Llevando nuestra WiFi a sitios remotos

Taking our WiFi Network to Remote Sites

F. J. Esteban, J. Ginés, F. J. Lacalle y V. M. Delgado

Resumen

El artículo presenta una solución desarrollada por la Universidad de Córdoba para la extensión de su conexión WiFi a aquellos lugares en los que no tienen disponibilidad de infraestructura de red propia. Consta de tres elementos:

- Un conjunto de puntos de acceso WiFi con la misma configuración que los del resto de la universidad para ofrecer los SSID disponibles y gestionar el acceso 802.1x cuando se requiere.
- Un ordenador Linux con pocos requerimientos de potencia, por lo que puede llegar a instalarse en un portátil. Sus funciones son las de Portal Cautivo, servidor DHCP y cortafuegos.
- Una caja VPN, que permite el acceso seguro a la red de la UCO, mediante el modelo "site-to-site VPN".

La autentificación de usuarios tiene lugar en los servidores Radius corporativos, evitando tareas adicionales de administración. De este modo, el servicio queda disponible para los usuarios internos y los de la iniciativa EDUROAM.

El único requisito en la ubicación en que se quiere dar servicio es contar con una conexión básica a Internet, preferentemente con una IP pública (no es necesario que ésta sea fija). La conexión habitual que se viene usando es una línea ADSL de cualquier proveedor.

Palabras clave: Movilidad, WiFi, EDUROAM, Red privada virtual (VPN), Linux, Portal cautivo.

La autentificación de usuarios tiene lugar en los servidores Radius corporativos, evitando tareas adicionales de administración

Summary

The paper presents a solution developed by the University of Cordoba in order to extend ist WiFi connection to sites without own network infrastructure. It consists of three elements:

- A set of WiFi access points configured like the other University's devices. They offer the available SSID's and manage 802.1x access when required (the EDUROAM SSID).
- A Linux computer, not much power needed, so it can be a laptop. It acts as Captive Portal, DHCP server and firewall.
- A VPN box, which gives secure access to the University's network, in a "site to site VPN" paradigm.

The user's authentication take place in the corporate Radius servers, avoiding additional administration tasks, so service is available to internal users and those of EDUROAM project. The only requirement in the remote location is a basic Internet Access, better with a public IP (not necessarily static). The most usual is an Internet provider's ADSL connection.

Keywords: Movility, WiFi, EDUROAM, Virtual private network (VPN), Linux, Captive Portal.

La red desplegada se basó en los estándares IEEE 802.11b/g, que era la única opción disponible en Europa en ese momento

1. Introducción

La primera instalación WiFi en la Universidad de Córdoba (UCO) se inauguró en octubre de 2003 para dar cobertura a la titulación propia de Graduado Superior en Aviación Comercial. En noviembre de ese mismo año, se desarrolló una solución basada en Portal Cautivo para extender el servicio en condiciones aceptables de control de usuarios. Dos años más tarde, en noviembre de 2005, la Universidad se adhirió al proyecto EDUROAM, introduciendo una nueva forma de acceso basada en 802.1x. La página oficial del servicio WiFi es: http://sinhilos.uco.es.

2. Infraestructura y despegue de la red

La red desplegada se basó en los estándares IEEE 802.11b/g, que era la única opción disponible en Europa en ese momento, y la que ha tenido más desarrollo. El fabricante elegido para llevar a cabo el

despliegue fue Cisco, usando equipos de la serie Aironet 1100 y 1200. La solución basada en Portal Cautivo se basó en el *software* libre Nocat (*http://nocat.net/*) y para el acceso 802.x se siguieron las recomendaciones de la iniciativa EDUROAM, contando además con la colaboración técnica del personal de RedIRIS y de instituciones ya adheridas a la iniciativa con equipamiento similar (CICA y Universidad de Granada).

Con esta infraestructura ya en explotación, el Servicio de Informática recibe la petición de dotar de cobertura WiFi a la Residencia Universitaria de Belmez, un pueblo de la provincia de Córdoba en el que se ubica la Escuela Universitaria Politécnica de la UCO. El edificio no cuenta inicialmente con ninguna infraestructura de red y su localización no permite llevarle la red de la UCO sin un gran desembolso, no justificable por el volumen de usuarios afectados. Dado que el esquema usado hasta entonces requiere de conectividad a nivel 2 (existe una correspondencia entre SSID y VLAN, conectándose los puntos de acceso en modo IEEE 802.1q y dándose el servicio DHCP de forma centralizada), era necesario estudiar una nueva solución.

