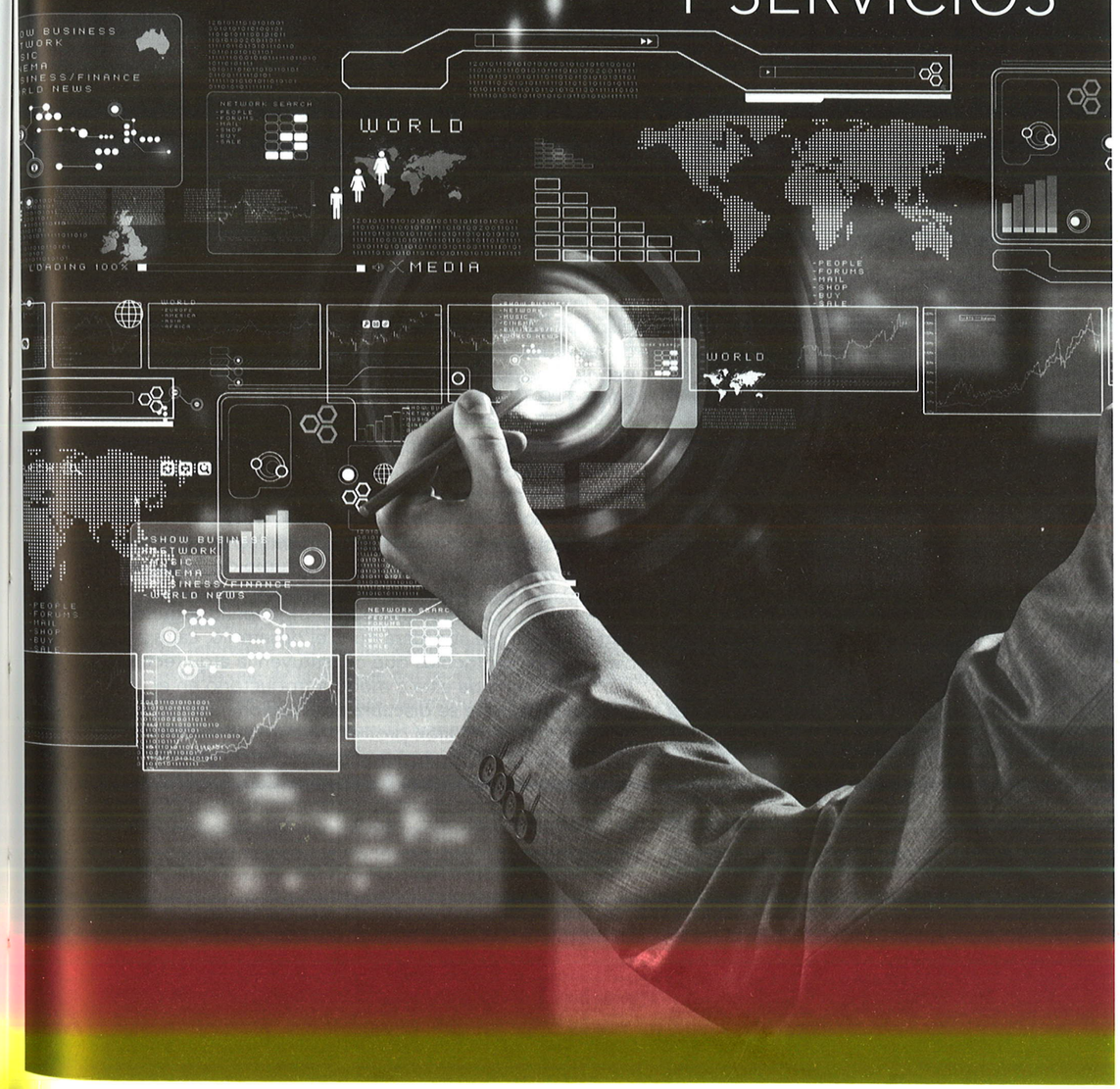
J. Heinanen, R. Guerin. RFC 2697: «A Single Rate Three Color Marker», 1999.
J. Heinanen, R. Guerin. RFC 2698: «A Two Rate Three Color Marker», 1999.
B. Braden, D. Clark, J. Crowcroft, B. Davie, S. Deering, D. Estrin, S. Floyd, V. Jacobson, G. Minshall, C. Partridge, L. Peterson, K. Ramakrishnan, S. Shenker, J. Wroclawski, L. Zhang. RFC 2309: «Recommendations on Queue Management and Congestion Avoidance in the Internet», 1998.

