Descripción técnica de Campus Virtual Multimedia como propuesta para la aplicación de la teleenseñanza y el teletrabajo en la innovación docente

José Luis Gordo Rivera; José Luis González Sánchez; Alfonso Gazo Cervero; Pilar Bachiller Burgos; Pablo García Rodríguez y Fernando Sánchez Figueroa.
Departamento de Informática
Universidad de Extremadura
Avda. Universidad s/n. (10.071) Cáceres (España)
e-mail: jlgr@norba.unex.es; Tfno. 646.951500 - 927.257.259; Fax. 927.257.202

1. Resumen

Este trabajo presenta una plataforma integrada como modelo de campus virtual para ofrecer servicios de teleeducación y teletrabajo. CVM (Campus Virtual Multimedia) [2, 3] es una exitosa experiencia piloto, actualmente en explotación, soportada sobre sistema operativo Linux. Hemos implementado un prototipo de bajo coste pero de elevadas prestaciones. Es ampliamente usado en nuestra universidad para acceso remoto a las salas colapsadas (en horario lectivo) o cerradas (en periodos no lectivos). CVM es también usado como sistema móvil cuando nuestra universidad organiza eventos para ofrecer conectividad a los asistentes.

El artículo describe el hardware usado y el software implementado para construir CVM como modelo para soluciones de enseñanza a distancia. Presentamos detalladamente la configuración del sistema y la integración de todos sus componentes. RADIUS es usado como control de acceso robusto y escalable. El artículo resume el software implementado para ofrecer seguridad y disponibilidad a los usuarios del sistema. Hemos puesto especial atención para ofrecer servicios de videoconferencia y proponemos *MBone* como la tecnología para distribuir tráfico isócrono a grupos de usuarios dispersos. El sistema ofrece la distribución de material docente a través de aplicaciones desarrolladas sobre tecnología Web. *RealVideo* ofrece acceso a sesiones diferidas y también tutoriales y encuentros virtuales entre estudiantes y profesores. La gestión del sistema es otra importante decisión de diseño porque CVM es también propuesto como un interesante modelo para ofrecer servicios de teletrabajo a empresas. El administrador del sistema puede definir perfiles de usuario, determinar controles de acceso, asignar tiempos de presencia en el sistema y permitir las horas de conexión autorizadas. El administrador también define usuarios con conexión gratuita a través de mecanismos de *callback* y también obtiene estadísticas de uso para la toma de decisiones.

Actualmente trabajamos para ofrecer aplicaciones de teleeducación que faciliten la elaboración de material docente y su anuncio a través de directorios de sesiones en CVM. Actualmente se están migrando las conexiones externas a tecnología RDSI y las comunicaciones internas a través de ATM.

2. Abstract

This work presents an integrated platform as model of virtual campus to offer teleeducational and teleworking services. MVC (Multimedia Virtual Campus) is a pilot and successful project, now in exploitation, supported over Linux operating systems. We have implemented a prototype of low cost and high performance. It is massively used for our university community to virtual access when the classrooms are collapsed or closed. MVC is also used as mobile system when our university organizes events, to offer connectivity to congress's assistants.

The paper describes the hardware used and the software implemented to build MVC as an engineering model for telelearning solutions. The system provides distribution of educational documents through applications developed over web technology. MVC is also proposed as an interesting model to offer teleworking services at whatever enterprise. The system administrator can define profiles of user, determines access control, assigns elapsed time in the system, allows the hours of authorized connections and disposes full access statistics to take decisions.

We explain widely the system configuration and the integration of all MVC resources. RADIUS is used as a robust and scalable access control system. The paper also resumes the software we have developed to offer securitty and availiability to the final system users. We have focused part of our work to offer videoconference and we propose *MBone* as the technology to send isochronous traffic to sparse user groups. Using *RealVideo*, we offer access to deferred sessions, meetings, tutorials, etc.

Now we are working to offer tele-education applications to make easy the development of docent material and it distribution using session directories in CVM. We are also migrating now the external connection systems to ISDN technology and our internal network to ATM.

3. Introducción

En este artículo presentamos el sistema Campus Virtual Multimedia (CVM), como un prototipo de sistema informático orientado a la teleeducación y al teletrabajo. En la actualidad el sistema está trabajando plenamente en el campus universitario de la Universidad de Extremadura en Cáceres en fase experimental, lo que nos permite ir refinando el diseño del mismo y comprobar los resultados de esos refinamientos sucesivos en la realidad con un considerable volumen de usuarios.

Unas de las premisas de diseño del sistema fueron el desarrollo de un sistema plenamente escalable y distribuido, que fuera sencillo de mantener y administrar, y, al mismo tiempo, que la relación prestaciones/coste fuera lo suficientemente equilibrada. Tras estudiar todos los requerimientos del sistema optamos por una plataforma basada en hardware x86 y Linux como sistema operativo. Este núcleo del sistema se ubica en una red en la que otros equipos heterogéneos también participan, en distinta medida, en el correcto funcionamiento del sistema.

En la actualidad CVM se está utilizando de manera global tanto por el personal docente de la escuela como por parte de los alumnos de la misma, lo que resulta en un nuevo canal de comunicaciones entre alumnos-profesores que repercute positivamente en la relación diaria entre todos los estamentos de la universidad.

CVM permite el acceso virtual a los equipos multiusuario de la escuela cuando estos están siendo utilizados en cursos o clases prácticas, y además permite a los usuarios de ellos tener acceso a los mismos desde su domicilio los días en los que su presencia física sea imposible o cuando las instalaciones de la universidad se encuentren cerradas (fines de semana y días festivos). Además, CVM es utilizado para ofrecer servicios de conectividad a los asistentes a eventos organizados por la universidad.

Utilizamos un rígido control de acceso al sistema basándonos en RADIUS y en los datos que nos ofrece un SGBD relacional con información acerca de todos los usuarios del sistema. Como veremos en este artículo, esta organización nos permite obtener un sistema distribuido para controlar el acceso a CVM con una buena

tolerancia a fallos y fácilmente escalable que nos garantizará la posibilidad de acceder al sistema bajo prácticamente cualquier circunstancia.

En este artículo trataremos de describir tanto el software que estamos utilizando como el que estamos desarrollando para administrar y mantener el sistema de un modo óptimo y garantizando un alto grado de seguridad. Además describiremos los servicios de videoconferencia que estamos ofreciendo en la actualidad a través de CVM basados en *MBone*. Utilizando este sistema estamos distribuyendo documentos docentes a través de aplicaciones desarrolladas para la tecnología Web. Utilizando *RealVideo*, los usuarios del sistema tienen acceso a clases en diferido, a congresos o conferencias y además se ofrece la posibilidad de crear nuevos "puntos de encuentro" entre estudiantes y profesores.

