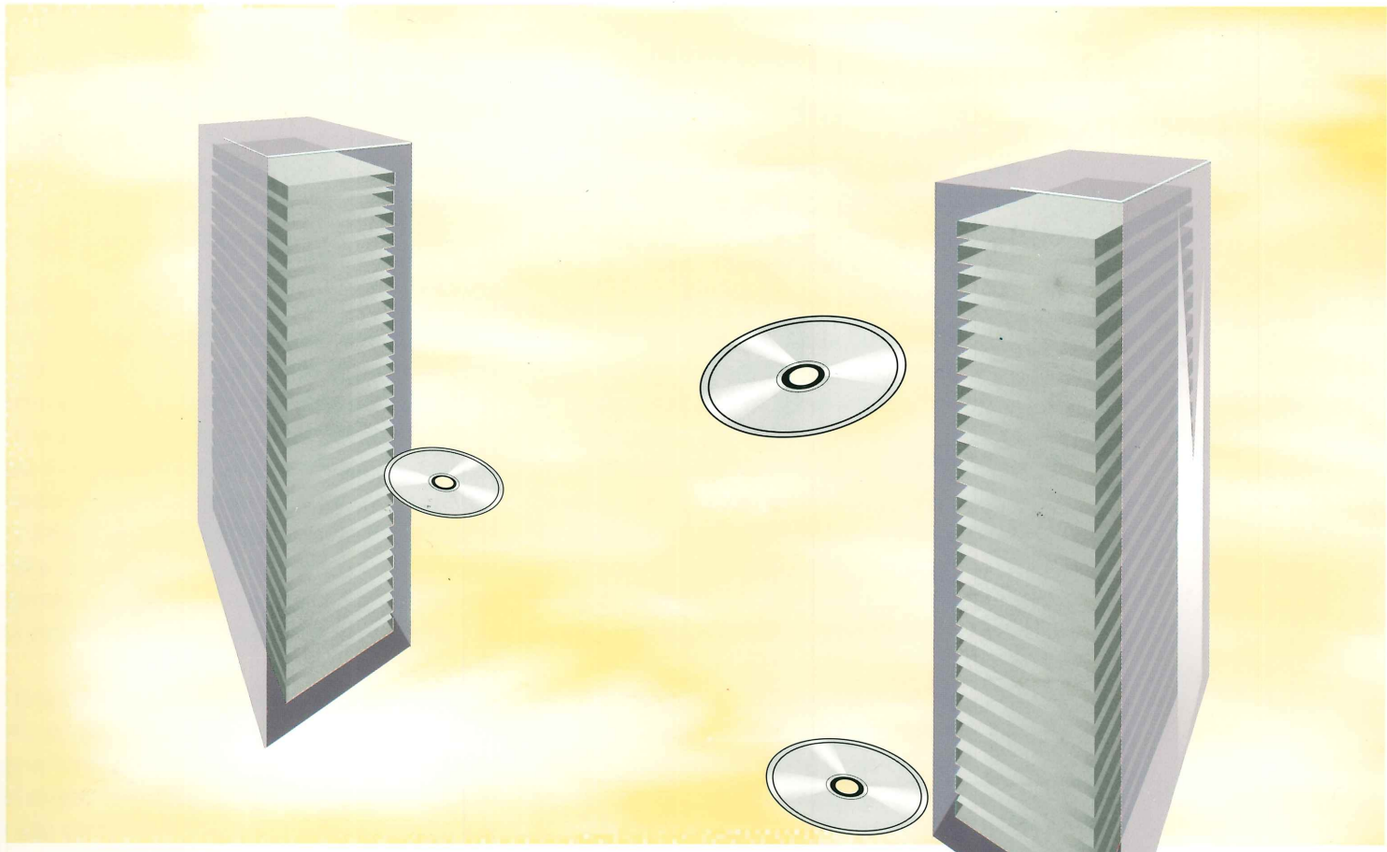
Red IRIS

Plan Nacional de I+D

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

nº 32



nº 32
julio 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.:5855150 Fax: 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

Víctor Castelo

El World Wide Web está siendo la estrella y al mismo tiempo la locomotora de la Internet ya que con su uso tremendamente atractivo y versátil casi se ha convertido en la panacea universal. El único problema es que las imágenes que contiene, a veces de un tamaño considerable, son grandes consumidoras de ancho de banda y con las líneas de que disponemos en estos momentos, sobre todo en algunos sitios (aunque pensamos que ya queda poco para remediarlo), pueden suponer la puntilla definitiva o la mala suerte de ni siquiera poder hacer un buen salto de Web.

RedIRIS deberá seguir siendo la red académica y de investigación con un alto contenido de experimentación en nuevas tecnologías y de recursos dentro del mundo de la I+D.

Creo que el uso indiscriminado o incorrecto de las redes, es una mala práctica. En las redes se hacen pruebas, se navega en busca de lo desconocido y a veces se juega un poco, pero hay que tener una cierta conciencia ecológica que nos lleve a un buen uso de los recursos limitados de que disponemos. Es "bueno" que las redes se colapsen, porque es señal de que se usan, pero que ese uso sea mayoritariamente un buen uso de acuerdo a los fines previstos. Lo difícil es concienciar a la gente de esas buenas costumbres sobre todo cuando no les viene luego la factura de la luz por habersela dejado encendida. Los tamaños de las imágenes, el empleo de videoconferencias, el uso inadecuado de las listas de distribución, las NEWS que tienden al infinito, el FTP brutal de cosas que no nos hacen falta para nada, son algunas de esas malas costumbres (al menos en las circunstancias actuales) con las que habría que sensibilizar a los usuarios para que se lo pensasen dos veces antes de hacerlas.

Incluso creo, aún con el estado de saturación en que nos podamos encontrar ya, que en algunas instituciones todavía no se hace un uso muy extendido de las aplicaciones telemáticas y que todavía quedan muchos usuarios que no utilizan multimedia y sólo hacen uso del correo electrónico. Así pues, está claro que en las mismas condiciones de aplicación actuales aún tenderá a crecer mucho el tráfico. Esperemos que ese crecimiento vaya acompañado de unos anchos de banda adecuados.

Y este tirón de la Internet ha supuesto un movimiento en todos los sentidos y sobre todo en el de que la demanda está haciendo que aparezcan proveedores todos los días hasta que dentro de poco tengamos un quiosco de Internet en cada esquina. Incluso algunos particulares cuando llaman a RedIRIS equivocadamente para conectarse y se les dice que esto es la red académica y de investigación y que no se les puede dar servicio ya no preguntan por los proveedores, sino cómo se pueden hacer ellos proveedores. Otro de los efectos derivados ha sido el bombardeo de todo tipo de noticias en prensa y otros medios de comunicación, a veces no del todo ciertas y la proliferación de infinitos cursos sobre la Internet. Parece en efecto que el fenómeno Internet ya está cuajando y lo importante es que está llegando también a un gran número de personas y empresas que van a ver ampliados sus horizontes en todos los sentidos y que la imaginación se está desarrollando para poner a punto productos de uso y sobre todo consumo en Internet.

En esta película de Internet en España, RedIRIS es la red pionera pero con la humildad de que aunque en estos momentos tengamos el mayor número de usuarios (seguramente con el mayor conocimiento sobre Internet) tal vez dentro de un cierto tiempo la parte comercial sea aun mayor. En todo caso RedIRIS deberá seguir siendo la red académica y de investigación con un alto contenido de experimentación en nuevas tecnologías y de recursos dentro del mundo de la I+D.

En este segundo Boletín del 95 el apartado de Actualidad comienza con una noticia sobre RedIRISdial, servicio que procede de la evolución del anterior Servicio Central de Buzones, que creemos imprescindible, pero en cada momento habrá que estudiar la demanda y

dimensionarlo según las circunstancias. Además tenemos una serie de noticias sobre convenios: con la Universidad Jaume I, para potenciar nuestro WWW, y con Sun Microsystems y Apple Computer España que aumentarán la información de interés disponible en nuestros servidores. El resto son noticias sobre algunas de las actividades acontecidas en los diversos proyectos y organizaciones en los que estamos implicados con un resumen sobre el último JENC celebrado en Tel-Aviv.

La segunda parte del artículo de Lourdes López y Eloy Portillo completa su visión sobre la seguridad en redes en diferentes entornos y presenta proyectos y aplicaciones prácticas para las que ha llegado el momento y que seguramente dentro de muy poco comenzaremos a utilizar de forma más o menos habitual.

En "Veinticinco años de Internet: una retrospectiva autobiográfica" José Barberá presenta una panorámica histórica de la Internet, desde dentro, en primera persona, con un punto de vista muy especial de cómo "sintió" el desarrollo de los acontecimientos, incluida la fase OSI, al menos en Europa, hasta la situación de predominio actual evidente, e incluso hace una reflexión de la evolución y los retos que se plantean de cara a un futuro próximo.

Por último quiero señalar la inclusión en el Boletín de la nueva sección Prontuario, que tiene el objetivo de dar en soporte papel (a veces muy útil) un resumen de datos para tener siempre a mano y que trataremos de completar, mantener y mejorar.

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

Servicio RedIRISdial

A finales del pasado año se lanzó un proyecto piloto destinado a dar acceso a Internet vía Red Telefónica Conmutada utilizando protocolos SLIP. Esto suponía una notable mejoría con respecto al anterior Servicio que se venía ofreciendo vía conexión a una máquina intermedia. Después de una larga migración de casi 30 organizaciones y 200 buzones, a principios de junio de 1995 este Servicio RedIRISdial se puede considerar ya como consolidado con un amplio abanico de aplicaciones. Con este Servicio se ha visto por una parte aumentada la problemática (seguridad, rendimiento de los accesos debido al uso de interfaces gráficas, etc), pero por otra además de la mejora del entorno para el usuario, aumentan las perspectivas de acoplarse de forma muy sencilla a la nueva tecnología emergente: RDSI.

Este Servicio únicamente permite la conexión individual de PC´s a Internet. Está dirigido a Organizaciones afiliadas a RedIRIS con un número reducido de usuarios reales de comunicaciones, que no dispongan de recursos técnicos ni de personal especializado . También sería útil como paso inicial para una conexión plena mientras se obtiene una masa crítica de usuarios. Es importante resaltar que no se ofrece acceso a peronas que no pertenezcan a una Organización. Los únicos conocimientos requeridos para poder disponer de Internet como una potente herramienta de trabajo a costo muy reducido son los del Sistema Operativo de su PC: MS-Windows o MAC. RedIRIS les proporciona los servicios de conectividad: gestión del servidor de nombres, routing, servidor de correo electrónico....

RedIRISdial proporciona un acceso eventual, completo y directo a Internet. Las Organizaciones englobadas en este Servicio tienen los mismos derechos y obligaciones que aquellas englobadas en el Servicio SIDERAL. Evidentemente tendrán ciertas desventajas o inconvenientes algunas de las cuales podrán neutralizarse optimizando el tiempo de conexión de las aplicaciones on-line. La intención de RedIRIS es ofrecerles la posibilidad de que dispongan de un servidor "lógico" WWW, es decir, RedIRIS pondría a disposición de estas organizaciones su servidor WWW, a condición de que sean ellas las responsables del mantenimiento del mismo. También se les ofrecería el mismo servicio para FTP/anonymous.

Las aplicaciones que se ofrecen a las organizaciones que utilizan el servicio RedIRISdial son: archie, ftp, gopher, news, whois, Web y correo electrónico. De todas ellas sólo el correo electrónico será off-line, lo que les permitirá un ahorro económico ya que será la herramienta más usada por estas organizaciones. RedIRISdial permite un número razonable de buzones por Organización.

Para poder ofrecer este Servicio RedIRIS dispone actualmente de 9 accesos asíncronos hasta 14.400 bps (V32bis) dentro de un único grupo de salto en Madrid. También soporta MNP clase 5 para compresión de datos (V42), contemplándose la posibilidad, según la demanda, de ampliar el número de accesos.

Como interface de acceso se recomienda utilizar el paquete Chameleon, que será el único al que se dé soporte. El objetivo de recomendar la utilización de una única interface por parte de los clientes permite fundamentalmente una mejor gestión y soporte del Servicio. Existe además una rebaja en el precio del paquete para aquellas organizaciones afiliadas a RedIRIS.

El protocolo de acceso soportado para este servicio es SLIP. Se utiliza asignación estática, hasta 4 direcciones IP por Organización, cada una de ellas con un login y password. Se ha elegido esta política de acceso para tener cierto control de los usuarios. Ha sido la política más adecuada para una puesta en marcha del Servicio de forma rápida.

Actualmente se está trabajando en aras de mejorar el Servicio en tres campos que considero muy importantes:

(1) Ampliación de los puntos de acceso en otras zonas.
(2) Acceso vía RDSI.
(3) Seguridad.

El objetivo del primer punto consiste en ubicar alguna sucursal de acceso en zonas donde vaya existiendo demanda de este tipo de Servicio. Estas sucursales consistirían en un servidor SLIP/PPP con un número adecuado de accesos asíncronos.

Inicialmente los objetivos del segundo punto son experimentales, como por ejemplo:

Servicio RedIRISdial

Servicio RedIRISdial

Convenio con la Universidad Jaume I

Reunión en Madrid del Task Force ATM de TERENA

seleccionar hardware y software asequible para TCP/IP sobre RDSI; obtener conocimientos sobre equipamiento (tarjetas y routers) de PPP sobre RDSI; seguridad tipo CLIP (Calling Line Identification Presentation) y por supuesto poder ofrecer el servicio en un futuro siempre que la infraestrucutra de la red lo permita. En lo referente al tema de seguridad inicialmente se intentará implementar CHAP (Challenge Authentication Protocol) y más adelante algún tipo de seguridad tipo Kerberos. Cualquier modificación del servicio tanto a nivel de seguridad, protocolo, tecnología sera fácil de implementar por los usuarios que utilicen Chameleon como interface. Cualquiera de estos temas sobre acceso a Internet vía RDSI/RTC se tratan en la lista:

dialforo@listserv.rediris.es.

(Jesus.Heras@rediris.es)

Convenio de colaboración con la Universidad Jaume I

La Universidad Jaume I de Castellón y el Consejo Superior de Investigaciones Científicas próximamente van a firmar un convenio de colaboración que ya se encuentra en fase de estudio muy avanzada y cuyos objetivos principales son los siguientes :

a) Diseño y desarrollo de un servidor basado en la tecnología World Wide Web sobre RedIRIS y los servicios que presta a la comunidad I+D.

b) Ayuda y soporte en la instalación de la aplicación W1WW a la comunidad I+D española.

c) Desarrollo de una guía electrónica dirigida a usuarios finales y en formato hipertexto, sobre recursos de información disponibles en la comunidad RedIRIS.

