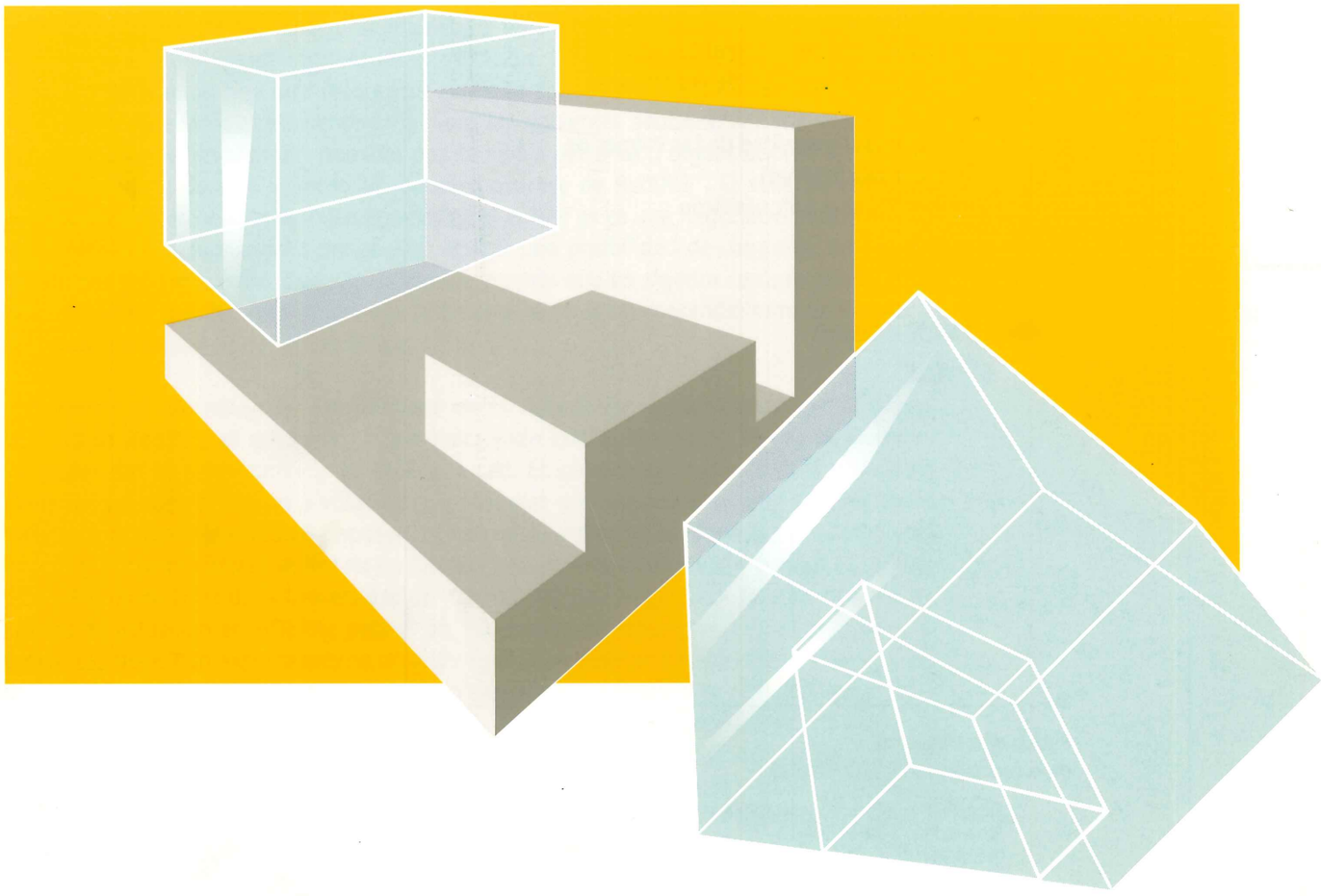
Red IRIS

Plan Nacional de I+D

Boletín de la red nacional de I+D, RedIRIS.

nº 31



nº 31
Abril 1995

Boletín de la
Red IRIS

Sumario

Publicación trimestral
de la red nacional de I+D, RedIRIS.

Edita: Centro de Comunicaciones CSIC/ RedIRIS
Serrano, 142 . 28006 Madrid.
Tel.: (91) 5855150 Fax: (91) 5855146
Director: Víctor Castelo Gutierrez
Coordinación: María Bolado
Filmación: .CROMOTEX

Producción: Javier Pascual
Portada: Clara Alvarez Cabiró
Autoedición: María Bolado
Imprime: Closas Orcoyen, S.L.
Distribución: B.D. Mail, S.A.
ISSN: 1133-5408
Depósito legal: M. 15844-1989

Presentación

Victor Castelo

En las Jornadas Técnicas de RedIRIS 94 expusimos nuestras ideas sobre la evolución de la red en cuanto a cambio de los nodos (en número y paso a IP) y aumento de la velocidad de las líneas. Ya a lo largo del 94 y del 95 se realizaron algunas intervenciones puntuales en cuanto a nuevos enlaces, subidas de velocidad y cambio de X.25 a IP, pero el día H del supercambio parece que no llega nunca. Todo se debe a la existencia de transcendentes y por tanto largas negociaciones con los operadores que nos tienen atados de manos y que al final nos están resultando interminables, de manera que algo que en estas mismas fechas del 94 podría haber sido razonable, en el 95, y más según han ido aumentando las necesidades, nos está suponiendo auténticos colapsos en algunos puntos.

Pero parece que las negociaciones, que podríamos decir incluso que comenzaron a finales del 93, se están acabando, esperemos que con resultados muy interesantes y que pronto podamos realizar el "cambiazo". Me atrevería a decir que para el verano podría estar ya casi todo operativo.

Se siguen produciendo solicitudes de afiliación a RedIRIS al ritmo habitual de los últimos tiempos (elevadísimo). Estas suponen normalmente el establecimiento de un enlace al nodo más próximo de RedIRIS, pero en algunos casos, por razones obvias, la conexión se produce a través de otra organización ya conectada como es el caso de coexistencia en determinados campus. Pues bien, esto que es algo lógico debe ir acompañado de una solicitud de la nueva organización a RedIRIS para obtener la autorización. En la cláusula décima de los nuevos acuerdos de afiliación hay una referencia explícita sobre este tema en la que se dice lo siguiente: " ... quedan expresamente prohibidas las siguientes acciones: Facilitar el acceso a cualquiera de los servicios proporcionados por RedIRIS a personas u organizaciones ajenas a la entidad signataria de este acuerdo sin permiso expreso de RedIRIS". El acuerdo entre las organizaciones interconectadas y que comparten el enlace es ya una negociación entre ambas partes. Hacemos estas manifestaciones para aclarar una posibilidad de conexión, tal vez no conocida por todo el mundo. Desgraciadamente creemos que en algunos casos se pueda estar dando el caso de que se estén ofreciendo servicios a terceros sin consentimiento de RedIRIS e incluso con la publicación de tarifas de uso.

Comentando el contenido de este número en su Actualidad comenzamos con la nueva estructura de RedIRIS, en evolución, y que sobre todo está aumentando en capital humano para poder dar el mejor servicio posible a la red. El cambio del nodo central se realizó felizmente sin contratiempos y sobre todo pensamos que supone una gran mejora en la infraestructura que Telefónica ha dispuesto como red de acceso hasta nuestras instalaciones. El conocido y eficiente Listserv se instala en RedIRIS gracias a la colaboración de Cati Parals del CESCA y Fernando Durá de la Universidad de Valencia. Miguel Angel Sanz hace un relación de las líneas de actuación en SIDERAL para el 95, esperemos que muy pronto sean llevadas a la práctica. Las News han experimentado un gran empuje en cuanto a los medios humanos y de equipamiento dedicados de los que esperamos den como resultado una evidente mejora del servicio. Por último noticias sobre la reunión de EuroCAIRN en Ginebra, que por cierto la próxima será organizada por RedIRIS, y sobre todo algo que creemos muy importante: la firma por nuestra parte de la participación el proyecto TEN-34 por expreso encargo del Plan Nacional de I+D para el establecimiento de una red europea de 34/155 Mbps subvencionada por la UE. Esto supondrá un nuevo avance significativo para nuestras conexiones internacionales y desde luego servirá tanto de revulsivo a nuestras conexiones internas como de puente a las incipientes redes de alta velocidad de las Comunidades Autónomas.

Las nuevas afiliaciones suponen normalmente el establecimiento de un enlace al nodo más próximo de RedIRIS, aunque en algunos casos la conexión se produce a través de otra organización ya conectada, siempre previa autorización de RedIRIS.

Nuestra intención es dedicar ciertos recursos humanos,para comenzar a coordinar la seguridad desde todos sus niveles entre nuestras instituciones afiliadas.

En Enfoques el primer artículo de Enrique Rubio y Antonio Ocón nos expone la clara apuesta de la Universidad de Las Palmas de Gran Canaria por las Nuevas Tecnologías de la Información que se está desarrollando con una evolución constante en todos los aspectos de su red (ULPnet): infraestructura interna y externa de comunicaciones (con un paso muy reciente de gigante de 9.600 bps a 2 Mbps), correo electrónico, en el que han demostrado siempre una gran experiencia en la aproximación a la plataforma de uso personal, accesos remotos muy elaborados, etc. Todo ello con el ánimo de proporcionar, a todos los niveles, el mejor acceso a los recursos disponibles en cada momento y con metas muy altas pero tremendamente coherentes.

Eloy Portillo y Lourdes López en su artículo nos ofrecen una primera entrega sobre seguridad en redes telemáticas, haciendo un repaso de las soluciones propuestas por organismos de normalización, con una especial introducción sobre Internet y sus problemas estándar. En realidad revisan un tema que como estamos viendo tiene cada vez más importancia o al menos deberíamos dársela. A este respecto, como ya señalábamos en las Jornadas Técnicas de San Sebastián, nuestra intención es dedicar ciertos recursos humanos, ya previstos entre las nuevas incorporaciones que mencionamos en la Actualidad, para comenzar a coordinar la seguridad desde todos sus niveles entre nuestras instituciones afiliadas y comenzar así esta etapa con una nueva ventana de servicio.

Víctor Castelo
Director de RedIRIS
Victor.Castelo@rediris.es

Estructura funcional

Debido a una reestructuración interna en RedIRIS, a continuación informamos de los cambios que han tenido lugar, aunque tal y como se puede ver, aún hay algunos puestos que no están cubiertos. Una vez se haya finalizado esta evolución daremos más detalles sobre el estado final de los diferentes servicios.

La relación de tareas y personas en la actualidad queda tal y como aparece en la tabla adjunta.

Dirección:	Víctor Castelo
Secretaría:	Mónica Núñez
Gerencia y Admón.:	Ana Mª Dotor Eduardo Funcia
Difusión:	María Bolado
Area Rel. Institucionales:	**Manuel Rincón**
Area Aplicación:	**Celestino Tomás** Clara Alvarez Juan Antonio García Jesús Sanz de las Heras Javier Masa Técnico de S.I. (*)
Area Red:	**Miguel Angel Sanz** Susana Gayo Juan Carlos Moreno Operador de red (*)

CERT - Técnico de sistemas (*)
Operador - Técnico de microinformática (*)

Nota: los puestos con (*) se encuentran en proceso de selección

(Víctor.Castelo@rediris.es)

Traslado Nodo Central ARTIX

El pasado día 10 de febrero, se procedió a realizar el traslado del Nodo Central de la red ARTIX desde su ubicación original en la Escuela Técnica Superior de Ingenieros de Telecomunicación de Madrid hasta RedIRIS/CSIC en la C/ Serrano, 142.

Varios han sido los motivos que han dado lugar a este traslado:

- Una vez que la red de transporte se encontraba en fase de producción ya no tenía mucho sentido el que estuviera en un Centro Docente e Investigador como lo es el DIT.UPM.

- Puesto que los servicios de news y correo electrónico se encuentran centralizados en RedIRIS se parecía lógico que éstos estuvieran lo más cerca posible de los usuarios, el centro de la red.

- Se veía lógico que ante la próxima migración hacia una red IP se centralizaran ambas gestiones, la de la red ARTIX como red de transporte y el Servicio SIDERAL.

Durante el año 1994, el Centro de Gestión de ARTIX proyectó en colaboración con RedIRIS el traslado del Nodo Central y la migración hacia una red más eficiente con protocolo de transporte IP. Es la tendencia que han seguido la mayoría de las redes de nuestro entorno.

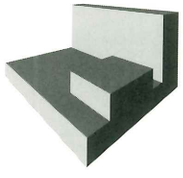
La idea inicial sobre el traslado era realizarlo a lo largo del año 94. La imposibilidad de llevarlo a cabo surgió de Telefónica.

Una de las tareas iniciales y más importante era dotar a los locales de RedIRIS con la infraestructura necesaria.

Telefónica comenzó con las obras de infraestructura a mediados del mes de noviembre y estas finalizaron poco antes del día definitivo del traslado. La primera fecha que dio Telefónica para realizar el traslado, fue la del día 27 de enero y ésta fue difundida por RedIRIS a todos sus usuarios, así como al resto de redes con conectividad. Dos días antes de esta fecha, el 25 de enero, Telefónica comunicó a RedIRIS la imposibilidad de realizarlo por falta de tarjetas de modems y nos emplazó definitivamente al día 10 de febrero.

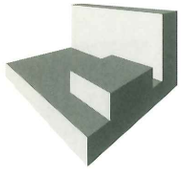
El viernes 10, comenzamos el traslado. con incertidumbre en cuanto a la duración del mismo y si todas las líneas trasladadas iban a funcionar en ese mismo día, aunque teniamos todo un fin de semana por delante para tratar de resolver los problemas que se produjesen.

Estructura funcional



Traslado Nodo Central ARTIX

Traslado Nodo Central ARTIX



Cambio de la línea de Iberpac a RedIRIS

Servicio de LISTSERV

Para realizar el traslado, Telefónica destacó a 8 técnicos muy cualificados por lo que pudimos observar, y todo transcurrió según los planes de última hora.

Como puntos destacados, amén del propio traslado, se instalaron líneas de nuevos centros y nos sorprendieron trasladando también, en el mismo paquete, la línea de Iberpac de 64 Kbps. que inicialmente nos aseguraron que no se podría trasladar y había que mantener en el DIT. Esto hizo que, una vez levantada la red, tuviéramos que modificar urgentemente, las tablas de encaminamiento hacia/desde Iberpac.

Sobre las 12:30 encendimos los equipos y empezaron a levantarse líneas a medida que Telefónica iba configurándolas en un MD (Multiplexor/Demultiplexor) instalado en RedIRIS. Este es un equipo que se instala en las centrales de Telefónica y de él parten los bucles de abonado. Ahora nuestro bucle de abonado tienen una distancia física a la central de Telefónica de escasamente 3 metros. Esto, es de suponer que estabilizará en gran medida las líneas que cuelgan del nodo central.