La administración del sistema es un importante punto a tener en cuenta en el diseño de CVM dado que el modelo de CVM puede aplicarse en diversos entornos empresariales orientados al teletrabajo. Con las herramientas que estamos utilizando, el administrador del sistema tiene una capacidad plena en la definición de cada perfil de usuario del sistema, pudiendo determinar parámetros como pueden ser la franja horaria en la que un usuario puede o no conectarse al sistema, el tiempo máximo de conexión permitido por día, el acceso o no a determinados servicios del sistema, etc. Para mantener todo este sistema se está desarrollando una aplicación basada en el Web que reduce notablemente el alto grado de mantenimiento que requiere una aplicación de estas características. Generamos dinámicamente información para publicarla en el Web mediante herramientas como el PHP-3 basándonos en la información que almacenan dos gestores de bases de datos relacionales basados en MySQL en los que se ha realizado un diseño redundante de la base de datos. Así conseguimos distribuir las tareas de administración de un modo lógico y conseguimos una herramienta que nos permitirá administrar todos nuestros servicios independientemente de la topología de nuestro sistema ni del volumen de usuarios que accedan al mismo.

4. Evolución y Trabajos previos

CVM es una evolución de una serie de proyectos anteriores que pretendían demostrar la viabilidad de ofrecer un acceso remoto a la red y a los recursos de la universidad para disminuir los problemas causados por la congestión de las aulas y para permitir el acceso a las mismas de modo remoto durante los periodos en los que permanecían cerradas. Inicialmente, en el proyecto Aula Virtual [1], se partió de un único equipo sobre el cual se llevó a cabo un diseño de todo el sistema, de los requerimientos en cuanto a recursos, información y seguridad que debía reunir el sistema. En base a los resultados obtenidos por este diseño se desarrolló el software apropiado para permitir el acceso remoto mediante una única línea de comunicaciones a nuestro sistema. Con este proyecto se consiguió demostrar la viabilidad de la idea y la posibilidad de llevarla a la práctica con unos mayores recursos que permitieran el uso del sistema por un mayor número de usuarios.

El siguiente paso vino de la mano del proyecto Aula Virtual Multimedia (AVM) [2], en el cual se amplió el sistema a dos equipos y a ocho líneas de acceso externas a través de módems de 33.600 bps. Para soportar este crecimiento no fue necesaria ninguna modificación en el software utilizado; tan sólo hubo que hacer uso del servicio NFS para que los dos equipos tuvieran acceso a los datos requeridos por las aplicaciones desarrolladas. AVM añadió extensiones multimedia al anterior proyecto y una serie de servicios (web, e-mail, listas de discusión), que, además del servicio de acceso remoto son utilizadas plenamente en la actualidad.

4.1.CVM en la actualidad

El proyecto CVM ha recogido todo el trabajo realizado por los proyectos anteriores, extendiendo el concepto de *Aula Virtual* a *Campus Virtual*, e intentando aplicar la misma idea de la que partió Aula Virtual a todo un campus universitario. Para implantar un sistema eficaz de comunicaciones multimedia se han añadido mecanismos que soporten este tipo de flujos de información. Estos mecanismos, utilizados experimentalmente por la red *MBone* (*Multicast BackBone*), ofrecen la ventaja de reducir la carga global de tráfico en la red cuando envían la misma información a varios destinatarios. Este tipo de tráfico requiere la instalación de *routers*, *mrouters,* con capacidades de gestionar tráfico *Multicast*, ya que los mecanismos tradicionales de enrutamiento no son capaces de gestionar este tipo de tráfico.

Aprovechando la topología de nuestra red estamos trabajando en la integración de tráfico IP *Multicast* sobre redes ATM, tecnología hacia la cual estamos migrando toda nuestra red interna. En cuanto a los métodos externos de acceso al sistema, estamos migrando nuestras baterías de módems a sistemas de acceso basados en RDSI.

Como consecuencia de la configuración de CVM y de los servicios que se están ofreciendo, el tráfico de información generado nos está sirviendo para estudiar los flujos de información multimedia y para desarrollar un nuevo modelo de protocolo de transporte para redes *multicast* y para estudiar la integración del tráfico IP sobre redes ATM. En los próximos apartados de este artículo describiremos por completo este sistema. Comenzaremos viendo el diseño de la red en la que se encuentra y los sistemas en los que se basa. Posteriormente estudiaremos el sistema de acceso remoto al sistema y las medidas de seguridad implementadas. Describiremos también las herramientas que estamos utilizando para administrar el sistema y finalmente analizaremos los resultados obtenidos durante el periodo de tiempo en que el sistema ha estado trabajando a pleno rendimiento.

5. Diseño del sistema

En este apartado estudiaremos el diseño del sistema dividiéndolo en dos partes fundamentales:

- Un análisis topológico de la red en que se encuentran los equipos de CVM, las relaciones que existen entre ellos y el uso actual que recibe cada uno de los equipos o conjuntos de equipos ubicados en aulas y laboratorios.

- Un análisis tanto del software como del hardware empleado en el sistema, en el que describiremos los servicios que ofrece cada máquina y la implicación e importancia de cada sistema dentro de CVM.

