Un modelo de gestión automatizada de dispositivos IP mediante Software Libre

A Model for Automated Management of IP Devices Using Open Source Components

J. Guijarro, M. Jiménez y M. Griera

Resumen

En este artículo se describe una solución de desarrollo propio de inventario y gestión de red basada en productos Open Source. La solución permite la automatización de la gestión de servicios clave de la red como el DNS y el DHCP.

Palabras Clave: gestión de red, Software Libre, inventario, identificación, control de red, seguridad, Sauron, Netdisco.

Summary

In this article we describe a home developed solution for network management and inventory built on existing open software components. This solution provides the automation of key network services such as DNS and DHCP.

Keywords: Network Management, open source, inventory, identification, network control, security, Sauron, Netdisco.

La solución que se presenta permite la automatización de la gestión de servicios clave de la red como el DNS y el DHCP

1. Introducción

Desde que se conectó el primer ordenador y se creó la red de la UAB, hemos intentado mantener un inventario actualizado de los ordenadores que están conectados a ella: saber quién es responsable de cada IP en uso y dónde está conectada cada máquina de la red es una información irrenunciable para los administradores de la misma.

Ha sido una tarea dura y de una fiabilidad bastante relativa ya que queríamos combinar la libertad de movimiento del usuario con la exactitud del inventario. Con el modelo que presentamos aquí y que hemos implantado recientemente, creemos que hemos resuelto razonablemente este problema: no pretendemos tener el inventario totalmente perfecto, pero sí acercarnos a este ideal.

La universidad usa direccionamiento IP público y estático asignado por DHCP

2. Contexto

La red de la universidad se compone de unos 10.000 ordenadores (incluidas las aulas, equipos de laboratorio, ordenadores del PAS/PDI...). Aunque se intenta homogeneizar al máximo el tipo de ordenadores, lo cierto es que hay de todo y para todos los gustos.

Los ordenadores están conectados a equipos de red, normalmente *switches* de nivel 2, que, aunque de diferentes fabricantes, todos soportan la gestión por SNMP.

La universidad usa direccionamiento IP público y estático asignado por DHCP. Cada ordenador tiene una IP en función de su MAC y la obtiene por DHCP.

La información que nos interesa inventariar para cada dispositivo de usuario es la IP del equipo, su MAC, el responsable de la máquina, la relación roseta/despacho y el equipo de red incluyendo el número de puerto que le da o le ha dado servicio.

3. Situación inicial y problemática

Hasta hace poco toda la gestión de la asignación de direcciones y modificación del inventario se hacía de forma manual; los usuarios debían solicitar el alta del ordenador, la modificación de la MAC o el cambio de ubicación y desde el servicio de informática se actualizaban los datos tanto en el inventario como en las aplicaciones de DNS y DHCP.

Hasta hace poco toda la gestión de la asignación de direcciones y modificación del inventario se hacía de forma manual

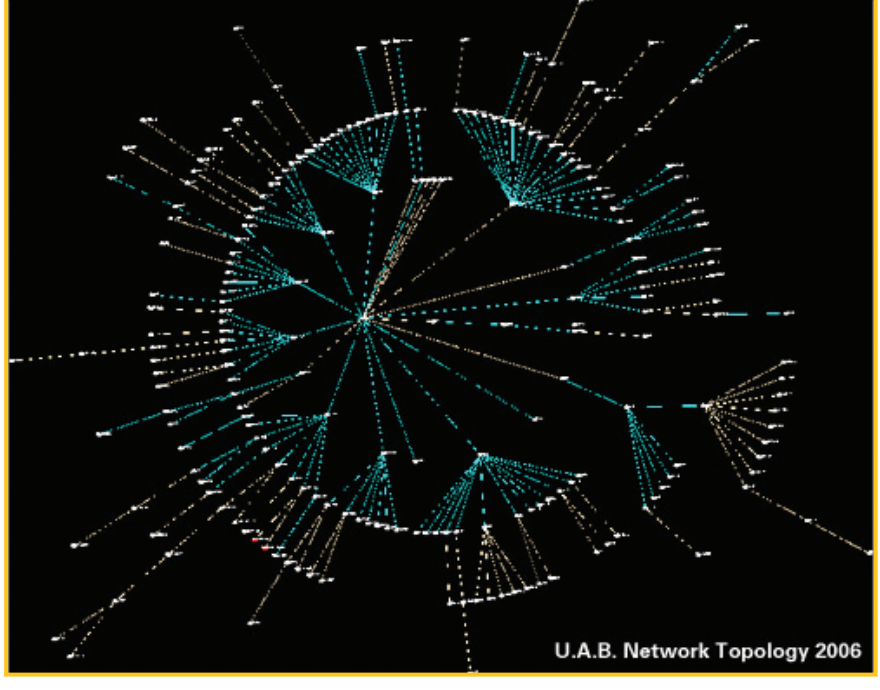
A medida que iba creciendo el número de ordenadores conectados a la red, este tipo de gestión se hacía más compleja. El día a día de la gestión ocupaba gran parte del trabajo de explotación. El inventario estaba cada vez menos actualizado, ya que es más importante la conexión a la red que el hecho de cumplimentar adecuadamente las solicitudes. Así llegamos al extremo de que los usuarios sólo rellenaban solicitudes cuando no les funcionaba la conexión, mientras tanto habían hecho cambios de máquina, se habían fijado la IP a mano, habían movido la máquina de roseta, etc.