Sobre las 14:30 h. estaban levantados todos los enlaces salvo la línea MAD-CEDEX, que se aprovechó la desconexión del traslado, para utilizando el mismo bucle de abonado del lado del CEDEX, instalar una nueva línea de 64 Kbps. sustituyendo a la anterior de 9.600 bps. Estaba operativa sobre las 17 horas aproximadamente.

El número de líneas trasladadas fue de 24 tal y como se detalla a continuación.

- 2 de 2 Mbps.
- 2 de 256 Kbps.
- 16 de 64 Kbps.
- 1 de 19.200 bps.
- 3 de 9.600 bps.
- 1 de Iberpac

Actualmente el nodo de Madrid de RedIRIS acoge un total de 38 líneas punto a punto y ya no todas llegan a la red ARTIX, las nuevas instaladas se conectan a equipos de SIDERAL, montándose protocolo IP directamente.

Ciertamente salió mejor de lo esperado. Tuvimos que confiar en Telefónica y aunque fue a la segunda vez, ésta no nos defraudó.

Desde aquí, quiero agradecer el buen hacer de sus técnicos y resaltar la labor de planificación que se llevó a cabo en colaboración entre el centro de gestión de ARTIX y RedIRIS.

(JuanCarlos.Moreno@rediris.es)

Cambio de la línea de Iberpac a RedIRIS

A continuación se indican los servicios que se verán afectados por la eliminación de la línea de Iberpac de 9.6 Kbps. de RedIRIS.

a) El acceso a los servicios centrales de buzones.

El NRI cambia de 215067410 a 217098505

b) La dirección del MTA central EAN de RedIRIS.

El NRI cambia de 2150674105 a 2170985055

c) La dirección del MTA central en UNIX de RedIRIS
La dirección del servidor X.500 central de RedIRIS
El acceso público X.500 de RedIRIS, user=directorio

El NRI pasa de 2150674103 a 2170985053

d) El acceso a la utilidad TELPAD.

El NRI pasa de 2150674100 a 2170985050

Ambas direcciones serán validas durante todo el mes de marzo, eliminándose la antigua el 31 de marzo de 1995.

(JuanCarlos.Moreno@rediris.es)

Servicio de LISTSERV

Ya está operativo en RedIRIS el servicio de listas distribución LISTSERV conectado al backbone internacional de Listservs. Este servicio no es nuevo ya que los usuarios de la comunidad de RedIRIS han estado disfrutando hasta el momento del LISTSERV ubicado en el CESCA en la máquina EBCESCA1.BITNET (puigmal.cesca.es). A partir de ahora residirá en una máquina de RedIRIS.

Los servicios que ofrecerá a la comunidad son:

- Acceso a las listas de distribución internacionales de múltiples temas conectados al backbone LISTSERV.

- Creación bajo demanda de los usuarios de RedIRIS de listas de distribución de ámbito internacional. La solicitud de creación de estas listas se deberá enviar a: listman@rediris.es

- Servidor y almacén de documentos y revistas que pueden consultarse mediante GOPHER o FTP.

- Todas las listas estarán conectadas con grupos de NEWS. Algunos se preguntarán las diferencias entre las listas de distribución y los grupos de news pero esto ya es digno de un amplio debate.

• ¿Qué es el LISTSERV ?

LISTSERV es un gestor de listas de distribución bastante evolucionado, depurado y extendido. Tanto es así que en cada país existe un backbone de LISTSERV consistente en una red de nodos con este paquete. Esta red LISTSERV tiene unos algoritmos de encaminamiento de mensajes que evita congestiones, tráfico redundante e incecesario. Veamos un ejemplo: un mensaje enviado a una lista de distribución residente en Japón con 5 usuarios de la Comunidad RedIRIS llegará solamente en una ocasión a España, donde el LISTSERV de RedIRIS se encargará de distribuirlo a estos 5 usuarios.

En LISTSERV existen tres clases de usuarios: **Postmasters** (responsables de la instalación y operación), **Propietarios** (responsables de la gestión de una lista) y **Suscriptores** (reciben mail y ficheros de una lista). Aquellos que no estén suscritos a ninguna lista pueden coger copias, preguntar,... a un LISTSERV.

En LISTSERV existen dos clases de listas de distribución: **Internacionales** son las visibles en toda la red LISTSERV y **locales** son listas propias de cada Comunidad no visibles desde otros nodos. Es decir el LISTSERV de RedIRIS puede crear listas locales internacionales y nacionales. Las que los usuario puede solicitar a RedIRIS son listas locales visibles en la red. Las listas locales de ámbito nacional serán fundamentalmente las de coordinación de los servicios de RedIRIS y de otros temas de interés.

• ¿Cómo se utiliza ?

El diálogo con el LISTSERV es vía correo electrónico, poniendo el comando en el cuerpo del mensaje. Todos los comandos se enviarán a:

listserv@listserv.rediris.es

aunque también se puede dialogar con el listserv de otros nodos.

Los comandos para empezar son:

help ->	Los comandos más utilizados
list global ->	Información de todas las listas que existen en la red de LISTSERV. Hay que tener cuidado ya que es un mensaje bastante grande.
list global xyz ->	Información de todas las listas que contengan en su identificación o descripción las letras xyx.

Ej.: si deseo solicitar todos las listas relacionadas con temas de Química, pondré: list global chem

Obtención de ficheros de interés general sobre LISTSERV:

get listpres memo ->	Recibirás un fichero de presentación.
get listserv memo ->	Recibirás un fichero con información general de LISTSERV.

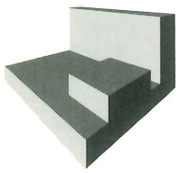
(Jesus.Heras@rediris.es)

SIDERAL/Internet: líneas de actuación 1995

A lo largo de 1994 el Servicio de Interconexión de Redes de Area Local IP de RedIRIS (SIDERAL/Internet) ha continuado con la fuerte demanda que viene experimentando desde sus orígenes en 1991. La eclosión de nuevas aplicaciones en Internet, cada vez más potentes y más sencillas de utilizar, ha atraído nuevos usos y usuarios. La aplicación "asesina" (de ancho

Servicio de LISTSERV

SIDERAL/Internet: líneas de actuación 1995



SIDERAL/Internet: líneas de actuación 1995

de banda) por excelencia, el WWW, ha capturado en su tela de araña a veteranos y neófitos. El crecimiento ha sido explosivo en todos los aspectos, pero especialmente significativo en lo que a tráfico cursado se refiere: el tráfico IP internacional se multiplicó por cuatro entre enero y mayo y en diciembre superaba los 10 Gbytes diarios (en dias laborables) suponiendo alrededor del 98% del total de tráfico internacional de RedIRIS. Otros datos de la situación a finales de 1994 son: 125 organizaciones conectadas, más de 300 redes IP en las tablas de encaminamiento de SIDERAL, 27.000 equipos conectados (registrados en el DNS).

A lo largo de 1995 es necesario llevar a cabo importantes actuaciones que permitan seguir ofreciendo un servicio de calidad a un número cada vez mayor de instituciones y usuarios con aplicaciones cada vez más sofisticadas a la vez que "hambrientas" de recursos.

Esquemáticamente, las líneas de actuación para 1995 en SIDERAL/Internet, han de ir encaminadas hacia los siguientes objetivos:

- Mejor infraestructura de transporte (mayores anchos de banda)
- Evolución tecnológica y arquitectónica
- Nuevo equipamiento
- Nuevas formas de acceso
- Nuevos servicios
- Nuevo Centro de Gestión de Red

Un requisito imprescindible a corto plazo es la disponibilidad de mayores anchos de banda a nivel nacional y en esa dirección se está trabajando, con el fin de disponer cuanto antes de capacidades entre 256 Kbps y 2 Mbps en las líneas troncales de la red, que puedan absorber la demanda creciente y permitir la introducción gradual de nuevos servicios multimedia.

Junto con el aumento de capacidad de los enlaces troncales es necesario acometer lo antes posible importantes cambios tecnológicos y arquitectónicos. La situación actual del servicio, representada en la figura 1, en la que el tráfico IP ha de ser encapsulado sobre X.25, tanto en el "backbone" como en los accesos de los centros, para poder ser transportado sobre ARTIX, supone una considerable pérdida de eficiencia en el aprovechamiento del ancho de banda disponible (tanto mayor cuanto mayor sea éste), así como una merma importante en cuanto a prestaciones se refiere. Debido al fuerte incremento del tráfico IP (porcentualmente cada vez más importante frente a los demás protocolos) se hace urgente llevar a cabo una migración de tecnología en la infraestructura de transporte de RedIRIS, adquiriendo el equipamiento que permita cursar el tráfico de interconexión de redes IP dominante en modo nativo (directamente sobre el nivel de enlace), tanto en los enlaces troncales como en los de acceso de los centros, eliminando el nivel de conmutación X.25 existente que supone una sobrecarga cada vez mayor e impide una utilización óptima de los costosos medios de transmisión subyacentes.

TOPOLOGIA ACTUAL IP/X.25

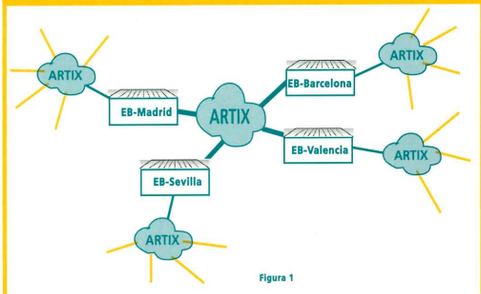


Figura 1

El objetivo para 1995 queda reflejado en la figura 2, en el que los nuevos nodos de la red están constituidos por los equipos encaminadores ("routers") multiprotocolo de SIDERAL, que pasan a constituir el nuevo núcleo de la red donde se conectan tanto los enlaces troncales como los enlaces de acceso de las distintas instituciones. El protocolo de nivel de enlace entre nodos puede ser el más óptimo en función del equipamiento disponible (HDLC propietario, por ejemplo, en el caso de ser todos del mismo fabricante). Todo enlace internodal dispone de backup por RDSI convenientemente dimensionado en función de su capacidad. El tráfico X.25 se

TOPOLOGIA FUTURA

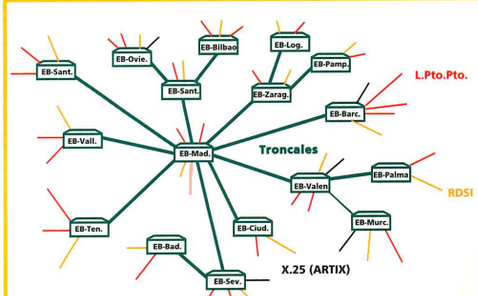


Figura 2

transporta mediante encapsulación sobre TCP/IP (al revés de lo que hasta ahora se venía haciendo) según el método descrito en el RFC 1623. De esta forma se asegura una migración "no traumática", manteniéndose allí donde sea necesario el servicio X.25 de ARTIX (cuyos conmutadores quedan durante la transición "detrás" de los routers de SIDERAL) de forma transparente al usuario, aunque los enlaces troncales hayan sido ya migrados a IP nativo.

El acceso de las organizaciones al servicio podrá ser mediante línea dedicada (a velocidades entre 9.6 y 2048 Kbps), RDSI (acceso básico) o a través de terceros ya conectados de los que se obtenga permiso de tránsito. En cuanto a los protocolos de nivel de enlace a usar entre el equipo de acceso del centro y el nodo más próximo de RedIRIS, podrá ser HDLC propietario (el más eficiente si los dos equipos son del mismo fabricante) u otro estandarizado (PPP, LAPB, X.25) que mejor se adapte al equipamiento del centro.

En función de los requerimientos específicos los nuevos nodos pueden estar compuestos por varios equipos interconectados entre sí, todos bajo la gestión de RedIRIS. La figura 3 presenta, por ejemplo, un nodo compuesto por 3 routers interconectados entre sí mediante una red de routing nodal (una ethernet o ethernet conmutada por ejemplo). Los centros acceden al servicio mediante RDSI o línea dedicada entre su router de acceso y el nodo (salvo en el caso del centro o centros ubicado(s) físicamente en el mismo lugar que el nodo que lo harán de forma local mediante un cable serie). La figura también muestra la situación del conmutador X.25 de ARTIX preexistente en el nodo una vez migrados los enlaces troncales, que queda detrás del router hasta la migración de la totalidad de los accesos X.25 existentes, manteniendo de esta forma el anterior servicio X.25 mientras sea necesario.

ESTRUCTURA DE NODOS

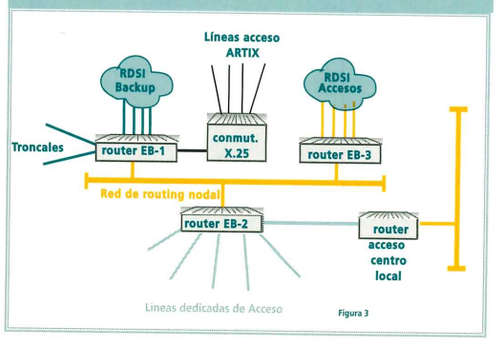
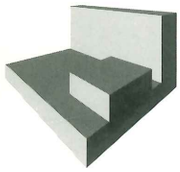


Figura 3

Evidentemente uno de los objetivos primordiales de la migración de tecnología en la red es que sea lo más transparente posible de cara a las organizaciones actualmente usuarias, con interrupciones mínimas del servicio y la menor intervención e inversión posible por su parte. Todos los nuevos accesos se harán desde este momento y en la medida de lo posible de acuerdo con la nueva tecnología/topología. La migración de los enlaces troncales se llevará a cabo lo antes posible (en cuanto se disponga del equipamiento necesario), pues de ella se derivarán los mayores beneficios en cuanto a mejora de prestaciones en la red, al igual que ha ocurrido con el paso a IP nativo del acceso internacional de 2 Mbps el pasado mes de noviembre y de la línea de 2 Mbps entre Barcelona y Madrid el pasado mes de Febrero, con un considerable aumento del "throughput" y una drástica reducción de los tiempos de respuesta (superior a un orden de magnitud en el caso del tráfico IP internacional). Por último, la migración de los accesos existentes en la actualidad exige un estudio caso por caso en coordinación con las organizaciones implicadas; en algunos casos será más sencilla e inmediata, mientras que en otros más complejos la transición podrá durar más tiempo.

