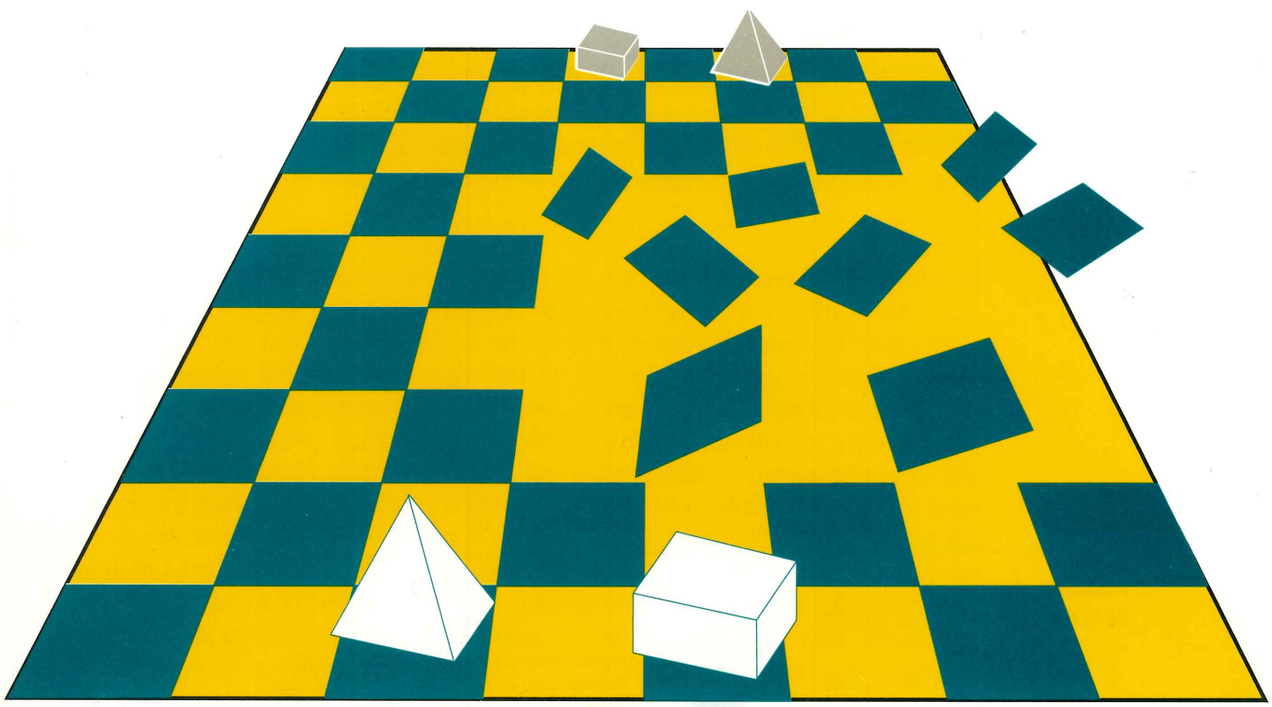
Red IRIS

Plan Nacional de I+D

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

nº 23



nº 23
Mayo 1993

Boletín de la
Red IRIS

Sumario

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

Edita: RedIRIS
Alcalá 61, 1ª Plta. 28014 Madrid.
Tel.: 435 12 14.
Director Técnico: José Barberá Heredia
Coordinación: María Bolado
Filmación: BOCETTO, S.L.

Producción: Estudio 5
Portada: Clara Alvárez Cabiró
Autoedición: María Bolado
Imprime: GRAFISUR, S.L.
Distribución: B.D. Mail, S.A.
Depósito legal: M. 15844-1989

Presentación

José Barberá

Uno de los principales factores que han contribuido al éxito y expansión de la Internet es, sin duda, la distinta manera de concebir, elaborar y poner en práctica los "estándares", en comparación con los procedimientos seguidos en los organismos típicos de normalización tales como ISO. Las comillas anteriores son importantes, por cuanto que estándares, como tales, sólo son aquellos que producen las organizaciones internacionales de normalización. Nos referimos, pues, a "estándares de facto" que, en el caso de la Internet, pueden encontrarse fácilmente dentro de la popular serie de RFCs (*Request for Comments*).

El órgano de la Internet que lleva a cabo las tareas de discusión, especificación y desarrollo de estándares (nos olvidamos ya de la comillas) es el IETF (*Internet Engineering Task Force*). De su última reunión, que tuvo lugar a principios del pasado mes, se da cuenta en este boletín. Uno de los temas candentes, tratados a lo largo de las sucesivas sesiones, fue el de la discusión sobre las distintas propuestas para sustituir al actual protocolo IP. Como es sabido, la rápida expansión de la Internet está agotando el espacio de direcciones disponible, el cual, hace tan sólo unos años, se pensó que sería prácticamente inagotable (podríamos decir por ello que la Internet está "muriendo de éxito"). De ahí la necesidad de encontrar un sustituto al actual protocolo que realiza la interconexión de redes. Tres son los candidatos que compiten para ello. Se entra así en el proceso habitual seguido para la adopción de un nuevo estándar.

La diferencia básica entre los estándares de ISO y los de la Internet está en que aquellos se producen de arriba a abajo, mientras que la Internet sigue el camino inverso: primero desarrollar y luego estandarizar. Este matiz no es trivial, porque en ISO las propuestas se discuten en abstracto entre los diferentes comités implicados, para dar lugar luego a subconjuntos de estándares o perfiles funcionales que, llegado el momento (tras unos cuantos años, quizás), habrá que ver si los fabricantes los producen, si funcionan y si son compatibles entre sí. (Todo esto para la mayor perplejidad y desesperación de los usuarios; ¿nos recuerda algo?). Por contra, el IETF -que no tiene una estructura demasiado formal- funciona como una "banda" de francotiradores cualificados, provistos todos ellos de municiones RFC dispuestas a ser utilizadas cuando llegue el momento. Y, así, se llega a producir estándares en la Internet. Seguramente, esta forma tan peculiar de estandarizar es lo que ha llevado a la Internet a la situación presente: más de un millón de máquinas conectadas, más de 100.000 redes de diversos tipos, unos cinco millones de usuarios. Mientras tanto, los sumos pontífices de OSI se siguen rasgando las vestiduras.

Parece que, coincidiendo con la caída del bloque del Este, han acabado también las guerras de protocolos (recalco lo de "parece"). Ahora, lo que queda bien es hablar de redes multiprotocolo. Con ello normalmente se hace referencia a los tres protocolos del nivel 3 (red): X.25 (una servidumbre del pasado, obra y "gracia" de los operadores telefónicos), IP (la tecnología del presente: del presente para nosotros, porque en EE.UU. ya tiene una cierta solera) y CLNP o ISO-IP (una posible solución de futuro para abordar el problema del agotamiento de direcciones IP). A todo esto, me refiero a la situación en Europa, porque en este lado del Atlántico nuestras peculiaridades culturales nos llevan normalmente a hacer las cosas un poco más complicadas. Una vez logrado el consenso sobre la necesidad de tener una red multiprotocolo a la carta, ¿estamos ya todos de acuerdo?. Pues parece que ni aún así. Por eso tenemos en Europa dos *backbones* multiprotocolo para las redes de I+D: Ebone y EuropaNET. En la sección Noticias se comparan sucintamente ambas. Al final, lo que subyace como desacuerdo no es la tecnología en sí, sino el modelo de gestión: ¿se dedican los expertos en redes del mundillo de la I+D a desarrollar la tecnología y proporcionar el servicio?, o, ¿dejamos a los operadores tradicionales (en este caso el PTT Telecom) que se ocupen de esa tarea?. Ahí parece estar ahora el punto álgido de la discusión.

La diferencia básica entre los estándares de ISO y los de la Internet está en que aquellos se producen de arriba a abajo, mientras que la Internet sigue el camino inverso: primero desarrollar y luego estandarizar

Lo que subyace como desacuerdo no es la tecnología en sí, sino el modelo de gestión: ¿se dedican los expertos en redes del mundillo de la I+D a desarrollar la tecnología y proporcionar el servicio?, o, ¿dejamos a los operadores tradicionales que se ocupen de esa tarea?

RedIRIS ha puesto en marcha un embrión de red CLNS que forma parte de la red europea experimental

Y ya que hablabamos de los problemas de las direcciones de la Internet y del protocolo ISO-IP, en la sección Enfoques se presenta la experiencia española en el tema CLNS de ISO. El grupo que la ha llevado a cabo ha sentado las bases necesarias para -llegado el caso- hacer la migración del IP actual al ISO-IP, uno de los tres posibles sustitutos. De hecho, RedIRIS ha puesto en marcha un embrión de red CLNS que forma parte de la red europea experimental. Que el CLNP (ISO-IP) vaya a desplazar al actual IP depende de lo que finalmente se decida en la Internet, con su peculiar manera de adoptar estándares. En ese sentido se discuten las ventajas tecnológicas del CLNP frente a los otros dos competidores. Sin embargo, parece que uno de los argumentos en contra del CLNP es que parte de la comunidad Internet no ve con buenos ojos la adopción de un estándar de ISO, con quien, por tradición, se arrastra un enfrentamiento casi permanente. De este modo, la candidatura del CLNP tiene en su contra el estigma NIH: *Not Invented Here*. La solución final, por lo menos para después del verano. Aún es tiempo para hacer apuestas.

En función del nivel de seguridad deseado se pueden construir redes de mayor o menor valor añadido

En nuestra experiencia CLNS, una vez puesta en marcha la red, está la cuestión de las aplicaciones que vayan por ella. El candidato más necesitado parece ser DECNET (que ya agotó su espacio de direcciones mucho antes que en la Internet). Lo que se conoce como DECNET Fase V utiliza precisamente ese protocolo de red. De ahí el interés del grupo español de DECNET (FAE-CAD), estrechamente vinculado a HEPnet, en participar activamente en este proyecto. Con todo, tras una lectura detenida del artículo en cuestión, a uno le queda la duda del significado exacto de la expresión "pérdida de visibilidad o conectividad entre España y el exterior (HEPnet)". Queda apuntado como problema a resolver. Al final, el quid de la cuestión es si los usuarios de DECNET en España estarán en una red gestionada por RedIRIS o, por el contrario, dependerán de la gestión de HEPnet-Europa. Asunto ya demasiado manido como para sorprender a nadie a estas alturas (o, ¿todavía se sorprende alguien?).

El otro artículo de Enfoques versa nuevamente sobre el tema de la seguridad en las redes. Los mismos autores de la UPC que en el anterior boletín escribieron sobre aspectos de seguridad en el correo electrónico descienden ahora hasta el nivel de transporte, para investigar sobre los mecanismos que permiten diseñar redes seguras en lo que a transmisión de datos se refiere. Con ello se trata de evitar posibles agresiones tales como: suplantación de identidad, monitorización o espionaje y alteraciones de tráfico. En función del nivel de seguridad deseado se pueden construir redes de mayor o menor valor añadido (lo que lógicamente vendría acompañado de un coste añadido y, seguramente, de un menor rendimiento efectivo: el ancho de banda es finito). El artículo se basa en los resultados de un proyecto ESPRIT y sus autores anuncian la aparición, en breve, de una versión beta, que es de esperar sirva como banco de pruebas, lo que llevaría a producir versiones posteriores en un proceso de refinamiento progresivo. En último término, lo que se vaya a utilizar en las redes dependerá de su aceptación como estándar (*de iure* o *de facto*). Al principio de esta presentación hablaba de dos procedimientos posibles: el de los comités de ISO y los RFCs que bendice el IETF. Dado que, por lo que se ve, hay ahora otros asuntos más urgentes a resolver, la seguridad real en las redes reales es un aspecto que, desgraciadamente, tardaremos todavía algún tiempo en verlo materializado.

José Barberá
Director de RedIRIS
jose.barbera@rediris.es
C=es; ADMD=mensatex;
PRMD=iris; O=rediris;
S=Barbera; G=Jose

Instalado el nodo de ARTIX en Santiago de Compostela

Ha quedado instalado y operativo en el Centro de Supercomputación de Galicia, en Santiago de Compostela, el nodo de la red ARTIX previsto para conectar a los centros académicos y de investigación gallegos integrados en RedIRIS. Este nodo está unido con el de Madrid mediante un enlace de 64 Kbps.

Con las nuevas instalaciones del Centro de Supercomputación de Galicia ya están conectados, o en fase avanzada de instalación, las tres universidades de la zona: La Coruña, Santiago y Vigo, incluyendo los campus universitarios que poseen en El Ferrol, Lugo, Orense y Pontevedra, y los centros del Consejo Superior de Investigaciones Científicas (CSIC) ubicados en Vigo, Pontevedra y Santiago.

Este nodo de Santiago completa el desarrollo planificado de la red de transporte ARTIX extendiendo su cobertura a todo el territorio nacional.

¿Cómo iniciar el servicio X.500 en un centro?

Los centros que deseen instalar el servicio de directorio, se deben poner en contacto con el 'help-desk' del directorio que se describe al final de estas líneas.

La puesta en marcha de este servicio en un centro necesitará de un análisis previo que permita llegar a una solución óptima entre la infraestructura informática y las posibilidades que ofrece el piloto. Muy resumidamente se indican estas posibilidades de conexión.

El piloto X500 de RedIRIS ofrece dos tipos de acceso. Los centros pueden optar por instalar su propio servidor, o mantener su información en los sistemas centrales de RedIRIS, instalados en Barcelona, Madrid y Sevilla.

Sistemas Centrales.

Los servicios centrales están formados por un acceso público de consulta, y por cuentas nuevas de gestión de la información. Estas últimas tendrán 'password', y existirá una por organización que elija este medio de gestión de sus datos. Los sistemas centrales son accesibles desde IBERPAC y ARTIX mediante XXX y en Internet por telnet. Las restricciones en este caso son mínimas. El centro debe disponer de algunos de los dos accesos anteriores por terminal remoto.

Servidores en los centros.

