



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

Índice Tema 9

1. La red Internet: arquitectura de red.
2. Principios de funcionamiento.
3. Servicios: evolución, estado actual y tendencias.
 - 3.1. Correo electrónico (e-mail).
 - 3.2. Transferencia de ficheros (FTP).
 - 3.3. Emulación de terminal (Telnet),.
 - 3.4. Foros temáticos (News).
 - 3.5. Gopher.
 - 3.6. Wais.
 - 3.7. World Wide Web (WWW).
 - 3.8. URL (Universal Resource Locator).
 - 3.9. Visualizadores o navegadores.
 - 3.10. Servidores.
 - 3.11. HTML (HyperText Markup Language).
 - 3.12. Escritura de documentos HTML.
 - 3.13. IRC y servicios de conferencia en tiempo real.
 - 3.14. Herramientas para propósitos específicos.
 - 3.15. Bases de datos y publicaciones.

2

3

4

5



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

TEMA 9

La red Internet: arquitectura de red. Principios de funcionamiento. Servicios: evolución, estado actual y tendencias.

1. LA RED INTERNET: ARQUITECTURA DE RED.

Contrariamente a la creencia popular, internet no es una red única ni nueva, sino miles de redes interconectadas por un conjunto común de protocolos, herramientas y servicios. Hace ya más de veinte años que empezó a instancias del DoD (Departamento de Defensa americano) como motor para desarrollar un modo suficientemente robusto para interconectar ordenadores que garantizara que pudieran ser accesibles en caso de un conflicto con potencias enemigas (red ARPANet). Inicialmente sobre esta red estaban conectados contratistas del DoD, instalaciones militares, universidades y laboratorios federales. Este diseño inicial, que incorpora numerosas conexiones redundantes, es la base de la Internet actual.

Desde la perspectiva de la posibilidad de comunicarse con cualquier otro en la Red, Internet aparece como una red única, y que no está administrada por una única autoridad, sino por muchas autoridades de redes públicas y privadas. El uso de Internet ha crecido exponencialmente en años recientes y aún lo continúa haciendo, principalmente desde que apareció el servicio World Wide Web. Hasta la fecha, se considera que el número de sistemas conectados a la Red se dobla cada año.

• ARQUITECTURA DE RED.

La naturaleza descentralizada de Internet hace necesario que existan órganos de coordinación que administren los recursos comunes y marquen la dirección que ha de seguir la red para hacer frente a los retos impuestos por su crecimiento y la constante evolución tecnológica.

Con este fin se creó en 1992 la Internet Society (ISOC), sociedad que está abierta a usuarios, novedades, fabricantes de equipos e instituciones gubernamentales. La ISOC dispone de una serie de órganos con distintas responsabilidades:

- IAB (Internet Architecture Board), encargado de determinar las necesidades técnicas a medio y largo plazo y de la toma de decisiones sobre la orientación tecnológica de Internet.
- IETF (Internet Engineering Task Force) e IRTF (Internet Research Task Force) que sirven de foros de discusión y trabajo sobre los diversos aspectos técnicos y de investigación que afectan a Internet, respectivamente.
- IESG (Internet Engineering Steering Group) e IRSG (Internet Research Steering Group), coordinan los trabajos del IETF y del IRTF, respectivamente.
- IANA (Internet Assigned Number Authority), responsable último de los diversos recursos asignables de Internet.

Hay que destacar que la topología de Internet es desconocida y cambiante, ya que en cualquier momento, una nueva organización puede poner a la disposición de la red de redes su red interna, que a partir de ese instante pasaría a formar parte de Internet. Del mismo modo, otras organizaciones pueden desconectarse, si lo desean, de Internet.

En cuanto a la gestión, cada grupo conectado a Internet es el encargado de gestionar y mantener sus propios recursos. Se puede decir que Internet se gestiona sola. Si una conexión falla, no es posible acceder a los servicios ofrecidos por las máquinas que dependan exclusivamente de dicha conexión, pero el resto de nodos de la red continuará siendo accesible. Esto se explica debido a su descentralización y a que la idea original de Internet era la de que siguiera funcionando ante la eventualidad de la destrucción de alguna de sus partes. Cuando la conexión se recupera, todos los servicios vuelven a estar operativos automáticamente.

Existen tres entidades principales dentro de todo el entramado Internet: usuarios, PSI o Proveedores de Servicio Internet y carriers o portadores. Dentro de la categoría de usuarios se pueden englobar todos los agentes (usuarios domésticos o empresas) que acceden a Internet en busca de un determinado servicio, bien para comunicar con otros u obtener o publicar información.

Los PSI ofrecen conexión a Internet, contratando líneas de alta capacidad o ancho de banda hacia los distintos nodos de Internet. Estas líneas son contratadas a compañías denominadas carriers o portadoras, que son compañías encargadas de ofrecer servicio de tránsito hasta los nodos principales de Internet. Las empresas que basan su negocio en ofrecer servicio de conexión a Internet han proliferado bastante. Concretamente en España existen cientos de proveedores a través de los cuales se puede obtener acceso a Internet.

Para contratar un servicio de conexión a Internet es necesario pagar una tarifa, cuya cuantía dependerá de la modalidad de acceso que se desee utilizar. Algunas instituciones públicas tienen, por otro lado, derecho a conectarse gratuitamente como es el caso de las Universidades y Centros de Investigación españoles, a través de RedIris.

En cuanto a los medios físicos de conexión a Internet, se puede realizar de formas muy diversas. Las más comunes son las siguientes:

- Conexión mediante línea telefónica (RTB). Una línea de teléfono permite, en función del modem utilizado, alcanzar velocidades de hasta 33.600 bps. Actualmente los modems incorporan chips que se conocen como x2 y que llegan a alcanzar velocidades de 56 Kbits por segundo. Sin embargo los modems x2 plantean dos dificultades: sólo se puede realizar una comunica-

ción a esta velocidad entre el proveedor y el usuario, nunca entre dos modems de 56Kb, y esta velocidad sólo se consigue en uno de los extremos, en la recepción.

- Conexión mediante RDSI (Red Digital de Servicios Integrados). Este tipo de línea digital ofrece un gran ancho de banda además de una serie de servicios suplementarios gracias a sus características. Existen dos tipos de líneas RDSI; el primero es el conocido como acceso básico. Consta de dos canales de datos de 64 Kbits cada uno (128 Kbits en total) llamados canales B y uno de control de 16 Kbits llamado D. Este tipo de líneas son también conocidas como 2B + D. El segundo tipo es el conocido como acceso primario, que consta de 30 canales de datos de 64 Kbits (unos 2 Mbits) y de uno de señalización de 64 Kbits.
- Conexión mediante una línea de datos dedicada de tipo ATM, Frame Relay o Punto a Punto. Estos dos tipos de líneas proporcionan conexión permanente a Internet y permiten una velocidad de transmisión muy superior a las anteriores.

Según datos históricos compilados por MIDS, consultora de Austin, Texas, existen del orden de 160 millones de usuarios de Internet en el mundo, servidos por más de 30 millones de sistemas.

Tal crecimiento no era esperado por la industria y de ser ciertas las previsiones, la tecnología actual es insuficiente para tal demanda. Por esta razón existen actualmente diversos foros en los que se están definiendo nuevos estándares, como por ejemplo IPv6, que permitirá direccionar un número de direcciones IP tal que en un metro cuadrado del planeta tierra puedan existir 1564 direcciones diferentes.

Internet está estructurada según un modelo cliente-servidor. Por un lado, el usuario ejecuta una aplicación en el ordenador local: el programa cliente. Este programa se encarga de ponerse en contacto con el ordenador remoto, para solicitar la información deseada. A su vez, el ordenador remoto responde al programa cliente a través de otro programa que es capaz de proveer la información solicitada. Este programa es el programa servidor. Los términos cliente-servidor se extienden también a los ordenadores donde son ejecutados dichos programas.

La arquitectura de la WWW se basa en el mismo modelo cliente-servidor. Los clientes presentan la información en formato hipertexto y para ello usan el lenguaje HTML cuyas características se verán más adelante. Además los clientes llevan implementados varios protocolos tales como FTP, etc. Cuando, en la WWW, un cliente hace una consulta a un servidor FTP, los directorios se ven como objetos hipertexto. A los clientes de WWW se les suele denominar navegadores o Browsers.