5.1. Topología de CVM

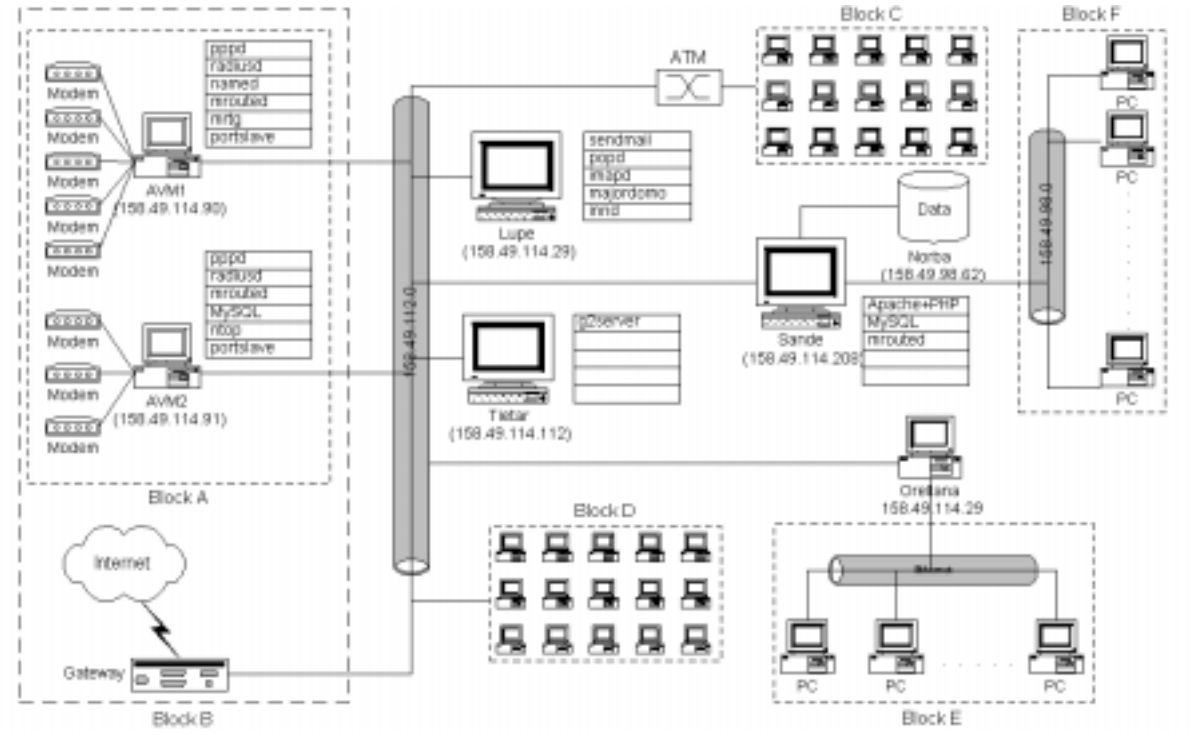

Fig. 1- Topología de Campus Virtual Multimedia

En la *Figura 1* podemos ver parte de la red en la que se encuentran ubicados los equipos que constituyen el sistema CVM. En ella tenemos, además, parte de las aulas y laboratorios a los que CVM facilita el acceso.

El bloque A representa las posibles vías de acceso a CVM y a la red de la escuela. En él podemos ver la conexión a Internet proporcionada por RedIris y, en el bloque B, la batería de ocho módems que permiten el acceso a CVM mediante la RTC.

Los equipos pertenecientes al bloque C pertenecen a una red local ATM conectada directamente al tronco principal de la red del campus; mientras que los equipos incluidos en el bloque D están conectados directamente a la misma red que los equipos de CVM y representan a un gran número de equipos, situados generalmente en los despachos de los profesores.

Los equipos englobados en el bloque E trabajan en red bajo Windows 3.11 y Novell, y son utilizados para asignaturas prácticas en las que no se necesita un hardware de altas prestaciones y para prácticas de asignaturas de redes locales. Para terminar, el bloque F representa a treinta equipos corriendo Linux y Windows 95 conectados a la red a través de una estación SPARC que actúa como router.

El resto de equipos que aparecen en el sistema y que no están englobados en ningún bloque son parte activa del sistema CVM y analizaremos su funcionamiento posteriormente.

5.2. Servicios y organización de CVM

La figura anterior nos muestra además los servicios relacionados con el sistema CVM que está ofreciendo cada uno de los servidores del sistema. Se ha conseguido un alto grado de distribución de los mismos, de manera que la repercusión de un fallo en cualquiera de ellos no sea crítica para el funcionamiento del sistema; además se ha aumentado el grado de utilización de los recursos existentes en la red, con lo que conseguimos reducir los costes totales del proyecto y seguir manteniendo un alto rendimiento del sistema al confiar parte de los servicios del mismo a servidores de gran capacidad de procesamiento.

Veremos el modo en que hemos organizado lógicamente nuestro sistema al mismo tiempo que describimos los servicios que ofrecemos a través de él. De este el lector alcanzará un mayor grado de comprensión de nuestras decisiones de diseño.

5.2.1. Correo electrónico

El servicio de correo electrónico está albergado en un servidor SPARC Station 2 (lupe) con SunOS 4.1.3 como sistema operativo. La primera tarea que hubo que realizar con este servidor fue la actualización del software servidor de correo, *sendmail*, ya que la versión distribuida junto al sistema operativo presenta reconocidos problemas de seguridad. Además se actualizó el servidor POP [4] de la máquina y se instaló un servidor de correo IMAP [5] con el que ofrecemos a nuestros usuarios la posibilidad de consultar el correo directamente desde el Web mediante una aplicación que reside en uno de nuestros servidores.

Los usuarios de CVM disponen de una cuenta de correo para su uso personal y para estar en contacto con los administradores del sistema, que pueden comunicarles periódicamente noticias con relación a los servicios ofrecidos por el sistema.

5.2.2. Listas de distribución

Se instaló un servidor de listas, *majordomo*, en la misma máquina que el servidor de correo para reducir el trasiego de información innecesaria en la red. En la actualidad este servicio es utilizado por los administradores del sistema para comunicarse con los usuarios, para crear grupos de discusión internos y, mediante la justificación oportuna, puede ser utilizado por los usuarios de CVM para crear listas públicas relacionadas con cualquier actividad docente con las cuales intercambiar información con todos los usuarios de Internet.

5.2.3. Servicio de Web

Cuando nos planteamos la necesidad de mantener un sistema de almacenamiento y representación de la información para los usuarios del sistema AVM decidimos utilizar un sistema basado en el Web. Tras realizar algunas aproximaciones para determinar un posible número de accesos al sistema (unos 20000 accesos mensuales en la actualidad), decidimos albergar estos servicios en una máquina con la suficiente capacidad como para soportar holgadamente esta alta carga de trabajo. Finalmente este trabajo se le asignó a un servidor SPARC System 10 que únicamente se utilizaba como *gateway* entre diferentes redes de la escuela. Como ventaja añadida a esta disposición conseguimos además reducir el tráfico en la red cuando se realizan accesos al servidor desde las distintas subredes que conecta este servidor.

Se instaló Apache como servidor Web y un gestor de bases de datos, mSQL, para recuperar la información almacenada en el sistema. Durante la implantación de CVM, este gestor de bases de datos fue reemplazado por el SGBD MySQL.

Cada usuario del sistema CVM puede disponer de un espacio en el servidor Web para albergar sus páginas web y tiene la posibilidad de acceder al SGBD para poder implementar cualquier aplicación docentemente justificada.