Creemos que de esta colaboración entre los responsables de los servicios de información de RedIRIS y los expertos de la UJI, que han demostrado una brillante trayectoria en este campo, va a resultar un magnífico producto que permita acceder a la información sobre Internet, los servicios que proporciona RedIRIS y lo más importante, los recursos de I+D de este país, de una forma fácil y eficiente.

(Victor.Castelo@rediris.es)

Reunión en Madrid del Task Force ATM de TERENA

El 5 de mayo se celebró en El Centro de Comunicaciones CSIC RedIRIS la reunión de trabajo del piloto ATM de TERENA. En las siguientes líneas se describe muy brevemente los puntos tratados en aquella reunión, y la situación en que se encuentra el piloto en RedIRIS.

Inicialmente se trató sobre el estado de la conectividad dentro del piloto. Con la conexión próxima de otras redes, se planteó modificar alguno de los caminos virtuales, de tal modo que la topología lógica se adapte al máximo a las líneas físicas existentes entre las diferentes PNOS y no se supere el caudal máximo permitido a cada una de las organizaciones que participan.

Con posterioridad, la discusión se centró en las aplicaciones sobre ATM. Las aplicaciones multicast (video y audio en MBONE) servirán como marco de pruebas de esta nueva infraestructura ya que son las que requieren un mayor ancho de banda y el ATM les proporciona unas posibilidades que no disponen con otras tecnologías de conmutación.

Durante varias horas se estuvo discutiendo el mejor modo de establecer nuevos túneles de MBONE, de tal forma que se minimice el impacto en la red actual. Se optó por hacer uso del protocolo multicast DVMRP, con estaciones de trabajo como encaminadores multicast, frente a la opción de PIM con routers en ciscos.

Por último se comentaron los diferentes esquemas de direccionamiento en ATM (formato E.164 y NSAP) a partir de un documento presentado por la red inglesa UKERNA.

RedIRIS, después de haber tenido un problema con la tarjeta ATM del router, éste

tiene establecidas dos conexiones virtuales sobre ATM. Los perfiles de estos dos caminos son: RedIRIS-SURFnet con un caudal máximo de 2 Mbit/s durante las 24 horas del día los siete días de la semana y RedIRIS-SWITCH con un caudal máximo de 2 Mbit/s de lunes a viernes de 8:00 a 15:00.

Según la petición de participación en el piloto ATM firmado por RedIRIS con Telefónica, la red académica dispone de un caudal máximo de 10 Mbit/s, de tal modo que será posible aumentar en un día de la semana (los miércoles) uno de los caminos a 8 Mbit/s, tal como estaba previsto inicialmente.

En la reunión de Madrid, se decidió dividir a finales de mayo o principios de junio la conexión RedIRIS-SURFNET en otras dos, RedIRIS-UKERNA, UKERNA-SURFNET, que se tratan de conexiones más sensatas teniendo en cuenta la topología física de la red.

Actualmente RedIRIS dispone de una red local sobre ethernet compuesta por una estación de trabajo que mantendrá un encaminador multicast y un server con news para hacer uso de las conexiones sobre ATM. En un futuro próximo esta red se sustituirá por una LAN ATM.

(Celestino.Tomas@rediris.es)

Nominación del Centro de Comunicaciones CSIC RedIRIS como SunSITE

Como una de las acciones emprendidas dentro del nuevo marco de colaboración establecido entre Sun Microsystems y el CSIC la Corporación de Sun Microsystems nos ha confirmado la nominación del Centro de Comunicaciones CSIC RedIRIS como SunSITE.

Como consecuencia de dicha nominación Sun realizará la donación de un servidor UNIX (SparcServer 1000) con el objeto de facilitar el acceso, vía Internet, fundamentalmente al software de dominio público e información de tecnología. Esta donación complementará la ampliación de los servicios de información de RedIRIS y de otras aplicaciones que ya en estos momentos se encuentran en fase de instalación en otros dos SparcServer 1000 recientemente adquiridos.

Aprovechamos la ocasión para agradecer a Sun Microsystems Ibérica y en especial a José Cabrera, Carlos Grau y Ángel Ramos el interés personal que han manifestado para hacer realidad esta nominación que esperamos redunde en el máximo beneficio para todos.

(Victor.Castelo@rediris.es)

Apple Virtual Campus

Apple Computer España y RedIRIS han suscrito recientemente un convenio de colaboración para la instalación de un servidor de información basado en la idea de Apple Virtual Campus. Se contará con un servidor WWW conteniendo información especializada de Apple de interés para la comunidad académica y de investigación tal como:

- Material informativo de Apple para la Universidad
- Documentación técnica de nuevos productos
- Actualizaciones y software de sistema
- Proyectos de colaboración Apple-Universidad
- Revista powerScience
- Índice de publicaciones
- Índice de servidores de Apple
- Librería de software educativo
- Testimoniales y colaboraciones
- Eventos, seminarios y cursos.

Las características técnicas del servidor que soportará el World Wide Web son un Apple Internet Server basado en un Servidor Power Macintosh 8150 y el programa servidor WWW para plataforma Mac OS WebSTAR.

Nuestro agradecimiento a Apple Computer España y en particular a Eduardo Santos que en todo momento se han mostrado abiertos a la realización de todo tipo de experiencias dentro del marco de colaboración establecido.

(Victor.Castelo@rediris.es)

Reunión en Madrid del Task Force ATM de TERENA

SunSITE

Apple Virtual Campus

Proyecto de red paneuropea de alta velocidad (TEN-34)

El pasado día 9 de mayo tuvo lugar en Amsterdam la reunión del comité ejecutivo del proyecto TEN-34. Este proyecto trata de lograr la implantación de una red paneuropea de alta velocidad en un período aproximado de 2 años, utilizando la tecnología ATM y en él participaron todas las redes académicas de la Unión Europea.

En esta reunión DANTE informó de la aceptación del proyecto por parte de la Unión Europea dentro del programa Telematics. El resto de la reunión discurrió en la discusión de la financiación de la red y de los posibles suministradores de infraestructura. La subvención de la Unión Europea será de un 30% aproximadamente del coste total del proyecto. Se van a pedir ofertas a los consorcios de comunicaciones más importantes (UNISOURCE, BT, France-Telecom, etc) para poder diseñar la topología más idónea minimizando en lo posible el coste de la red.

El precio por punto de acceso a la red será aproximadamente el mismo para cada país, al tratarse de una "red virtual". Dada la importancia estratégica de este proyecto más adelante en este mismo boletín se dará información pormenorizada del desarrollo e implantación del mismo, pues se espera que la red empiece a estar operativa en el año 1996.

(Manuel.Rincon@rediris.es)

Asamblea General de TERENA

TERENA ha pasado por una delicada situación, ya que no ha existido entendimiento entre el Comité Ejecutivo y la secretaría general, lo que ha llevado a una paralización de las actividades de la misma, durante casi un año.

Los días 18 y 19 de mayo coincidiendo con la 6ª Conferencia conjunta europea sobre redes (JENC), se celebró la asamblea general, que tenía como punto principal del orden del día el voto de confianza a el actual Comité Ejecutivo

UKERNA ha criticado duramente a TERENA por no estar de acuerdo con su funcionamiento.

El Presidente Frode Greisen, ignoraba estos problemas. La mañana anterior a la Asamblea dimitieron los vicepresidentes en bloque dado el mal ambiente reinante. Se presentó una propuesta de reducción de la Junta Directiva a cuatro miembros (tres vicepresidentes y un tesorero) y el Presidente y esta propuesta fue aceptada por mayoría.

Varios países entre ellos Italia y España, propusieron una Junta que conservase antiguos vicepresidentes, pero nombrase a un nuevo presidente. Se propuso a Stefano Trumpy y fue aceptado por mayoría. Esta elección supone romper con el pasado de EARN y RARE. De esta forma Stefano Trumpy es el nuevo presidente de TERENA por un período de dos años y además será el Chairman del JENC del próximo año.

Ahora la nueva directiva tiene ante sí el duro trabajo de reorganizar la Secretaría General que constituye el verdadero órgano ejecutivo de la asociación, y relanzar todas las actividades. Desde aquí les deseamos buena suerte y esperamos participar activamente en todos los proyectos de TERENA.

Desde el punto de vista español, parece una buena elección pues existen relaciones excelentes con la nueva junta.

En el plano económico se pagará una cuota inferior a la suma de las de RARE y EARN, abonándose aparte la participación en proyectos concretos en los que RedIRIS sea activa..

(Manuel.Rincon@rediris.es)

Proyecto EuroCAIRN

Madrid será la sede de la próxima reunión de EuroCAIRN que tendrá lugar durante el mes de junio. Para preparar este evento visitaron Madrid el pasado 9 de mayo el Dr. Chalmers (Chairman de EuroCAIRN) y el Sr. Duxbury (Jefe del Proyecto). Además de preparar la agenda, se realizó una visita a las instalaciones de Rediba (Telefónica I+D),

donde pudieron apreciar algunos de los avances españoles en materia de banda ancha y ATM en el campo de la I+D.

En la próxima reunión se tratará del futuro de EuroCAIRN y de la política española en redes de comunicaciones durante la presidencia española de la Unión Europea en el próximo semestre, cuestión a la que se le da mucha importancia.

El estudio de viabilidad de red pan-europea realizado por DANTE ha sido aceptado y por tanto ha finalizado la primera fase de EuroCAIRN. En el futuro la vocación de este proyecto es coordinar toda la política de desarrollo y expansión de las comunicaciones internacionales entre las diferentes redes académicas, así como la implementación de los distintos servicios previsibles, no sólo a corto plazo sino en horizontes lejanos, estableciendo planos estratégicos.

(Manuel.Rincon@rediris.es)

6th JENC

Durante los pasados días 15-18 de mayo tuvo lugar en Tel-Aviv (Israel) la celebración de la 6ª Conferencia Conjunta Europea sobre Redes (6th JENC), con una participación de más de 300 personas procedentes de unos 30 países y de ellos un nutrido número de españoles que participaron de forma muy activa con varias aportaciones. El congreso, que fue precedido de reuniones de los grupos de trabajo de Terena y una tutoría sobre IPng, se desarrolló con una estructura de sesiones paralelas dividida en los siguientes bloques:

- Tecnología e ingeniería de red
- Soporte informático para trabajo en equipo
- Seguridad y privacidad
- Suministro de información y acceso a ella
- Temas organizativos
- Temas regionales

También se realizaron demostraciones permanentes de varios proyectos y aplicaciones de servicios de red en el entorno académico y de investigación.

Así pues, hubo conferencias para todos los gustos, no hubo preponderancia de ninguno de los diferentes apartados, sino que se mantuvo una tónica general siempre elevada y tan sólo habría que destacar, por sus contenidos más polémicos y políticos, alguna de las conferencias que se celebraron de forma plenaria.

Señalar también el marco impresionante de la celebración como cuna de religiones y la intervención como Chairman de nuestro compatriota José Barberá.

El próximo JENC se celebrará en Budapest (Hungría) del 13 al 16 de mayo de 1996.

(Victor.Castelo@rediris.es)

Proyecto EuroCAIRN

6th JENC

ENFOQUES

Seguridad en redes telemáticas Parte II: Entornos seguros

Lourdes López, Eloy Portillo

La cantidad y el tipo de servicios de seguridad que son necesarios en una red depende de las características de las aplicaciones que se desean proteger. Por lo tanto, no se puede hablar de redes seguras en general, sino de entornos seguros formados por una serie de sistemas integrados para la seguridad.

Introducción

En la primera parte de este artículo titulada *La problemática de la seguridad* se vio cómo los organismos de normalización proponen dotar a las redes telemáticas de una serie de servicios de seguridad para protegerlas contra posibles ataques y operaciones ilegales. Estos servicios de seguridad se proporcionan a través de una serie de mecanismos de seguridad que se basan, en su mayoría, en técnicas criptográficas.

La cantidad y el tipo de servicios de seguridad que son necesarios en una red depende de las características de las aplicaciones que se desean proteger. Por lo tanto, no se puede hablar de redes seguras en general, sino de entornos seguros formados por una serie de sistemas integrados para la seguridad, que incluyen además de una serie de servicios de seguridad sobre varias aplicaciones, una gestión de claves global.

En esta segunda parte del artículo se va a presentar un resumen de las experimentaciones sobre varios sistemas seguros, en las que ha participado el Departamento de Ingeniería y Arquitecturas Telemáticas (DIATEL) de la E.U.I.T. de Telecomunicación de la UPM. Como se verá a continuación, estos sistemas permiten proporcionar servicios de seguridad sobre una o varias aplicaciones que realizan transferencia de información a través de redes y la mayoría de ellos utilizan en su base, criptografía de clave pública.

La necesidad de establecer un entorno seguro

En la actualidad, la falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios en su labor de piratería.

Tal y como se avanzaba en la primera parte de este artículo, la criptografía por sí sola no es suficiente para prevenir los posibles ataques que se perpetran sobre las redes, sino que es necesario establecer unos mecanismos más complejos que utilizan los distintos sistemas criptográficos en sus cimientos. Pero el problema no queda solucionado instalando en una serie de servidores herramientas de seguridad, porque ¿quién tendría acceso a esas herramientas?, ¿a qué aplicaciones se aplicarían?, ¿qué sucedería si sólo uno de los dos interlocutores en una comunicación tiene acceso a herramientas de seguridad?. Por lo tanto, cuando se habla de seguridad en redes es necesario definir el entorno en el que se va a aplicar.

La definición de un entorno seguro implica la necesidad de estudiar varios aspectos y de establecer una infraestructura que dé soporte a los servicios de seguridad que se quieren proporcionar. Lo primero que hay que establecer es qué aplicaciones necesitan seguridad y cuántos servicios se necesitan. En segundo lugar hay que determinar cómo se van a proporcionar esos servicios, si van a ser transparentes al usuario, si se le va a dejar elegir el tipo de servicio, etc. También es necesario determinar en qué nivel se van a proporcionar, si en el nivel de aplicación o en niveles inferiores. Y sobre todo, tanto si se utiliza criptografía de clave secreta, como si se utiliza criptografía de clave pública es necesario diseñar un sistema de gestión de claves y definir una política que determine la forma en la que se debe operar.