Para comunicarse en el WWW, además de integrar estos protocolos, los clientes añaden uno nuevo, el HTTP (HyperText Transfer Protocol), que es el protocolo nativo entre los servidores WWW y los clientes. Éste es un protocolo muy simple implantado sobre TCP/IP y es similar en muchas funcionalidades al protocolo Gopher. El cliente HTTP envía al servidor un identificador de documento con o sin palabras de búsqueda y el servidor responde con documentos hipertexto o simplemente texto. HTTP es un protocolo que no mantiene una conexión permanente.

En la WWW es importante que las herramientas de navegación (clientes) que se usen sean aquellas que permitan acceder a los distintos servicios de una forma homogénea. Para hacer esto posible, es necesario que exista una forma unificada de identificar los distintos recursos. Es decir, es necesario disponer de una forma de escribir direcciones de servidores, que contengan toda la información necesaria para poder hacer uso del servicio solicitado.

Esto se realiza por medio del URL (Uniform Resource Locator). A través de los URL's se da toda la información necesaria para acceder a los distintos recursos, por lo que hacen el papel de direcciones de los servicios Internet. Se puede decir que el URL es el camino que tendría que seguir un usuario para encontrar un fichero en Internet.

La estructura básica de un URL es la siguiente:

protocolo_de_acceso://nombre_del_ordenador/ruta_de_acceso

Así, por ejemplo, para acceder a la página web del BOE, debería usarse el siguiente URL en el navegador correspondiente:

<http://www.boe.es>

con lo que se accedería a la página principal.

Por lo visto hasta este punto, podría decirse que la WWW es un sistema hipermedia mundial de intercambio de información y recursos informáticos, utilizando, como vínculo, los documentos de hipertexto.

Como ya se ha comentado, para establecer la comunicación entre clientes y servidores en la WWW se hace uso del protocolo HTTP. De cara a acceder a los servidores de WWW y visualizar documentos de hipertexto, es necesario disponer de un programa cliente capaz de comunicarse con dichos servidores. Estos programas se llaman navegadores (Browsers en la jerga de Internet).

Un navegador es una aplicación que permite visualizar páginas hipertexto en un ordenador. Además suelen tener la capacidad de acceder a otros protocolos y servicios de Internet como el E-mail, FTP, etc. Es por ello que, mediante un navegador, se puede acceder a la mayoría de los servicios de Internet a través de una sola aplicación y con un procedimiento unificado.

Existen actualmente en el mercado varios navegadores disponibles. Los más extendidos en la actualidad son el Communicator de Netscape y el Internet Explorer de Microsoft. Además llevan una serie de funcionalidades extra que amplían las capacidades de las páginas de la Web y que se comentan más adelante.

2. PRINCIPIOS DE FUNCIONAMIENTO.

La tecnología básica sobre la que se ha desarrollado Internet es el conjunto o familia de protocolos TCP/IP. Algunos de estos protocolos proporcionan funciones de bajo nivel necesarias para muchas aplicaciones, como es el caso de IP, TCP y UDP que se verán algo más en detalle con posterioridad. Otros protocolos de la familia TCP/IP son específicos para tareas tales como transferencia de ficheros, envío de correo electrónico, encontrar quién está conectado a otro ordenador, obtener información de gestión de sistemas y dispositivos, conectarse a un ordenador remoto, etc.

Bajo el nombre de familia de protocolos TCP/IP, se engloban no solamente protocolos del nivel de transporte y red (Transmission Control Protocol e Internet Protocol) sino también protocolos a nivel de aplicación como telnet, ftp, smtp, etc.

TCP/IP es un conjunto de protocolos en capas. Para comprender lo que esto significa, consideremos un ejemplo de envío de correo electrónico. Existe un protocolo (SMTP, Simple Mail Transfer Protocol) que especifica cómo se compone un mensaje, cómo especificar el destinatario y qué comandos se intercambian dos sistemas para que el mensaje se transfiera de un sistema a otro. Por debajo de este protocolo, TCP (Transmission Control Protocol) es responsable de que los comandos lleguen al otro extremo, para lo cual realiza una traza de lo que se envía y lo retransmite si no llega a destino. Si el mensaje es muy grande, lo «trocea» en datagramas y asegura que lleguen correctamente.

De un modo análogo, TCP se apoya en los servicios proporcionados por una capa inferior (IP, Internet Protocol) y que no solamente pueden ser llamados por TCP sino por otros protocolos.

Generalmente las aplicaciones TCP/IP utilizan cuatro capas:

- Capa de protocolos de aplicación (como SMTP por ejemplo).
- Un protocolo como TCP que garantiza que los datagramas lleguen correctamente.
- IP, que proporciona el servicio de que los datagramas lleguen a destino.
- Una serie de protocolos para manejar el medio físico, tal como Ethernet o una línea Punto a Punto.

El nivel IP TCP/IP está basado en el «modelo catenet», que asume que existe un gran número de redes independientes conectadas entre sí mediante pasarelas. Los datagramas pasan de una red a otra a través de las pasarelas antes de llegar a su destino final y de un modo transparente para los usuarios. Éstos solamente necesitan conocer la «Dirección Internet» del destino. Actualmente esta dirección está representada por 32 bits agrupados de ocho en ocho formando 4 octetos (lo que se conoce como IPv4), como por ejemplo 195.47.35.24 y que es única en toda la red Internet, de modo análogo a como un número telefónico es único en toda la red telefónica.

Las direcciones IPv4 especifican de un modo unívoco una red y un sistema en esa red, por lo que contienen una parte de «dirección de red» y otra de «sistema en esa red». La forma no es siempre la misma. El número de bits para expresar la red y los sistemas dependen de qué clase de red se trate. Hay varias Clases de Redes, (Clases A, B, C, D, E), siendo las más comunes las Clases A, B y C. Según el número de bits que ocupe la «parte de red» y «la parte de host»:

CLASE	RANGO DE DIRECCIONES	PARTE DE RED	PARTE DE HOST
A	0.0.0.0-127.0.0	1 byte	3 bytes
B	128.0.0 191.255.0.0	2 bytes	2 bytes
C	192.0.0.0 223.255.255.0	3 bytes	1 byte
D y E	224.0.0.0 255.255.255.0	Especial reservadas multicast	

Examinando los primeros bits de una dirección, el software de IP determina rápidamente la «clase de red» y por tanto, su estructura.

El número de redes posibles, por tanto, es:

Clase A: 128

Clase B: $64 * 256 = 16.128$

Clase C: $32 * 256 * 2 = 2.097.152$

Y en cuanto al número de hosts por red:

Clase A: $256 * 3 = 16.777.216$

Clase B: $256 * 2 = 65.536$

Clase C: 256

Ahora bien, los usuarios se refieren normalmente a los sistemas por un nombre en lugar de una dirección, por lo que existen servicios que traducen nombres a direcciones y viceversa (DNS, Domain Name Services).

TCP/IP es un protocolo «sin conexión». Cuando un mensaje se «trocea» en datagramas, éstos se envían a través de la red y pueden llegar a destino por caminos diferentes. Al final, todos los datagramas son re-ensamblados en un mensaje. Cuando los datagramas están en tránsito, la red no sabe que hay conexiones entre ellos. Puede ocurrir que el datagrama 325 llegue antes que el 12 por ejemplo, e inclusive que alguno no llegue, en cuyo caso se retransmitirá.

A veces se confunden datagrama y paquete. Técnicamente la palabra correcta al referirse a TCP/IP es datagrama, como unidad de datos con la que trata un protocolo. Un paquete es algo físico que aparece en una red Ethernet o algún cable. En la mayor parte de los casos, un paquete contiene simplemente un datagrama, por lo que hay poca diferencia, aunque a veces un datagrama se tiene que descomponer en varios paquetes, como ocurre en el caso de TCP/IP sobre X.25. Cuando un mensaje se «trocea» en datagramas, TCP pone en cada trozo una cabecera con la siguiente información:

- Puerto de origen y puerto destino.
- Número de secuencia.
- Datos de comprobación del datagrama (checksum).
- Datos.

Cada uno de estos datagramas es pasado a la capa inferior (IP) que a su vez le añade más cabeceras a cada datagrama, conteniendo como información fundamental y más importante:

- Dirección Internet del origen del datagrama.
- Dirección Internet del destino del datagrama.

- Datos de comprobación del datagrama (checksum).
- Datos de «time to live» que se decrementa cada vez que el datagrama pasa por un sistema. Cuando llega a cero, el datagrama se pierde.

Con la información que hasta ahora acarrea el datagrama, sería suficiente para llegar a destino si todos los ordenadores estuvieran conectados físicamente. Como los medios físicos de interconexión son múltiples, para que se pueda entregar el datagrama hay que añadir información del medio físico.