PARTE II

INTERNET, ARQUITECTURA TCP/IP, PROTOCOLOS Y SERVICIOS



Continuando con la línea seguida hasta el momento, el próximo capítulo a estudiar correspondería a la capa de transporte, primera de las capas denominadas extremo a extremo, por cuanto que las funciones a implementar solo involucran las estaciones finales no los elementos y dispositivos propios de la subred. Si bien en el contexto de las redes que siguen el modelo OSI se encuentran definidos varios protocolos de capas superiores tales como TP0-TP4, en la capa de transporte, o FTAM, en la de aplicación, estos no han encontrado una gran difusión en las redes actuales. Frente a OSI, TCP/IP sí constituye un conjunto de protocolos con una enorme implantación gracias a la creciente expansión de Internet. ¡Quién no ha oído hablar de servicios tales como DNS o HTTP! Es por ello que en esta segunda parte centraremos nuestra atención de forma exclusiva en el estudio de las capas del modelo TCP/IP, en definitiva, de Internet.

A lo largo de los temas que componen la segunda parte del libro se abordará pues el desarrollo, capa a capa, de los protocolos que constituyen la arquitectura TCP/IP. Presentada esta a modo introductorio en el Capítulo 8, donde se discutirá el direccionamiento IP, en el Tema 9 se estudiarán protocolos como IP, ICMP, BGP e IGMP, todos ellos relacionados con funciones propias de la capa de red. Por su parte, en el Capítulo 10 se presentan los protocolos de transporte TCP y UDP y en el Capítulo 11 protocolos correspondientes a servicios ampliamente usados a nivel de aplicación tales como DNS, SMTP o HTTP. Adicionalmente a estos protocolos que forman parte de la arquitectura básica de Internet, en los dos últimos capítulos del libro se abordarán cuestiones de gran relevancia. Así, en el Capítulo 12 se tratarán aspectos de gestión y seguridad en Internet, mientras que en el Tema 13 se analizará de forma breve un aspecto de alta transcendencia: la movilidad.

CAPÍTULO 8

FUNDAMENTOS DE INTERNET

8.1. Introdución
8.2. Historia y organización de Internet
8.3. Estructura y arquitectura de Internet
8.4. Direccionamiento Internet
8.5. Protocolos de resolución de direcciones
8.6. Debilidades del direccionamiento IP
8.7. Máscaras de red
8.8. Traducción de direcciones de red

Tras el estudio realizado en los temas precedentes sobre las capas inferiores del modelo, incluyendo la capa de red, este capítulo es el primero de cuatro dedicados en exclusiva al análisis de la arquitectura TCP/IP, en la cual se fundamenta Internet. Como tema introductorio que es, este capítulo comienza presentando generalidades sobre Internet acerca de su génesis, evolución y organización. Seguidamente, en el tercer apartado se estudia la estructura y arquitectura de Internet. En el Apartado 8.4 se presentan los diferentes esquemas de direccionamiento para las tres capas del modelo de referencia TCP/IP, haciéndose hincapié en el direccionamiento IP. Tras ello, como paso previo al estudio que de la capa de red de TCP/IP se realizará en el próximo capítulo, en el siguiente apartado se abordan los protocolos de resolución de direcciones. En el Apartado 8.6 se identifican las debilidades del direccionamiento IP, y motivados por la escasez de direcciones, en el Apartado 8.7 se define el concepto de máscara de red y se explica la asignación de direcciones con sub-redes y súper-redes. Por último, en el Apartado 8.8 se estudian los esquemas de traducción de direcciones, utilizados también para mejorar el uso del espacio de direcciones IP. El capítulo concluye con las habituales secciones de resumen, ejercicios y bibliografía relevante.

