

Redes en educación 2

Capítulo 4

Internet



ÍNDICE

Introducción.	
1.1. ¿Qué es Internet?	3
1.2. La historia continúa.	3
2. La conexión a Internet.	5
2.1. Proceso de conexión.	5
3. Protocolos TCP/IP.	7
3.1. Definición. Modelo.	7
3.2. Protocolo TCP.	9
a) Definición y Características.	9
b) Segmento TCP.	10
c) Establecimiento de una conexión.	14
d) Control del flujo.	15
e) Control de errores.	16
f) Cierre de la conexión.	17
g) Puertos y Zócalos (Sockets).	18
h) Puertos y seguridad.	20
3.3. Protocolo UDP.	21
a) Introducción	21
b) Formato del segmento UDP.	22
3.4. Protocolo IP.	23
a) Definición. Características.	23
b) Relación con otros Protocolos.	26
c) Modo de Operación.	26
d) Formato de un Datagrama IP.	27
e) Direcciónamiento.	29
3.5. Protocolo ARP. Resolución de direcciones.	38
3.6. Protocolo RARP.	40
3.7. Protocolo BOOTP.	40
3.8. Protocolo ICMP.	40
a) Orden ping.	41



Anotaciones

Capítulo 4

b) Orden tracert.	41
4. Servicios de Internet.	42
4.1. Introducción.	42
4.2. Servidores de acceso.	42
4.3. HTTP.	43
4.4. News.	44
a) Funcionamiento de las News.	45
4.5. FTP.	47
4.6. VNC.	48
4.7. IRC.	49
4.8. Telnet.	49
4.9. DNS.	51
4.10. Correo electrónico.	53
4.11. SMTP.	54
4.12. POP.	55
4.13. IMAP.	57
4.14. Sincronización horaria.	57
5. Internet como red p2p.	58
5.1. Tecnologías.	60
a) Freenet.	60
b) Aimster.	60
c) Gnutella.	60
d) Mensajes instantáneos.	60
e) Búsquedas personales.	60
f) Caso NAPSTER.	61
5.2. Utilidades.	61
6. Posibilidades de futuro.	62
Ilustraciones	65

Anotaciones

Introducción.

1.1. ¿Qué es Internet?

Internet es un sistema mundial de redes de ordenadores interconectadas mediante la pila de protocolos TCP/IP que pueden comunicarse sobre distintos medios y tecnologías. Este sistema de interconexión permite que cualquier usuario de cualquier red pueda acceder a equipos integrados en otras redes de otros países, siempre que tenga permiso para ello, para compartir información o comunicarse empleando, para ello, los distintos servicios de esta red de redes.

En la actualidad emplea parte de los recursos públicos de telecomunicaciones y es autosuficiente y autorregulado, constituyéndose como un medio preferente de comunicación y de colaboración entre sus usuarios.

1.2. La historia continúa.

En el capítulo 1 realizamos una referencia histórica sobre el origen de la comunicación entre computadoras y lo dejamos en 1969, con la creación de la primera red de ordenadores. Sin embargo, si algo caracterizó este hito fue, sin duda, la ausencia de celebraciones. La idea con la que trabajaba la agencia ARPA era mucho más ambiciosa, y esa primera red no era sino un paso más en un camino del que todavía faltaba mucho por recorrer.

La historia continua en un proceso de crecimiento continuo y mejoras. ARPANET, la primera red, es el embrión de Internet y, el desarrollo de esta red hay que entenderlo de forma similar al desarrollo de un embrión; de un conjunto simple de sistemas indiferenciados o con poca especialización se llega a sistemas complejos altamente especializados a través de:

- Especialización funcional.
- Diferenciación de sistemas.
- Complejidad estructural.

El desarrollo de Internet no hubiera sido posible si no hubiera existido una idea clara del objetivo que se perseguía y no se hubieran adoptado las medidas necesarias para su crecimiento. En este sentido es conveniente destacar la edición de los RFC (Request for comments) documentos mediante los cuales se llega a normalizar el funcionamiento de las redes y que permiten a los fabricantes de hardware y software elaborar productos compatibles con la tecnología existente.

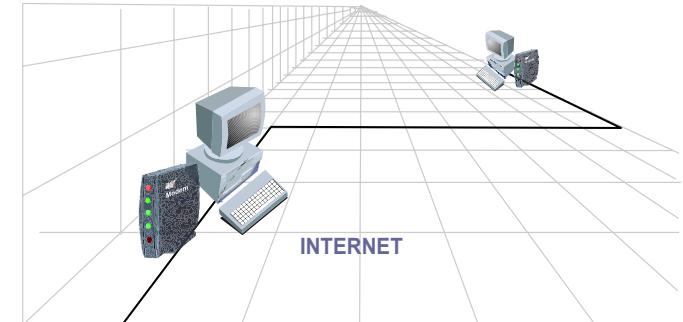


Ilustración 1: Internet

Anotaciones

Nota:

El primer RFC se editó el 7 de abril de 1969, su título era "Host Software". El primer documentalista responsable de estos documentos fue Jon Postel, que se encargó de este trabajo 28 años.

Actualmente se puede acceder a estos RFC a través de la página web <http://www.rfc-editor.org/>

Otro elemento fundamental para el desarrollo de Internet fue la creación de la pila de protocolos TCP/IP, sin embargo, no fueron estos los primeros protocolos que se emplearon en la primera red creadas por ARPA, ARPANET, el protocolo original era el Network Control Protocol (embrión de TCP/IP) y ALOHA, primer protocolo de comunicaciones por conmutación de paquetes vía radio.

En 1971 se crea el primer programa de correo electrónico, su desarrollador fue Ray Tomlinson, pero no fue hasta 1972 que se incorporó el popular carácter @ para separar el nombre de usuario y el servidor de correo de dicho usuario. Un año después se realiza la primera demostración pública de ARPANET realizándose, entre otras cosas, una demostración del chat. Además, en esta Conferencia Internacional de Comunicación entre Ordenadores, celebrada en Washington, se decide la creación del INWG, grupo internacional de trabajo sobre redes.

En 1973, y un año después de la publicación del RFC sobre telnet, se realiza la primera conexión internacional entre ordenadores, y se comienza a estudiar la necesidad de emplear mecanismos de interconexión para la comunicación entre redes. La utilización de news, la creación del RFC sobre transferencias de ficheros, demuestran un enorme trabajo de desarrollo que contrasta con el bajo número de usuarios, alrededor de 2000.

Un paso que debemos considerar fundamental para la creación de Internet es la publicación del artículo "A Protocol for Packet Network Interconnection" donde se explicaba el protocolo TCP. Un año después se realizaban los primeros ensayos mediante este sistema de comunicación y, en función de los resultados de las distintas pruebas se adopta en 1977 la división del protocolo TCP en dos TCP e IP. Ya existían programas de correo con funcionalidades similares a los que utilizamos ahora, y se había empleado para una transmisión de email transcontinental.

En 1979 se crea USENET. Un año después se produjo el parón del 27 de octubre en ARPANET debido a la amenaza de la propagación accidental de un virus. Se empieza a ser consciente de los problemas que se pueden asociar al desarrollo de Internet. Entre los años 1981 y 1982 se crean redes privadas y de ámbito nacional.

-
- 1971 ● Primer programa de correo electrónico
- 1973 ● Primera conexión internacional entre ordenadores
- 1977 ● Aparecen TCP e IP como protocolos segregados
- 1979 ● Se crea USENET
- 1983 ● ARPANET se separa de la red de comunicación militar
- 1984 ● Se crea el Sistema de nombres de dominio
- 1985 ● Se registra el primer nombre de dominio

Ilustración 2: Cronología del desarrollo de Internet

Anotaciones

Nota:

El ataque del virus más famoso de Internet (el gusano virus de Morris) afectó a 6000 de los 60000 host que se encontraban conectados a la red en 1988.

En 1983 ARPANET se separa de la red de comunicaciones militar. A la vez, se decide la adopción de TCP/IP como el protocolo para ARPANET y en 1984 se crea el sistema de nombre de dominios para interpretar las direcciones IP., para en 1985 atribuir al SRI la responsabilidad de asignar los nombre de dominio que residían en el ISI (Information Sciences INstitute), siendo en 1985 cuando se registra el primer nombre de dominio symbolics.com. Internet nace como fenómeno social, económico y tecnológico. A partir de ese momento Internet empieza a ser lo que hoy conocemos, con sus debilidades y virtudes, sus hackers, virus, problemas de crecimiento, etc.

La década de los años noventa, comienza con el pasado inmediato ve como aparece el hipertexto como forma de interactuar con Internet, se desarrolla el primer navegador en 1993 y en ese mismo año se crea el primer servidor web español, Internet desarrolla un crecimiento exponencial en cuanto a usuarios, posibilidades de comunicación, etc. sólo posible gracias al principio con el que se creó, simplicidad en la comunicación, el trabajo difícil lo debían realizar los host.

2. La conexión a Internet.

Podríamos considerar que todos los usuarios de un mismo servidor de acceso a Internet constituyen una red WAN, pues mediante la utilización de una tecnología de telecomunicación llegan a unirse gran cantidad de redes LAN.

2.1. Proceso de conexión.

Para poder realizar una conexión a Internet nos debemos dar de alta en un Proveedor de Servicios de Internet (en adelante PSI), como por ejemplo, Terra, EresMas, Wanadoo, Arrakis,... en los cuales existe un servicio básico gratuito y un servicio profesional, de mayor calidad, de pago.

Una vez dados de alta, y en función de la tecnología que empleemos, por ejemplo, RTB o RDSI, tenemos un número de teléfono, un nombre de usuario y una contraseña.

PROVEEDOR DE SERVICIO

1º Comprueba el nombre de usuario y la contraseña.

2º Acepta el acceso



Ilustración 3: PSI: Los proveedores de servicio permiten realizar la conexión a Internet una vez que nos hemos identificado

Anotaciones

Capítulo 4

La conexión se realiza del siguiente modo: en nuestro Centro Educativo realizamos una conexión telefónica a través del módem conectado a nuestro ordenador. El número de teléfono que marcamos es el del Nodo de Acceso que nos han proporcionado.

El Nodo de Acceso nos conecta con el PSI a través de una Red de Acceso de ámbito nacional. Dicha red de acceso tiene por objeto que nos podamos conectar a Internet desde cualquier lugar a precio de llamada metropolitana, pues siempre habrá un nodo de acceso local cerca.

Al principio debíamos buscar el número de teléfono del Nodo de Acceso local correspondiente para nuestra localidad pero, en la actualidad, cada PSI ha habilitado un único número nacional para las conexiones y por tanto ya no es necesario buscar el número de teléfono de cada localidad.

Nota:

Es necesario indicar que el proceso descrito hasta este momento describe la conexión mediante una tecnología de marcación. Si hubiéramos empleado una conexión ADSL esta descripción no sería válida, ya que en este caso hemos creado un circuito dedicado de conexión permanente.

Una vez seleccionado el número de teléfono correspondiente y realizada la llamada telefónica se establece una conexión con el PSI donde un servidor de autenticación y control de acceso nos permite la conexión hacia Internet tras comprobar que el nombre de usuario y contraseña son válidos.

Una vez en Internet podemos acceder al Centro Proveedor de Información (CPI) donde se encuentran las páginas web y servicios que queremos utilizar (correo electrónico, grupos de noticias, servidor de chat, ...)

Algunas Redes de Acceso son:

- InfoVía Plus (Red de Telefónica): Se trata de la plataforma de Telefónica más utilizada, pues, miles de usuarios y centenares de Proveedores la emplean diariamente para establecer conexión. Infovía dispone actualmente de 160 Nodos de Acceso repartidos por todo el territorio español y para aquellas zonas donde todavía no existe nodo local, dispone del número 901.505.055 que permite a sus usuarios conectarse a precio de llamada metropolitana.

Anotaciones

- **Retenet (Red de Retevisión):** Retenet es la red de Retevisión y presta servicios a Iddeo, su filial para Internet y a eresMas.
- **InterPista (Red de BT Telecomunicaciones):** Es la red de acceso de BT Telecomunicaciones, filial española de British Telecom. InterPista ha pasado de dedicarse casi en exclusiva a clientes empresariales a apostar por el cliente particular tras la compra del proveedor Arrakis.

Otras empresas de telecomunicación que disponen de redes son Airtel (Airtelnet), Uni2, Jazztel...

Si bien el precio de la conexión es el precio de una llamada telefónica local, los PSIs han creado bonos de conexión para un cierto número de horas y 'tarifa plana' en un horario determinado para reducir los costes y así ganar más clientes.

3. Protocolos TCP/IP.

El desarrollo actual de Internet ha sido posible gracias a la utilización de esta pila de protocolos. Su extrema sencillez ha facilitado la intercomunicación entre múltiples redes y que se haya erigido como el protocolo de transmisión por autonomía.

3.1. Definición. Modelo.

TCP/IP es el protocolo usado en Internet. Con este protocolo tiene que funcionar cualquier ordenador que quiera utilizar cualquier servicio de Internet.

En Internet hay muchas clases distintas de ordenadores, con distinto hardware, distinto software, integrados o no en distintos tipos de redes; pero todos ellos tienen que tener en común el protocolo TCP/IP.

En realidad TCP/IP, no es un único protocolo, sino un conjunto de ellos, que cubren las distintas capas del modelo de referencia OSI. Como los dos protocolos más importantes son TCP e IP, estos son los que han dado el nombre al conjunto.

TCP/IP fue desarrollado a principio de los años 70 por el ministerio de Defensa norteamericano, para la red ARPANET. Adoptó su forma actual en 1983, como consecuencia del proyecto DARPA (*Defense Advanced Research Projects Agency*), de la defensa norteamericana. Nació para interconectar distintas redes en entorno operativo UNIX. Soluciona básicamente el problema de interconectar distintas redes, divididas en subredes, enrutando el tráfico entre ellas.



Anotaciones

Capítulo 4

Como la comunicación entre ordenadores es de una gran complejidad, el problema se ha dividido en otros menos complejos, creándose varios niveles. Cada nivel soluciona un problema en la comunicación y tiene asociado uno o varios protocolos para ello.

El modelo de red Internet tiene 4 capas o niveles, que son:

1. **Aplicación:** aquí están incluidos los protocolos destinados a proporcionar servicios, tales como transferencia de ficheros (FTP), navegación en Internet (HTTP), correo electrónico (SMTP), etc.
2. **Transporte:** aquí están incluidos los protocolos destinados a proporcionar el transporte de los datos con la fiabilidad suficiente.

En este nivel la información es dividida en paquetes, para que la transmisión sea más eficiente. Cuando llega al receptor, este mismo nivel se encarga de reordenar los paquetes y unirlos para recomponer la información. Los protocolos que se encargan de esto son, **TCP (Transfer Control Protocol)** y **UDP (User Datagram Protocol)**.

Equivale a las capas de *transporte* del modelo de referencia OSI.

3. **Internet o red:** se encarga de enviar cada paquete de información a su destino, es decir encaminar los datos. Para ello coloca los paquetes del anterior nivel en datagramas IP y los envía al nivel inferior. Cuando recibe estos datagramas del nivel inferior, comprueba su dirección IP y los envía al nivel superior o los encamina a otro ordenador, si no son para éste. Los protocolos que actúan en este nivel son:

- IP (Internet Protocol),
- ICMP(Internet Control Message Protocol),
- IGMP(Internet Group Management Protocol),
- ARP (Address Resolution Protocol),
- RARP (Reverse Address Resolution Protocol),
- BOOTP (Bootstrap Protocol).

Equivale a las capas de red del modelo de referencia OSI.

4. **Enlace:** se encarga de la transmisión a través del medio físico, que une todos los ordenadores de la red. En este nivel tenemos protocolos como Ethernet, DLC (IEEE 802.2), X.25, Frame Relay, etc.

Equivale a las capas física y de enlace del modelo de referencia OSI.

4	Aplicación		HTTP, FTP, SMTP, etc.
3	Transporte		TCP, UDP
2	Red	Internet	IP
		Host a red	ICMP, ARP, etc.
1	Enlace	Acceso a la red	Ethernet, Token Ring, etc.
		Enlace físico	Tipo cable

Ilustración 5: Modelo de capas de TCP/IP

Anotaciones

La capa física nos define el medio físico por el que se transmite la información (cable, ondas, etc.). La capa de enlace o acceso al medio define la forma en que los ordenadores envían o reciben la información. Cuestiones como; de qué forma se transmite la información, en qué momento puede un ordenador transmitir, saber si el mensaje es para él o no, etc.; las soluciona esta capa.

Analogía:

Supongamos que se nos ocurre la peregrina idea de enviar "El Quijote" a un amigo, empleando palomas mensajeras. Evidentemente, una sola paloma no puede llevar todo el libro. Microfilmamos las páginas y a cada paloma le damos un microfilm. Para facilitar el trabajo de nuestro amigo, numeramos las filminas, puesto que ordenar después todo el libro, sin una numeración, resultaría muy difícil.

A lo largo de todo el viaje, alguna paloma puede ser cazada, decidir que se va a otro lugar o, simplemente, perder su mensaje. Cuando esto sucede, nuestro amigo nos manda una paloma diciendo que algo no ha llegado o que ha llegado defectuoso. Así, hasta que complete el libro y lo pase a papel.

Ahora, en lugar de emplear las palomas, envío El Quijote en formato pdf por correo electrónico. Aparentemente, el libro va completo, sin embargo, los protocolos de comunicación realizarán las mismas tareas que tendríamos que hacer mi amigo y yo empleando las palomas. De algo tendrían que valer las TIC.

3.2. Protocolo TCP.

a) Definición y Características.

Protocolo de control de transmisión de la capa de transporte, que regula las cuestiones relativas al transporte de la información. Pertenece a la suite de protocolos TCP/IP. Este protocolo se encuentra descrito en el documento [RFC 793](#).

El protocolo TCP se encarga de regular el flujo de la información, de tal forma que éste se produzca sin errores y de una forma eficiente. Proporciona calidad de servicio. Por esto, se dice que este protocolo es:

- **Orientado a la conexión:** esto significa que se establece una conexión entre emisor y receptor, previamente al envío de los datos. Se establece un *circuito virtual* entre los extremos. Este circuito crea la ilusión, por esto se llama virtual, de que hay un único circuito por el que viaja la información de forma ordenada.

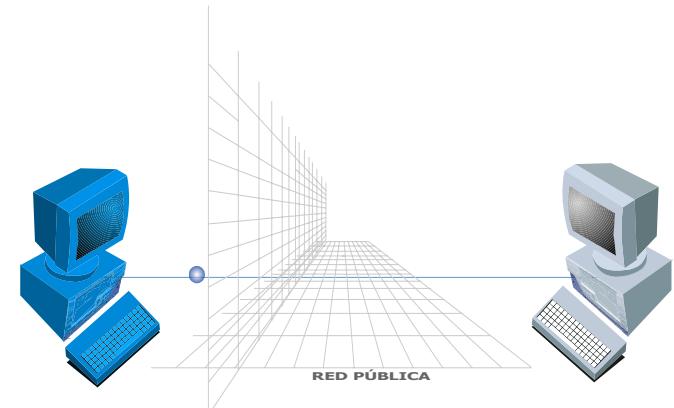


Ilustración 6: Protocolo orientado a conexión es el que permite la creación de un circuito virtual

Anotaciones

Esto, en realidad no es cierto, la información viaja en paquetes desordenados por distintas vías hasta su destino y allí, tiene que ser reensamblada.

- **Fiable:** significa que la información llega *sin errores* al destino. Por esto, la aplicación que usa este protocolo, no se tiene que preocupar de la integridad de la información, se da por hecho.

El protocolo **TCP** actúa de puente entre la aplicación, que requiere sus servicios, y el **protocolo IP**, que debe dirigir el tráfico por la red, hasta llegar a su destino.

Este protocolo usa la tecnología de *comunicación de paquetes*. La unidad de información es el **byte** y estos se agrupan en **segmentos**, que son pasados al protocolo IP. Estos segmentos viajan encapsulados en los *datagramas IP*. Es un flujo de información no estructurado, información binaria sin ningún formato. La aplicación de destino tiene que interpretar esta información. Los datos viajan en los segmentos junto a información de control. Usa una memoria intermedia llamada *buffer* para hacer más eficiente la transferencia. La transmisión es *punto a punto*, origen y destino, y *full-duplex*, es decir en ambas direcciones, para hacer más eficaz el tráfico en la red.

Como hemos dicho, antes de poder enviar información, hay que establecer una conexión entre los extremos. En una transmisión hay tres fases:

1. Apertura de conexión.
2. Transferencia de datos.
3. Cierre de conexión.

b) Segmento TCP.

Como ya hemos dicho, el protocolo TCP divide los mensajes en paquetes, llamados **segmentos TCP**. Cada uno de estos segmentos se integran en el campo de datos de un datagrama IP, y el protocolo IP se encarga de dirigirlos a través de la red o redes, hasta su destino.

La unidad de información en el protocolo TCP, es el **byte (8 bits)**. Estos bytes se numeran y cada segmento TCP indica en su cabecera el número del primer byte que transporta. También la cabecera de cada segmento lleva el *puerto de origen, el puerto destino, confirmaciones o acuses de recibo (ACK)*, etc.

Para que la transmisión sea eficaz, el tamaño de los segmentos es muy importante. Hay dos límites para el tamaño de los segmentos: por un lado el *tamaño máximo de un paquete IP*; que es de 64 Kbytes, aunque casi nunca llega a este tamaño; y por otro, el tamaño máximo que soporta la red local, que viene dado por la *Unidad de Transferencia Máxima (MTU)*. Es conveniente elegir el tamaño de los segmentos de tal forma que no haya que fragmentarlos.

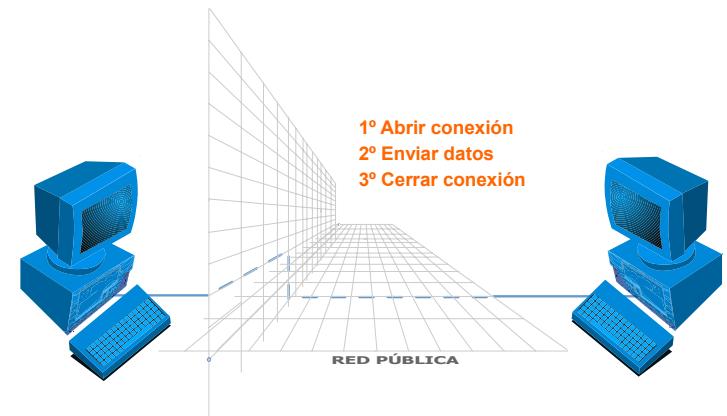


Ilustración 7: La transmisión de datos en Internet constituye un proceso de tres fases

Anotaciones

Capítulo 4: Internet

Los datagramas IP no tienen porqué llegar en el orden correcto al destino, pueden llegar en cualquier momento y en cualquier orden, e incluso puede que algunos no lleguen a su destino o lleguen con información errónea. El protocolo TCP se encarga de corregir estos problemas, numera los datagramas antes de ser enviados y en el destino se encarga de reensamblarlos en el orden adecuado. Además solicita el reenvío de los datagramas que no hayan llegado o sean erróneos. No es necesario normalmente reenviar el mensaje completo.