Actualmente la mayor parte de las redes utilizan Ethernet, que tiene su propio modo de direccionamiento físico. A los datagramas habrá que añadirles la información de Ethernet.

Los diseñadores de Ethernet lo hicieron pensando en que no existiesen dos máquinas con una dirección Ethernet igual, para lo cual ésta viene de fábrica incluida en los controladores de red. Se reservaron 48 bits para la dirección Ethernet, y se asignaron a los fabricantes por una autoridad que controlaba que eran únicas.

El datagrama se encapsula con cabeceras Ethernet de origen y destino y con datos de comprobación (checksum) y se entrega a la red. Nótese que no existe conexión entre direcciones IP y direcciones Internet. Cada máquina tiene una tabla de qué direcciones Ethernet corresponden a cada dirección Internet y viceversa. Además de las direcciones Ethernet, la cabecera del datagrama lleva un campo de 32 bit con el código de tipo, que se utiliza para permitir que el medio físico pueda ser utilizado por otros protocolos distintos de TCP/IP.

Hasta ahora hemos visto cómo un flujo de datos se divide en datagramas, se le añaden cabeceras y se entrega al ordenador remoto, donde ocurre el proceso inverso y reconstruye el flujo de datos. Se necesita algo más para poder realizar algo útil. Tiene que haber un modo de abrir una conexión en un ordenador remoto, conectarse, decir qué fichero queremos, controlar la transmisión del mismo, etc. Esto lo realizan los protocolos de aplicación que corren por encima de TCP/IP, que solamente se encargan de los detalles de red.

Para arrancar un proceso en el sistema remoto se necesita algo más que la dirección IP. En cada sistema remoto existen procesos de aplicación que están «escuchando» peticiones de la red en «puertos» específicos, iguales en todos los sistemas y conocidos como los «well known services» o wks. Estos puertos para cada protocolo de nivel de aplicación tienen números específicos, como por ejemplo SMTP usa el puerto 25, FTP el 21 y 23, HTTP el 80, etc.

Con lo visto hasta ahora podemos ver que una conexión queda descrita por cuatro números:

- Las direcciones Internet de cada extremo (que van en las cabeceras IP).
- Los puertos de aplicación (que van en la cabecera TCP).

Hay muchas situaciones en que la información a transmitir cabe en un solo datagrama, como cuando se pide una resolución de un nombre a dirección IP y viceversa. Resulta «pesado» usar los mecanismos de TCP de desagregación/agregación de datagramas. En este caso se ha definido otro protocolo (UDP, User Datagram Protocol) que no incluye información de secuencia de datagrama. Los datagramas UDP se ensamblan de modo análogo a los TCP, se envían a IP, que añade las cabeceras IP con un número de protocolo UDP que también son «well known ports». En consecuencia las cabeceras UDP son mas cortas que las cabeceras TCP. Adicionalmente existe otro protocolo destinado al propio software TCP/IP en lugar de

a las aplicaciones. Es el ICMP (Internet Control Message Protocol), utilizado para mensajes de error, etc. Es similar a UDP, pero aún mas corto y simple ya que no existen «puertos» o «servicios» «well known».

• **EL PROBLEMA DEL DIRECCIONAMIENTO EN INTERNET: IPV6.**

Como ya se ha comentado anteriormente, para direccionamiento se escogieron inicialmente 32 bits, que se suponía que permitiría el direccionamiento de un número prácticamente inalcanzable -en aquel tiempo de sistemas interconectados, dando lugar al direccionamiento que se conoce como IPv4 (Internet Protocol Version 4). Tras el gran crecimiento experimentado por Internet se ha visto que estas direcciones podrían agotarse con rapidez, por lo que se ha desarrollado un nuevo direccionamiento que empieza a ser utilizado -aunque no se encuentra totalmente definido formalmente-, IPv6 (Internet Protocol version 6), permitiendo que sobre la red puedan coexistir ambos tipos de direccionamiento durante un período de transición. Las características más importantes de este protocolo son:

- a) Cabecera: de doble longitud que en IPv4. Para reducir el coste de procesar los datagramas y la anchura de banda necesaria para transmitirlos, se ha reestructurado el formato de la misma, que contiene los siguientes campos:

VERSION	PRIORITY	FLOW LABEL	
PAYLOAD LENGTH		NEXT HEADER	HOP LIMIT
SOURCE ADDRESS			
DESTINATION ADDRESS			

- b) Versión campo de 4-bit que contiene la versión del Internet Protocol.
- c) Prioridad campo de 4-bit que permite a una fuente determinar la prioridad de entrega del datagrama y que puede tomar los valores:

- 0 – Tráfico sin caracterizar.
- 1 – Tráfico tipo «netnews».
- 2 – Tráfico desatendido como e-mail.
- 3 – reservado.
- 4 – Tráfico de transferencia masivo como FTP.
- 5 – reservado.
- 6 – Tráfico interactivo, como telnet.
- 7 – Tráfico de control como SNMP.

Los valores 8 a 16 se utilizan multimedia (vídeo y sonido) para especificar prioridad de tráfico.

- d) Etiqueta de flujo, campo de 24-bit para indicar que se requiere una secuencia de datagramas para ser manejada de modo especial por los enrutadores, como en vídeo en tiempo real.
- e) Longitud de la carga útil, campo de 16 bit que define la longitud del paquete que sigue a la cabecera. IPv6 especifica que la carga pueda ser de 536 octetos, pudiendo llegar hasta 65.535 octetos en enlaces limitados. Si se tienen que enviar paquetes de mayor tamaño que los que permiten el enlace, puede utilizarse una Cabecera de Fragmentación (8 octetos) y fragmentar el paquete, que será reensamblado en destino. Otra cabecera, la Hop by Hop Header es la opción de carga de alta capacidad (Jumbo Payload) que puede usarse si los paquetes tienen que ser mayores de 65.535 octetos.
- f) Siguiente cabecera, campo de 8 bit que identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6, como por ejemplo una cabecera TCP, Cabecera de Enrutamiento o Fragmentación (o combinación de ellas).

Hop Limits, campo de 8 bit que se decrementa cuando el datagrama atraviesa un nodo. Si llega a cero, se descarta el datagrama.

- g) Dirección Origen de 128 bit de quien envía el datagrama.
- h) Dirección Destino de 128 bit.
- i) Direccionamiento:

IPv6 tiene tres tipos de direccionamiento:

- Unicast para una única interfaz de red.
- Anycast para una única interfaz del grupo de interfaces disponibles.
- Multicast para un grupo de interfaces. Los datagramas se entregan a todas las interfaces de un grupo.

Para evitar la experiencia habida con IPv4 (32 bit de direccionamiento), IPv6 usa 128 bit, con lo que se pueden direccionar 2^{128} interfaces o conjuntos de interfaces de red. El esquema de direccionamiento no está definido formalmente todavía, pero podría ser algo como:

<proveedor><organizacion ><red><interfaz>

con 32 bits para cada apartado.

Por tanto, el espacio de direcciones utilizable sería significativamente más pequeño que 2^{128} . Estudios realizados demuestran que con este esquema de direccionamiento podrían existir entre $8 \cdot 10^{17}$ y $2 \cdot 10^{33}$ nodos. Utilizando la estimación menor, por cada metro cuadrado de la Tierra existirían 1564 direcciones disponibles, existiendo direcciones suficientes para el futuro lejano, cuando además de ordenadores existan televisores, webfonos, etc.

- j) Enrutamiento: no difiere mucho del de IPv4 excepto en el tamaño de las direcciones (128 bit), por lo que los algoritmos de enrutado existentes funcionarán con IPv6, aunque se añaden nuevas capacidades de enrutado potentes como:

- Selección de proveedor basado en rendimientos, política de acceso, etc.
- Movilidad.
- Auto Redireccionamiento a una nueva dirección.

k) Seguridad. La autenticación y Encapsulado pueden usarse por separado o en combinación.

l) IPv6 Cabecera de autenticación.

Proporciona autenticación e integridad y no incluye confidencialidad, puesto que los datagramas IPv6 no son encriptados. Está propuesto el algoritmo MD5 para autenticación extremo a extremo, previniendo el «spoofing» o enmascaramiento de direcciones IP.

m) IPv6 Cabecera de Encapsulación de Seguridad.

Proporciona integridad y confidencialidad a los datagramas IPv6 de un modo independiente del cifrado. Por razones de interoperabilidad en Internet se está utilizando el algoritmo DES CBC. Se permite encriptar todo el datagrama o solamente la carga útil del mismo.

n) Transición de IPv4 a IPv6.