Cuando se utiliza únicamente criptografía de clave simétrica, aunque el sistema de generación de claves suele ser sencillo, ya que no se requiere una gran infraestructura para soportarlo, los

mecanismos de distribución de las claves suelen ser muy complejos. En este caso, los principales parámetros que hay que tener en cuenta son el modo de difundir la clave secreta de forma segura a las dos entidades que van a utilizarla y la frecuencia con la que se deben renovar las claves para evitar que sean desveladas.

Cuando se utiliza criptografía de clave pública, el sistema de gestión de claves se complica. En primer lugar es necesario almacenar las claves públicas en un lugar al que tengan libre acceso todos los usuarios que forman parte del entorno de seguridad. ITU, en su recomendación X.509 [1], propone la utilización del Directorio para este fin; pero no todos los usuarios de seguridad tienen acceso al Directorio X.500, por lo que en muchos entornos es necesario crear o utilizar otro tipo de bases de datos.

El segundo problema que se plantea al utilizar criptosistemas de clave pública, es que las claves públicas, por el simple hecho de ser públicas, están expuestas a la manipulación por parte de todos los usuarios, por lo que es necesario buscar un mecanismo que permita confiar en su validez. Siguiendo el ejemplo de los actuales sistemas legales, aparece la figura de una autoridad de confianza que se encarga de certificar las claves públicas. Estas autoridades, conocidas con el nombre de Autoridades de Certificación (CA "Certification Authority"), emiten certificados de las claves públicas de los usuarios firmando con su clave secreta un documento, válido por un período determinado de tiempo, que asocia el nombre distintivo de un usuario con su clave pública. En la recomendación X.509 [1] se define en sintaxis ASN.1 el siguiente modelo de certificado:

Un problema que se plantea al utilizar criptosistemas de clave pública, es que las claves públicas, por el simple hecho de ser públicas, están expuestas a la manipulación por parte de todos los usuarios.

```
Certificate ::= SIGNED SEQUENCE{
        version                 [0] Version DEFAULT 0,
        serialNumber            CertificateSerialNumber,
        signature               AlgorithmIdentifier,

        issuer                  Name,
        validity                Validity,
        subject                 Name,
        SubjectPublicInfo       SubjectPublicInfo,
        issuerUniqueId          [1] IMPLICIT BIT STRING OPTIONAL,
        BJECTUniqueId           [1] IMPLICIT BIT STRING OPTIONAL}
```

Además, para que los usuarios puedan estar seguros de la validez de los certificados de las claves pública de sus interlocutores, la CA debe mantener una lista con los certificados emitidos por ella y que han sido revocados por detección de un uso fraudulento de la clave pública certificada o de la clave secreta asociada. Estas listas se conocen con el nombre de Listas de Certificados Revocados (CRL, "Certificate Revocation List").

Cuando la comunidad de usuarios crece, una sola CA puede verse desbordada por el número de certificados que tiene que gestionar. En otros casos, las empresas o instituciones quieren tener cierto control sobre la manera en que sus usuarios generan las claves, la caducidad de los certificados, etc. Esto hace conveniente distribuir las funciones de certificación entre varias CAs, cuya política de seguridad puede ser diferente. En la recomendación X.509 [1] ya se prevé la necesidad de una organización de CAs donde se certifiquen unas a otras, sin indicar el tipo de relación organizativaorganizativaorganizacionalorganizativaorganizativaorganizacional que se

La transferencia segura de información a través de las redes es en la actualidad, el principal problema que los investigadores intentan solucionar.

debe establecer entre ellas. De esta forma, dependiendo de las necesidades de cada entorno han aparecido distintos modelos de organización de CAs.

Entorno seguro para la transferencia de información

Uno de los puntos más vulnerables de las redes frente a ataques de intrusos, es la captura de información durante su transferencia. Aunque cada sistema que forma parte de una red se proteja internamente a sí mismo y a la información que tiene almacenada, cuando la información se transfiere de un sistema a otro no se conoce a priori el encaminamiento que va a seguir ni las medidas de seguridad que poseen los sistemas por los que atraviesa y los medios por los que se transmite. Por este motivo la transferencia segura de información a través de las redes es en la actualidad, el principal problema que los investigadores intentan solucionar.

DIATEL ha estado trabajando en los últimos años en el proyecto de la UE, COST225 "Secure Communications", cuya coordinación en la última fase, ha sido llevada a cabo por uno de los miembros del grupo de seguridad del Departamento, que ha realizado la función de "chairman" [2]. El objetivo de este proyecto, que ha concluido al inicio de 1995, ha sido el de estudiar y experimentar en varios entornos seguros en los que se realiza transferencia de información, como son el correo electrónico y la transferencia de ficheros a través de FTP y FTAM. Concretamente, en DIATEL se ha montado un entorno de seguridad que permite transferir información con distintos niveles de seguridad, a través de cualquier aplicación.

El desarrollo consta de dos partes fundamentales. La primera parte consiste en una aplicación, denominada **SECKit** [3], que permite a un usuario manejar distintas herramientas de seguridad con el fin de poder convertir a un fichero normal, en un fichero con un cierto nivel de seguridad. La aplicación SECKit que por su carácter experimental no incluye un interfaz de usuario amigable, presenta un único menú en el que aparece la lista de operaciones que permite realizar.

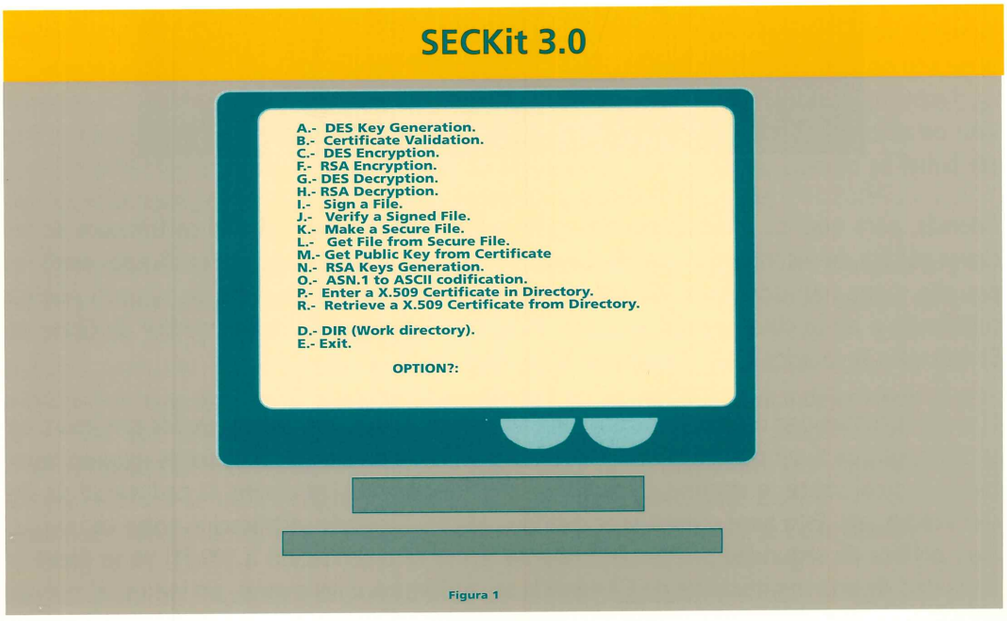


Figura 1

La segunda parte consiste en el desarrollo de un servidor de seguridad denominado **SECServer** [4]. Este servidor de seguridad no sólo oferta los servicios de una autoridad de certificación (generación de certificados de claves públicas), sino que además ofrece la posibilidad de generación de claves RSA para aquellos usuarios que no sean capaces de generarlas, y se encarga del almacenamiento y distribución de los certificados de los usuarios que lo soliciten. Las peticiones de servicios al SECServer se realizan a través de correo electrónico y el SECServer envía los certificados o las claves solicitadas a través de correo electrónico, FTP o FTAM.

En este entorno de seguridad los usuarios antes de transferir un fichero lo pueden transformar en un fichero firmado, en un fichero encriptado con DES o RSA, o en lo que en el entorno se denomina, un fichero seguro. Y cuando reciben un fichero firmado, encriptado o seguro, procedente de otro usuario, lo pueden transformar en el fichero original, verificando la validez de la información recibida.

Un fichero seguro es el resultado de combinar los mecanismos de seguridad de firma y encriptado con el fin de proporcionar los servicios de autenticación de origen y destino, integridad, confidencialidad y no repudio de origen.

Un fichero seguro es el resultado de combinar los mecanismos de seguridad de firma y encriptado con el fin de proporcionar los servicios de autenticación de origen y destino, integridad, confidencialidad y no repudio de origen.

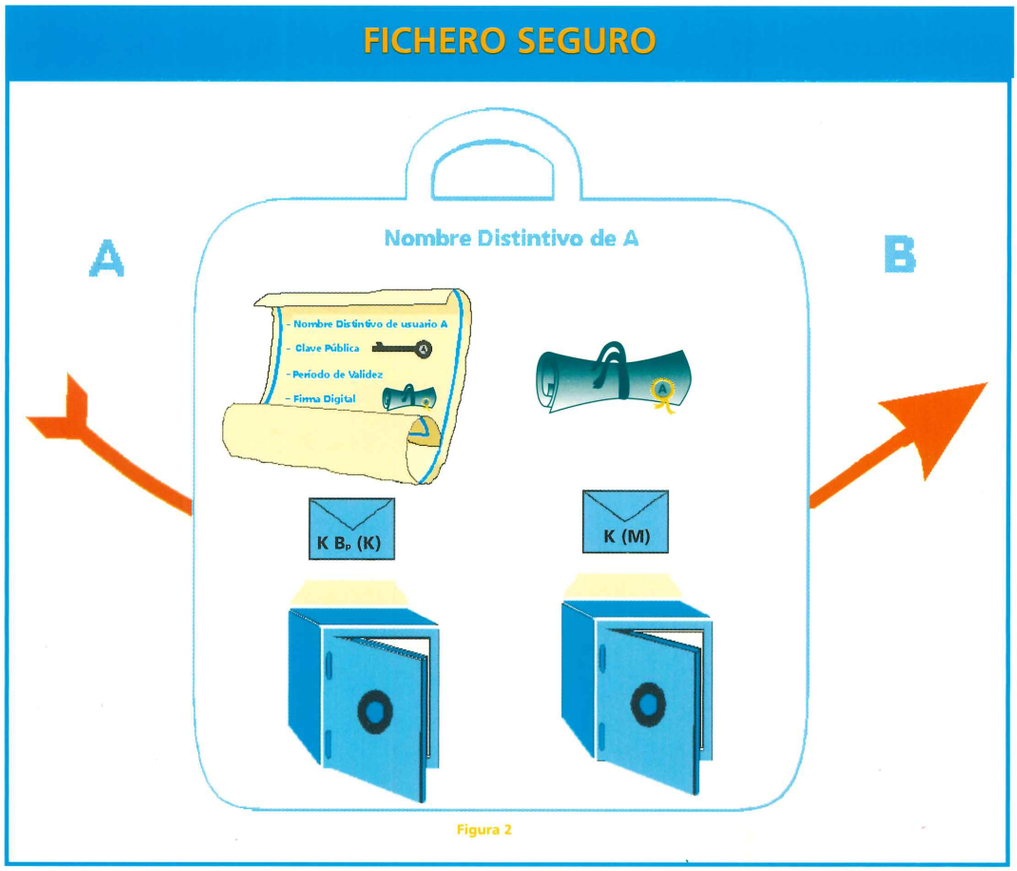


Figura 2

Cuando un usuario A desea enviar un fichero seguro a un usuario B, debe seguir los siguientes pasos:

1. A debe cifrar el fichero que quiere enviar a B. Para cifrarlo utilizará una clave simétrica K, generada en ese momento, y un algoritmo de cifrado DES.

Cualquier usuario de Internet que tenga correo electrónico puede acceder al SECServer para solicitar claves RSA o certificados.

2. Para que B pueda descifrar el contenido del fichero necesita conocer la clave K empleada. A debe enviar a B la clave K de una forma segura. Para ello, A utilizará un algoritmo de cifrado asimétrico RSA y cifrará K con la clave pública de B. De esta forma se garantiza que el único destinatario que puede recibir el fichero original es B. Cuando B reciba el fichero seguro, deberá utilizar su clave secreta para obtener la clave K, de esta forma sólo B podrá conocer la clave de cifrado empleada, con lo que queda totalmente garantizada la confidencialidad del contenido del fichero.

3. Para proporcionar el servicio de integridad y de autenticación del origen de los datos, A firmará el fichero original comprimiendo el contenido con una función hash y cifrando el resultado con su clave secreta. Cuando B reciba el fichero podrá verificar la firma comprobando así la integridad del mismo y autenticando al originador de los datos. Para verificar la firma, B deberá descifrarla utilizando la clave pública de A, obteniendo así el contenido del fichero comprimido. Si B obtiene la clave pública de A de su certificado, queda garantizado ante la CA que A es quien ha enviado el certificado. Una vez descifrado el fichero original, B puede comprimirlo con la función hash que se ha empleado en la firma, comparando el resultado con el obtenido de la firma, de forma que si ambos coinciden queda garantizado que el contenido del fichero original no ha sido manipulado durante su transferencia.

El entorno diseñado en esta experimentación es un entorno muy abierto. Cualquier usuario de Internet que tenga correo electrónico puede acceder al SECServer para solicitar claves RSA o certificados. Si los usuarios del servidor tienen acceso al Directorio X.500 [5], ellos mismos pueden guardar sus certificados en su entrada correspondiente y pueden recuperar los certificados de sus interlocutores. Los usuarios que tienen certificadas las claves públicas por la CA del entorno no necesitan obligatoriamente tener instalada la aplicación de usuario SECKit para realizar comunicaciones seguras; basta con que los usuarios tengan un traductor de sintaxis ASN.1 y una implementación de los algoritmos utilizados en el entorno.