Como consecuencia, teníamos conectadas rosetas en despachos en los que ya no había ordenadores, provocando un crecimiento irreal de equipos de red, lo que provocaba que se ampliaran continuamente teniendo puertos conectados que ya no se estaban usando.

La única parte del inventario que se actualizaba correctamente era la relación entre la roseta y el equipo de red (*switch*) y puerto, ya que era introducida directamente por los operadores de red que administraban las conexiones

El día a día de la gestión ocupaba gran parte del trabajo de explotación

FIGURA 1.
TOPOLOGÍA DE LA UAB PROPORCIONADA POR NETDISCO



4. Evaluación de alternativas

La primera opción fue analizar el mercado del momento (estamos hablando de hace 2 ó 3 años) para buscar algún producto que nos permitiera liberar trabajo del día a día y conseguir un inventario más fiable.

Analizamos productos de inventario de IPs que ligaban la base de datos de inventario con el DNS y el DHCP y productos más orientados a infraestructura como ALM [1]. En su momento no nos convenció ninguna de estas soluciones porque o bien no permitían un inventario riguroso o no se adaptaban a la gestión modular que necesitábamos.

Analizamos soluciones que implementan seguridad en la red a nivel del acceso. Éstas se basan en securizar la red desde el momento de la conexión, autenticando al usuario que accede a ésta y dándole privilegios según su perfil (UPN de Enterasys [2], NAC de Cisco [3]...).

Analizamos soluciones que implementan seguridad en la red a nivel del acceso

Con soluciones de este tipo pensábamos automatizar totalmente la gestión de IPs, ya que el control que necesitábamos nos lo daría la aplicación; pero al realizar el análisis vimos algunos inconvenientes:

- Normalmente están basadas en propagar VLANs por perfiles y en configuración de los equipos de red que nos complicaba la gestión de los equipos de acceso.
- Todos los usuarios deben estar dados de alta con un perfil asociado, los cambios en el personal deben propagarse automáticamente, tanto altas y bajas como cambios de cargo, debe existir un método rápido para registrar cualquier persona que necesite una conexión permanente, sea cual sea su relación contractual con la Universidad.
- Hay que configurar el tipo de acceso en cada puerto de cada *switch* de la universidad. No es lo mismo un puerto de *up link* o para conectar una impresora que uno de acceso a un usuario.
- Normalmente se usa el protocolo 802.1x para autenticar al usuario; esto supone asegurar que todos los ordenadores tienen el *driver* necesario o de lo contrario no tendremos información de todos los accesos.
- Si hay muchas excepciones, es decir, puertos de acceso sin autenticación por problemas con *drivers* o usuarios no registrados, el sistema no es válido.
- Sigue siendo difícil averiguar qué IP se ha conectado y desde dónde.

Finalmente analizamos la opción de hacer un desarrollo a medida que cumpliera con todos nuestros requerimientos

Montar una solución de este tipo es complejo y no sólo involucra a la unidad de comunicaciones, sino que también afecta a otras áreas que deben proporcionar la información de usuarios y perfiles. En nuestro caso y en este momento, lo único que pretendíamos era un inventario fiable de lo que tenemos conectado a la red, por tanto se descartó como solución inmediata.

Finalmente, y vistos los resultados, analizamos la opción de hacer un desarrollo a medida que cumpliera con todos nuestros requerimientos. Fue factible convertirlo en un proyecto interno y propusimos hacer un desarrollo propio.

