Comunicación TECNIMAP 2010:

Despliegue de software libre en Comunicaciones y Seguridad

Javier Ferriols Delgado

Jorge Gil Guerra

Andrés Monje Romero

José Luis San Martín

Biblioteca Nacional de España

Despliegue de software libre en Comunicaciones y Seguridad Informáticas

Palabras clave

Software libre, Comunicaciones, Seguridad, Nagios, PRTG, NFSEN-NETFLOW, Wiki, Portal cautivo con pfSense, Filtrado de contenidos, Squid, SquidGuard, Red Privada Pirtual, openVPN, NMAP, Nessus

Introducción

El Servicio de Comunicaciones y Seguridad, integrado en la Unidad de Coordinación Informática de la Biblioteca Nacional de España, tiene encomendadas, entre otras, las competencias de gestión de la Red de Datos y del Centro de Proceso de Datos.

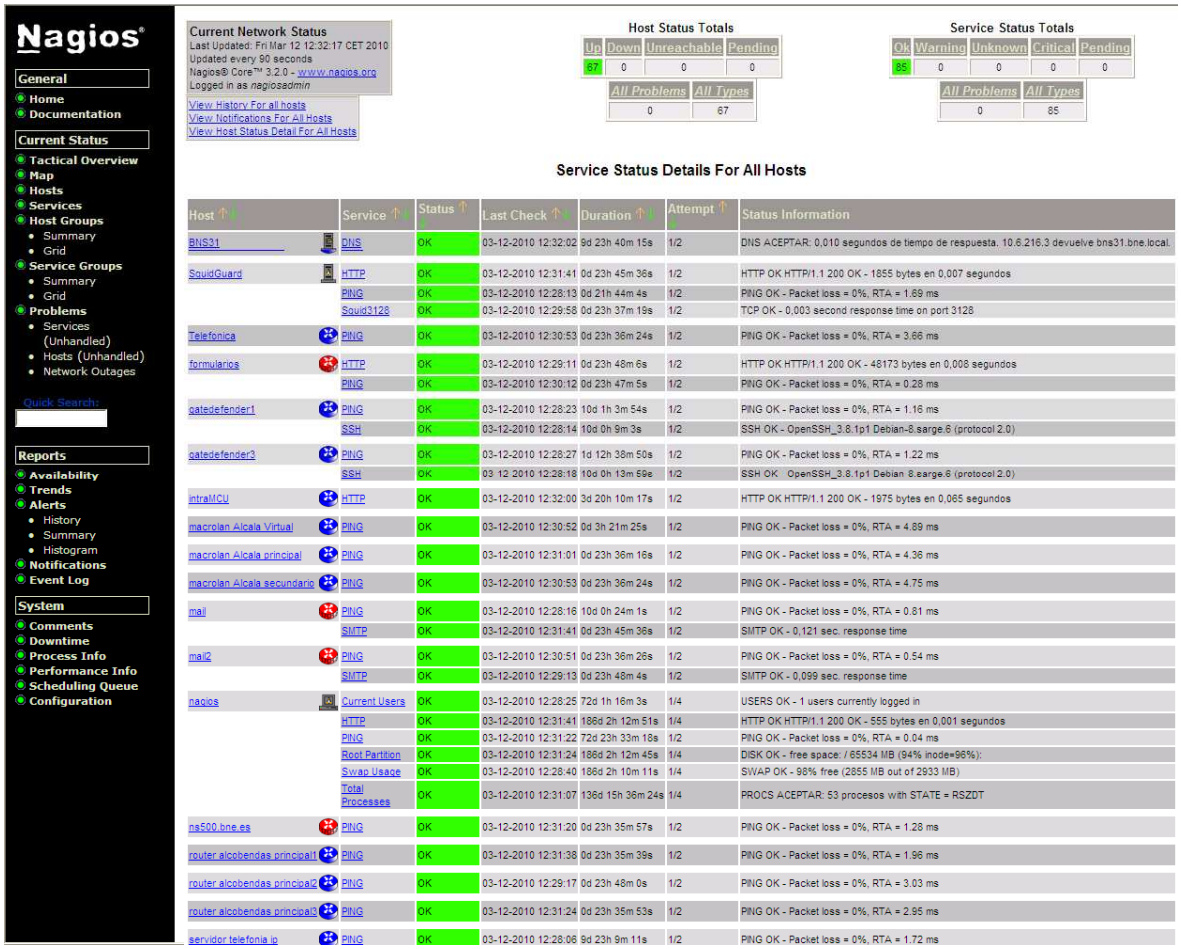
A pesar de la impresión inicial, la envergadura de la Biblioteca Nacional de España, en cuanto a número de usuarios (mil), sedes (una en Madrid y otra en Alcalá de Henares), servidores (casi cien), es acorde con las aplicaciones que ofrece, cada vez más complejas en línea con la evolución de nuestro negocio hacia la difusión de imágenes de alta resolución. Esto tiene implicaciones por supuesto en la gestión de la red y sobre todo en fiabilidad. Debemos garantizar la capacidad, disponibilidad, eficiencia y seguridad de nuestras comunicaciones corporativas.