Para pensar:

Antes de continuar leyendo, os proponemos que cojáis un lápiz y un papel y vayáis completando la tabla que viene a continuación con la información que os ofrecemos.

El formato estándar de un segmento TCP es el siguiente:

Siendo el significado de sus campos:

- **Puerto TCP origen:** especifica el puerto del host origen que envía el segmento TCP. Ocupa 16 bits y es obligatorio.

Para pensar:

Empleando 16 bits en binario ¿cuántos puertos distintos pueden definirse?.

- **Puerto TCP destino:** especifica el puerto del host destino al que se envía el segmento TCP. Ocupa 16 bits y es obligatorio. Los puertos proporcionan una manera práctica de distinguir entre las distintas transferencias de datos, ya que un mismo ordenador puede estar involucrado en varias transferencias simultáneas.

Analogía:

Los puertos de un ordenador son como los andenes de una estación. Madrid-Atocha tiene más de 30 andenes, todos los trenes llegan a Madrid, pero en función de su origen las personas que esperan a los viajeros deben situarse en un andén u otro.

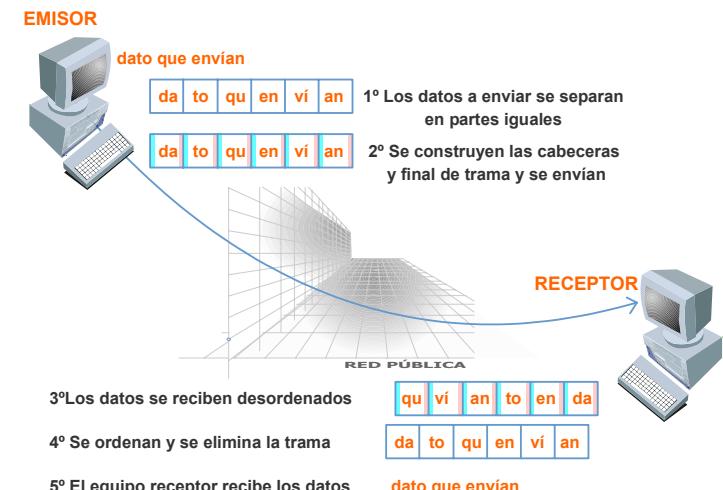


Ilustración 8: TCP/IP: Permite un uso óptimo de las redes de medio compartido ya que evita el colapso del canal de comunicación

Anotaciones

Capítulo 4

- **Número de secuencia:** indica el primer byte de datos que transporta el segmento. Ocupa 32 bits y es obligatorio. Al principio de la conexión, se asigna un número de secuencia inicial (ISN, Initial Sequence Number). Los siguientes bytes se numeran consecutivamente.

Analogía:

El número de secuencia es la forma que utiliza TCP de numerar los mensajes. Sería la numeración de las páginas de nuestro Quijote..

- **Número de acuse de recibo (ACK):** indica el número de secuencia del siguiente byte que se espera recibir. Ocupa 32 bits y es obligatorio. El número ACK - 1 sería el último byte reconocido.
- **Longitud de cabecera (HLEN):** indica el número de palabras de 32 bits (4 bytes) que hay en la cabecera. Ocupa 4 bits y es obligatorio. Por este campo sabemos dónde acaba la cabecera y dónde empiezan los datos. Normalmente el tamaño de la cabecera es de 20 bytes y este campo será 5, este es el valor mínimo y 15 el máximo.

Nota:

Hasta ahora, todos los datos que aparecen en la cabecera son obligatorios y tienen una longitud fija, es decir, el ordenador que recibe la información la puede interpretar perfectamente y sabe qué parte de la cabecera está leyendo en cada momento. Sin embargo, a partir de un cierto momento, el tamaño de los elementos de cabecera son variables, por lo tanto, es necesario indicar en un momento en el que todavía se sabe qué parte del mensaje se está leyendo, cuándo empiezan los datos. Esta es la función de HELEN.

- **Reservado:** está reservado para usos futuros, actualmente se pone a 0. Ocupa 6 bits.



Los paquetes salen ordenados y se desordenan al entrar en el receptor

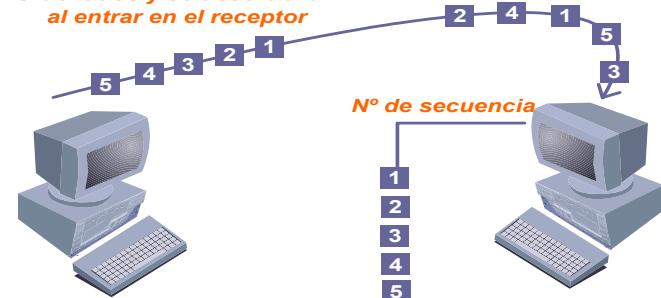


Ilustración 9: Número de secuencia: es el campo que permite ordenar los paquetes de datos al equipo receptor

Anotaciones

- **Indicadores o campos de control:** indican el propósito del segmento. Contienen funciones de control (como, por ejemplo, configuración y terminación de una sesión). Ocupa 6 bits. Cada bit es un indicador y solamente tiene significado cuando su valor es 1. El significado de cada bit es el siguiente:
 - **URG (puntero de urgencia):** Indica que el segmento contiene datos urgentes, esto hace que el número de secuencia se traslade donde están dichos datos. Se complementa con el campo "Marcador urgente", que indica el número de datos urgentes que hay en el segmento.
 - **ACK (acuse de recibo):** Indica que tiene significado el número que hay almacenado en el campo "Número de acuse de recibo".
 - **PSH (push):** Indica que la aplicación ha solicitado enviar los datos almacenados en la memoria temporal, sin esperar a completar el segmento de dimensión máxima.
 - **RST (interrupción de la conexión actual):** sirve para hacer un reset de la conexión. Se usa cuando hay un problema en la conexión, por ejemplo, cuando un paquete llega al receptor y no hay ninguna aplicación esperándolo.
 - **SYN (sincronización de los números de secuencia):** se usa cuando se crea una conexión e indica al otro extremo cuál va a ser el primer número de secuencia con el que va a comenzar a transmitir, que puede ser diferente de cero.
 - **FIN (fin):** indica al destino que ya no hay más datos a transmitir. Se usa para solicitar el cierre de la conexión actual.
- **Ventana:** indica el número de bytes que el emisor está dispuesto a aceptar. Ocupa 16 bits.
- **Checksum TCP:** contiene una suma de comprobación de errores del segmento actual. Se calcula a partir de la cabecera, los campos de datos y las direcciones IP de origen y destino. Ocupa 24 bits. Para poder controlar la fiabilidad de la transmisión de datagramas que forman el mensaje, y detectar los posibles errores y pérdidas de información, se incluye en la cabecera de los mismos un campo de 16 bits, calculado a partir de la información contenida en el datagrama completo, denominado **checksum** (suma de chequeo).

Pendiente: wmf del flash "4rtramatcp1"

Anotaciones

Cuando el equipo destino recibe el datagrama, vuelve a calcular el checksum del mismo, comprobando que es igual que el incluido por el emisor en la cabecera. Si son distintos, el datagrama se ha recibido con errores, por lo que se vuelve a solicitar de nuevo su envío. Si es el mismo, el cliente envía un datagrama de confirmación al servidor, que contiene en su cabecera un campo de validación 32 bits, llamado *Acknowledgment Number*. El servidor está a la espera de la llegada de estos paquetes especiales de confirmación, por lo que, si transcurrido un tiempo determinado, no ha recibido la confirmación correspondiente a un datagrama, lo vuelve a enviar, aunque por razones de eficiencia, los datagramas se suelen enviar sin esperar esta confirmación.

- **Marcador urgente:** indica que se están enviando datos urgentes, que tienen preferencia sobre todos los demás. Indica el siguiente byte del campo datos que sigue a los datos urgentes. Tiene sentido cuando el indicador URG está activo. Un mismo segmento puede contener datos urgentes y normales. Ocupa 8 bits.
- **Opciones:** es opcional. Indica una de las siguientes opciones:
 - Timestamp, para indicar en qué momento se transmitió el segmento. De esta manera se puede medir el retardo del segmento desde el origen hasta el destino.
 - Aumentar el tamaño de la ventana.
 - Indicar el tamaño máximo del segmento que el origen puede enviar.
- **Relleno:** bits de relleno para que el tamaño del segmento TCP sea múltiplo de 32 bits.
- **Datos:** información, propiamente dicha, que envía el origen al destino.

c) Establecimiento de una conexión.

Para abrir la conexión se envían **tres segmentos**, por eso se llama "saludo de tres vías".

1. El ordenador 1(O1), hace una *apertura activa* y envía un segmento TCP (S1), al ordenador 2 (O2). Este segmento lleva el bit SYN activado y el primer nº de secuencia que usará para mandar sus segmentos.

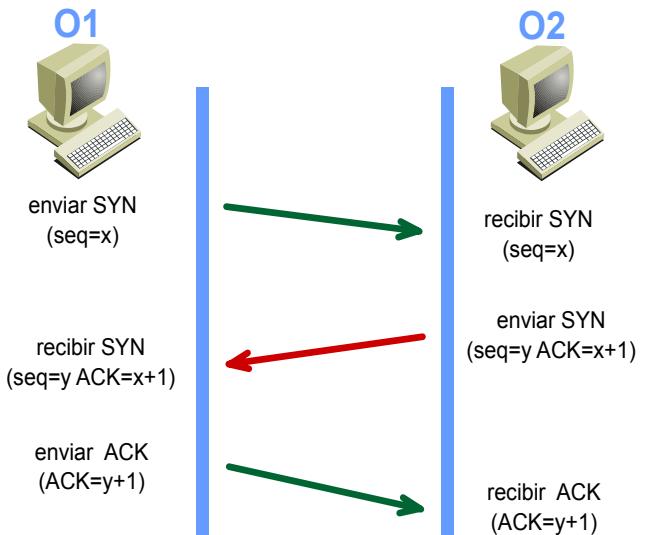


Ilustración 10: Proceso de apertura de conexión

Anotaciones

2. O2 recibe el segmento (S1). Si desea abrir la conexión, responde con un segmento acuse de recibo (ACK), con el bit SYN activado, con ACK = $x + 1$ y con su propio nº de secuencia inicial (y), y deja abierta la conexión por su extremo. Si no desea abrir la conexión, envía un segmento, con el bit RST activado, a O1.
3. O1 recibe el segmento y envía su segmento de confirmación con ACK = $y + 1$.
4. O2 recibe la confirmación y decide que *la conexión ha quedado abierta* y puede enviar mensajes también en el otro sentido.

Los números de secuencia usados (x e y), son distintos en cada sentido y son aleatorios para evitar conflictos.

A partir del paso 4 comienza la transmisión de datos hasta el final. Cuando ya no hay más datos que transferir, hay que *cerrar la conexión*.

d) Control del flujo.

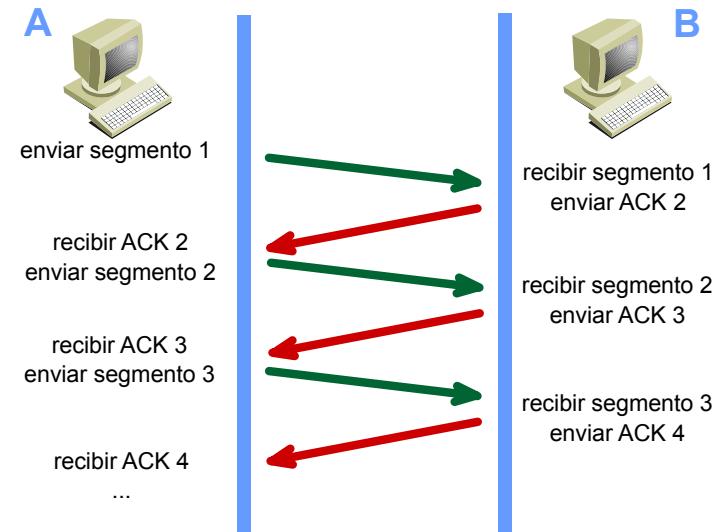
Para controlar el flujo de la transmisión, el protocolo TCP, usa unas técnicas conocidas con el nombre genérico de “*Solicitud de Repetición Automática*” (ARQ), que usan el “*acuse de recibo positivo con retransmisión*” (PAR), mediante el cual el receptor (O2) envía un mensaje de acuse de recibo (ACK), cada vez que recibe un segmento TCP del emisor (O1).

La técnica más simple es, la conocida como *control de flujo mediante sistema de parada y espera*. En esencia funciona así:

1. El ordenador 1(O1), envía un segmento TCP (S1), al ordenador 2 (O2) y espera un ACK antes de enviar el siguiente. También arranca un temporizador con un tiempo de expiración (timeout). Si el temporizador expira antes de que O1 reciba un ACK, retransmite el segmento y reinicia el temporizador.
2. O2 recibe el segmento y envía su segmento de confirmación con ACK.
3. O1 recibe la confirmación y envía el 2º segmento.
4. El proceso continua de esta manera sucesivamente.

Para controlar la transmisión, TCP numera los segmentos secuencialmente. En el receptor, TCP reensambla los segmentos como estaban en el inicio. Si falta algún número de secuencia en la serie, se vuelve a transmitir el segmento con ese número.

La numeración se hace contando los bytes de cada segmento. Si el primer segmento contiene 100 bytes y empezamos numerando con el 0, el siguiente segmento será el número 100.



Anotaciones

Capítulo 4

La cantidad de datos en bytes que se pueden transmitir antes de recibir un ACK se denomina "*tamaño de ventana*".

Con un tamaño de ventana = 1 y ventana simple:

Esta técnica es la más eficaz para evitar errores en la transmisión. Es muy usada cuando se transmiten tramas muy grandes, pero tiene el inconveniente que el canal de transmisión está desaprovechado la mayor parte del tiempo.

Una técnica más avanzada, conocida como "*ventana deslizante*", hace un uso más eficaz del canal de transmisión. En esta técnica el emisor envía varios segmentos sin esperar los ACK correspondientes.

Con un tamaño de ventana negociado = 3 y ventana deslizante:

Una tarea que tiene que realizar el protocolo TCP, es controlar la *congestión* de la transmisión. Para esto controla dinámicamente el tamaño de la ventana, aumentando o disminuyendo su tamaño, para que no haya congestión.

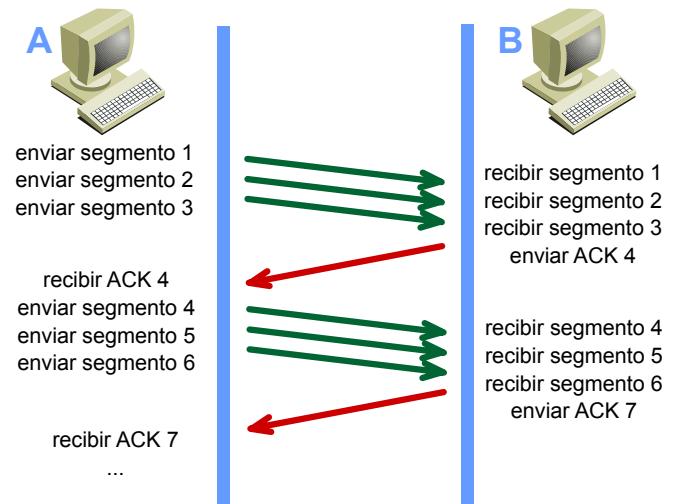
e) Control de errores.

Hay varias técnicas para detectar y corregir los posibles errores en la transmisión. Las más usadas son las siguientes:

- *Comprobación de la paridad*: se añade un bit de paridad a los datos, para que el número de bits con valor 1 sea par. Es un control bastante elemental.
- *Suma de chequeo (checksum)*: se calcula un valor a partir de la cabecera, los campos de datos y las direcciones IP de origen y destino, en el segmento enviado. En el otro extremo, se calcula el mismo valor para el segmento recibido. Los dos valores deben ser iguales, para que la transmisión sea correcta.
- *Comprobación de la redundancia cíclica (CRC)*: si hay un bloque de n bits a transmitir, el emisor le suma los k bits necesarios para que $n + k$ sea divisible por algún número, conocido tanto por el emisor como por el receptor.

Los métodos para informar de que ha habido errores en la transmisión son variados:

- *Confirmaciones positivas*: el receptor devuelve un acuse de recibo positivo (ACK), por cada segmento recibido correctamente. Se usa para detectar y solicitar el reenvío de tramas perdidas.



Anotaciones

- **Confirmación negativa y transmisión:** el receptor confirma sólamente los segmentos recibidos erróneamente, para que el emisor las vuelva a enviar de nuevo.

Para pensar:

Supongamos que hemos inventado una clave secreta en la que cada dos dígitos en sistema decimal significan una letra, si enviáramos un mensaje con cuatro dígitos sabemos que es una palabra de dos letras, pero, ¿cómo comprobamos que el mensaje que nos llega es correcto? Nos ponemos de acuerdo emisor y receptor para añadir, por ejemplo, 10 dígitos más al final del mensaje, de manera que estos últimos dígitos se obtengan sumando los números que efectivamente corresponden al mensaje, los cuatro primeros.

- Un mensaje correcto sería el siguiente: 12340000000010. $1+2+3+4=10$
- Un mensaje erróneo sería 24530000000045. $2+4+5+3 \neq 45$

Así podemos saber siempre si el mensaje, debido a alguna alteración en el proceso de transmisión, ha sido modificado.

Analogía:

En una conversación telefónica representaría cuando una persona dice "lo siento, ¿podrías repetir?"

- Expiración de intervalos de tiempo (timeout): El emisor arranca un temporizador con un tiempo de expiración (timeout). Si el temporizador expira antes de que el emisor reciba un ACK por parte del receptor, retransmite el segmento y reinicia el temporizador.

f) Cierre de la conexión.

El proceso es una variación del *saludo de tres vías*:

1. O1ya no tiene más datos para transferir. Envía un segmento TCP con el bit FIN activado y cierra la conexión activa, en el sentido de envío. La recepción está abierta todavía.



Ilustración 13: Checksum es el campo que permite averiguar si los datos de la trama TCP contienen errores

Anotaciones

2. O2 recibe el segmento, informa a la aplicación receptora del cierre y devuelve la confirmación (ACK) a O1.
3. O1 recibe el ACK de O2.
4. O2 decide cerrar la comunicación y envía un segmento TCP con el bit FIN activado.
5. O1 lo recibe y envía un ACK a O2.
6. O2 lo recibe y cierra la conexión definitivamente.

g) Puertos y Zócalos (Sockets).

La noción de **puerto**, es introducida por la capa de transporte para distinguir entre los distintos destinos, dentro del mismo host, al que va dirigida la información.

La capa de red solamente necesita, para dirigir la información entre dos ordenadores, las direcciones IP del origen y el destino. La capa de transporte añade la noción de puerto .

Un ordenador puede estar ejecutando a la vez varios procesos distintos, por ello no es suficiente indicar la dirección IP del destino, además hay que especificar el puerto al que va destinado el mensaje.

Cada aplicación utiliza un número de puerto distinto. Cuando una aplicación está esperando un mensaje, lo hace en un puerto determinado, se dice que está "escuchando un puerto".

Analogía:

Podemos imaginar el concepto de puerto como el de un andén en una estación de trenes. El destino es el mismo, por ejemplo Zaragoza, sin embargo, los trenes se detienen en andenes distintos dentro de la misma estación y es allí donde se bajan los pasajeros y las mercancías, será un andén distinto si se llega de Madrid o de Barcelona, si se es un pasajero, el correo, un vehículo, etc.

Un puerto es un número de 16 bits, por lo que existen $2^{16}=65536$ números de puerto posibles, en cada ordenador. Las aplicaciones utilizan estos puertos para enviar y recibir mensajes. Se llama *conversación* al enlace de comunicaciones entre dos procesos.

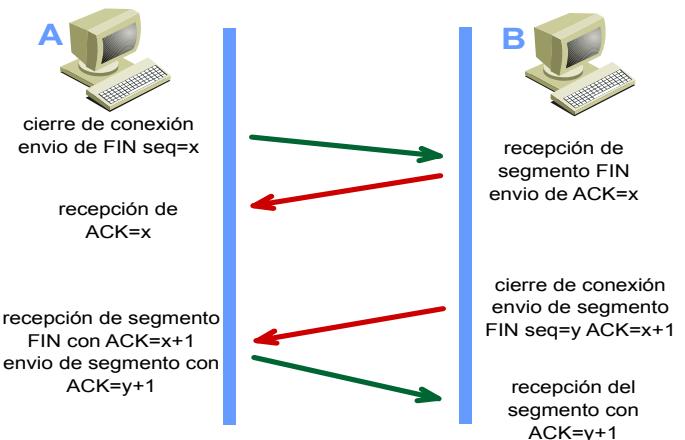


Ilustración 14: ACK: el número de acuso de recibo ACK tiene múltiples utilidades, una de ellas es para cerrar la conexión

Anotaciones

Aparte del concepto de puerto, la capa de transporte, usa el concepto de **socket o zócalo**. Los sockets son los puntos terminales de una comunicación, que pueden ser nombrados y direccionados en una red. Un socket está formado por la dirección IP del host y un número de puerto.

Una dirección de socket está formada por la tripleta:

{protocolo, dirección local, proceso local}

Por ejemplo, en el protocolo TCP/IP un socket sería: {tcp, 193.53.214.3, 1345}

Si una aplicación cliente quiere comunicarse con una aplicación servidora de otro host, el protocolo TCP, le asigna un número de puerto libre, en el otro extremo, la aplicación servidora permanece a la escucha en su puerto bien conocido. Por ejemplo, el envío de correo con el protocolo POP3, utiliza el número de puerto 110.

Para que la transmisión sea más eficaz, los puertos usan una memoria intermedia, llamada "*buffer*". Existe un buffer en el origen, usado por la aplicación cliente, y otro en el destino, donde se van almacenando los datos enviados hasta que los pueda recoger la aplicación receptora. Los buffers son embalses que contienen o dejan salir el caudal de información.

Nota:

Es lógico que se necesite un buffer que almacene los paquetes según llegan, ya que lo hacen desordenados, y no se puede procesar el mensaje hasta que no se completa en un determinado orden.

Con el comando **netstat**, podemos ver las conexiones activas y los sockets en uso.