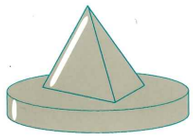
Se recomienda, siempre que sea posible, la instalación de servidores por diversas razones técnicas, entre ellas, un mejor uso de las comunicaciones y disminución del tiempo de respuesta en consultas locales.

Pero no siempre será posible esta instalación. Las restricciones en este caso las impone el software de directorio y el tipo de conexión externa del centro. QUIPU será el software utilizado para prestar este servicio a los centros. En el listado siguiente se detallan los sistemas UNIX y los tipos de red sobre los que se puede instalar.

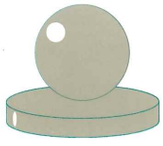
Sistemas UNIX	TCP/IP	X.25
AIX 3.2	X	
Apollo	X	
A/UX release 2.0.1	X	
generic 4.2BSD UNIX	X	
generic 4.3BSD UNIX	X	
RT/PC with 4.3BSD	X	
4.4BSD UNIX with OSI	X	
Concurrent RTU 6.0	X	
HP-UX	X	X
MIPS RISC/OS	X	
Olivetti LSX 30xx	X	
Ridge Operating System	X	
Solbourne	X	
SunOS release 3 with SunLink OSI/X.25 release 5.2	X	X
SunOS release 4 with SunLink OSI/X.25 release 6.0	X	X
SunOS release 4 with SunNet OSI release 7.0	X	X
SunOS release 4 with SunNet X.25 release 7.0	X	X
SunOS release 3	X	
SunOS release 4	X	
SunOS release 4.1	X	
SVR2 UNIX with EXOS	X	
RT/PC with AIX	X	
SVR2 UNIX emulation on SunOS release 3	X	
SVR2 UNIX with WIN/TCP	X	
generic SVR3	X	
generic SVR4	X	
Ultrix 3.1	X	X

Instalado el nodo de ARTIX en Santiago de Compostela

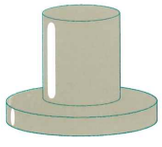
¿Cómo iniciar el servicio X.500 en un centro?



¿Cómo iniciar el servicio X.500 en un centro?



Conexiones internacionales para tráfico IP



¿Un backbone común en Europa?

La máquina debe tener una conexión externa TCP/IP (Internet) o x25 (IBERPAC, ARTIX).

Puntos de información.

Para ultimar detalles sobre la solución posible u óptima, contacte con el servicio de información X.500, en las direcciones de correo <infodir@rediris.es> e <infodir@cica.es>. Esta última dirección sólo para centros en Andalucía.

Conexiones internacionales para tráfico IP

Las principales novedades en este terreno están constituidas por la anunciada entrada en servicio del nuevo enlace internacional de 128 Kbps Madrid-Amsterdam (EBONE), en sustitución del anterior de 64 Kbps, el pasado dia 26 de Marzo, y por el mejor aprovechamiento de EMPB para tráfico IP internacional gracias a la creación de conexiones directas (mediante túneles IP sobre X.25) con aquellos lugares con los que se puede obtener una mejor conectividad por esta via que por EBONE.

De esta forma la situación actual de conectividad IP internacional es la siguiente:

- Conexiones bilaterales directas via EMPB (acceso a 64 Kbps) con: SWITCH (Suiza), JANET (Reino Unido) y Portugal. Las comunicaciones con este último país han experimentado una considerable mejora, al aprovecharse ahora la capacidad de la línea que EMPB tiene entre Lisboa y Madrid (64 Kbps) para el intercambio del tráfico IP.

- Resto de destinos via Ebone (acceso a 128 Kbps).

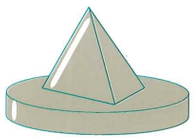
- Tanto EMPB como Ebone se utilizan como caminos de backup respectivos para los destinos que en primera opción se encaminan por el otro.

¿Un *backbone* común en Europa?

La idea manejada durante el año pasado de disponer en Europa de un *backbone* común para las diferentes redes de I+D se ha materializado en determinadas acciones específicas, aunque lejos todavía de cristalizar en una infraestructura común de comunicaciones. 1993 no va a ser el año que vea la consolidación de tal empeño. Por el momento "coexisten" (a la francesa) dos iniciativas: Ebone y EuropaNET (antes EMPB, mucho antes IXI). Por su especial relevancia para los servicios de RedIRIS, damos aquí una reseña sobre la situación de ambas redes.

Ebone (o mejor Ebone 93) continúa su operación en este año como esfuerzo cooperativo de varias organizaciones europeas de redes, aunque con una estructura organizativa algo más formal que durante 1992. En la figura 1 puede verse la topología actual. Tres de los enlaces troncales que interconectan los EBS (*Ebone Boundary System*) han aumentado el ancho de banda a un mínimo de 1,5 Mbps. Del mismo modo ha aumentado la capacidad intercontinental en una proporción parecida. Existe un cierto desequilibrio en las conexiones del EBS de Londres, que sólo llegan a 256 Kbps (en esta situación el camino más rápido entre Londres y París y entre Londres y Estocolmo es por EE.UU.). Este es uno de los problemas pendientes a resolver.

Ebone ofrece un servicio global IP (acceso global a la Internet) a los proveedores de servicio europeos, tanto redes de I+D como otros de tipo comercial. Desde el punto de vista de las reglas de acceso Ebone es neutro, es decir que no impone restricciones en los EBS. Los RBS (*Regional Boundary System*) de cada red conectada pueden imponer -si lo desean- las restricciones de acceso que determinen. Las conexiones RBS-EBS pueden ser locales (caso de los RBS situados en el mismo lugar que el EBS) o remotas, mediante enlaces contratados a los operadores correspondientes. La conexión del RBS de RedIRIS se hace con el EBS de Amsterdam mediante un enlace de 128 Kbps (desde finales de marzo de este año).



¿Un backbone común en Europa?

En cuanto a la distribución de costes entre cada "cooperativista", ésta se hace, en 1993, de la siguientes manera. Se calcula el coste global de:

- todos los enlaces troncales (entre EBS)
- los enlaces intercontinentales (parte europea)
- la amortización de equipos que materializan las funciones de EBS
- el personal de operación de los EBS y del equipo de gestión de la red
- el 75% de los enlaces de acceso RBS-EBS de las redes nacionales de I+D

El coste global se reparte entre todos los RBS de modo proporcional al ancho de banda "contratado" para el acceso. Para cada socio se calcula la diferencia (a favor o en contra) entre su cuota global así resultante y su aportación en recursos (líneas, equipos, mano de obra) a Ebone. Uno de los problemas por resolver satisfactoriamente es el del "ancho de banda contratado". Evidentemente, para una organización con un RBS remoto ese ancho de banda ha de ser la capacidad de la línea de acceso. Sin embargo, el problema surge cuando hay organizaciones cuyo acceso es local (Ethernet a 10 Mbps) y "contratan" un ancho de banda inferior al máximo disponible (por ejemplo 64 Kbps). La solución provisional decidida por los socios es medir el tráfico cursado y, en caso de que éste supere a la capacidad contratada, obligar a la organización a aumentar la cuota, o bien poner un línea serie de la velocidad correspondiente.

En la figura 2 se ve la topología de EuropaNET a principios de 1993. Esta red es gestionada por el PTT Telecom (Holanda) y los clientes son las organizaciones y redes (privadas y públicas) que allí se muestran. En la actualidad el servicio de EuropaNET es

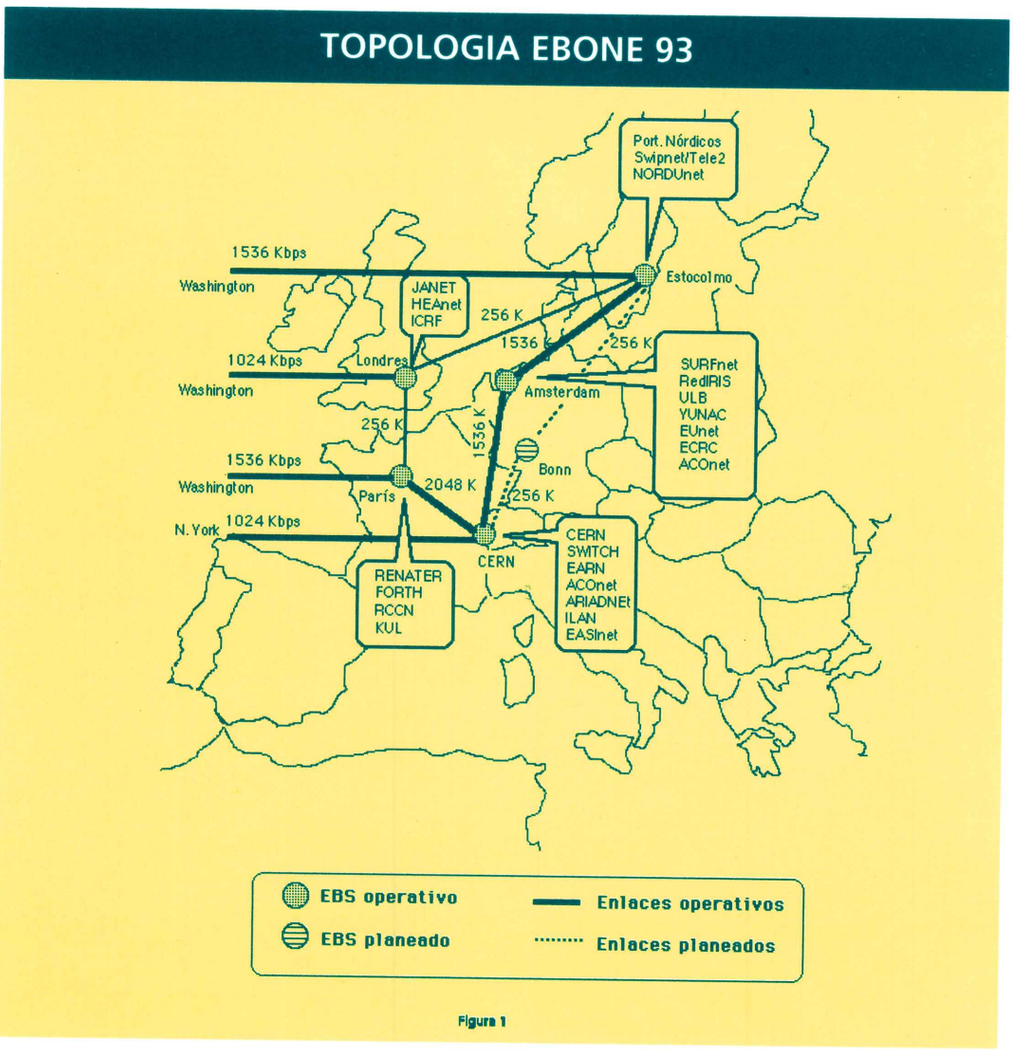


Figura 1

¿Un backbone común en Europa?

TOPOLOGIA EuropaNET

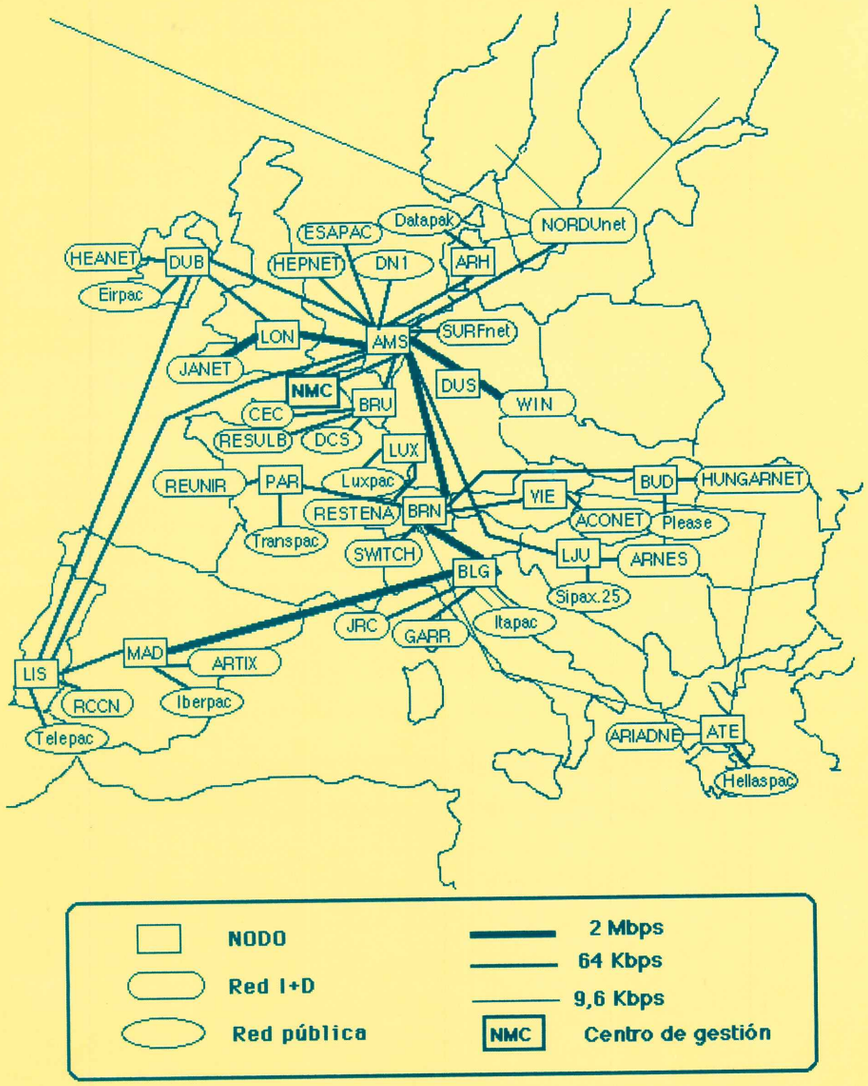


Figura 2

X.25, aunque hay intención de ofrecer en breve un servicio IP (nativo). Para ello habrá una fase piloto previa de 4 meses que está prevista empiece en abril. De momento el tráfico IP que se puede cursar por EuropaNET ha de encapsularse sobre X.25 (como se hacía con IXI) estableciendo túneles IP/X.25 mediante acuerdo bilaterales entre organizaciones usuarias, o bien haciendo uso de la facilidad general de conversión IP/X.25 que ofrece JANET (previo acuerdo) y que es similar a lo que venía haciendo el instituto NIKHEF de Amsterdam.