Por razones que se escapan del alcance de este documento, ha habido ocasiones en que se han producido caídas repentinas e incluso intermitentes de algunos servicios.

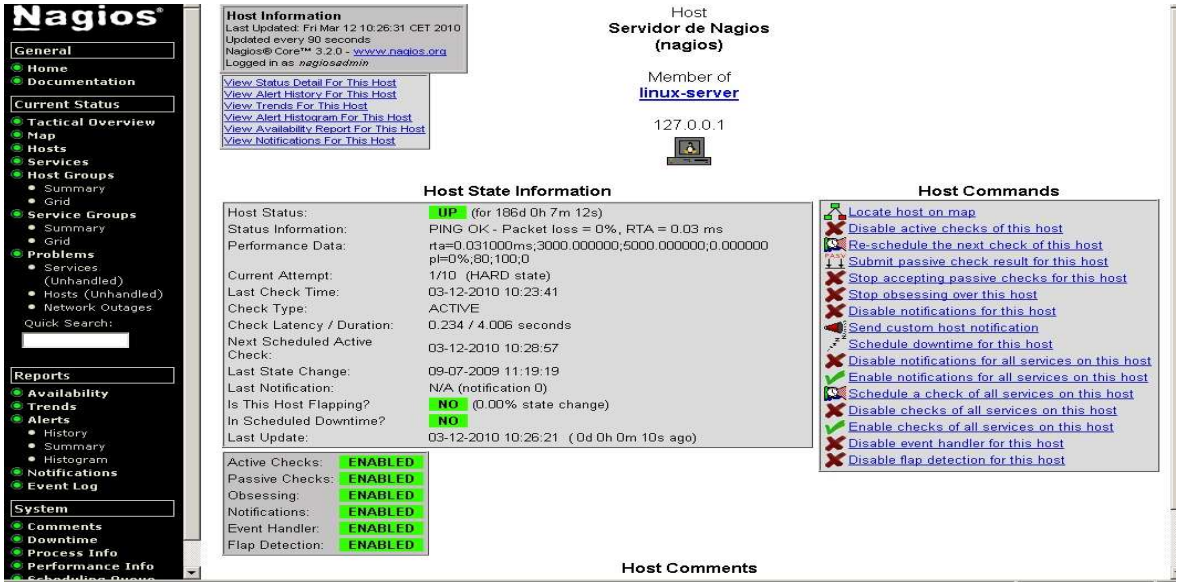
En el entorno actual de avance del software libre[1] y de recortes presupuestarios, las diferentes soluciones que se comentan en este artículo son muy útiles para los efectos comentados, fáciles de implementar, y de reducido coste, lo que las convierte en ideales.

1. Monitorización con Nagios

Debido a que la red de datos de la Biblioteca Nacional de España se vuelve cada vez más compleja y que la necesidad de operación es cada vez mayor, surge la necesidad de conocer el estado de los dispositivos (servidores, hardware de red, etc.) de forma instantánea.



Nagios es un sistema de monitorización publicado bajo licencia libre, que se conoce en algunos ministerios ya[2].



Permite la monitorización de servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP), monitorización de los recursos de un host (carga del procesador, uso de los discos, logs del

sistema), diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, notificaciones a los contactos cuando ocurren problemas.