En caso de fallo de este sistema o del sistema de almacenamiento de datos, también se producirán fallos sobre el enrutado (*unicast* y *multicast*) que esta máquina realiza entre varias subredes. Por ello, la posibilidad de fallo de este sistema debería ser mínima no sólo por su implicación en el sistema CVM, sino porque es una máquina que realiza una importante labor dentro de la red de la universidad.

5.2.4. Servicios Multimedia

Aprovechando la infraestructura sobre la que se basa el sistema, un servicio de acceso remoto y un sistema de información basado en el web nos propusimos desarrollar un sistema para almacenar y acceder a información multimedia, aunque además intentamos ofrecer un servicio multimedia propio a la comunidad universitaria.

Algunas de las herramientas que hemos conseguido ofrecer a los profesores son:

- La transmisión en tiempo real de clases teóricas y prácticas a los estudiantes que no pueden acudir físicamente a las clases.

- Herramientas tales como una pizarra compartida, que puede ser utilizada tanto por el profesor como por los usuarios remotos para permitirles participar de un modo más activo en las clases prácticas.

- La grabación de clases para poder acceder a ellas en diferido.

- La posibilidad de anunciar nuevas clases transmitidas por la red y permitir el acceso a material grabado previamente.

Una vez que dotamos a nuestro sistema de capacidades *multicasting* pudimos comenzar a utilizar aplicaciones orientadas a la transmisión de audio (*RealAudio, RAT, VAT*) y video (*RealVideo*, VIC, IVC) *multicast*. Todas estas herramientas están a disposición de los usuarios del sistema desde las páginas Web de información del servicio. Es importante resaltar que las transmisiones en diferido no utilizan el modo de transporte *multicast*. Para poder retransmitir una sesión diferida utilizando métodos *multicast*, todos los receptores de la misma deberían solicitar su recepción simultáneamente.

Los anuncios de las sesiones se hacen mediante la herramienta *multicast* SDR. De esta modo, los anuncios de las sesiones se realizan de modo *multicast* a todos los clientes simultáneamente. Hemos desarrollado además un sistema basado en el Web que permite obtener información sobre los anuncios de nuevas sesiones.

La información sobre las sesiones grabadas se almacena en la base de datos de MVC. Dado que esta información es enviada de modo *unicast*, no necesitamos ninguna herramienta *multicast* para acceder a estas sesiones, aunque podríamos acceder también a ellas mediante aplicaciones basadas en *multicasting*. El acceso a estas sesiones grabadas se realiza a través del servidor Web, que se encarga de recuperarlas de la base de datos de MVC.

5.2.5. Servicio de acceso remoto

El sistema Aula Virtual Multimedia ofrecía acceso mediante ocho líneas RTC mediante un software de diseño propio que resultaba complicado de mantener y de escalar en caso de aumentar las capacidades del sistema. Por ello, una de las modificaciones realizadas por el proyecto CVM fue actualizar el sistema de acceso remoto para conseguir ofrecer una alto grado de escalabilidad, que fuera totalmente distribuido y que garantizara unos correctos niveles de tolerancia a fallos.

Las líneas telefónicas que ofrecen acceso al sistema están agrupadas mediante un *dispositivo de salto*. Este dispositivo agrupa todas las líneas bajo un número principal. Cuando un usuario pretende acceder al sistema, el dispositivo de salto le asigna la primera línea sin ocupar del mismo.

A la hora de elegir el protocolo de conexión a emplear optamos por el protocolo PPP [6] en lugar de SLIP [7], los protocolos básicos de conexión en Internet, debido a que PPP nos permite realizar una negociación dinámica de dirección IP y que, además, soporta un mayor número de algoritmos de compresión sobre los datos a transmitir, con lo que se puede aumentar el rendimiento de las líneas.

Debido a la relativa baja potencia de procesamiento necesitada para procesar las conexiones de estas líneas, optamos por utilizar como soporte hardware adicional dos ordenadores personales con tarjetas serie multipuerto. El sistema operativo instalado en ambos equipos es Linux, ya que, aunque prácticamente todos los sistemas operativos actuales soportan internamente las conexiones PPP, cada uno de ellos modifica levemente el protocolo original [8], y Linux es capaz de manejar todas esas modificaciones en el protocolo mediante actualizaciones y extensiones, con lo que nos aseguramos un alto grado de conectividad con respecto a cualquier otro sistema operativo que trabaje como cliente durante la vida de una conexión. Teniendo además en cuenta que los usuarios remotos pueden ser clientes de aplicaciones *multicast* y que Linux es un sistema operativo gratuito, lo consideramos como la mejor elección.

Para facilitar la configuración de los clientes, se desarrollaron una serie de páginas web[17] que explican a los usuarios cómo configurar sus equipos para acceder a CVM.

Aunque utilizamos módems de tan sólo 33.600 bps, lejos de las prestaciones que ofrecen los módems actuales, nuestras líneas están optimizadas para soportar la compresión hardware V.42, con lo que el ancho de banda disponible es aprovechado mejor. Además nuestros servidores Linux habilitan algoritmos de compresión software soportados por el protocolo PPP que aumentan aún más las prestaciones de nuestras líneas. En un futuro migraremos esta tecnología a RDSI, con lo que podremos ofrecer unos mayores anchos de banda y una mayor calidad en el tráfico de información multimedia contra las conexiones de los usuarios remotos.

Para mejorar los tiempos de respuesta de nuestras conexiones remotas consideramos la aplicación de técnicas para disminuir los tiempos de respuesta en las resoluciones de nombres contra servidores DNS [10, 11]. Para ello instalamos un servidor DNS[9] en una de las dos máquinas encargadas de dar conexión remota. Este servidor DNS se comporta como servidor de nombres secundario de la zona en la que está comprendido dentro de la universidad, por lo que realmente se comporta como una caché.

Cabe preguntarse el porqué de no haber instalado un servidor DNS en cada una de las máquinas encargadas de dar acceso remoto. Esta configuración no mejoraría el rendimiento del sistema, sino lo contrario porque los datos almacenados en la caché de un único servidor estarían distribuidos entre todos los servidores DNS, con lo que aumenta la posibilidad de peticiones fallidas y con ello el aumento medio de tiempo en la resolución de las peticiones. Además, como los equipos encargados del acceso remoto están conectados directamente a través de una red ethernet de 10Mbps, el tiempo de resolución de una petición satisfactoria entre uno de los servidores y el servidor corriendo el daemon DNS es prácticamente despreciable.