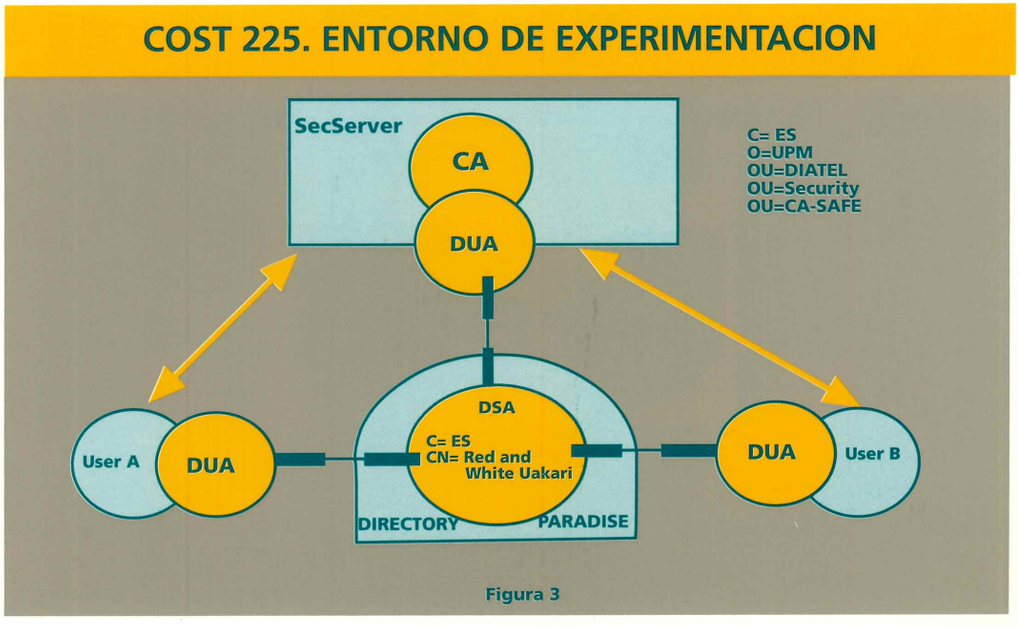


Figura 3

En la última fase del proyecto COST 225, varias de las instituciones participantes, y entre ellas DIATEL, han centrado sus esfuerzos en plantear nuevos modelos en los que participan varias CAs [6]. Se han estudiado distintas arquitecturas de organización de las CAs y se han buscado soluciones para que los usuarios puedan conocer los caminos de certificación compuestos por los certificados que se deben examinar para que un usuario A tenga plena confianza en la validez de la clave pública de un usuario B.

El proyecto PASSWORD tenía como objetivo central el desarrollo de un entorno de seguridad apropiado para la comunidad investigadora europea.

Un experiencia de entornos seguros en el ámbito académico: Proyecto PASSWORD

El proyecto PASSWORD *Piloting an European Security Infraestructure for Network Application* financiado por la Unión Europea dentro del programa VALUE tenía como objetivo central el desarrollo de un entorno de seguridad apropiado para la comunidad investigadora europea. Se trataba de poner a prueba la madurez de las tecnologías empleadas en la provisión de servicios de seguridad en redes telemáticas en aspectos como la adecuación y completitud de los protocolos y herramientas criptográficas, adecuación del hardware disponible (tarjeta inteligente), aspectos ergonómicos, etc. [7]

Para probar la dificultad real de desarrollar independientemente sistemas que interoperen entre sí, se constituyeron tres consorcios. Cada uno de los consorcios desarrolló un sistema de seguridad completamente independiente a partir de cero, con los que luego se probarían distintas comunicaciones seguras. Cada consorcio estaba formado por instituciones de un país distinto de la Unión Europea y cada uno estaba liderado por una prestigiosa institución investigadora.

- Gran Bretaña, (encabezaba el consorcio el University College de Londres)
- Alemania (GMD), y
- Francia (INRIA)

El diseño inicial incluye una infraestructura de gestión de claves basada en claves certificadas según X.509 y el aseguramiento de varias aplicaciones de uso común: Directorio X.500, documentos ofimáticos en formato ODA y correo electrónico, tanto X.400 (versión 88) como Internet PEM. Cada aplicación era modificada para hacer uso de los servicios de seguridad y todas ellas usaban una misma infraestructura de claves. El directorio cumplía una doble función de aplicación asegurada y colaborador de la infraestructura de certificados al ser la vía preferida para la distribución de estos.

Diatel participó en el proyecto como institución piloto, instalando una DSA segura y dos Autoridades de Certificación con varios usuarios. Durante la experiencia se pudieron realizar varias comunicaciones seguras con los otros participantes en el proyecto. Las aplicaciones probadas fueron, correo Internet PEM y Directorio seguro X.500 utilizando autenticación fuerte en peticiones y respuestas. Para ello se utilizó el software público SecuDE 4.2 del GMD [8] e ISODE 8.0. En el transcurso del proyecto se contribuyó a depurar el software y afloraron algunas de las limitaciones de este modelo que se exponen más adelante.

Uno de los requisitos para el uso de los certificados de clave pública consiste en que se deben establecer mecanismos que eviten el mal uso de las claves, evitando así que se extienda la jerarquía más allá de sus límites naturales.

El Correo PEM

PEM (Privacy Enhancement for Internet Electronic Mail) es el formato de correo seguro normalizado por Internet [9]. Incluye los servicios de autenticación fuerte de origen, integridad, no repudio en el origen y, opcionalmente, privacidad. Los tres primeros servicios se consiguen por medio de la firma digital tal y como se pudo ver en la primera entrega de este trabajo. Para implementar la confidencialidad se hace uso del algoritmo simétrico DES: para cada mensaje se utiliza una clave DES que llamaremos de sesión. Se cifra el mensaje con esta clave y a continuación se envía encriptada con la clave secreta del destinatario. De esta manera se garantiza que sólo el destinatario puede recuperar la clave de sesión y leer el mensaje.

En cualquiera de los casos (con o sin privacidad) tanto el mensaje como la firma y la clave de sesión se encapsulan en un formato imprimible (7 bits) que luego puede ser incluido en un mensaje RFC 822 o bien transmitido por cualquier otro medio. El formato de un correo PEM ya ha sido comentado con detalle en las páginas de este boletín [10]. En la actualidad se trabaja en la implementación de los mismos servicios al correo multicuerpo y multimedia MIME.

Jerarquía de certificación

Como se expuso anteriormente, la existencia de múltiplesmultiples CAs obliga a establecer algún modelo organizativo entre ellas. Si la organización es jerárquica, los problemas de autoridad y consistencia se simplifican. Se llama camino de certificación al conjunto de certificados que se deben comprobar para llegar de un usuario A a otro usuario B. Cuando se adopta una estructura perfectamente piramidal, cada usuario necesita únicamente comprobar los certificados que de cada CA emite su superior hasta llegar a un punto de confianza común que en el peor de los casos será el vértice de la pirámide.

En el proyecto PASSWORD se planteó inicialmente una arquitectura basada en una CA de máximo nivel (Top Level CA o TLCA) por país y una serie de Policy CAs en un segundo nivel. Dependiendo de cada Policy CA se extienden una serie de CAs cuyos usuarios deben cumplir la política de Seguridad establecida por esta Policy CA. De modo parecido, la comunidad Internet había establecido para su correo seguro PEM, una jerarquía similar donde todas las Policy Cas son certificadas "a efectos de registro" por una TLCA llamada Internet Policy Registration Authority IPRA [9]. La dificultad para usar simultáneamente ambas jerarquías, y el deseo de utilizar correo PEM hizo que finalmente se cambiaran las especificaciones y se adoptara una jerarquía PEM. Al no estar operativa la IPRA en el momento de las experiencias, se sustituyó por una TLCA creada al efecto que fue operada por el UCL.

Uno de los requisitos para el uso de los certificados de clave pública consiste en que se deben establecer mecanismos que eviten el mal uso de las claves, evitando así que se extienda la jerarquía más allá de sus límites naturales. Una CA no debe certificar usuarios fuera del ámbito para el que fue creada. Un usuario tampoco debe usar su clave pública para emitir un certificado. Para facilitar la detección de estas irregularidades, tanto la jerarquía inicialmente planteada en PASSWORD como la jerarquía PEM, establecen la "regla de subordinación" que indica que el Distinguished Name (DN) de una CA debe ser un subconjunto del DN del usuario que certifica, garantizando así que el usuario pertenece a la organización o unidad organizativa asociada con la CA. Por ejemplo, se detectaría

inmediatamente que es fraudulento un certificado extendido por la CA <C=ES; O=Banca Hispano-Gibratareña; OU=Compras y Suministros> a favor de un usuario <C=ES; O=UPM; OU=Diatel; CN=Pérez>. Sólo las TLCAs y las Policy CAs quedan exentas del cumplimiento de esta regla.

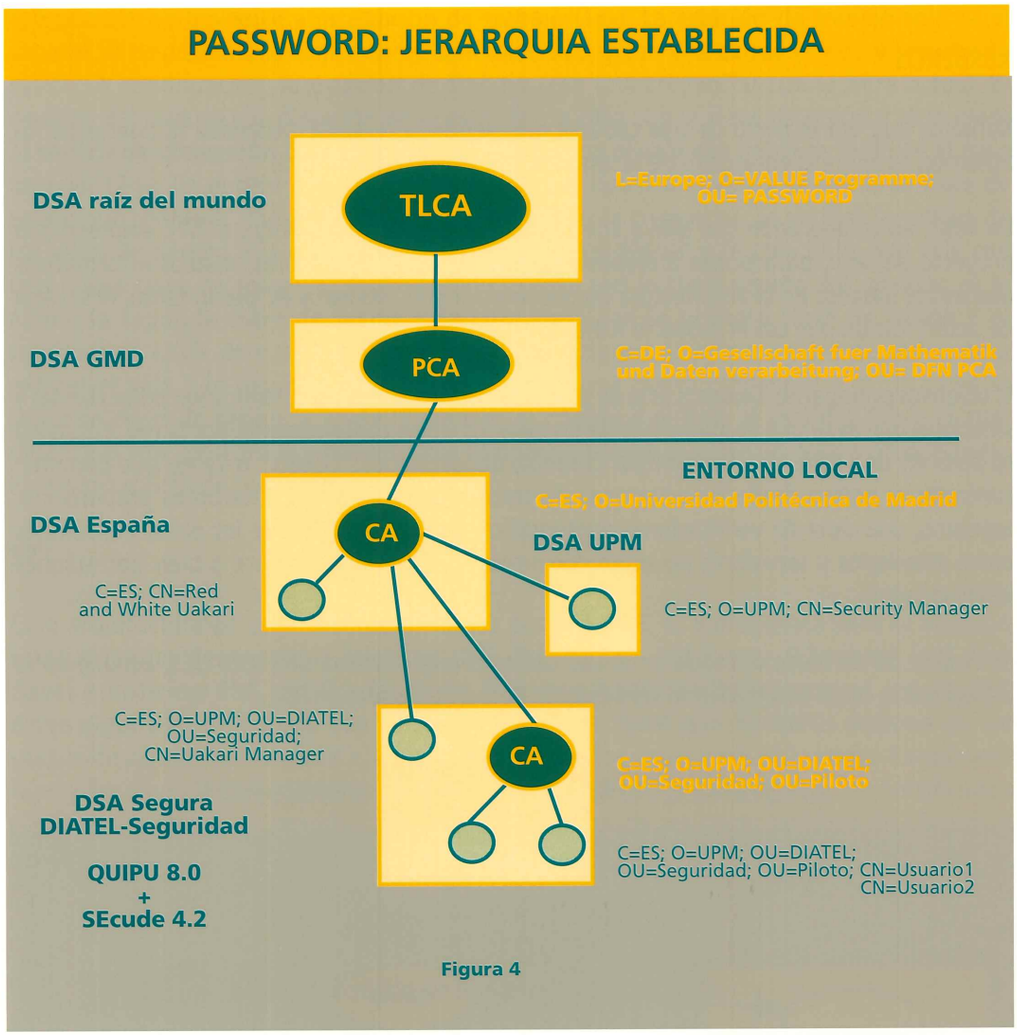


Figura 4

Esta regla, aunque eficaz, se considera demasiado estricta y plantea problemas derivados, entre otras cosas, de la equivalencia que se hace del nombre de una organización o un departamento con su CA. Muchas veces, una organización puede necesitar varias CAs en el mismo lugar de su árbolarbol organizativo, bien para implementar varias políticas con distintos grados de confianza, bien para separar usos diferenciados de las claves (comunicaciones internas frente a externas ...). Para solucionar éste y algunos otros problemas detectados durante el proyecto PASSWORD, se han propuesto algunas medidas transitorias sobre maneras de organizar la certificación usando la norma X.509 versión 2 (véase [5]). Además toda la experiencia obtenida durante este proyecto y la prueba simultánea de los servicios PEM en la Internet está siendo de gran utilidad en el proceso de modificación del formato de certificado. Como resultado existe ya un borrador de X.509 versión 3 que incluye, entre otros, varios campos opcionales para distinguir varias claves públicas del mismo usuario, distintas políticas de seguridad y privilegios o acreditaciones asociados a la clave certificada.

Entornos seguros comerciales

El objetivos principal de Kerberos es el de proporcionar un sistema de autenticación entre clientes y servidores que evite que las passwords de los usuarios viajen continuamente por la red.

Hoy en día existen ya algunos sistemas integrados de seguridad que van más allá de desarrollos experimentales y que se pueden obtener en el mercado informático. DIATEL ha realizado un estudio paralelo de tres de los sistemas comerciales más conocidos.

KERBEROS

Kerberos que era el perro de tres cabezas que, según la leyenda, guardaba la puerta de los infiernos, es ahora el encargado de la seguridad en el proyecto Athena.

En 1983, en colaboración con IBM y con Digital Equipment Corporation, el MIT emprendió el proyecto Athena, para poner a disposición de alumnos y profesores, medios informáticos avanzados basados en la arquitectura cliente-servidor [11]. Kerberos es, por lo tanto, el sistema de autenticación que usa el proyecto Athena.

El objetivos principal de Kerberos es el de proporcionar un sistema de autenticación entre clientes y servidores que evite que las passwords de los usuarios viajen continuamente por la red. El sistema se basa en una serie de intercambios cifrados, denominados "tickets" o vales, que permiten controlar el acceso desde las estaciones de trabajo a los servidores. Kerberos proporciona, asimismo, una serie de verificaciones criptográficas para garantizar que los datos transferidos entre estaciones y servidores no están corrompidos, bien por accidente o bien por ataques intencionados.

La versión de Kerberos utilizada en el MIT utiliza el criptosistema simétrico DES, aunque en la actualidad se están desarrollando versiones de Kerberos basadas en RSA.