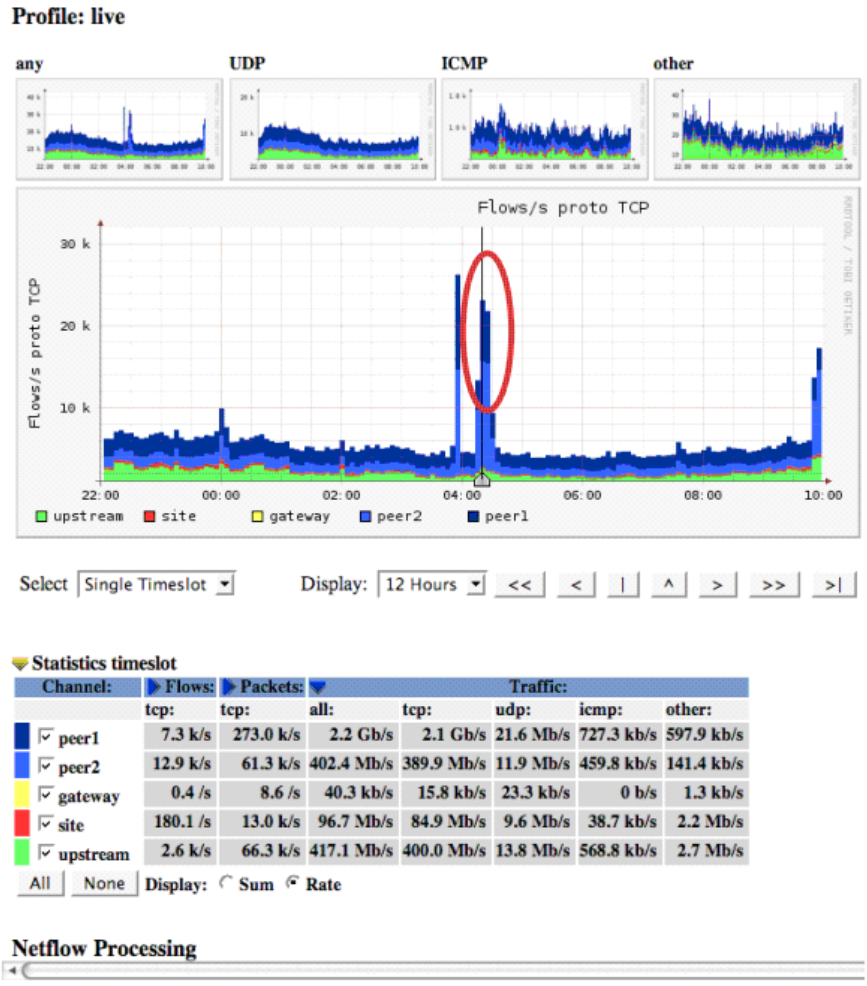
Actualmente el sistema se encuentra en explotación y mejora continua. Queremos integrarlo con MRTG, pero por el momento usamos PRTG (con licencia gratis pero no libre[3]):

Con la implantación de este sistema, la Biblioteca Nacional ha mejorado su productividad, se ha producido una antelación de incidencias con su consiguiente agilización en su tratamiento.

2. MONITORIZACIÓN CON NFSEN-NETFLOW SENSOR

Con la implementación de este sistema, la Unidad de Coordinación Informática ha conseguido identificar y analizar problemas de seguridad.

Permite detectar grandes picos de consumo, realizar gráficas y estadísticas, analizar cómo se propaga el malware por la red, etc.Morbi in mauris quis augue iaculis dictum.



Está basado en un interface web intuitivo y fácil de usar en dónde se muestra gráficamente la situación actual de la red de datos de la Biblioteca Nacional.

Gracias a esta implementación, la Biblioteca Nacional ha mejorado e incrementado su productividad y eficiencia en su red de datos mejorando problemas de seguridad.

3. DOCUMENTACIÓN CON UNA WIKI

3.1 NECESIDADES PREVIAS

Las necesidades de acceso a la información por parte de los distintos miembros de un mismo departamento, nos llevó a preguntarnos cuál sería la manera más adecuada de que dicha información estuviera accesible.

En un principio se disponía de un directorio de carpetas con los diferentes temas en una unidad de red departamental. Lamentablemente, al no tener definido un método único de ordenación, este sistema provocaba demasiadas redundancias, al poder guardar un mismo documento dependiendo de diferentes ramas del árbol. También la búsqueda era demasiado laboriosa.