Otro aspecto importante son los protocolos de encaminamiento a emplear. Como protocolo de routing externo se seguirá empleando BGP4, adoptado por RedIRIS el pasado mes de abril y necesario para la implementación de CIDR ("Classless Inter Domain Routing") a nivel global de Internet y, por tanto, para aportar nuestro granito de arena de cara a un aprovechamiento eficiente del espacio de direcciones IP y a una reducción significativa del tamaño de las tablas de encaminamiento en Internet. En cuanto al protocolo de encaminamiento a emplear en el acceso de los centros, se seguirá, como hasta ahora, estudiando cada caso para adaptarse dentro de lo posible al que mejor satisfaga sus necesidades o preferencias (estático, RIP, IGRP, etc.). La actuación más importante a acometer en este terreno es el cambio del protocolo interno de routing dentro de SIDERAL, pasando del empleado actualmente IGRP (protocolo de "vector distancia") a uno más avanzado que

SIDERAL/Internet: líneas de actuación 1995



SIDERAL/Internet: líneas de actuación 1995

Servicio de News

ofrezca una convergencia mucho más rápida y un menor consumo de ancho de banda. El protocolo de vector distancia mejorado EIGRP ("Enhanced IGRP") desarrollado por CISCO presenta estas ventajas además de otras como facilidad de configuración y migración desde IGRP y menor consumo de CPU y memoria en los routers frente a otras opciones como OSPF (protocolo de "estado de línea").

Para 1995 también está prevista la especificación e introducción de un servicio piloto de IP Multicast. Esta técnica permite un aprovechamiento eficiente del ancho de banda en la transmisión de aplicaciones multimedia en tiempo real (audio y videoconferencia por ejemplo), frente a técnicas basadas en "unicast" (con multicast un paquete IP puede ser enviado a un grupo de ordenadores, en lugar de tener que enviar un paquete a cada miembro del grupo). En la medida en que el equipamiento lo permita, la implementación de este servicio se efectuará usando los propios routers de SIDERAL, mediante el empleo del recientemente desarrollado PIM ("Protocol Independent Multicast"). Esto optimizaría al máximo los recursos de la red, al ser tratado el tráfico de multicast por los mismos equipos que encaminan el tráfico unicast normal. La introducción de este servicio piloto permitirá la distribución de MBONE (sistema para la transmisión de aplicaciones multimedia en tiempo real por Internet) a aquellos centros que cumplan los requisitos necesarios para ello (fundamentalmente ancho de banda y recursos materiales y humanos suficientes).

Paralelamente a todo lo anterior se va a proceder a la creación del denominado Centro de Gestión de Red de RedIRIS (RedIRIS NMC), que se encargará de las funciones de diseño y planificación de red, actividades del NIC (RedIRIS NIC y ES-NIC) y tareas de operación de red (Centro de Operación de Red o RedIRIS NOC). Es importante que este último, encargado de tareas críticas como son, entre otras, la monitorización en todo momento de la red y de sus prestaciones, ofrezca una cobertura lo más extensa posible. En este sentido, el objetivo para 1995 es disponer del personal necesario para que el Centro de Operación de Red tenga una cobertura de 12 horas diarias de 8 a 20 durante todo el año de lunes a viernes (salvo festivos), pudiendo contactar con él fuera de ese tiempo mediante correo electrónico, fax y contestador automático.

Dentro de las labores de registro delegado de Internet en España (ES-NIC), desempeñadas como es sabido por RedIRIS, el objetivo es continuar con la estrecha colaboración con el RIPE NCC, así como con el asesoramiento y coordinación de proveedores Internet en España (actividad cada vez más importante debido al incipiente surgimiento de nuevos de ellos). En este sentido, es intención de RedIRIS, en aras a una adecuada evolución de la parte española e Internet, la especificación y puesta en marcha de un punto neutro de interconexión (NIX) que ofrezca un medio físico para el intercambio de tráfico entre proveedores a nivel nacional (los proveedores habrán de cumplir una serie de requisitos para poder ser considerados como tales y conectarse al NIX). La existencia de un NIX sólo facilita el medio físico pero no elimina la necesidad de acuerdos entre los proveedores para el intercambio de sus tráficos respectivos.

Por último, conviene destacar que no todo se reduce a mejoras en equipamiento, tecnología e infraestructura de la red, puesto que la demanda crece y crecerá a un ritmo muy superior a lo que pueden hacerlo las inversiones; es importante la concienciación por parte de todos de la necesidad de optimizar el uso de los recursos disponibles mediante una adecuada información/formación del usuario final y el establecimiento por parte de los centros y de RedIRIS de todos aquellos mecanismos que permitan acercar la información al usuario y hacer una utilización lo más eficiente posible de la red.

(Miguel.Sanz@rediris.es)

Servicio de News

News: grupos distribuidos de discusión. Desde sus comienzos allá por el año 1979 han experimentado un crecimiento impresionante, pasando de unas decenas de grupos, a los más de 6.000 que existen en la actualidad. Esto supone una cantidad desorbitada de información que navega por la Internet, siendo capaz de colapsar líneas y servidores. Y esto último fue precisamente lo que ocurrió en RedIRIS cuando decidimos implantar un servidor que abasteciese a todos los nodos nacionales, en un intento de conseguir un mejor aprovechamiento de los recursos de la red académica y evitar la saturación de nuestro enlace internacional con tráfico duplicado. La máquina que soportaba la mayor parte de los servicios

ofrecidos por RedIRIS se vio, de esta forma desbordada con esta nueva aplicación.

Como solución a este problema, a finales del año pasado el servicio de News se migró a una "máquina dedicada". Se trata de una SPARCserver 20 con una capacidad de 2 Gb. para el almacenamiento de artículos y significó una mejora del servicio ofrecido por RedIRIS.

Durante la primera quincena del mes de enero del presente año, el servicio estaba completamente desplazado a la nueva máquina, y el espacio de almacenamiento se aumentó a 3,5 Gb., lo que nos permitió mantener durante una semana los artículos de los 5.900 grupos de News que recibimos.

Estas medidas, resolvieron el primer problema, que era poder abarcar el volumen de información y soportar la carga del sistema que representan las News. Al mismo tiempo tenía lugar el cambio de nuestro enlace de 2 Mbs a EMPB, que pasaba de encapsular IP sobre X.25 a convertirse en un enlace IP nativo, y suponía, de este modo, una mejora muy significativa en el tráfico de News. Esto nos permite recibir puntualmente una media de 80.000 artículos diarios, que llegan a nosotros desde Suiza (SWITCH) y la Universidad de Oregón.

Actualmente nuestra principal preocupación es la saturación del ancho de banda de las líneas nacionales, repercutiendo de manera importante en la eficacia del servicio de News. Este es el principal problema con el que nos encontramos, provocando importantes atascos en el envío vía NNTP, principalmente con aquellos nodos que disponen de enlaces de 64 Kbs.

Ante este problema se nos plantean dos soluciones no excluyentes: por un lado la migración de estas líneas a IP nativo, como medida más inmediata y a más largo plazo el aumento del ancho de banda de los enlaces troncales de ARTIX; y por otro lado, el envío comprimido de News a los nodos secundarios. Sobre este último punto, hemos estado estudiando las diversas posibilidades (sendbatches, rshell,...) y buscando un procedimiento fiable, sólido y eficaz. En esta línea de actuación agradecemos la colaboración de Javier Achirica, de la Universidad de Valladolid que está realizando un importante trabajo en la mejora del software INN para el envío comprimido. En breve esperamos tener asegurada la estabilidad de este procedimiento, en particular su tolerancia a la perdida de conectividad, de manera que podamos utilizarlo contra los nodos más saturados.

Como medio de información a administradores y usuarios, hemos instalado un punto central de información sobre el servicio, constituido por un servidor WWW y Gopher cuyos URL's son:

http://news.rediris.es/
gopher://news.rediris.es:70/

en ellos se pueden consultar las estadísticas semanales del tráfico de News entre el servidor central de RedIRIS, y los distintos nodos, tanto nacionales como internacionales. Estamos trabajando en mejorar este servicio, para que permita, principalmente a los administradores, disponer de una información técnica, útil y actualizada de la evolución y estado del servicio de News.

Finalmente, tenemos en perspectiva aumentar el espacio de almacenamiento de artículos, para evitar que una caída temporal de una línea o servidor, produzca una perdida de artículos como consecuencia de su pronta expiración.

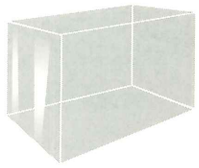
(Juan.Garcia@rediris.es)

Reunión de EuroCAIRN

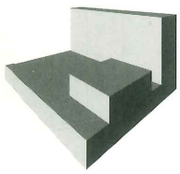
Los pasados días 19 y 20 de enero se celebró en Ginebra la primera reunión del año de todos los delegados nacionales del proyecto EuroCAIRN. Se trataba de una reunión importante tanto por los temas a tratar como por ser prácticamente la última de la primera fase de EuroCAIRN, que como se ha informado en ocasiones anteriores, consiste en la definición de un modelo paneuropeo de red de alta velocidad incluyendo los aspectos económicos del proyecto.

El primer tema tratado fue la posible elección de un suministrador de servicios de una red como la que se proyecta, que tendría que ser un grupo con capacidad multinacional. Se ha detectado interés en DANTE, UNISOURCE, British Telecom y France Telecom por el momento.

Servicio de News



Reunión de EuroCAIRN



Reunión de EuroCAIRN

Red paneuropea de alta velocidad

En segundo lugar DANTE presentó el borrador de su estudio, que resulta bastante amplio, e incluye modelos económicos de financiación de la red. Este borrador es por el momento un documento interno de trabajo y por lo tanto confidencial.

Se pasó a continuación a una discusión sobre las fuentes de financiación de la futura red. Estas fuentes procederán de:

- Comisión Europea (50%)
- Países participantes (50%)

El proyecto continuará en su segunda fase siendo Eureka, para permitir la participación de los países del Este.

En el caso español, el dinero será aportado por Telefónica I+D, el CDTI y la CICYT. Hasta que no se determinen exactamente las tareas a realizar no se podrá dar una cantidad exacta, no obstante por parte española se piensa en unos 500.000 ecus para el primer año, como continuación a la creación de la red.

La próxima reunión de EuroCAIRN será la última de la primera fase y en ella previsiblemente se aceptará el estudio de DANTE, con las modificaciones oportunas y se distribuirá el trabajo. Por último se discutirá el enlace de EuroCAIRN con la nueva iniciativa de la UE que se comenta también en este boletín.

(Manuel.Rincon@rediris.es)

Red paneuropea de alta velocidad

El proyecto EuroCAIRN va a permitir definir de una manera clara la futura red europea de alta velocidad, en principio para redes académicas. Esta red para ser implementada precisa financiación. Por ello la UE ha lanzado una iniciativa de destinar 30 Mecus en los años 95-96 para poder materializar la red.

El día 13 de febrero se presentó esta iniciativa a las redes nacionales académicas y a los operadores (Telefónica, France Telecom, Unisource, etc). Los operadores nacionales pueden participar en esta iniciativa.

El 20 de febrero hubo una reunión esta vez sólo de redes nacionales y se comisionó a DANTE para que realice la propuesta a la Unión Europea.

El Proyecto será financiado en parte por la UE con fondos de los Programas ESPRIT y TELEMATICS. La cantidad que la UE aporta no cubre más que un 30% del coste previsto para esta red. El resto deberá ser sufragado por las redes nacionales y los operadores que finalmente decidan ser patrocinadores.

En estos momentos se está trabajando en España para conseguir ir conjuntamente al proyecto. En el siguiente boletín informaremos de cual ha sido el resultado final y qué pasos son previsibles para el futuro.

(Manuel.Rincon@rediris.es)

Seguridad en redes telemáticas Parte I: La problemática de la seguridad

Eloy Portillo y Lourdes López

Introducción

Desde el comienzo de la utilización de sistemas informáticos ha existido una gran preocupación por la seguridad de la información que almacenan. Los responsables de los Centros de Cálculo se han encargados desde hace años de implantar controles de seguridad física frente a intrusos interesados en acceder a los sistemas, y han realizado periódicamente copias de seguridad para prevenir posibles pérdidas involuntarias de los datos.

La extensión de la microinformática y de las redes de ámbito mundial que interconectan recursos informáticos de todo tipo, ha hecho que los peligros que sufre la información almacenada en los diversos sistemas crezcan considerablemente y se diversifiquen, y que las medidas adoptadas internamente en los Centros de Cálculo resulten insuficientes.

La extensión de la microinformática y de las redes de ámbito mundial, ha hecho que los peligros que sufre la información crezcan considerablemente y se diversifiquen.

En los últimos meses no sólo la prensa especializada en informática, sino todos los medios de difusión han hecho eco del futuro de las autopistas de la información, cuyo embrión está representado por la red Internet. A raíz de la interconexión del mundo empresarial a esta red, viaja por ella y se almacena información de todo tipo, que abarca desde noticias o cotilleos, documentos, normas y aplicaciones informáticas de libre distribución hasta complejas transacciones que requieren medidas de seguridad que garanticen la confidencialidad, la integridad y el origen de los datos.

La escucha electrónica, que permite la obtención y posible manipulación de información privada, y los sabotajes realizados tanto por atacantes externos como internos, están causando últimamente la pérdida de grandes cantidades de dinero.

El objetivo de la criptografía es el de proporcionar comunicaciones seguras sobre canales inseguros.

Pero, ¿cómo controlar el acceso indebido a aplicaciones y a la información almacenada?, ¿cómo garantizar la integridad o la confidencialidad de la información que viaja a través de las redes?, ¿cómo comprobar de manera fiable que el emisor y el receptor de una información son realmente quienes dicen ser?, o ¿cómo garantizar que el emisor no niegue haber enviado algo y el receptor no niegue haberlo recibido?.

En este artículo se pretende dar una respuesta a estos interrogantes. El artículo está dividido en dos partes, en la primera parte titulada *La problemática de la seguridad* se presenta un estudio de las soluciones que proponen los organismos de normalización para evitar los posibles ataques y operaciones ilegales a los que pueden estar sometidas las redes telemáticas. Estas soluciones consisten en dotar a las redes de una serie de servicios de seguridad que utilizan en su mayoría técnicas criptográficas como principal herramienta básica. La primera parte de artículo concluye reflejando de forma práctica los problemas de seguridad que tiene Internet y presenta la soluciones que se pueden adoptar. En la segunda entrega, titulada *Entornos seguros,* se describen con más detalle estas soluciones, planteándose cómo debe ser un entorno de seguridad. Se presentará también el resultado de varias experiencias sobre aplicaciones seguras que se han realizado en el Departamento de Ingeniería y Arquitecturas Telemáticas (DIATEL) de la E.U.I.T. de Telecomunicación de la UPM.