IPv6 se ha diseñado de modo que puedan interoperar sistemas IPv4 e IPv6 con una transición no traumática:

- Actualización incremental e implantación de enrutadores.
- Dependencias de actualización mínimas. La única limitación es que se actualiza primero el DNS (Domain Name Service).
- No necesidad de cambio del plan de direccionamiento existente en cada instalación. Los sistemas y enrutadores pueden seguir usando las direcciones IPv4.
- Bajo coste de arranque, los mecanismos de transición a IPv6 son:
 1. La estructura de direccionamiento IPv6 lleva embebidas las direcciones IPv4 y codifica otra información requerida para la transición.
 2. Técnica de encapsulación de paquetes IPv6 packets dentro de cabeceras IPv4 para transportar los datagramas a través de enrutadores y segmentos no actualizados a IPv6.
 3. Técnica de traducción de cabeceras que permite una eventual introducción de topologías de enrutamiento solamente de tráfico IPv6.

• DOMINIOS, RESOLUCIÓN DE NOMBRES.

Para alcanzar un sistema remoto hemos visto que se precisa solamente la dirección IP y que ésta es única en toda la red Internet. Pero resulta más cómodo usar nombres en lugar de números, para lo cual existen servicios de conversión de direcciones IP a nombres y viceversa (DNS, Domain Name Service). Si la red fuera pequeña, bastaría que existiera en cada máquina una base de datos -análoga a una guía telefónica que correlacionara nombres y direcciones-. Como esto es impracticable hoy en día

por el número de nodos existentes, se han creado una serie de nodos en la red que contienen información de otros nodos. Para hacerlo más manejable, se han agrupado los nodos en distintas categorías, creando una arborescencia de nodos o «dominios» de nodos. Los nodos de primer nivel son:

SÍMBOLO	DOMINIO	INSTITUCIÓN	UBICACIÓN
COM	Dominio Comercial	Network Solutions, Inc.	Herndon VA USA
EDU	Dominio Educación	Network Solutions, Inc.	Herndon VA USA
GOV	Dominio Gubernamental	Network Solutions, Inc.	Herndon VA USA
INT	Dominio internacional	ARPA/CSTO	Arlington VA USA
MIL	Dominio Militar	DDN Network Information Center	Chantilly VA USA
NET	Dominio de redes	Network Solutions, Inc.	Herndon VA USA
ORG	Dominio de organizaciones	Network Solutions, Inc.	Herndon VA USA
XX	Dominios globales de cada país. XX es el código de país	Institución NIC de cada país	

A su vez, «colgando» de estos nodos o «dominios primarios» existen otros nodos y subdominios.

Cuando un sistema trata de buscar una dirección, se desencadenan una serie de preguntas mediante datagramas UDP a los nodos por encima del que realiza la búsqueda, hasta que se encuentra el sistema que resuelve la dirección.

Este esquema lleva aparejado un sofisticado método de mantenimiento de las bases de datos del DNS (Domain Name Service) en Internet, de un modo distribuido. Adicionalmente, en los registros del DNS no solamente se guarda información sobre la dirección IP de los sistemas, sino sobre alias de máquinas, registros que indican cómo entregar correo electrónico a un dominio determinado, etc. Se comprende pues que este mecanismo es básico para el funcionamiento correcto de la red y que gracias a la jerarquización y delegaciones de gestión de los distintos dominios, resulte imposible la conexión indiscriminada de sistemas a la red, ya que si no se dispone de un «dominio registrado» y por tanto de direcciones IP «legales», la conexión es imposible.

Hasta 1995, el registro de un dominio era gratuito, solamente se requería cumplimentar unos formularios que se encontraban en la misma red. Desde entonces, InterNIC requiere una cuota anual mínima por el mantenimiento de los datos administrativos (del orden de 10.000 ptas./año).

• ENRUTAMIENTO EN INTERNET.

Con lo visto hasta ahora ya sabemos cómo encontrar un nodo en la red (DNS), cómo comunicar con él (mecanismos de TCP/IP) y nos queda comprender cómo los datagramas se trasiegan de una red a otra ya que Internet es una red de redes. Este «trasiego» es el enrutamiento.

IP asume que el sistema está conectado a una red local. Si el destino está en la misma red local, no hay problema en entregar el datagrama. Pero si el sistema pertenece a otra red, deben poder encaminarse los datagramas a la red destino mediante equipamiento al efecto. Este tipo de equipos se conocen como enrutadores (routers).

Un enrutador tiene dos interfaces al menos, cada una con una red diferente. La visión que podemos tener ahora de Internet es la de una serie de redes unidas entre sí mediante enrutadores.

Cuando un sistema trata de enviar un datagrama, primero comprueba -por su dirección IP-, si el sistema destino está en la misma red. Si es así, lo envía directamente. Si no es así, lo envía al enrutador. Sabe que lo debe entregar al enrutador gracias a que tiene definida una «ruta» por defecto, que es la que utiliza cuando no sabe cómo entregar el datagrama.

De este modo, se delega el enrutamiento en el enrutador, que debe mantener «tablas» de rutas a cada red. Puesto que resulta impensable que un enrutador conozca todas las rutas a todas las redes de Internet, utilizan el mismo esquema de «ruta por defecto» para ir encaminando el datagrama a través de la red.

También entre los enrutadores se intercambia información de las tablas de enrutamiento, mediante diferentes protocolos. Algunos de éstos son OSPF (Open Shortest Path First), propietario, y RIP (Routing Information Protocol) o EGP (External Gateway Protocol) estándares de Internet.

3. SERVICIOS: EVOLUCIÓN, ESTADO ACTUAL Y TENDENCIAS.

Una vez que ya conocemos el funcionamiento de la red Internet, vamos a comentar algunos de los servicios que se ofrecen en la misma:

3.1. CORREO ELECTRÓNICO (E-MAIL).

Casi con toda probabilidad es el servicio de mayor difusión y uso en la Red. La gran ventaja del correo electrónico de Internet reside en su difusión a nivel mundial. Se trata de un correo basado en el protocolo SMTP (Simple Mail Transfer Protocol), que forma parte del perfil de protocolos TCP/IP. Permite el intercambio de mensajes con cualquier usuario del planeta que esté conectado a Internet.

El correo electrónico gira alrededor del concepto de «dirección de correo». Esta dirección debe proveer toda la información necesaria para permitir la entrega del mensaje a cualquier parte del mundo. El destinatario no tiene por qué ser necesariamente una persona, sino que podría ser un servidor de ficheros, una lista de distribución, un mensáfono, un teléfono GSM, etc.

Las direcciones de correo utilizan el formato Internet: destinatario@sistema-donde-reside, en donde el símbolo @ (at) separa al destinatario y al sistema donde reside el destinatario.

El sistema donde reside el destinatario debe ser un nombre de dominio totalmente cualificado (FQDN, Fully Qualified Domain Name) según hemos visto en el apartado correspondiente a la resolución de nombres en Internet, como por ejemplo carro.mma.es, que es el sistema «carro», del dominio de segundo nivel «mma» que a su vez está en el dominio de primer nivel «es» de España.

Para enviar/recibir correo, el usuario debe utilizar en su puesto de trabajo un «agente de correo» o Agente de Usuario (UA) que intercambia los mensajes con un Agente de Transferencia de Mensajes (MTA) que despacha el correo.

Este MTA, a su vez, intercambia los mensajes con otros MTA en destino mediante el protocolo SMTP (Simple Mail Transfer Protocol).

Entre el UA y el sistema en que reside el MTA la comunicación se realiza con protocolos POP3 (Post Office Protocol v3) o IMAP (Internet Mail Agent Protocol) o si el UA y MTA están en el mismo sistema, con programas específicos como «mail» en el mundo Unix.

Veamos qué ocurre cuando un usuario envía un correo a pperez@cea.mma.com, por ejemplo.

En primer lugar el mensaje se transfiere por el UA al sistema donde reside el MTA y es «capturado» para proceder a despacharlo. El MTA pregunta a la red mediante el sistema de resolución de nombres (DNS), quién sabe cómo entregar correo al sistema cea.mma.com y si este sistema y dominio existen, recibirá un datagrama UDP con la dirección IP del sistema remoto, sacada de un registro tipo MX (Mail eXchanger) de la base de datos de DNS.

Llegados a este punto se establece una comunicación entre los agentes MTA origen y destino con el protocolo SMTP en uno de los Well Known Services en el puerto 25, asignado a SMTP y tiene lugar la transferencia.