Para pensar:

Ejecuta el comando netstat. ¿qué datos te aporta?

Los primeros 256 puertos son los llamados "*puertos bien conocidos*" (well-known), y se usan para servicios comunes, como HTTP, FTP, etc. TCP asigna los números de puerto bien conocidos, para aplicaciones servidoras (aquellas que ofrecen servicios) y el resto de los números disponibles a las aplicaciones cliente (aquellas que solicitan servicios), según los van necesitando.

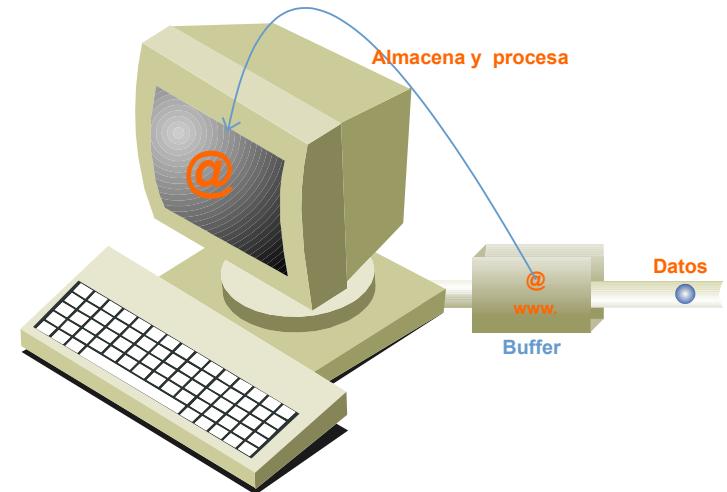


Ilustración 15: Los buffers son una memoria intermedia en donde se almacenan los datos hasta que pueden ser procesados por la aplicación correspondiente

Anotaciones

Capítulo 4

Los números de puerto tienen asignado los siguientes intervalos :

- Del 0 al 255 se usan para aplicaciones públicas.
- Del 255 al 1023 para aplicaciones comerciales.
- Del 1023 en adelante, no están regulados.

Los puertos bien conocidos están definidos en la RFC 1700 y se pueden consultar en <http://www.ietf.org/rfc/rfc1700.txt>

Estos puertos son controlados y asignados por IANA ("Internet Assigned Numbers Authority").

Los más usuales son:

Palabra clave	Puerto	Descripción
cho	7/tcp/udp	Eco
daytime	13/tcp/udp	Fecha y hora
ftp	21/tcp	Protocolo de Transferencia de Ficheros
telnet	23/tcp	Telnet
smtp	25/tcp	Protocolo de correo sencillo
domain	53/TCP-UDP	Servidor de nombres de dominio (DNS)
gopher	70/TCP	Gopher
www-http	80/TCP	World Wide Web HTTP (servicio de páginas web)
pop3	110/TCP	Post Office Protocol - Versión 3
irc	194/TCP	Internet Relay Chat Protolol (Protocolo de Internet para Chat)

h) Puertos y seguridad.

Al ser los puertos las "puertas" de entrada a un ordenador, pueden usarse por los "piratas" para sus ataques. Son puntos vulnerables. Se recomienda que, en general, no se tengan más puertos abiertos que los que sean imprescindibles.

El ataque puede ser directamente al ordenador cliente, o al servidor a través de éste. Hay diversas aplicaciones usadas por los piratas informáticos, para accesos no autorizados. Se basan, generalmente, en la apertura de puertos de número mayor que 1023 para estos accesos.

Es conveniente, por lo tanto, comprobar los puertos que tenemos abiertos, con **netstat** por ejemplo, y cerrar los que no necesitemos.

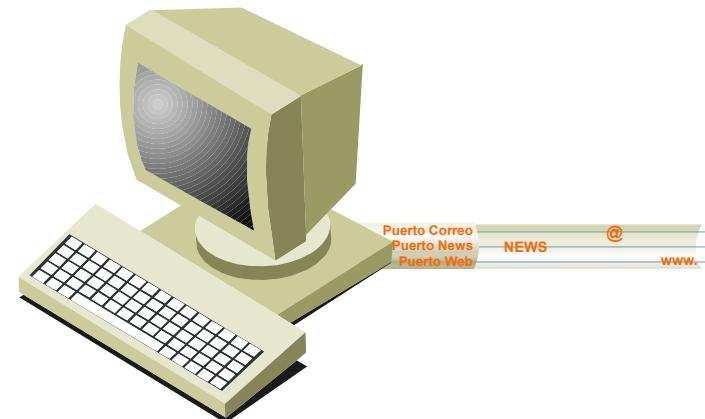


Ilustración 16: Puerto: un equipo dispone de distintas destinos que deben ser identificados para que los paquetes de datos lleguen correctamente

Anotaciones

3.3. Protocolo UDP.

a) Introducción

El Protocolo de Datagrama de Usuario (UDP). Proporciona una comunicación sencilla entre dos ordenadores, y que no consume muchos recursos. Es un protocolo que pertenece a la capa de transporte.

Es un protocolo:

- **No confiable:** no hay un control de paquetes enviados y recibidos. Estos pueden llegar erróneos o no llegar a su destino.
- **No orientado a conexión:** no se realiza una conexión previa entre origen y destino, como ocurre en el protocolo TCP.

Este protocolo se describe en: <http://www.rfc-es.org/rfc/rfc0768-es.txt>

Es un protocolo útil, en casos en los que no es necesario mucho control de los datos enviados. Se usa cuando la rapidez es más importante que la calidad, en los casos en que la información cabe en un único datagrama. Una de sus usos más comunes es el envío de mensajes entre aplicaciones de dos ordenadores. No es tan fiable como el protocolo TCP, pero es simple, con baja sobrecarga de la red, y por lo tanto ideal para aplicaciones que usen masivamente la red, como DNS y SNMP.

Utiliza el protocolo IP para transportar los mensajes, es decir, va encapsulado dentro de un datagrama IP. No añade ninguna mejora a este protocolo, en cuanto a control de errores.

Incorpora los puertos origen y destino en su formato. El número de puerto de destino, en la cabecera UDP, se utiliza para dirigir el datagrama UDP a un proceso específico, que se está ejecutando en el ordenador destino. El número de puerto origen, permite al proceso contestar adecuadamente.

No controla errores, cuando se detecta un error en un datagrama, se descarta. Esto hace que deban ser las aplicaciones que lo usen, las que controlen los errores, si les interesa.

UDP no numera los datagramas, tampoco utiliza confirmación de entrega, como ocurre en TCP. Esto hace que no hay garantía de que un paquete llegue a su destino, ni que los datagramas puedan llegar duplicados o desordenados a su destino.

Anotaciones

Nota:

Una de las aplicaciones que usa el protocolo UDP es la solicitud de DNS. Cada vez que un usuario solicita la conexión a un host, lo hace escribiendo en el navegador la dirección DNS, sin embargo, esa dirección no puede circular por la red, ya que para ello se emplean direcciones IP. Así, se pide a un servidor de DNS que indique cuál es realmente la dirección IP del equipo al que nos queremos conectar.

b) Formato del segmento UDP.

El formato del segmento UDP es el siguiente:

El significado de cada campo es:

- **Puerto UDP de origen:** especifica el puerto del host origen. Ocupa 16 bits.
- **Puerto UDP de destino:** especifica el puerto del host destino. Ocupa 16 bits.
- **Longitud del datagrama:** especifica la longitud en bytes del datagrama, incluyendo la cabecera. La longitud mínima es de 8 bytes. Ocupa 16 bits.
- **Checksum UDP (Suma de verificación):** en él se almacena una suma de comprobación de errores del datagrama, que se calcula a partir de una pseudo-cabecera, que incluye las direcciones IP origen y destino. En redes Ethernet es corriente que no se calcule el checksum y puede ser ignorado.
- **Datos:** contiene los datos que se envían las aplicaciones

Los datagramas van quedando en una cola, de la que va leyendo la aplicación destino. Si el puerto no estuviera abierto o se sobrepasara la capacidad de la cola, los datagramas serían ignorados.

Algunas situaciones en las que es más útil el protocolo UDP, son:

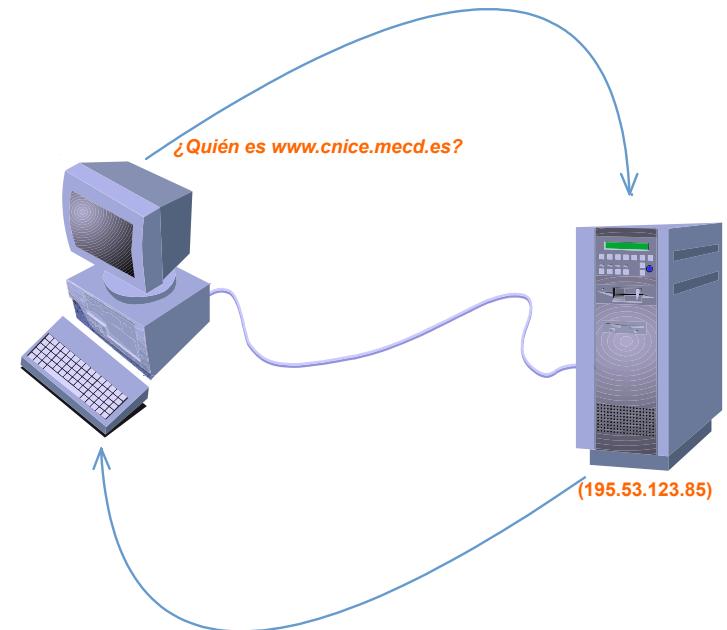


Ilustración 17: Solicitud de dirección IP a servidor para traducir direcciones de dominio

Anotaciones

- Aplicaciones en *tiempo real* como audio o video, donde no se admiten retardos.
- Situaciones en las que se necesita conectar con un ordenador de la propia red, usando una IP interna o un nombre. Habría que conectar primero con el servidor de red apropiado que transforme dicha dirección en una dirección IP válida.
- Consultas a servidores en las que se envían uno o dos mensajes solamente, como es el caso del DNS.
- En transmisiones en modo multicast (a muchos destinos), o en modo broadcast (a todos los destinos), ya que si todos los destinos enviaran confirmación el emisor se colapsaría.

Entre los protocolos superiores que usan UDP están: DNS (Domain Name Server), SNMP (Simple Network Management Protocol), TFTP (Trivial File Transfer Protocol), NFS (Network File System), etc.

Analogía:

Nos encontramos en la sala de profesores y suena el teléfono en secretaría, entonces, una persona que parece estar más ocupada dice "Carlos, ¿puedes coger el teléfono?", no se ha preocupado si Carlos le ha oído, simplemente le llama y espera a que coja el teléfono, no se ha preocupado de llamarle, esperar que le conteste y decirle lo que desea que haga.

3.4. Protocolo IP.

a) Definición. Características.

<http://www.rfc-es.org/rfc/rfc0791-es.txt>

Este protocolo, funciona transmitiendo la información por medio de paquetes. A este sistema se le conoce como "catenet". Da las normas para la transmisión de bloques de datos llamados **datagramas**, desde el origen al destino. Para hacer esto, identifica a los host origen y destino por una dirección de longitud fija, llamada **dirección IP**. Se encarga también, si fuera necesario, de la fragmentación y reensamblaje de grandes datagramas para su transmisión por redes de trama pequeña. Es un protocolo que pertenece a la capa de red.

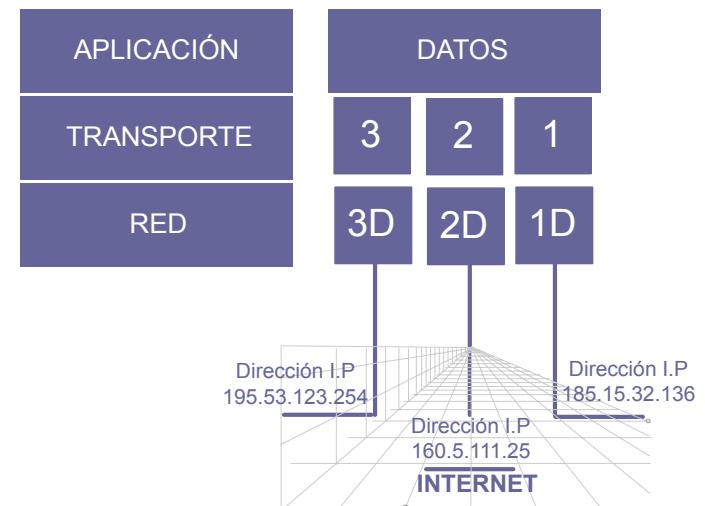


Ilustración 18: La IP presta servicio de transporte de red a TCP

Anotaciones

Para pensar:

Si queremos conectar nuestro ordenador a Internet, debemos asignarle una dirección IP para que sea reconocido por el resto de los ordenadores interconectados a la red, además, deberemos instalar el protocolo IP, ya que de otra forma sería imposible que los paquetes de datos pudieran ser transmitidos a través de Internet.

Es un *sistema de conmutación de paquetes no orientado a conexión*, ya que cada paquete viaja independientemente de los demás; *no fiable*, los paquetes se pueden perder, duplicar o cambiar de orden. Es decir este protocolo no soluciona estos problemas, esta tarea queda para otros protocolos.

Este protocolo utiliza, a su vez, protocolos de redes locales, que se encargan de llevar el datagrama IP a través de la red local hasta su salida, por medio de una pasarela (*gateway*), hasta la próxima red.

El protocolo IP realiza dos funciones básicas: **direcciónamiento y fragmentación**.

- Cada datagrama IP tiene una cabecera en la que figuran la dirección de origen y de destino. El módulo internet usa estas direcciones para llevar el datagrama hasta su destino. Este proceso se llama *encaminamiento o enrutamiento*.
- El módulo Internet usa campos en la cabecera para fragmentar y reensambla los datagramas IP, si fuera necesario, para su transmisión por redes de trama pequeña.

Nota:

En función de la tecnología de transmisión empleada, las redes admiten un tamaño máximo de paquete de datos. Las máquinas que interconectan las redes (los routers) deben encargarse que los datagramas que entran en una red sean soportados por esta, por lo que pueden llegar a dividir los paquetes. Si un paquete de datos se divide, ya no se vuelve a unir hasta llegar a su destino, aunque vuelva a circular por redes que permitan mayor tamaño en los datagramas..

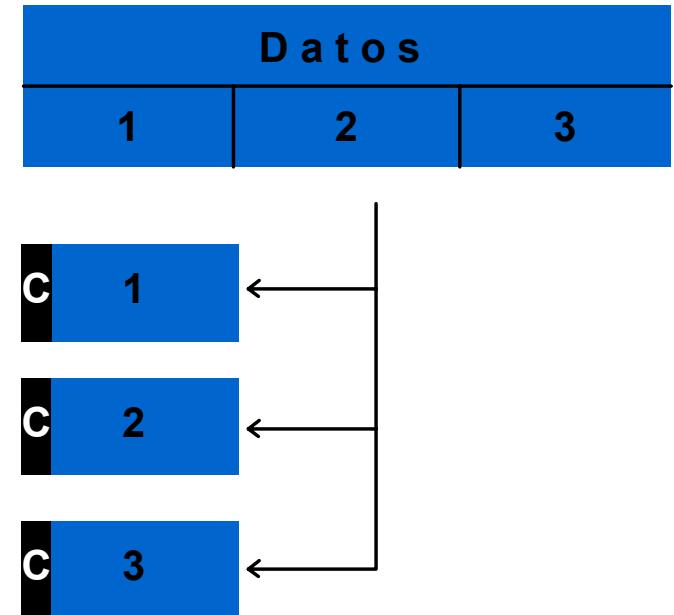


Ilustración 19: Fragmentación es cuando los requisitos de la red lo hacen necesario IP divide los paquetes añadiéndolas una cabecera de datos IP

Anotaciones

En cada host y en cada pasarela que interconecta redes, reside un módulo Internet. Estos módulos tienen reglas comunes para interpretar las direcciones y para fragmentar y reensamblar los datagramas IP. Estos módulos, en las pasarelas, saben cómo encaminar los datagramas IP.

Cada datagrama IP, se trata como una entidad independiente, no relacionada con ningún otro datagrama IP. No existen conexiones o circuitos lógicos (virtuales o de cualquier otro tipo).

Analogía:

El protocolo IP actúa como los señalizadores en un vía pública. No saben si los coches que circulan por la calle llegan o no llegan a su destino, simplemente informan, si usted quiere ir al zoo, vaya por allí, hasta que se vuelva a encontrar otro cartel indicador o haya llegado ya. Así todos los carteles, uno tras otro, hasta que el coche llega a su destino.

El protocolo Internet utiliza cuatro mecanismos clave para prestar su servicio: **Tipo de Servicio, Tiempo de Vida, Opciones y Suma de Control de Cabecera**.

- El **Tipo de Servicio** se utiliza para indicar la calidad del servicio deseado como prioridad, retardo, rendimiento, etc.
- El **Tiempo de Vida** es una indicación de un límite superior en el periodo de vida de un datagrama IP. Es fijado por el remitente del datagrama y reducido en 1 en cada router que atraviesa en su camino. Si el tiempo de vida se reduce a cero antes de que llegue a su destino, el datagrama IP es destruido.
- Las **Opciones** proporcionan funciones de control necesarias o útiles en algunas situaciones. No son obligatorias.
- La **Suma de Control de Cabecera** sirve para verificar que la información ha sido transmitida correctamente. Si la suma de control de cabecera falla, el datagrama IP es descartado.

Este control es sólo para la cabecera, no hay control de error para los datos en este nivel. El protocolo Internet no proporciona ningún mecanismo de comunicación fiable, no existen acuses de recibo entre extremos, ni entre saltos. No existe control de flujo.

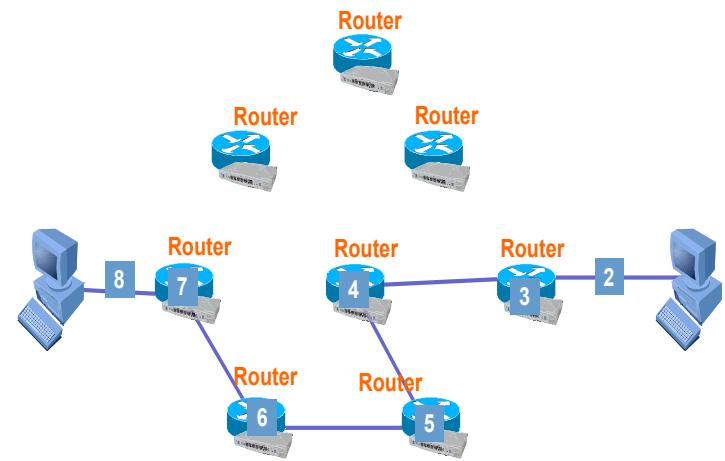
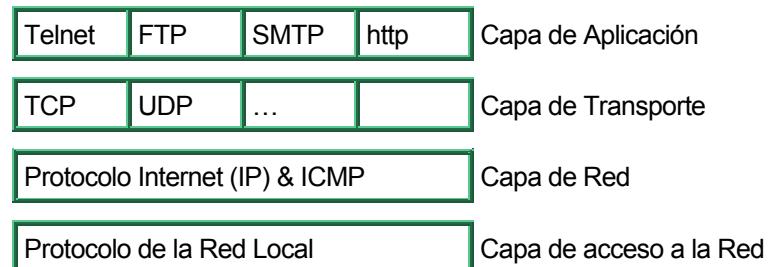


Ilustración 20: El tiempo de vida de un paquete de datos determina el nº máximo de veces que puede cambiar de red un datagrama IP

Anotaciones

b) Relación con otros Protocolos.

El siguiente diagrama ilustra el lugar del Protocolo Internet en la jerarquía de protocolos:



El protocolo Internet interactúa por un lado con los protocolos de la capa de transporte y por otro con el protocolo de la red local.

c) Modo de Operación.

Para transmitir un datagrama de una aplicación a otra, procede de la siguiente manera:

Supongamos dos hosts, que quieren intercambiar información; cada uno estará integrado en su respectiva red local, y supongamos que haya una pasarela intermedia entre ambos.

La aplicación remitente prepara sus datos y llama a su módulo internet local, que se encargará de enviar esos datos como datagramas IP, para ello, prepara la cabecera del datagrama y adjunta los datos a él con la dirección de destino y otros parámetros como argumentos de la llamada. Decide, por la dirección IP del destino, que debe enviarlo a la pasarela de la red local primera y lo envía a la interfaz de red local. Esta, crea una cabecera de red local (según las normas del protocolo de red la red local que sea), le adjunta el datagrama y envía el resultado a través de la red local.

El datagrama llega a la pasarela encapsulado en la cabecera de red local.

Esta pasarela, a su vez llama a su módulo internet. Este, comprueba si el datagrama debe ser reenviado a otro host en una segunda red. Así sucesivamente, hasta llegar a la red local a la que pertenece el host de destino.

Este host, a su vez, llama a su módulo internet, que lo pasa a la aplicación a la cual va dirigido el datagrama, en este host. Pasa los datos a la aplicación en respuesta a una llamada del sistema, pasando la dirección de origen y otros parámetros como resultado de la llamada.

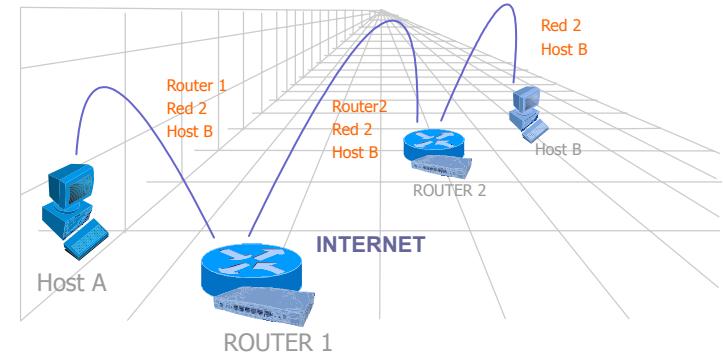


Ilustración 21: Los datagramas IP incluyen la dirección de red de los dispositivos que hacen de pasarela entre redes hasta que lleguen a la red de destino

Anotaciones

Capítulo 4: Internet

Como vemos, los datagramas van pasando desde un módulo internet a otro hasta que se alcanza el destino. En el camino puede haber distintas redes interconectadas. Los módulos internet residen en hosts y pasarelas.

Todo este proceso se basa en la interpretación de una dirección internet. Por eso, un importante mecanismo del protocolo IP es la **dirección internet**.

En su ruta, los datagramas pueden necesitar atravesar una red cuyo tamaño máximo de paquete es menor que el tamaño del datagrama. Para salvar esta dificultad, el protocolo IP proporciona un mecanismo de fragmentación.

d) Formato de un Datagrama IP.