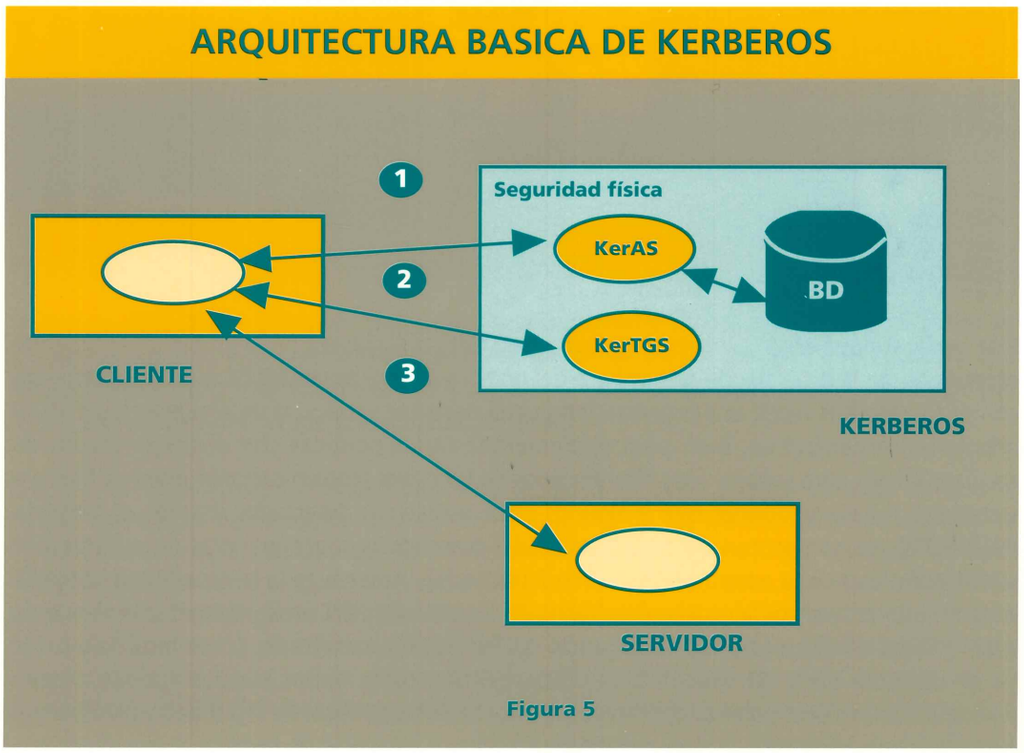


Figura 5

En el entorno Kerberos cuando un usuario desea utilizar un determinado servicio, envía su "login" (1->) a un **centro distribuidor de claves (KerAS)**, el cual genera un vale con el "login" del usuario, la hora, un período de validez, el nombre de la estación de trabajo y una clave de sesión. El vale se cifra con la clave secreta del centro servidor de claves, se añade de nuevo la clave de sesión y se cifra todo con la contraseña del usuario, y esta información se devuelve a la estación de trabajo (1<-). La estación de trabajo solicita al usuario su contraseña, la convierte en una clave DES, y con ella extrae el vale y la clave de sesión. A continuación, la estación de trabajo crea una credencial con la hora actual, el nombre del usuario y la dirección de la estación, la cifra con la clave de sesión y se la envía al **centro de concesión de vales (KerTGS)** junto con el vale que había recibido en el paso anterior (2->). En el centro de concesión de vales se descifra el vale y se extrae la clave de sesión que contenía, y se usa esta clave para descifrar la credencial. Se verifica la validez de los sellos de tiempo y la concordancia entre vale y credencial y se crea un nuevo vale con una nueva clave de sesión. El segundo vale se cifra con la clave secreta del servidor, se le añade la segunda clave de sesión y se cifra todo con la primera clave de sesión y el resultado se envía de vuelta al cliente (2<-). El cliente usa la primera clave de sesión para extraer el vale y la segunda clave de sesión, crea una nueva credencial y la cifra con la segunda clave de sesión, y envía la credencial cifrada y el vale al servidor (3->), el cual descifra el vale, descifra la credencial, los compara y si todo es correcto pasa a proporcionar el servicio solicitado (3<-).

Pretty Good Privacy es un programa de libre distribución escrito por Phil Zimmermann para poner la criptografía al alcance de cualquiera.

SPX

Es la arquitectura de seguridad desarrollada por Digital E. C. y propuesta para su elección como estándar dentro de la iniciativa DCE del llamado "Grupo de Gibraltar" [12]. Usa claves asimétricas RSA certificadas según la norma X.509 combinadas con el uso de DES como algoritmo de cifrado con claves de sesión. Al igual que Kerberos dispone de un centro de autenticación ante el que se identifican los usuarios (LEAF: Login Enrollment Agent Facility). El otro componente básico es un Centro de Distribución de Certificados (CDC) que gestiona un repositorio con los certificados de las claves públicas de clientes y servidores.

El proceso de autenticación se basa en el uso inicial de una clave privada RSA por parte del usuario que se autentica, esta clave se sustituye por una clave temporal llamada clave de delegación disminuyendo la exposición de la clave privada del usuario.

El uso de una jerarquía de certificados de clave pública permite solucionar los problemas de escalabilidad que presenta Kerberos.

Pretty Good Privacy (PGP)

Pretty Good Privacy es un programa de libre distribución escrito por Phil Zimmermann, un programador independiente y activista de los derechos civiles, para poner la criptografía al alcance de cualquiera. Se ha extendido rápidamente por todo el mundo con el consiguiente disgusto del gobierno norteamericano, que como dijimos mantiene la política de limitar en lo posible la exportación de material criptográfico. De formato parecido a PEM, coinciden fundamentalmente en que están concebidos como 'filtros' que producen, a partir de una entrada cualquiera, un encapsulado seguro que se codifica en un formato imprimible (ASCII 7 bits). Este resultado puede luego incluirse en un correo electrónico, puede ser transferido como un fichero, enviado en disquete, etc.

Los objetivos principales del proyecto EDISE consisten en dotar de servicios de seguridad a un servicio EDI que utiliza sintaxis EDIFACT y en incluir servicios de seguridad en correo electrónico X.400.

Al contrario que PEM usa claves de sesión IDEA, un algoritmo simétrico, estoésto es, de claves secretas, mucho más sólido que DES. La clave de sesión se protege igualmente con un cifrado RSA usando la clave pública del destinatario.

Para la distribución de claves se ha diseñado un sencillo formato de certificado, no compatible con X.509, que sirve tanto para que una autoridad certifique claves ajenas (desempeñando el papel de CA) como para que un usuario certifique sus propias claves. Queda así al arbitrio del usuario el establecer sus propios criterios para confiar o no en las claves ajenas según los certificados que la avalen. En definitiva, cada cual es responsable de fijar su política de seguridad. En la práctica se establecen caminos de confianza muy fáciles de extender que recuerdan la rapidez con que se extendieron en tiempos las rutas de correo sobre protocolo UUCP. Al igual que el UUCP, plantea problemas parecidos de escalabilidad si no se establecen autoridades de certificación y servidores de claves.

Con sus inconvenientes y sus ventajas, entre las que destaca su facilidad de uso, la gran difusión de PGP ha hecho de él un estándar de facto para correo. En la actualidad diferentes grupos trabajan en el desarrollo de herramientas que faciliten de alguna manera el acceso simultaneo tanto al mundo PEM como al de PGP.

Entorno seguro para intercambio electrónico de mensajes EDI y mensajería electrónica X.400

En la actualidad DIATEL se encuentra trabajando en el proyecto EDISE. EDISE es el acrónimo de un proyecto de seguridad cuyo título completo es "Desarrollo de funciones y servicios de seguridad según las normativas X.400 y X.509 y su integración en entornos EDI". En este proyecto, que forma parte del programa PASO, colaboran junto con DIATEL la Universidad Carlos III, las empresas P3K y el CCS, el Ministerio del Interior y el CSIC.

Los objetivos principales de este proyecto consisten en dotar de servicios de seguridad a un servicio EDI que utiliza sintaxis EDIFACT y en incluir servicios de seguridad en correo electrónico X.400, con el fin de integrar los resultados obtenidos para proporcionar el servicio EDI sobre MTAs X.400, conforme a la norma X.435.

Un intercambio EDIFACT está formado por uno o varios mensajes que llevan una serie de cabeceras y colas con información específica. Los servicios de seguridad, integridad de secuencia de mensaje, integridad de contenido del mensaje, autenticación del origen del mensaje y no repudio de origen pueden estar integrados en el mensaje o se pueden proporcionar en un mensaje separado [14].

Todos los servicios mencionados se pueden proporcionar incluyendo cabeceras y colas de seguridad, después de la cabecera de mensaje y antes de la cola de mensaje, respectivamente. Las cabeceras de seguridad especifican los métodos de seguridad asociados al mensaje, y los datos necesarios para poder realizar los cálculos de validación (identificación de algoritmos, certificados, etc). Las colas de seguridad especifican los resultados de seguridad correspondientes a las funciones especificadas en la cabecera. La cabecera y cola de seguridad se repiten por cada conjunto de servicios y originador.

Los servicios de seguridad se pueden proporcionar también, utilizando un mensaje de seguridad asociado, denominado AUTACK. Este mensaje específico proporciona los servicios de seguridad para uno o más mensajes. También se puede utilizar para proporcionar el servicio de no repudio en destino, dando al emisor un reconocimiento seguro de que el receptor ha recibido el mensaje original, sin tener que retornarlo.

El servicio de confidencialidad se proporciona utilizando un nuevo tipo de mensaje llamado CIPHER.

En la actualidad la tecnología existente permite incluir seguridad en las aplicaciones con unos costes razonables.

Conclusiones

Una vez extendidas las redes, no cabe duda que en algunas aplicaciones telemáticas resulta imprescindible incorporar servicios de seguridad para que cubran los objetivos para los que fueron previstas. En aplicaciones de nuevo desarrollo sería conveniente que se tengan en cuenta los requerimientosrequirimientos de seguridad antes de su implantación.

En la actualidad la tecnología existente permite incluir seguridad en las aplicaciones con unos costes razonables. Los interfaces de usuario deben ser suficientemente amigables para conseguir que los servicios de seguridad añadidos dificulten lo menos posible el manejo de las aplicaciones.

Referencias

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

[2] "COST225 Secure Communications Final Report", J. Carracedo, A. Gómez (Editors), COST Telecommunications Secretariat, Brussels Mar. 1995.

[3] "A toolkit to provide the users with security functions to send and to recive secure information", A. Gómez, J. Carracedo, L. López, Proceedings of the COST225 International Workshop Secure Applications with Public Key Certification, Stockholm Feb. 1994.

[4] "Provisión de servicios de autenticación, integridad y confidencialidad en la transferencia de ficheros", J. Carracedo, A. Gómez, L. López, URSI 93, Valencia Sep. 1993.

[5] "Almacenamiento de Certificados en el Directorio X.500", L. López, E. Portillo, J. Carracedo, URSI 94, Las Palmas Sep. 1994.

[6] "Proposal of CAs infrastructure in the framework of the COST225 Project", L. López, J. Carracedo, COST Document 225TD(95)002, Brussels Feb. 1995.

[7] "PASSWORD R1.1: Service Requirements", M. Roe. et al. Ago. 1992.

[8] "SecuDE: Vol. 3: Security Applications Guide. Ver. 4.3". W. Schneider (editor). GMD Darmstadt, Alemania May. 1994.

[9] "Privacy Enhancement for Internet Electronic Mail (PEM)". Internet RFCs 1421-1424. Feb. 1993.

[10] "Seguridad en el correo electrónico: Proyecto P8 de COSINE". F. Jordán, M. Medina y E. Peig. Boletín RedIRIS num. 22. Mar. 1993.

[11] "Kerberos: An Authentication Service for Open Network Systems". J. Steiner, C. Neuman, J. Schiller. pp. 191-202 in USENIX Conference Proceedings, Dallas. Texas. Feb. 1988

[12] "SPX. Global Authentication Using Public Key Certificates". J. Tardo, K. Apagappan, Digital E. C. May. 1991.

[13] "PGP User's Guide". P. Zimmermann. May. 1994.

[14] "Recommendations for UN/EDIFACT message level security from the UN/EDIFACT Security JWG", Dic. 1993.

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

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

Veinticinco años de Internet: una retrospectiva autobiográfica

José Barberá

Este artículo, planteado en cierta medida como una catarsis personal, quiere ser un homenaje a todos aquellos que, con su esfuerzo y colaboración desinteresada, han hecho posible la creación de la Internet actual y el fenómeno sociocultural que ese hecho conlleva.

Lo quiero dedicar a todos los amigos y compañeros de la ETSI de Telecomunicación de Madrid, del Instituto Tecnológico para Postgraduados, del MIT, de Telefónica, de Fundesco y del Centro de Comunicaciones CSIC-RedIRIS, que de un modo u otro han intervenido en esta historia que relato, salpicada de referencias autobiográficas.

Mención especial la que hago a Larry Landweber, profesor de la Universidad de Wisconsin y vicepresidente actual de la Internet Society. Su claridad de ideas, su disposición a facilitar la comprensión de los acontecimientos que iban a llevar a la extensión mundial de la Internet a principios de esta década, y su interés personal por ayudar y seguir los desarrollos propios de cada país –y en particular los del nuestro–, le hacen acreedor de una deuda de gratitud de todos los usuarios de RedIRIS.

¿Se hablaba en 1969 de la Internet? ¿Qué acontecimiento tuvo lugar entonces para señalar ese año como el comienzo de la era de los internautas?

1.- Un sistema de comunicación "de dudosa eficacia"

En otoño del año pasado se celebraron simbólicamente las "bodas de plata" de la Internet, al cumplirse los 25 años de su puesta en marcha. ¿Se hablaba en 1969 de la Internet? Evidentemente, no. ¿Qué acontecimiento tuvo lugar entonces para señalar ese año como el comienzo de la era de los internautas? Lo que ocurrió realmente en ese otoño del año en que el hombre había llegado a la luna fue la instalación y puesta en funcionamiento del primer nodo de ARPANET, en la Universidad de California en Los Angeles (UCLA). En diciembre ya había otros tres más: en el Instituto de Investigación de Stanford (SRI), en la Universidad de California en Santa Bárbara (UCSB) y en la Universidad de Utah. Se constituía de ese modo el embrión de lo que hoy es la red de redes Internet que se extiende por todos los continentes. Pero volvamos un poco más atrás para comprender cuales eran las motivaciones y propósitos de un experimento del Departamento de Defensa de los EE.UU.

La red no sería nunca fiable y todos los nodos debían ser iguales, con la misma autoridad para enviar, pasar y recibir los mensajes.

A principios de la década de los 60 nos encontrábamos en plena psicosis de guerra fría. La posibilidad de un ataque nuclear era un supuesto manejado por las autoridades de EE.UU. Tras el temor a un desastre de ese tipo, la pregunta que se hacían era: ¿cómo nos podríamos comunicar tras una guerra nuclear?