Una vez en el sistema destino, el MTA remoto chequea que sabe cómo entregar al usuario a quien iba destinado el mensaje (pperez), porque tenga cuenta de correo y lo deja en espera de ser consultado por el destinatario en cualquier momento. No es necesario que el usuario esté conectado en ese momento, sino que basta con que tenga «cuenta de correo». De no existir el destinatario, el mensaje es devuelto al originador.

Por tanto, debe asumirse que si el mensaje no ha sido devuelto, ha llegado a destino, se ha entregado aunque no se pueda saber si el destinatario lo ha leído o no, que es un hecho diferente.

Para compartir correo entre usuarios con intereses comunes existen las listas de correo (mailing lists) que aparecen con una única dirección de correo. Cuando se dirige un correo a esa única dirección, el sistema replica el correo a todos los usuarios que pertenecen a la lista de correo.

Asociado al sistema de correo existen sistemas de gestión automática de listas de correo conocidos como «listservs», uno de los conocidos es el «Majordomo». Uno puede dirigirse a un usuario específico para suscribirse a listas de correo, darse de baja, pedir información, etc. El «listserv» responde a un conjunto de comandos de usuario como: suscribe, Unsubscribe, list, etc.

En todos los sistemas de correo existe un usuario especial, el Postmaster o responsable del sistema de correo, los Agentes de Correo de usuario (UAs) pueden ser programas específicos (como Eudora, de dominio público) o bien vienen incluidos con navegadores de la red (p. ej., Netscape Communicator).

3.2. TRANSFERENCIA DE FICHEROS (FTP).

Este servicio FTP (File Transfer Protocol) permite al usuario la transferencia de ficheros entre nodos de la red Internet. El nombre del protocolo y el nombre del programa que lo implementa generalmente se llaman igual, ftp.

Asumiendo que existen los permisos convenientes, es posible transferir ficheros entre Nueva Zelanda y Madrid por ejemplo, a una velocidad razonable.

Generalmente se requiere tener «cuenta» en el sistema al que se quiere acceder, aunque puede estar habilitado un servicio FTP Anónimo, que permite a cualquier usuario acceder a los ficheros existentes en un área especial del sistema. De este modo, se pueden poner ficheros a disposición del público en general sin tener cuentas específicas.

El proceso para conectarse a un servicio ftp anónimo es introducir la palabra «anonymous» cuando el sistema remoto solicita el nombre y la dirección de correo electrónico cuando solicita la password. Esto último no es estrictamente necesario, pero se considera una cortesía de las que habitualmente existen en la red (Netiquette).

Cuando un usuario desea conectarse a un servidor ftp, normalmente invoca el protocolo con: ftp algunsitio.dominio, como por ejemplo, ftp cea.mma.es para invocar el servicio ftp del servidor cea del dominio mma.es. Una vez conectado, el sistema remoto solicita que se introduzca nombre de usuario y password (que podrían ser las que el usuario tuviera asignadas o bien anonymous y la dirección de e-mail).

Tras la validación, se entra en modo de diálogo y existen una serie de comandos para ver el directorio de ficheros y moverse por él (is, dir, cd, etc.), transferir (get, put, mget, mput) o, para cambiar envío de datos ASCII o datos binarios (bin, ascii), y de finalización de la sesión (be).

Dada la enorme dimensión de la Red, resulta difícil saber dónde encontrar un fichero y su contenido temático. Para paliar esta carencia se ha desarrollado por la McGill University de Canadá el sistema Archie: este sistema permite realizar búsquedas de ficheros por la red, manteniendo un enorme índice que correlaciona los nombres de ficheros con breves descripciones de su utilidad y contenido (base de datos whatis), así como su localización.

El servicio Archie está accesible a través de sesiones interactivas con Telnet (que veremos posteriormente), peticiones desde correo electrónico, línea de comandos y clientes X-Terminal, etc. El servicio FTP utiliza dos puertos wks (Well Known Services), el 20 para transferencia de datos y el 21 para control de la transferencia, mediante datagramas tcp en ambos puertos.

3.3. EMULACIÓN DE TERMINAL (TELNET).

Es el principal protocolo de Internet para establecer conexiones remotas con cualquier ordenador de la red Internet, como si de un terminal local se tratara. El usuario está en un ordenador trabajando con otro ordenador que puede estar situado a miles de kilómetros de distancia y con una conexión libre de errores. En esencia, se consigue el efecto de simular que el teclado y la pantalla del usuario están físicamente conectados a ese ordenador remoto.

Cuando un usuario desea conectarse con una sesión Telnet a un servidor remoto, normalmente invoca el protocolo con:

telnet algunsitio.dominio

como por ejemplo, «telnet cea.mma.es» para invocar el servicio Telnet del servidor cea del dominio mma.es. Una vez conectado, el sistema remoto solicita que se introduzca nombre de usuario y password. Al contrario que con el servicio FTP, no existe la posibilidad de usuario anonymous.

El puerto por defecto para el servicio Telnet es el 23 (también wks), con datagramas TCP aunque en cada instalación puede haber otros puertos asignados para conexiones directas a otros servicios.

3.4. FOROS TEMÁTICOS (NEWS).

Existen multitud de Foros especializados o «newsgroups» como son más comúnmente conocidos, en temas tan variados como lo permite el saber humano.

En esencia se trata de un sistema que permite la difusión masiva de información a los usuarios que se suscriben voluntariamente a un «foro» temático, resultando en un sistema que actúa como punto de encuentro con otros usuarios para compartir opiniones sobre el tema en cuestión, aportando ideas, opiniones, preguntas o respuestas, a preguntas de otros usuarios.

El sistema de news puede verse como un sistema de organización automática de correo electrónico temático. Cuando un usuario se suscribe a un foro de news, recibe todos los mensajes que otros suscriptores han enviado al foro temático, pudiendo responder a ellos bien a todo el «foro» -por tanto a todos los suscriptores-, o bien al autor de uno de los mensajes.

Existe la figura de moderador del foro, que en última instancia realiza un control de lo que se difunde o no, para prevenir actitudes no deseables en la «armonía» de la red. Este esquema hace que los sistemas de news requieren gran cantidad de almacenamiento masivo ya que crecen exponencialmente. Basta imaginarse el gran trasiego de información que puede ocurrir con los mas de 20.000 foros temáticos «oficiales» en la red Internet (Usenet News).

Cualquier persona puede provocar una votación en la red para que se incluya un «foro de news» o «newsgroup» entre los foros oficiales. Para ello hay que seguir los procedimientos conocidos como RFDs (Request For Discussions), poniendo en el foro «news.announce.newgroups» la propuesta. Después de un período de discusión, que es obligado y de que el foro se desea, por la «comunidad» se ha acordado un nombre y se ha determinado si el foro será moderado o no y por quién, se lanza un procedimiento CFV (Call For Votes) enviando un mensaje o «posteando» un mensaje en el foro «news.announce.newsgroup».

La palabra «postear» se utiliza como derivada de la inglesa «post», poner una noticia en un determinado foro temático, aunque una vez más sea incorrecta desde el punto de vista de la Real Academia de la Lengua en esta acepción.

El período de votación suele estar entre 21 y 31 días. El voto es individualizado para cada propuesta, no existe el voto «global» para un área temática. Además el voto debe ser explícito con frases como: «Yo voto a favor del grupo xxxx.yyy.zzzz tal y como ha sido propuesto» o «Yo voto en contra del grupo xxx.yyy.zzzz tal y como ha sido propuesto». Una vez recontados los votos, el «newsgroup» puede crearse si existen al menos 100 votos más a favor que en contra (margen de 100 votos) o al menos 2/3 del total de votos emitidos son a favor de la creación.

Si falla la Propuesta, el proceso puede recomenzar tras un período de «enfriamiento» de seis meses. Si tras un par de intentos resulta obvio que la «comunidad» no considera de interés la creación del grupo, el proponente debe aceptar la opinión de la mayoría y desistir de la creación del grupo.

La comunicación de news entre los distintos servidores se realiza con el protocolo NNTP (Network News Transfer Protocol), con un wks 119 y datagramas TCP, de un modo totalmente cooperativo.

Las news están organizadas en una estructura arbórea, llamadas jerarquías.

Hay siete categorías principales:

- «comp». Tópicos de interés para profesionales de la computación, amantes de los ordenadores, ciencias de la computación, hardware y software.
- «sci» Tópicos sobre la Ciencia.
- «soc» Tópicos sobre temas sociales.
- «talk» Tópicos sobre temas de difícil resolución (interminables ...).
- «news» Tópicos sobre el propio sistema de news.
- «rec» Tópicos sobre actividades recreativas.
- «misc» Misceláneos. El cajón de sastre.