El datagrama IP viaja encapsulado en el campo de datos de las tramas físicas (Ethernet), de las distintas redes que va atravesando. Estas tramas físicas pueden ser distintas, dependiendo del tipo de red. De este modo, un mismo datagrama IP, puede atravesar redes distintas: redes Ethernet, ATM, Token Ring, Frame Relay, enlaces punto a punto, etc.

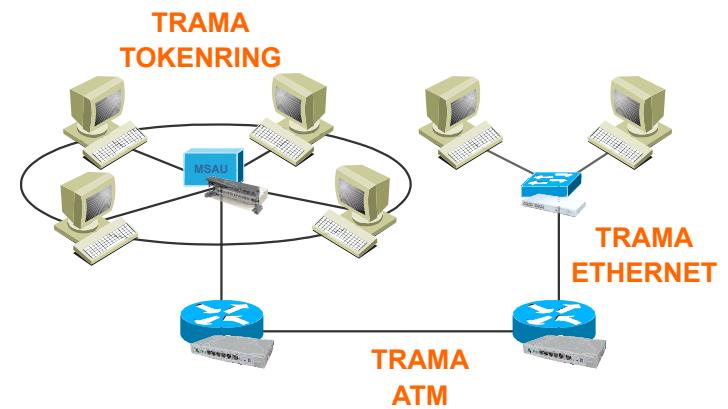
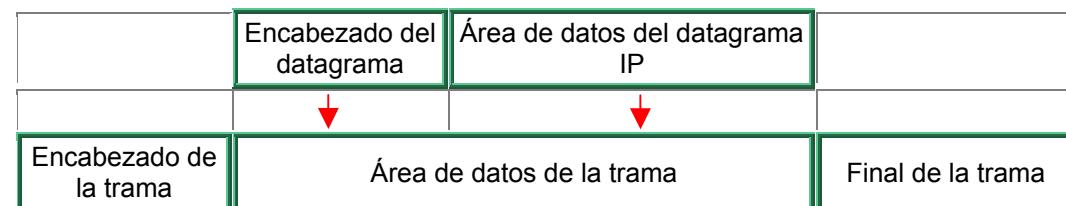


Ilustración 22: IP puede viajar encapsulado en tramas distintas en función del tipo de red por el que se mueve

Anotaciones

Campos del datagrama IP

- **Versión (4 bits)**. Indica la versión del protocolo IP utilizado. Actualmente se utiliza la versión 4 (IPv4), aunque ya se está preparando la siguiente versión, la 6 (IPv6).
- **IHL (4 bits)**. Longitud de la Cabecera Internet, expresada en palabras de 32 bits. Apunta al comienzo de los datos. El valor mínimo es 5, correspondiente a 160 bits = 20 bytes.
- **Tipo de servicio (Type Of Service) (8 bits)**: indica la prioridad, retardo, rendimiento, etc.
- **Longitud total (16 bits)**: indica la longitud total del datagrama, expresada en bytes (8 bits), incluye la longitud de la cabecera y los datos. Como el campo tiene 16 bits, la máxima longitud posible de un datagrama será de 65535 bytes.
- **Identificación (16 bits)**: número de secuencia del datagrama. Si se tratara de un datagrama fragmentado, llevaría la misma identificación que los otros fragmentos.
- **Flags o indicadores (3 bits)**: son indicadores de control. El bit (MF) indica que hay más fragmentos. El bit (NF) prohíbe la fragmentación del datagrama.
- **Posición del fragmento (13 bits)**: indica la posición del fragmento actual dentro del datagrama completo, medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor de cero.
- **Tiempo de vida o TTL (8 bits)**: tiempo máximo que puede estar el datagrama en Internet. Cada vez que el datagrama atraviesa un router se resta 1 a este número. Cuando llegue a cero, el datagrama se descarta y se devuelve un mensaje ICMP de tipo "tiempo excedido" para informar al origen, y se descarta el datagrama.
- **Protocolo (8 bits)**: indica el protocolo del siguiente nivel utilizado en el campo de datos: 1 para ICMP, 2 para IGMP, 6 para TCP y 17 para UDP.
- **Suma de control de cabecera (CRC) (16 bits)**: para comprobar si hay errores en la cabecera del datagrama. La verificación de errores de los datos corresponde a las capas superiores.



Ilustración 23: Los datagramas IP viajan encapsulados en tramas de datos de las capas físicas (Ethernet, ATM, ...) cada vez que llega a otra red un dispositivo de red desencapsula los datos y los reenvía en función del encabezado del datagrama (red de destino)

Anotaciones

- **Dirección origen (32 bits)**: contiene la dirección IP del origen.
- **Dirección destino (32 bits)**: contiene la dirección IP del destino.
- **Opciones**: distintas opciones especificadas por el origen, referidas generalmente a pruebas de red y depuración. Este campo es opcional.
- **Relleno (variable)**: se usa para que la longitud de la cabecera Internet sea múltiplo de 32 bits.

A continuación de estos campos, van la auténtica información que se quiere transmitir.

Explicación ampliada en <http://www.rfc-es.org/rfc/rfc0791-es.txt>

Para pensar:

¿Serías capaz de escribir un ejemplo de secuencia de bits de un encabezado de datagrama IP? Tal como lo hemos hecho con el protocolo TCP

Direccionamiento.

Hay una distinción entre nombres, direcciones y rutas.

- Un **nombre** indica qué buscamos.
- Una **dirección** indica dónde está.
- Una **ruta** indica cómo llegar allí.

El protocolo IP maneja únicamente direcciones, la **dirección Internet**. Es tarea de los protocolos de mayor nivel, hacer corresponder nombres con direcciones.

El módulo internet hace corresponder direcciones de internet con direcciones de red local.

Es tarea de los protocolos de menor nivel (de red local o pasarelas) realizar la correspondencia entre direcciones de red local y rutas.

Dirección Internet.

Explicación ampliada en: <http://www.rfc-es.org/rfc/rfc0791-es.txt>

Cuando queremos enviar un mensaje a través de un sistema de redes no podemos emplear la dirección física de la tarjeta ya que no existe un modo estandarizado de identificar un host dentro de una red, dentro de un sistema de múltiples redes, que sea efectivo. Así, se ha ideado la dirección IP, que permite identificar la red en la que se encuentra el ordenador y, a la vez, ubicar la posición de este PC dentro de la red.

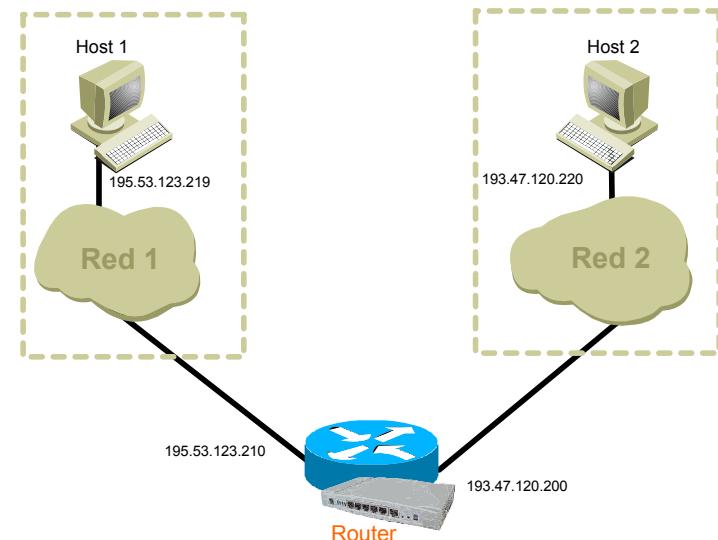


Ilustración 24: El protocolo IP maneja como únicas direcciones, la dirección de Internet

Anotaciones

Nota:

Pensar en el sistema de numeración binario es complejo, a pesar de utilizar únicamente dos números, el 1 y el 0. Con estos números tendríamos que realizar todas las operaciones. Así, el simple hecho de contar sería, 0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011,...

Cuando llegamos a 11111111 nos estamos refiriendo al número 255 en el sistema decimal y lo obtendríamos asignando a cada dígito de 111111111 el valor de la potencia de dos con el exponente en valor decimal.

10000000	2^7	128
1000000	2^6	64
100000	2^5	32
10000	2^4	16
1000	2^3	8
100	2^2	4
10	2^1	2
1	2^0	1
11111111	$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$	255

Así el número binario 11111111 equivale al 255 decimal, pero permite 256 valores puesto que se cuenta desde el 0 al 255.

El sistema de direccionamiento IP consiste tal como hemos indicado en una serie de dígitos. Como es el sistema que se emplea para identificar cualquier servidor en Internet, cuando quisieramos conectar con un equipo, deberíamos identificarlo por esta serie de números, en muchos casos, difíciles de recordar. Así, se desarrolló el sistema de identificación por nombres de dominio. De esta manera, las direcciones del nivel de red en Internet pueden representarse de manera simbólica o numérica. Una dirección simbólica es por ejemplo www.cnice.mecd.es. Una dirección numérica se representa por cuatro campos separados por puntos, como 193.144.238.1, no pudiendo superar ninguno de ellos el valor 255 (11111111 en binario). La correspondencia entre direcciones simbólicas y numéricas las realiza el **DNS** (Domain Name System).

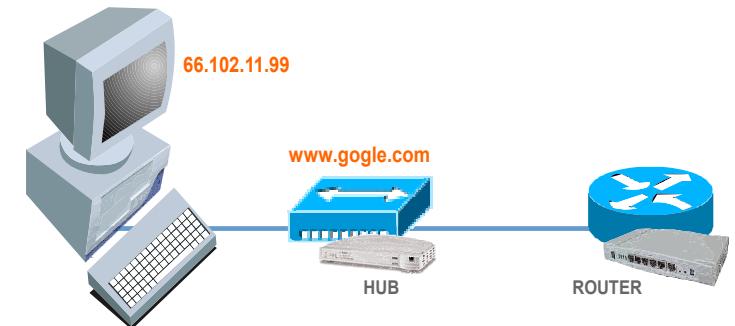


Ilustración 25: Las direcciones IP pueden tener una correspondencia con direcciones de nombre de dominio

Anotaciones

Para pensar:

Cuando configuramos un acceso a Internet, en un momento dado debemos introducir las direcciones DNS, se trata de direcciones IP de host donde se almacena una base de datos con la traducción de nombres de dominio a direcciones IP. Estamos diciendo en qué servidor queremos que se busque la información para realizar la traducción.

Para poder identificar una máquina en Internet cada una de ellas tiene una **dirección IP** (Internet Protocol) la cual es asignada por **IANA**, organismo internacional encargado de asignar las direcciones IP públicas, aunque se dedica a asignar las direcciones de red de las empresas y estas ya se encargan de administrar sus equipos.

Las direcciones numéricas son las que entiende la máquina y se representan por 32 bits con 4 campos de 8 bits cada uno, aunque normalmente se pasan de binario a decimal. Por ejemplo 139.3.2.8 es en numeración binaria:

10001011	00000011	00000010	00001000	Binario
139	3	2	8	Decimal

Cualquier dirección IP de un host tiene dos partes, por un lado, aquella que identifica la red a la que pertenece el ordenador y por otro, el ordenador dentro de la red en la que se encuentra. Debemos analizar este sistema desde la perspectiva de la gran cantidad de ordenadores que existen conectados a Internet.

Analogía:

La forma de determinar las direcciones IP sería muy similar al antiguo sistema de matriculación de un coche, donde las primeras letras indicarían la provincia, y el resto el coche en concreto, que es distinto si pertenece a León o a Murcia.

- LE-3456-A
- MU-3456-A

Son dos coches distintos que pertenecen a provincias distintas. Lo mismo sucedería con las direcciones IP.

La diferencia radica en que existen distintos tipos de redes y es necesario determinar qué parte de la dirección IP pertenece a la red y cual al ordenador.

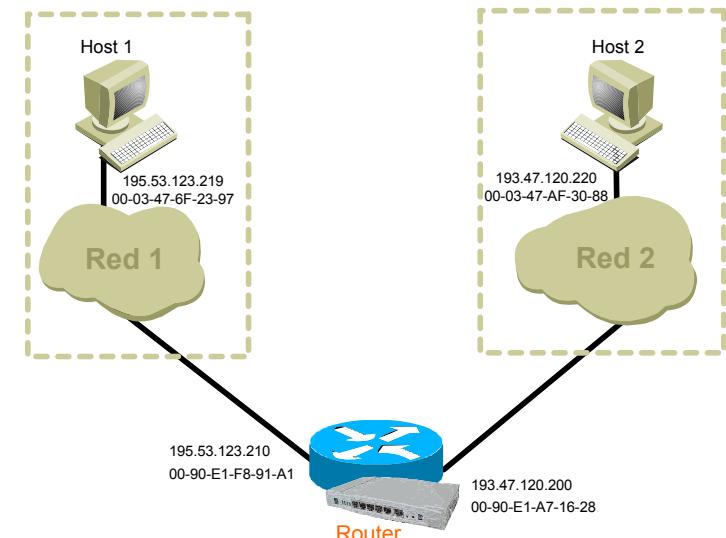


Ilustración 26: La dirección IP identifica direcciones de Internet, pero viaja acompañada de la dirección física del dispositivo de red al que se dirige el paquete.

Anotaciones

Capítulo 4

Para determinar qué parte de la dirección de Internet se refiere a la red y cuál pertenece al ordenador debemos introducir la máscara de subred que nos permite identificar los dígitos de la dirección IP que pertenecen a cada una de sus partes.

El sistema para realizar esta distinción es el siguiente. Si la dirección IP se compone de cuatro grupos de ocho bites, creamos una máscara en la que, de alguna forma se nos indica cuáles de esos bites pertenecen a la red y cuales al host. Los dígitos de valor uno de la máscara de subred indican la parte de la dirección IP que identifica la red, y los de valor cero, indican el ordenador. Así, la dirección IP de un equipo siempre debe estar asociada a una máscara de subred.

Máscara de subred	11111111	11111111	11111111	00000000
Dirección IP	11000000	10101000	00000000	10101100
Significado	Red			Ordenador

Para pensar:

¿Serías capaz de, empleando la calculadora de Windows (Ver ▶ Científica) sustituir los valores que te hemos puesto en el ejemplo y que se encuentran en el sistema de numeración binario por sus valores decimales? Escribe el resultado.

Máscara de subred				
Dirección IP				
Significado	Red			Ordenador

Para pensar:

Cuando introducimos en una configuración de red la máscara de subred estamos indicando a todo el mundo a qué red pertenece nuestro ordenador y cómo identificarlo dentro de la misma.

Por ejemplo:

Dirección IP	192.168.0.100
Máscara de subred	255.255.255.0

Es la red 192.168.0 y el equipo 100 dentro de esta red

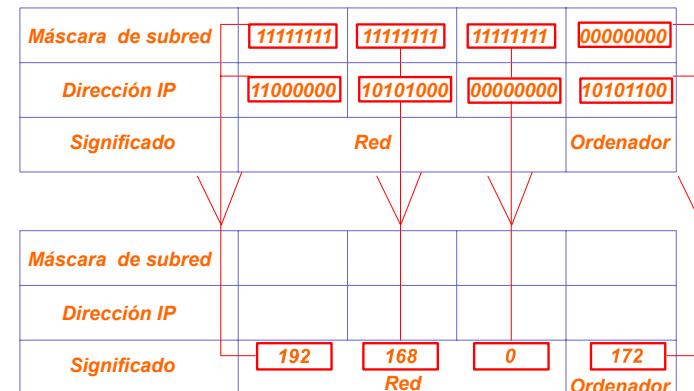


Ilustración 27: La máscara de subred define la parte de la dirección IP que corresponde a la red y la que corresponde al equipo

Anotaciones

Clases de direcciones IP.

Como ya hemos explicado, una parte de los bits representa la red y el resto la máquina (host). Existen cinco clases de direcciones IP según la manera de repartir los bits entre la dirección de red y el número de host.

Esta idea pretende asignar direcciones de red que se adapten a las necesidades de los usuarios. Así, si tenemos una red en donde la máscara de subred es del tipo 255.0.0.0, puede llegar a tener 256³ mientras que si la máscara de subred es 255.255.255.0 sólo podrá haber 256 direcciones de host distintas.

Utilizando las direcciones IP y las máscaras de subred podemos definir tres tipos de redes.:

	Máscara de subred	Dirección de red	Número	
			Redes	Host
Clase A	255.0.0.0	0xxxxxx	127	16.777.214
Clase B	255.255.0.0	10xxxxxxxx.xxxxxxxxxx	16.384	65.534
Clase C	255.255.255.0	110xxxxx.xxxxxxxxxx.xxxxxxxxx	2.097.151	254

En estas clases las direcciones con la parte de número de host con todos los bits puestos a '0' indican la red por lo que no se pueden asignar a ningún host; igualmente tampoco se pueden asignar a un host las direcciones con el número de host con todos los bits puestos a '1' porque se dejan para los paquetes broadcast dirigidos a todas las máquinas de la red. Por ejemplo en la red anterior que es clase B la red es 139.3.0.0 y la dirección broadcast 139.3.255.255.

- Las direcciones de Clase A usan 7 bits para el número de red dando un total de 126 (128-2) posibles redes de este tipo ya que la dirección 0.0.0.0 se utiliza para reconocer la dirección de red propia y la red 127 es la del lazo interno (loopback) de la máquina. Los restantes 24 bits son para el número de host (quitando las que son todos los bits a 0 ó a 1), con lo cual tenemos hasta $2^{24}-2=16.777.216-2=16.777.214$ direcciones. Son las redes 1.0.0.0 a 126.0.0.0
- Las direcciones de Clase B utilizan 14 bits para la dirección de red (16.382 posibles redes de este tipo) y 16 bits para el host (hasta 65.534 máquinas). Son las redes 128.0.0.0 a 191.255.0.0

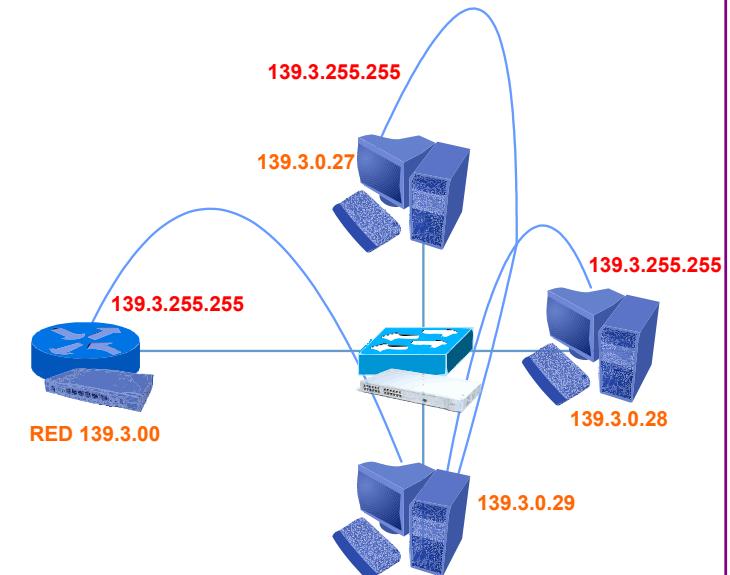


Ilustración 28: Red Clase B se realiza un mensaje de Broadcast poniendo a 1 los dos últimos octetos de la dirección IP

Anotaciones

- Las direcciones de clase C tienen 21 bits para la red (2.097.150 redes) y 8 bits para el host (254 máquinas). Son las redes 192.0.0.0 a 223.255.255.0

Además de estas tres clases, existen otros dos tipos de características peculiares:

- Las direcciones de clase D están reservadas para multicasting que son usadas por direcciones de host en áreas limitadas.
 - La dirección comienza por 1110
 - El rango de direcciones va desde 224.0.0.0 a 239.255.255.255
- Las direcciones de Clase E están reservadas para uso futuro.
 - La dirección comienza por 11110
 - El rango de direcciones va desde 240.0.0.0 a 247.255.255.255

Nota:

Si una máquina está conectada a varias redes debe tener una dirección IP para cada una de ellas. Además, al poderse configurar varias conexiones distintas, una máquina puede tener varias direcciones IP en una misma red.

La clase que se elija para una red dada dependerá del número de máquinas que tenga y las que se prevean en el futuro. Como vimos antes el número de red es asignado por el NIC o por el organismo de cada país en quien él delegue. El número de host lo asignará el administrador que controla la red.

Subredes y máscaras de subred.

Puede darse el caso de que una red crezca en un número de máquinas significativo o que se quiera instalar una nueva red además de la que ya existía.

Para conseguir mayor funcionalidad podemos dividir nuestra red en subredes dividiendo en dos partes el número de host, una para identificar la subred, y la otra parte para identificar la máquina (subnetting). Esto lo decidirá el responsable de la red sin que intervenga el NIC.

Podemos tener asignada una red –normalmente de las clases B ó C– y dividirla en dos o más subredes según nuestras necesidades comunicados por routers.

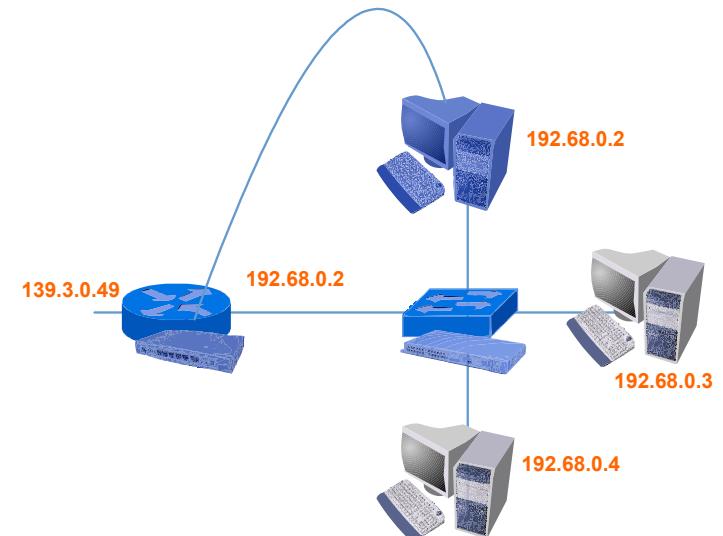


Ilustración 29: Direcciones Clase B y Clase C: Un dispositivo puede disponer de una dirección Clase C y otra Clase B en función de las redes que interconecte

Anotaciones

Capítulo 4: Internet

El conjunto formado por la subred y el número de host se conoce como **dirección local o parte local**. Un host remoto verá la dirección local como el número de host.

El número de bits correspondientes a la subred y al número de host son elegidos libremente por el administrador. Esta división se realiza utilizando una **máscara de subred**. Esta es un número binario de 32 bits. Los bits que estén a "1" indicarán el campo de la dirección IP dedicada a la red y los bits puestos a "0" indicarán la parte dedicada al host. La máscara de subred se representa normalmente en notación decimal.