Aunque en la figura 2 se muestra la capacidad de los diversos enlaces troncales de EuropaNET, hay que tener en cuenta que esa topología es transparente al usuario, quien ve únicamente una "nube" con diversas velocidades de acceso, en múltiplos de 64 Kbps, hasta 2 Mbps. En la actualidad sólo WIN (Alemania) y JANET (Reino Unido) tienen el servicio (X.25) a 2 Mbps. El acceso actual de RedIRIS (ARTIX) es de 64 Kbps, el mismo que había con IXI. Está previsto poder contratar el acceso a 2 Mbps. cuando ese servicio esté disponible, lo que no sucederá antes del próximo otoño. En cuanto a la conectividad intercontinental de EuropaNET hay que decir que, aunque hay planes de establecer un enlace con EE.UU., de momento su uso queda delimitado a Europa.

Comparando Ebone y EuropaNET vemos que cada una de ellas ofrece determinadas ventajas, aunque presentan ciertas limitaciones. Por el interés que ello puede tener para los usuarios de RedIRIS, se enuncian a continuación los puntos fuertes y débiles de cada una de ellas.

Puntos fuertes de Ebone:

- conectividad IP (acceso a Internet) global
- tecnología de punta
- puesta en servicio rápida y gran flexibilidad de adaptación a la evolución tecnológica
- acceso neutro (no restringido)

Puntos débiles de Ebone:

- organización inestable a medio plazo ("cooperativa de socios")
- esquema de distribución de costes no totalmente equitativo (favorece a las conexiones locales) y variable de año en año
- no se asegura una calidad de servicio específica
- costes de acceso relativamente altos para RBS con acceso remoto

Puntos fuertes de EuropaNET:

- tarifas bastante atractivas
- calidad de servicio predeterminada
- gestión y operación profesional

Puntos débiles de EuropaNET:

- lentitud de respuesta a la demanda de servicio multiprotocolo
- no ofrece (todavía) conectividad global IP
- a pesar de los buenos resultados obtenidos en las pruebas, existen aún incertidumbres respecto a su comportamiento frente a tráfico IP real y su interacción con otras redes.

Aparte de todo ello, la realidad es que se libra una batalla más o menos encubierta entre dos enfoques contrapuestos: contratar la operación a un proveedor externo (EuropaNET) y que los expertos en la comunidad de redes de I+D se ocupen de esa tarea (Ebone). Tras ese enfrentamiento hay, evidentemente, determinados intereses (comerciales, de protagonismo,...) en ambos bandos.

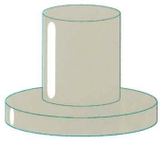
Dados los recursos disponibles en RedIRIS, nuestra actitud es mantenerse al margen de las polémicas y ser pragmáticos. Por eso se mantienen las conexiones a ambas redes y en las condiciones antes señaladas. La idea que se maneja en los círculos de iniciados en redes es que Ebone parece tener un futuro brillante como punto neutro de interconexión global para Europa, no tanto así como proveedor de servicios *backbone* para redes. En este sentido EuropaNET resulta mucho más prometedor con las tarifas actuales. Queda por ver cuando puede tener lugar esa sustitución de funciones, manteniendo o mejorando la conectividad y a un precio inferior. Cuando eso ocurra -si ocurre- RedIRIS no tendrá inconveniente en decantarse por la solución más eficaz. Mientras tanto no queda más remedio que seguir jugando con dos barajas.

Reunión IETF

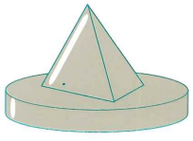
Entre los días 29 de Marzo y 2 de Abril tuvo lugar en Columbus, Ohio, la reunión número 26 del IETF (Internet Engineering Task Force).

El IETF es el órgano encargado de llevar a cabo la fase de especificación, discusión y desarrollo de estándares de la Internet y se estructura en diferentes grupos que abarcan todos los niveles (desde servicios de aplicación, atención e información a los usuarios, hasta tecnologías de niveles bajos) de que consta el esqueleto tecnológico de la Internet.

Durante la reunión se procedió a la designación de nuevos miembros del IAB (Internet Architecture Board) encargado de la orientación tecnológica de la Internet y del IESG (Internet Engineering Steering Group) u órgano coordinador de las tareas del IETF. Otro plato fuerte lo constituyó la presentación de diferentes propuestas para el sustituto del actual protocolo IP (versión 4), debido a los problemas que plantea el previsible agotamiento del actual espacio de direcciones. En sucesivas sesiones plenarias, así como en demostraciones prácticas, se presentó el estado actual de los diferentes candidatos:



¿Un backbone común en Europa?



Reunión IETF

Reunión IETF

- **TUBA** (TCP and UDP with Bigger Addresses) Sustitución de IP v. 4 por el protocolo de red no orientado a la conexión de ISO (CLNP). Las direcciones IP de 32 bits se sustituyen por NSAPs (hasta 20 octetos).

- **SIP** (Simple IP) Utiliza unos cabeceros IP en los que se eliminan los campos que actualmente no se usan y se da cabida a direcciones IP de 64 bits de asignación jerárquica -geográfica /proveedor-). La migración se realiza mediante encapsulamiento de IP sobre IP utilizando IPAE.

- **PIP** (Protocolo P-IP) Un recambio para IP totalmente nuevo y lleno de nuevas facilidades (selección de proveedor en base a preferencia del originador y mecanismos de asignación de flujo entre las mas llamativas).

Estas propuestas habrán de seguir el camino habitual de normalización dentro de la Internet, que conlleva los siguientes pasos: Especificación, desarrollo de productos, planes de migración, proposición de estándar, promulgación de estándar oficial, ... en su devenir hasta que alguna de ellas sea considerada finalmente como el protocolo oficial (IP versión 7) de la futura Internet.

En otra de las sesiones se presentó el nuevo NIC (Network Information Centre)de la Internet: el **InterNIC**. Este servicio será prestado por una serie de compañías, entre las que destaca ATT, bajo contrato con la NSFnet. El InterNIC actuará como coordinador de otros centros regionales como el RIPE NCC en Europa. Por primera vez se plantea el que los servicios ofrecidos por el NIC puedan ser facturados a determinadas organizaciones fuera del ámbito de I+D o que determinadas aplicaciones (bases de datos particulares o accesos de gran volumen) puedan asimismo ser facturadas a sus clientes. Los servicios del InterNIC estarán disponibles mediante una gran variedad de mecanismos de acceso: telnet, FTP, archie, whois, gopher, WAIS, WWW, X.500, ...

Todas las sesiones plenarias y algunas de las reuniones de los grupos de trabajo fueron retransmitidas mediante video y audioconferencia a través de la Internet. En próximos números del boletín de RedIRIS se dará cuenta de los mecanismos que están actualmente disponibles en la Internet para este tipo de aplicaciones.

A continuación se detallan algunas de las líneas de actuación actuales de los diferentes grupos de trabajo del IETF:

- **Servicios de directorio integrados:** WHOIS++ (páginas blancas) y X.500 (páginas amarillas).

- **Acceso a bases de información distribuidas:** WWW (World Wide Web) y protocolos para la manipulación y acceso a *hipermedios* (HTTP). Identificadores Universales de Recursos (URLs).

- **Correo electrónico:** *Multimedia* (MIME, HARPOON). Extensiones SMTP (8 bits). Utilización del directorio X.500 por X.400 (MHS-DS). Gestión de X.400 mediante SMTP (MADMAN). Seguridad (PEM).

- **Gestión de red:** SNMP versión 2.

- **Routing:** BGP4. OSPF2. Requisitos para routers IP (RREQ).

- **Niveles bajos:** Multicast IP. PPP sobre varios medios. IP sobre ATM.

La próxima reunión del IETF tendrá lugar en Amsterdam durante los días 12 a 16 de Julio de 1993.

La experiencia española ISO-CLNS

David Fernández, Celestino Tomás y Grupo de trabajo de DECnet-OSI

1.- Introducción

El grupo de trabajo 4 de RARE, cuya actividad se centraba en la tecnología de red, propuso a COSINE un proyecto sobre el servicio CLNS de OSI. El CLNS (ConnectionLess mode Network Service) está basado en la familia de protocolos CLNP, también llamados ISO-IP, que soportan el servicio de red no orientado a la conexión de OSI.

Este nuevo proyecto se formalizó en Mayo de 1991 con el subproyecto 4.1 de RARE y COSINE. Su duración fue hasta Marzo de 1993, y en él participaron 16 redes europeas y organizaciones internacionales, entre ellas RedIRIS.

Sus actividades y objetivos fueron, entre otros: adquirir experiencia sobre este nuevo protocolo, realizar test de sistemas de diferentes casas comerciales, diseño de un servicio a nivel europeo y creación de un primer embrión de red con conexión a otros pilotos CLNS existentes en Estados Unidos.

El servicio CLNS, por el direccionamiento que utiliza y su routing jerárquico, soluciona muchos de los problemas que tienen algunas de las redes actuales.

El servicio CLNS, por el direccionamiento que utiliza y su routing jerárquico, soluciona muchos de los problemas que tienen algunas de las redes actuales.

De este modo, el CLNP es el protocolo utilizado, entre otros, en DECnet/OSI o DECnet fase V para solucionar el problema de agotamiento del espacio de direcciones de DECnet fase IV.

Un problema similar tendrá a medio plazo la actual versión de la arquitectura de comunicaciones IP. La Internet se encuentra en un crecimiento continuo y su actual espacio de direcciones, IP versión 4, se está agotando. El problema se agrava aún más al considerar su direccionamiento que imposibilita una estructura jerárquica, obligando a los routers a almacenar grandes tablas de encaminamiento.

Se han presentado varias propuestas en la Internet destinadas a sustituir el actual IP por otro protocolo, denominado IP versión 7. Uno de los candidatos más firmes para ello es TUBA. TUBA consiste en montar las actuales aplicaciones y IP sobre CLNP.

Por otra parte, varias casas comerciales han sacado al mercado software basado en esta nueva tecnología de red, posiblemente, debido a que el CLNS se ha convertido en un requisito en los perfiles de interconexión de sistemas abiertos de la Administración de algunos países, perfiles denominados GOSIP.

Por todos estos motivos se inició el proyecto de COSINE anteriormente mencionado. En paralelo y dentro de este proyecto europeo, RedIRIS puso en marcha una experiencia ISO-CLNS. Con objeto de seguir las evoluciones de esta tecnología y crear un primer embrión de red a nivel de nacional.

Seis centros participan en esta experiencia: el CICA, el Grupo de Altas Energías de UNICAN, el Departamento de Ingeniería de Sistemas Telemáticos de la UPM, el CIEMAT, la UIB y FUNDESCO.

En las siguientes secciones se describe la situación actual de esta experiencia, los avances en la ardua tarea de migración de DECNET fase IV a OSI, el posible uso del CLNS por Internet, y los futuros planes tanto a nivel nacional como europeo sobre esta nueva actividad de red.

2.- Tutorial sobre ISO-IP

2.1.- Introducción a CLNP

La importancia de CLNP se prevé creciente, aunque su implantación en el entorno académico depende en gran medida del éxito de TUBA

El protocolo ISO 8473, conocido normalmente por CLNP (ConnectionLess Network Protocol) o simplemente por ISO-IP, es el protocolo propuesto por ISO para ofrecer el servicio de red no orientado a conexión dentro de la arquitectura OSI. Es un *protocolo interred*, esto es, un protocolo independiente del tipo o tecnología de las subredes empleadas. Se sitúa por encima de los protocolos propios de cada subred (X.25, IEEE 802, etc) y se aísla de ellos mediante un subnivel de convergencia, que adapta el servicio que ofrecen las subredes al servicio esperado por CLNP. Por ser un protocolo interred, CLNP se adapta bien a redes de gran tamaño y diversidad.

CLNP es muy similar al protocolo IP de Internet, de ahí su "apodo" ISO-IP. Tanto las funciones de ambos protocolos como el servicio que ofrecen al nivel de transporte son semejantes, aunque incompatibles.

No obstante, dos son las características básicas que diferencian a CLNP respecto de IP: las direcciones utilizadas (NSAP) y la arquitectura de protocolos de encaminamiento asociados. Estas dos características son las que, como veremos, hacen de CLNP un firme candidato a sustituir a IP en Internet, ya que solucionan sus problemas más apremiantes.

Varias son la razones que avalan la importancia de CLNP. Citaremos a continuación algunas de las principales:

* La nueva arquitectura de protocolos de Digital, conocida popularmente por DECNET phase V utiliza a CLNP como protocolo de red.

* Algunos perfiles de protocolos gubernamentales, tales como U.S.GOSIP, incluyen a CLNP. Esto implica que los productos de comunicaciones financiados por esos gobiernos deben incluir CLNP obligatoriamente.

* Existen ya en el mercado múltiples implementaciones de CLNP, para sistemas intermedios y sistemas finales. A destacar la nueva versión del sistema operativo UNIX BSD, que contribuyó a principios de los años 80 a la popularización de IP, y que en su última versión incluye CLNP.

* La sustitución de IP por CLNP (TUBA) se perfila como una de las principales propuestas de solución a los graves problemas que sufre Internet en la actualidad.

* Existen varios proyectos piloto, tanto a nivel nacional como internacional, de utilización de CLNP y sus protocolos de encaminamiento asociados. Además, un número creciente de redes, entre ellas grandes backbones como NSFnet, EuropaNET o EBONE, ofrecen o tienen previsto ofrecer CLNP.