5. Detalles de la solución

Dado que íbamos a desarrollar nuestra propia solución, replanteamos lo que queríamos que fuese una solución "ideal" y llegamos a una serie de requerimientos:

- Mejorar al máximo la fiabilidad del inventario. La máxima fiabilidad la conseguiremos maximizando la información que obtenemos de los equipos de red y minimizando la que nos

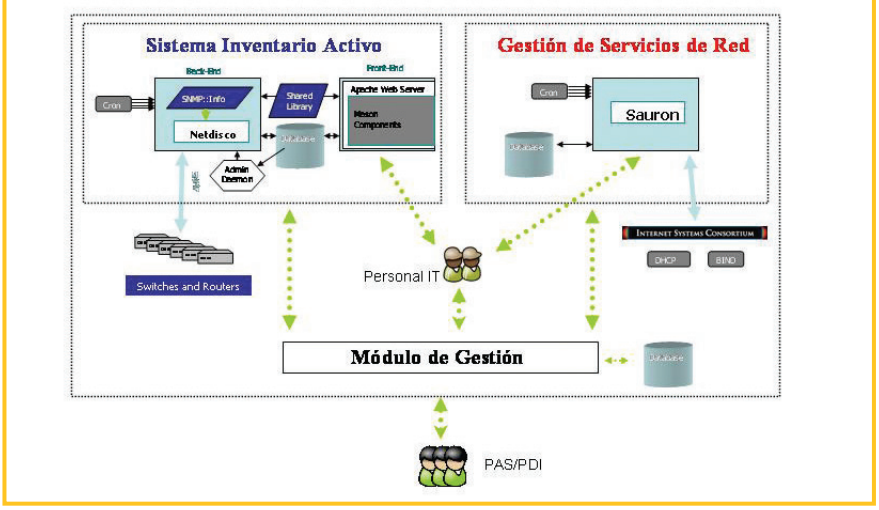
debe proporcionar el usuario. El usuario sólo registrará las altas y los cambios de MAC, la información sobre la situación del ordenador la obtenemos de la propia electrónica de red.

- Mejorar el tiempo de servicio. Las solicitudes que tenga que hacer el usuario (sólo altas y cambios de máquina) deben ejecutarse al momento en la modalidad de autoservicio. Liberamos de esta tarea a los gestores de la explotación de red y facilitamos que el usuario registre sus máquinas. La información registrada debe reflejarse rápidamente en los servicios de DNS y DHCP. Para conseguirlo fácilmente habría que ligar estos servicios a una base de datos.
- Obtener suficiente información para optimizar el uso de la infraestructura de red y del direccionamiento, pudiendo desconectar o dar de baja lo que no se esté utilizando sin necesidad de que el usuario lo solicite.

Evaluando el trabajo necesario para la implementación de los requerimientos descubrimos que con un par de herramientas Open Source y un doble desarrollo que las ligara podíamos tener una solución completa.

Descubrimos que con un par de herramientas Open Source y un doble desarrollo que las ligara podíamos tener una solución completa

FIGURA 2.
ARQUITECTURA DE LA SOLUCIÓN



Para mejorar la fiabilidad del inventario usamos Netdisco, una herramienta Open Source basada en web para la gestión de red

En primer lugar, para mejorar la fiabilidad del inventario usamos Netdisco [4], una herramienta Open Source basada en web para la gestión de red. Esta herramienta interroga por SNMP a todos los equipos de red y da la información actualizada de lo que realmente está conectado:

- Inventario de los equipos que se conectan a la red: IP, MAC y puerto en el que están conectados.
- Inventario de los equipos de red.
- Histórico de cambios.
- Búsquedas por IP, MAC o equipo de red.
- Entorno web amigable.

En segundo lugar, para mejorar el tiempo de servicio usamos Sauron [5], una herramienta GPL que gestiona los productos de DNS y DHCP de ISC [6]. Usa una base de datos para guardar la información y genera los ficheros de zonas para el DNS y el fichero de configuración para el DHCP. Tiene una interfaz web y una interfaz de comandos.