Por ejemplo si no utilizamos subredes y dejamos la red como una sola, para una red clase B la máscara será:

11111111	11111111	00000000	00000000
255	255	0	0

Si queremos dividirla en subredes tomaremos los 16 bits de la parte local y pondremos a "1" la parte que queremos represente a las subredes. Por ejemplo si queremos 8 subredes necesitaremos en binario 3 bits para referenciarlas. La máscara que necesitamos será:

11111111.11111111.11100000.00000000

es decir 255.255.224.0 en decimal. Al emplear 13 bits para el host podríamos tener hasta $2^{13}-2=8190$ máquinas en cada subred.

Nota:

Debemos recordar que $2^3 = 8$. Empleando el sistema binario de numeración podemos establecer la siguiente numeración: 000, 001, 010, 011, 100, 101, 110, 111. En total, con tres dígitos binarios podemos identificar ocho subredes distintas.

Lo normal a la hora de añadir "unos" a la máscara inicial para definir las subredes es hacerlo de manera contigua para ver los campos claramente.

Si tenemos una red clase C cuya máscara sin subredes es 255.255.255.0 y queremos dividirla en 4 subredes solo necesitamos 2 bits para definirlas:

11111111	11111111	11111111	11000000	Binario
255	255	255	192	Decimal

Esta máscara permitiría hasta $2^6-2=62$ hosts en cada subred.

Anotaciones

Para pensar:

¿En una red tipo C, cuantos dígitos necesitarías para definir 32 redes y de cuantos host contaría cada subred?

Métodos de división en Subredes.

Hay dos formas de dividir una red en subredes: *longitud estática* y *longitud variable*. Se pueden utilizar según el protocolo de encaminamiento. El encaminamiento IP nativo solo soporta longitud estática al emplear el protocolo RIP. Con el protocolo RIP2 se consigue utilizar longitud variable.

La *longitud estática* implica que todas las subredes deben tener la misma máscara lo que obligará a poner la que necesite la que tenga más ordenadores. La *longitud variable* permite que no haya que variar las direcciones de red caso de cambios en una de sus subredes. Una subred que necesita dividirse en otras dos puede hacerlo a añadiendo un bit a su máscara sin afectar al resto. No todos los routers y host soportan la longitud variable de máscaras. Si un host no soporta este método deberá encaminarse hacia un router que sí lo soporte.

Ejemplo de Subneting estática:

Supongamos que tenemos una red clase B, 140.155, y sabemos que no tendremos más de 256 subredes y no más de 254 hosts, podemos dividir la dirección local con 8 bits para las redes y otros 8 para el número de hosts con una máscara del tipo 255.255.255.0 (es decir que en binario sería 11111111.11111111.11111111.00000000).

Si tenemos una red clase C con muchas subredes y con pocos hosts podemos poner una máscara 255.255.255.224 (recordando que 224 es 11100000 en base 2) es decir que hemos dividido la dirección local en 3 bits para redes y 5 para hosts. O sea $2^3=8$ subredes y $2^5-2=30$ hosts.

Las subredes serían:

Binario	Decimal
00000000	0
00100000	32
01000000	64
01100000	128
10000000	160
10100000	192
11100000	224

Anotaciones

Por ejemplo si nuestra red clase C es 193.144.238 y tomamos la máscara 255.255.255.224 anterior:

SUBRED	NÚMEROS DE HOST PARA CADA SUBRED		
193.144.238.0	193.144.238.1	a	193.144.238.30
193.144.238.32	193.144.238.33	a	193.144.238.62
193.144.238.64	193.144.238.65	a	193.144.238.94
193.144.238.96	193.144.238.97	a	193.144.238.126
193.144.238.128	193.144.238.129	a	193.144.238.158
193.144.238.160	193.144.238.161	a	193.144.238.190
193.144.238.192	193.144.238.193	a	193.144.238.222
193.144.238.224	193.144.238.225	a	193.144.238.254

Direcciones Broadcast.

Hay diferentes tipos de broadcast:

- Direcciones de broadcast limitadas: La dirección con todos los bits a "1" (255.255.255.255) se usa en redes que soportan broadcasting, e indica todos los host de la subred. Los routers no reenvían la información fuera de la subred. Se trata de un envío a todos los ordenadores de la subred.
- Direcciones de broadcast de red: En una red sin subredes poniendo a "1" los bits del campo de número de host.
- Direcciones de broadcast de subred: Poniendo a "1" solo la parte del número de host de la dirección local.
- Broadcast a todas las subredes: Poniendo toda la parte local a "1".

Multicasting.

Para tener más flexibilidad que la proporcionada por el método *broadcast* que se dirige a todos los miembros de una subred o de una red, existe el método **multicast**, el cual nos permite dirigirnos a grupos de hosts dentro de la red.

El datagrama IP para multicast como vimos antes es de clase D, cuyos cuatro primeros bits son 1110 (el primer octeto va de 11100000 a 11101111) luego el rango de direcciones será de 224.0.0.0 a 239.255.255.255.

Existen dos tipos de grupos:

Anotaciones

- **Grupos permanentes:** Son los que han sido estandarizados. Los hosts asignados a estos grupos no son permanentes, pueden afiliarse a él o ser quitados de él. Grupos importantes de este tipo son:
 - 224.0.0.0 Dirección reservada de base.
 - 224.0.0.1 Todos los sistemas de la subred.
 - 224.0.0.2 Todos los routers de la subred.
 - 224.0.0.1 Todos los routers OSPF.
 - 224.0.0.1 Todos los routers OSPF designados.
- **Grupos transitorios:** Son los grupos que no son permanentes y se van creando según las necesidades.

Direcciones IP PRIVADAS.

Las redes privadas de organizaciones que no están directamente conectadas a Internet (esto es, las redes que se conectan por medio de un **proxy** o un **router** a una única línea con una sola dirección IP dada por un proveedor de servicios) tienen asignado unos rangos de direcciones IP para su funcionamiento interno. Estos son:

- Para *clase A*: una única dirección de red: 10
- Para *clase B*: 16 redes del rango 172.16 a 172.31
- Para *clase C*: 256 direcciones de red: 192.168.0 a 192.168.255

Estas direcciones IP no son utilizadas por los **routers** para su comunicación con Internet, y se utilizan *sólo dentro de la organización*. Estas redes (Intranet) tienen la ventaja de ser mucho menos accesibles a ataques desde el exterior.

3.5. Protocolo ARP. Resolución de direcciones.

<http://rfc.net/rfc0826.html>

Es tarea de los protocolos de menor nivel (de red local o pasarelas) realizar la correspondencia entre direcciones de red local y rutas.

En una red local, los ordenadores se comunican por medio de *tramas físicas*.

Por ejemplo, en una red Ethernet, la comunicación se realiza por medio de las *tramas Ethernet*. En cada trama va un campo con la *dirección física de origen* y otro campo con la *dirección física de destino*. Cada host está *identificado de fábrica con una dirección física*, de la forma: A3-FF-00-DA-08-09. Está expresada en notación Hexadecimal.

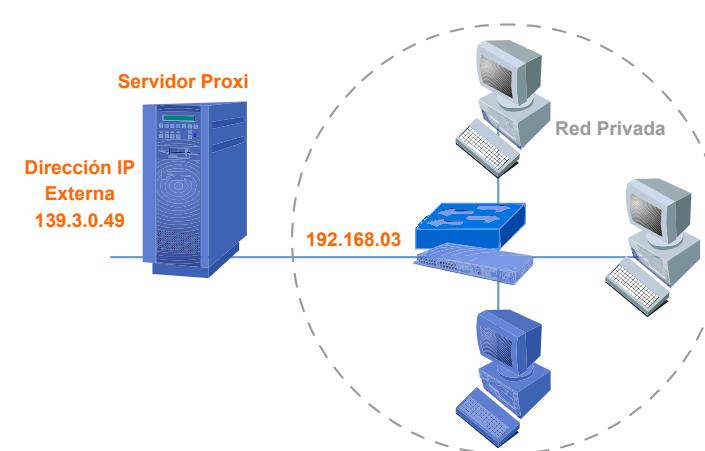


Ilustración 30: Red privada: Se identifica hacia afuera por la dirección IP externa del servidor proxy, quien determina, en función de los datos que incorpora el paquete, cual es la dirección interna de destino

Anotaciones

Capítulo 4: Internet

En una red Internet, la comunicación es por medio de *datagramas IP*, que van con *direcciones IP*.

Necesitamos, entonces, obtener la dirección física de un ordenador por su dirección IP. Esto es lo que hace el **protocolo ARP** (Address Resolution Protocol) (Protocolo de resolución de direcciones).

Veamos cómo funciona el protocolo **ARP**, con un ejemplo:

Supongamos dos redes distintas, en la red 1 está el host1 que quiere enviar un mensaje al host 2, que está en la red 2.

1. El host 1 envía un datagrama, con IP origen 195.53.123.219 y con IP destino 193.47.120.220. Como el host destino está en otra red, el datagrama viajará a través de la red 1, hasta el router, que es la salida de esta red. Para ello hay que conocer la dirección física de la tarjeta de red 1 del router (el router tiene dos tarjetas de red).
2. Entra en funcionamiento el protocolo **ARP**: Se manda un mensaje ARP a todos los ordenadores de la red 1, para ver quien tiene la dirección IP 195.53.123.210. Este mensaje es de *multidifusión* o *broadcast* y lleva la dirección física e IP del ordenador origen.
3. El router contesta mandando su dirección física 1, 00-90-E1-F8-91-A1. La respuesta va directamente al host que preguntó.
4. Host 1 manda la trama física, que contiene encapsulado el datagrama IP, al router.
5. El router pasa el datagrama IP a la red 2.
6. Se repiten los pasos 2 a 4 en la red 2.
7. El datagrama es recogido por el host 2, ya que su dirección IP de destino, coincide con la de él.

Vemos que el protocolo **ARP** ha hecho dos conversiones de *dirección IP a dirección física*. Si el recorrido fuera a través de n redes, se haría esto n veces.

Cada ordenador tiene una tabla **ARP (caché ARP)** que relaciona las direcciones físicas con las IP. Esta tabla la va construyendo según el proceso anteriormente descrito. Cada vez que el protocolo ARP hace una búsqueda, almacena la respuesta en la tabla ARP, así no tiene que repetir siempre el mismo proceso, sino que primero mira la tabla ARP y, si encuentra la respuesta en ella, la manda directamente al ordenador que la requirió.

La tabla ARP se está actualizando cada cierto tiempo, para que recoja las modificaciones de direcciones IP, que haya podido haber.

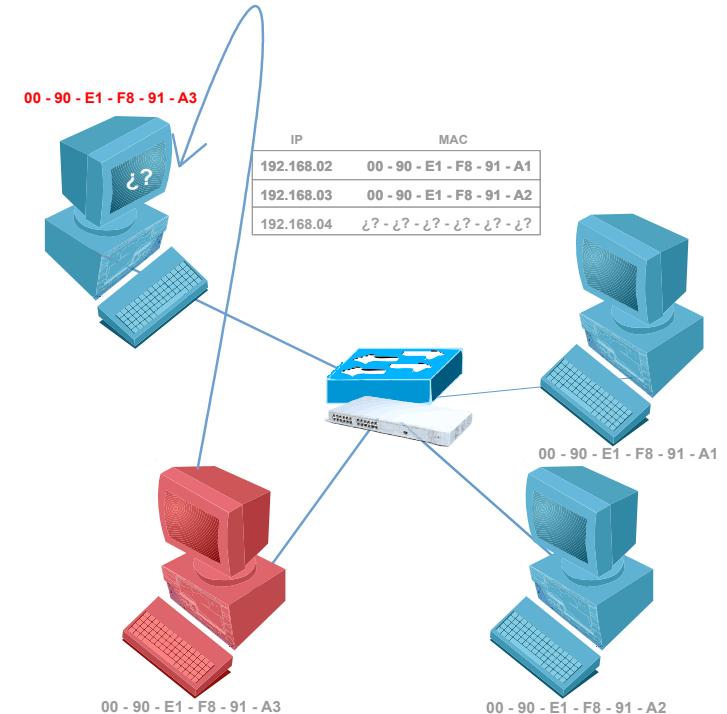


Ilustración 31: Protocolo ARP: Permite averiguar la dirección física de un dispositivo del que se conoce su dirección

Anotaciones

3.6. Protocolo RARP.

A veces, el problema se plantea al revés, se conoce la *dirección física* de un host y se necesita conocer la *dirección IP*. Esto es lo que hace el **protocolo RARP** (Reverse Address Resolution Protocol) (Protocolo de resolución de direcciones inverso).

Una máquina utiliza el protocolo RARP para obtener su dirección **IP** a partir de un servidor. RARP utiliza el mismo formato de mensaje que ARP y al igual que un mensaje ARP, es encapsulado en la parte de datos de una trama Ethernet. La red debe tener un servidor RARP, que conteste al host, enviándole la dirección IP, a partir de la dirección física.

Esto ocurre en el caso de un ordenador que accede vía módem a Internet, y el proveedor le asigna cada vez una dirección IP, de las que tiene libres en ese momento. El ordenador envía un mensaje broadcast con su dirección física, para que el proveedor le mande la dirección IP.

3.7. Protocolo BOOTP.

El protocolo **BOOTP** (Bootstrap Protocol) es algo más eficiente que el anterior, además de la dirección IP del solicitante, se manda información adicional, para facilitar el mantenimiento y movilidad de los ordenadores.

El protocolo BOOTP se utiliza para efectuar arranques remotos en ordenadores que no tienen una dirección IP.

(Explicación detallada en: <http://ditec.um.es/laso/docs/tut-tcip/3376c417.html>)

3.8. Protocolo ICMP.

El Protocolo **ICMP** (Internet Control Message Protocol), proporciona un mecanismo que puede informar de los posibles errores. También da información de control, como congestión en la red, cambios de ruta, etc.

Está definido en la RFC: <http://rfc.net/rfc0792.html>

Los mensajes ICMP van *encapsulados* en los datagramas IP. ICMP utiliza el soporte básico de IP como si se tratara de un protocolo de nivel superior. Sin embargo, ICMP es realmente una parte integrante de IP, y *debe ser implementado por todo módulo IP*.

El protocolo ICMP no está diseñado para ser absolutamente fiable. El propósito del protocolo es darnos información, no solucionar, sobre los problemas que pueda haber en la comunicación. Existe la posibilidad de que algunos datagramas no sean entregados, sin ningún informe sobre su pérdida. Los protocolos de nivel superior que usen IP son los encargados de que la comunicación sea fiable.

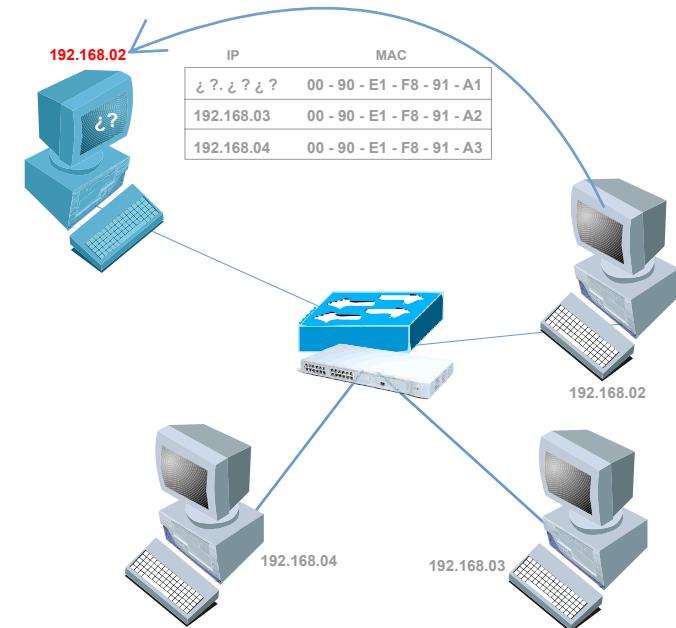


Ilustración 32: Protocolo RARP: Conocida la dirección física de un dispositivo permite averiguar la dirección IP

Anotaciones

Capítulo 4: Internet

Los mensajes ICMP comienzan con un campo de 8 bits, con el tipo de mensaje. Los tipos de mensaje principales son:

- 0 Respuesta de eco.
- 3 Destino inaccesible.
- 4 Disminución tráfico de origen.
- 5 Redirigir datagrama.
- 8 Solicitud de eco.
- 11 Tiempo excedido.

Los mensajes tipo 8 y 0 se usan a menudo para ver si hay comunicación entre dos hosts, pero simplemente a nivel de capa de red.

a) Orden ping.

Esta orden envía mensajes ICMP, de solicitud de eco, desde un host origen a otro destino y nos muestra los resultados.

Para pensar:

Ejecutar una orden ping a una dirección URL conocida. ¿qué sucede?

- ¿Cuál es la dirección IP?
- ¿Cuánto es el tiempo de respuesta?

b) Orden tracert.

Sirve para saber por donde va pasando la información. Manda mensajes ICMP de solicitud de eco, con tiempos de vida 1,2,3, etc., hasta alcanzar el host destino. El 1º datagrama IP expira en el 1º router, mandando un mensaje tipo 11 (Tiempo excedido) y el router que lo envía. El 2º informa del 2º router y, así sucesivamente. Con esto se consigue tener una traza de los nodos por donde ha ido pasando el datagrama.

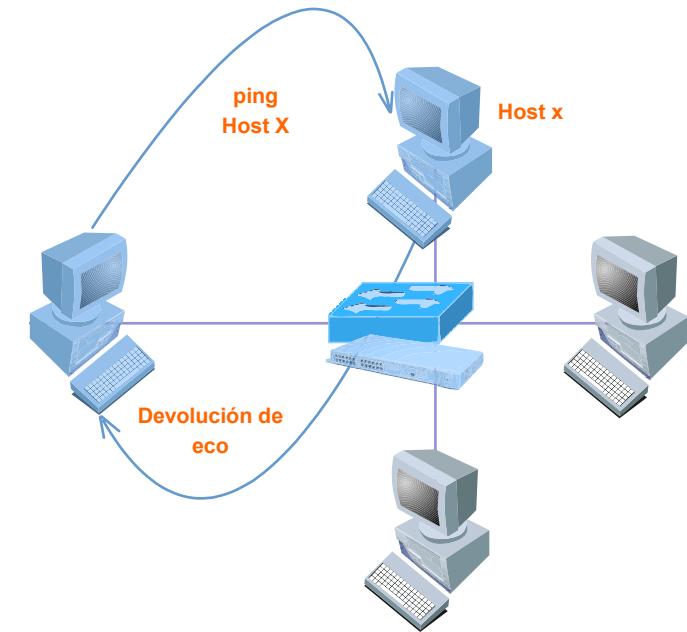


Ilustración 33: Protocolo ICMP: Permite la obtención de información sobre el estado de una red.

Anotaciones

4. Servicios de Internet.

4.1. Introducción.

Internet es algo más que una inmensa red de ordenadores, además de la intercomunicación, la inmensa cantidad de información y las ventajas que supone, Internet es la base sobre la que se apoyan ciertos servicios que han llegado a ser tan necesarios y populares que no entenderíamos Internet si éstos faltasen. Servicios tan indispensables como pueden ser el correo electrónico, el FTP, el World Wide Web, etc...

Estas utilidades van cambiando y actualizándose a las necesidades y demandas de los usuarios, y no sólo nacen cuando son requeridos, sino a veces cuando las capacidades de la red hacen posible su correcto funcionamiento. Por poner un sencillo ejemplo, la videoconferencia es una técnica que está estudiada desde hace bastante tiempo, sin embargo su implantación depende de las características del medio de transmisión y es ahora cuando comienza a ser utilizada de manera habitual.

A continuación repasaremos de manera somera algunos de los servicios de Internet más utilizados, estos servicios establecen protocolos del nivel de aplicación de la pila TCP/IP y usan estos protocolos para moverse por la red.

4.2. Servidores de acceso.

Un servidor de acceso es un dispositivo especializado que conecta usuarios remotos, básicamente de acceso telefónico, a redes. Una forma muy directa de entenderlo sería decir que un servidor de acceso es una máquina que actúa como un concentrador por un lado y como un módem por el otro. El usuario remoto se conectaría mediante la línea telefónica por el lado del módem y el servidor de acceso le conectaría a una red mediante el concentrador.

La mayoría de los puertos de los servidores de acceso en el mundo los administran los ISP para atender las llamadas telefónicas de los abonados a Internet. Un ISP (Internet Service Provider) es una compañía que proporciona acceso a Internet. Existen numerosos ISP, gratuitos muchos de ellos. El CNICE, por ejemplo, se podría considerar como un ISP, puesto que proporciona conexión telefónica a Internet a sus usuarios.

El ISP proporciona un paquete de software, un número telefónico de acceso, un nombre de usuario y una contraseña. Mediante un módem, y usando la línea telefónica, el usuario puede identificarse y el servidor de acceso le da salida a Internet.

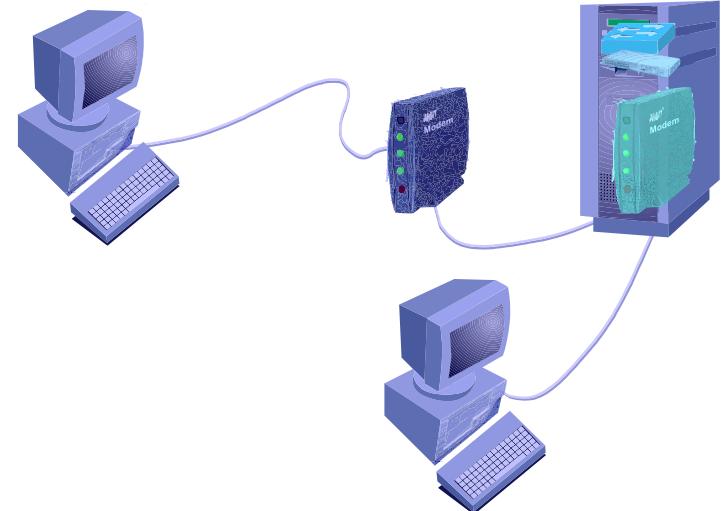


Ilustración 34: Servidor de acceso a Internet: Es una máquina que actúa como un modem por un lado y como un concentrador por el otro

Anotaciones

4.3. HTTP.

El Protocolo de Transferencia de HiperTexto (Hypertext Transfer Protocol) es un sencillo protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores http.