En resumen, la importancia de CLNP se prevé creciente, aunque su implantación en el entorno académico depende en gran medida del éxito de TUBA.

2.2.- Direccionamiento en CLNP

CLNP utiliza como direcciones de red los llamados NSAP (Network Service Access Point). Brevemente, sus principales características, confrontadas con las de las direcciones IP, son las siguientes:

* Son *direcciones globales*, al igual que las direcciones IP. Pero, a diferencia de ellas, un sistema con conexiones a varias subredes sólo tiene un NSAP, frente a las múltiples direcciones del mismo sistema en IP.

* Permiten una *asignación descentralizada y jerárquica*. En Internet la asignación no es jerárquica y, hasta hace poco tiempo, se hacía de forma centralizada.

* Ofrecen un *amplio rango de direccionamiento*. Los NSAPs tienen una longitud máxima de 20 octetos, frente a los 4 de las direcciones IP.

Los NSAPs son direcciones globales, permiten una asignación descentralizada y jerárquica y ofrecen un amplio rango de direccionamiento

A grandes rasgos el formato de un NSAP es el que aparece en la figura 1. Se divide en dos partes: Initial Domain Identifier (IDP) y Domain Specific Part (DSP). El IDP identifica la autoridad de direccionamiento encargada de asignar las direcciones de este dominio (todas las que comienzan con el valor indicado en el IDP). El IDP indica, además, el tipo de NSAP de que se trata. El DSP no tiene un formato predefinido y debe ser la autoridad de direccionamiento indicada en el IDP quién lo especifique.

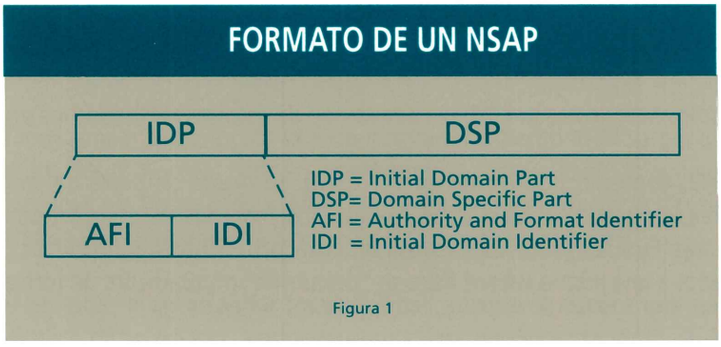


Figura 1

Existen varios tipos de NSAPs. Entre ellos destacaremos dos, que son los que se están utilizando actualmente en CLNP: *ISO-DCC* e *ISO-ICD*. El ISO-DCC (Data Country Code) está pensado para NSAPs asignados geográficamente y, por ello, el IDP incluye un código identificativo de país (por ejemplo, el código correspondiente a España es el 724). El formato ISO-ICD (International Code Designator) se ideó para organizaciones internacionales e incluye en su IDP un código identificativo de organización (por ejemplo, NORDUNET utiliza el 0023).

Actualmente, existen diversos planes de asignación de NSAPs. Entre los más interesantes podemos citar el ideado para Internet, recogido en [rfc1237] y que hace uso del formato ISO-ICD.

Uno de los objetivos del proyecto piloto ISO-IP de RedIRIS es la generación de un plan de asignación de direcciones para la comunidad académica española. El utilizado hasta ahora de forma temporal se ha basado en las recomendaciones de RARE [RARE].

2.3.- Encaminamiento en CLNP

Otra de las novedades que aporta CLNP es su arquitectura de protocolos de encaminamiento. ISO divide el problema del encaminamiento global en varios entornos y

propone soluciones independientes para cada uno de ellos. Esto le permite adaptar el encaminamiento a las características de cada entorno e independizar unos ámbitos de otros.

La división de una interred según ISO es la que aparece reflejada en la figura 2. Existen, en primer lugar, una serie de regiones denominadas *Dominios Administrativos (DA)*, que se corresponden con las distintas organizaciones que encontramos en las redes reales. La característica que marca las fronteras entre DAs es la confianza mutua de puertas adentro y la desconfianza entre distintos DAs.

Los DAs pueden subdividirse en *Dominios de encaminamiento (DE)*. Esta división, a diferencia de la que delimita los DAs, tiene un carácter técnico y su finalidad es doble: jerarquizar el encaminamiento dentro de los DAs, para reducir así la información manejada; y acomodarse a situaciones en las que, por alguna causa, es necesario dividir un DA en varias regiones y tener cierto grado de aislamiento entre ellas (por ejemplo, algunas partes de un DA pueden requerir, por sus características especiales, el uso de protocolos de encaminamiento particulares, distintos de los del resto del dominio).

Por último, los DEs pueden subdividirse en *áreas*, con el objeto de jerarquizar el encaminamiento dentro de ellos y reducir así la información de encaminamiento manejada.

Los protocolos propuestos por ISO para cada uno de estos entornos son los siguientes:

* **ISO 9542**, conocido popularmente por **ES-IS**. Se ocupa de parte del encaminamiento intra-área, en particular, del que se lleva a cabo entre los Sistemas Intermedios (SI ó IS)) y Sistemas Finales (SF ó ES). Es un sencillo protocolo mediante el cual SIs y SFs conectados a una misma subred física se "descubren" mutuamente de forma dinámica, sin

Figura 2

necesidad de intervención manual. ES-IS es un estándar internacional desde el año 88 y existen en la actualidad múltiples implementaciones comerciales de él.

* **ISO 10589**, conocido popularmente por **IS-IS**. Se ocupa de parte del encaminamiento intra-área, el que se realiza entre SIs, y del encaminamiento inter-área. Es un moderno protocolo de encaminamiento basado en un algoritmo de estado de enlaces, lo que le confiere unas propiedades de robusted, rapidez de convergencia y bajo coste. Es muy similar al protocolo OSPF desarrollado recientemente para IP.

  IS-IS es un estándar internacional desde finales de 1991 y ya existen en la actualidad implementaciones de él en los SIs multiprotocolo más difundidos. Sin embargo, y tal como se ha demostrado en las pruebas realizadas en el piloto de RedIRIS, las implementaciones probadas no han alcanzado todavía la madurez suficiente como para ser usadas en redes en producción.

* **ISO 10747**, conocido popularmente por **IDRP** (Inter-Domain Routing Protocol). Se ocupa del encaminamiento entre DAs y entre DEs. Dada la posible "desconfianza" que existe entre diferentes DAs, IDRP incluye mecanismos para garantizar la independencia entre organizaciones y el cumplimiento de las políticas de cada uno de ellos. Por ejemplo, permite definir a un dominio las condiciones que debe cumplir el tráfico en tránsito a través de él, en función del origen, destino, calidad de servicio, etc.

  IDRP es muy similar al protocolo BGP de Internet. De hecho IDRP surgió a partir de BGP. Además, los dos protocolos tienden a converger, y aunque IDRP incluye en la actualidad funciones que no tiene BGP, existe una propuesta de modificación de este último (denominada BGP-4) que tiende a limar las diferencias entre ambos.

  IDRP no es todavía un estándar internacional, aunque se espera que en los próximos meses alcance dicho estado. No existen por ahora implementaciones de él, más allá de los prototipos utilizados para su desarrollo. Para mediados de este año está anunciada la disponibilidad de versiones preliminares de implementaciones comerciales.

La tabla 1 resume los protocolos de encaminamiento propuestos para cada entorno. Una primera lectura sobre ellos puede encontrarse en [Perlman] o en [Tutorials].

IDRP incluye mecanismos para garantizar la independencia entre organizaciones y el cumplimiento de las políticas de cada uno de ellos

PROTOCOLOS DE ENCAMINAMIENTO OSI

Encaminamiento INTER-DOMINIO	Encaminamiento INTER-DAs (IDRP)	
	Encaminamiento INTER-DEs (IDRP)	
Encaminamiento INTRA-DOMINIO	Encaminamiento INTER-AREA (IS-IS)	
	Encaminamiento INTRA-AREA	Entre SFs y SIs (ES-IS)
		Entre SIs (iS-IS)

Tabla 1

El partner de OSI en cada país es la autoridad de registro de NSAP para el formato ISO-DCC

Mencionar, por último, que existe una tendencia actual al desarrollo de protocolos de encaminamiento independientes del protocolo de red al que sirven. En este sentido, hay propuestas firmes de utilización de IS-IS e IDRP para IP, e incluso para otros protocolos de red como AppleTalk e IPX.

3.- Topología de la red CLNS

Siguiendo las recomendaciones elaboradas por el grupo de trabajo cuatro de RARE, se optó por utilizar el formato de direcciones NSAP que utiliza el código de país ISO-DCC (Data Code Country). El AFI en este caso tiene como valor 39, y el código para España es el 724. Este último no se debe confundir con el código de la norma X121, que trata el direccionamiento en X25, cuyo valor es el 214 para España.

El partner de OSI en cada país es la autoridad de registro de NSAP para este formato. Se solicitó a AENOR el prefijo 39.724F.1001 para la red CLNS de RedIRIS.

Fue necesario elaborar una descomposición provisional del espacio de direcciones de RedIRIS para permitir la puesta en marcha de la red. La asignación se realizó tal y como aparece en la tabla 2:

Las 'H' son dígitos hexadecimales. Se crearon dentro del dominio de RedIRIS dos redes identificadas por los siguientes prefijos:

39.724F.1001.0000	***Red Nacional***
39.724F.1001.0001	***Red RICA.***

Inicialmente se instaló un Sistema Intermedio conectado al piloto europeo. Este router constituye el servidor externo del dominio de direcciones de RedIRIS. Esta conexión se realizó con FUNET, red académica de Finlandia, y Switch, red de Suiza, utilizando la infraestructura X25 de EMPB.

ASIGNACION PROVISIONAL DE NSAP.

VALOR	CAMPO	DESCRIPCION
39	AFI	Formato ISO-DCC.
724F	IDI	Código OSI de España con un semiocteto de padding.
1001	DA RedIRIS	Identificador de direcciones registradas para RedIRIS.
HHHH	Red	Identifica una macroorganización o red.
HHHH	Org	Identifica una organización integrada en una red.
HHHH	Dominio	Identifica un dominio de routing dentro de una organización.
HHHH	Area	Identifica un área.
HHHH.HHHH.HHHH	Host	Identificador de sistema.
HH	N-SEL	Selector.

Tabla 2

A finales de Marzo de 1993 se sustituyeron estas conexiones internacionales por otra al servicio CLNS proporcionado por el proveedor EuropaNET.

En los centros participantes se instalaron Sistemas Intermedios y se llevaron a cabo pruebas de routing dinámico utilizando el protocolo propietario de cisco. Estas pruebas se realizaron en coordinación con el proyecto europeo, con el fin de no duplicar esfuerzos. Finalmente y mientras no apareciese el protocolo IDRP, se optó por utilizar routing estático entre diferentes dominios.

Como Sistemas finales se instalaron aplicaciones OSI y DECNET. Tanto estos como los sistemas intermedios y la topología de la red se muestran en la figura 3.

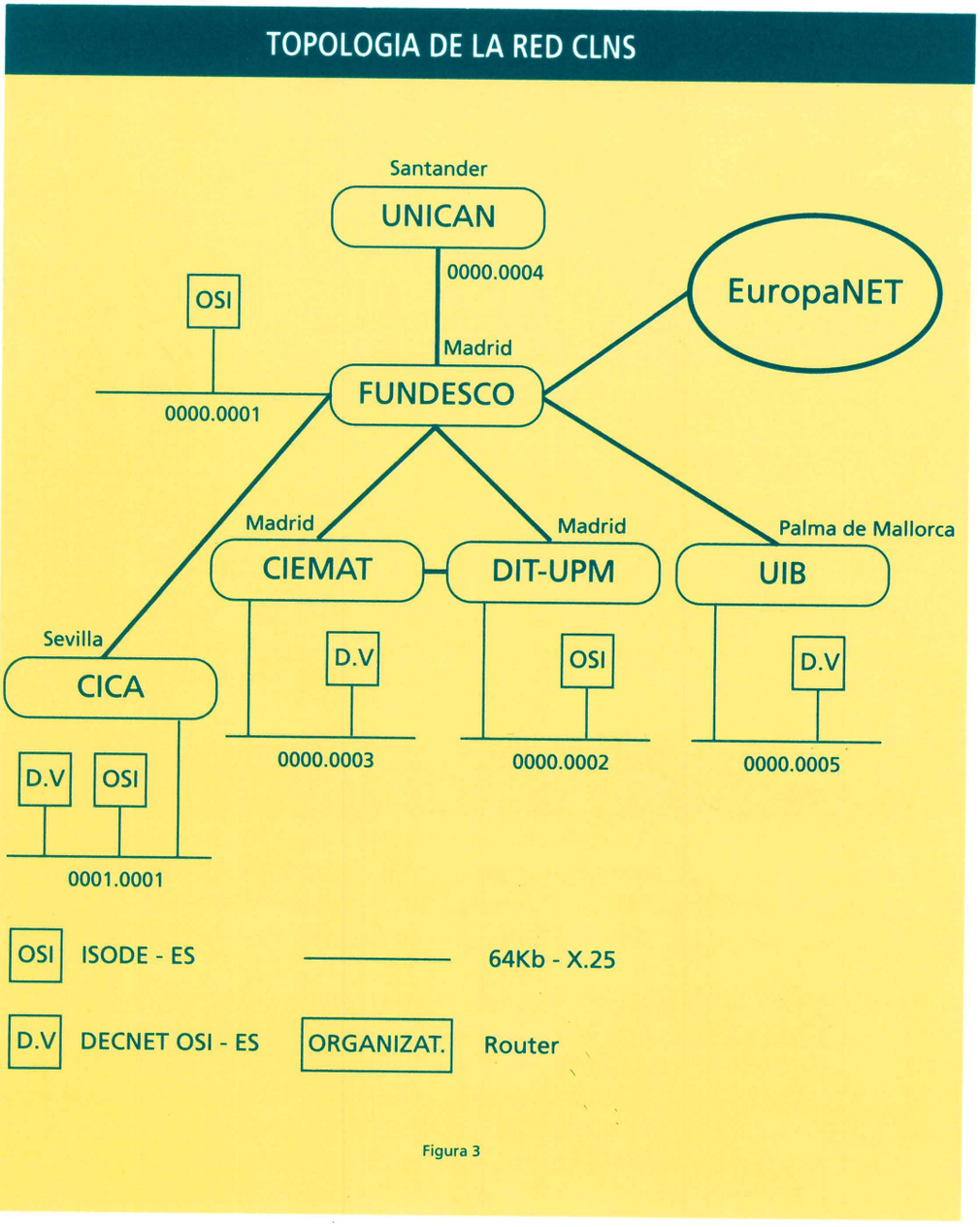


Figura 3

4.- La transición Decnet IV a Decnet/OSI

La migración es la primera y posiblemente por ahora única oportunidad para implantar un estándar internacional (OSI) y sus aplicaciones asociadas

Se conoce por DECnet/OSI (o también DECnet Phase V) la familia de productos DIGITAL que, implementando toda la pila OSI y en particular los protocolos de red ISO-CLNS (ISO 8473, ISO 9542 y DIS 10589), ofrecen soporte de aplicaciones OSI (FTAM, X.400, CMIP, etc) y mantienen la compatibilidad con las aplicaciones existentes de DECnet Phase IV e interoperabilidad con las correspondientes que corren sobre TCP/IP.