6. Mecanismos de acceso remoto

Hasta ahora hemos comentado la disposición lógica y física de los equipos encargados de dar acceso remoto a nuestro sistema, pero hemos obviado todos los procesos de autentificación, control y auditoría que se llevan a cabo en el sistema. El acceso telefónico se convierte en una nueva vía de acceso a la red de la universidad y, potencialmente, en un nuevo punto débil del sistema frente a ataques externos, por lo que deberemos de habilitar todos los mecanismos necesarios para asegurarnos que las posibilidades de ataque por este nuevo punto sean mínimas, y en caso de que se produzcan causen un mínimo impacto al funcionamiento de nuestro sistema y al resto de la red de la universidad. Además deberíamos disponer de un conjunto de aplicaciones que nos permitieran controlar el uso que los usuarios del sistema están dando a los recursos que se les están ofreciendo.

Dado que los objetivos principales de este proyecto eran la implantación de todos los servicios citados anteriormente, no se realizó inicialmente ningún esfuerzo por dotar al sistema de un control de seguridad eficiente. El único módem del que se disponía no suponía un riesgo para nuestro sistema, por lo que se implementó una aplicación muy rudimentaria que era la encargada de dar acceso a la red de la universidad.

Cuando instalamos la batería de ocho módems aparecieron algunos puntos débiles que no se habían descubierto con la configuración básica descrita anteriormente. El sistema presentaba una correcta capacidad de escalabilidad, pero siempre que la batería de módems fuera controlada por un único equipo. La utilización de ocho módems nos obligó a utilizar dos ordenadores para controlar el acceso remoto. Los módems se distribuyeron equitativamente entre los equipos, lo que nos obligó a hacer que todo nuestro sistema de autentificación fueran compartidos por todos los equipos servidores PPP del sistema. Este punto implicaba que todos los archivos de datos con la información de los usuarios, de sus cuentas y los archivos de registro debían ser compartidos mediante NFS[15], lo cual se convertía en un punto vulnerable del sistema[16].

El sistema de acceso remoto de AVM recibe en la actualidad una media de 800 llamadas mensuales, aun estando en fase experimental. Debido al incremento en el volumen de usuarios (de 12 a cerca de 100 en la actualidad) y al proceso de migración que está realizando el proyecto Campus Virtual Multimedia, nos dimos cuenta de que el sistema de control y gestión de los equipos encargados de ofrecer acceso remoto no podía seguir funcionando con una aplicación débil ante ataques externos, con una baja escalabilidad y que, además, no estaba diseñada para trabajar en entornos distribuidos.

Tras replantearnos el funcionamiento del sistema actual y definir los requerimientos de nuestro nuevo sistema y las necesidades de CVM, fuimos capaces de identificar una serie de características que nuestro nuevo sistema debería reunir.

- Ha de ser un sistema fácilmente escalable y eficiente.
- Debe estar basado en el modelo cliente-servidor para poder adaptarlo a entornos distribuidos.
- Finalmente, este sistema debería ser transparente tanto para el usuario final como para el sistema operativo.

Todos estos requisitos nos llevaron a escoger RADIUS[13] como modelo de autentificación porque cumple holgadamente con los requisitos que establecimos y porque, además, proporciona al sistema una serie de características que le dan un valor añadido como herramienta de gestión:

- Puede centralizar todos los mecanismos de autentificación y autorización del sistema CVM (e-mail, acceso a cuentas UNIX, acceso remoto) utilizando las características PAM (Pluggable Authentication Modules) de los sistemas UNIX que forman CVM.
- Su capacidad de funcionamiento con un SGBD relacional.

- Un diseño capaz de tolerar fallos en el sistema de un modo eficiente.

- Las comunicaciones entre cliente y servidor se realizan mediante UDP, con lo que se reduce el tráfico en la red.

- Ofrece una detallada auditoría [14] sobre las conexiones de los usuarios al sistema.

Los sistemas de autentificación basados en RADIUS se organizan en clientes y servidores. En la figura 2 podemos ver los equipos de CVM que toman parte en el proceso de autentificación de una llamada entrante. En ella también representamos los servicios relacionados con esta tarea que ejecuta cada máquina.

Los clientes RADIUS, *portslave*, que utilizamos son programas encargados de atender las llamadas telefónicas y autentificar a los usuarios llamantes contra nuestro servidor RADIUS. Por supuesto, todo el intercambio de información entre clientes y servidores se realiza utilizando mecanismos de encriptación basados en algoritmos MD-5.

El servidor RADIUS más utilizado de nuestro sistema está funcionando sobre la máquina AVM2, y su misión es responder las peticiones de los clientes. El servidor tiene capacidad para reconocer a clientes autorizados, por lo que un intento de petición de conexión por parte de un equipo ajeno al sistema es ignorado.

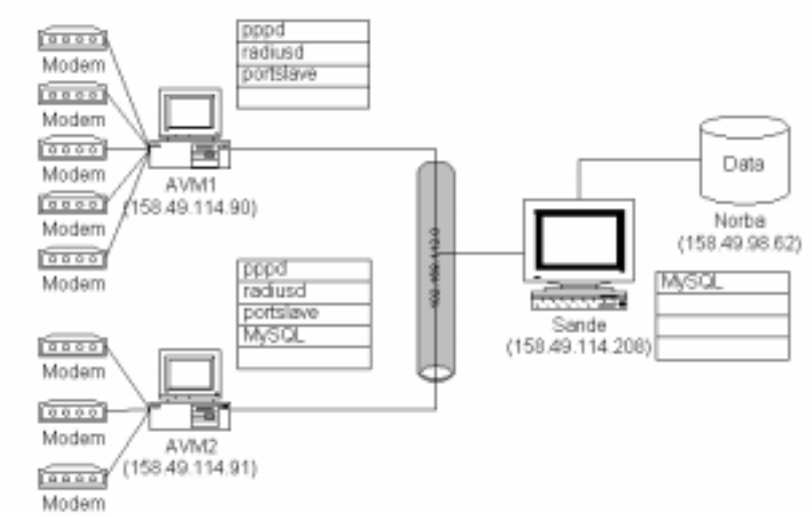

Fig. 2- Equipos de CVM implicados en el control de acceso remoto al sistema

Todos los usuarios que tienen permiso para acceder a los recursos de CVM tienen un perfil asociado que se almacena en un gestor de bases de datos SQL (MySQL). Como vemos en el esquema de la figura 2, tanto los servidores RADIUS como los SGBD aparecen duplicados en diferentes máquinas. Esta organización aumenta la tolerancia a fallos en el sistema tal y como veremos a continuación.

6.1. Organización lógica del servidor de acceso remoto

Podemos distinguir tres elementos que intervienen en los mecanismos de autentificación del sistema: clientes y servidores RADIUS y el SGBD relacional que guarda los perfiles de los usuarios de CVM. Podemos ver el modo en que el sistema procesa una petición en la figura 3.