Se diseñó específicamente para el World Wide Web: es un protocolo rápido y sencillo que permite la transferencia de múltiples tipos de información de forma eficiente y rápida. Se puede comparar, por ejemplo, con FTP, que es también un protocolo de transferencia de ficheros, pero tiene un conjunto muy amplio de comandos, y no se integra demasiado bien en las transferencias multimedia.

HTTP está soportado por los servicios de conexión TCP/IP. Cada vez que un cliente realiza una petición a un servidor, se ejecutan los siguientes pasos:

1. Un usuario accede a una URL, seleccionando un enlace de un documento HTML o introduciéndola en el navegador. (Fig. 10.2)
2. El cliente Web decodifica la URL, separando sus diferentes partes. Así identifica el protocolo de acceso, la dirección DNS o IP del servidor, el posible puerto opcional (el valor por defecto es 80) y el objeto requerido del servidor.
3. Se abre una conexión TCP/IP con el servidor webs, llamando al puerto TCP correspondiente (80).
4. Se realiza la petición. Para ello, se envía el comando necesario (GET, POST, HEAD,...), la dirección del objeto requerido (el contenido de la URL que sigue a la dirección del servidor), la versión del protocolo HTTP empleada (casi siempre HTTP/1.0) y un conjunto variable de información, que incluye datos sobre las capacidades del navegador, datos opcionales para el servidor...
5. El servidor devuelve la respuesta al cliente. Consiste en un código de estado y el tipo de dato MIME de la información de retorno, seguido de la propia información.

Nota:

MIME es un estandar que permite codificar distintos tipos de datos para su utilización en aplicaciones de correo electrónico.

6. Se cierra la conexión TCP.

Este proceso se repite en cada acceso al servidor HTTP. Por ejemplo, si se recoge un documento HTML en cuyo interior están insertadas cuatro imágenes, el proceso anterior se repite cinco veces, una para el documento HTML y cuatro para las imágenes.

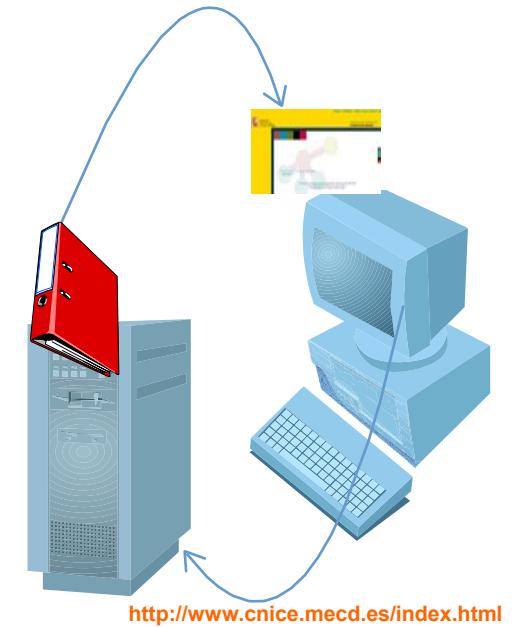


Ilustración 35: HTTP: Permite el intercambio de información entre servidores web y navegadores. Utilizan TCP/IP para transferir los archivos. Es un protocolo del nivel de aplicaciones

Anotaciones

En la actualidad se ha mejorado este procedimiento, permitiendo que una misma conexión se mantenga activa durante un cierto periodo de tiempo, de forma que sea utilizada en sucesivas transacciones. Este mecanismo, denominado HTTP Keep Alive, es empleado por la mayoría de los clientes y servidores modernos.

Nota:

Un servidor webs es un equipo que dispone de un software que permite moderar peticiones por parte de clientes.

Elementalmente diremos de http que:

- Es protocolo simple de solicitud-respuesta.
- Es usado por las aplicaciones Web.
- Usa el HTML como lenguaje de transmisión.
- Rápido y simple, aunque carece de estado. Lo que significa que, en principio, un servidor de HTTP carece de medios para relacionar información concerniente a una petición con otra petición anterior o posterior. Los datos de la respuesta se basan exclusivamente en la información que el cliente envía en la petición. El protocolo HTTP no conoce a la persona a quien está enviando una página ni cuántas páginas le haya podido enviar, incluso aunque nos hayamos conectado hace escasamente algunos segundos, ya que cada petición de página se procesa independientemente.

4.4. News.

News es un servicio de la red Internet que permite el acceso a foros de discusión o conferencias multitudinarias sobre los temas más diversos. Esta herramienta es conocida también con el nombre de Usenet News o simplemente Usenet, porque el servicio tuvo su origen en la red Usenet, que es una red que une centros de investigación y Universidades de todo el mundo.

Del mismo modo que las listas de correo, las News es un medio para intercambiar información. Pero se diferencian en que las News no están basadas en el correo electrónico: no es necesario darse de alta en la lista, y los mensajes no se distribuyen a los buzones personales de los usuarios. En este servicio, los mensajes que se envían son públicos: todo el mundo tiene la posibilidad de acceder a ellos. En este sentido, las News son comparables a un gran número de tablones de anuncios públicos, clasificados por temas, a los que todo el mundo puede acceder para dejar un mensaje y/o para leer el resto de mensajes que están expuestos.

Anotaciones

a) Funcionamiento de las News.

El acceso a los artículos y opiniones de los llamados newsgroups, grupos de discusión o grupos de noticias, se realiza a través los servidores de News en los que hay instalados programas que se encargan de ofrecer ese servicio a los usuarios que se conectan. Estos servidores pueden dar acceso a las News por web.

Sin embargo, a veces, los usuarios necesitan un programa cliente (lector de News) para poder enviar a esos servidores sus opiniones, artículos, comentarios, noticias, respuestas a otros artículos,... o bien, sencillamente, para consultar las intervenciones de los diferentes grupos de noticias. Por poner un ejemplo, Outlook Express puede funcionar como gestor de correo así como lector de News.

Los mensajes o artículos que se envían a un determinado grupo de discusión quedan almacenados en el servidor de News, a donde han de acudir el resto de usuarios para consultarlos. De esa manera, no importa el número de personas que leen o envían un mensaje, en cualquier caso sólo es necesario almacenar una copia de dicho mensaje en un servidor de la red. Esto supone, con respecto a las listas de correo, un importante ahorro de tráfico en la red y de volumen de almacenamiento en los buzones particulares de los usuarios.

Existen en la red Internet miles de grupos de discusión o newsgroups sobre prácticamente cualquier tema que uno pueda imaginar, desde el más serio al más banal. Pueden encontrarse temas científicos, lúdicos, educativos, religiosos, políticos, etc. Frente a este inmenso caudal de información, al usuario no le queda otro remedio que aprender a navegar por él, y en última instancia, seleccionar y elegir únicamente los grupos de discusión que tratan temas en los que verdaderamente está interesado.

El nombre de un determinado grupo de discusión suele expresarse con palabras separadas por puntos. Por ejemplo:

news.announce.newsgroups

En España, el servidor de News de Rediris propone para la denominación de sus grupos un nombre en el que antepone a estas categorías la palabra "es". Así, los nombres de algunos grupos de discusión en ese servidor son, por ejemplo: es.alt.anuncios; es.rec.deportes; es.news.groups.

Para facilitar tanto la localización como la identificación de los diferentes grupos, éstos se organizan jerárquicamente en categorías o áreas de contenido. La primera palabra del nombre del grupo identifica la categoría mayor de contenido en la que se encuadra ese grupo. Las principales categorías de contenido son las siguientes:

Anotaciones

- **alt** Es una categoría bastante amplia. Pueden encontrarse excelentes temas de debate, pero también temas triviales y algunos bastante controvertidos.
- **bit** Redistribución de un subconjunto de listas de correo.
- **comp** ordenadores y temas relacionados con informática
- **misc** Temas de difícil clasificación dentro del resto de las categorías.
- **news** Grupos de discusión en Internet: anuncio de nuevos grupos, programas de News, preguntas generales sobre las News.
- **rec** Pasatiempos, arte, entretenimiento.
- **sci** Ciencia e investigación.
- **soc** Asuntos sociales y culturales de todo el mundo.
- **talk** Está orientado sobre todo a temas que se prestan a un debate sin fin. Temas políticos, religiosos, éticos, sobre la salud.
- **biz** Negocios.

Los grupos de discusión pueden tener o no un moderador. En los grupos en los que existe un moderador, las intervenciones no llegan directamente al grupo, sino al moderador, que es quien decide si merece o no la pena incluir el artículo.

La gran controversia que existe con referencia a las News proviene del hecho de su carácter público, ya que algunos de los temas que se tratan pueden resultar ofensivos para algunas personas. La libertad de expresión, que muchos usuarios de las News defienden, supone el no poner coto alguno a cualquier opinión y que puedan tratarse temas que incluso puedan rozar la ilegalidad. Hay desde luego opiniones y temas absolutamente inapropiados para personas que se encuentran aún en periodo de formación como pueden ser los menores. Frente a este aspecto negativo, las News son al mismo tiempo un vivo ejemplo de la libertad de prensa, porque el usuario no necesita tener a su disposición un medio impreso para poder publicar sus propias ideas: las News le facilitan una plataforma.

Cada día nacen nuevos grupos de discusión. Algunos tienen una larga vida, pero otros mueren enseguida. Algunos se archivan en ficheros que pueden recobrarse meses e incluso años después.

Anotaciones

4.5. FTP.

FTP responde a las iniciales de File Transfer Protocol, es decir, Protocolo de Transmisión de Ficheros. Este protocolo es usado para “subir” o “bajar” archivos entre una estación de trabajo y un servidor FTP.

Existen en la red Internet cientos de ordenadores que son servidores de acceso público, es decir, que el usuario puede acceder a ellos y obtener ficheros sin necesidad de tener abierta una cuenta. Se pueden encontrar muchos tipos de ficheros disponibles en estos servidores de acceso público: documentos históricos, libros y periódicos electrónicos, gráficos y dibujos, fotografías, ficheros de sonido, programas, etc.

Existen programas clientes que permiten hacer FTP de una manera sencilla y completa.

Aunque también se puede utilizar el propio Navegador. Como te habrás podido ya dar cuenta, los navegadores incluyen muchas funciones, no sólo navegar por la Web. Esto es debido a que la Web ha ido integrando poco a poco la mayoría de los servicios que se ofrecen en Internet.

Existen dos maneras de realizar FTP con un programa cliente, y en ambas es necesario incluir ciertos datos:

- FTP anónimo:
 - **Profile Name:** En este campo se introduce un nombre cualquiera que sirva para identificar la conexión. Un ejemplo podría ser Servidor ftp de RedIRIS.
 - **Host Name/Address:** Dirección del servidor con el que se desea conectar. En nuestro caso: ftp.rediris.es.
 - **Host Type:** En este campo es conveniente dejar el valor Automatic detect que aparece seleccionado por defecto.
 - **User ID y Password:** Estos campos se rellenan automáticamente al marcar la casilla Anonymous situada a la derecha del campo User ID.
 - **Account:** Este campo puede dejarse vacío.
- FTP identificado:
 - **Profile Name:** Se introduce un nombre que sirva para identificar la conexión. Podría ser, por ejemplo, Mi cuenta.
 - **Host Name/Address:** Dirección del servidor en el que se está dado de alta. En nuestro ejemplo, platea.pntic.mec.es.
 - **Host Type:** En este campo es conveniente dejar el valor Automatic detect que aparece seleccionado por defecto.

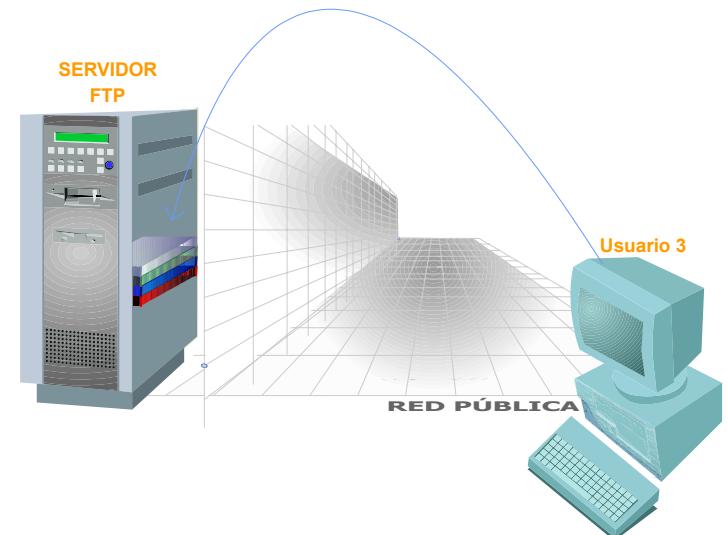


Ilustración 36: Servidor FTP: Permite realizar operaciones, transferir archivos entre clientes y servidores FTP y realizar operaciones sencillas como mover directorios

Anotaciones

- **User ID:** login del usuario.
- **Password:** password del usuario. Al lado de este campo existe una casilla (Save Pwd) que puede activarse o no con el fin que se guarde la password. Si no se activa, habrá que introducirla cada vez que se conecte.
- **Account:** Este campo puede dejarse en blanco.

Para hacer FTP con el navegador tienes que poner en la barra de direcciones "ftp://" seguido de la dirección del servidor al que quieras acceder.

4.6. VNC.

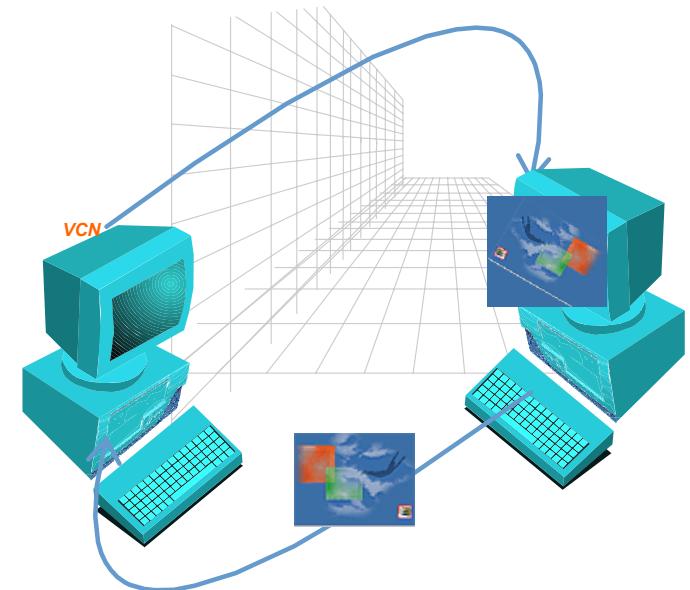
VNC son las siglas de *Virtual Network Computing*. Esencialmente es un sistema remoto de visualización que te permite ver el escritorio de un sistema operativo desde otra máquina diferente. Por ejemplo podríamos usar VNC para visualizar en nuestro PC el entorno UNIX de nuestro servidor situado en otra parte del edificio.

Un método similar de contacto remoto es la instalación de un servidor X en nuestro PC. Sin embargo VNC se diferencia de otros sistemas en varias características:

- Podemos abandonar la máquina a mitad de un trabajo, ir a otro equipo al otro lado de la puerta o muchos kilómetros más allá, conectarnos y finalizar nuestro trabajo. Con VNC todas las operaciones remotas se mantienen incluso si el PC es reiniciado.
- Es pequeño (se puede transportar en un disquete) y muy sencillo, y no requiere proceso de instalación.
- Es independiente del tipo de plataforma. Un sistema operativo Linux puede ser visualizado en un PC, y también una máquina Solaris, así como otras muchas arquitecturas. La sencillez del protocolo lo hace posible.
- Un mismo escritorio puede ser visualizado desde numerosos equipos simultáneamente.
- Es gratuito. Se puede descargar y distribuir bajo los términos de la licencia pública GNU. Para más información consultar la siguiente web:

<http://www.uk.research.att.com/vnc/>

VNC consta de dos tipos de componentes: Un servidor, el cual genera un “display” o imagen de la pantalla, y un visor, que realmente *captura* y *muestra* el “display” del servidor VNC.



Anotaciones

El servidor y el visor pueden estar en máquinas independientes y con arquitecturas independientes. El uso más generalizado es la visión de un sistema operativo UNIX desde un PC. El protocolo que conecta el servidor y el visor es sencillo, abierto e independiente del tipo de plataforma.

Para usar VNC es necesario la instalación del software del servidor. Una vez echo esto se lanza el visor y se conecta con el servidor. VNC requiere una conexión TCP/IP entre servidor y visor. Si por ejemplo tenemos un servidor de nombre `sauce`, con entrada al DNS podemos conectarnos escribiendo:

```
Vncviewer sauce:2
```

El dos simplemente marca el número de “display”. Si no especificamos ninguno es el cero el que se elige automáticamente. En el caso de no disponer una entrada válida al DNS, es posible la conexión con la dirección IP.

4.7. IRC.

IRC son las siglas en inglés de *Internet Relay Chat*. El comúnmente llamado Chat es una aplicación de Internet que permite mantener conversaciones en directo a través del ordenador en las que pueden participar varios usuarios a la vez.

Originalmente el Chat se llevaba a cabo por medio de texto escrito en pantalla, y aunque este modo sigue siendo mayoritario, recientemente está empezando a surgir, apoyado en los equipos multimedia, otro tipo de Chat que se realiza transmitiendo la voz e imagen.

Para mantener una conversación por Chat es necesario un cliente IRC y una conexión a Internet. El cliente IRC es el programa que está instalado en la máquina del usuario y envía y recibe los mensajes de un servidor IRC. Este servidor es el encargado de asegurar que los mensajes llegan a todos los miembros de una conversación.

En el caso de plataformas Windows, uno de los programas más populares y gratuito es mIRC y una alternativa podría ser Pirch. En el caso de plataformas UNIX, podríamos destacar Xchat, BitchX, o ircII. Este último es quizás el cliente estandar IRC para linux y posiblemente el más potente.

4.8. Telnet.

El protocolo TELNET proporciona el servicio de conexión remota y es un emulador de terminal que permite acceder a los recursos y ejecutar los programas de un ordenador remoto en la red, de la misma forma que si se tratara de un terminal real directamente conectado al sistema remoto.

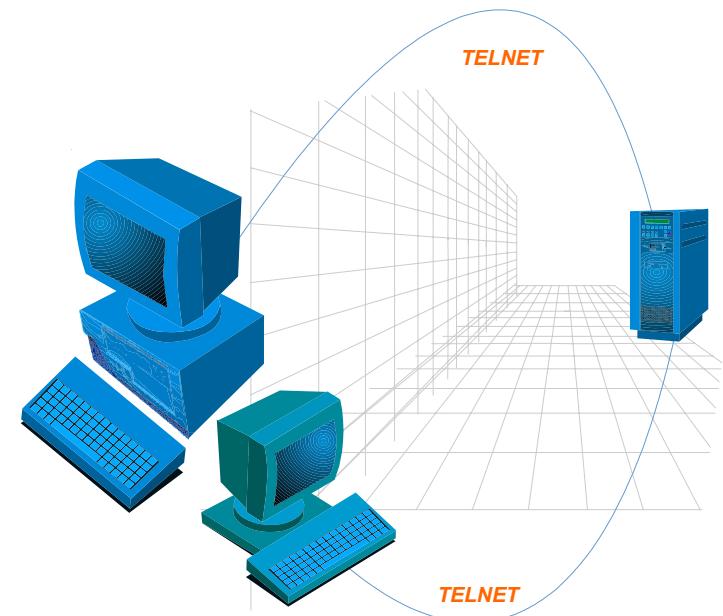


Ilustración 38: Telnet: Permite acceder a un servidor a través de Internet transformando el PC en un terminal de red

Anotaciones

El sistema local que utiliza el usuario se convierte en un terminal "no inteligente" donde todos los caracteres pulsados y las acciones que se realicen se envían al host remoto, el cual devuelve el resultado de su trabajo. Para facilitar un poco la tarea a los usuarios, en algunos casos se encuentran desarrollados menús con las distintas opciones que se ofrecen. Generalmente Telnet no ofrece gráficos bonitos o enlaces en el texto, pero es una cómoda y eficiente, si bien rudimentaria, forma de dar acceso remoto a una red a las personas interesadas e incluso al público en general.

Algunas bibliotecas, centros académicos, de investigación y de información usan Telnet para colocar sus bases de datos a disposición del público o a personal autorizado para consulta con su sistema informativo actual, sin tener que invertir en trasladarlo a la telaraña mundial y HTML.

Una vez establecida la conexión, se nos pide una identificación para darnos acceso (un nombre o login y una contraseña o password). A partir de ahí, si nos identificamos correctamente, estaremos dentro de la red con acceso a los servicios disponibles para el usuario con el cual nos identificamos.

Es posible ejecutar una aplicación cliente TELNET desde cualquier sistema operativo, pero hay que tener en cuenta que los servidores suelen ser sistemas VMS o UNIX por lo que, a diferencia del protocolo FTP para transferencia de ficheros donde se utilizan ciertos comandos propios de esta aplicación, los comandos y sintaxis que se utilice en TELNET deben ser los del sistema operativo del servidor.

Las direcciones Telnet consisten típicamente en la dirección numérica (IP address) del servidor de la red que deseamos acceder, formada por una serie de cuatro números separados por un punto.

Desde el sistema operativo Windows, por ejemplo, se pincha sobre el botón Inicio y se escoge la opción "Ejecutar".

En la ventana que aparece escribir "Telnet direccion.host.remoto".

Por ejemplo la dirección de EnviroNET: 128.183.104.16

Esta dirección proporciona acceso a su base de datos relacionada con el espacio.

Para acceder a un sitio Telnet desde nuestro navegador, basta con escribir su dirección en la barra de direcciones, precediéndola del término telnet://

telnet://128.183.104.16/

Nuestro navegador se encargará automáticamente de ejecutar un programa adicional para Telnet y este establecerá la conexión con el servicio deseado.

Anotaciones

4.9. DNS.

Las siglas DNS pertenecen a *Domain Name Server*, Servidor de Nombres de Dominio. Básicamente es un conjunto de software y protocolos que traducen los nombres de dominio como www.mecd.es en una dirección IP del tipo 195.53.133.44, por ejemplo.

Internet está basado en direcciones IP pero muy pocas veces usamos una dirección IP para visitar cualquier página en el navegador. Evidentemente, nos es mucho más sencillo el recordar nombres que números, de ahí el sentido de los DNS. Cada vez que usamos un nombre de dominio un DNS se encarga de traducirlo a una dirección IP.

Para ello usa lo que se denomina *Resolver*: un conjunto de bibliotecas de las aplicaciones clientes, o sea, las que solicitan información acerca de un dominio de nombre.

El *Resolver* tiene como tareas:

- Interrogar al servidor de nombres.
- Interpretar respuestas. Que serán registros o errores.
- Devolver información al programa que la solicita.