La migración es la primera y posiblemente por ahora única oportunidad para implantar un estándar internacional (OSI) y sus aplicaciones asociadas dentro de un contexto de red académica operativa tan compleja y extensa como es HEPnet/SPAN (y su parte española FAECAD). [HEPnet]

La transición de DECnet Fase IV a DECnet OSI es una tarea importante que supone un gran esfuerzo y una gran coordinación por parte de todos los que forman la comunidad DECnet. Esta migración es necesaria y resolverá muchos de los problemas de limitación de espacio que se tienen actualmente en DECnet.

En un proceso como éste están involucradas una gran cantidad de tareas. Unas puramente técnicas que abordan la problemática de la transición de los sistemas individuales y de las subredes (p.e. redes de cada universidad) que configuran una red como FAECAD. Otro grupo de tareas está compuesto fundamentalmente de actividades de gestión y coordinación que armonicen la migración al menor coste posible. Aquí únicamente se va a tratar el primer grupo por actividades, centrándose en la experiencia tenida hasta el momento con los elementos modificados (direccionamiento y routing) y los introducidos nuevos (espacio de nombres DNS).

4.1.- Direccionamiento

Es el primer parámetro a introducir en los nuevos nodos con el software DECNET/OSI. Esta dirección ya no mantiene el formato de 16 bytes sino que introduce el nuevo NSAP de 20 bytes.

El formato definido y aceptado hasta la fecha en la experiencia piloto ISO-CLNS y recomendado por Digital para mantener la conectividad con Fase IV es el que se presenta a continuación:

AFI	IDI	pre-DSP	DSP	sel
39:	724fF	1001:	red:Org:0001:AreaFaseIV:Nodoid:	sel

áreaFaseIV' es el numero de Area en hexadecimal. Las Organizaciones que tengan máquinas DECnet deberán de reservar las Areas en hexadecimal desde 0001 a 0041 (para uso exclusivo de máquinas decnet), que representan el rango de áreas actuales Fase IV 1 a 63.

'Nodoid' o dirección ethernet de la máquina (o también la physical_decnet_address, ya que en realidad se calcula a partir de la dirección decnet Fase IV del nodo), del tipo aa-00-04-00-xx-xx.

Como se aprecia, el prefijo 39.724F es diferente del adoptado como NSAP intermedio por el grupo de coordinación de E-HEPnet, que es 47.0020, lo que implicará, posiblemente, una pérdida de visibilidad inter-fase entre España y el exterior, manteniéndose la conectividad intra-fase y inter-fase dentro de España. En cualquier caso es un problema adicional a resolver.

4.2.- Routing

Para el proyecto de migración se utiliza la infraestructura CLNS de RedIRIS basada en routers CISCO, se aprovecha una de sus facilidades como es la de conversión de direcciones Fase IV a Fase V y viceversa (ésta, actualmente probándose). La actual topología Fase IV de FAECAD, basada fundamentalmente en CISCOs, podrá convivir de forma paralela con la creciente Fase V, hasta que se considere que todos los nodos están integrados y entonces se elimine.

La actual topología Fase IV de FAECAD, podrá convivir de forma paralela con la creciente Fase V, hasta que se considere que todos los nodos están integrados y entonces se elimine

En principio, cada router DECnet Cisco mantendría durante la migración la siguiente configuración:

* Configuración CLNS.
* Dos circuitos: el actual Fase IV , y otro CLNS (Interface Links)
* Tener habilitada la conversión FaseIV-FaseV

Con este esquema se pretende que las Areas Fase IV sean adyacentes al Dominio de Routing de Fase V. Por ahora sólo se han realizado pruebas inter e intra-fase dentro del dominio de routing de España usando como IDP el 39.724F. Queda por probar la conectividad inter e intra-fase con HEPnet y su esquema de direccionamiento (con un IDP propio). Se supone que cuando haya finalizado la migración este espacio de direcciones será trasladado a uno global.

Esta topología se ha estado ensayando con éxito durante los últimos meses entre los Routing Domain del CIEMAT, la UIB y el CICA. Ya que además de la perfecta visibilidad de las máquinas fase IV y fase V se ha montado sobre esta topología una aplicación imprescindible para el funcionamiento de DECNET/OSI como es el DNS.

Todo el routing descrito hasta ahora vía CLNS se hace de forma estática (según las directrices del Proyecto Piloto CLNS RARE/COSINE) estando previsto emplear routing dinámico cuando éste esté disponible en los CISCOS. Están previstas también pruebas con Routers multiprotocolo de DIGITAL (de funcionamiento e interoperabilidad entre DECnis y CISCOS) en el momento en que se disponga de máquinas DECnis.

4.3.- El espacio de nombres (DNS)

La implementación por parte de DEC de los protocolos OSI conlleva un Servicio Distribuido de Nombres, cuya misión es facilitar a los usuarios y/o aplicaciones toda la información que necesitan conocer acerca de un recurso de la red (nodo, impresora, discos, ficheros, etc), sin necesidad de saber la ubicación física de este, sino sólo su nombre. Digital, hasta que implemente un servicio "X500" (estándar de OSI sobre espacio de nombres) para lo cual existe un compromiso en firme por su parte, ha optado por usar su propio DNS (Distribute Namespace Service) con una estructura del tipo de la de Internet.

Digital, hasta que implemente un servicio "X500" para lo cual existe un compromiso en firme por su parte, ha optado por usar su propio DNS (Distribute Namespace Service) con una estructura del tipo de la de Internet.

El DNS de Digital tiene una estructura jerárquica de directorios, que comienza con un directorio raíz (".") del que se ramifican los diversos directorios que contienen los diferentes recursos de la red; asimismo tiene una estructura distribuida, es decir, los objetos (recursos) están almacenados en varias bases de datos (clearinghouses), localizadas en diversos nodos de la red (DNSservers). Estas Clearinghuoses contienen copias (réplicas) de directorios y su contenido, pudiendo éstas ser REPLICA MASTER (se puede modificar) o REPLICA READ_ONLY (no se modifica manualmente, solo de forma automática). Al estar los

En la última reunión del comité técnico de FAECAD se acordó adoptar para España un espacio de Nombres llamado PIVE: (Proyecto Piloto Fase_V España) con una estructura de directorios similar a la de la Internet

directorios replicados y propagándose las actualizaciones de forma automática no hace falta disponer de una política clásica de BACKUP de la información.

En la última reunión del comité técnico de FAECAD para la migración a DECnet/OSI se acordó adoptar para España un espacio de Nombres llamado PIVE: (Proyecto Piloto Fase_V España) con una estructura de directorios similar a la de la Internet, con un primer nivel (root o ".") donde estarían localizadas las CLEARINGHOUSES (debe existir al menos una por cada entidad) y los directorios comunes y los específicos de la migración (DNA_backtranslation, DNA_nodesynonym y dtss_globaltimeservers). Del directorio raíz colgaría el directorio ".ES" que configuraría el segundo nivel de directorios. Y colgando de .ES estaría el tercer nivel de directorios, uno por cada organización (CIEMAT, CICA, UIB, UNICAN, etc...) colgando de cada una de estos estaría la estructura de directorios hijos que cada entidad considere necesaria.

En la actualidad nos encontramos con dos incertidumbres cuando hablamos de DNS, una de ellas es la futura conexión a un Espacio de Nombres internacional (¿OMNI: de hepnet u otro?) que nos lleva a colgar nuestros directorios de ".ES" y no de "." para obtener mayor flexibilidad de migración. La otra es la inexistencia de una autoridad de nombres que crea la incertidumbre de saber si los directorios de las diversas entidades van a colgar directamente de ".ES" o se intercalara otro nivel de directorio entre ".ES" y ."ORGANIZACION" (del tipo de RedIRIS, mensatext, etc).

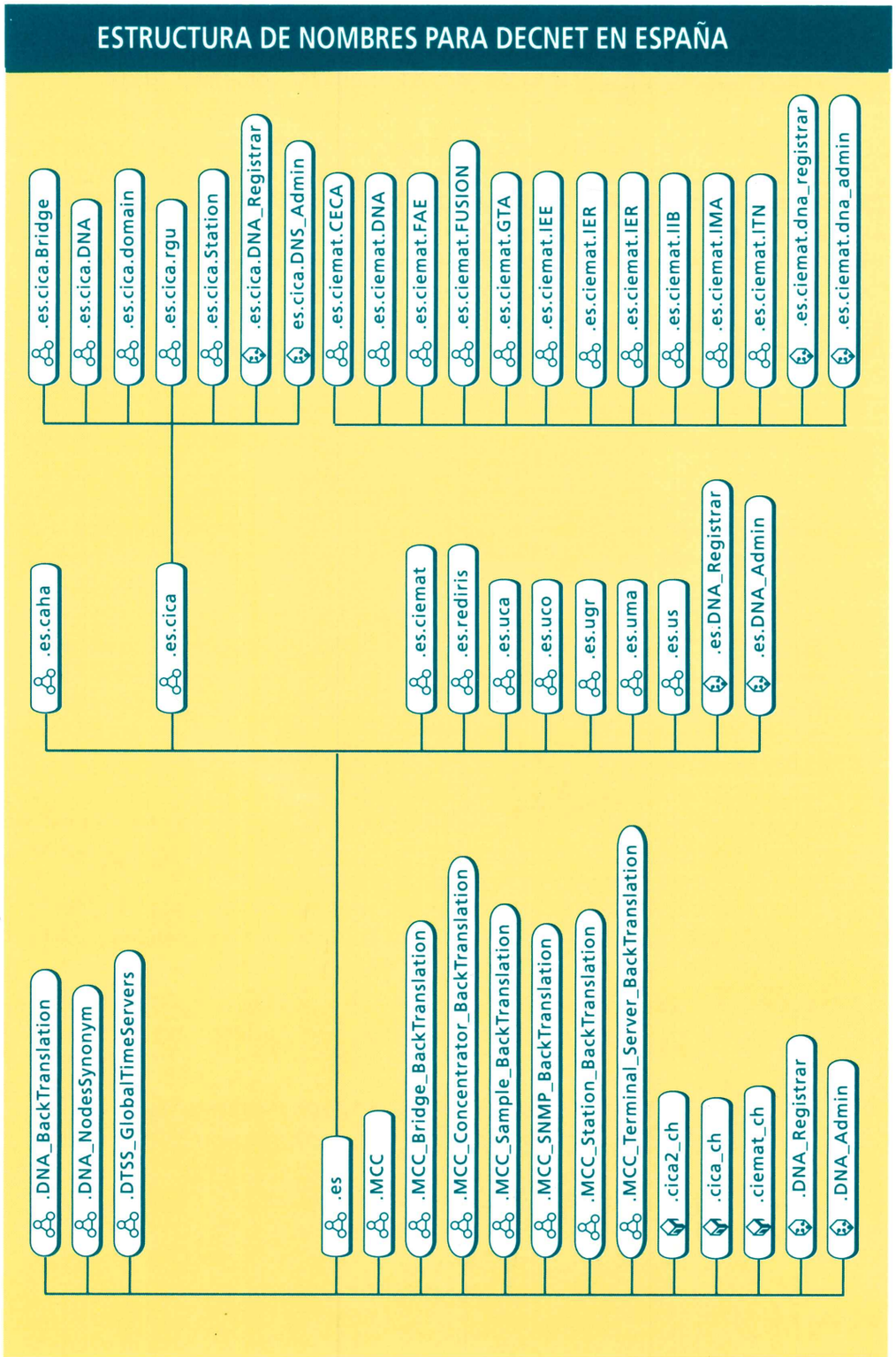
El CIEMAT como Entidad subcontratada por RedIRIS para la gestión de la red académica española basada en protocolos DECnet se hace cargo de la Gestión/operación de este Espacio de Nombres.

Cada uno de los directorios tiene la réplica master localizada en la clearinghouse de su entidad y una o varias réplicas Read_Only localizadas en otras clearinghouses. Los directorios comunes (root, y los directorios que de él cuelgan) tienen la replica master en la clearinghouse del CIEMAT y réplicas de Read_only en otras clearinghouses.

A cada uno de los directorios, y dentro de él a cada uno de los objetos que contiene se le puede asignar un control de acceso independiente con diferentes privilegios para cada usuario. Para facilitar la tarea se crean unos grupos de control de acceso que contienen miembros o usuarios, y es a estos grupos a los que se da los diferentes grados de acceso a los distintos directorios y/o objetos del namespace.