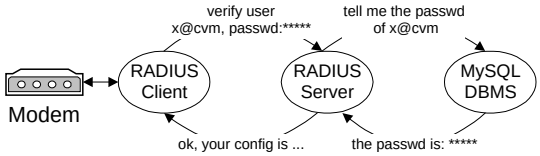

Fig. 3- Procesamiento de una petición de conexión en un sistema RADIUS

El módem es atendido por un cliente RADIUS que pide al servidor que verifique si el usuario está dado de alta o no en el sistema. El servidor genera una consulta SQL contra el SGBD para recuperar la información correspondiente al usuario que se desea autentificar. En caso que este esté en el sistema, el SGBD devolverá su perfil de usuario, que el servidor RADIUS utilizará para configurar la conexión solicitada por el servidor. En nuestro sistema se ha modificado esta organización simple para aumentar la tolerancia a fallos del sistema tal y como veremos a continuación.

Las características del protocolo RADIUS permiten la existencia de un servidor principal y de servidores secundarios. Como ya hemos dicho anteriormente, nuestro primer servidor, que no el principal, está ubicado en la máquina AVM2, mientras que el servidor secundario funciona sobre AVM1. Como los perfiles de usuario se almacenan sobre el SGBD de AVM2, esta disposición reduce el tráfico de información en la red y por ello mejora los tiempos de respuesta del servidor.

Las líneas telefónicas están asignadas consecutivamente a los equipos. El primero de ellos, AVM1, atiende a las cinco primeras, mientras que AVM2 se hace cargo de las tres últimas. Los clientes RADIUS que funcionan sobre AVM1 consideran el servidor RADIUS de AVM2 como servidor principal, y al de su propia máquina como el servidor secundario. Los clientes RADIUS de AVM2 tan sólo tienen especificado como servidor el que corre en la misma máquina que ellos.

Las bases de datos que almacenan los perfiles de los usuarios están replicadas en AVM2 y en Sande. Esta última base de datos es utilizada por el servidor RADIUS de AVM1 para autentificar a los usuarios del sistema. A la base de datos de AVM2 tan sólo se puede acceder desde el propio equipo, mientras AVM1 y AVM2 tienen acceso a la base de datos de Sande. Esto refuerza la seguridad de nuestro sistema, ya que restringe el acceso a los datos de cada usuario a únicamente los servidores RADIUS que intervienen en la autentificación.

Utilizando esta configuración conseguimos que el sistema sea capaz de funcionar correctamente en los siguientes casos:

- Las tres máquinas activas: Los clientes de AVM1 autentifican contra el servidor de AVM2.
- AVM1 y AVM2 activas: Igual que en el caso anterior.
- AVM1 y Sande activas: Los clientes de AVM1 intentan resolver las peticiones contra AVM2; al no obtener respuesta, las peticiones se redirigen contra el servidor local que autentifica contra la base de datos de Sande.
- AVM2 activa: El dispositivo de salto al que están asociadas las líneas detecta que las cinco primeras líneas no son atendidas y pasa la llamada a las líneas de AVM2, que facilita el acceso a la red a través de sus servidores locales.

6.2. Distribución de los servicios de autentificación y control en CVM

Una interesante característica de los sistemas RADIUS es que un servidor puede actuar como *proxy* contra otros servidores, con lo que podemos definir una estructura jerárquica de servidores que se repartan el volumen total de usuarios del sistema (en nuestro campus hay 20000 usuarios potenciales del mismo) y que permitan ser

administrados independientemente pero formando parte del mismo sistema. Una posible organización en nuestro sistema vendría dada del hecho de la separación geográfica existente entre los campus de Cáceres y Badajoz. La administración del servicio de acceso remoto podría dividirse con una correcta situación de los servidores RADIUS, manteniendo siempre la misma configuración para los usuarios sin depender del campus en el que se encuentren, tal y como vemos en la figura 4.

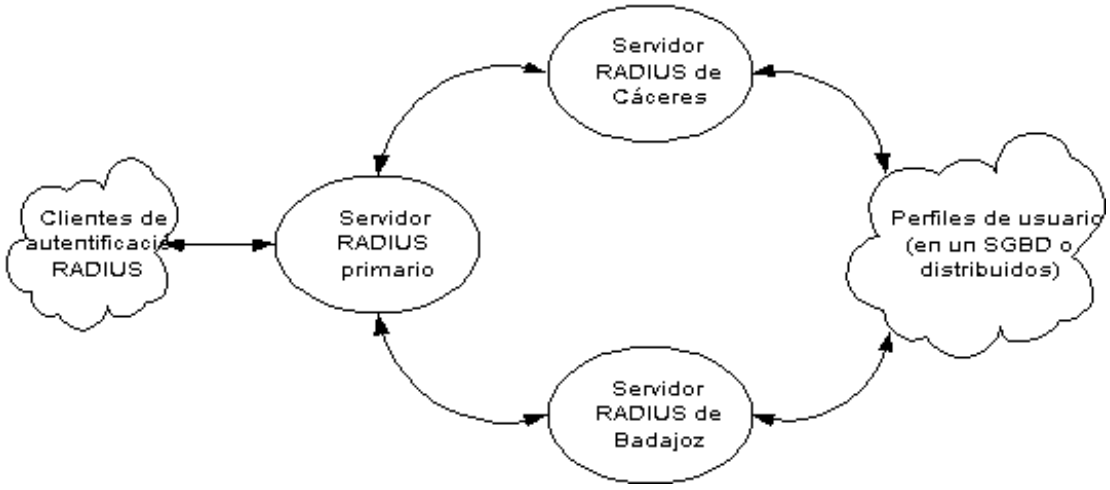

Fig. 4- Una correcta ubicación de los servidores reduce el tráfico de la red y facilita el mantenimiento del sistema

Esta organización de los servidores favorece el crecimiento y la implantación del sistema en todo el campus. Del mismo modo, los clientes RADIUS y las baterías de módems podrían estar en distintas ubicaciones, pudiendo seguir distintos criterios para su agrupamiento.

6.3. Trabajos a partir del sistema de acceso remoto

El tráfico generado por el servicio de acceso remoto nos permite estudiar los flujos de información para desarrollar una propuesta de protocolo de transporte *multicast* que pueda soportar flujos de datos híbridos. Un flujo de datos híbrido es un flujo de información en el que cada uno de los cuatro parámetros del *QoS* [12] (throughput, delay, jitter, reliability) tienen la misma importancia. En la actualidad los protocolos de transporte *multicast* dan mayor importancia a los tres primeros parámetros, lo que los hace adaptables para la transmisión de información *multicast*, o son diseñados para ofrecer mayor fiabilidad a costa del resto de parámetros del *QoS*. Esta última clase de protocolos de transporte *multicast* los hace útiles para la transmisión de ficheros y para la ejecución de transacciones.