Estaba claro que la América de esa época iba a necesitar una red robusta de mando y control, que uniera entre sí las bases esparcidas por todo el país. Sin embargo, por mucho que se protegieran los nodos y las líneas de comunicaciones, siempre subsistía la posibilidad de que una bomba nuclear alcanzase el centro de control, objetivo primordial del enemigo, con lo que la red quedaría inservible.

La corporación RAND, nido de estrategas de la guerra fría, hizo en 1964 una propuesta encaminada a combatir esa eventualidad: en primer lugar tal red no tendría una autoridad central; además habría que diseñarla desde el principio para que pudiera funcionar incluso en condiciones adversas, de modo que la destrucción de una parte no afectase al resto de los nodos. Así pues, se partía de que la red no sería nunca fiable y de que todos los nodos debían ser iguales, con la misma autoridad para enviar, pasar y recibir los mensajes. Estos se dividirían en "paquetes", cada uno de ellos con su propia identidad, que serían transportados independientemente desde un nodo de origen hasta otro de destino.

En 1971 ARPANET contaba con 15 nodos y en 1972 ya había 40.

La ruta particular de cada paquete no importaba, sólo contaba el resultado final, es decir que existieran los mecanismos adecuados para recomponer el mensaje original en el lugar de destino. En esencia, cada paquete iría saltando de nodo en nodo como una patata caliente, más o menos en dirección a su destino. Si en el camino algún nodo fallaba, los paquetes quedaban como flotando en el aire, dirigiéndose a otros nodos vecinos que les permitirían sobrevivir. Nacía de este modo el concepto de red de conmutación de paquetes, un sistema de comunicación que podría ser dudosamente eficaz desde el punto de vista convencional (sobre todo si se compara con la red telefónica ordinaria), pero que sería enormemente robusto frente a adversidades y fallos.

2.- ARPANET: ¿una red de ordenadores?

Lo que inicialmente se concibió como una red de ordenadores se había transformado en una red para la comunicación de personas y grupos.

La idea de crear una red a prueba de bombas, descentralizada y basada en la conmutación de paquetes, fue tomando cuerpo y encontró eco entre RAND, el Instituto Tecnológico de Massachusetts (MIT) y UCLA. Curiosamente fue el Laboratorio Nacional de Física del Reino Unido quien primero construyó un prototipo de esas características en 1968. Poco después la Agencia de Proyectos de Investigación Avanzada del Pentágono (ARPA) decidió subvencionar un experimento similar, aunque más ambicioso, en EE.UU.; los nodos de la red se utilizarían para unir "superordenadores" de aquella época, costosas máquinas dedicadas a los proyectos nacionales de investigación y desarrollo, que ciertamente iban a necesitar un sistema de comunicaciones robusto.

Como se dijo antes, en diciembre de 1969 ARPANET, llamada así en honor a sus patrocinadores, tenía cuatro nodos, a los que se los conocía por las siglas IMP (*Interface Message Processor*), que unían los "superordenadores" por líneas dedicadas de "alta velocidad" (56 Kbps). Los científicos e investigadores podían de ese modo compartir recursos informáticos remotos e incluso programar remotamente los ordenadores, lo que resultaba particularmente interesante en aquellos años en los que el tiempo de máquina era un recurso especialmente valioso. En 1971 ARPANET contaba con 15 nodos y en 1972 ya había 40.

Sin embargo, durante el segundo año de funcionamiento, apareció un hecho no previsto inicialmente al diseñar el proyecto; los científicos usuarios de la red habían encontrado una funcionalidad adicional: podían enviar por ella mensajes personales para discutir sobre los trabajos en curso. Los usuarios-diseñadores habían convertido así la red de compartición de recursos informáticos en una red privada de correo "electrónico" ¡subvencionada con fondos públicos! Porque una vez abierta esa vía, con cuentas de usuario y direcciones personales de correo electrónico, la información que viajaba por la red no era solamente científica; los mensajes también trataban otros temas particulares e incluso cotilleos. Los usuarios estaban entusiasmados: ese servicio de comunicación personal era mucho más interesante que el diálogo remoto entre máquinas.

El paso siguiente fue el descubrimiento de las listas de distribución electrónicas, que permitían difundir un mismo mensaje a un gran número de personas interesadas sobre temas variopintos. Uno de los más populares fue el de ciencia-ficción, que no tenía que ver demasiado con el objetivo del proyecto, lo que en cierta medida contrarió a los responsables de ARPA. A pesar de ello, éstos no quisieron impedir ese uso heterodoxo de la red. Lo que inicialmente se concibió como una red de ordenadores –para comunicarlos entre sí– se había transformado en una red para la comunicación de personas y grupos, basada en ordenadores y en la conmutación de paquetes.

3.- El proyecto "Internetting"

Durante los años 70 la red ARPA fue creciendo. Su estructura descentralizada facilitaba la expansión. A diferencia de las redes de ordenadores corporativas (homogéneas), ARPANET admitía sistemas diferentes (DEC-10, PDP-8, PDP-11, IBM 360, Multics, Honeywell...). La condición imprescindible: todas debían hablar un mismo lenguaje discontinuo, basado en la técnica de conmutación de paquetes. A este lenguaje se le denominó inicialmente NCP (*Network Control Protocol*). Mientras tanto iban desarrollándose proyectos de redes de conmutación de paquetes basadas en otras tecnologías y medios de transmisión como la radio y el satélite, caso este último de la red ALOHA, desarrollada en la Universidad de Hawaii en 1972 mediante técnicas de acceso múltiple y colisión de paquetes. Esta tecnología posteriormente dio origen a la Ethernet desarrollada en el centro de investigación de Xerox en Palo Alto.

La idea era desarrollar protocolos de comunicación que permitieran a los ordenadores comunicarse de modo transparente a través de distintas redes de paquetes interconectadas.

A la vista de esa situación, en 1973 ARPA –rebautizada entonces como DARPA– lanzó una nueva iniciativa con el objetivo de investigar técnicas y tecnologías para unir redes de paquetes de varios tipos. La idea era desarrollar protocolos de comunicación que permitieran a los ordenadores comunicarse de modo transparente a través de distintas redes de paquetes interconectadas. Esta iniciativa fue bautizada como Proyecto *Internetting*, del que ha derivado el nombre actual de Internet. El sistema de protocolos desarrollados en el curso de ese proyecto es lo que se conoce como la serie de protocolos TCP/IP, por el patronímico de los dos primeros : *Transmision Control Protocol* (TCP) e *Internet Protocol* (IP), sucesores del NCP original. El primero de ellos trocea en paquetes los mensajes generados en el origen, y luego los recompone en el nodo de destino. El Protocolo IP se ocupa del direccionamiento de los paquetes, de modo que estos puedan viajar por rutas diversas, atravesando múltiples nodos e incluso por diferentes redes con distintos estándares de comunicación.

En aquellos años el estudio de los protocolos TCP e IP no formaba parte de la enseñanza reglada.

4.- Visión personal de las redes de paquetes

Los años 1974-76 los pasé en el MIT realizando estudios de postgrado e investigación en el Departamento de *Electrical Engineering and Computer Science*. Procediendo de un grupo español de investigación en transmisión de datos, pronto me decidí a dedicarme al tema de las redes de ordenadores, tan en boga en aquellos momentos en los que parecía que ya estaba todo dicho sobre la teoría de comunicaciones y el análisis espectral de las señales.

De este modo conocí la red ARPA y la técnica de conmutación de paquetes. Tuve ocasión de asistir a seminarios protagonizados por profesores del MIT, la Universidad de Harvard y de BBN[1] (Bolt, Beranek and Newman), activa empresa de Cambridge (Massachusetts) en el desarrollo de ARPANET, que en 1969 había fabricado el primer nodo IMP (basado en un Honeywell DDP 516) que se instaló en UCLA.

En aquellos años no tuve ocasión de experimentar la red ARPA como usuario. Aquella tarea estaba reservada a los investigadores de primera línea; el uso no era fácil, ni mucho menos accesible a los neófitos que solamente estábamos de paso. El estudio de los protocolos TCP e IP, los IMP los TIP (Terminal IMP), etc. no formaba entonces parte de la enseñanza reglada. Había que seguir los temas a base de seminarios, charlas y alguna que otra tesis doctoral de las que

1.- En la actualidad BBN es un "superproveedor" de servicio Internet en EE.UU., al haber adquirido las redes regionales NEARnet (Nueva Inglaterra), BARRnet (Area de San Francisco) y muy recientemente SURAnet (red de las Universidades del Suroeste).

iban saliendo entonces. Yo hice mi tesis de *Master of Science* sobre modelos de encaminamiento en redes de ordenadores, basados en la teoría de la difusión, algo que casi 20 años después apenas recuerdo, ni sé si ha servido para algo (probablemente no).

A mi vuelta a España presenté la tesis doctoral sobre otro tema de redes de ordenadores, ahora centrándome en el control dinámico de redes con canales de acceso múltiple (como el sistema Aloha y la Ethernet). Ni que decir tiene que me resultaría imposible actualmente entender muchas cosas de las que entonces escribí, más allá de que había muchas colisiones entre los múltiples paquetes que surgían de todas partes y variadas probabilidades de retransmisión

Sin embargo, una cosa era cierta: sabía claramente qué eran las redes de paquetes y cómo funcionaban esos protocolos tan caóticos que, milagrosamente, eran capaces de recomponer en el destino los mensajes originales. ¿Lo sabía realmente?

Sabía claramente qué eran las redes de paquetes y cómo funcionaban esos protocolos tan caóticos que, milagrosamente, eran capaces de recomponer en el destino los mensajes originales. ¿Lo sabía realmente?

Eso me creía yo hasta que empecé a colaborar con un grupo de expertos de la División de Informática de Telefónica que empezaba a trabajar sobre redes de datos de conmutación de paquetes[2]. Pero esas redes eran distintas de las que había conocido en EE.UU. Se basaban en algo llamado X.25, que no era un protocolo de comunicación entre nodos de red (como el IP), sino más bien un interfaz de acceso a la misma desde el terminal de datos del abonado, normalizado por el CCITT para las redes públicas de datos de los operadores telefónicos.

La recomendación X.25, además de no aclarar para nada lo que les ocurre a los paquetes cuando viajan de un nodo a otro, presentaba una característica muy rara respecto a lo que yo había aprendido: al contrario que en ARPANET, en donde los paquetes se mueven caóticamente siguiendo caminos diferentes, ahora esos paquetes van todos ordenados por unas rutas fijas entre origen y destino (llamadas "circuitos virtuales"), que no se alteran mientras se mantiene abierta la llamada. Pero entonces, ¿qué clase de red es esa en la que antes de empezar a enviar paquetes hay que hacer una llamada y asegurar un camino fijo entre el origen y el destino? ¿Acaso no es eso como la red telefónica normal? La sorpresa inicial desaparece enseguida cuando uno piensa que, a fin de cuentas, el diseño lo ha hecho la compañía que da el servicio telefónico.

A finales de los 70 se anuncia que la Organización Internacional de Normalización (ISO) está desarrollando un modelo arquitectónico de referencia basado en la interconexión de sistemas abiertos (OSI).

A finales de los 70 se anuncia que la Organización Internacional de Normalización (ISO) está desarrollando un modelo arquitectónico de referencia basado en la interconexión de sistemas abiertos (OSI).

Una vez superado el impacto inicial, empiezo a comprender la motivación que sostiene el X.25. Las líneas de entonces no tienen la calidad suficiente para la transmisión de datos, puede haber errores y, por tanto, el protocolo de comunicación ha de ser lo suficientemente redundante para permitir retransmisiones y corrección de esos errores. De este modo, la tecnología X.25 proporciona una red de alta calidad que asegura a los equipos terminales de datos (así designa el CCITT a los ordenadores y a los terminales de usuario) que la información que les llega es correcta. Además, X.25 permite negociar determinados parámetros y tarificar en distintas modalidades. Pequeño detalle este del pago en el que no había caído en la cuenta hasta entonces.

Pero hay más; a finales de los 70 se anuncia que la Organización Internacional de Normalización (ISO) está desarrollando un modelo arquitectónico de referencia basado en la interconexión de sistemas abiertos (OSI), que es el futuro en lo referente a redes. Decidí olvidarme de ARPANET y sus protocolos; aquello era algo de los americanos y, en cualquier caso, pertenecía al pasado: ¡el futuro era OSI! Volvamos ahora al otro lado del Atlántico.

2.- Curiosamente Telefónica fue uno de los operadores (entonces "administraciones") de telecomunicación pioneros en este campo. Ya en 1991 había puesto en marcha una red pública de datos de conmutación de paquetes llamada Red Especial de Transmisión de Datos (RETD), precursora de Iberpac (todavía no se había normalizado el interfaz de acceso X.25).

5.- La década de los 80. Primera parte: el nacimiento de la Internet

A comienzos de esa década surgen en el mundo científico de EE.UU. otras redes afines, tales como CSNET (*Computer Science Net*) y BITNET. Esta última, de naturaleza interdisciplinar, conectaba los ordenadores IBM de los centros de cálculo de diversas universidades con líneas de baja velocidad y mediante la serie de los primitivos protocolos RSCS de IBM. CSNET fue en un principio patrocinada por la National Science Foundation (NSF) para unir grupos de investigación en ciencia informática en universidades, centros públicos e industria. Inicialmente usaba el protocolo MMDF Phonenet como base para el correo electrónico sobre líneas telefónicas; es de destacar que fue la primera red que posteriormente experimentó el uso del TCP/IP sobre X.25 en redes públicas de datos.

Mientras tanto el uso de los protocolos TCP/IP se fue generalizando en otras redes para su conexión a ARPANET, que seguía creciendo de forma sostenida.

En 1983 se desgajó de ésta la parte relacionada con la defensa, que se llamó MILNET. A pesar de su crecimiento ARPANET fue quedando como una comunidad más reducida frente a otras que iban surgiendo, impulsadas por la necesidad de conectar las nuevas y potentes máquinas que proliferaban, las cuales se interconectaban entre sí mediante los protocolos TCP/IP, que actuaban como un pegamento transparente que unía múltiples redes sin costuras aparentes. Puesto que el software TCP/IP era de dominio público y la tecnología básica era descentralizada –y más bien anárquica–, era imposible frenar el impulso de interconexión de los usuarios. De hecho nadie quería impedir la interconexión de todas esas redes.