La solución fue instalar y configurar un servidor con una Wiki en el que la navegación entre los diferentes documentos estuviese implementada mediante enlaces entre ellos. De esta forma no tendríamos que conocer de antemano la ubicación exacta del documento y, simplemente, dejar este trabajo de búsqueda a la Wiki.

En Internet existen diferentes soluciones para implementar una Wiki, desde las más sencillas basadas en simples archivos de texto (DokuWiki) hasta soluciones mucho más estéticas (Twiki). Debido a que lo que se buscaba era principalmente la sencillez y funcionalidad se decidió realizarla con DokuWiki.

3.2 INSTALACIÓN

Se utilizó un simple PC al que se le instaló Ubuntu 8.04LTS. También se le añadió un servidor Web (Apache), MySQL y el lenguaje de programación PHP.

Una vez instalado el servidor LAMP (Linux-Apache-MySQL-PHP), se procedió a la instalación del software propiamente dicho en este caso DokuWiki.

3.3 CONFIGURACIÓN

La configuración es bastante sencilla y consiste, básicamente, en poner la página de inicio en el directorio del servidor Apache y darle al usuario DokuWiki los permisos oportunos de lectura y escritura sobre los directorios del servidor Apache.

La página de inicio de la Wiki comentada es la que se muestra en la figura.

Como se aprecia lo que prima de este software es la sencillez. Aun así existen en Internet diferentes plugins que aumentan la funcionalidad y le dan funciones más avanzadas, lo que permite ajustar la configuración dependiendo de las necesidades de cada usuario.

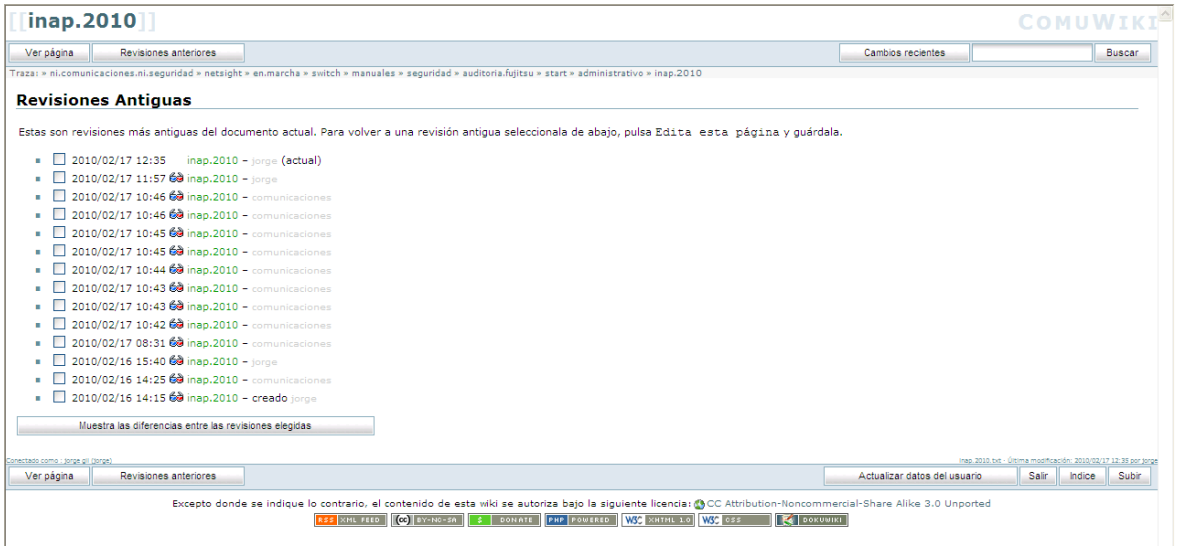
3.4 FUNCIONAMIENTO

Lo primero que solicita la Wiki es la creación de un usuario para su administración y control. Este súper usuario puede crear distintos usuarios con diferentes perfiles según las necesidades de cada uno (lectura, lectura-escritura, administración).