Las condiciones del edificio hacían que el único acceso posible en condiciones económicas y de rendimiento aceptables fuera una línea ADSL. Dado que el servicio iba a estar dirigido a estudiantes, debería realizarse un control de acceso a la red mínimamente seguro y equiparable con el del resto de los usuarios de la UCO. Hubiera sido posible una instalación específica usando por ejemplo WPA-PSK, aunque con limitaciones, ya que los usuarios deberían compartir la misma credencial, tendrían que tener otro perfil de acceso para moverse al resto de la WiFi de la Universidad y el resto de los usuarios universitarios no podría acceder a la nueva zona WiFi, salvo que la credencial se diera a conocer de modo general (lo que equivaldría a crear una zona pública); además, en ese caso, el acceso inicial no hubiera sido a la red de la UCO sino a Internet, lo que hubiera precisado algún mecanismo adicional para equiparar sus servicios a los del resto de los usuarios.

Por estos motivos se buscó una solución que permitiera a los usuarios auntentificarse con sus credenciales de la UCO; que diera acceso a los mismos servicios que el resto de los usuarios y en las mismas condiciones; que permitiera al resto de los usuarios de la UCO acceder a la nueva zona WiFi en igualdad de condiciones y que permitiera la movilidad al resto de las zonas WiFi de la forma más cómoda posible, manteniendo los SSSID disponibles con los mismos requerimientos de configuración de cliente y servicios asociados.

Para los administradores de red, se buscó la máxima homogeneidad con el equipamiento existente

3. Características de la red

Para los administradores de red, se buscó la máxima homogeneidad con el equipamiento existente, tanto en *hardware* como en *software* y configuraciones. El sistema así desarrollado consta de tres elementos:

El sistema desarrollado consta de tres elementos:

- Un conjunto de puntos de acceso WiFi
- Un ordenador Linux
- Una caja VPN

1.- Un conjunto de puntos de acceso WiFi con la misma configuración que los del resto de la universidad. Su función es ofrecer los diferentes SSID (idénticos a los ofrecidos en las instalaciones de la UCO) y gestionar el acceso 802.1x en aquellos SSID que lo requieran (en nuestro caso, el llamado 'EDUROAM').
2.- Un ordenador Linux. Sus requerimientos de potencia no son excesivos, por lo que puede llegar a instalarse en un portátil. Sus funciones son las de Portal Cautivo, servidor DHCP y cortafuegos. Al requerir sólo una conexión básica a Internet, suele montarse también con NAT, aunque no es requisito indispensable. En este equipo se hace también la correspondencia entre VLAN's y SSID, asignando estáticamente las primeras a los segundos.
3.- Una caja VPN, que permite el acceso seguro a la red de la UCO, mediante el modelo "site-to-site VPN". El modelo elegido ha sido la serie VPN-1 Edge de CheckPoint, por compatibilidad con la instalación de seguridad corporativa.

En la red corporativa se realiza la autentificación de usuarios mediante los servidores Radius corporativos, por lo que no se requiere carga adicional de administración, y el servicio queda disponible para todos los usuarios internos y, a través de EDUROAM, a todos los de las instituciones afiliadas.

El montaje del edificio se realizó dotándolo de cableado interno para la ubicación de los puntos de acceso y dejando en el armario técnico correspondiente el acceso ADSL, la caja VPN y el ordenador Linux. Una vez montada la localización, la nueva red se integra en la infraestructura WiFi de la UCO sin ninguna complicación, quedando los puntos de acceso visibles y gestionables en igualdad de condiciones que los del resto de la UCO, siendo posible también consultar y administrar el estado del Portal Cautivo con sus herramientas web incorporadas.

En la red corporativa se realiza la autentificación de usuarios mediante los servidores Radius corporativos

El nuevo equipamiento tiene algunas limitaciones conocidas; para el usuario, el nuevo espacio WiFi es una isla de direccionamiento, de modo que no hay comunicación entre un cliente de la nueva zona con otro de la antigua; sin embargo, dado que la red WiFi es básicamente de acceso, no ha habido quejas al respecto; por otra parte, la conexión 802.1x de la nueva zona atraviesa un nodo NAT, lo que le quita algo de funcionalidad. Este último requerimiento podría evitarse, aunque habría que aumentar la capacidad de la caja VPN (cada cliente WiFi daría lugar a un nuevo túnel). Por otra parte, de cara al administrador de la red aparece un nuevo Nocat que gestionar y si se añaden reglas IPTables específicas (por ejemplo para hacer una autorización por MAC), hay que distribuirlas al nuevo nodo.

La solución desarrollada puede reducirse a la caja VPN, un portátil con Linux y un punto de acceso conectados directamente. Este equipamiento es fácilmente transportable y por ello, puede usarse para disponer de una "unidad móvil" que permitiría desplegar nuestra WiFi de forma rápida en cualquier lugar que cuente con una conexión básica a Internet; por ejemplo, para la realización de eventos fuera de nuestras sedes, campañas itinerantes, viajes y estancias o el montaje de oficinas temporales.

Francisco José Esteban Risueño
(fjesteban@uco.es)
Juan Ginés de Sepúlveda Guitart
(jgines@uco.es)
Francisco Javier Lacalle Villamor
(fjlacalle@uco.es)
Víctor Manuel Delgado Lorente
(vmdelgado@uco.es)
Servicio de Informática
Universidad de Córdoba