La criptografía como herramienta base de la seguridad

El objetivo de la criptografía es el de proporcionar comunicaciones seguras sobre canales inseguros, es decir, permitir que dos entidades, bien sean personas o bien aplicaciones, puedan enviarse mensajes por un canal que puede ser interceptado por una tercera entidad, de modo

La criptografía no es en sí la seguridad, sólo es la herramienta básica que utilizan mecanismos más complejos para proporcionar, además de confidencialidad, otros servicios de seguridad.

que sólo los destinatarios autorizados puedan leer los mensajes. Pero la criptografía no es en sí la seguridad, sólo es la herramienta básica que utilizan mecanismos más complejos para proporcionar, además de confidencialidad, otros servicios de seguridad.

La criptografía viene utilizándose desde la Antigüedad para enviar mensajes bélicos y amorosos de forma confidencial. Uno de los primeros criptosistemas conocidos es el llamado *cifrado de Cesar*, que consiste en sustituir cada letra del mensaje original por otra, la cual está determinada por la tercera siguiente en el alfabeto.

Este tipo de criptosistemas que basan su seguridad en mantener secreto el algoritmo son fáciles de descifrar utilizando medios estadísticos. En la actualidad sólo los emplean los aficionados mientras que en medios profesionales han sido sustituidos por criptosistemas que basan su seguridad en mantener en secreto una serie de parámetros, llamados claves, de forma que el algoritmo puede ser conocido. Entre este tipo de criptosistemas hay que distinguir entre los de *Clave Secreta*, en los que el emisor y el receptor de un mensaje utilizan la misma clave para cifrar y descifrar respectivamente el mensaje, la cual deben mantener ambos en secreto, y los de *Clave Pública* en los que cada usuario está en posesión de un par de claves, una que mantiene en secreto y otra que es pública.

El criptosistema de clave secreta más utilizado es el *Data Encryption Standard (DES) [1]* desarrollado por IBM y adoptado por las oficinas gubernamentales estadounidenses para protección de datos desde 1977. Este criptosistema consiste en un algoritmo de cifrado-descifrado de bloques de 64 bits basado en permutaciones, mediante una clave, también de 64 bits. El algoritmo es fácil de implementar tanto en hardware como en software, sin embargo presenta problemas respecto a la distribución de claves, ya que dos usuarios que quieren comunicarse deben seleccionar una clave secreta que deberá transmitirse de uno a otro y respecto al manejo de claves, ya que en una red de n usuarios, cada pareja necesita tener su clave secreta particular, lo que hace un total de $2^{n(n-1)}$ claves para esa red.

En 1976 Diffie y Hellman describieron el primer criptosistema de clave pública conocido como el *cambio de clave Diffie-Hellman* [2] que utilizaba una clave doble compuesta por una componente pública y una privada. Con este algoritmo cuando alguien quiere que le envíen un mensaje secreto le envía a su interlocutor su clave pública, el cual la usa para cifrar el mensaje. Sólo el usuario que está en posesión de la componente secreta de la clave puede descifrar el mensaje. Si el mensaje es interceptado, aunque el intruso conozca la componente pública utilizada, no podrá descifrar el mensaje porque no estará en posesión de la componente privada. Con este tipo de algoritmos la clave secreta ya no tiene que transmitirse entre los interlocutores y tampoco es necesario tener claves diferentes para cada pareja de interlocutores, es suficiente con que cada usuario tenga su clave doble con su componente pública y privada.

El más extendido de los sistemas de clave pública fue desarrollado por Rivest, Shamir y Adleman en el MIT en 1977 y se conoce como criptosistema *RSA*. La clave pública y la privada están compuestas por un exponente y un módulo que es producto de dos números primos grandes. La fiabilidad del sistema se basa en que si los primos se escogen lo suficientemente grandes, el proceso de factorización del producto es inabordable en un tiempo razonable, gracias a ello, la difusión de la componente pública no pone en peligro a la privada. El algoritmo de cifrado RSA es reversible, es decir, además de permitir cifrar con la clave pública y descifrar con la privada, permite cifrar con la clave privada y descifrar con la pública. Este modo de cifrado no proporciona confidencialidad ya que cualquiera puede descifrar un mensaje cifrado con una clave secreta al poder obtener siempre la componente pública de su interlocutor, sin embargo el hecho de cifrar un mensaje con la clave secreta de un usuario

implica una identificación del usuario al igual que lo hace una firma, por lo que este proceso se conoce con el nombre de firma digital.

A partir de mediados de los 80 se empezaron a buscar nuevos criptosistemas de clave pública que utilizaran menos cantidad de recursos para generar claves y para cifrar y descifrar. Así, en 1985, EL Gamal propuso un esquema de clave pública basado en la exponenciación discreta sobre un grupo finito de orden n, conocido como criptosistema *El Gamal,* y en la primera mitad de los 90 está progresando el estudio de criptosistemas de *curvas elípticas* en los que las operaciones de multiplicación se sustituyen por sumas y las exponenciaciones por productos.

Los servicios de seguridad

El documento de ISO que describe el Modelo de Referencia OSI, presenta en su Parte 2 una *Arquitectura de Seguridad [3].* Según esta arquitectura, para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas de los siguientes **servicios de seguridad:**

- **Autenticación de entidad par.** Este servicio corrobora la fuente de una unidad de datos. La autenticación puede ser sólo de la entidad origen o de la entidad destino, o ambas entidades se pueden autenticar la una a la otra.

- **Control de acceso.** Este servicio se utiliza para evitar el uso no autorizado de recursos.

- **Confidencialidad de datos.** Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

- **Integridad de datos.** Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor.

- **No repudio**. Este servicio proporciona la prueba ante una tercera parte de que cada una de las entidades comunicantes han participado en una comunicación. Puede ser de dos tipos:

    - **Con prueba de origen.** Cuando el destinatario tiene prueba del origen de los datos.

    - **Con prueba de entrega.** Cuando el origen tiene prueba de la entrega íntegra de los datos al destinatario deseado.

Para proporcionar estos servicios de seguridad es necesario incorporar en los niveles apropiados del Modelo de Referencia OSI los siguientes **mecanismos de seguridad:**

- **Cifrado.** El cifrado puede hacerse utilizando sistemas criptográficos simétricos o asimétricos y se puede aplicar extremo a extremo o individualmente a cada enlace del sistema de comunicaciones.

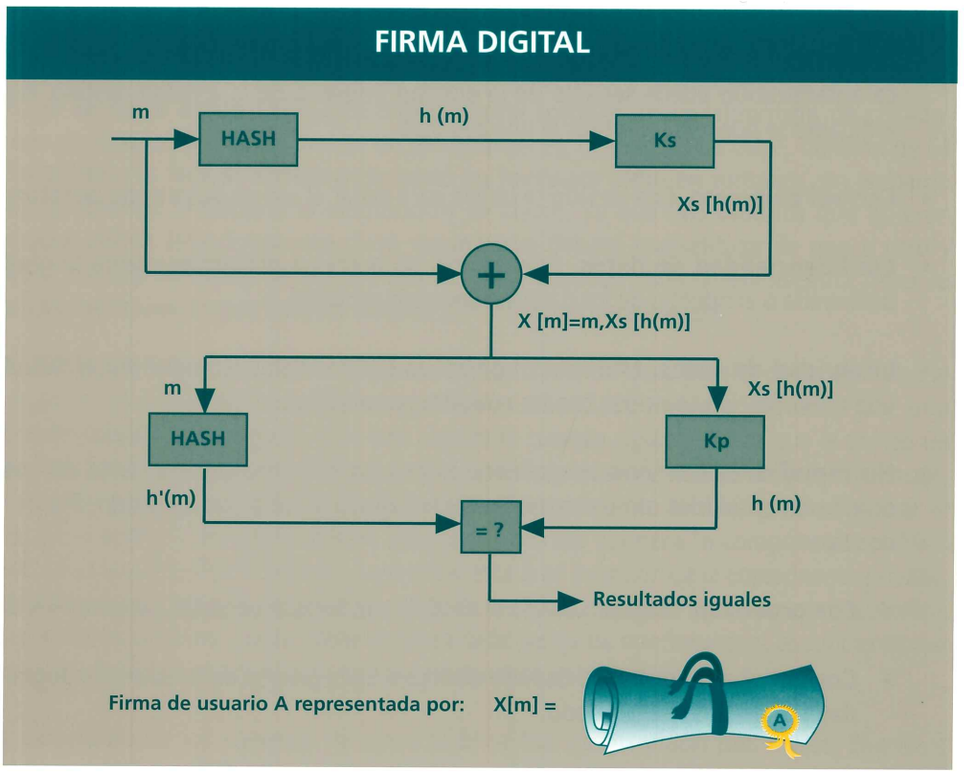
  El mecanismo de cifrado soporta el servicio de confidencialidad de datos al tiempo que actúa como complemento de otros mecanismos de seguridad.

El mecanismo de firma digital soporta los servicios de integridad de datos, autenticación de origen y no repudio con prueba de origen.

- **Firma digital.** Se puede definir la firma digital como el conjunto de datos que se añaden a una unidad de datos para protegerlos contra la falsificación, permitiendo al receptor probar la fuente y la integridad de los mismos. La firma digital supone el cifrado, con una componente secreta del firmante, de la unidad de datos y la elaboración de un valor de control criptográfico.

  La firma digital descrita por ITU y OSI en el *Entorno de Autenticación del Directorio* [4] utiliza un esquema criptográfico asimétrico. La firma consiste en una cadena que contiene el resultado de cifrar con RSA aplicando la clave privada del firmante, una versión comprimida, mediante una función hash unidireccional y libre de colisiones, del texto a firmar.

  Para verificar la firma, el receptor descifra la firma con la clave pública del emisor, comprime con la función hash al texto original recibido y compara el resultado de la parte descifrada con la parte comprimida, si ambas coinciden el emisor tiene garantía de que el texto no ha sido modificado. Como el emisor utiliza su clave secreta para cifrar la parte comprimida del mensaje, puede probarse ante una tercera parte, que la firma sólo ha podido ser generada por el usuario que guarda la componente secreta.



El mecanismo de firma digital soporta los servicios de integridad de datos, autenticación de origen y no repudio con prueba de origen. Para proporcionar el servicio de no repudio con prueba de entrega es necesario forzar al receptor a enviar al emisor un recibo firmado digitalmente.

- **Control de acceso.** Este mecanismo se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee. El control de

acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el enviante está autorizado a comunicar con el receptor y/o a usar los recursos de comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo.

El mecanismo de control de acceso soporta el servicio de control de acceso.

- **Integridad de datos**. Es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad.

  Para proporcionar la integridad de una unidad de datos la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede ser una información suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión.

  Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, alguna forma de ordenación explícita, tal como la numeración de secuencia, un sello de tiempo o un encadenamiento criptográfico.

  El mecanismo de integridad de datos soporta el servicio de integridad de datos.

- **Intercambio de autenticación**. Existen dos grados en el mecanismo de autenticación:

  - **Autenticación simple**. El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.

  - **Autenticación fuerte.** Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta. Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública.

  Para que un usuario confíe en el procedimiento de autenticación, la clave pública de su interlocutor se tiene que obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación. La Autoridad de Certificación utiliza un algoritmo de clave pública para certificar la clave pública de un usuario produciendo así un certificado.

  Un certificado es un documento firmado por una Autoridad de Certificación, válido durante el período de tiempo indicado, que asocia una clave pública a un usuario.

  El mecanismo de intercambio de autenticación se utiliza para soportar el servicio de autenticación de entidad par.

Para que un usuario confíe en el procedimiento de autenticación, la clave pública de su interlocutor se tiene que obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación.

Los protocolos de la Internet fueron diseñados deliberadamente para que fueran simples y sencillos. Esto jugó eficazmente a favor de su implantación generalizada, pero tanto las aplicaciones como los niveles de transporte carecían de mecanismos de seguridad que no tardaron en ser echados en falta.

Seguridad en redes complejas: el caso de Internet

El fenómeno de la extensión de la Internet ha adquirido una velocidad tan rápida y unas proporciones, que el panorama actual y muchos de los efectos que se dan en su seno resultan sorprendentes y difícilmente imaginables hace sólo una década.

Inicialmente Internet nace como una serie de redes que promueven el intercambio de información entre investigadores que colaboran en proyectos conjuntos o comparten resultados usando los recursos de la red. En esta etapa inicial, la información circulaba libremente y no existía una preocupación por la privacidad de los datos ni por ninguna otra problemática de seguridad. Estaba totalmente desaconsejado usarla para el envío de documentos sensibles o clasificados que pudieran manejar los usuarios. Situación ésta muy común, pues hay que recordar que la Internet nace como un contrato del Departamento de Defensa Americano -año 1968- para conectar entre sí tanto las Universidades como los centros de investigación que colaboran de una manera u otra con las Fuerzas Armadas Norteamericanas.

Los protocolos de la Internet fueron diseñados de una forma deliberada para que fueran simples y sencillos. El poco esfuerzo necesario para su desarrollo y verificación jugó eficazmente a favor de su implantación generalizada, pero tanto las aplicaciones como los niveles de transporte carecían de mecanismos de seguridad que no tardaron en ser echados en falta.

Más recientemente, la conexión a Internet del mundo empresarial se ha producido a un ritmo vertiginoso muy superior a la difusión de ninguna otra tecnología anteriormente ideada. Ello ha significado que esta red de redes se haya convertido en "la red" por excelencia. Esto es, el medio más popular de interconexión de recursos informáticos y embrión de las anunciadas autopistas de la información.

Se ha incrementado la variedad y cantidad de usuarios que usan la red para fines tan diversos como el aprendizaje, la docencia, la investigación, la búsqueda de socios o mercados, la

cooperación altruista, la práctica política o, simplemente, el juego. En medio de esta variedad han ido aumentando las acciones poco respetuosas con la privacidad y con la propiedad de recursos y sistemas. *Hackers, frackers, crakers* ... y demás familias han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. Además de las técnicas y herramientas criptográficas antes citadas, es importante recalcar que una componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los gestores de la red. Como ejemplo, en la tabla 1 se recoge una lista exhaustiva de problemas detectados, extraída del libro *"Firewalls and Internet Security. (...)"* [5].

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo.