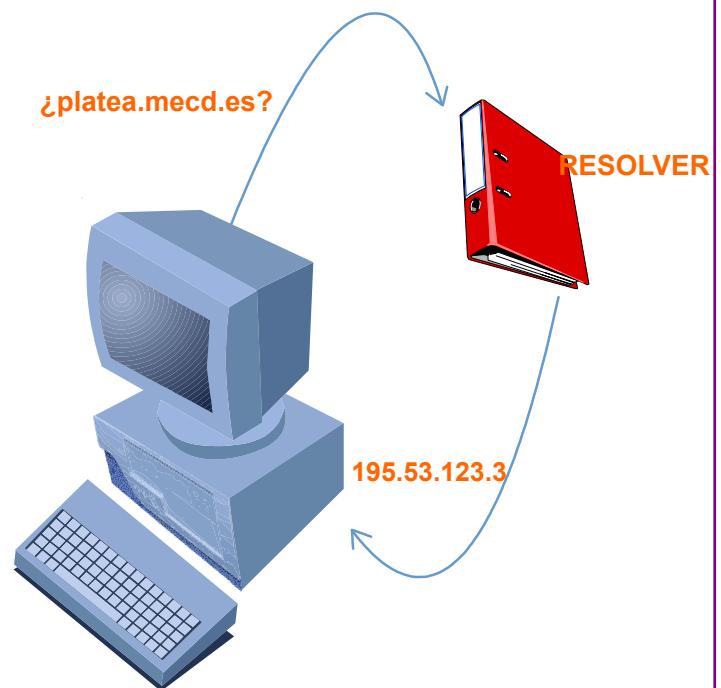
El Proceso de trabajo para conseguir esta dirección IP supone de alguna forma que los DNS trabajan en su propia red. Por ejemplo, si el DNS asociado a un cierto equipo desconoce la dirección IP de un nombre de dominio traslada la cuestión a otro DNS, y de esta manera hasta que la correcta dirección IP sea devuelta. Más concretamente el proceso es el siguiente:

Primero el servidor de nombres verifica sus tablas de máquinas a ver si allí consigue el nombre por el cual le están preguntando. Si es así, entonces retorna la dirección IP asociada con ese nombre. Si la información pertenece a otro dominio, entonces el servidor de nombres busca en su cache y si no está allí comienza un proceso que se puede comportar de estas dos formas:

- De manera **Recursiva**:

Un servidor de nombres envía una respuesta recursiva cuando es el servidor y no el cliente el que pregunta a otros servidores de nombres por la información del dominio solicitada. Esto ocurre cuando el servidor de nombres sabe que el *resolver* no tiene la inteligencia de manejar una referencia a otro servidor de nombres (Es decir, el resolver hace explícitamente una pregunta recursiva). A medida que un servidor de nombres pregunta (obtenga respuesta o no) va guardando los nombres encontrados en su cache para evitarse búsquedas innecesarias.

- De manera **Iterativa**:



Anotaciones

El servidor de nombres da la mejor respuesta que ya sabe a quien preguntó (es decir, da una referencia al servidor de nombres más cercano a la información de dominio interrogado). Primero consulta sus datos locales, si no está allí busca entonces en su cache y si aún no encuentra nada entonces devuelve la respuesta (servidor) más cercano al dominio buscado. Si el servidor falla, no lo vuelve a intentar. Las bibliotecas del resolver hacen búsquedas recursivas e iterativas, mientras que entre servidores de nombres solo se hacen búsquedas iterativas.

cnice.mecd.es

tiene el nombre de dominio de

sauce.cnice.mecd.es

La dirección completa de la máquina se lee de izquierda a derecha (Desde lo más específico, el nombre del host, pasando por cada uno de los "dominios" a los cuales pertenecen).

Los dominios más usuales son los siguientes:

- **com** Se utiliza por las empresas comerciales de EE.UU. En España se suele usar siempre el dominio **es**.
- **edu** Direcciones de instituciones educativas como colegios o universidades. Por ejemplo wisc.edu se refiere a la universidad de Wisconsin.
- **gov** Nombre de dominio para instituciones gubernamentales dentro de EE.UU.
- **mil** Sitio militar, por ejemplo af.mil (Air Forces).
- **net** Pasarelas y nodos de administración de una red. Por ejemplo near.net
- **org** Este dominio está reservado para organizaciones privadas sin ánimo de lucro. Por ejemplo Greenpeace, que tiene de nombre greenpeace.org

Todos los dominios anteriores se usan en los EE.UU, en el resto de los países se usan otros dominios, que indican el país al que pertenecen. Por citar algunos:

- **es** España
- **fr** Francia
- **au** Australia
- **uk** Gran Bretaña

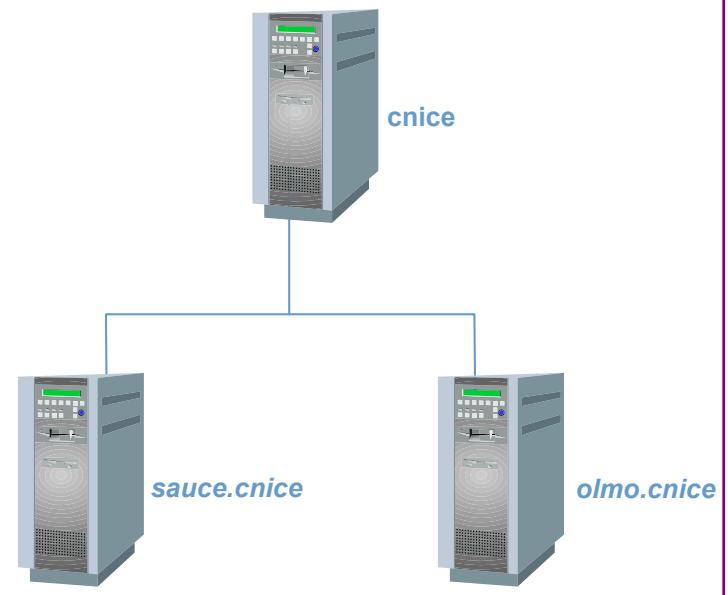


Ilustración 40: Nombres de dominio

Anotaciones

Cada máquina en la red pertenece a un dominio, cuyo servidor de nombres contiene la información acerca de la máquina. Esta información puede incluir direcciones IP, información acerca de enrutamiento de correo, etc. (Una máquina también puede tener uno o más alias de dominio, lo cual quiere decir que existen 2 referencias hacia la máquina, una de ellas es un apuntador de un dominio (alias) a su nombre canónico (u oficial).

DNS permite eliminar los problemas que presentaba la existencia de un archivo de datos planos:

- Elimina el problema de nombres repetidos (a cada organización se le asigna un dominio único, por lo que pueden existir dos máquinas con el mismo nombre mientras estén en dominios separados).
- Elimina el problema de carga y tráfico de red en una sola máquina ya que la información está distribuida y disponible de manera redundante.
- Finalmente hay consistencia, ya que la actualización de la información se hace de manera automática, sin intervención del administrador de la red.

En la siguiente figura (Fig.10.8.2) se puede apreciar esquemáticamente en dónde nos podemos encontrar servicios de DNS.

El DNS primario conoce los servidores de nombres de dominios inferiores. Digamos que actúan marcando la dirección en la que tiene que ir la pregunta para conseguir la respuesta correcta.

4.10. Correo electrónico.

El correo electrónico, llamado también habitualmente e-mail, es la aplicación más extendida en Internet, y la que muchos usuarios consideran la más útil. Permite al usuario enviar y recibir mensajes escritos a otros usuarios de la red situados en cualquier lugar del mundo siempre que dispongan de una dirección de correo electrónico (e-mail address).

Nota:

El signo @ se eligió en 1972 para separar la dirección de usuario de la del host donde se almacena su correo.

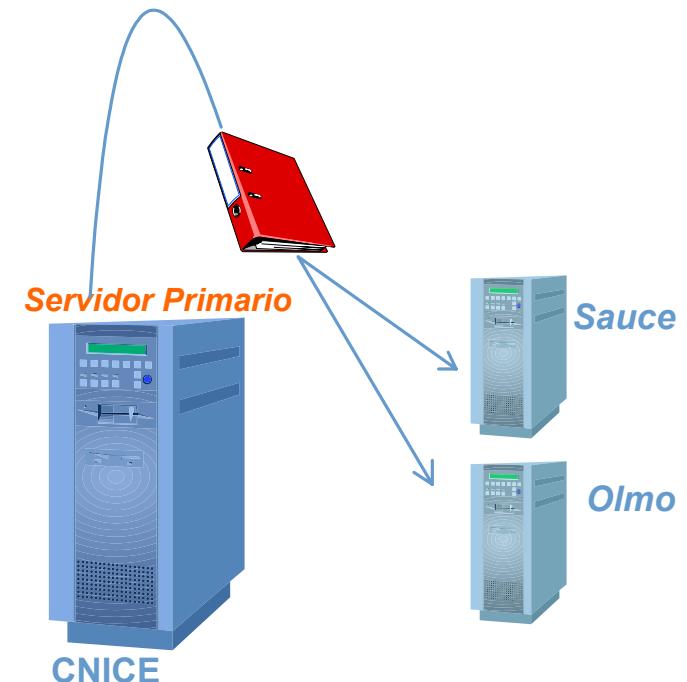


Ilustración 41: Servidor primario: Conoce los nombres de dominio inferior

Anotaciones

Una característica importante del correo electrónico es que no es necesario que el destinatario de un mensaje esté frente a la pantalla en el momento en que otro usuario se lo envía. Y tampoco es necesario que su ordenador esté conectado a la red o que esté encendido. Los mensajes que le llegan se almacenan en el ordenador servidor en el que el destinatario está dado de alta. Después, cuando éste se conecta con el servidor utilizando su programa de correo, le pide al servidor que le envíe a su ordenador los mensajes que tiene almacenados.

El primer software de correo ordinario permitía sólo una función básica: un mensaje era tecleado y enviado desde un ordenador, a través de la Red, a otro ordenador.

Los sistemas actuales de correo electrónico soportan servicios más completos que permiten acciones más complejas como pueden ser:

- Mandar un mismo mensaje a muchas personas.
- Incluir texto, voz, vídeo o gráficos.
- Conectar con un usuario fuera de Internet.
- Enviar mensajes de forma automática.

El correo electrónico se está convirtiendo en un importante medio de comunicación porque, además de ser rápido y económico, ofrece muchas posibilidades: permite intercambiar información, comunicar ideas, debatir temas, compartir ficheros, editar y revisar documentos, etc.

La gran mayoría de redes tienen funcionando un sistema de gestión de correo, o poseen pasarelas a otros sistemas de máquinas que les facilita este servicio.

El servicio de correo necesita de varios protocolos para su funcionamiento. Normalmente, la mayoría de los sistemas de correo utilizan SMTP para enviar mensajes de un servidor a otro. Estos mensajes pueden ser recuperados por aplicaciones cliente usando los protocolos POP o IMAP, pero el SMTP es también usado para enviar el correo desde las aplicaciones cliente al servidor.

4.11. SMTP.

SMTP son las siglas en inglés de *Simple Mail Transfer Protocol*, un protocolo de transferencia de correo entre servidores. La máquina que envía el mensaje establece una conexión TCP al puerto 25 de la máquina destinatario. *Escuchando* este puerto se halla un *daemon* o *demonio* que utiliza SMTP. Este demonio acepta los mensajes que llegan y los copia a sus apropiados buzones de correo. Si el mensaje no puede ser entregado, se genera un mensaje de error que es enviado al remitente.

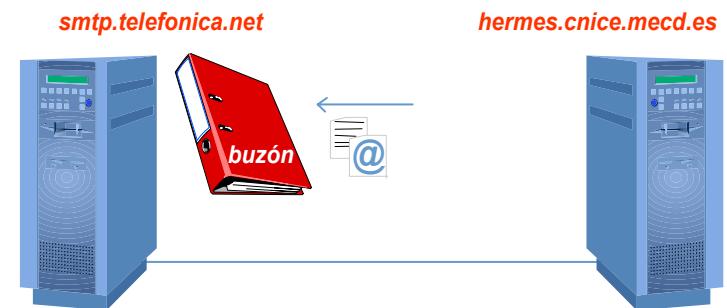


Ilustración 42: Servicio SMTP: Realiza la transferencia de correo entre servidores de este tipo de servicio

Anotaciones

Daemon es un término originalmente de UNIX, aunque muchos otros sistemas operativos lo utilizan. Básicamente un daemon o demonio es un proceso que está funcionando en segundo plano y que realiza alguna operación específica en momentos predefinidos, o como respuesta a ciertos eventos. El término proviene de la mitología griega, donde un daemon es un espíritu guardián.

SMTP es un sencillo protocolo escrito en ASCII. Una vez establecida la conexión TCP en el puerto 25, la máquina que envía el mensaje y actúa como cliente, espera que el servidor *hable* primero. El servidor envía un texto con su identidad y si puede o no recibir mensajes. Si no puede, el cliente abandona la conexión y lo intenta más adelante.

Si el servidor está preparado para recibir, el cliente envía información diciendo de quién es el mensaje y a quién va dirigido. Si el servidor reconoce al destinatario, manda un mensaje con la autorización de envío y el cliente manda los mensajes. Cuando se han mandado todos los mensajes en ambas direcciones, se corta la conexión.

Aunque el protocolo SMTP esta muy bien definido (RFC 821), puede que existan algunos problemas. Por ejemplo, antiguas implantaciones tienen problemas con la longitud de los mensajes y dan fallos con el tratamiento de mensajes que exceden los 64 Kb. Otro inconveniente es cuando existen distintos *timeouts* entre cliente y servidor. Puede suceder que uno de ellos abandone la conexión inesperadamente porque el otro esté todavía ocupado. Todos estos detalles han sido tratados en la Extensión de SMTP: ESMTP (RFC 1425).

El intercambio de correo usando TCP/IP es realizada por los MTA (*Message Transfer Agent*) comúnmente conocidos como los programas de servidor de correo. UNIX Sendmail y Microsoft Exchange Server, serían claros ejemplos de MTA.

SMTP permite que el correo pueda ser enviado desde una aplicación cliente a una aplicación SMTP, la cual almacena el mensaje en un dispositivo o tipo de memoria especial. Esta memoria la conocemos como Buffer. Así, el mensaje es incluido en esta estación de espera hasta que el proceso se pueda realizar con absoluta normalidad.

4.12. POP.

A menudo es imposible mantener un sistema de transporte de correo en ciertos pequeños nodos de Internet. Por ejemplo una estación de trabajo puede no tener suficiente espacio en su disco duro o recursos para mantener un servidor SMTP continuamente funcionando. O también puede ser tremadamente caro el mantener una máquina conectada a la red durante considerables cantidades de tiempo para realizar las tareas de gestión de correo. A pesar de esto es posible el manejo del correo desde uno de estos pequeños nodos. Para ello, el nodo mayor que mantiene un sistema de correo ofrece un

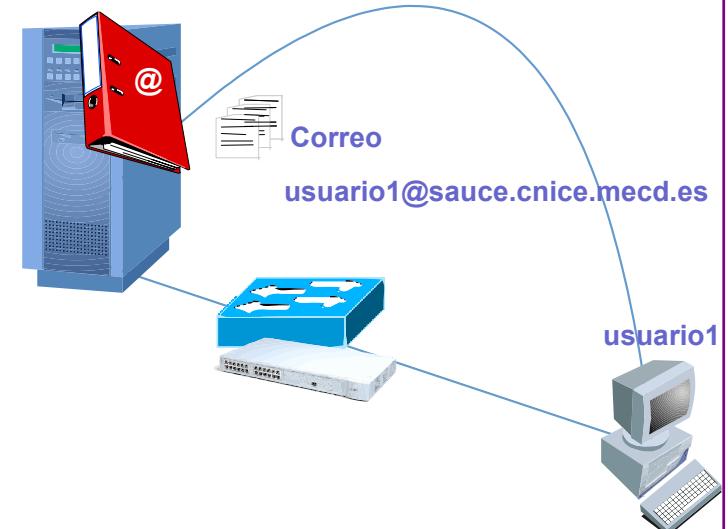


Ilustración 43: Pop: Permite descargar el correo de un servidor

Anotaciones

Capítulo 4

servicio de entrega de correo al nodo menor, que estará equipado con una aplicación cliente. Aquí es donde interviene el protocolo POP, siglas de *Post Office Protocol*.

Este protocolo es usado para permitir que una estación de trabajo pueda tener acceso a los mensajes de correo que un servidor almacena para ella. El *cliente* será la maquina que usa el servicio POP y el *servidor* el que proporciona este servicio.

POP no intenta proporcionar multitud de operaciones de gestión de correo, normalmente *baja* los mensajes de correo y los borra del servidor.

Inicialmente, el servidor está usando una conexión TCP y *escuchando* el puerto 110. Cuando un cliente quiere hacer uso del servicio, establece una conexión TCP con el servidor, que le responde dándole la bienvenida. El cliente y el servidor POP intercambian órdenes y respuestas (respectivamente) hasta que la conexión llega a su fin y es cortada.

Existen numerosos servidores de correo POP, y en muchos casos de carácter gratuito. Por poner algún ejemplo podríamos citar hotmail o yahoo. Uno de las situaciones más típicas es el uso casual de estos servicios por parte de los clientes, con lo que la descarga de los mensajes del servidor no es habitual y éste se sobrecarga. Muchas veces también, los mensajes leídos no son borrados, sino mantenidos en el servidor. Además POP no permite una eficaz descarga de mensajes de cientos o miles. Todo ello lleva a los administradores de los servidores POP a tomar ciertas medidas como por ejemplo:

- Limitar al usuario la cantidad de espacio libre en el servidor para el almacenamiento del correo. Como consecuencia de ello, cuando la cuota es excedida, el usuario es incapaz de recibir nuevos mensajes. Normalmente los clientes son informados de esta situación.
- Imponer una política de tratamiento del correo. Por ejemplo, un sitio puede borrar los mensajes que no son leídos al cabo de 60 días y borrar los leídos a los 7 días.

Para pensar:

Cuando configuramos una cuenta de correo, el programa cliente (Outlook, Outlook express, Eudora, etc.) nos solicita la dirección de los servidores pop y smtp, lo que nos están pidiendo son dónde se alojan los servidores con los que nos vamos a comunicar a través de estos protocolos y cuya función es la recepción o entrega de correo.

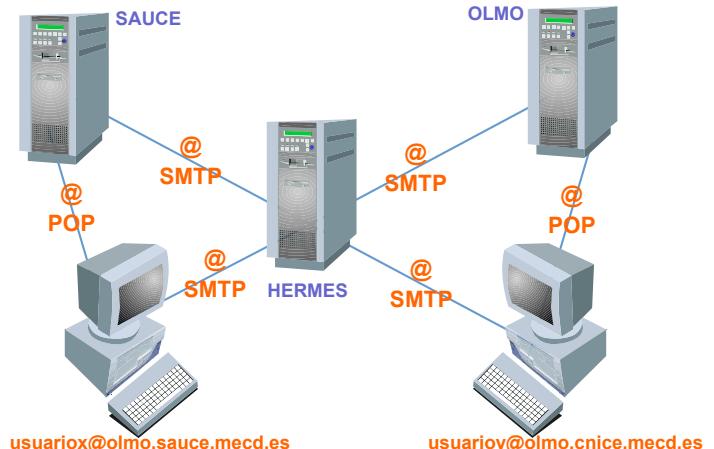


Ilustración 44: Comunicación completa de correo

Anotaciones

4.13. IMAP.

Otro protocolo usado para el manejo del correo es IMAP (*Internet Message Access Protocol*). Es muy similar al protocolo POP, aunque tiene ciertas características adicionales. Por ejemplo, mediante IMAP se puede realizar una búsqueda por palabras en los mensajes mientras que éstos están todavía en el servidor, eligiendo así cuáles quieras descargar. En otras palabras, IMAP permite a una aplicación cliente el acceso a los mensajes almacenados en un servidor como si estuvieran localmente almacenados. El correo puede ser manipulado desde distintos equipos. Por ejemplo desde el equipo en casa, la estación de trabajo en la oficina o el portátil mientras se viaja *sin la necesidad de transferir archivos* entre estos equipos.

El protocolo POP da mejores resultados para cuando el tratamiento del correo es desde un solo equipo: los mensajes son descargados y borrados del servidor. Evidentemente este método no es lógico cuando se necesita consultar el correo desde distintos sitios. Se tendrían repartidos los mensajes en los distintos equipos.

Algunas características de IMAP son:

- Es completamente compatible con los estándares usados en los mensajes de Internet, por ejemplo MIME.
- Permite el acceso y tratamiento de los mensajes desde más de un equipo.
- Proporciona acceso en línea, off-line, y en modo desconectado.
- El software del cliente no necesita saber el formato de almacenamiento del servidor.

El protocolo incluye operaciones para crear, borrar y renombrar buzones de correo, comprobar si hay nuevos correos, borrarlos permanentemente y operaciones de búsqueda entre otras.

4.14. Sincronización horaria.

Un aspecto que puede pasarnos por alto, pero que sin embargo es muy importante, es el tema de la sincronización horaria de nuestro equipo. En muchos casos es importante que nuestro servidor tenga la hora exacta, o que una red de ordenadores mantenga la misma hora. Para ello existen diversas aplicaciones que conectan nuestras estaciones de trabajo con servidores que supuestamente son más fiables, o están conectados a una fuente horaria casi perfecta. Esta fuente suele ser un reloj atómico o poseer unidades de sincronización GPS.

Estos servidores soportan protocolos como NTP, Time/UDP, o Time/TCP.



Ilustración 45: Imap: Permite hacer una selección en el servidor de correo de los mensajes que se encuentran almacenados

Anotaciones

NTP (Network Time Protocol), por ejemplo, es un protocolo basado en TCP/IP que asegura una sincronización al milisegundo de la estación de trabajo con el reloj del observatorio naval de los EE.UU. en Washington. Para ello es necesario que una aplicación cliente esté funcionando en la estación de trabajo. NTP envía peticiones periódicas a servidores, obteniendo información precisa para ajustar el reloj cliente.

Esto se consigue gracias a que una serie de máquinas (stratum 1) "preguntan" la hora a relojes atómicos, osciladores precisos, o máquinas que reciben señales GPS. Otras máquinas (stratum 2) "preguntan" a su vez a las maquinas de stratum 1. Y a su vez las stratum 3 "preguntan" a los stratum 2. Finalmente las máquinas de los usuarios se sincronizan con los stratum 3.

Cuanto más nos alejemos de los stratum 1 menos exactitud tendremos al sincronizar nuestra máquina, pero teniendo en cuenta que los ordenes de magnitud son de milisegundos, este desfase es despreciable.