Puesto que el software TCP/IP era de dominio público y la tecnología básica era descentralizada –y más bien anárquica–, era imposible frenar el impulso de interconexión de los usuarios.

De este modo, nace en 1983 la Internet como red de interconexión entre ARPANET, MILNET y CSNET, unidas todas ellas por los protocolos TCP/IP, y a las que se irían añadiendo posteriormente otras redes, de EE.UU. y de otros países.

6.- La década de los 80. Segunda parte: el declive de ARPANET

En 1986 la NSF, ante las dificultades burocráticas que encontraba para conectar por ARPANET sus centros de superordenadores, puso en marcha una nueva iniciativa para unirlos mediante líneas de alta velocidad, creando de este modo una red troncal (*backbone*) de extensión nacional, con enlaces cuya capacidad fue aumentando gradualmente hasta 1,5 Mbps. Era la NSFnet, que en 1992 ya contaba con enlaces troncales de 45 Mbps. Paralelamente otras agencias del gobierno de EE.UU. (la NASA, el Departamento de Energía, el Instituto Nacional de la Salud) fueron poniendo en marcha sus propias redes, creando de este modo una confederación Internet, aunque en una situación organizativa propia de reinos de taifas.

Los diferentes nodos de esa red de redes, algunos de los cuales alcanzaban ya Europa (Reino Unido y Noruega), fueron catalogados de acuerdo con el país de origen, pero la mayoría de los de EE.UU. decidieron dividirse en seis "dominios" básicos: edu, mil, gov, org, com y net (tipo este de abreviaciones comunmente encontrado en la Internet), para designar el campo de actividad de los usuarios. Además de los ámbitos tradicionales académicos, militares y del gobierno, entraban en escena otras organizaciones no lucrativas, aunque también empresas comerciales que pronto vieron la utilidad de pertenecer a este club un tanto anárquico, aunque apasionante.

Entraban en escena otras organizaciones no lucrativas, aunque también empresas comerciales que pronto vieron la utilidad de pertenecer a este club un tanto anárquico, aunque apasionante.

ARPANET, que había comenzado su declive desde la entrada en escena de NSFnet, expiró pacíficamente en 1989, víctima de su propio éxito; sus usuarios apenas notaron su desaparición, por cuanto que su funcionalidad no solamente permaneció sino que fue mejorando continuamente.

Desde el punto de vista práctico las complejas torres OSI no habían ido mucho más allá del nivel de red X.25.

7.- Las redes abiertas. El mito de OSI

Simultáneamente a los desarrollos anteriores, los últimos años de la década de los 80 habían dejado patente la consolidación del modelo OSI para interconexión de redes en modo abierto. Sin embargo, desde el punto de vista práctico las complejas torres OSI no habían ido mucho más allá del nivel de red X.25, servicio ofrecido por bastantes redes públicas de datos, especialmente en Europa. Solamente el correo electrónico X.400 llegó a escalar los niveles superiores sobre distintos sistemas, dando lugar a productos tanto académicos como de cierta implantación comercial, productos que en ocasiones eran más que nada material de ferias y exhibiciones de interoperatibilidad.

El nonato FTAM no consiguió ir más allá de la T. La A y la M no lograron despegar nunca de su lugar en el abecedario.

Sin embargo, no había que perder la esperanza. Era sólo cuestión de tiempo que los fabricantes de ordenadores y las casas de software empezaran a ofrecer los productos adecuados a los distintos niveles de OSI. Ofrecer, lo que se dice ofrecer, era cierto que los ofrecían; pero había que ver a qué precio y con qué grado de compatibilidad. En las redes de I+D que empezaban a utilizar el correo X.400 pronto se implantaron los productos académicos, menos completos que los comerciales y sin un mantenimiento estable, pero más fáciles de instalar y con mejores interfaces de usuario. Tales redes usaban normalmente la infraestructura X.25 de las redes públicas de datos, lo que era una ventaja a la hora de la gestión, que quedaba en manos del operador. Asimismo, el acceso desde un terminal remoto quedaba solucionado por las facilidades XXX (X.28, X.3 y X.29) que ofrecían esas redes. Sólo había que aprenderse los números de la dirección X.121 correspondiente (¡9-13 cifras!), y a teclear.

En cuanto al nonato FTAM, no consiguió pasar de experimentaciones de dudosa eficacia, pero sin lograr ir más allá de la T. La A y la M no lograron despegarse nunca de su lugar en el abecedario.

El problema de cómo hacer compatibles los dos mundos: el nuestro, el mundo abierto de OSI, con el de los pobres desdichados de la Internet.

Las declaraciones de apoyo a OSI iban en creciente aumento -sobre todo en países europeos mejor organizados o más firmes y ortodoxos en sus convicciones: Alemania, Reino Unido-, en relación inversamente proporcional al desarrollo e implantación real de productos. Con todo había un hecho esperanzador: el Departamento de Defensa y la NSF de EE.UU. habían anunciado la decisión de sustituir los protocolos TCP/IP por los de OSI, en un plazo "relativamente breve" (¿1992?, ¿1993...?). Inmejorable situación para los de las redes de I+D europeas que andábamos ya más avanzados por el buen camino. Quedaba únicamente por solucionar el problema de cómo hacer compatibles los dos mundos: el nuestro, el mundo abierto de OSI, con el de los pobres desdichados de la Internet, encerrados en su isla por los protocolos TCP/IP.

8.- UNIX y Ethernet: una combinación explosiva

Un aspecto obviado hasta ahora ha sido el de la evolución del concepto de red en los años 80, precisamente durante la etapa de despegue y expansión inicial de la Internet. A la vez que grandes ordenadores, cada vez más potentes, iban desarrollándose nuevos minis y surgían los ordenadores personales y las estaciones de trabajo.

La descentralización de la informática en las universidades y centros de investigación fue consolidándose progresivamente, aislando de este modo a los usuarios de los recursos comunes, lo que iba asimismo en detrimento de la comunicación personal. Surgieron así las redes locales de diversas tecnologías, que restauraban esa conectividad perdida; la Ethernet fue encontrando una mayor aceptación en los ámbitos académicos y de investigación. Por otro lado, el uso del sistema operativo UNIX se iba generalizando masivamente entre los científicos informáticos.

La Ethernet fue encontrando una mayor aceptación en los ámbitos académicos y de investigación.

La combinación de UNIX con Ethernet y otras tecnologías de red de área local dispara el crecimiento de productos Internet a partir de 1985. DARPA había invertido fondos significativos para que BBN desarrollase una implementación de TCP/IP sobre UNIX que fue después trasladado al UNIX de Berkeley V4.2. El paso siguiente fue la adopción de BSD por Sun como sistema de base para sus productos comerciales.

A partir de entonces, y coincidiendo con la implantación de la NSFnet, comienza una demanda creciente de conectividad Internet y de ancho de banda. Los operadores de EE.UU. proporcionan los enlaces y aparecen empresas informáticas que sacan al mercado máquinas especializadas para el encaminamiento (los *routers*).

La combinación de UNIX con Ethernet y otras tecnologías de red de área local dispara el crecimiento de productos Internet a partir de 1985.

Por otro lado, como tentáculos del pulpo gigante en el que se va convirtiendo NSFnet, entran en escena las redes de nivel intermedio o redes regionales, impulsadas y patrocinadas por la NSF como parte de las iniciativas de NSFNet. Algunos de esos tentáculos llegan ya a otros continentes: Europa, Australia, Japón... Además surgen los primeros proveedores comerciales, que proporcionan el servicio a empresas privadas sin relación de patrocinio con la NSF.

Resultado: la red de redes Internet había extendido su capilaridad hasta llegar prácticamente hasta el mismo puesto de trabajo de los usuarios conectados a sus redes locales. Ahora éstos tenían a su alcance una serie de recursos informáticos (correo, ficheros, listas, acceso remoto...) distribuídos por todo el mundo, recursos que hasta entonces veían solamente de modo local. El diseño del TCP/IP y la posibilidad de su infiltración a todos los niveles, sobre diferentes tecnologías y medios, habían hecho posible semejante proeza. Algo no considerado cuando se diseñaron los protocolos TCP/IP, con la consiguiente influencia sobre el espacio de direcciones de la Internet que, como se verá más adelante, se quedó corto, siendo en la actualidad uno de los problemas a los que debe enfrentarse esta red.

Internet había extendido su capilaridad hasta llegar prácticamente hasta el mismo puesto de trabajo de los usuarios.

9.- La interconexión LAN/WAN: un desafío estéril

Volvamos nuevamente hacia el este y observemos el escenario europeo de las redes. Estamos a finales de los años 80. La informática se ha distribuído y las redes de área local (LAN) se han generalizado en los centros universitarios y de investigación. Como es lógico, se han adoptado los correspondientes estándares, en este caso bajo la tutela del IEEE (*Institute of Electrical and Electronic Engìneers*), la conocida serie 800 para las tecnologías Ethernet, Token ring, Token bus, etc. Posteriormente ISO hará suyas esas normas sin más que preceder cada uno de esos números por un 8.

Florecen las redes de I+D en Europa; en España ya ha comenzado el Programa IRIS para crear la red académica nacional. Es entonces cuando surge el problema de la interconexión de las redes de área local mediante redes de área extensa: el famoso problema LAN/WAN que figuró con uno de los objetivos estratégicos del Proyecto COSINE.

¿Qué había ocurrido en esos años para que todos los supuestos de los sistemas abiertos de ISO fueran quedando como material de archivo?

No quiero entrar ahora en las complejidades técnicas del asunto. Por simplificar diré únicamente que se trataba de interconectar (principalmente) Ethernets mediante redes de paquetes X.25 (públicas o privadas), en el nivel 3 (de red) del esquema OSI. La dificultad radicaba en unir redes diferentes en cuanto a conectividad extremo a extremo: las locales (no conectivas) y las X.25 (conectivas). Se propusieron varias soluciones: pasarelas de transporte (por encina del nivel de red), pasarelas de red (¡llevar el nivel de red X.25 sobre el del enlace de la LAN!), poner el IP sobre X.25 (¡pero el IP de ISO, ya que el IP de Internet se suponía iba a ir migrando hacia OSI!). Y mientras tanto, dada la existencia de aplicaciones TCP/IP en las LAN de los investigadores y la necesidad de comunicación con los de la Internet, se proponía un escenario lleno de pasarelas de aplicación: correo electrónico, terminal remoto, ¡transferencia de ficheros!

El resto de la historia es bien conocida: el fracaso de todas las predicciones fue algo tan sonado como cuando la crisis del petróleo de los años 70. Afortunadamente para mí –y para todos los usuarios de RedIRIS, creo– en aquellos años "oscuros", entre el 87 y el 90, tuve la fortuna de mantenerme en contacto con el mundo Internet gracias a los seminarios que organizaba Larry Landweber. Anualmente nos reuníamos un grupo relativamente reducido de 40-60 personas de diversos países para tratar de entender el problema global de la interconexión de redes de I+D. Esos encuentros finalizaron en un momento dado para dar lugar a la primera conferencia internacional INET'91 en Copenhague, en la que se anunció la constitución de la Internet Society (ISOC) para enero del año siguiente.

En la Internet las aplicaciones han ido unidas desde el principio a los protocolos TCP/IP.

De este modo, la nave de RedIRIS que entonces dirigía pudo virar 180° y tomar el rumbo adecuado. Volvía a mis orígenes de los 70 en el tema de las redes. ¿Qué había ocurrido en esos años para que todos los supuestos de los sistemas abiertos de ISO fueran quedando como material de archivo?

10.- La clave (técnica) del éxito: IP sobre todo

En 1993, asistiendo en San Francisco a la conferencia anual de la Internet Society, vi un día a su presidente, Vint Cerf, tan serio y tan formal normalmente, que nos sorprendió a todos llevando una camiseta con la inscripción "*IP on everything*". Para entonces ya estaba claro el vuelco que se había producido en las redes de I+D, que aunque con algunas argucias más bien dialécticas tales como "redes multiprotocolo" habían basado su servicio de red en IP, dejando así la puerta abierta a los usuarios para que eligieran las aplicaciones que les resultasen más convenientes, y facilitando de este modo la conexión a la Internet y la expansión de ésta por todo el mundo.

La clave del éxito estaba en la camiseta de Vint Cerf, precisamente uno de los principales artífices del desarrollo de los protocolos TCP/IP. La simplicidad y flexibilidad del protocolo IP habían hecho posible su funcionamiento sobre todo tipo de tecnologías de red: LAN, X.25, FDDI, Frame Relay, RDSI, ATM... lo que llevaba seguidamente al uso del resto de protocolos TCP/IP y de las correspondientes aplicaciones. Otro factor importante del éxito frente a las redes X.25 era que mientras en éstas las aplicaciones quedaban al margen del proveedor de red, dejando a los diferentes usuarios la decisión sobre los servicios que querían transportar, en la Internet aquellas han ido unidas desde el principio a los protocolos TCP/IP. Y así, además de las tradicionales de SMTP, FTP, Telnet y News, hemos podido ver cómo se ha expandido rápidamente una plétora de nuevos servicios de búsqueda y acceso a información tales como Archie, Gopher, WAIS y WWW, que han convertido a la Internet en una colección de

comunidades virtuales que han traspasado las barreras políticas y geográficas, en la que participan sectores de todo tipo: académicos, científicos, comerciales, culturales, de la administración, de la enseñanza media, etc.

Pero, ¿qué es lo que ha llevado a toda esa gente tan diversa a querer estar conectados a la Internet?

11.- La clave (estratégica) del éxito: libertad y cooperación

El deseo de ser libre y poder comunicarse con sus semejantes es una características común a la mayoría de los seres humanos (no así de las instituciones); incluso se podría añadir que en el fondo de ello subyace una mayor o menor dosis de anarquía que todos tenemos. Con esas premisas, ¿qué mejor oportunidad que la que ofrece una red verdaderamente ubicua, moderna y funcionalmente "anárquica"?

La Internet no tiene dueño, no hay un consejo de administración, ni junta de accionistas; no hay negociados, no hay jefes, no hay censores oficiales...

La Internet no va acompañada de siglas como S.A., Inc., Ltd., ... No tiene dueño, no hay un consejo de administración, ni junta de accionistas; no hay negociados, no hay jefes, no hay censores oficiales... Hay solamente una serie de normas técnicas (TCP/IP) y otras de buen uso y costumbre que se espera sigan todos los usuarios. Es una red democrática: todos los nodos pueden "dialogar" entre ellos de igual a igual. Lo mismo ocurre entre los individuos: todos pueden comunicarse entre sí y navegar por ese océano inmenso de información que es la Internet actualmente. La gente en la Internet se siente como en su propia casa o en su organización. Es una "institución" que se resiste a ser institucionalizada. Pertenece a todos y a nadie a la vez; cada individuo y cada organización es el dueño de sus máquinas y de su información.