Lista de peligros más comunes en sistemas conectados a Internet.
Fuente: *"Firewalls and Internet Security. Repelling the Wily Hacker"* [5]

1.- De todos los problemas, el mayor son los fallos en el sistema de passwords.
2.- Los sistemas basados en la autenticación de las direcciones se pueden atacar usando números consecutivos.
3.- Es fácil interceptar paquetes UDP.
4.- Los paquetes ICMP pueden interrumpir todas las comunicaciones entre dos nodos.
5.- Los mensajes ICMP Redirect pueden corromper la tabla de rutas.
6.- El encaminamiento estático de IP puede comprometer la autenticación basada en las direcciones.
7.- Es fácil generar mensajes RIP falsos.
8.- El árbol inverso del DNS se puede usar para conocer nombres de máquinas.
9.- Un atacante puede corromper voluntariamente la caché de su DNS para evitar responder peticiones inversas.
10.- Las direcciones de vuelta de un correo electrónico no son fiables.
11.- El programa sendmail es un peligro en sí mismo.
12.- No se deben ejecutar a ciegas mensajes MIME.
13.- Es fácil interceptar sesiones *telnet*.
14.- Se pueden atacar protocolos de autenticación modificando el NTP.
15.- Finger da habitualmente demasiada información sobre los usuarios.
16.- No debe confiarse en el nombre de la máquina que aparece en un RPC.
17.- Se puede conseguir que el encargado de asignar puertos IP ejecute RPC en beneficio de quien le llama.
18.- Se puede conseguir, en muchísimos casos, que NIS entregue el fichero de passwords al exterior.
19.- A veces es fácil conectar máquinas no autorizadas a un servidor NIS.
20.- Es difícil revocar derechos de acceso en NFS.
21.- Si está mal configurado, el TFTP puede revelar el /etc/passwd .
22.- No debe permitirse al ftp escribir en su directorio raíz.
23.- No debe ponerse un fichero de passwords en el área de ftp.
24.- A veces se abusa de FSP, y se acaba dando acceso a ficheros a quien no se debe dar.
25.- El formato de información de WWW debe interpretarse cuidadosamente.
26.- Los servidores WWW deben tener cuidado con los punteros de ficheros.
27.- Se puede usar ftp para crear información de control del gopher.
28.- Un servidor WWW puede verse comprometido por un script interrogativo pobremente escrito.
29.- El MBone se puede usar para atravesar algunos tipos de cortafuego.
30.- Desde cualquier sitio de la Internet se puede intentar la conexión a una estación X11 (X-Server).
31.- No se debe confiar en los números de puerto facilitados remotamente.
32.- Es casi imposible hacer un filtro seguro que deje pasar la mayoría del UDP.
33.- Se puede construir un túnel encima de cualquier transporte.

Aunque el acto de securizar el mensaje cae bajo la responsabilidad del usuario final, dicho usuario debería usar una herramienta amigable proporcionada por el responsable de seguridad de su organización.

34.- Un cortafuego no previene contra niveles superiores de aquellos en los que actúa.

35.- Las X11 son muy peligrosas incluso a través de una pasarela.

36.- Las herramientas de monitorización de red son muy peligrosas si alguien accede ilegítimamente a la máquina en que residen.

37.- Es peligroso hacer peticiones de finger a máquinas no fiables.

38.- Se debe de tener cuidado con ficheros en áreas públicas cuyos nombres contengan caracteres especiales.

39.- Los *caza-passwords* actúan silenciosamente.

40.- Hay muchas maneras de conseguir copiar el /etc/password

41.- Registrando completamente los intentos fallidos de conexión, se capturan passwords.

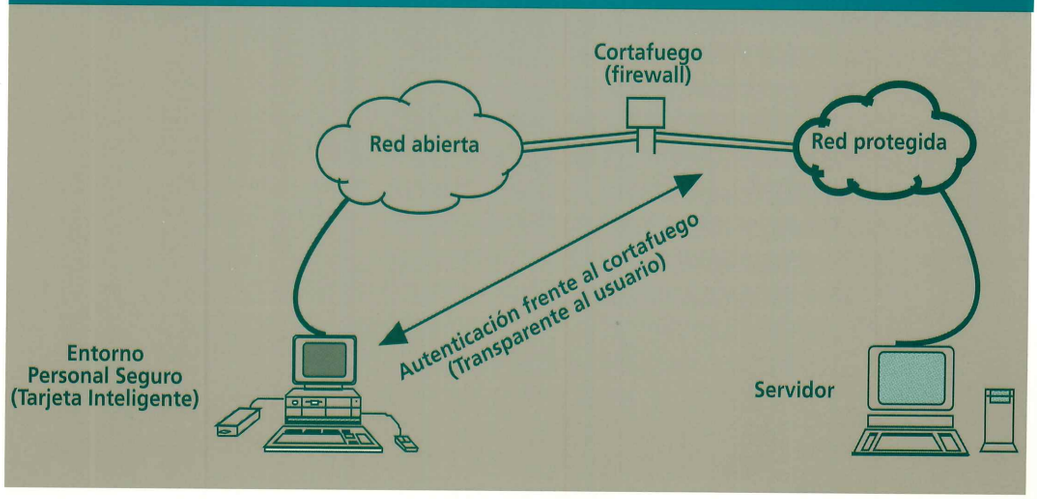
42.- Un administrador puede ser considerado responsable -si se demuestra conocimiento o negligencia- de las actividades de quien se introduce en sus máquinas.

A la hora de plantearse en que elementos del sistema se deben de ubicar los servicios de seguridad podrían distinguirse dos tendencias principales:

- Protección de los sistemas de transferencia o transporte. En este caso, el administrador de un servicio, asume la responsabilidad de garantizar la transferencia segura de la información de forma bastante transparente al usuario final. Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, de un servicio de mensajería con MTAs seguras, o la instalación de un cortafuego, (*firewall*), que defiende el acceso a una parte protegida de una red.

- Aplicaciones seguras extremo a extremo. Si pensamos por ejemplo en correo electrónico consistiría en construir un mensaje en el cual en contenido ha sido asegurado mediante un procedimiento de encapsulado previo al envío, de forma que este mensaje puede atravesar sistemas heterogéneos y poco fiables sin por ello perder la validez de los servicios de seguridad provistos. Aunque el acto de securizar el mensaje cae bajo la responsabilidad del usuario final, es razonable pensar que dicho usuario deberá usar una herramienta amigable proporcionada por el responsable de seguridad de su organización. Este mismo planteamiento, se puede usar para abordar el problema de la seguridad en otras aplicaciones tales como videoconferencia, acceso a bases de datos, etc.

USO DE CORTAFUEGO CON AUTENTICACION FUERTE



En ambos casos, un problema de capital importancia es la **gestión de claves**. Este problema es inherente al uso de la criptografía y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro. En el caso de las claves secretas el problema mayor consiste en mantener su privacidad durante su distribución, en caso de que sea inevitable su envío de un punto a otro. En el caso de clave pública, los problemas tienen que ver con la garantía de que pertenecen a su titular y la confianza en su vigencia (que no haya caducado o sido revocada).

Una manera de abordar esta gestión de claves está basada en el uso de los ya citados Certificados de Clave Pública y Autoridades de Certificación. El problema de la vigencia de la clave se resuelve con la generación de Listas de Certificados Revocados (*CRLs*) por parte de las CAs.

La seguridad informática es rica en implicaciones legales. Las leyes españolas restringen la manipulación abusiva de datos personales tan comunes como la dirección, teléfono, etc. obligando a proteger los ficheros que contengan este tipo de datos.

Sistemas integrados para la seguridad

Todos estos planteamientos de diversas ubicaciones de servicios de seguridad, algoritmos criptográficos utilizados y diferentes formas de gestionar las claves, dan lugar a una gran variedad de sistemas para la seguridad. Normalmente cada sistema incluye además de cierta gestión de claves -infraestructura para la seguridad- una serie de aplicaciones seguras (aseguradas en base al planteamiento de extremo a extremo, al de servicio seguro o una mezcla de ambas) y una serie de recomendaciones sobre como asegurar nuevas aplicaciones. Esta última labor se facilita habitualmente con la existencia de librerías de funciones que ejecutan tareas relacionadas con la seguridad.

En la segunda entrega de este artículo se hará una revisión de los sistemas más conocidos (Kerberos, SPX, SecuDE, OSISEC) así como algunos productos y estándares que cumplen alguna de las funciones de seguridad citadas (PGP o los productos compatibles PEM).

Implicaciones legales

La seguridad informática es rica en implicaciones legales. Las leyes españolas restringen la manipulación abusiva de datos personales tan comunes como la dirección, teléfono, etc. [6] obligando a proteger los ficheros que contengan este tipo de datos. Otros datos personales como los sanitarios, ideología, religión o vida sexual están especialmente protegidos, requiriéndose permiso escrito del afectado para su tratamiento o bien, sólo en algunas excepciones, una legislación especial.

Aunque aún no se ha desarrollado un reglamento, y su incumplimiento es manifiesto, la ley está en vigor desde enero de 1992. El pasado verano la Agencia de Protección de Datos solicitó la inscripción de todos los ficheros automatizados con datos personales existentes, solicitando a la organización responsable que indicase qué ámbito tiene cada fichero, qué tipo de información guarda, etc.

También el uso y la exportación de criptografía están contemplados en la legislación de muchos países despertando no poca polémica. En la mayoría de los países de nuestro entorno, incluida España, se permite libremente el uso de la criptografía pero no su exportación, basándose en el hecho de que se consideran tecnologías de doble uso que pueden tener una utilización militar. España adoptó las limitaciones a la exportación habituales dentro de la Alianza Atlántica por un Real Decreto en 1993.

Ni en el derecho mercantil ni en el administrativo hay jurisprudencia en la aplicación de estas leyes, ya que los interesados que usan estos procedimientos prefieren llegar a acuerdos antes que recurrir a los tribunales.

Finalmente, la validez de la firma digital ante posibles conflictos o reclamaciones, también está perfectamente avalada en la legislación vigente. Respecto a su uso en el ámbito de la contratación privada, -para dar validez a una oferta, encargo u orden de pago hecha por medios electrónicos- la ley se refiere únicamente a que se pueda demostrar la voluntad de contratar.

En el ámbito de la Administración Pública, se reconoce explícitamente la validez de los métodos electrónicos de transferencia de la información siempre que se garantice la identidad (servicio de autenticación) [7]. Esta normativa contempla tanto las relaciones entre los diferentes departamentos como las de los administrados con la Administración.

Sin embargo hay que reconocer que, ni en el derecho mercantil ni en el administrativo hay jurisprudencia en la aplicación de estas leyes, ya que los interesados que usan estos procedimientos prefieren llegar a acuerdos antes que recurrir a los tribunales.

Dentro de Europa, es excepcional el caso de Francia donde el simple uso de la criptografía está prohibida a no ser que se disponga de una licencia. En sentido contrario, algunos países nórdicos no tienen ningún tipo de limitación respecto a la exportación. Hay que tener en cuenta que este tipo de limitaciones tienen muy poca efectividad ante la dificultad existente para vigilar la exportación de software. Por otra parte, aunque se prohíba la exportación de los sistemas seguros, los algoritmos criptográficos y protocolos para la consecución de servicios de seguridad son frecuentemente públicos, con lo que los sistemas se pueden volver a desarrollar en el país de destino.

Referencias

[1] "Contemporary Cryptology. The Science of Information Integrity", Gustavus J. Simmons (Editor), IEEE Press. 1992.

[2] "Security Mechanisms for Computer Networks", Sead Muftic, Ed. John Wiley & Sons, 1984.

[3] "Information Processing Systems. OSI Reference Model - Part 2: Security Architecture", ISO/IEC IS 7498-2, Jul. 1988.

[4] "Inf. Tech. - OSI. The Directory - Authentication Framework", ITU X.509, ISO/IEC IS 9594-8, Dic. 1991.

[5] "Firewalls and Internet Security: Repelling the Wily Hacker", William R. Cheswick y Steven M. Bellovin, Addison Wesley, 1994.

[6] "Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD)" B.O.E. 5/92 de 31 de enero de 1992.

[7] "Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común" B.O.E. 285/92 de 27 de noviembre de 1992.

Eloy Portillo y Lourdes López
Profesores del DIATEL
E.U.I.T. de Telecomunicación de la UPM

eloy.portillo@diatel.upm.es
lourdes.lopez@diatel.upm.es

La Red de la Universidad de Las Palmas de Gran Canaria (ULPnet)

Enrique Rubio y Antonio Ocón

1.- Introducción

Desde diferentes ámbitos y contextos, analistas de la situación actual concluyen que nos encontramos en una situación de cambio generalizado y constante, caracterizado por la presencia cada día más palpable, de unos valores emergentes frente a unos valores dominantes que configuran el tránsito hacia la llamada Sociedad de la Información o del Conocimiento.

La Universidad de Las Palmas de Gran Canaria (ULPGC), pese a su juventud, ha estado desde un principio convencida de la tremenda importancia que las Nuevas Tecnologías de la Información están adquiriendo en todos los aspectos del quehacer humano, y muy especialmente en todo lo relativo a docencia e investigación. Por todo ello, se ha planteado un Modelo de Innovación Tecnológica, basado en la implantación e integración de las Tecnologías de la Información, que proporcione las bases para alcanzar los objetivos institucionales que el actual equipo de gobierno propuso como línea prioritaria en su programa de gestión.

Desde la anterior visión conceptual, pretendemos mostrar a continuación la evolución y planteamientos de futuro de la infraestructura informática y de comunicaciones en nuestra Universidad.

1.1.- Breve reseña histórica

El embrión de la actual ULPGC fueron los centros adscritos a la Universidad de La Laguna que se fundaron en la isla de Gran Canaria, especialmente en el ámbito tecnológico (Escuelas Universitarias y Técnicas Superiores de Arquitectura e Ingeniería Industrial). Posteriormente, a finales de los años setenta, se creó el Colegio Universitario de Las Palmas, con primeros cursos de Medicina, Veterinaria e Informática. Fue por estas fechas cuando se crea la Universidad Politécnica de Canarias, a la que se adscriben los citados centros. La primera adquisición informática de importancia se realizó en 1.980, con el miniordenador HP-3000 de la Escuela Universitaria de Informática. Posteriormente, en 1.985, se adquirieron dos miniordenadores VAX 11/750, instalados en la E.T.S.I.I. y la Escuela de Informática, respectivamente. Coincidiendo con las primeras etapas del Programa IRIS, en 1.987 se solicita y obtiene la conexión del VAX de la ETSII a la Red IBERPAC, proporcionando inicialmente servicios de correo electrónico (EAN) y emulación de terminal remoto a sus usuarios. En 1.992 se produce la integración de la ya completa Universidad de Las Palmas de Gran Canaria en la Red ARTIX, y la conexión de varios de sus centros al Servicio de Interconexión de Redes de Área Local (SIDERAL).

Durante la primera etapa del Programa IRIS, en 1.987 se obtiene la conexión del VAX de la ETSII a la Red IBERPAC, proporcionando inicialmente servicios de correo electrónico (EAN) y emulación de terminal remoto a sus usuarios y en 1.992 se produce la integración de la Universidad de Las Palmas de Gran Canaria en la Red ARTIX.