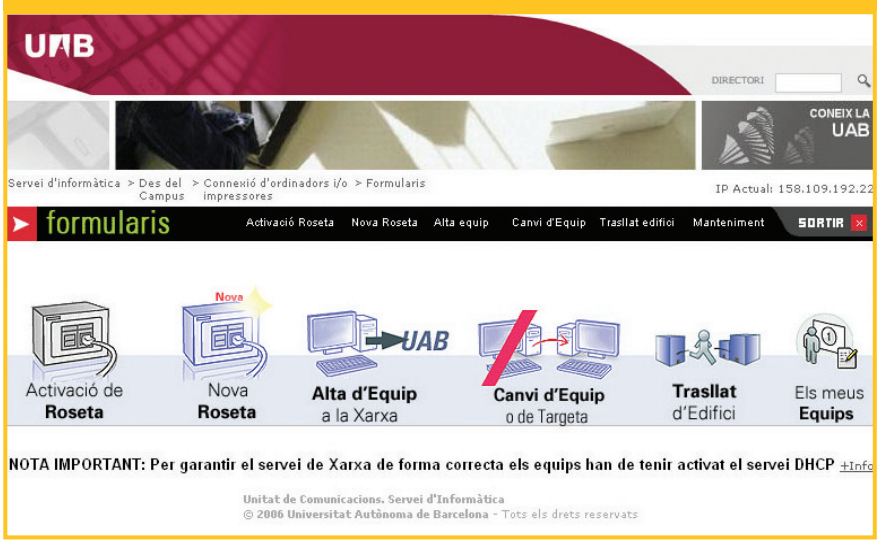
INFRAESTRUCTURA DE RED	
#Dispositivos de red*	253
#Interficies	13.995
#IPs de Gestión	426
#Links Layer 2	427
#Nodos**	23.868
#IPs	13.954

* Dispositivos L3 y stacks de L2
** Detectados desde la puesta en marcha del modelo

Tabla resumen de la infraestructura de red proporcionada por Netdisco

Aprovechando la interfaz de comandos de Sauron se ha desarrollado una aplicación web para que los usuarios puedan gestionarse sus máquinas. Pueden asignar una IP a un nuevo ordenador, ver todas sus máquinas, cambiar la MAC de una máquina o incluso añadir IPs de diferentes zonas a una misma máquina (básicamente para el caso de portátiles que tienen que funcionar con diferentes direcciones según el segmento de red en el que estén).

FIGURA 3.
PANTALLA DE LA APLICACIÓN DE AUTOSERVICIO PARA EL USUARIO FINAL



Se ha desarrollado una aplicación complementaria que permite consultar la información disponible de un ordenador cualquiera de la red

También se ha desarrollado una aplicación complementaria para usuarios privilegiados que permite, desde un entorno web controlado, consultar la información disponible de un ordenador cualquiera de la red; se muestra tanto la información proporcionada por Netdisco (información "real" de la red) como la que existe en los registros de altas (Sauron) y que es la que se publica en el DNS y DHCP.

En tercer lugar, para optimizar el uso de la infraestructura de red y del direccionamiento, utilizamos la información histórica de la herramienta de gestión de red (Netdisco). Actualmente tenemos rosetas parcheadas a la red pero sin ordenador conectado y también direcciones IP asignadas en el DNS a máquinas que ya no existen. Para racionalizar el uso de estos recursos, queremos ser capaces de reaprovechar lo que no se está usando. La herramienta Netdisco nos proporciona todas las fechas en que se han visto los ordenadores en la red y en qué puertos; con esta información podemos saber qué rosetas o direcciones IP no se han usado en los últimos meses y decidir si se reaprovechan o no. Por ahora es una tarea controlada y puntual.

Después de más de medio año de funcionamiento, podemos afirmar que tenemos la red más controlada y a los usuarios más contentos

6. Conclusiones

Después de más de medio año de funcionamiento podemos afirmar que:

- Tenemos la red más controlada y a los usuarios más contentos.
- Podemos localizar rápidamente cualquier ordenador que se ha conectado a la red y desconectarlo inmediatamente si está implicado en algún incidente de seguridad
- Se compran *switches* cuando realmente es necesario, ya que los puertos que no se usan son reutilizados.

- Hemos liberado a una persona que estaba casi íntegramente dedicada a la gestión del direccionamiento IP.
- Tenemos totalmente actualizada la topología de la red.
- Se ha facilitado el trabajo al personal que da soporte a los usuarios ya que les podemos ofrecer información actualizada mejor y más precisa.

En definitiva con este sistema se ha conseguido una gestión de red ágil y dinámica, más allá de lo que se puede conseguir con las soluciones que actualmente ofrece el mercado.

Con este sistema se ha conseguido una gestión de red ágil y dinámica

Referencias

[1] Access Layer Management:
http://alm.usal.es
[2] UPN de Enterasys:
www.enterasys.com/solutions/secure-networks/
[3] Cisco Network Admission Control:
www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html
[4] Network Discovery:
www.netdisco.org
[5] Sauron: DNS & DHCP Management System:
sauron.jyu.fi/
[6] Internet Systems Consortium:
www.isc.org
[7] BIND 9 Administrator Reference Manual:
www.isc.org/sw/bind/arm93/

Jordi Guijarro
(jordi.guijarro@uab.cat)
Maribel Jiménez
(maribel.jimenez@uab.cat)
Martí Griera
(marti.griera@uab.cat)
Servei d'Informàtica
UAB