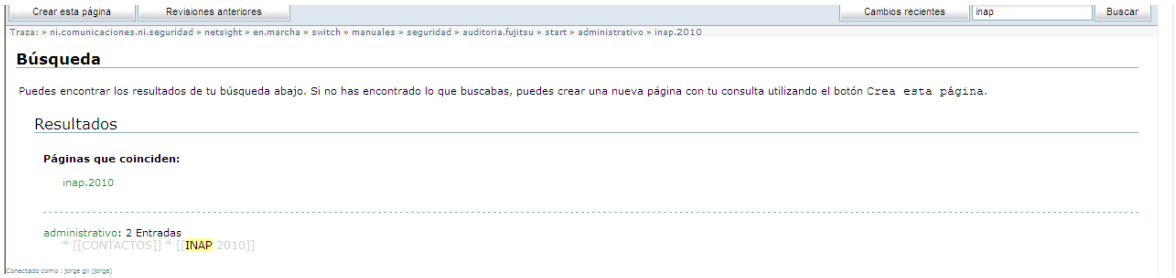
Existe una completísima ayuda, llamada Wiki:dokuwiki, que nos proporciona información sobre como crear, actualizar y eliminar documentos.

También existe la "zona de pruebas", denominada playground donde podremos practicar sin poner en riesgo la información.

Por supuesto también hay funcionalidades para revisiones anteriores y verificar los cambios que se han hecho de la página que estemos consultando:



Por supuesto podemos cargar imágenes, documentos pdf y enlaces a Internet. También realizar búsquedas:



Y todo ello de una forma amigable y sencilla.

De este modo toda la información estará disponible a unos clicks de distancia, y no habrá problemas de redundancia ni perderemos tiempo en búsquedas.

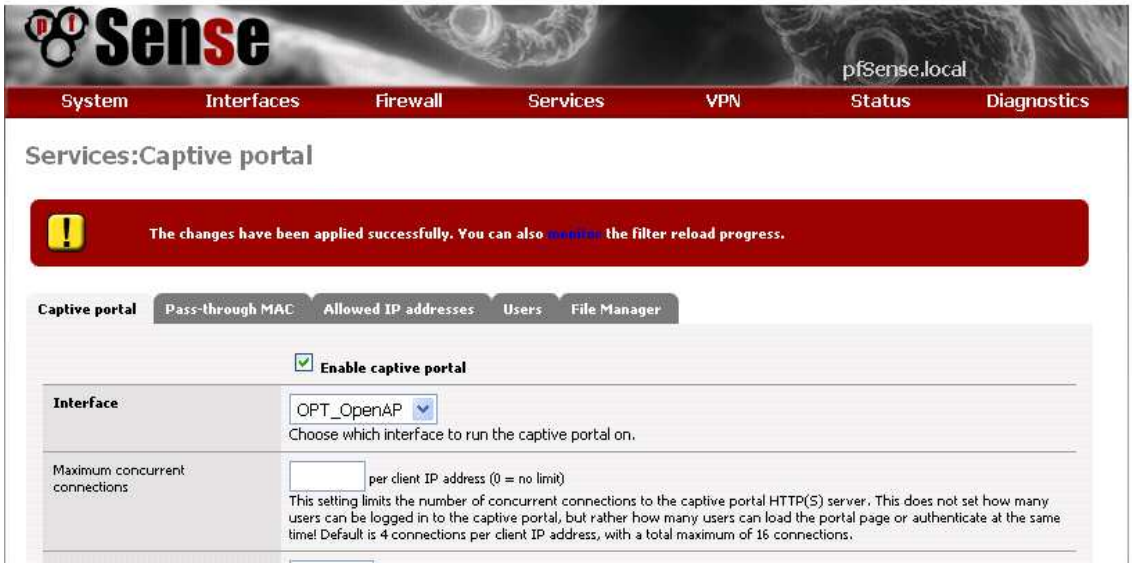
4. UN PORTAL CAUTIVO CON PFSENSE

pfSense es una distribución basada en FreeBSD, derivada de monowall, es instalable en cualquier PC, e incluye un cortafuegos como parte del Kernel. Esto nos permite aislar la red dedicada al wifi de Lectores (visitantes) de la Biblioteca.

Por otra parte estandariza y automatiza la configuración de los navegadores en lo que se refiere proxy y la configuración de red de todas las máquinas, pues lo intercalamos en la red de forma transparente.

Además, el portal cautivo da la bienvenida a los visitantes:

Se configura muy sencillamente en su interfaz web:



Debido a la necesidad de filtrar virus y otras amenazas, que no ha podido ser resuelta con los paquetes que pueden instalarse en pfsense, actualmente está en fase de studio y pruebas un servidor equivalente, basado en Endian[4].