8.1. Introducción

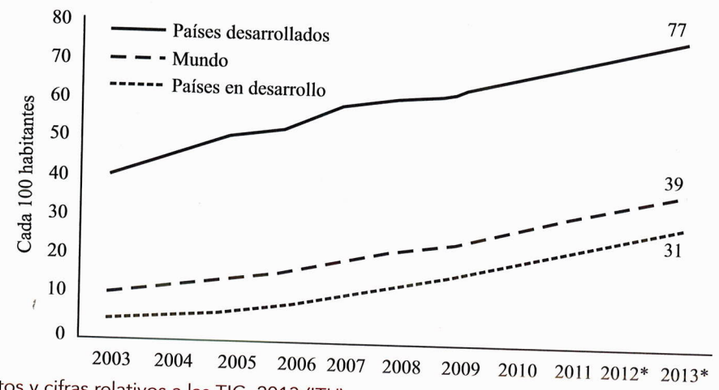
Resulta incuestionable la proyección social, económica y cultural alcanzada por Internet. La Red, como así se le conoce, ha supuesto una verdadera revolución en nuestra forma de vida, proporcionando no solo un medio de comunicación más rápido y eficaz, con las implicaciones que ello tiene

en diversos aspectos de la vida cotidiana, sino modificando incluso nuestros hábitos y relaciones personales.

Internet, adoptando la arquitectura TCP/IP, se ha desplegado con notable éxito en todo el mundo. El volumen de tráfico, el número de usuarios, el número de equipos y otros indicadores muestran una tendencia creciente año tras año. Este crecimiento (Figura 8.1) se materializó en una predicción para 2013 según la cual más de 2.700 millones de personas utilizan Internet, es decir, el 39% (casi el 80% si se consideran solo países desarrollados) de la población mundial tiene acceso a Internet; frente al 10% que lo tenía en 2003.

Algunos de los principios de diseño adoptados para la arquitectura TCP/IP y que justifican el éxito de Internet son los siguientes:

1. *Evolución y cambio permanente*. El sector de las tecnologías de la información y las comunicaciones se caracteriza por una evolución permanente. En este contexto tan cambiante, principios que parecían inmutables hace unos pocos años son desechados con el devenir de tiempo conforme avanza la tecnología. Uno de los pilares en los que se basa el éxito de Internet es adoptar, en coherencia, una actitud de cambio permanente, siendo quizás este el único principio de Internet que nunca cambiará.
2. *Heterogeneidad*. Esta es otra de las características diferenciadoras de Internet. Lejos de adoptar una visión monolítica, en Internet se proponen soluciones para un conjunto siempre variado y diverso de elementos. Esto implica, por ejemplo, considerar diferentes dispositivos de usuario, diferentes tipos de tráfico generados por servicios diversos, diferentes API («Application Programming Interface»), además de diferentes tecnologías para las capas inferiores, entre otras muchas cuestiones.
3. *Escalabilidad*. Si algo se propone y se adopta en Internet debe ser escalable. Es decir, cualquier solución debe funcionar con iguales prestaciones con independencia del volumen o tamaño del universo al que se aplique. Directamente relacionado con esto, el principio de amplificación establece que pequeñas perturbaciones en grandes infraestructuras (en nuestro caso redes) pueden desencadenar inestabilidades globales. El diseño de Internet debe garantizar que estas perturbaciones ocurran raramente.



Fuente: Datos y cifras relativos a las TIC, 2013 (ITU).
* = Predicciones realizadas cuando se publicó este estudio.

Figura 8.1. Número de usuarios con acceso a Internet por cada 100 habitantes.

4. *Robustez e interoperabilidad*. Según estos principios, el diseño ha de prever cualquier tipo de error, por pequeño e improbable que sea. En consecuencia, este principio persigue maximizar la interoperabilidad entre las diferentes implementaciones.
5. *Modularidad y acoplamiento débil*. Estos principios (inspirados en el modelo OSI) aluden a la necesidad de dividir las distintas funcionalidades en módulos o capas bien diferenciadas. Además, según el principio de acoplamiento débil, el diseño ha de ser tal que cada componente dependa lo menos posible de los demás.
6. *Complejidad en los extremos*. Este principio implica que ningún procedimiento debería ser ejecutado dentro de la red (en los nodos de interconexión) mientras pueda ser ejecutado en los extremos. Como principal consecuencia, la red es agnóstica respecto al tipo y detalles de la comunicación entre las aplicaciones, lo que permite dar soporte a aplicaciones muy diferentes entre sí.
7. *Sencillez*. Este principio establece que, en caso de duda, se debe optar siempre por la solución más sencilla.