En nuestro espacio de nombres hemos creado dos grupos por cada nivel de directorios (.dns_admin y .dna_registrar , .es.dns_admin y .es.dna_registrar ,y .es.entidad.dns_admin, y .es.entidad.dna_registar); teniendo los miembros de los grupos ".*..DNS_ADMIN" pleno acceso a su directorio y a todos los de nivel inferior y los de los grupos ".*..DNA_REGISTRAR" acceso sólo a los directorios comunes y a los de la de la migración. Por último todo el mundo tiene acceso de READ y TEST para todos los directorios y todos los objetos.

En la actualidad la estructura del namespace PIVE: queda de la forma que muestra el gráfico adjunto, formando un embrión de namespace, al que próximamente se unirán más entidades de forma que podamos ver con qué problemas nos encontramos y que solución les podemos dar. Ya han aparecido algunos problemas con la sincronización horaria (DTSS) de los DNSSERVERs.



Todas las pruebas de DNS han sido realizadas entre la UIB, el CICA y el CIEMAT.

5.- Futuro de Internet. TUBA

Tanto el agotamiento de direcciones clase B como la explosión del número de rutas son problemas que exigen solución a corto plazo

5.1.- Problemas de Internet

El fuerte crecimiento experimentado por Internet en los últimos años es la causa de los principales problemas que la aquejan. Para dar una idea de la magnitud de este crecimiento podemos citar que en apenas 10 años ha pasado de conectar a pocos centenares de máquinas a más de un millón en la actualidad. El número de direcciones asignadas sobrepasa las 100.000 y este número crece exponencialmente (se ha venido duplicando anualmente).

Tres son los problemas básicos que afronta Internet:

* *Agotamiento de las direcciones clase B*. Analizando la evolución de las solicitudes de direcciones clase B en los últimos años, se llega a la conclusión de que, de seguir así al mismo ritmo, en el plazo aproximado de un año las direcciones clase B se habrán agotado.

* *Agotamiento total de la direcciones*. A pesar de que teóricamente el rango de direcciones IP es suficiente para direccionar a más de 4.000 millones de máquinas, la falta de flexibilidad del sistema de clases de direcciones hace que se desperdicien muchas de ellas. Este hecho causará a medio plazo el agotamiento total de las direcciones IP.

* *Explosión del número de rutas manejadas*, debida a la no utilización de encaminamiento jerárquico flexible. Varias veces los nodos de las principales redes de Internet se han visto desbordados por el gran número de rutas que deber manejar (cerca de 8.000 en NSFnet).

La tabla 3 resume el estado actual de asignación de direcciones IP en Internet.

Tanto el agotamiento de direcciones clase B como la explosión del número de rutas son problemas que exigen solución a corto plazo. El agotamiento total de las direcciones, aunque importante, no es tan apremiante como los anteriores.

5.2.- Soluciones Propuestas

Dentro de la comunidad Internet se buscan activamente soluciones a los problemas citados. De ellas, algunas se plantean simplemente como "remedios" a corto plazo, esto es,

DIRECCIONES ASIGNADAS EN INTERNET (MARZO 93)

Clase	Numero Total	Asignadas (%)
A	126	115 (91%)
B	16.383	8.361 (51%)
C	2.097.151	128.709 (6%)

Tabla 3

pequeñas modificaciones que alarguen el tiempo de vida de los esquemas actuales, para ganar tiempo y dedicarlo al desarrollo e implantación de las soluciones a medio/largo plazo.

Entre las soluciones a corto plazo debemos destacar, sin duda, la denominada CIDR [CIDR], que está siendo ya implantada en algunas redes. Propone, entre otras cosas, relajar el concepto de clase de dirección, sustituyéndolo por el de dirección + máscara, y asignar las direcciones de forma jerárquica.

En cuanto a las soluciones a largo plazo, denominadas genéricamente IP versión 7, existen actualmente tres con posibilidades de éxito: SIP, PIP y TUBA. La primera, SIP, propone modificar mínimamente IP para aumentar su campo de direcciones a 64 bits. La segunda, PIP, propone un protocolo de red totalmente nuevo, adaptado a las nuevas redes de alta velocidad y al encaminamiento inter-administrativo (policy routing). Por último, TUBA [TUBA] propone la sustitución del protocolo IP por CLNP en la arquitectura TCP/IP, y sustituir los protocolos de encaminamiento actuales por los nuevos diseñados para CLNP.

En cuanto a las soluciones a largo plazo, denominadas genéricamente IP versión 7, existen actualmente tres con posibilidades de éxito: SIP, PIP y TUBA

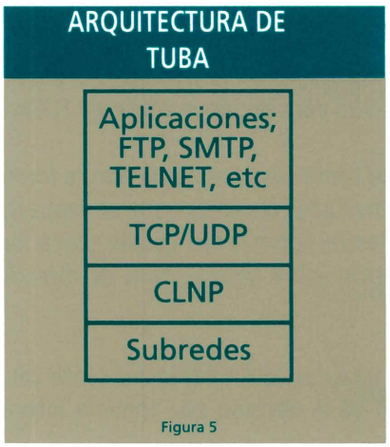


Figura 5

Existe una gran controversia sobre las ventajas e inconvenientes de cada una de las tres propuestas. Una discusión detallada sobre el tema cae fuera del ámbito de este artículo. Citaremos, únicamente, las ventajas que a nuestro juicio hacen de TUBA una de las propuestas con más futuro:

* La utilización de CLNP en Internet supondría un medio de hacer converger tres arquitecturas históricamente distintas: TCP/IP, OSI y DECNET. Este hecho contribuiría a una drástica reducción de la complejidad de gestión de las actuales redes multiprotocolo.

* Existe ya cierta base de equipos y experiencia de manejo de CLNP, adquirida en parte a través de proyectos piloto como éste. La mayoría de los fabricantes con implantación en redes académicas incluyen a CLNP entre su oferta.

Sin embargo, una de las desventajas de TUBA no es de índole técnica, sino administrativa. Parte de la comunidad Internet no ve con buenos ojos la adopción de un estándar perteneciente a ISO, principalmente por la diferencia entre los procedimientos de normalización entre los dos (mucho más dinámicos en Internet). En este sentido, no cabe duda de que la posible adopción de TUBA debe pasar primero por un acercamiento y entre Internet e ISO, históricamente enfrentados.

En RedIRIS la experiencia piloto continuará hasta que ésta se formalice en un servicio a partir de los resultados de ella

Existen en la actualidad varios prototipos de TUBA funcionando sobre ordenadores personales, máquinas UNIX y SIs. En la última reunión del IETF celebrada recientemente se realizó con éxito una demostración de su funcionamiento sobre varias redes de Estados Unidos. En las próximas jornadas JENC 93 a celebrar en mayo en Trondheim está previsto realizar también una demostración de TUBA entre varios sistemas distribuidos por Europa y USA.

6.- Planes futuros

A principios de abril se propuso, mediante un estudio realizado por un Task Force de RARE, una continuación del proyecto 4.1. de COSINE. La propuesta define un nuevo grupo denominado "CLNS coordination Group" que se convertiría en un foro sobre CLNS, donde participarían proveedores de servicios europeos, redes nacionales y grupos de usuarios concretos, que ofrecen o utilizan esta nueva tecnología de red.

Esta propuesta incluye así mismo dos nuevo Task Force, uno para definir una política de routing utilizando el protocolo IDRP y otro para iniciar un piloto de TUBA a nivel europeo.

En RedIRIS la experiencia piloto continuará hasta que ésta se formalice en un servicio a partir de los resultados de ella. Las actividades concretas que se realizarán en los próximos meses se descomponen en aspectos generales sobre la red y sobre aplicaciones usuarias. En el primer caso se realizará una primera versión sobre asignaciones de direcciones destinada a un servicio ampliamente extendido.

Las tareas sobre aplicaciones usuarias se centrarán en continuar las pruebas de migración de DECnet a OSI, y dependiendo de la decisión que tome la Internet sobre IPv7, se iniciaría un piloto nacional de TUBA.

Referencias

[Perlman] Radia Perlman. "Interconnections. Bridges and Routers" Addison-Wesley, 1992.

[Tutorial] Tutorials sobre CLNP, ES-IS, IS-IS e IDRP. Accesibles en chico.rediris.es, directorio isoip/doc.

[rfc1237] R. Colella, E. Gardner y R. Callon. "Guidelines for OSI NSAP Allocation in the Internet". RFC 1237. Julio, 1991.

[RARE] Grupo 4 de RARE. "RARE WG4 Recommendation for NSAP Address Format for National Research Network Organisations". Noviembre, 1990.

[HEPnet] "Usuarios HEPnet. Transicion a DECnet Phase V". Por Angel J. Camacho Rozas. Boletín RedIRIS, num 10-11, Febrero 1991.

[DNSDECnet] " Política de seguridad y control de acceso a los nombres del Namespace (DNS)". Por Diego López del CICA. Documento disponible en el servidor de ficheros de FAECAD. MAILSERV@DEC.CIEMAT.ES (Feb.1993).

[rfc1347] Ross Callon. "TCP and UDP with Bigger Addresses (TUBA). A simple Proposal for Internet Addressing and Routing". RFC 1347. Junio, 1992.

[CIDR] V. Fuller, T. Li, J, Yu y K. Varadham. "Supernetting: an Address Assignment and Aggregation Strategy". RFC 1338. Junio, 1992.

David Fernández
Profesor del Departamento de Ingeniería
y Sistemas Telemáticos
ETSI Telecomunicación de Madrid
dfernandez@dit.upm.es

Celestino Tomás
Coordinador de Proyectos de RedIRIS
celestino.tomas@rediris.es

Grupo de trabajo de DECnet-OSI
Integrado por:
Angel Camacho (Universidad de Cantabria)
David Cuesta (CIEMAT)
Diego López (CICA)
Manuel Martín (CICA)
Antonio Mollinedo (CIEMAT)
Gustavo Rodríguez (CICA)
Jesús Sanz de las Heras (CIEMAT)
Antonio Sola (Universidad Islas Baleares)
isopp@rediris.es

SECTRAS. Un servicio de comunicaciones seguras

Francisco Jordán y Manel Medina

SECTRAS introduce seguridad en la transmisión de datos a nivel de transporte

1.- Introducción

En un boletín anterior [1] se presentaba una introducción general a la seguridad en comunicaciones de datos y se desarrollaba el caso de la seguridad en la aplicación de correo electrónico. En este artículo vamos a centrarnos en otro apartado dentro de la seguridad en comunicaciones, la transmisión o transporte seguro de datos.

Teniendo en cuenta la arquitectura de niveles OSI de ISO, se puede incluir seguridad en cualquiera de sus niveles:

- en el físico o el de enlace, cifrando bits o tramas;
- en los de red o de transporte con protocolos como el TLSP [2];
- en el nivel de presentación, utilizando una sintaxis de transferencia adecuada;
- en el de aplicación usando elementos de servicios de seguridad específicos;
- en cada aplicación en particular, valiéndose de mecanismos de seguridad propios.

En definitiva, existe un abanico de posibilidades teóricas sobre las cuales se investiga y se normaliza, pero sobre las que todavía se está por concretar un marco común a nivel global.

SECTRAS[1] son siglas extraídas de la frase en inglés: **SEC**ure **TRA**nsmission-**TRA**nsport **S**ervice, y da nombre a un conjunto de facilidades y servicios que introducen seguridad en la transmisión de datos a nivel de transporte (nivel 4) en redes de sistemas abiertos. Se ha decidido incluir los servicios de seguridad en este nivel, por ser éste el primero en ofrecer un servicio extremo a extremo, sin intervención de sistemas intermedios, y por tanto independiente del servicio de red empleado.

En el artículo pretendemos proporcionar conceptos generales sobre comunicaciones seguras, a la vez que éstos nos servirán para explicar la arquitectura y funcionalidad de SECTRAS. Empezamos con una presentación de las posibles amenazas que se pueden encontrar en una transmisión de datos así como las contramedidas para combatirlas, enfatizando como ejemplo el caso de sistemas abiertos en Internet. A continuación se introduce la arquitectura y funcionalidad de SECTRAS, pasando después a describir algunas experiencias realizadas con dicha arquitectura. Por último concluimos con un pequeño resumen de todo lo expuesto.

2.- ¿Qué se entiende por comunicación de datos segura?

O planteado de otra forma, ¿Cuándo puede decirse que la comunicación de datos es segura?. Se pueden aplicar varios grados de protección, dependiendo de las amenazas que se quieran combatir. Destacamos a continuación aquellas amenazas causadas explícitamente por terceros, que de forma intencionada pueden afectar a la comunicación, o al funcionamiento normal y correcto de los sistemas implicados en dicha comunicación[2].

1.- SECTRAS es un producto diseñado e implementado por el grupo de seguridad del Dept. de Arquitectura de Computadores de la Universidad Politécnica de Cataluña. Es un trabajo parcialmente subvencionado por la CEE bajo el proyecto COMADOS ESPRIT-2071 y la CICYT-89-0391.

2.- Seguridad engloba además otros tipos de amenazas como desastres, problemas con los sistemas físicos, disponibilidad de la información, rechazo de información recibida o enviada, etc.

1) **Suplantación o mascarada**. Esta amenaza se produce cuando una de las entidades[3] participantes en el intercambio de datos no es quien dice ser, es decir, ha adoptado por completo la identidad de otra. Por ejemplo, en una red de área local, fácilmente una estación de trabajo puede asumir cualquier dirección de red. De forma análoga se puede suplantar el originador de un mensaje de correo electrónico.

   Uno de los agujeros de seguridad más patentes en los servicios ARPA de Internet es la confianza de las máquinas (hosts) entre ellas. Como ejemplo, valga decir que los servicios *rlogin, rsh, rcmp, rcp*, etc. solamente verifican que la petición de servicio provenga de un host autorizado por medio de un fichero (fichero *.rhosts*). El protocolo verifica que la dirección Internet sea la de algún host autorizado, por lo cual, si alguien puede manipular la dirección Internet de una máquina en la red, éste podrá hacerse pasar por cualquier host y por consiguiente entrar en sistemas supuestamente protegidos.

