.

El presente artículo describe el funcionamiento de una red de acceso abierta y explica la experiencia de su implantación en la Universitat Pompeu Fabra.

Palabras clave: wireless, autenticación, redes abiertas.

Summary

In January 2004 Universitat Pompeu Fabra started a wireless authentication service based on open access networks. An open access network allows several organizations to share a common access infrastructure preserving different access policies. Main aspects of the architecture and configuration chosen are explained in this paper.

Keywords: wireless, authentication, open access networks.

La Universitat Pompeu Fabra dispone desde enero de una sistema de acceso a su red inalámbrica wifi basada en la arquitectura de redes abiertas

1.- Punto de partida

Las redes inalámbricas son ya un elemento más dentro de la red de comunicaciones de cualquier universidad. Los usuarios las agradecen por su facilidad de uso, los fabricantes las fomentan y desde las organizaciones se ven como un elemento diferenciador y de prestigio.

Crear una red inalámbrica es fácil: basta con conectar un punto de acceso (que proporciona la interfaz radio) a una red clásica y ya podemos disfrutar de la tecnología sin hilos. Sin embargo los problemas llegan pronto, especialmente en el caso de las organizaciones complejas: enseguida aparecen las amenazas a la seguridad en la transmisión de la información y la estabilidad de la red tradicional.

En la mayoría de los casos el sentido común nos lleva a crear una red virtual dedicada exclusivamente a los puntos de acceso para conexión inalámbrica, también denominada red de acceso. De este modo aislamos los posibles problemas que se puedan producir. Si se dispone de una infraestructura de red adecuada esta solución presenta múltiples ventajas adicionales. Entre ellas, cabe destacar la utilización de los denominados 'servidores de acceso' (access servers) para la conexión de la red inalámbrica al resto de nuestra red. A diferencia de los routers y firewalls tradicionales, un servidor de acceso permite la validación de los usuarios (por ejemplo con una clave de paso y contraseña almacenadas en un servidor LDAP) como paso previo a permitir el tráfico de datos a través suyo.

Una arquitectura basada en una red y un servidor de acceso soluciona la mayor parte de los problemas que la tecnología wifi presenta a los administradores de red. Sin embargo, muchas veces la dinámica de las universidades precisa de soluciones que den respuesta a retos adicionales. La validación de usuarios y contraseñas en un servidor LDAP puede resultar insuficiente; a veces se precisa dar acceso a colectivos que no forman parte de la comunidad universitaria en sentido estricto (congresistas, estudiantes de formación no reglada, ...), también puede ser conveniente compartir una

misma red de acceso por parte de varias organizaciones con distinta conexión Internet (por ejemplo la universidad y un vivero de empresas anexo a la misma). Una solución basada en una arquitectura de red de acceso abierta permite dar respuesta a estas necesidades.

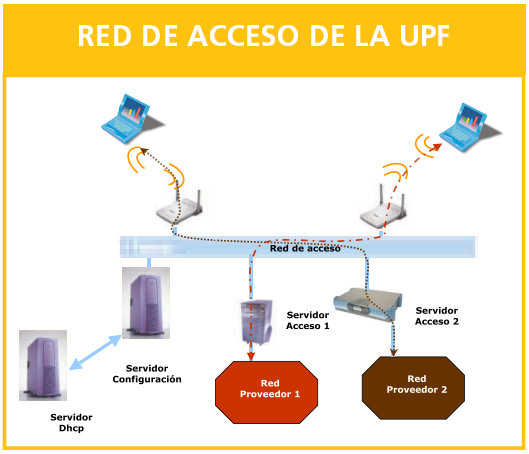
2.- Solución implantada

La red de acceso de la UPF consiste en una red virtual compartida, sin acceso directo a Internet, a la que se conectan más de 35 puntos que proporcionan cobertura a las bibliotecas, auditorios, salas de reuniones, despachos y otras zonas susceptibles de ser utilizadas para el acceso a las redes en los cinco campus de los que dispone la universidad.

A esta misma red se conecta un servidor de configuración [2] que es el encargado de recoger la asociación entre direcciones MAC y proveedores de usuario y de configurar los equipos terminales en consecuencia. También se encuentran en la red de acceso los servidores que interconectan la propia red de acceso con otras redes, por ejemplo Internet. Finalmente se dispone de un servidor para la monitorización y configuración de los puntos de acceso.

La red de acceso es una red de nivel 2 sobre la que coexisten diversas redes a nivel IP, una para cada proveedor de servicio más una para aquellos terminales que aún no están registrados a ningún proveedor

La red de acceso es una red de nivel 2 sobre la que coexisten diversas redes a nivel IP, una para cada proveedor de servicio más una adicional para aquellos terminales que todavía no están registrados a ningún proveedor. De estos últimos decimos que pertenecen al proveedor default. A modo de ejemplo en la UPF se ha elegido el rango 10.10.0.0/24 para el proveedor default, y los rangos 10.10.1.0/24 y sucesivos para otros proveedores. También es posible la inclusión de proveedores que utilicen direccionamiento público.



La configuración de los equipos terminales se realiza mediante el protocolo DHCP [3], por lo tanto el usuario que desee conectarse a la OAN deberá configurar su interfaz WiFi para que se configure mediante dicho protocolo.