Hemos añadido un servicio de *callback* dentro del sistema de acceso remoto. Los usuarios que pueden acceder a este servicio tan sólo tienen que llamar al sistema y autentificarse. El sistema de acceso remoto termina la conexión y devuelve la llamada al número predefinido por el usuario, que deberá tener su módem dispuesto para recibir la llamada. Con este mecanismo conseguimos que el usuario pueda acceder al sistema eliminando el coste de la llamada telefónica, ya que este corre a cargo de la universidad.

Debido a que el tráfico de información generado por el servidor de acceso remoto puede estar dirigido hacia una red local ATM de nuestro sistema y al uso mayoritario del protocolo IPv4 en CVM, podemos estudiar la integración del protocolo IP sobre redes ATM, además de plantear nuevas propuestas de protocolos de transporte. Utilizando herramientas como *ntop* obtenemos la información necesaria sobre el tráfico que se mueve en la red generado por el sistema, que es el que utilizamos en nuestros análisis.

7. Administración del sistema

Con las estructuras lógicas propuestas anteriormente para el sistema de acceso remoto basado en RADIUS, la administración del sistema se puede hacer muy complicada, teniendo además en cuenta el resto de servicios que intervienen en el sistema. En este apartado veremos una propuesta de herramienta de administración de un sistema de basado en RADIUS y en un SGBD relacional como sistemas principales de autentificación y autorización que permite controlar todos los servicios ofrecidos por el sistema desde un sencillo interfaz basado en el web. Esta aplicación [], aún en fase de desarrollo, aumenta la eficiencia de los administradores del sistema, y con ella se puede administrar todo el sistema CVM o una parte del mismo, tal y como vimos en el apartado anterior.

El sencillo interfaz de usuario (diseñado en PHP 3.0) oculta una potente aplicación que se ajusta a todos los requerimientos de nuestro sistema. Mediante ella ofrecemos al administrador un control total sobre los usuarios de CVM. Algunas de las herramientas de trabajo que ofrece al administrador son la gestión total de cuentas de usuario en el sistema: altas, bajas o modificaciones del perfil de acceso de los mismos, la gestión a un alto nivel de los servicios del sistema y obtención de resultados de funcionamiento del mismo mediante un completo conjunto de herramientas estadísticas que permiten a los responsables del sistema ser conscientes de la evolución y los requerimientos del mismo día a día. Además facilita el acceso a los registros de actividades de los usuarios del sistema para realizar tareas de auditoría.

Como ejemplo de esta aplicación podemos fijarnos en la figura 5, en la que se está haciendo uso de esta aplicación para realizar un control de los usuarios dados de alta en el sistema.

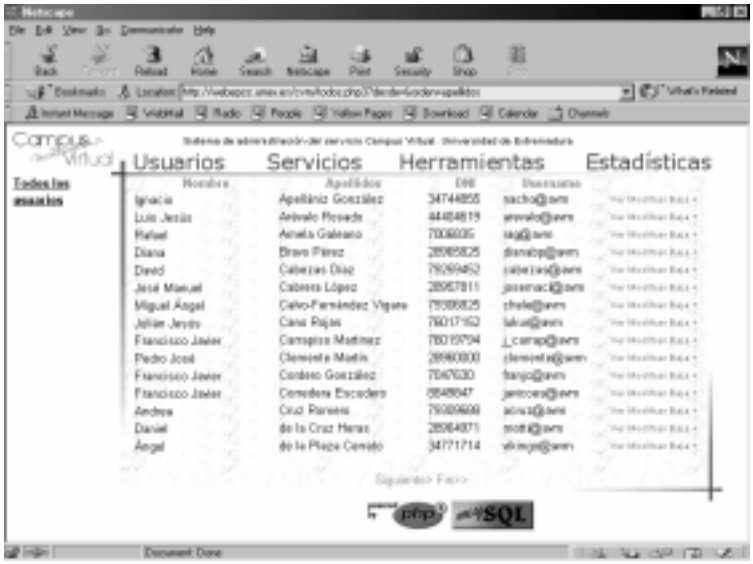

Fig. 5- La herramienta de administración simplifica el mantenimiento del sistema y la gestión de los usuarios

8. Estadísticas del sistema

Debemos ser capaces de calcular la aceptación de los servicios que estamos ofreciendo por parte de los usuarios del mismo y, además, conocer la repercusión que tiene el tráfico de información generado por CVM con respecto al resto del tráfico generado por la red de la universidad.

La herramienta de gestión citada anteriormente es capaz de generar informes de uso periódicos y de mostrar gráficos de utilización del sistema, y además integra los datos generados por la herramienta *mrtg* que sirve para

obtener información de equipos de la red mediante el protocolo SNMP. Además, el uso de ntop como sniffer, nos permite medir volúmenes de tráfico específicos por puesto, servicio o protocolo, con lo que el administrador del sistema dispone de información suficiente para detectar puntos a corregir o depurar. Toda esta información, interpretada en conjunto es útil, además, para realizar análisis de tráfico y para avanzar en la investigación de nuevos protocolos.

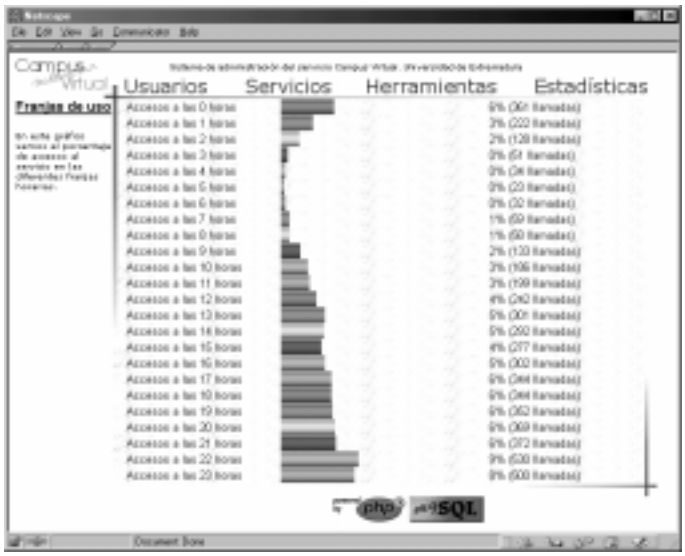

Fig. 6- Conexiones remotas al sistema agrupadas por horas

En la figura 6 podemos ver un gráfico de accesos por franja horaria generado por la aplicación de gestión, mientras que en la figura 7 tenemos un gráfico generado por la aplicación *mrtg* que nos informa acerca de la evolución del tráfico generado por el equipo AVM1 durante el último año.