2) **Análisis de tráfico**. Es posible la monitorización y análisis, por un tercero, del intercambio de datos entre entidades, resultando en una amenaza consistente en desvelar información que pueda después ser utilizada en contra de los intercomunicadores. Ejemplos muy claros son: robo de passwords -llevando después a una suplantación-, captura y almacenamiento de datos y posterior procesado de forma que se pueda construir por ejemplo el formato de una transacción bancaria, o revelado de información útil para comerciar después con ella (espionaje industrial, etc). Además, simplemente con el análisis de volumen de tráfico se pueden inferir acontecimientos.

   De nuevo en el caso de servicios Internet como los citados anteriormente la seguridad brilla por su ausencia. Estos servicios utilizan un control de acceso simple, basado en nombre y contraseña, por lo que se exige a los usuarios que acrediten su capacidad para hacer uso de dichos servicios. La paradoja es que después de solicitar la contraseña al usuario sin reflejar ésta en el terminal (otro mecanismo de seguridad más!), el programa la transmite tal cual por la red. Existen numerosos programas (p.e. *etherfind*) cuyo único objetivo es el capturar datos de la red, algunos hasta disponen de filtros para seleccionar el tráfico a conveniencia. No resulta difícil generar la siguiente orden con alguno de estos programas: almacenar en un fichero los paquetes siguientes al que contenga la cadena "Username:" o la cadena "Password:".

3) **Alteración de tráfico**. En este caso la amenaza se encuentra en la inserción, borrado, modificación o contaminación en general de los datos por un tercero. Uno de los ejemplos más claros se encuentra en redes de topología en anillo, en las cuales cualquier estación puede regenerar los datos de forma distinta a como los recibió. Otros ejemplos son: la repetición de una transacción anteriormente realizada, la inserción de un virus en el flujo de datos, etc.

Existen otras amenazas no mencionadas pero son de menor interés respecto a la comunicación de datos.

Una vez identificadas las posibles amenazas, se debe definir una serie de medidas que respondan ante dichas anomalías, esto es, se debe definir una *política de seguridad*. Volviendo

La política de seguridad determina las medidas de protección adoptadas en un sistema

3.- A lo largo del artículo nos referiremos a un usuario humano, a un servicio, al cliente o al servidor de una aplicación como *entidad* en general

La política de seguridad debe adaptarse al resultado del análisis del riesgo de cada sistema

a la pregunta planteada al principio, la respuesta no tiene una solución absoluta, sino que como ya se ha mencionado anteriormente, existen diferentes grados de seguridad que resuelven ciertos niveles de anomalías. Un sistema o la comunicación entre dos de éstos será más segura cuantas más amenazas sea capaz de vencer. La respuesta a las amenazas citadas pasa por la utilización de servicios de seguridad de *autenticación, confidencialidad e integridad* mediante *mecanismos de cifrado privados o públicos* como se describió en [1].

Existen diferentes criterios para la evaluación de políticas de seguridad, y éstos generalmente coinciden con el entorno donde se definen dichos criterios. Por ejemplo, el grado de seguridad apropiado para una organización militar no es el mismo que para una universidad. Existen diversas publicaciones con requisitos e ideas para la evaluación de la seguridad de sistemas, p.e. el ITSEC europeo (Information Technology Security Evaluation Criteria) [3], los libros rojo y naranja del DOD del gobierno de USA [4], etc.

3.- Arquitectura SECTRAS

SECTRAS comenzó como resultado de una primera aproximación a la implementación de un entorno seguro en OSI. Se decidió empezar incluyendo seguridad en la transmisión de datos, adoptando el protocolo de transporte seguro TLSP [2]. El primer prototipo fue desarrollado utilizando ISODE v7.0, que se amplió con TLSP bajo TP0. El TLSP introducía servicios de confidencialidad e integridad basados en mecanismos simétricos, concretamente basado en algoritmos de cifrado DES [5]. Al mismo tiempo, se estaba investigando en la autenticación de entidades siguiendo la norma X.509 [6], así como en la gestión y distribución de claves necesarias para implementar los servicios de cifrado. Dos fueron los acontecimientos que nos hicieron cambiar de dirección: el conocimiento de la existencia de la plataforma de seguridad Kerberos [7] y nuestra participación en el proyecto COMANDOS [8]. A partir de estos momentos los esfuerzos se dirigieron a conseguir servicios de comunicaciones seguras en entornos Internet. Por otro lado, debido a la gran cantidad de sistemas que utilizan los protocolos Internet y a la disponibilidad de una implementación de Kerberos, ésto nos permitió una mayor flexibilidad a la hora de diseñar y crear prototipos.

La estrategia seguida fue la de diseñar e implementar un prototipo que encajara dentro de las especificaciones del proyecto COMANDOS, pero que a la vez fuera lo suficientemente abierto y general como para poder ser utilizado en cualquier aplicación basada en protocolos Internet. El resultado ha sido una arquitectura cuyas principales características son las siguientes:

1) Servicios de autenticación, así como la gestión y distribución de claves basada en Kerberos.

2) Protocolo de comunicación segura TLSP que incluye servicios de confidencialidad e integridad de los datos a transmitir.

3) Tanto Kerberos como el protocolo TLSP se han basado en técnicas de cifrado simétricas utilizando DES.

4) Se ofrecen servicios de seguridad a nivel de transporte en ambas modalidades, orientado a conexión (CONS) y sin conexión (CLNS), esto es, transportes TCP y UDP.

5) Los servicios de transmisión segura se obtienen a partir de un interfaz totalmente análogo al existente para la abstracción socket en UNIX.

A continuación se describen cada una de las partes que constituyen la arquitectura SECTRAS (figura 1). El objetivo de los siguientes apartados no es sólo describir de una manera más o menos profunda la función de cada módulo, sino, además tratar de clarificar cómo se resuelven las amenazas planteadas anteriormente con la presencia de dicha funcionalidad en particular.

SECTRAS se basa en el protocolo de ISO "TLSP" y en ISODE

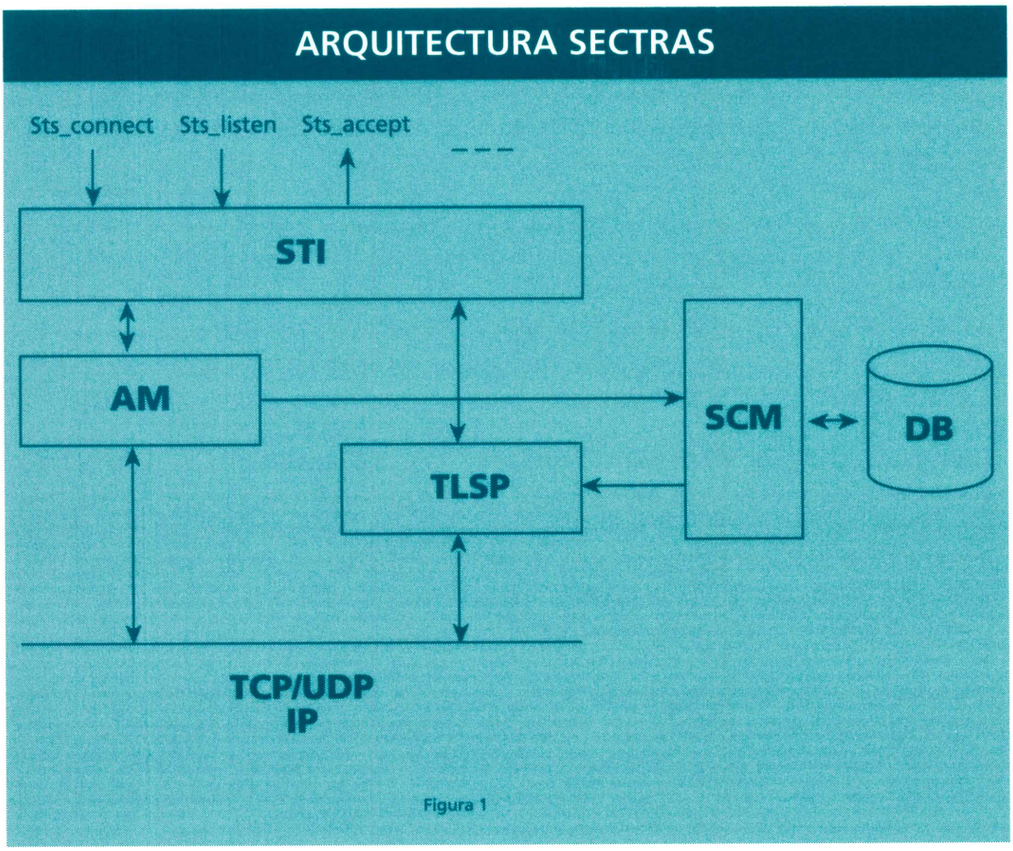


Figura 1

3.1.- Autenticación (AM)

El módulo de autenticación es el responsable de iniciar y controlar el proceso de autenticación entre dos entidades que quieren establecer un entorno seguro para una futura transmisión de datos. En la autenticación se verifican la identidad y los derechos de las entidades implicadas en la comunicación. El proceso de autenticación es necesario si se quiere realizar una comunicación segura.

Dos entidades que quieren comunicarse sobre un canal seguro deberán autenticarse frente a una tercera entidad llamada *servidor de autenticación*. Después de realizarse con éxito la identificación mutua, las entidades entran en una fase de negociación, en la cual se acuerda un *contexto seguro*, aceptado por ambas partes.

De esta forma se elimina el riesgo de suplantación entre entidades, ya que ambas deben corroborar mutuamente su identidad, utilizando para ello el protocolo de autenticación definido e implementado en Kerberos.

La calidad del servicio se acuerda durante la fase de autenticación

3.2.- Gestión de contextos seguros (SCM)

La misión del módulo de gestión de contextos seguros es la de mantener y controlar los contextos negociados durante la autenticación. Se encarga de registrar y borrar los contextos de la base de datos segura, en la cual cada registro corresponde a un contexto diferente.

Un contexto seguro está formado por un conjunto de parámetros y valores que definen una calidad de servicio para el intercambio seguro de datos. Algunos parámetros significativos que forman dicho contexto son: nivel de seguridad, algoritmos de cifrado, claves de cifrado, granularidad de las claves (vigencia y ámbito de aplicación), direcciones (en nuestro caso, direcciones de transporte) de las entidades implicadas, etc.

La información almacenada en un contexto seguro es utilizada durante todo el período de validez de éste, para construir las unidades de protocolo de transporte seguras. El período de validez se define en la autenticación y durante este tiempo las entidades pueden utilizar el contexto para intercambiar datos sin necesidad de una nueva autenticación.

3.3.- Protocolo de comunicación seguro (TLSP)

El módulo de protocolo de comunicación seguro se encarga de convertir las unidades de datos de protocolo de transporte (TPDUs) generadas por el nivel de transporte, a unidades de datos de protocolo de transporte seguras (STPDUs) antes de enviarlas al servicio de red. Este módulo implementa el protocolo seguro de nivel de transporte (TLSP), que define un subnivel justo debajo del de transporte. El protocolo TLSP soporta los dos modos de operación de la red, esto es, orientado a conexión (CONS) y sin conexión (CLNS).

El protocolo implementado introduce servicios de confidencialidad e integridad en el intercambio de datos, pero la seguridad introducida por medio de este protocolo depende exclusivamente de la correcta gestión del entorno seguro (gestión de claves, protección de los contextos, etc). En nuestro caso, la gestión del entorno seguro es llevada a cabo por el módulo de autenticación apoyado por el módulo de gestión de contextos.

La inclusión del TLSP en los protocolos de Internet rompe de hecho la filosofía de dicho protocolo ya que éste debería situarse por debajo del nivel de transporte. Podríamos justificar esto diciendo que hemos implementado una extensión del TLSP, con el fin de poder integrarlo de una manera sencilla en los computadores que proporcionan servicios Internet a nivel de sistema operativo.

3.4.- Interfaz de transporte seguro (STI)

El módulo de interfaz de transporte seguro define un conjunto de rutinas que ofrecen un servicio de transporte seguro, además del servicio de transporte básico. Este es el único punto de acceso al servicio por parte de los usuarios, en realidad, dicho módulo construye una librería de funciones que encapsula toda la complejidad de la arquitectura SECTRAS en un conjunto de llamadas a sistema totalmente análogas a las tradicionales de UNIX (connect, write, read, send, recv, sendto, recvfrom, close, etc) para la abstracción socket del servicio de transporte de Internet (TCP y UDP).

La realización de un interfaz igual al que ya se disponía supone una gran ventaja en cuanto a la migración de una aplicación que no disponía de servicios de seguridad, a la misma aplicación

incluyendo servicios seguridad. Básicamente, el esfuerzo para realizar tal migración es el de montar la aplicación original (si se dispone de programas fuentes u objetos) con la librería de SECTRAS.

El acceso SECTRAS se realiza con un interfaz equivalente al del servicio de transporte de UNIX

4.- Funcionalidad SECTRAS

La calidad del servicio de comunicaciones seguras depende directamente del *nivel de seguridad*, el cual viene determinado por la política de seguridad adoptada. Pero, hay que mencionar que, independientemente del nivel de seguridad escogido, quien determina la base y el carácter del entorno seguro es el proceso de autenticación, como ya se ha mencionado anteriormente. Por eso, las técnicas privada o pública para la autenticación constituyen dos plataformas de entornos seguros marcadamente diferentes.

4.1.- Niveles de seguridad

El nivel de seguridad en SECTRAS es un valor definido entre 0 y 3 (este rango no es original sino que se encuentra definido en el modelo arquitectónico de referencia de ISO para OSI [9], en TLSP,...). Cada uno de estos niveles define una política de seguridad diferente a aplicar en el entorno donde se incluya. Dichas políticas son:

1) Nivel 0. No se aplican servicios de seguridad, esto es, la comunicación transcurre sin ningún tipo de protección.