Al encender el equipo o al detectar éste una red WiFi disponible se realiza una petición DHCP. El servidor de configuración dispone de un servicio de DHCRelay modificado que recoge dicha petición para reenviarla al DHCP server del proveedor el cual la reenvía al terminal que está asociado. En caso de que el terminal todavía no esté asociado a ningún proveedor (por ejemplo, un terminal que se conecta por primera vez a la OAN) es redirigido al servidor DHCP default.

El servidor DHCP default configurará la IP, netmask, default gateway y DNS server del equipo terminal. Concretamente le asignará una IP correspondiente al rango del proveedor default (recordemos que es 10.10.0.0/24 para el caso de la UPF) por un periodo muy breve de tiempo (unos 30 segundos en nuestro caso). También le asignará como default gateway el servidor de configuración. Dicho servidor permite únicamente el tráfico DNS y redirige todo el tráfico por los puertos http y https hacia su propio servidor web.

De este modo cuando el usuario abre un navegador y solicita una URL cualquiera, se produce la resolución DNS y a continuación la petición http. El servidor de configuración intercepta dicha petición y, en respuesta, presenta al usuario un formulario en el cual pide al usuario que seleccione uno de los proveedores de servicio disponibles. A continuación el usuario es redirigido hacia la página de autenticación del proveedor de servicio elegido.

La elección del usuario se guarda en la base de datos presente en el servidor de configuración, de tal modo que cuando el terminal realiza una nueva petición de IP, la petición sea redirigida al DHCP del proveedor de servicio seleccionado. Esta vez, el DHCP server asignará una IP correspondiente al rango de dicho proveedor de servicio, y como default gateway configurará el access server del proveedor elegido.

El access server es un gateway con un software que permite el tráfico únicamente de usuarios autenticados y autorizados. Típicamente, cuando un usuario intenta navegar le presenta un formulario en el que se le solicita un identificador y contraseña. Estos se verifican utilizando el fichero de password local, o un servidor como LDAP, RADIUS o KERBEROS. Si el usuario tiene permiso, se abre el firewall para él. El access server debe monitorizar de algún modo si el usuario está todavía en activo para cerrar el firewall una vez concluida la sesión. Existen diversas implementaciones de access server [4], unas propietarias y otras de código libre, cada una con sus ventajas e inconvenientes. De todos modos no es el objetivo de este artículo hacer una comparativa detallada de dichas soluciones. En el caso de la UPF se ha optado por software de código abierto tanto para el servidor de configuración como para el de acceso.

La solución implantada ofrece a los usuarios registrados una red de acceso de gran cobertura y facilidad de uso al tiempo que garantiza la seguridad del resto de redes que se encuentran protegidas por los access servers

3.- Conclusiones y líneas de futuro

La solución implantada ha permitido ofrecer al millar de usuarios registrados, una red de acceso de gran cobertura y facilidad de uso al tiempo que garantiza la seguridad del resto de redes, que se encuentran protegidas por los access servers. Además permite un trato diferenciado de los distintos tipos de usuario usando distintos proveedores.

Se ofrecen servicios de interconexión a otras redes como a la de la propia universidad y a la red experimental i2cat, y se espera que a corto plazo aparezcan nuevos servicios de interés. Desde la UPF se está trabajando para ofrecer servicios de localización tanto al usuario final como a proveedores autorizados. De todos modos, el abanico de posibilidades de la arquitectura adoptada es muy ancho.

A nivel técnico, el hecho de que la red de acceso deba ser de nivel 2 es una limitación, y se está investigando para encontrar soluciones escalables que permitan redes de acceso a nivel 3 sin que sea necesario replicar servidores de acceso y configuración. También sería una mejora permitir redundancia de los servicios de configuración para hacer el sistema más tolerante a fallos en sus elementos críticos.

Hasta ahora la red de acceso no utiliza ningún tipo de encriptación, y la seguridad debe ofrecerse a nivel de aplicación. Ofrecer la opción de utilizar WEP e IPSec es otra de las líneas de trabajo. La seguridad, junto con la necesidad de proporcionar garantías de calidad de servicio y herramientas de accounting son obstáculos a superar para poder expandir la idea de las redes abiertas más allá de las universidades y proporcionar un modelo de negocio sostenible y atractivo.

Como primer paso, está previsto para el próximo año el desarrollo de toda una serie de herramientas y mejoras de la red de acceso junto a un proyecto de extensión de la cobertura que abarque a todas las universidades catalanas.

Referencias

1.- R. Battiti, R. Lo Cigno, F. Orava. B. Pehrson, "Global Growth of Open Access Networks: from WarChalking and Connection Sharing to Sustainable Business"

2.- A. Escudero, B. Pehrson, J.-O.Vatn E. Pelleta, and P. "Wireless Access in the Kista-IT University"

3.- ETF. "Dynamic Host Configuration Protocol, RFC 2131"

4.- Martin Hedenfalk "Access Control in an Operator Neutral Public Access Network"

Jaume Barceló
(jaume.barcelo@upf.edu)
Miquel Oliver
(miquel.oliver@upf.edu)
Departament de Tecnologia
Marc Vives
(marc.vives@upf.edu)
Servei d'Informàtica
UPF