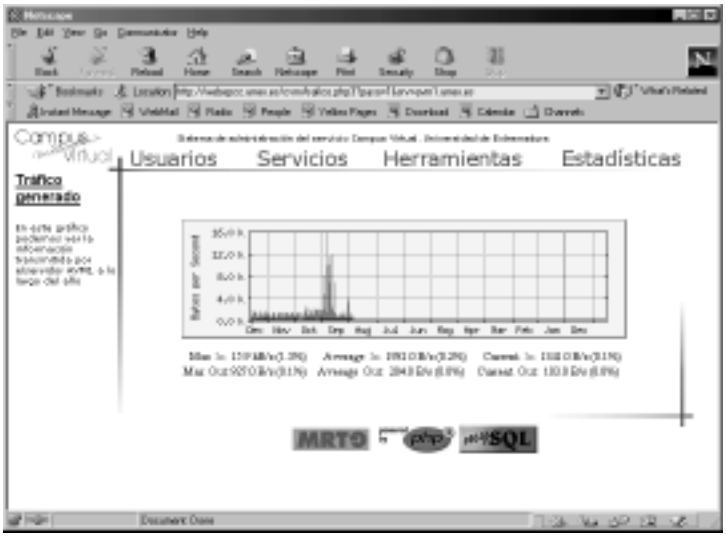

Fig. 7- La integración de mrtg en la aplicación nos permite llevar un sencillo control del tráfico de la red

En la figura 8 podemos ver el análisis del tráfico generado en la subred en la que se encuentran los equipos de CVM.

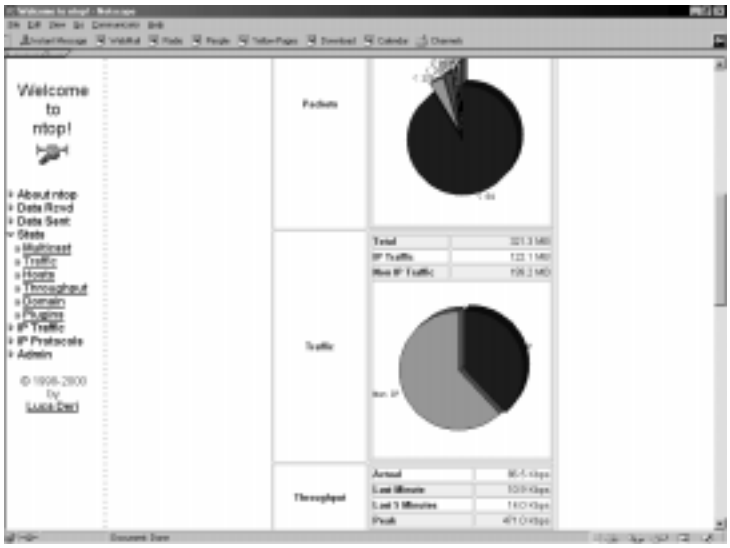

Fig. 8- Parte del análisis realizado por ntop del tráfico de la subred de CVM

9. Trabajos futuros

Basándonos en el sistema propuesto en este artículo se intentará crear una *Freenet* para toda la comunidad universitaria, la cual, al mismo tiempo nos será útil para avanzar modelos de protocolos de transporte de información multimedia. La información que se mueva en esta red nos será útil para realizar análisis de los flujos de la información y para justificar la migración del *BackBone* de la red del Campus a tecnología ATM. En cuanto a la seguridad de acceso a nuestra red a través de Internet se propondrá el uso de tecnologías de VPN que nos permitirá controlar aún más los niveles de acceso a nuestro sistema.

10. Conclusiones

Con el desarrollo del proyecto CVM hemos demostrado la posibilidad de crear un sistema distribuido de bajo coste que aprovecha al máximo los recursos de la red de nuestra universidad, que ofrece un conjunto de servicios multimedia inexistentes hasta el momento en nuestra Universidad, los cuales se pueden aplicar perfectamente a otros entornos. Hemos conseguido, además, que nuestro sistema sea fácil de mantener, que cumpla unos mínimos de seguridad aceptables y que sea fácilmente escalable debido a la flexibilidad que nos ofrece su arquitectura distribuida. Además ofrecemos una plataforma óptima para el desarrollo de nuevas vías de investigación y amplio abanico de posibilidades por los que el sistema puede seguir creciendo.

11. Referencias

[1] J.L. González S., A.Gazo C, A. Plaza M.,A. Gómez M. y M. Sánchez A. “Multimedia Virtual Classroom”, Proceedings INFONOR 98, Antofagasta (Chile) 1998.

[2] J.L. González S., A.Gazo C, J.L. Gordo R. y M. Sánchez A. “Multimedia Virtual Campus. An approach to new research in Tele-Formation and Tele-Working”. Proceedings Advances in Multimedia and Distance Education ISIMADE’99, Baden-Baden (Alemania), august 1999.

[3] J.L. González, A.Gazo, J.L. Gordo, J.M. Murillo. “MVC: Technical description of a proposal in multimedia and distance education”. International Symposium on Telemedicine and Teleeducation in Practice. Marzo 2000 - Kosice (Eslovaquia).

[4] Post Office Protocol. RFC 1460.

[5] Interactive Mail Access Protocol. RFC 1203.

[6] Nonstandards for transmission of IP datagrams over serial lines: SLIP. RFC 1055.
[7] The Point-to-Point protocol. RFC 1661.
[8] PPP Vendor Extensions. RFC 2153.
[9] Domain names – implementation and specification. RFC 1035.
[10] Clarifications to the DNS Specification. RFC 2181.
[11] Negative Caching of DNS queries. RFC 2308.
[12] Steinmetz, R., and Wolf, L.C.,"Quality of Service: Where are We?," IWQOS'97, pp.211-221, (1997).
[13] Remote Authentication Dial In User Service: RADIUS. RFC 2138.
[14] RADIUS Accounting. RFC 2139.
[15] NFS Version 3 Protocol Specification. RFC 1813.
[16] Wietse Venema. "Murphy Laws and Computer Security". Eindhoven University of Technology. 1998
[17] http://webepcc.unex.es/avm AVM web site