2) Nivel 1. Se aplican servicios de autenticación y confidencialidad. Los datos se transmiten encriptados combatiendo de esta forma las amenazas de mascarada y análisis de tráfico.

3) Nivel 2. Se aplican servicios de autenticación e integridad. Los datos se transmiten en claro (en su forma originar, sin cifrar) añadiendo un código de integridad criptográfico combatiendo de esta forma las amenazas de mascarada (gracias a la autenticación) y alteración de tráfico.

4) Nivel 3. Se aplican ambos niveles 1 y 2. De esta forma se combaten todas las amenazas descritas de mascarada, análisis y alteración de tráfico.

Es razonable pensar que a mayor nivel de seguridad, se obtiene mayor protección, pero a la vez, se está bajando el rendimiento del sistema, ya que parte de los recursos se dedican a implementar la política de seguridad definida.

4.2.- Kerberos como servidor de autenticación

SECTRAS utiliza Kerberos como servicio de autenticación. Se utilizan servicios de Kerberos para implementar el servidor de autenticación y para la generación y distribución de claves incluidas en los contextos seguros.

Kerberos es un servicio de autenticación basado en técnicas privadas e implementado en el MIT (Massachusetts Institute of Technology). Es utilizado básicamente para la protección de las contraseñas transmitidas por redes Internet. El modelo de autenticación se basa en la confianza en un tercero (el servidor de Kerberos) y en el concepto de ticket (contiene información cuya lectura sería: a utilizar por.., válido para.., durante...). Los usuarios reconocidos por Kerberos

Como servidor de autenticación y de claves se usa Kerberos

dispondrán de un ticket personal que a su vez podrán utilizar para obtener otros tickets para la utilización de servicios. De esta forma, el acceso a cualquier servicio protegido de la red por parte de los usuarios está supervisado directamente por Kerberos.

La implementación de Kerberos está realizada para sistemas operativos BSD y para redes con protocolos Internet (utiliza UDP para la comunicación con el servidor de autenticación). Kerberos está disponible de forma pública e incluye servicios ARPA como *rlogin, rsh, rcmd, ftp,* etc. extendidos con seguridad.

4.3.- Interacción entre entidades

En la figura 2 se muestra la interacción básica entre entidades cuando se realiza una comunicación segura. La entidad que inicia la comunicación (entidad A) debe primero identificarse ante el servidor de autenticación (Kerberos) y solicitar un ticket para utilizarlo en la autenticación ante la entidad B. El servidor de autenticación verifica la identidad de A y si está autorizado genera y entrega un ticket para el propio para A y un ticket de servicio para B. A partir de estos momentos la entidad A dispone de credenciales para comunicarse con B, entonces, en el momento que quiera podrá iniciar la comunicación con B presentándole el ticket de servicio. La entidad B antes de aceptar o rechazar la comunicación deberá identificarse ante el servidor de autenticación y conseguir un ticket propio, con éste podrá verificar el entregado por A y actuar en consecuencia. En el caso de autenticación mutua, B incluye parte del ticket de servicio modificado en la respuesta (sólo si se trata de B, ha podido descifrar el ticket y modificarlo correctamente). Por lo tanto, sólo si ambas entidades disponen de las credenciales correctas podrá iniciarse la comunicación de datos.

Una vez realizada la autenticación, del ticket de servicio B se extrae la información que completa el contexto seguro para esta comunicación, por ejemplo, el ticket contiene una clave temporal DES generada por Kerberos, llamada clave de sesión, y que sólo conocen las

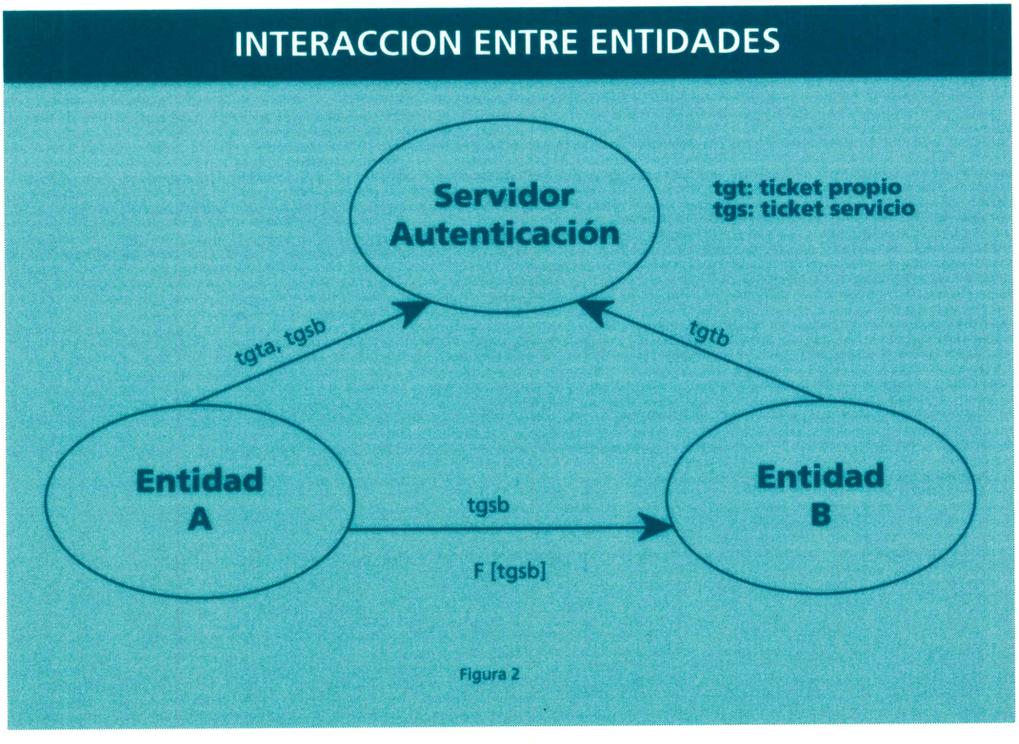


Figura 2

entidades involucradas en la comunicación. De esta forma se pueden implementar los servicios de confidencialidad e integridad.

En la figura 2 aparece el caso más general en el cual las tres entidades involucradas residen en tres sistemas (máquinas) diferentes. Generalmente sólo existe un servidor de autenticación por dominio de seguridad (que suele coincidir con la red local) y reside en una máquina protegida físicamente, en cambio, pueden existir numerosas entidades solicitando servicios de autenticación a lo largo de la red, residiendo en máquinas diferentes o en el mismo sistema.

Hay que hacer notar que la descripción realizada de la interacción entre las entidades, y en particular, la descripción del funcionamiento de Kerberos mediante tickets, se ha hecho de una forma muy general y resumida. Para más información se recomienda la lectura de [7].

La sobrecarga introducida por SECTRAS en el sistema se reduce, prácticamente, al tiempo de cifrado en DES

5.- Experiencias realizadas

Como se ha mencionado, SECTRAS es resultado en parte del proyecto COMANDOS de ESPRIT. COMANDOS es una plataforma de sistema operativo distribuido orientada a objetos, en la cual existe un subconjunto que implementa comunicaciones seguras entre núcleos y objetos en general del sistema operativo. El módulo de comunicaciones seguras se implementa utilizando SECTRAS (en COMANDOS se le denominó STS, Secure Transmission Subsystem). Una aplicación interesante fue la implementación de un servicio de procedimientos remotos (RPCs) seguro utilizando el transporte seguro proporcionado por SECTRAS.

SECTRAS permitirá el intercambio confidencial e íntegro de datos a partir de la segunda mitad de 1993

A nivel interno, se han diseñado e implementado aplicaciones seguras como ejemplo de utilización del sistema, y a la vez se han realizado medidas de funcionamiento y sobrecarga por la inclusión de los servicios de seguridad. En resumen, las medidas nos permitieron concluir que casi la totalidad de sobrecarga introducida es debida a las rutinas de encriptación (DES) ya que éstas se encuentran implementadas por programa.

6.- Conclusiones

A lo largo del artículo hemos realizado una descripción de posibles amenazas que podemos encontrar en una comunicación de datos y hemos particularizado éstas para el caso de protocolos Internet en entornos de sistemas abiertos. La principal conclusión es que podemos combatir los problemas de seguridad mediante la utilización de servicios de autenticación, confidencialidad e integridad.

Se ha desarrollado una arquitectura que incorpora los elementos de seguridad necesarios para contrarrestar las amenazas descritas en la comunicación de datos. Al mismo tiempo se ha intentado explicar en pocas palabras cual es la funcionalidad de dicha arquitectura.

Por último decir que en estos momentos existe una versión beta de SECTRAS para sistemas operativos SunOs (Sun3 y Sun4) y Ultrix (Mips) que incluye parte de Kerberos, un kit de desarrollo de aplicaciones seguras, un conjunto de ejemplos de implementaciones y documentación de usuario, instalación y referencia. Nuestra intención es la de hacer pública la versión 1.1 a principios del mes de Junio de este año.

Referencias

[1] Seguridad en Correo Electrónico. Francisco Jordán, Manel Medina y Enric Peig. Boletín de RedIRIS nº 22. Marzo de 1993.

[2] ISO/IEC DIS-10736. (JTC1/SC6 N-6779). Information Technology - Telecomunications an Information exchange between systems - Open System Interconnection - Transport Layer Security Protocol. 1991/11/21.

[3] Information technology Security Evaluation Criteria. Harmonized criteria. Ver. 1.1. 1991/01/10.

[4] Truested Computer System Criteria (The Orange Book) USA Dept. of Defense (DoD).

[5] DES. Data Encrytion Algorithm.

[6] CCITT Blue Book Fasc. VIII, Recommendations X.500 to X.509 (Authentication Framework).

[7] J.G.Stein, C.Newman & J.L.Schiller. "Kerberos: An Authentication Service for Open Network Systems". USENIX Conference Proceedings. Dallas (USA). Winter 1988. pp. 203-211.

[8] V.J. Achilles, R.Palter, N.Harris, X.Russet (Editors). "The COMANDOS Distributed Applications Platform" Sprinter-Verlag. 1993.

[9] ISO-7498-DAD/2: ISO Open Systems Interconnection Reference Model. Addendum 2 on security.

Francisco Jordán
Universidad Politécnica de Cataluña
Departamento de Arquitectura de Computadores
jordan@ac.upc.es,

Manel Medina
Universidad Politécnica de Cataluña
Departamento de Arquitectura de Computadores
medina@ac.upc.es

CONVOCATORIAS

Redes de Información 93: " Utilizando la red"

Londres-Gran Bretaña
18-20 mayo 1993

Organizada por Meckler, Tecnología de Gestión de Información, en asociación con UKOLN, la Oficina para Redes de Información y Bibliotecas.

Esta primera conferencia y exhibición anual que tendrá lugar en Londres (Earl´s Court Park Inn) va dirigida a todos aquellos miembros de la comunidad académica y bibliotecaria que en la actualidad utilizan redes de área extensa o que estudian las posibilidades de las redes para sus organizaciones.

PROGRAMA

* Entrega de documentos
* Redes para la investigación académica e industrial
* Redes para la gestión de bibliotecas
* Redes de uso comunitario y recreativo
* Redes para el campo educativo
* Redes para editores
* Teletrabajo
* Redes - El futuro próximo

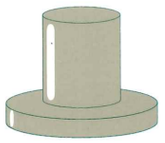
además de seminarios específicos sobre temas básicos tales como protocolos y estándares y servicio de información.

Para mayor información :

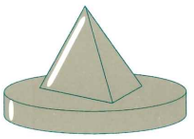
Meckler
Artillery House, Artillery Row,
London SW1P 1RT
Tel.: +44 71 976 04 50
Fax: +44 71 976 05 06

Redes de Información 93: " Utilizando la red"

1993 IEEE Symposium on Research in Security and Privacy



ECT 93



Super-computación Vectorial y Paralela, 93

1993 IEEE Symposium on Research in Security and Privacy

Claremont Resort
Oakland - California
24-26 mayo

No existe posibilidad de inscribirse mediante correo electrónico.

Para mayor información :

TRW Defense System Group,
One Space Park,
Redondo Beach,
CA 90278

El programa preliminar está disponible de forma electrónica en la Secretaría de RARE <raresec@rare.nl>

3rd International Forum on Electronic Communication Technology for the 90´s

Moscú - Rusia
27 junio-2 julio

Juri Gornostaev o
Juri Andrianov
ECT 93 Programme Committee
EMail: enir@ccic.icsti.msk.su

Supercomputación Vectorial y Paralela, 93

C.I.E.M.A.T
Madrid-España
10-14 mayo

Está reconocido como curso de doctorado por la Universidad Politécnica de Madrid.

PRESENTACION Y OBJETIVOS

El desarrollo de los diversos tipos de Superordenadores, ha hecho factible el tratamiento de sistemas extremadamente complejos. (Predicción Atmósferica, Estructura Molecular, etc.) que hasta hace poco tiempo resultaban numéricamente inabordables si se deseaba analizarlos con un mínimo realismo.

Sin embargo, el aprovechamiento real de las capacidades de los ordenadores vectoriales y paralelos no es, en absoluto, trivial. Un análisis cuidadoso de las técnicas de programación es fundamental para la obtención de las prestaciones esperadas, cuya magnitud ha abierto nuevas perspectivas para el conocimiento científico.

PROGRAMA:

- Introducción
- Arquitecturas de super-computadores
- Programación paralela
- Programación vectorial
- FORTRAN 90
- Manipulación de datos
- Aplicaciones en:
  - Predicción atmósferica
  - Elementos finitos
  - Fusión
  - Simulación de redes neuronales
  - Química.
- Proyección futura

MAS INFORMACION:

Instituto de Estudios de la Energía.
Avda. Complutense, 22
28040 MADRID
Tfno.: (91) 3466365
Telefax: (91) 3466005
SUPERCOM@DEC.CIEMAT.ES

Fundesco