2.- Infraestructura actual de la red

Desde entonces, se ha ido produciendo (al igual que en la mayoría de instituciones afiliadas a RedIRIS), una auténtica revolución en el uso de estos recursos, promovida en gran parte por la implantación del germen de la futura red Integrada de la Universidad de Las Palmas de Gran Canaria (ULPnet), consistente en un "backbone" de fibra óptica FDDI en el campus de Tafira, y un conjunto de enlaces con los diferentes subcampus. No obstante, somos conscientes que tan sólo un treinta por ciento de los más de 22.000 alumnos matriculados en esta universidad disponen actualmente de acceso a la red, quedando por tanto un largo camino que recorrer de cara a un deseado "acceso ubicuo y universal" a los sistemas y recursos de información.

Antes de proceder a detallar la topología de la red, es importante resaltar que la ULPGC ha sido una de las primeras universidades españolas en abrazar la filosofía emanada de la LRU, de forma que su estructura interna es marcadamente departamental, considerándose como unidades funcionales los edificios. Así, todos los edificios modernos poseen una estructura multicurricular, siendo sede de uno o más departamentos (a nivel de campus) afines (Edificios

La actual ULPGC está configurada alrededor de tres subcampus: Tafira (fundamentalmente tecnológico), el Área de San Cristóbal (Ciencias de la Salud) y Obelisco (Humanidades).

Departamentales de Ingenierías, de Telecomunicación, de Ciencias Básicas, de Humanidades, etc.). Por tanto, se considera el edificio como unidad funcional, pudiendo coexistir en el mismo diferentes Titulaciones y Departamentos con relativa autonomía, tanto a nivel presupuestario como funcional.

Tabla 1.- La actual ULPnet, en cifras

Alumnos	22.000
Redes Conectadas	28
Cuentas de Usuario	5.000
Servidores UNIX	45
Servidores NOVELL	12
Servidores VAX/VMS	8

Geográficamente, y por su propio acontecer histórico, la actual ULPGC está configurada alrededor de tres subcampus: Tafira (fundamentalmente tecnológico) a unos seis kilómetros del centro urbano, constituye un campus "clásico", sito en terrenos de la Universidad, mientras que las Áreas de San Cristóbal (Ciencias de la Salud) y Obelisco (Humanidades), en cambio, se encuentran más o menos inmersas en la zona urbana de Las Palmas de Gran Canaria.

SITUACION ACTUAL DE LA RED I+D EN LA ULPGC

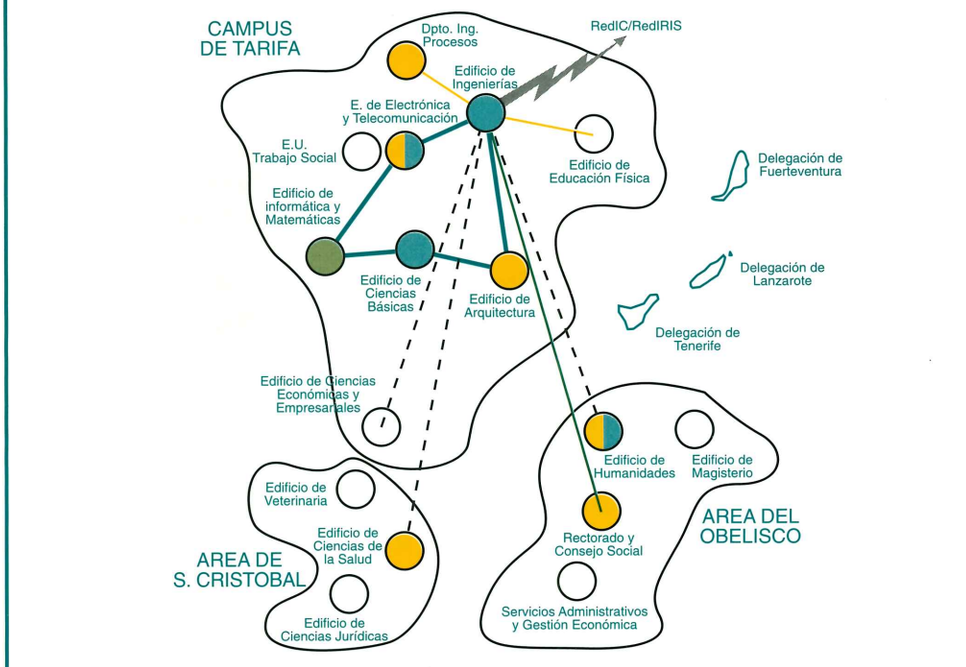


FIGURA 1

2.1.- Nivel de campus

Cómo se observa en la figura 1, el anillo de fibra enlaza siete edificios del campus principal de la ULPGC (Tafira). Dicho anillo, integrado actualmente por seis "routers" serie 4000 de CISCO, proporciona servicio de datos a alta velocidad (100 Mbits/seg.) para un total de 18 segmentos Ethernet (10 Mbits/seg.), repartidos por los edificios siguientes:

Tabla 2.- Edificios conectados mediante FDDI

- Edificio de Ingenierías :	4 segmentos Ethernet
- Edificio de Telecomunicaciones:	4 Segmentos Ethernet
- Edificio de Informática y Matemáticas:	4 Segmentos Ethernet
- Edificio de Arquitectura:	2 Segmentos Ethernet
- Edificio de Ciencias Básicas:	2 Segmentos Ethernet
- Edificio de Educación Física :	1 Segmento Ethernet
- Departamento de Ingeniería de Procesos:	1 Segmento Ethernet

Los dos últimos edificios se encuentran conectados al anillo FDDI a través de conexiones Ethernet sobre fibra óptica (FOIRL), accediendo al CICEI (Centro Informático y de Comunicaciones del Edificio de Ingenierías), donde se encuentra ubicado actualmente el centro de gestión y control de la red, así como la conexión de la misma con el exterior.

Asimismo, desde el CICEI se proporciona servicio a los restantes subcampus de la ULPGC, que configuran respectivamente las áreas de Ciencias de la Salud (San Cristóbal), Humanidades (Obelisco) y de gestión administrativa (Rectorado). Este servicio se establece en base a enlaces seriales a velocidades de 2 Mbits/seg. (Rectorado) y 64 Kbits/seg. (Empresariales, Humanidades y CULP). En cada uno de estos extremos se encuentran "routers" de la serie 3000 de CISCO, proporcionando conectividad a un segmento Ethernet por edificio, tal y como se observa en la tabla 3.

Tabla 3.- Edificios conectados mediante enlace serial

Edificio del Rectorado (2 Mb/s)	1 Segmento Ethernet
Edificio de Humanidades (64 Kb/s)	1 Segmento Ethernet
Edificio de Ciencias Médicas (64 Kb/s)	1 Segmento Ethernet

2.2.- Modelo informático y de comunicaciones a nivel de edificio

En la misma figura 1 se puede comprobar el estado actual de cada edificio, siendo este muy variable. Aunque una de las premisas del actual equipo de gobierno es la homogeneidad tecnológica entre edificios, a la espera de ser puesto definitivamente en práctica el Plan de Tecnologías de la Información (del que hablaremos más adelante), se dispone de muy diferentes niveles de accesibilidad a la red desde los diferentes edificios.

El primer edificio en ser dotado de una red corporativa, con integración de servicios de voz y datos fue el Edificio de Ingenierías. Desde 1.991 se encuentra operativo en el mismo un sistema de cableado corporativo PDS de AT&T, compuesto de 230 rosetas duales (voz/datos). Mediante la adecuada distribución ("HUBs" enlazados entre sí y al "router" central por fibra óptica) los diferentes repartidores de planta proporcionan conectividad Ethernet en todas las dependencias del edificio (aulas, despachos, salón de actos, salas de informática, etc.). Sobre esta infraestructura Ethernet se configura una red multiprotocolo, orientada a la arquitectura cliente/servidor, de forma que cualquier usuario final dispone de acceso a los diferentes servidores instalados dentro o fuera del edificio. Básicamente:

Aunque una de las premisas del actual equipo de gobierno es la homogeneidad tecnológica entre edificios, a la espera de ser puesto definitivamente en práctica el Plan de Tecnologías de la Información, se dispone de muy diferentes niveles de accesibilidad a la red desde los diferentes edificios.

Aspecto importante es la dotación de Aulas de Informática, operando las 24 horas del día, 365 días al año.

- Servidores NOVELL (versiones 3 y 4) :
  - -Servicios de disco (herramientas de productividad), impresión y plotter
  - -Correo electrónico (Pegasus Mail)
- Servidores UNIX y VAX:
  - -Emulación de Terminal
  - -Correo Electrónico (EAN, Pine, Elm, Unix-mail, etc.)
  - -Servicios de disco, impresión y plotter
  - -Servicios de valor añadido (WWW, Gopher, Bases de Datos, OPACs, etc.)
- Servidores IBM/SNA (accesibles desde la red IP mediante pasarela)
  - -Servicios de gestión administrativa
  - -Acceso a la Biblioteca Universitaria

La conectividad con el exterior ha evolucionado de la línea de 9.600 bps. que enlazaba a la ULPGC con RedIRIS a una conexión de alta velocidad perteneciente a la incipiente Red Canaria de I+D (REDIC).

Todos estos servicios son accesibles para diferentes tipos de "estación cliente", típicamente:

- Ordenador PC compatible con tarjeta Ethernet
  - -Entorno MS-DOS/WINDOWS
  - - Coexistencia de redes NOVELL y TCP/IP-NFS ó Pathworks (DECnet)
- Ordenador Macintosh con tarjeta Ethernet
  - - Coexistencia de Novell y TCP/IP
- Máquina Unix/Estación X
  - - TCP/IP-NFS

Tanto desde el interior de la red como mediante acceso remoto (a través de los servicios ULPmail, ULPmodem y ULPlink, descritos más adelante).

Aspecto importante es la dotación de Aulas de Informática, que operando las 24 horas del día, 365 días al año (gracias a un sistema de control de accesos mediante tarjeta personal), se encuentran en funcionamiento ininterrumpido desde 1.991, proporcionando accesos a la red a más de 1.900 alumnos (en el Edificio de Ingenierías).

En la figura 2 se ilustra este modelo de servicios proporcionados a la comunidad de usuarios, considerándose como el prototipo de implantación en el resto de la Universidad.

2.3.- Conectividad con el exterior

La conectividad con el exterior ha evolucionado de forma pareja a la conectividad interna, pasando en muy breve período de tiempo de la línea de 9.600 bps. que mantenía RedIRIS y que enlazaba a la ULPGC con RedIRIS dentro de la red ARTIX a una conexión de alta velocidad (actualmente de 2 Mbits/seg.), perteneciente a la incipiente Red Canaria de I+D (REDIC), organismo que, en primera instancia, interconecta los tres principales centros de investigación y desarrollo de la Comunidad Canaria: Universidad de La Laguna (ULL), Instituto de Astrofísica de Canarias (IAC) y Universidad de Las Palmas de Gran Canaria (ULPGC), accediendo a dicha red, a través de las dos universidades, los restantes centros mediante conexiones RDSI. Igualmente, el "backup" de los enlaces troncales de esta red (los enlaces de 2 Mbits/seg. IAC-ULL e IAC-ULPGC) se realiza a través de RDSI. A su vez, el IAC mantiene la conectividad de la Red Canaria con RedIRIS, a través de una línea que en la actualidad es de 256 Kbits/seg., esperándose en breve su incremento a 2 Mbits./seg.).

PROTOTIPO DE MODELO INFORMATICO Y DE COMUNICACIONES (EDIFICIO DE INGENIERIAS)

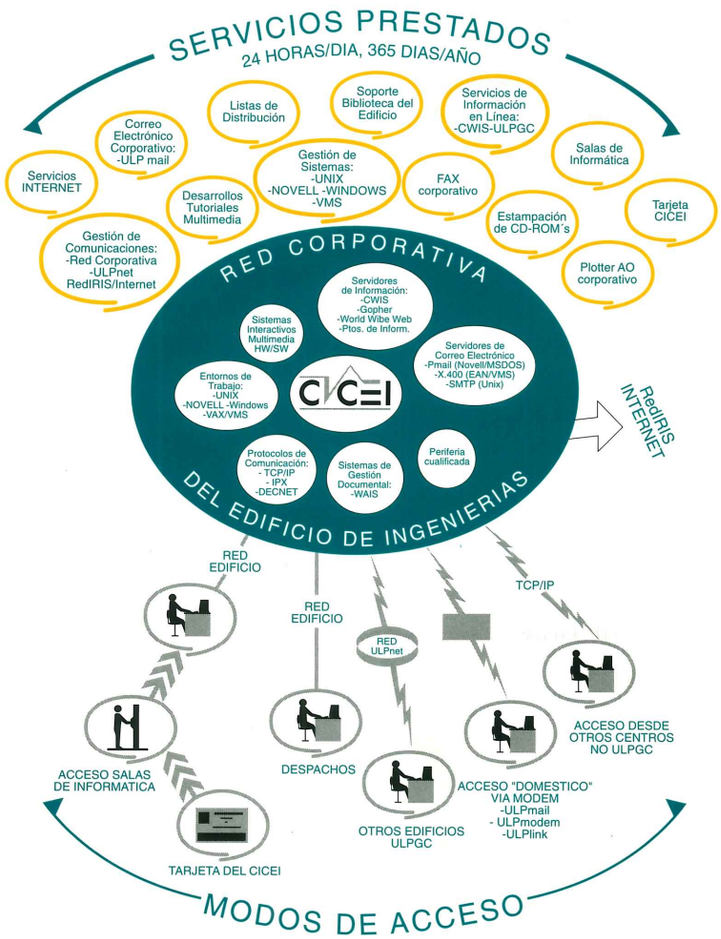


FIGURA 2

Básicamente son tres los protocolos de comunicaciones utilizados: TCP/IP, IPX/SPX y DECnet., siendo los dos primeros con mucho, los más empleados en la actualidad.

2.4.- Protocolos de comunicaciones

Básicamente son tres los protocolos de comunicaciones utilizados: TCP/IP, IPX/SPX y DECnet. Los dos primeros son con mucho los más empleados en la actualidad, ya que el modelo informático y de comunicaciones a nivel de edificio contempla básicamente una arquitectura cliente/servidor con dos entornos fuertemente potenciados: Servidores UNIX y NOVELL frente a clientes MS-DOS/Windows, Macintosh y estaciones X. No obstante, aún se encuentran en funcionamiento máquinas de arquitectura propietaria de DEC, principalmente VAXes, MicroVAXes y procesadores Alpha/AXP.