Existen otras jerarquías «alternativas»:

- «alt» Dónde todo cabe, desde sexo a los Beatles o los Simpson.
- «gnu» para tópicos sobre el proyecto GNU y la Free Software Foundation.
- «biz» para tópicos relacionados con el mundo de los negocios.

Si hay un servicio en la red donde conviene observar cierta cortesía (lo que se ha llamado muchas veces «Netiquette») siendo educado y cortés, es en las news, algunas de cuyas principales reglas no escritas son: Es conveniente disfrutar con la lectura de los foros favoritos por una temporada y acostumbrarse al «protocolo» de las news (Usenet), no desde el punto de vista informático, sino de educación y cortesía, antes de participar activamente en los foros.

3.5. GOPHER.

Es un servicio de información sobre los recursos de Internet organizado en más de 3.000 servidores interconectados. Cada servidor se encarga de organizar una parcela local de la información, pero la creación de referencias cruzadas entre ellos permite que funcionen como una sola entidad en la práctica.

La información se presenta clasificada por tipos y es accesible mediante menús jerárquicos, la mayor parte de servicios de la red, como ficheros, áreas de mensajes, bases de datos accesibles vía Telnet, documentación de todo tipo, etc., aparecen ante los ojos del usuario según se requiera. El menú raíz del que dependen jerárquicamente el resto de servidores reside en el ordenador llamado gopher.micro.umn.edu. Para acceder al servicio, no es realmente necesario conectar con esa máquina; basta hacerlo con el servidor Gopher más cercano y navegar por menús hasta localizar la información deseada.

3.6. WAIS.

Wais (Wide Area Information Server) permite realizar búsquedas por contenido en grandes documentos textuales o bases de datos. En lugar de navegar por menús de opciones, al conectar con un servidor Wais el usuario final proporciona al sistema una serie de palabras que caracteriza el tema concreto que le interesa. Como resultado, se devuelve una lista de documentos que se ajustan a la demanda de información.

Existen numerosos servidores Wais en la red Internet, cada uno especializado en un tema concreto. Para acceder a ellos es preciso, como en el caso de Gopher, ejecutar una aplicación cliente en el ordenador del usuario.

3.7. WORLD WIDE WEB (WWW).

Es sin lugar a duda el servicio «estrella» de la Red y el responsable del tremendo crecimiento actual que está desbancando de algún modo otros servicios.

Este servicio está basado en la arquitectura Cliente/Servidor nativa del sistema operativo Unix: en la máquina servidor existe un programa que continuamente atiende las peticiones de servicio procedentes de los programas cliente que los usuarios de Internet ejecutan en sus puestos de usuario, proporcionándoles la información que el administrador WWW de dicho sistema servidor ha preparado para ser accedida.

Este proceso servidor es un Daemon (Device And Execution MONitor) permanente «escuchando» peticiones en una serie de puertos. WWW no se limita a mostrar documentos textuales, sino que puede mostrar gráficos e iconos a todo color e integra en sus páginas la posibilidad de acceso a servidores de información de tipos diversos (FTP, Archie, News, Bases de Datos, etc.) o establece conexiones Telnet cuando es necesario.

El servicio World Wide Web, WWW o W3 o simplemente Web, tuvo su origen en el CERN (Centro Europeo de Investigación Nuclear) cuando se plantearon un sistema que permitiera la búsqueda de información en la red, enlazando documentos con tecnología de hipertexto y con la creación de un visualizador de la información que permitiera inicialmente la visualización de texto y gráficos.

En el planteamiento inicial se optó porque las funciones de formato del texto, visualización de gráficos, etc., fuera realizada por el visualizador en lugar de por el sistema que enviaba el documento. De este modo, el servidor solamente enviaba una serie de bytes al visualizador y éste sería el que formateaba.

De este planteamiento surgieron inmediatamente dos necesidades:

- Cómo especificar la ubicación de los documentos.
- Cómo iba a saber el visualizador como formatear el documento.

3.8. URL (UNIVERSAL RESOURCE LOCATOR).

Para solucionar la primera necesidad, definieron el concepto de URL (Universal Resource Locator) o Localizador Universal de Recursos. De este modo quedó definido como alcanzar cualquier recurso de Internet. Su forma exacta depende del tipo de recurso que se quiera alcanzar. La sintaxis es la siguiente: tipo-de-recurso://host.dominio/directorio/fichero.

El tipo de recurso actualmente puede ser:

- file: especifica un recurso en el sistema local.
- ftp: especifica un recurso al que se accede con el protocolo File Transfer Protocol.
- Telnet: especifica un recurso de emulación de terminal virtual.
- Gopher, WAIS, news: especifica los correspondientes servicios de Internet.
- http: especifica un recurso al que se accede con el HyperText Transfer Protocol.

El URL puede apuntar a cualquier recurso, no sólo a documentos hipertexto. Es el visualizador el que determinará qué hacer con el recurso una vez accedido. No todos los visualizadores del mercado soportan todos los tipos de recursos definidos anteriormente. Para solucionar cómo el visualizador iba a reconocer el modo de formatear el documento, se acordó utilizar un subconjunto de las normas SGML (Standardized General Markup Language) de formateo de documentos. Ese subconjunto es el HTML, HyperText Markup Language. En contra de la opinión común, HTML no es un lenguaje de programación, sino una especificación de formateo de documentos.

De este modo, cuando un cliente solicita un documento a un servidor, recibe un flujo de bytes, que lleva embebidas marcas (tags) que hacen saber al visualizador la acción a realizar (resaltarlo, aumentar el tamaño, centrarlo, darle forma de lista. etc.).

Entre las marcas que puede recibir el visualizador están a su vez referencias a otros documentos o recursos en la red (URL's). Cuando el usuario selecciona una de estas referencias, se va a buscar el documento en el sistema al que apunta el URL, produciéndose un «salto» a otro sistema que puede estar en cualquier lugar del mundo. De este modo, en la red empiezan a aparecer documentos que a su vez referencian a otros documentos -que suelen estar en otro servidor- creándose una especie de «telaraña» de alcance mundial.

3.9. VISUALIZADORES O NAVEGADORES.

Existen muchos en el mercado, una gran parte de dominio público. Entre ellos:

- Mosaic. Del NCSA (Centro Nacional de Aplicaciones de Supercomputación) de los EE.UU., en la Universidad de Illinois en Urbana-Campaign. De los primeros visualizadores y fue durante mucho tiempo el más popular, tanto que mucha gente llama Mosaic al WWW.
- Netscape. Introducido en el mercado por Netscape Communications, empresa creada por los diseñadores de Mosaic. Supera en funcionalidad y prestaciones a Mosaic, permitiendo la visualización de la información mientras se carga, mejorando la seguridad con soporte de mecanismos SSL (Secure Sockets Layer), e incorporando pasarelas para el tratamiento de muy diferentes tipos de ficheros, no sólo HTML y de servicios (Telnet, ftp). Actualmente incorpora Java.
- Ubique Sesame. Aparecido en 1995. Incluye la posibilidad de ver qué usuarios están en un momento determinado en un servidor, establecer conversaciones interactivas con ellos e incluso invitarlos a que se dejen guiar a través del Web. Aparte de estas características, es superado por Netscape.

- Arena. Para Unix (Linux), DOS y Mac.
- Cello, Enhanced Mosaic, Galahad, Quadralay, MacWeb, SlipKnot, Viola, WebSurfer. Para diferentes plataformas.
- Lynx. Sólo funciona en modo texto. De utilidad para tener acceso al Web desde pantallas tipo vt100.
- MS Internet Explorer.

La importancia en dominar el mercado de visualizadores tiene que ver con la especificación HTML. Desde su primera aparición han ido incorporándose nuevas marcas o tags para añadir funcionalidad a las páginas Web. Puede ocurrir que un documento que se visualiza de un modo con un visualizador, aparezca mal formateado por otro.

3.10. SERVIDORES.

Existen para todas las plataformas del mercado. Muchos de ellos son gratuitos y pueden obtenerse de la propia red Internet. La gran mayoría están sobre plataformas Unix. Los mas populares públicos son el NCSA y el del CERN.

En este entorno, Microsoft ofrece junto con sus productos Windows 2000 Advanced Server un servidor (MS Internet Information Server) sin coste. Éste es, en gran parte, el origen de la actual lucha por el mercado entre Windows 2000- Advanced Server y Unix, ya que la tecnología de Internet empieza a ser utilizada por las empresas en las Intranets.