Los principios enumerados con anterioridad han sido pieza clave en el éxito de Internet. Sin embargo, la práctica universalización de Internet (especialmente en países desarrollados) no habría sido tal sin el despliegue de un número importante de servicios eficaces que responden a una demanda real de los usuarios. Entre otros, los más significativos (explicados con detalle en el Capítulo 11) son:

— *Web*. Aplicación Internet por antonomasia, esta aplicación posibilita, mediante un entorno gráfico, el acceso universal a recursos (texto, imágenes, gráficos, etc.) y el desplazamiento (o «navegación») por el entramado de «hiperenlaces» (concepto clave en el desarrollo de Internet) existentes en la Red. En el contexto de esta tecnología, se han desarrollado nuevos servicios como el comercio electrónico, fundamental en el desarrollo de la nueva economía, así como las denominadas *redes sociales*. Estas últimas, aunque no implican una tecnología diferenciadora, han popularizado aún más si cabe la web.
— *Correo electrónico*. Es otra de las aplicaciones determinantes del éxito de Internet. El servicio de *e-mail* consiste en la transferencia de mensajes electrónicos entre usuarios con independencia de su localización espacial y temporal. Hoy día se ha convertido en una herramienta estratégica en el entorno empresarial y de negocios.
— *Transferencia de ficheros*. A través de este servicio se posibilita la transmisión de archivos entre dos *hosts*. Fue una aplicación esencial para el despegue de Internet, aunque en la actualidad está siendo sustituida por el servicio web y las redes P2P («Peer-to-Peer»).
— *Acceso remoto*. El servicio *telnet* —también esencial en los comienzos de Internet aunque cada vez menos usado— o el más utilizado, reciente y seguro *ssh*, permite el acceso o ejecución de procesos en máquinas remotas. Así, podemos conectarnos a un *host* distinto del nuestro y trabajar como si este fuese local, haciendo uso de sus recursos de disco, memoria, etc. como si fuesen propios.
— *Audio, vídeo y juegos*. Las aplicaciones multimedia (en sus distintas modalidades: interactivas, de *streaming*, de pago por consumo, etc.) son otro de los pilares fuertes de Internet. No en vano, una predicción para el 2017 estima que el 70% del tráfico total (incluyendo entornos fijos y móviles) será de vídeo sobre IP. La tecnología de interconexión y los protocolos de Internet, aunque inicialmente no fueron concebidos especialmente para ello, se han erigido en la tecnología de convergencia. Esto significa que todo el tráfico (incluso servicios de telefonía fija y móvil o de TV) está siendo cursado por los operadores sobre la Red.

Antes de proceder a un estudio en profundidad de TCP/IP, y más allá de todas las cuestiones mencionadas previamente, diremos que el nombre de la arquitectura hace referencia a los dos protocolos más importantes de la misma:

— El protocolo IP («Internet Protocol»), perteneciente a la capa de red, adopta una tecnología de conmutación de paquetes para ofrecer un servicio de transmisión no orientado a conexión y no fiable. El servicio prestado se denomina como de *mejor esfuerzo* («best effort»), ya que aun sin garantías (es decir, sin por ejemplo incluir mecanismos de recuperación de errores) transmite paquete a paquete lo mejor que puede. IP es la tecnología fundamental a través de la que se posibilita la interconexión de redes, objetivo esencial de la arquitectura TCP/IP. Además, su especificación incorpora estrictamente los principios de diseño de Internet anteriormente comentados. IP se estudiará en detalle en el Capítulo 9.

— El protocolo TCP («Transmission Control Protocol»), estudiado más adelante en el Capítulo 10, está situado en la capa de transporte. Proporciona extremo a extremo (es decir, entre las entidades finales, origen y destino) un servicio orientado a conexión y fiable. TCP resuelve los problemas que IP, salto a salto, deja sin resolver en la subred. Así, TCP relega a las aplicaciones de tener que ocuparse de la recuperación de errores, del control de flujo y del control de congestión.