En cuanto a los protocolos SNA, propios de la arquitectura IBM, empleada en la red de gestión universitaria, hay que resaltar que no se integran en la red ULPnet, sino que en la actualidad se accede a los "hosts" IBM a través de pasarelas IP-SNA, a la espera de que en un futuro más o menos próximo se conecten todos los equipos directamente, implementando la pila de protocolos TCP/IP en los citados "hosts".

3.- Servicios en la Red ULPnet

Además de los servicios propios de cada edificio (acceso a los servidores locales o remotos de disco e impresoras, para emplear las herramientas de productividad personal), se deben considerar los servicios de red propiamente dichos. De entre todos, es sin duda el correo electrónico el más extendido, tanto por ser el primero en distribuirse como debido a su componente corporativa, que le confiere innumerables ventajas desde el punto de vista de la productividad, tanto académica cómo investigadora y de gestión. A continuación, se describirán los restantes servicios disponibles en la red, accesibles tanto de forma interna como externa.

Actualmente, la ULPGC se conecta con el exterior mediante protocolos SMTP, mientras que internamente, se emplean diferentes protocolos de transporte.

3.1.- Correo electrónico

Desde los primeros tiempos del programa IRIS, se instaló el software EAN en una serie de equipos VAX, conectados al exterior mediante enlaces IBERPAC en un principio y ARTIX posteriormente. A raíz de la creación de SIDERAL, y debido al creciente empuje de los protocolos IP frente a OSI, se decidió dar prioridad al transporte SMTP, quedando X.400 relegado a la conectividad interna entre los sistemas EAN "a extinguir". Actualmente, la ULPGC se conecta con el exterior mediante protocolos SMTP, mientras que internamente, tal y como se aprecia en la figura 3, se emplean diferentes protocolos de transporte. A nivel de Agentes de usuario, el más empleado con diferencia es el Pegasus Mail (para DOS en castellano, Windows y Macintosh), desarrollado por David Harris. Sus principales características son:

A nivel de Agentes de Usuario, el más empleado con diferencia es el Pegasus Mail.

Tabla 4.- Correo Electrónico PEGASUS MAIL

- Variedad de sistemas de transporte (IPX, POP3, UUPC, etc.)
- Variedad de plataformas (DOS, Windows, Macintosh)
- Excelentes prestaciones (ayuda sensible al contexto, etc.)
- Versión DOS en castellano
- Compatible con el estándar MIME
- Totalmente gratuito
- Excelente servicio (solución de problemas, actualizaciones, etc.)
- Manual en castellano (elaborado por el CICEI)
- Igualmente, se dispone de agentes de usuario "clásicos", como el EAN para VAX/VMS, Pine, Elm, X-mail, Mail y otros para UNIX, etc.

ORGANIZACION DEL CORREO ELECTRONICO EN LA ULPGC

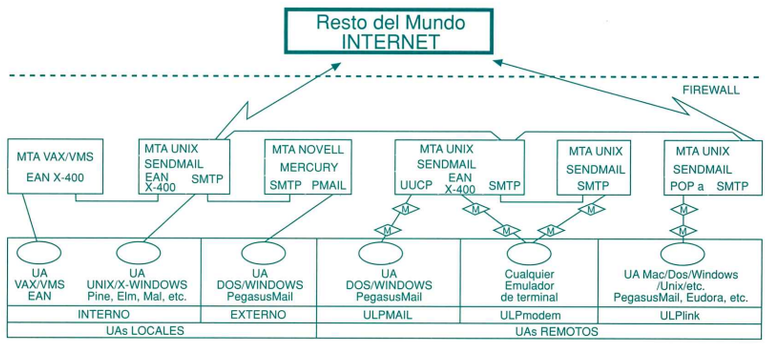


FIGURA 3

En el esquema se indica igualmente la existencia de un cortafuegos ó "firewall" en el "router" de salida de la Universidad, de forma que sólo determinados MTAs puedan establecer conexiones con el exterior. Esta medida resuelve tanto problemas de seguridad (son conocidas las "debilidades" de ciertos gestores de correo como el Sendmail) como de armonización del correo (al garantizar que toda máquina susceptible de intercambiar correo con el exterior se encuentre debidamente autorizada y registrada en la red). Asimismo, y siguiendo la tendencia mayoritaria actualmente, se ha apostado por el empleo de las extensiones multimedia MIME como estándares para la difusión de información, tanto textual como binaria, en todos los mensajes intra-organizativos.

La ULPGC está empezando a trascender el mero empleo del correo electrónico como herramienta de productividad personal para comenzar su empleo a NIVEL CORPORATIVO.

No cabe duda de que en una organización con más de 5.000 direcciones de correo electrónico, uno de los mayores problemas es el de localizar la dirección de una determinada persona o servicio. Mientras se finaliza la puesta a punto del servidor de directorio X.500, se dispone de un servidor CSO, bastante más sencillo de operar, accesible desde el Sistema de Información Universitario (CWIS) vía WWW, Gopher y también desde correo electrónico. Para hacer uso de esta última funcionalidad, se puede enviar un mensaje conteniendo el texto AYUDA ó HELP a la dirección:

directorio@ulpgc.es

Otro aspecto digno de mención es el de las LISTAS DE DISTRIBUCION de correo electrónico. Desde hace años se encuentran en funcionamiento una serie de servidores de correo, bajo diferentes entornos operativos (MERCURY/NOVELL, LISTSERV/UNIX y MAJORDOMO/UNIX) que mantienen diversas listas de distribución acerca de muy variados temas. Especial mención merece la lista de la Dirección General de Universidades del Gobierno de Canarias (**DGUI@cicei.ulpgc.es**), y la lista a nivel mundial sobre ecología pesquera **FISH-ECOLOGY@searn.sunet.se**, moderada desde el CICEI por Aldo-Pier Solari, con la inestimable colaboración del equipo de Eric Thomas en SUNET (Suecia).

No quisiéramos finalizar este apartado sin hacer hincapié en la idea de que la ULPGC está empezando a trascender el mero empleo del correo electrónico como herramienta de productividad personal para comenzar su empleo a NIVEL CORPORATIVO, como medio de implementación del modelo de Servicios de Información diseñado, en el sentido de que actúa como vehículo de transmisión de información desde las diversas fuentes de la misma (Secretaría General, Vicerrectorados, Servicios diversos, etc.) hasta el Sistema de Información en Línea (CWIS).

3.2.- Servidores FTP anónimo y NEWS

Otro de los servicios muy extendidos en la ULPnet es el de FTP anónimo. Desde el servidor principal, "**ftp.ulpgc.es**", con más de dos Gigabytes de información, incluyendo "espejos" de otros importantes servidores FTP mundiales, hasta otros servidores departamentales, se dispone de una enorme cantidad de información accesible "en línea", tanto a nivel de documentación, herramientas de producción y desarrollo, etc. Quizás merezca la pena resaltar el ofrecimiento que hacemos desde estas líneas del MANUAL DEL PEGASUS MAIL en castellano, desarrollado y mantenido por el CICEI, disponible a todos los interesados (en formato PostScript) en:

ftp://ftp.ulpgc.es/pub/doc/pmail/

Aunque de reciente incorporación (febrero de 1.995), el servidor de NEWS central de la Universidad, "**news.ulpgc.es**", dispone de todos los grupos de USENET NEWS distribuidos por RedIRIS, a los que se puede acceder de forma tanto local como remota, en el ámbito de toda la ULPnet.

Se ha creado un equipo de trabajo con la misión específica de realizar y mantener el CWIS de la ULPCG.

3.3.- Sistema de información en línea (CWIS). WWW y Gopher

Sin lugar a dudas, uno de los aspectos más importantes de una infraestructura de información como la que se desea implantar en la ULPGC es el desarrollo de un Sistema de Información en Línea o CWIS (Campus-Wide Information System). Desde hace varios años, se ha trabajado en el desarrollo de diferentes prototipos de sistemas de difusión de información, con tecnologías tan dispares como Videotext ó BBS, pero ha sido en los dos últimos años cuando a raíz de la "explosión" de sistemas basados en tecnologías Internet, como fue primero el Gopher de la Universidad de Minnesota y últimamente el WWW del CERN y la NCSA, cuando se ha creado un equipo de trabajo con la misión específica de realizar y mantener el CWIS de la ULPGC (ver figura 4). Actualmente, se dispone de dos servidores principales, en:

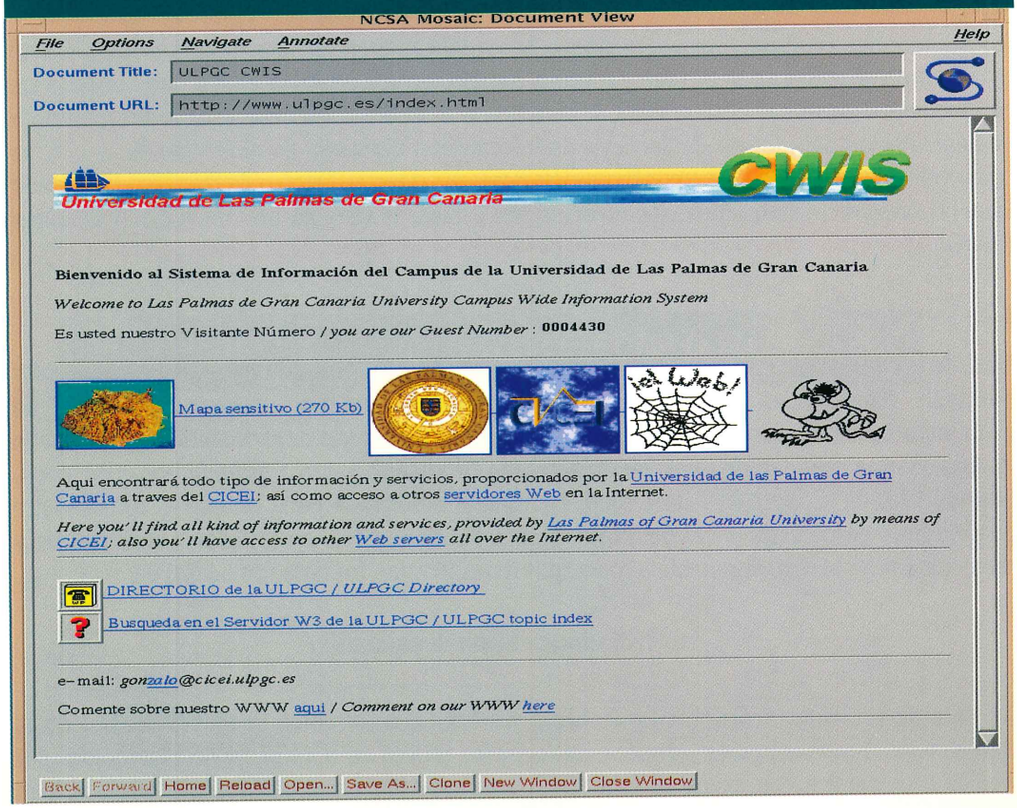
http://www.ulpgc.es/intro.html y **gopher://gopher.ulpgc.es::70**

Con información relativa a nuestra universidad. Merecen ser citados dos aspectos importantes:

- La UNICIDAD de la información mantenida en ambos servidores, lograda en base a sistemas automáticos de conversión de documentos HTML del servidor WWW a formato apto para el servidor Gopher.
- El MODELO de recogida de información de las diversas fuentes, previo a su inserción en el CWIS, basado principalmente en el empleo de correo electrónico a nivel corporativo.

En estos momentos se halla prácticamente finalizada la etapa de prototipo del sistema, y aprovechamos para invitar desde estas líneas al lector para que acceda al mismo, agradeciendo de antemano cualquier sugerencia o comentario.

PANTALLA INICIAL DEL PROTOTIPO DE CWIS EN LA ULPGC



3.4.- Servicios de gestión administrativa y biblioteca universitaria

No cabe duda de que las Tecnologías de la Información poseen la doble vertiente de comportarse como "enablers" (facilitadoras) de procesos evolutivos en las organizaciones y, a su vez, en algunos casos pueden llegar a producir "constraints" (ligaduras) en el desarrollo organizativo. La ULPGC se ha visto afectada por este último factor muy especialmente en el caso de la computación administrativa, vinculada desde un principio a entornos fuertemente propietarios (máquinas IBM con arquitectura de red SNA), y en la gestión de la Biblioteca Universitaria (DOBIS-LIBIS también sobre IBM).

Esto ha motivado la existencia de una Red de Gestión en la ULPGC, totalmente jerárquica como lo es el protocolo SNA, de modo que el CPD sito en el edificio de Humanidades es el centro de una configuración en estrella que lo une con todas las restantes sedes administrativas y de bibliotecas de la universidad. Básicamente, los equipos terminales (PC compatibles, impresoras, etc.) de cada unidad funcional se conectan a un "cluster controller" local que, a través de enlaces IBERCOM a 19.200 bps, acometen al "front end" de comunicaciones, conectado mediante "canal" a los dos "Hosts" principales.

Junto con la instalación del anillo de fibra óptica en el campus de Tafira, se contempló la creación de un centro piloto de gestión de la Red.

El problema radica entonces en que esta red se solapa con la existente Red de I+D, provocando duplicidades de esfuerzos (un usuario tendría que estar conectado a ambas para obtener todos los servicios necesarios), dificultades en el acceso a la información, etc.

Por tanto, se ha planteado una reingeniería de procesos, consistente básicamente en la reorientación de los modos de trabajo hacia entornos abiertos, de forma gradual:

- Acceso desde protocolos IP (Red de I+D) a ambos servicios: primero mediante la instalación de una pasarela IP-SNA (ya operativa) y posteriormente instalando IP en los "Hosts". Simultáneamente, se producirá el abandono de la red SNA en favor de la ULPnet.
- Posibilidad de migrar la gestión de Bibliotecas (y otras tareas administrativas) hacia entornos aplicativos y de computación más acordes con los tiempos actuales.

La ULPGC se ha planteado como aspecto prioritario el facilitar accesos remotos a la ULPnet.

3.5.- Gestión de la Red

Junto con la instalación del anillo de fibra óptica en el campus de Tafira, se contempló la creación de un centro piloto de gestión de la Red. Actualmente, este centro se encuentra en el CICEI, donde se controla a través de una Estación SUN dedicada, bajo software SunNet Manager y Cisco Works. Este sistema permite una "visión icónica" del estado de la misma, así como un control y seguimiento de aspectos de tráfico, diagnosis de problemas, actuaciones a tomar ante caídas de enlaces, etc.

Consideramos éste como uno de los aspectos principales en una red avanzada como la que se pretende implantar en un futuro próximo, y está prevista la posibilidad de instalar dos centros de control de red, trabajando en modo simultáneo o alternativo, que permitan garantizar una correcta capacidad de actuación ante cualquier eventualidad.

3.6.- Acceso Remoto. ULPmail, ULPmodem y ULPlink.