3.11. HTML (HYPERTEXT MARKUP LANGUAGE).

Ya se ha comentado, que aunque se hable de HTML como un lenguaje, no lo es, ya que carece de muchas de las características que debe tener un lenguaje, como estructuras de control, variables, etc. Es, en rigor, una norma de descripción de páginas Web mediante la inserción de Marcas (tags) en los documentos que controlan los diferentes aspectos de la presentación y el comportamiento de sus elementos.

La primera versión HTML 1.0, desarrollada por Tim Berners-Lee del CERN, ha sido rápidamente ampliada y mejorada. Para escribir un documento HTML sólo es preciso un editor ASCII. Las marcas o tags que controlan el comportamiento del documento son fragmentos de texto encerrados entre los signos <y> del modo «<marca>». Hay muchos tipos de marcas, que no son objeto de este tema y para las cuales el lector debe dirigirse a cualquiera de las múltiples publicaciones existentes, o consultar cualquiera de los múltiples Web existentes con esta información.

La estructura básica de un documento HTML es la siguiente:

<HTML>

<HEAD>

... Información de cabecera. No se visualiza. Hay marcas que sólo se aplican a la cabecera.

</HEAD>

</BODY>

.... Cuerpo del documento. Muchos tipos de marcas diferentes.

</BODY> ,

</HTML>

3.12. ESCRITURA DE DOCUMENTOS HTML.

Para escribir un documento HTML sólo es preciso un editor ASCII, aunque la tarea es tediosa para documentos de complejidad media, por lo que han aparecido en el mercado multitud de productos para escribir documentos con la especificación HTML. Hay muchos de dominio público para todo tipo de plataformas (Unix, DOS, Windows, Mac, etc.). Dado que la plataforma MS-Office es de las más difundidas como entorno ofimático, las últimas versiones del producto incorporan la posibilidad de generar documentos HTML a partir de documentos Word, Hojas Excel y presentaciones PowerPoint, sin necesidad de herramientas específicas, lo que permite una gran productividad. Para otros productos como FrameMaker, Latex, Troff, etc., existen convertidores.

No obstante, si los documentos tienen cierta complejidad es preferible el uso de herramientas específicas, como las proporcionadas por Netscape, u otras como HotMetal, HotDog, etc. Es tan amplia la posibilidad de herramientas, que suele ser aconsejable buscar en la propia red las herramientas más adecuadas antes de acometer un proyecto de publicación electrónica.

3.13. IRC Y SERVICIOS DE CONFERENCIA EN TIEMPO REAL.

En la red existe un gran número de servicios de conferencia en tiempo real, entre los cuales los más conocidos son «talk» e IRC (Internet Relay Chat). Todos estos servicios proporcionan un modo de interacción entre la gente. El correo electrónico y las news son servicios asíncronos, no es preciso que el usuario esté conectado para que pueda recibir, mientras que para los servicios de conferencia en tiempo real los usuarios necesitan estar «en línea».

El servicio «talk» es el sistema de conferencia más antiguo. Está disponible en la mayoría de sistemas Unix y permite que la gente mantenga una conversación uno-a-uno. El «usuario A» inicia una sesión «talk» ejecutando el comando «talk usuario B@sistema», especificando la dirección del otro usuario con el formato de una dirección de correo electrónico.

El destinatario recibe un mensaje del tipo «el usuario A está solicitando una sesión talk...». Cuando el usuario B la acepta, aparece una ventana con dos partes, la local y la remota. En cada una de ellas aparece lo que va tecleando cada usuario.

El servicio talk no introduce «inseguridad» por sí mismo, aunque si el sistema está detrás de un cortafuegos, puede forzar a introducir reglas de seguridad que dejan «inseguras» otras zonas del sistema.

IRC es como la Banda Ciudadana (CB) de los radioaficionados en Internet. Los usuarios acceden a IRC mediante «clientes» dedicados o sesiones Telnet con servidores que proporcionan «servicios de cliente IRC públicos». Los servidores IRC proporcionan cientos -a veces miles- de los llamados «cana-

les» a los que los usuarios se pueden unir. Los canales están cambiando continuamente. Cualquiera puede crear uno en cualquier momento. El canal permanece activo mientras existe algún usuario en él. Cualquier número de personas puede conectarse a un canal y por tanto la comunicación es muchos-a-muchos.

3.14. HERRAMIENTAS PARA PROPÓSITOS ESPECÍFICOS.

Existen multitud de herramientas y servicios sobre la red, prácticamente están apareciendo nuevos servicios cada día. A veces llegan a convertirse en estándares «de facto», mientras que otras veces llegan a formalizarse en documentos RFC (Conjunto de documentos con estándares de Internet). De entre todos estos, existen algunos de interés y que aquí mencionamos:

- «finger». Existe en muchos sistemas para conocer quién está conectado. Hay además extensiones para Internet, que toman la forma «finger@sistema» y nos dice los usuarios conectados a un sistema remoto, o bien «finger usuario@sistema» que nos da la información sobre un usuario concreto. Este comando no siempre funciona, pues no es infrecuente que las instalaciones lo tengan deshabilitado (por lo menos de cara al «exterior»).
- «ping». Se utiliza para comprobar si el sistema remoto está activo. El formato general es «ping sistema», donde sistema debe ser un FQDN (nombre totalmente cualificado). Es frecuente que la respuesta incluya datos sobre la calidad del enlace, tales como tiempos de circulación del paquete. Es utilidad básica para comprobar si un sistema está activo y poder chequear si es así, ante la sospecha de por qué no alcanzamos un sistema.
- «tracert». Utilidad para ver la ruta que se sigue hasta alcanzar un sistema.

3.15. BASES DE DATOS Y PUBLICACIONES.

Existen empresas que se dedican a mantener y ofrecer al público a través de Internet Bases de Datos Temáticas, accesibles al usuario final conectado a la Red, previo pago de una cuota de conexión o bien mediante abono por tiempo de consulta o por cantidad de información transferida.

Otras entidades ponen a disposición del público sus Publicaciones: diarios, revistas de información general o especializada, publicaciones técnicas y/o sectoriales.

Tanto la consulta a Bases de Datos como a Publicaciones se venía realizando en modo On-Line, mediante emulación de terminal. Sin embargo en los últimos meses los servicios de información han sufrido una transformación debido a la difusión mundial de la tecnología Web a la que se han añadido características multimedia y de comunicación entre el visualizador y el servidor, que permiten augurar una amplia y rápida difusión para el gran público. Este aspecto se analizará en el siguiente epígrafe.

El conjunto de servidores WWW forma una red de servidores dentro de Internet que ofrecen páginas hipertexto en un formato denominado HTML (HyperText Markup Language), un lenguaje de definición de páginas con extensiones hipertexto portable a cualquier tipo de plataforma gráfica. Estas páginas contienen, además de texto en varios formatos, imágenes, sonidos o vídeo, y permiten lanzar la lectura de páginas de otros servidores activando ciertas palabras resaltadas dentro del mismo documento. Lo que se hace al desarrollar páginas en HTML es crear documentos que dan indicaciones precisas al programa cliente (navegador) de cómo debe presentarse el documento en pantalla, señalando el formato de los textos y el lugar donde se deben insertar las imágenes.

Sin embargo este lenguaje es demasiado sencillo para realizar determinadas tareas. Es por ello que, debido a la necesidad de extender sus capacidades, se han ido creando componentes y funcionalidades nuevas que mejoran y extienden sus posibilidades. A continuación se exponen las características más destacadas de cada uno:

- **Javascript:** Javascript no es un lenguaje de programación propiamente dicho. Es un lenguaje script u orientado a documento creado por Netscape. Se trata de un lenguaje interpretado, cuyo código se incluye directamente en los documentos HTML. Con Javascript no se puede hacer un programa complejo, sólo mejorar las páginas HTML añadiendo formularios, efectos en barra de estado, animaciones, etc.
- **Plug-ins:** los plug-ins (literalmente, «añadidos») son aplicaciones que se integran con el navegador para gestionar determinados tipos de contenido y dar ciertas capacidades dinámicas a las páginas. Se trata de pequeños programas que extienden las capacidades de los navegadores dando la posibilidad de visualizar determinados tipos de documentos en el propio navegador, como por ejemplo vídeos o incluso reproducir ficheros de sonido directamente desde el navegador sin hacer uso de aplicaciones externas.
- **Cookies:** una cookie es una parte de información interna que se transmite entre el software servidor y el cliente (en este caso, un navegador). En esta información se guardan datos acerca de qué hizo el usuario la última vez que se conectó a la Web correspondiente y permite hacer uso de dicha información para conocer las preferencias de un usuario y poder ofrecer información personalizada en la Web. Además es un mecanismo utilizado para mantener sesiones permanentes lo cual es necesario en entornos transaccionales.
- **CGI (Common Gateway Interface):** CGI es un estándar para la ejecución de aplicaciones externas en servidores Web. No es un lenguaje, pero es una especificación que permite que una página HTML pueda comunicarse con un programa, que puede estar escrito en cualquier lenguaje, y que reside en el servidor. De este modo se amplían las capacidades de HTML. Esto podría usarse, por ejemplo, para acceder, a través de la WWW, a una base de datos y enviar al programa cliente la información que hubiera solicitado de dicha base de datos en tiempo real. Para ello haría falta un programa hecho en C, PERL o cualquier otro lenguaje, la interfaz CGI que es el que accede a la base de datos y un formulario en una página HTML desde el que hacer la llamada o petición.
- **ActiveX:** es una tecnología propiedad de Microsoft estrechamente relacionada con su modelo de objetos COM/DCOM y supone una evolución de la tecnología OLE. Se trata de módulos u objetos que se pueden descargar del servidor y ejecutar directamente en el sistema operativo. Un objeto ActiveX con la funcionalidad suficiente (en forma de interfaces) puede ser almacenado en bases de datos, transmitido por correo, visualizado en un documento Word o utilizado como parte de una aplicación desarrollada en Delphi, Visual C++ o cualquier otro entorno que entienda los controles OCX, en los cuales están basados. Al aprovechar la arquitectura y base existente de código OLE, prácticamente cualquier control OCX puede ser transformado en un control capaz de ser transferido a través de Internet y utilizado en una página Web con un mínimo de cambios.
- **Java:** éste es un lenguaje orientado a objetos que fue desarrollado inicialmente por la compañía Sun Microsystems, y posteriormente adoptado como estándar. Aunque en principio es un lenguaje de carácter general, su principal característica es la de ser independiente de cualquier plataforma, lo que le hace muy adecuado para ser utilizado en Internet, ya que puede ejecutarse en cualquier ordenador que tenga un navegador compatible con Java (actualmente los navegadores más utilizados soportan este lenguaje). Esto supone que un programa escrito en Java puede ser ejecu-

tado, sin ningún cambio, en un PC, un MAC o una máquina UNIX. Esto es así porque los programas escritos en JAVA no se ejecutan directamente en el ordenador, sino que lo hacen en una máquina virtual (la Máquina Virtual JAVA), quedando además limitado dentro de ella, lo que hace de JAVA un lenguaje seguro, ya que no puede acceder a otros recursos del ordenador.

- Applets: un applet es un pequeño programa ejecutable escrito en el lenguaje Java que envía el servidor al programa cliente para que funcione incorporado a la página. De esta manera, aunque el lector de páginas no incorpore ciertas funciones, éstas pueden ser añadidas desde el servidor para que pueda leer, por ejemplo, diversos formatos multimedia sin incorporar en el mismo programa el lector para dichos documentos. A diferencia de ActiveX, estos programas no se ejecutan directamente en el sistema operativo sino en el navegador.
- VRML (Virtual Reality Modeling Language): este lenguaje fue creado con la intención de extender las capacidades de HTML e introducir en las páginas web gráficos tridimensionales. Con VRML se puede definir y representar realidad virtual en Internet. De este modo se pueden crear mundos virtuales por los que se puede viajar y desplazarse. Para ello sólo hace falta un navegador que soporte VRML (los más usados Netscape y Explorer lo soportan sin problemas).
- ASP (Active Server Pages): esta tecnología de Microsoft ofrece a los desarrolladores de páginas Web la posibilidad de acceder de una forma sencilla y flexible a Bases de Datos compatibles con el estándar ODBC. Desde esta forma, desde las páginas de un servidor Internet o desde una Intranet se puede acceder a cualquier Base de Datos.

Al amparo de Internet y como factor clave para su rápida expansión se han desarrollado herramientas y sistemas que permiten acceder a multitud de servicios sin necesidad de poseer unos especiales conocimientos informáticos. Entre ellos destaca el WWW «World Wide Web» para el acceso transparente a servicios de información y bases de datos distribuidas.

Entre los beneficios del desarrollo de servidores WWW en las Administraciones Públicas cabe citar:

- La reducción de costes asociados con la elaboración y publicación de catálogos, revistas y boletines de información de difusión masiva.
- La mejora de la calidad de la información al permitir una actualización permanente.
- El acercamiento de la Administración al ciudadano a través de un servicio universal de bajo coste.

El objetivo de los poderes públicos con los ciudadanos, en su calidad de usuarios de los servicios de información que proporcionan, se ha de basar en el logro de dos objetivos básicos:

- Facilitar el conocimiento de la existencia, disponibilidad y medios de acceso a los productos de información elaborados a partir de los datos públicos.
- Promover políticas orientadas a asegurar que la información llegue al mayor número posible de usuarios y en las condiciones más favorables de tiempo y coste, contribuyendo de esta manera al crecimiento de la industria de la información electrónica.

Un ejemplo de iniciativa en esta dirección es el Hipercentro de Información Administrativa puesto en marcha por el Ministerio de Administraciones Públicas (MAP), el cual pretende proporcionar

una vía de acceso única, ser una entrada maestra que, a partir del mantenimiento de un catálogo de recursos, facilite la navegación por los servidores donde exista información pública. A título de ejemplo, también hay que destacar los esfuerzos de instituciones como la Generalitat Valenciana, la Xunta de Galicia o el Ayuntamiento de Barcelona que están introduciendo el concepto de ventanilla única en sus servidores con el objetivo de ofrecer la posibilidad de realizar ciertos trámites administrativos por medios electrónicos. Un primer paso lo ha dado la Xunta de Galicia, donde ya es posible consultar el estado de un expediente administrativo a través de Internet.

También es importante mencionar que junto al Boletín Oficial del Estado ya se puede acceder a Boletines Oficiales de varias Comunidades Autónomas y Diputaciones Provinciales, algunos de ellos incluso a texto completo.

De cara al futuro, es fácil pronosticar que, dado el auge que están adquiriendo las tecnologías de la información y las comunicaciones, su presencia también se hará notar en el ámbito administrativo.

Las Intranets son sistemas de información interna para entornos corporativos basados en tecnología Internet (servicios Web, protocolo TCP/IP y HTTP, páginas HTML, etc.). Las principales características de las Intranets se pueden resumir en los siguientes puntos:

- Es una forma de compartir los recursos (información) de una organización.
- Es una alternativa a los actuales SO de red y paquetes de trabajo en grupo, con las ventajas que supone el abandono de los estos sistemas propietarios y la adopción de arquitecturas abiertas.
- Una Intranet.
- No tiene por qué estar conectada a Internet, aunque es deseable.
- No es una LAN o WAN: no depende de las aplicaciones o SO del vendedor.
- No es tan sólo una forma de correo electrónico corporativo. Ofrece otros servicios como directorios, acceso a ficheros, impresoras compartidas y administración de red.
- Todo se basa en la administración de la información, que se hace de manera independiente de la plataforma y del software.
- Una Intranet es una herramienta que facilita:
 - La toma de decisiones: se comparten resultados con los compañeros.
 - La comunicación: permite acceder a cualquier tipo de información a cualquiera de los miembros.

Una Intranet aporta a una organización diversas ventajas como, por ejemplo, los servicios de directorio, capacidad de integración de datos de la empresa que pueden ser consultados por los empleados, coordinación de grupo de trabajo o disponer de correo electrónico integrado.

Por su parte, las Extranets son una variante de las Intranets. Mientras las Intranets facilitan las comunicaciones y la compartición de recursos dentro de una compañía, y generalmente son inaccesibles desde el exterior, las Extranets surgen para satisfacer las necesidades de comunicación que sobrepasan las fronteras de estas corporaciones, típicamente utilizando la propia Internet como medio de interconexión.

El ejemplo más claro de aplicación está en las compañías que deben gestionar una gran cantidad de pedidos con sus proveedores. Así, por medio de la Extranet los proveedores pueden acceder a determinadas páginas donde se encuentran una serie de pedidos emitidos por la compañía propietaria de la Extranet y responder a dichos pedidos emitiendo a su vez una oferta. De este modo, todo el proceso de gestión de pedidos se agiliza enormemente eliminando trámites burocráticos y tiempos de espera. En todo momento sólo pueden acceder a la Extranet aquellos proveedores autorizados para ello.

Como conclusión, se puede decir que las Extranets suponen una nueva actitud frente a la comunicación, y no sólo entre los miembros que integran la empresa (Intranets) sino también entre los distintos agentes externos (socios, consumidores, proveedores,...).