5. FILTRADO DE CONTENIDOS: SQUID Y SQUIDGUARD

La navegación por la red de la Biblioteca Nacional ha de tener un límite, pues el ancho de banda disponible no es infinito. Cada página no autorizada tiene su correspondiente justificación, y se decide de acuerdo con los bibliotecarios Responsables de Sala.

SquidGuard es un redirector libre y rápido que usa listas negras para evitar la navegación ociosa o perniciosa por Internet. A pesar de ello, actualmente parece que la alternativa dansGuardian es más popular.

Contenido no permitido

El contenido de la página solicitada no se considera apropiado,
según la Política de Uso de Recursos Informáticos de la Biblioteca Nacional
(haga click si desea leerla, por favor)

Esto incluye, por ejemplo, contenidos obscenos, pornográficos, exhibicionistas, lascivos, o excesivamente violentos.

Para más información contacte con el Responsable de Sala
o diríjase a uci_comunicaciones@bne.es.

Para volver al catálogo, espere unos segundos, por favor, o pulse aquí.

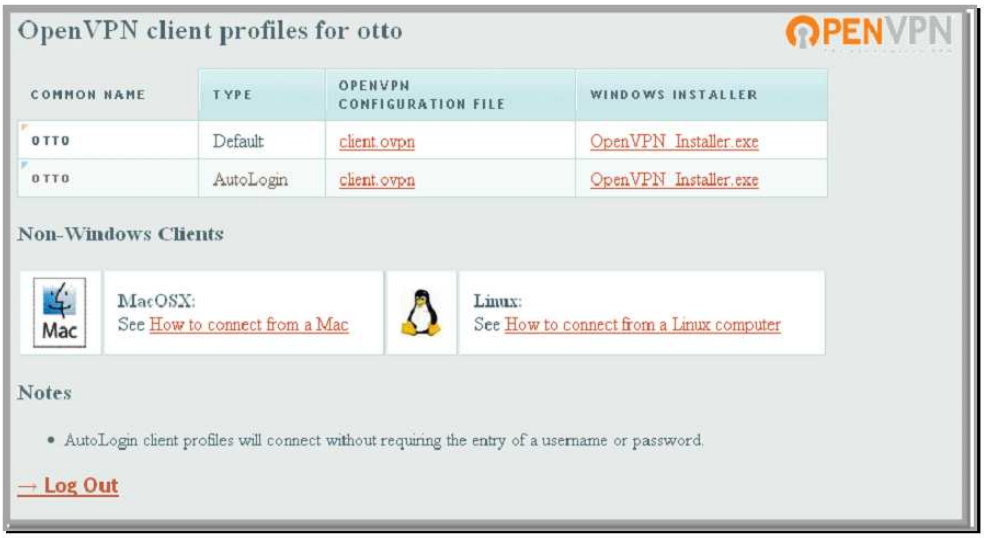
Además, se instala sobre squid, para acelerar la navegación.

6. Red Privada Virtual con OpenVPN

Con OpenVPN podemos extender nuestra red a cualquier lugar del mundo, haciendo que la identificación y la comunicación sean seguras, estando preparados para el teletrabajo.

Se puede integrar en los cortafuegos, tanto en pfsense como en Endian, o en un servidor independiente.

Es multiplataforma (incluyendo Linux y Mac):



Pero requiere instalarse un cliente en los ordenadores de usuario, por lo que sigue estudiándose la posibilidad de migrar a una VPN-sin-cliente (clientless vpn), como era SSLExplorer, lamentablemente descontinuada tras comprarla Barracuda). Por otra parte, la licencia libre de openVPN sólo permite dos usuarios concurrentes.

7. Otros proyectos

Usamos NMAP y Nessus periódicamente para analizar la red y los servidores.

Tenemos previsto, entre otros proyectos, implanter una solución tipo CRM para gestionar incidencias, en particular Vtiger.

[1] ttp://observatorio.cenatic.es/index.php?option=com_rubberdoc&view=doc&id=38&format=raw
[2] http://www.csae.map.es/csi/tecnimap/tecnimap_2006/01T_PDF/monitorizacion.pdf
[3] http://www.bne.es/es/LaBNE/InformacionPractica/ServicioDeConexionWiFi/
[4] http://www.endian.com/