Tener el ordenador puesto en hora, supone varias ventajas:

- Sabremos la hora correcta en cualquier momento.
- Tendremos una fiabilidad razonable en las fechas al usar el Correo electrónico. Por ejemplo, cuando mandemos un e-mail, la hora con la que llegue a su destino será correcta y no se producirán malentendidos ni paradojas.
- La detección de problemas de seguridad frecuentemente exige poder comparar logs de acceso de máquinas diferentes, para lo que es imprescindible la coincidencia horaria de las mismas.
- En general es muy útil el disponer de datos horarios precisos entre equipos, bien sea para la detección de problemas de hardware y /o software, así como para el estudio estadístico de los mismos.
- Y sobretodo porque si tenemos un servidor que dé servicios de red donde la hora sea algo vital necesitaremos tenerlo sincronizado.

5. Internet como red p2p.

Últimamente, las siglas P2P están incorporadas a la jerga de Internet, en los medios de comunicación y en todos los despachos que tengan relación con ordenadores.

Esta tecnología, por tanto, se basa en intercambios directos de información. No hay ningún elemento que pudiera hacer algún tipo de control centralizado.

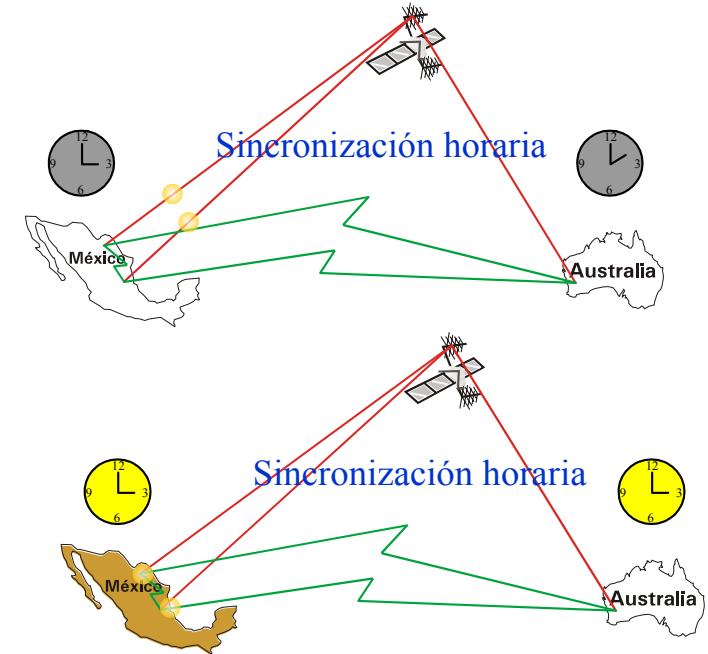


Ilustración 46: Sincronización horaria

Anotaciones

Capítulo 4: Internet

Según esto, se puede decir que se vuelve a los inicios de Internet cuando las grandes universidades se intercambiaban datos de igual a igual. Internet se diseñó inicialmente, con el propósito de intercambiar información entre ordenadores, a través de sus direcciones IP. Las grandes bases de datos, motores de búsqueda, portales, servidores, etc... han ido apareciendo después, según han ido surgiendo nuevas necesidades y también intereses comerciales o de otro tipo.

P2P permite que cualquiera pueda intercambiar ficheros de todo tipo con cualquiera, directamente, sin necesidad de ningún servidor que haga de intermediario. Puede poner a disposición de millones de personas, una obra de arte, música, etc. Representa el triunfo de la descentralización frente al control central. El PC de cualquier usuario, que hasta ahora era un elemento pasivo, únicamente recibiendo información, puede convertirse en un elemento activo, que también puede dar información a otros o participar en algún proceso común, aportando su capacidad de procesamiento. La gente tiene información que quiere compartir con los demás. Con esta tecnología se está dando más importancia al PC. Esta forma de trabajar se llama "**proceso distribuido**". Puede ser especialmente útil para la colaboración en tareas muy complejas, que a un ordenador único le costaría demasiado. Más controvertido resulta el intercambio libre de ficheros, obras de arte, música, etc., que están sujetas a leyes de propiedad.

Actualmente, para mandar un archivo por el correo electrónico hay que pegarlo en un mensaje, porque aunque los ordenadores estén unidos por una red, no se puede grabar el archivo directamente en el otro ordenador. Con la tecnología P2P se puede mandar información directamente de un ordenador a otro sin tener que pasar por máquinas centrales (servidores) que están en Internet.

Particulares, empresas, organizaciones, etc., pueden beneficiarse de este método de intercambio de información sencillo y gratuito.

Estamos aún en los comienzos de esta tecnología y habrá que resolver problemas como el ancho de banda, que es muy pequeña todavía en muchos usuarios, la falta de seguridad, etc.

Hay expertos que creen que la explotación comercial de Internet y su adopción en masa en los años noventa son una de las causas de la actual centralización de la Red. Esto hizo que surgieran empresas con grandes servidores que hacen de intermediarios y proveedores en Internet. Con P2P se puede compartir música, fotos en una comunidad de fotógrafos, juegos en línea, agendas o información sobre los stocks por parte de los proveedores de una empresa de suministro.

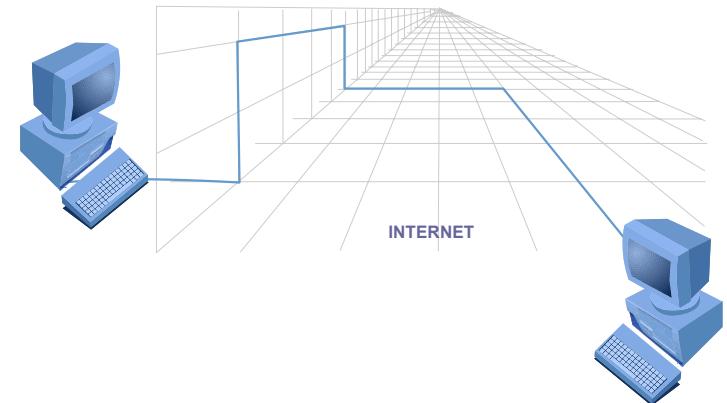


Ilustración 47: P2P: A través de Internet se pueden establecer comunicaciones p2p para realizar intercambios de datos

Anotaciones

5.1. Tecnologías.

a) Freenet.

Freenet es uno de los servicios P2P que está ganando adeptos con mayor velocidad. Aquí se puede intercambiar cualquier información, sin ningún tipo de censura. Su creador, Ian Clarke es un apóstol de las fórmulas de intercambio entre iguales y cree que Freenet supone una revolución en la distribución de contenidos. Su idea todavía no se ha traducido en beneficios, a pesar de que cobra por ciertos servicios de almacenamiento y ancho de banda.

Pero la polémica más fuerte gira en torno al carácter ilegal o inmoral de sus contenidos, el 59% de los textos que se intercambian tratan sobre drogas y el 89% de las imágenes son pornográficas.

b) Aimster.

Aimster permite el intercambio de archivos uniéndolos a mensajes instantáneos. Para ello, cifra la información y es imposible reconocer qué tipo de archivos están siendo enviados (música, datos, videos, etc.)

c) Gnutella.

Gnutella es, básicamente, una red de ordenadores descentralizada, carente de servidor central. No se trata de un programa, es más bien una tecnología, un protocolo que permite interconectar ordenadores que estén “escuchando” señales enviadas desde otros equipos. Va de usuario en usuario buscando la información que necesita, esto hace que la búsqueda sea muy laboriosa y si las comunicaciones entre ellos son muy lentas el proceso se puede colapsar. A pesar de sus siglas iniciales GNU, no está claro que sea un programa de código libre y abierto.

d) Mensajes instantáneos.

La mensajería instantánea es uno de los sistemas de intercambio de archivos entre iguales más extendidos en su uso. Se puede enviar correo o conversar en directo sin ningún servidor central. Este servicio es ofrecido por redes como Jabber o Aimster. Normalmente, son servicios gratuitos que hacen dinero cobrando comisiones por el tráfico que generan en la web.

e) Búsquedas personales.

Opencola ha trasladado el concepto de intercambio de archivos a los motores de búsqueda. Pone en contacto a distintas personas, que así pueden compartir sus direcciones favoritas de Internet. Permite comparar una solicitud de búsqueda de un usuario con los resultados obtenidos por otros de perfiles similares. El negocio de Opencola se centra en vender su innovación tecnológica a buscadores tradicionales.

Anotaciones

f) Caso NAPSTER.

Napster, aún no siendo estrictamente un programa P2P (hay algún servidor central entre los usuarios), es el programa que ha revolucionado el panorama de Internet.

El intercambio de música libremente, sin tener en cuenta los derechos de autor, ha hecho poner el grito en el cielo a las industrias discográficas que han demandado a esta compañía.

Napster guarda una relación de la música que ofrecen todos sus usuarios, él directamente no la ofrece, solamente hace de intermediario.

La jueza encargada del caso, ha obligado a Napster a parar este intercambio gratuito.

Fechas:

- (13/02/2001) Los jueces ordenan a Napster que cese el canje de música gratuita.
- (30/01/2001) El portal de música Napster pasará a ser de pago a mediados de año.
- (20/12/2000) EMusic demanda a MP3.com por violar los derechos de autor.

Estas sentencias han afectado a otras compañías que también pueden quedar al margen de la ley. En este caso se encuentra el programa **Aimster**, combina mensajería con intercambio de ficheros o **IMesh**, de origen israelí y muy extendido. Estos programas, para no ser demandados como en el caso de Napster, permiten sólo un intercambio entre amigos, cosa que legalmente no está tan clara que sea ilegal como en el caso anterior.

5.2. Utilidades.

Además de permitir el intercambio de información directamente, también es posible utilizar el P2P en plataformas de comercio mayorista. Las empresas podrían publicar en sus ordenadores todo aquello que quieren vender de forma que se pueda acceder directamente a sus catálogos. Sería una manera de suprimir intermediarios en el comercio mayorista. Este mercado está interesando a gran cantidad de empresas.

Para Andrew McAfee, profesor de la Harvard Business School en Boston, el modelo en que se apoya hoy el comercio electrónico mayorista "tiene los días contados". McAfee está convencido de que el modelo emergente basado en las redes punto a punto es mejor: "Permitirá que cualquier compañía esté donde esté localice otras empresas con las que hacer acuerdos comerciales en la Red de forma más ágil, segura y eficiente, sin necesidad de un servidor central".

Anotaciones

Con P2P las compañías, sobre todo las pequeñas, tendrán un método mucho más simple para operar. Una empresa que tenga ya la información en una base de datos propia, no tendría que hacer otra para colgarla en un servidor central.

Esto no significa que desaparezca el modelo anterior. Seguirá habiendo servicios que las compañías no pueden proporcionar por ellas mismas.

6. Posibilidades de futuro.

Durante los cinco últimos años estamos experimentando la entrada en nuestra vida de un fenómeno llamado Internet. De forma similar a la evolución de la telefonía móvil, la cual ha originado una nueva forma de comunicación entre las personas, mediante el uso de Internet, "la red", se han conseguido nuevas formas de comunicación y de colaboración tanto en el terreno personal como laboral.

Nacieron nuevas formas de comunicación, más interactivas, el chat, el correo electrónico, la videoconferencia, ... Hasta la irrupción de Internet, básicamente utilizábamos tres formas de comunicación principales: la comunicación oral, la epistolar y la telefónica. Si analizamos cada una de estas observaremos lo siguiente:

- Mediante la comunicación **oral**, se consigue un medio *interactivo* y de *realimentación* inmediata entre los interlocutores. Así mismo, la forma de *intercambio de documentación relacionada* con la comunicación es manual. Muchas veces es necesario establecer un espacio tanto temporal como físico para poder llevar a cabo el encuentro, lo cual no siempre es posible si los interlocutores se encuentran en lugares muy distantes o tienen dificultades varias de movilidad.
- Mediante la comunicación **telefónica**, los interlocutores tienen una comunicación similar a la oral, pero se pierden ciertos aspectos de *comunicación gestual*, los cuales durante una comunicación oral sí son explícitos. Una ventaja de esta comunicación es que no existen barreras espaciales. Pero no se permite la transferencia de documentación utilizando este medio. (Para evitar en parte este problema se utiliza el fax).
- Mediante la comunicación **epistolar**, se tiene un medio no interactivo de comunicación, ya que el origen de la comunicación envía su mensaje y la forma de transmisión de dicho mensaje hace que la recepción de dicho mensaje y la respuesta no sean inmediatas. Un factor importante a tener en cuenta en este tipo de comunicación es la *distancia entre los puntos de comunicación*. Sin embargo, a diferencia de la comunicación telefónica, esta sí permite el envío de documentación adjunta.

Con Internet se consiguió salvar la distancia geográfica, ya que mediante esta red, al igual que con la telefónica se permite la comunicación simultánea de personas situadas en puntos muy

Anotaciones

distantes. Además se mejoran ciertos aspectos de este tipo de comunicación, se permite la transferencia de todo tipo de documentación, tanto textual como multimedia. Sin embargo no se consigue transmitir la expresión gestual o la intencionalidad del texto que se comunica. La comunicación puede ser escrita (como en el caso del chat y del e-mail) o bien visual (como las conexiones de videoconferencia o las retransmisiones utilizadas últimamente, el streaming).

Además gracias a la popularidad de la tecnología informática y su rápida expansión por todo el mundo, cada vez existen más utilidades y aplicaciones para facilitar la comunicación, se trabaja en entornos universitarios junto con grandes organismos en el diseño de *traductores simultáneos* y lenguajes naturales que faciliten el uso y el trabajo conjunto de distintas sociedades lingüísticas para fines comunes.

Como no, Internet se ha convertido en la gran “biblioteca universal”, cualquier información que se necesite sobre cualquier tema, se puede localizar mediante los *buscadores*. Esta capacidad de la red, como en todas las disciplinas, puede ser un arma de doble filo, en cuanto a la privacidad o no de ciertos datos, pero a la vez permite un nivel nunca visto antes de aproximación a muy diversos temas, ya que la red contiene todo. No deja de ser un punto de unión entre personas de distintas culturas y sociedades.

Los gobiernos están haciendo grandes progresos en el desarrollo de plataformas para proveer de servicios *online* a sus ciudadanos. Cada vez se trabaja más en el estudio de formas de identificación remota de los individuos, protocolos de seguridad y firma electrónica. Poco a poco la legislación se va ajustando a los requerimientos que esta nueva red con tanta información requiere, poniendo las limitaciones jurídicas y penales necesarias según el uso que se haga de ella.

Se utiliza también como forma de protesta manifiesta ante situaciones sociales no deseables. No se tiene sensación de barreras físicas o de lejanía.

En estos últimos puntos, se abre un debate muy interesante a cerca de una forma de marginación hacia los países del mundo no desarrollado, ya que la falta de acceso a estas tecnologías, les sumerge en un mundo de no-conocimiento que en otros países sí se potencia y ya se está hablando de una nueva forma de marginación de dichos países respecto a los supuestamente más ricos.

Pero el ámbito de Internet no solo se queda en el entorno laboral o social, poco a poco se ha ido introduciendo en el entorno doméstico y educativo. En el ámbito doméstico, de momento no deja de ser un simple mecanismo de comunicación. Se estima que en el próximo año un 7% de hogares acceda a Internet, lo que supone 10 millones de hogares nuevos conectados a la Red (en Europa). A esto ayuda la inversión realizada en infraestructuras de **banda ancha**, lo cual facilita el que Internet se convierta en una herramienta habitual para la comunicación y la información.

Hasta ahora la forma más habitual de conexión a Internet en el entorno doméstico era el módem y la línea telefónica. Debido a los costes económicos de un uso continuado de las líneas telefónicas, surgieron las llamadas **tarifas planas**, para facilitar y animar a la población no laboral o

Anotaciones

Capítulo 4

bien a las personas que en su entorno de trabajo ya disponían de estos medios de comunicación, el uso de Internet en su ámbito doméstico. Pero en los últimos dos años se han ido introduciendo nuevas técnicas que permiten una mayor utilización de la red. La implantación cada vez más del **cable** o de la banda ancha están facilitando a los hogares la incorporación de esta nueva puerta de comunicación con el mundo, no solo con tu ciudad, ni con tu país.

Otra tecnología casi experimental hoy en día, excepto en lugares de difícil acceso o bien donde el montaje de infraestructura no sale rentable, es el inalámbrico, *wireless*. Cada vez en entornos rurales, donde no se dispone de la red cableada, como se entiende en las grandes ciudades, se opta por este tipo de conexión para no quedarse “aislado” ni atrás en esta carrera por la información. Se trabaja cada vez en trabajar los estándares (las reglas de funcionamiento) de este tipo de tecnología y esto se prevé que facilite la instalación de pequeñas redes en el entorno doméstico, ¿quien no ha oído hablar de una red que administre nuestros electrodomésticos, luces, calefacción y seguridad en general de la casa, lo que se está llamando “casa inteligente”?

Como reflexión final planteo una simbología entre la red de redes y la biología, se puede decir que Internet es una gran red neuronal, no deja de ser un punto de encuentro de toda la gente con espíritu de compartir algo o de comunicación, por lo que durante los siguientes años se irá viendo hasta donde se deja que entre dicha tecnología e información. De forma similar a la irrupción de los medios de comunicación, radio y televisión, durante los años 50 y 60, considero a Internet como la forma más rápida y completa para la comunicación. Considero que hoy por hoy es un sistema muy abierto, y durante los próximos años se irán delimitando los mecanismos de acceso y se depurarán las informaciones vertidas a la red.

Anotaciones

Ilustraciones

Ilustración 1: Internet	3
Ilustración 2: Cronología del desarrollo de Internet	4
Ilustración 3: PSI: Los proveedores de servicio permiten realizar la conexión a Internet una vez que nos hemos identificado	5
Ilustración 4: Pila de protocolo TCP/IP	7
Ilustración 5: Modelo de capas de TCP/IP	8
Ilustración 6: Protocolo orientado a conexión es el que permite la creación de un circuito virtual	9
Ilustración 7: La transición de datos en Internet constituye un proceso de tres fases	10
Ilustración 8: TCP/IP: Permite un uso óptimo de las redes de medio compartido ya que evita el colapso del canal de comunicación	11
Ilustración 9: Número de secuencia: es el campo que permite ordenar los paquetes de datos al equipo receptor	12
Ilustración 10: Proceso deertura de conexión	14
Ilustración 11: Control de flujo mediante sistema de parada y espera	15
Ilustración 12: Control de flujo mediante el método de ventana deslizante	16
Ilustración 13: Checksum es el campo que permite averiguar si los datos de la trama TCP contienen errores	17
Ilustración 14: ACK: el número de acuso de recibo ACK tiene múltiples utilidades, una de ellas es para cerrar la conexión	18
Ilustración 15: Los buffers son una memoria intermedia en donde se almacenan los datos hasta que pueden ser procesados por la aplicación correspondiente	19
Ilustración 16: Puerto: un equipo dispone de distintas destinos que deben ser identificados para que los paquetes de datos lleguen correctamente	20
Ilustración 17: Solicitud de dirección IP a servidor para traducir direcciones de dominio	22
Ilustración 18: La IP presta servicio de transporte de red a TCP	23
Ilustración 19: Fragmentación es cuando los requisitos de la red lo hacen necesario IP divide los paquetes añadiéndolas una cabecera de datos IP	24
Ilustración 20: El tiempo de vida de un paquete de datos determina el nº máximo de veces que puede cambiar de red un datagrama IP	25

Anotaciones

Capítulo 4

Ilustración 21: Los datagramas IP incluyen la dirección de red de los dispositivos que hacen de pasarela entre redes hasta que lleguen a la red de destino	26
Ilustración 22: IP puede viajar encapsulado en tramas distintas en función del tipo de red por el que se mueve	27
Ilustración 23: Los datagramas IP viajan encapsulados en tramas de datos de las capas físicas (Ethernet, ATM, ...) cada vez que llega a otra red un dispositivo de red desencapsula los datos y los reenvía en función del encabezado del datagrama (red de destino)	28
Ilustración 24: El protocolo IP maneja como únicas direcciones, la dirección de Internet	29
Ilustración 25: Las direcciones IP pueden tener una correspondencia con direcciones de nombre de dominio	30
Ilustración 26: La dirección IP identifica direcciones de Internet, pero viaja acompañada de la dirección física del dispositivo de red al que se dirige el paquete.	31
Ilustración 27: La máscara de subred define la parte de la dirección IP que corresponde a la red y la que corresponde al equipo	32
Ilustración 28: Red Clase B se realiza un mensaje de Broadcast poniendo a 1 los dos últimos octetos de la dirección IP	33
Ilustración 29: Direcciones Clase B y Clase C: Un dispositivo puede disponer de una dirección Clase C y otra Clase B en función de las redes que interconecte	34
Ilustración 30: Red privada: Se identifica hacia afuera por la dirección IP externa del servidor proxy, quien determina, en función de los datos que incorpora el paquete, cual es la dirección interna de destino	38
Ilustración 31: Protocolo ARP: Permite averiguar la dirección física de un dispositivo del que se conoce su dirección	39
Ilustración 32: Protocolo RARP: Conocida la dirección física de un dispositivo permite averiguar la dirección IP	40
Ilustración 33: Protocolo ICMP: Permite la obtención de información sobre el estado de una red.	41
Ilustración 34: Servidor de acceso a Internet: Es una máquina que actúa como un modem por un lado y como un concentrador por el otro	42
Ilustración 35: HTTP: Permite el intercambio de información entre servidores web y navegadores. Utilizan TCP/IP para transferir los archivos. Es un protocolo del nivel de aplicaciones	43
Ilustración 36: Servidor FTP: Permite realizar operaciones, transferir archivos entre clientes y servidores FTP y realizar operaciones sencillas como mover directorios	47
Ilustración 37: VNC (Virtual Network Computing): Permite el acceso a otro equipo vía internet y encontrarlo	48

Anotaciones

Capítulo 4: Internet

Ilustración 38: Telnet: Permite acceder a un servidor a través de Internet transformando el PC en un terminal de red	49
Ilustración 39: Resolver: Informa a la aplicación solicitante, por ejemplo un navegador, de la dirección IP correspondiente a un nombre de dominio	51
Ilustración 40: Nombres de dominio	52
Ilustración 41: Servidor primario: Conoce los nombres de dominio inferior	53
Ilustración 42: Servicio SMTP: Realiza la transferencia de correo entre servidores de este tipo de servicio	54
Ilustración 43: Pop: Permite descargar el correo de un servidor	55
Ilustración 44: Comunicación completa de correo	56
Ilustración 45: Imap: Permite hacer una selección en el servidor de correo de los mensajes que se encuentran almacenados	57
Ilustración 46: Sincronización horaria	58
Ilustración 47: P2P: A través de Internet se pueden establecer comunicaciones p2p para realizar intercambios de datos	59

Anotaciones