En la Internet cuando un estándar llega a ser estable ya hay productos que lo implementan.

Mucha gente se ha dado cuenta que la Internet es una ganga. Al contrario de lo que ocurre en el servicio telefónico, aquí no hay facturación en función de la distancia. La Internet, a diferencia de otras redes comerciales, tampoco factura por el tiempo de acceso y por el volumen de tráfico; (otra cosa es lo que haga cada proveedor de servicio en función de su esquema tarifario).

Además de lo anterior hay otro factor clave que ha permitido la expansión de ese fenómeno: la cooperación. Si bien es cierto que se ha contado con cuantiosas subvenciones estatales, también lo es el hecho de que ha habido numerosos individuos e instituciones que han colaborado desinteresadamente en el desarrollo de nuevos procedimientos y aplicaciones, cuyo uso se ha ido extendiendo porque otros han colaborado con críticas, sugerencias, pruebas y mejoras.

En ese sentido hay que reseñar una diferencia fundamental entre la forma de elaborar "estándares" en la Internet y los de las organizaciones de normalización como ISO. En ésta las distintas comisiones técnicas discuten propuestas complejas y muy elaboradas que luego elevan a los niveles superiores de decisión. El problema está en que durante ese proceso, en el que normalmente hay que consensuar diversos intereses encontrados, la tecnología avanza de forma imparable, y del mismo modo crecen las demandas y exigencias de los usuarios. Mientras tanto se espera que los fabricantes desarrollen productos para un mercado que no ven claro.

En la Internet, por el contrario, se ha seguido un proceso inverso: primero desarrollar, luego probar y después normalizar. De este modo, cuando un estándar llega a ser estable ya hay productos que lo implementan; el mercado ha surgido de forma natural.

En los años 73 y 74 se había considerado un número máximo de 256 redes.

En resumen, la estrategia de la Internet ha ido de abajo a arriba, por el impulso que han dado los propios usuarios al desarrollo y mejora del servicio, por la colaboración entre múltiples grupos e instituciones, y por la ausencia de innecesarias trabas de tipo burocrático y administrativo.

12.- Retos tecnológicos actuales de la Internet

El crecimiento exponencial de la Internet en los últimos años ha pillado por sorpresa a todos: usuarios, proveedores y diseñadores. Además del número de usuarios, al aumentar paralelamente la potencia de las máquinas, de uso común y personales, han surgido aplicaciones multimedia "asesinas" tales como el WWW, que devoran el ancho de banda disponible en detrimento de los servicios más tradicionales.

En este momento el ATM es sólo una promesa ante la falta de un estándar global y de equipos compatibles.

La propia red de teleconferencia MBONE, basada en la técnica del *IP Multicast*, está imbricada como una subred especializada dentro de la Internet general. A pesar de tener unos requisitos diferentes, al ser aplicaciones en tiempo real –más críticas en cuanto a pérdidas de paquetes y retardos–, esa técnica permite actualmente recibir audio y vídeo de diversas conferencias. De nuevo han sido los propios grupos de desarrollo de la Internet los que la han impulsado, por la necesidad de contar con un instrumento de trabajo para sus reuniones virtuales.

El ancho de banda, a pesar de haberse ido abaratando como consecuencia de la liberalización de las telecomunicaciones, sigue siendo un recurso escaso para este tipo de aplicaciones.

El otro tema acuciante es el del espacio de direcciones. En los años 73 y 74 se había considerado un número máximo de 256 redes. Había sólo una LAN en Xerox PARC y el resto eran regionales o nacionales en EE.UU. Cuando se hizo evidente que habría muchas más redes locales, los expertos inventaron el concepto de clases A, B y C, lo que racionalizaba considerablemente el problema del espacio de direcciones. Pero en lo que los expertos no cayeron en la cuenta entonces fue que los protocolos de encaminamiento y la topología de la Internet –cada vez más extensa y difusa– no se adaptaban bien a un número de redes tan grande como el que se avecinaba. Y eso resume el otro gran reto actual: la Internet no puede seguir creciendo con el mismo esquema.

Una posible vía de abordar el problema del ancho de banda es mediante la separación de servicios en clases y la correspondiente asignación de recursos, según la mayor o menor necesidad de respuesta en tiempo real y de la interactividad en un momento dado. También se contemplan otras tecnologías de red de banda ancha, tales como el ATM, que en este momento es sólo una promesa ante la falta de un estándar global y de equipos compatibles. Para el tema del direccionamiento IP se está desarrollando el IPng (IP nueva generación), con un espacio mayor de direcciones y con la posibilidad de encaminar los paquetes en función de la dirección de origen y del tipo de información transmitida. De igual modo está la posibilidad de elección dinámica del proveedor.

Por último, ante el creciente uso comercial de servicios, queda pendiente el desarrollo de mecanismos fiables de seguridad y confidencialidad, algunos de los cuales ya se usan de forma restringida, aunque con aspectos legales todavía no resueltos debida a la diferente jurisprudencia de cada país.

13.- Retos organizativos actuales de la Internet

Al haberse ensanchado la base inicial de usuarios académicos de la Internet incluyendo otros campos de actividad, y sobre todo ante el éxito innegable que tiene esta red en "régimen cooperativo de multipropiedad", todo el mundo quiere opinar y plantear cuestiones de diversa índole. Así por ejemplo, los usuarios de empresas quieren asegurar una estructura financiera más sólida antes de confiar la gestión de sus negocios sobre ese red, además de los mecanismos de seguridad y fiabilidad antes señalados. Las administraciones –¡cómo no!– quieren tener un entorno menos anárquico y más regulado; no entienden esa cooperación que sobrepasa fronteras y diluye responsabilidades. Los académicos e investigadores quieren –al menos eso creo yo– una red propia, que sientan como suya, como siempre ha sido; ellos se lo merecen más que nadie pues para eso hacen avanzar la ciencia e impulsan el progreso. Los militares quieren una red a prueba de espías, totalmente segura y robusta frente a fallos y ataques. Y así todos....

Las administraciones no entienden esa cooperación que sobrepasa fronteras y diluye responsabilidades.

Para estos conflictos de intereses no se ha hallado todavía una solución definitiva. Todo el mundo quiere tirar de la cuerda en su dirección y en su propio beneficio, aunque teniendo en cuenta que no se puede forzar demasiado desde un lado, no sea que se rompa el estado actual de consenso que ha hecho posible el éxito actual.

Ése ha sido hasta ahora el modo de hacer en la Internet: por consenso. Sería desafortunado que esos hábitos se vieran alterados por intereses particulares de grupos de presión. Por suerte, está la Internet Society que, aunque no es ni mucho menos un órgano de gobierno en la Internet, se ocupa de tutelar el desarrollo y evolución de la misma, racionalizando los recursos disponibles y proporcionando el foro para el necesario consenso.

De momento todo son promesas y especulaciones. Hasta ahora no se ha visto una estrategia definida que lleve a la consecución del objetivo propuesto.

14.- La Internet y las autopistas de la información

Es un tema de moda con el que frecuentemente nos bombardean los medios de comunicación: las (futuras) autopistas de la información. Gobiernos, empresas, instituciones, usuarios... todos hablan de esas nuevas autopistas digitales que se van a poner en marcha. La Iniciativa Nacional de la Información de la Administración Clinton-Gore en EE.UU., el Informe Bangemann de la Unión Europea, la Infraestructura de Info-comunicaciones de Japón... De momento todo son promesas y especulaciones, porque se espera construir esas autopistas uniendo los esfuerzos de gobiernos, operadores, medios de comunicación, fabricantes, etc. Pero hasta ahora no se ha visto una estrategia definida que lleve a la consecución del objetivo propuesto.

Por eso se suele plantear con cierta frecuencia la pregunta "¿es la Internet una de estas superautopistas de la información (al menos un embrión de las mismas)?". Seguramente muchos darán una respuesta afirmativa, especialmente al considerar la posibilidad de evolución de la Internet a una de esas superautopistas (yo mismo así lo he expresado en otras ocasiones). Otros dirán que no, que la Internet carece de las características que definen a esas vías de información del futuro, a saber: no integran voz, datos e imágenes en tiempo real; no tienen un soporte de transmisión de banda ancha (sobre fibra óptica) y no son utilizadas masivamente por todos los ciudadanos. Afirmaciones que sólo son parcialmente ciertas: tenemos el ejemplo de MBONE (ciertamente con una funcionalidad reducida respecto a la que ofrecen los canales de TV o la videoconferencia RDSI); también es posible ya charlar por la Internet con un simple PC y un software barato. En cuanto a la utilización de la fibra óptica de forma generalizada, es cuestión solamente de la extensión de esa infraestructura hasta las oficinas y hogares de los

usuarios. Y el uso masivo de la misma dependerá en gran medida de la oferta de información disponible, de la calidad del servicio y del coste (relación calidad/precio).

Creo que la Internet y las autopistas de la información son redes de comunicación conceptualmente diferentes.

A pesar de todo, quiero finalizar esta exposición diciendo que creo que la Internet y las autopistas de la información son redes de comunicación conceptualmente diferentes, y que espero que lo sigan siendo, del mismo modo que el sistema telefónico y la red de autopistas verdaderas (las carreteras) son diferentes en cuanto a su finalidad y uso.

Por ello, mi predicción –y posiblemente mi deseo– es que en el futuro habrá dos tipos de superautopistas de la información: una "Internet Plus", red digital de altas prestaciones, derivada de la Internet actual, de uso extendido entre diversas comunidades académicas, comerciales, culturales... pero cuyas raíces sigan estando en los sectores científicos e investigadores, financiada por el gobierno, las instituciones usuarias y los individuos particulares; con servicios comerciales, desde luego, pero sin depender apenas de publicidad y de anuncios. La otra superautopista surgiría de la tecnología y servicios de las industrias y medios de comunicación de masas, principalmente de las empresas de cable y de televisión, con una amplia gama de servicios interactivos multimeda que, para poder afrontar unas tarifas competitivas y razonables tendrá que apoyarse en reclamos publicitarios y propaganda comercial, al menos mientras se va implantando la infraestructura necesaria para ello. Este aspecto sería rechazado de forma contundente por los usuarios tradicionales de la Internet, normalmente más alejados de la contaminación y de las promesas vacuas de los medios de comunicación de masas. Eso no sería –no podría– ser ya la Internet; sería algo distinto, que en algunos círculos se ha bautizado como la "Antinet". Ambas superautopistas podrían compartir la infraestructura de comunicación banda ancha, pero funcionalmente serían redes diferentes.

La Internet que conocí hace 20 años será dentro de otros 20 algo muy distinto de lo que conocemos hoy.

15.- Conclusión

La Internet que conocí hace 20 años, la red de redes en la que, en años recientes, me esforcé por su implantación en España, la mayor red mundial de información distribuída, que se ha ido construyendo con la dedicación y el entusiasmo de los expertos, usuarios, suministradores, gobiernos... será dentro de otros 20 años algo muy distinto de lo que conocemos hoy.

Curiosa paradoja la de una red que nació en la época de la guerra fría, derivada de unas motivaciones un tanto siniestras. Muy pronto los usuarios la tomaron por asalto; desde entonces no la han soltado; la comunidad inicial se ha ampliado por todos los continentes, creando una nueva cultura de la información, con unas cotas de libertad que sobrepasan cualquier tipo de barrera artificial. A diferencia de lo que ocurre en organizaciones internacionales, aquí el consenso se ha logrado de forma natural. Quisiera que la probable y necesaria evolución de la Internet se mantuviera dentro de ese estilo machadiano y siguiera haciendo camino al andar.

José Barberá
Fundesco
Director del Dpto. de Redes
barbera@fundesco.es

PRONTUARIO

Centro de Comunicaciones CSIC RedIRIS

Serrano, 142
28006 Madrid

Tel.: (91) 5855150
Fax: (91) 5855146

Puntos de Información

Información general: infoiris@rediris.es
Información administrativa: secretaria@rediris.es

Centro de Gestión de red

E-mail: noc@rediris.es
Tel.: (91) 5855150
Fax: (91) 5855146

Registro delegado de Internet (ES-NIC)

E-mail: nic@rediris.es
Tel.: (91) 5855150
Fax: (91) 5855146

Para obtener formularios de solicitudes de información general, direcciones oficiales IP, registro de dominios o resoluciones de direcciones inversas:

FTP anonymous: ftp.rediris.es directorio: /es-nic

Servicio RedIRISdial

E-mail: redirisdial@rediris.es
Tel.: (91) 5855112/5855138
Fax: (91) 5855146

Para obtener formularios de solicitudes e información general:

FTP anonymous ftp.rediris.esdirectorio: /infoiris/redirisdial
Lista de distribución: redirisdial-L@listserv.rediris.es

Coordinación de correo electrónico

E-mail: postmaster@rediris.es
Tel.: (91) 5855138
Fax: (91) 5855146

Servidores de Información

www general:	http://www.rediris.es/	
X.500:	telnet x500.rediris.es	login:directorio
	http://x500.rediris.es/	
Archie:	telnet archie.rediris.es	login:archie
Gopher:	gopher.rediris.es	
FTP anonymous:	ftp.rediris.es	

Difusión

Para suscripciones o envío de colaboraciones al Boletín:

E-mail: boletin@rediris.es
Tel.: (91) 5855148
Fax: (91) 5855146

Listas de distribución

LISTSERV: Servidor central de listas: listserv@listserv.rediris.es

EXPLODE: iris-foro@noc.rediris.es (Temas de interés general)
iris-gaceta@noc.rediris.es (Gaceta electrónica de RedIRIS)
iris-mail@noc.rediris.es (Coordinación de correo electrónico en la comunidad de RedIRIS)

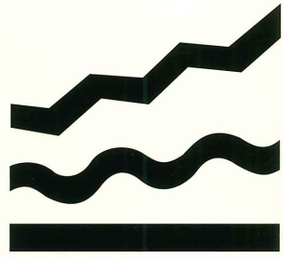
Para suscribirse o borrarse de las listas en EXPLODE enviar un mensaje a las direcciones:

iris-foro-request@noc.rediris.es
iris-gaceta-request@noc.rediris.es
iris-mail-request@noc.rediris.es

cuyo cuerpo sea: subscribe
stop

o bien

unsubscribe
stop



PLAN
NACIONAL
DE I+D