Consciente de la situación actual, marcada por una heterogeneidad tecnológica (edificios con red corporativa y acceso "casi ubicuo" a la red, frente a otros con conectividad muy deficiente), además de las necesidades actuales de acceso remoto a la información (durante viajes, desde domicilios particulares, etc.), la ULPGC se ha planteado como un aspecto prioritario el facilitar dichos accesos remotos. Fruto de esta iniciativa son tres productos en cierto modo complementarios y que pasamos a describir:

Con objeto de coordinar a nivel institucional y de manera integral los recursos y servicios de información, se ha creado la figura del "Coordinador de las Tecnologías de la Información".

- **ULPmail**: Se conoce con este nombre una distribución de correo electrónico (Pegasus Mail), que se instala en un ordenador PC compatible y que permite la gestión remota de varios buzones de correo, de forma que la conexión con el servidor central (instalado en el CICEI), se realiza mediante modem (con protocolo de transporte UUCP) y se limita al tiempo necesario para enviar y recibir los mensajes. Desde hace más de un año se vienen impartiendo seminarios de correo electrónico en todos los edificios de la Universidad, lo que ha motivado que existan en la actualidad más de 100 máquinas conectadas a este sistema, con cerca de 250 direcciones de correo operativas.

- **ULPmodem**: Es una extensión del anterior servicio, de forma que aprovechando la configuración efectuada al instalar el ULPmail, se proporciona acceso remoto (en modo carácter) a los servidores Gopher y WWW, así como a cuentas de usuario en máquinas de la red.

- **ULPlink**: A diferencia de los anteriores, este servicio se encuentra en fase de prototipo, y consiste en la integración remota de máquinas (vía RTB y RDSI) en la red ULPnet, con protocolos SLIP y PPP. De esta forma se accede a todos los servicios de la red de manera transparente, al igual que desde equipos directamente conectados a la misma.

4.- Perspectivas de futuro de la ULPnet

Con la presencia creciente de las Tecnologías de la Información en todos y cada uno de los diferentes ámbitos y rincones de la Universidad (administración, bibliotecas, centros, departamentos, servicios de reprografía y publicaciones, servicios de información, aulas de informática, etc.), se están produciendo solapamientos e interferencias funcionales, duplicaciones de esfuerzos y gastos, incompatibilidades técnicas (hardware, software, comunicaciones), tensiones personales, etc., que aconsejan analizar posibles cambios organizativos, con el objeto de coordinar a nivel institucional y de una manera integral los recursos y servicios de información.

A partir de una serie de iniciativas y planteamientos innovadores, procedentes de diferentes grupos de la Universidad, el actual equipo de Gobierno asumió estas ideas bajo el epígrafe de "Plan de Tecnologías de la Información", uno de cuyos primeros frutos ha sido la creación de la figura del "Coordinador de Tecnologías de la Información", cargo que depende directamente del Rector.

4.1.- Plan de Tecnologías de la Información

Citamos a continuación los aspectos más relevantes del citado Plan, auténtica referencia de futuro para el desarrollo universitario:

- **Apoyo institucional.**
- Desarrollo, lo más rápido posible, de una **Infraestructura de Información** a lo largo y ancho del campus.
- **Coordinación global** de los recursos y servicios de información.
- Potenciación del **usuario final**.
- Optimización de las **comunicaciones corporativas internas**.
- **Accesibilidad** controlada, desde todos los niveles, a los servicios y recursos de información.

- Desarrollar adecuadas **estructuras de soporte y facilitación**.
- Estimular la **participación y cooperación**.
- Estimular la **innovación y exploración**, mediante un uso juicioso de los recursos y proyectos piloto.
- Desarrollo de una **Infraestructura de Evaluación del Rendimiento y de Asignación de Recursos.**
- **Concepción integral** de la Organización desde el punto de vista de la Información.
- Promover la creación de **equipos multidisciplinares**.
- Contribuir a la construcción del **Sistema Ciencia - Tecnología - Sociedad**.

En este marco referencial, se contempla la puesta en marcha de un Plan de Innovación Tecnológica en la ULPGC

En este marco referencial, y como adecuación cultural y tecnológica al mismo, se contempla la puesta en marcha de un Plan de Innovación Tecnológica en la ULPGC, que se explicita en las siguientes acciones fundamentales:

1.- Desarrollo de la Red General de la Universidad (ULPnet)
2.- Desarrollo del modelo informático y de comunicaciones, a nivel de edificio y global.
3.- Integración de la Red de Gestión en la Red General.
4.- Desarrollo de una política de computación de sobremesa.
5.- Implantación del correo electrónico a nivel individual y corporativo.
6.- Implantación de Servicios de Información Avanzados.
7.- Puesta en marcha de Aulas de Innovación Educativa.
8.- Coordinación tecnológica de los diferentes recursos y servicios de información.
9.- Integración progresiva con el tejido socioeconómico (sistema C-T-S).

4.2.- ULPnet - Futura red integrada de la ULPGC

Como consecuencia del primer aspecto a considerar en el apartado anterior (desarrollo de una infraestructura de Información o INFOestructura), se han desarrollado una serie de trabajos y estudios conducentes a determinar la estructura física y lógica de la red integrada que permita una accesibilidad, desde todos los niveles, a los recursos de información.

Fruto de todo ello ha sido la definición de la ULPnet, tal y como se muestra en la figura 5, de la que los aspectos más relevantes son:

- Articulación de dos anillos de fibra óptica: la ampliación del actual instalado en el Campus de Tafira (transporte FDDI) y el establecimiento de un anillo metropolitano que conecte el anterior con los edificios situados fuera del campus central. Inicialmente, se prevé la adopción de transporte basado en Jerarquía Digital Síncrona (JDS), capaz de integrar voz (acogiendo así las comunicaciones IBERCOM internas) y datos a velocidades de 155 Mbps, ampliables hasta más de 500 Mbps.
- Integración total de las Redes de voz (IBERCOM) y datos (FDDI/JDS), es decir, capacidad de distribución de ancho de banda de acuerdo a las necesidades.
- Facilidad de migración a entornos de red avanzados: ATM, etc.
- Integración de las actuales redes de I+D y de gestión universitaria en una única Red (ULPnet).
- Empleo del actual modelo Centralizado/Descentralizado en la gestión de la Red General/Redes Departamentales.
- Consideración del "Edificio" como entidad básica de análisis de la organización desde el punto de vista de la Información.

Consideración del "edificio" como entidad básica desde el punto de vista de la información.

4.3.- Futuro modelo informático y de comunicaciones a nivel de edificio

Partiendo de la experiencia acumulada con las redes corporativas actuales, y teniendo en cuenta los planteamientos antes enumerados, se ha diseñado un modelo informático y de comunicaciones a nivel de edificio, cuyos aspectos fundamentales son:

- Red Corporativa "ubicua" (con tomas en todas las dependencias de Edificio), basada en cableado estructurado de nivel 5 (capaz de soportar hasta 100 Mbps).
- Aulas de Informática, abiertas 24 horas al día, 365 días al año.
- Modelo computacional Cliente/Servidor, con énfasis en la computación de sobremesa
- Coexistencia de redes departamentales, integradas en la red general ULPnet.
- Gestión Mixta (Centralizada a nivel de Edificio y Descentralizada a nivel Departamental)

ULPnet - FUTURA RED INTEGRADA DE LA ULPGC

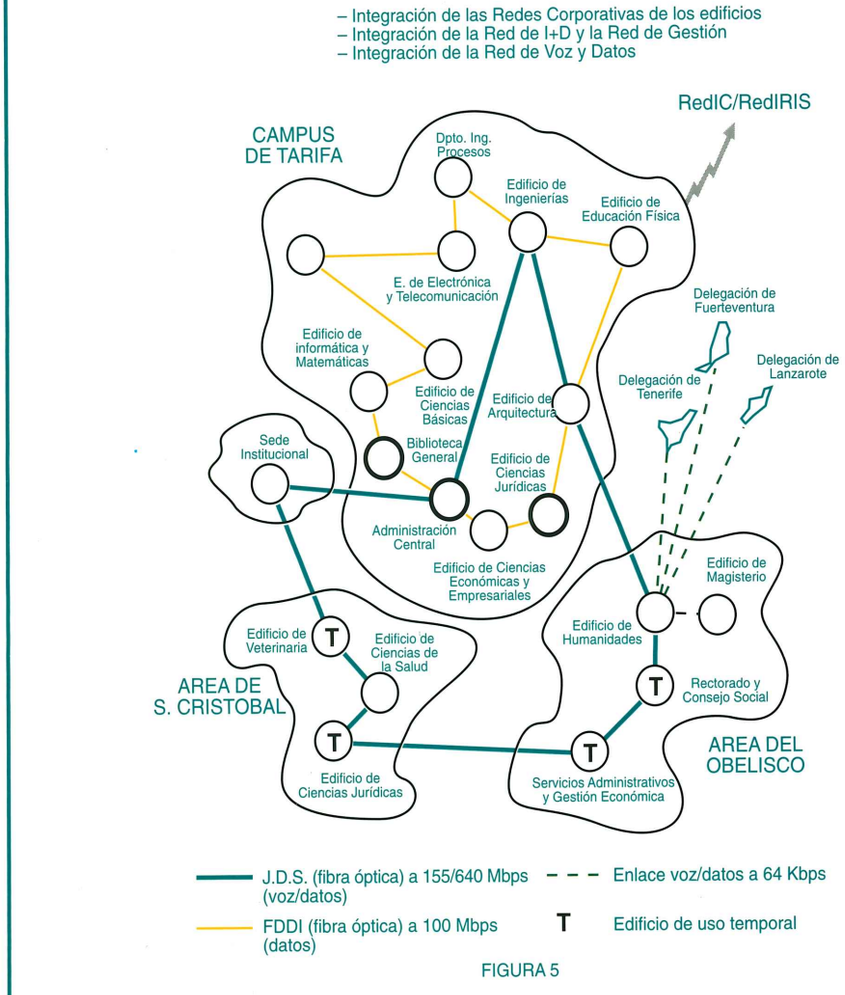


FIGURA 5

5.- Conclusiones

Si, tal como se ha dicho, las Tecnologías de la Información son el motor y el soporte de adecuación en el tránsito hacia la economía de la Información, debería de ser axiomático el que las instituciones académicas fueran profundamente modificadas, dada la misión fundamental de las mismas: "la creación y transmisión de conocimiento", lo que conlleva, amen de las comunes potencialidades relativas a la optimización de la productividad y calidad de los servicios, la posibilidad de transformar la organización del conocimiento, propiciando nuevas culturas de enseñanza y aprendizaje, independientes del modelo tradicional, y la necesidad de intensificar la coordinación y colaboración entre instituciones de enseñanza superior en este propósito de adecuación de las mismas.

Las Tecnologías de la Información transforman la organización del conocimiento, propiciando nuevas culturas de enseñanza y aprendizaje, independientes del modelo tradicional.

La ULPGC, a través de su equipo de gobierno, ha asumido este reto, encontrándose en una etapa de cambio tecnológico (previa al verdadero cambio, de tipo cultural) que le permita acometer con garantías de éxito los desafíos que están por venir. Así, con la definitiva puesta en marcha del Plan de Tecnologías de la Información, y habiendo ya conseguido la financiación necesaria, esperamos dotar a nuestra comunidad universitaria de los adecuados recursos y servicios de información, considerando que la implantación de estas tecnologías debe contemplarse como un proceso de aprendizaje organizacional permanente

Enrique Rubio Royo
Coordinador de Tecnologías de la Información
rubio@cicei.ulpgc.es

Antonio Ocón Carreras
Responsable de Comunicaciones
ocon@cicei.ulpgc.es

CSIC

PLAN NACIONAL DE I+D

CONVOCATORIAS

6 ª Conferencia conjunta europea sobre redes

◆ 6th JENC

Tel Aviv - Israel
15-18 mayo 1995

Esta Conferencia está organizada por TERENA (Trans-European Research and Education Networking Association), asociación nacida de la fusión entre RARE y EARN.

El programa de la reunión se divide en seis bloques temáticos, que constan a su vez de dos o tres sesiones por bloque. Así mismo habrá dos o tres grupos de sesiones paralelas.

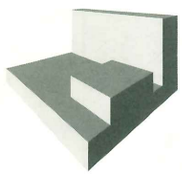
I.- Tecnología e ingeniería de red
II.- Soporte informático para trabajo en equipo.
III.- Seguridad y priva-cidad
IV.- Suministro de información y acceso a ella
V.- Temas organiza-tivos
VI.- Temas regionales: "hacia comunidades interconectadas"

ACTIVIDADES DE LA CONFERENCIA

GRUPOS DE TRABAJO DE TERENA

Con anterioridad a la conferencia tendrán lugar las reuniones de los grupos de trabajo de TERENA. Durante estas reuniones, los diferentes grupos de trabajo

6th JENC



harán una presentación de sus actividades en curso y tratarán sobre diversos temas de especial relevancia.

Estas reuniones serán de carácter abierto y por lo tanto pueden asistir todas aquellas personas que lo deseen.

TUTORIA SOBRE NUEVA GENERACION DE IP

Durante esta tutoría de un día de duración, que será impartida por Steeve Deering de Xerox Parc, USA y que está prevista para el 14 de mayo, se pretende instruir a profesionales con conocimientos previos sobre este tema.

SEMINARIO DE FORMACION EN TECNOLOGIA DE RED

Este seminario sobre instalación y uso de tecnología de red tendrá lugar la semana previa a la celebración de la conferencia. En él se tratarán todos los aspectos de conectividad TCP/IP y dial-up, y por lo tanto, es muy apropiado para regiones con poca o nula infraestructura de red.

Los participantes en el seminario aprenderán los principios básicos para el establecimiento y mantenimiento de una red TCP/IP y la integración en la Internet global. Los temas a tratar incluyen direcciones IP, routers, servidores de nombres, seguridad de red, monitorización, gestión de red y todos los aspectos de redes sobre modems de dial-up.

Para más información sobre este tema ponerse en contacto con David Sitman cuya dirección electrónica es: <david@ccsg.tau.ac.il>.

Durante los días de la conferencia se habilitará un área de demostraciones sobre proyectos y servicios de aplicaciones de red para la comunidad académica. Así mismo se instalará para ponerlo a disposición de los asistentes una sala de terminales conectados a Internet para correo electrónico y otros servicios de red.

Para mayor información sobre cualquier tema relacionado con la Conferencia dirigirse a:

TERENA Secretariat
Singel 466-468
NL-1017 AW Amsterdam
The Netherlands

E-mail: jenc6-sec@terena.nl
-conference information

Tel.: +31 20 639 1131
Fax: +31 20 639 3289