8.2. Historia y organización de Internet

La Agencia de Proyectos de Investigación Avanzados (para la Defensa) norteamericana —(D)ARPA, «(Defense) Advanced Research Projects Agency»— es la responsable, junto con algunas Universidades norteamericanas, de los inicios de la actual Internet. Los desarrollos y despliegues iniciales (ARPANET) se realizaron para conseguir la interconexión de redes militares (y de universidades) ubicadas en localizaciones remotas. El eje fundamental del proyecto fue la adopción de la conmutación de paquetes como tecnología para interconectar redes, de manera que se consiguiese robustez y seguridad en las comunicaciones, además de los otros principios de diseño enumerados en la introducción. Esta aproximación permite, ante la potencial caída de enlaces y/o nodos, que la red sea capaz de encontrar rutas alternativas y, en consecuencia, permite llevar a cabo con éxito la comunicación en circunstancias adversas.

A finales de la década de 1970 se especificaron el modelo de referencia y los protocolos principales asociados, que aún hoy constituyen la base de TCP/IP. En los años 1980 se dividió la red en dos partes o redes troncales: ARPANET y MILNET, la primera para la interconexión de centros de investigación (universidades, etc.) y la segunda para comunicaciones militares. En estos primeros años de su despliegue, el uso comercial estaba vetado.

Uno de los hechos principales que propició la gran extensión de TCP/IP tuvo lugar en 1983, cuando la API BSD («Berkeley Software Distribution»), desarrollada para el sistema operativo UNIX en la Universidad de California, incorporó no solo los nuevos protocolos, sino también una serie de servicios o aplicaciones (como telnet, ftp, etc.) que, basados en el concepto de *socket* (ver Capítulo 11), constituyeron el embrión de la Internet actual.

En 1986 aparece una nueva red troncal denominada NSFNET, desarrollada por la NSF («National Science Foundation») norteamericana. Esta fundación fue la responsable del enorme crecimiento que experimentó Internet en sus principios, siendo hasta fechas no demasiado lejanas la que ha sufragado buena parte de los costes de su mantenimiento. También en la expansión mundial de Internet cabe destacar el papel jugado por la UNESCO.

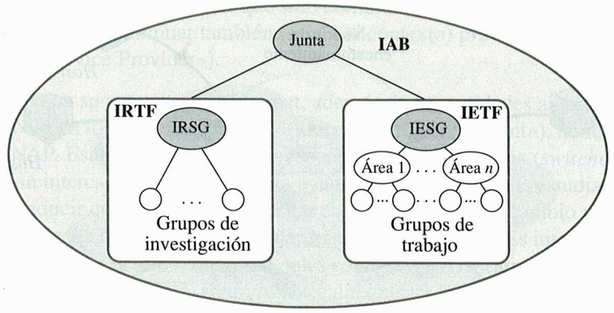


Figura 8.2. Organización del IAB.

Creado en 1983, el IAB («Internet Architecture Board», antes «Internet Activities Board» —ver http://www.iab.org—) es el organismo responsable de la coordinación internacional de Internet. Constituido inicialmente en grupos de tareas, el IAB fue reorganizado en 1989 de forma que, como se muestra en la Figura 8.2, se hizo una división en dos grandes grupos dependientes de la Junta principal:

— IRTF («Internet Research Task Force», http://www.irtf.org), dedicado a la coordinación de actividades de investigación relacionadas con los protocolos TCP/IP. A su vez, IRTF se divide en grupos más pequeños coordinados dentro del denominado IRSG («Internet Research Steering Group»).

— IETF («Internet Engineering Task Force», http://www.ietf.org). Centrado en tareas de ingeniería de red, el IETF se divide en áreas de trabajo, que a su vez se organizan en grupos de trabajo, coordinadas dentro del IESG («Internet Engineering Steering Group»).

NSFNET fundó un grupo en la AT&T destinado a llevar a cabo la gestión de aspectos administrativos y técnicos de TCP/IP y la Internet global. Es el conocido como INTERNIC («INTERnet Network Information Center», http://www.internic.org) o, simplemente, NIC. Por lo que se refiere a la documentación técnica acerca de Internet y los protocolos TCP/IP, esta se proporciona de forma libre y gratuita a través de los documentos denominados *solicitud de comentarios* o RFC («Request For Comments», ver http://www.rfc-editor.org). También cabe señalar que cierta documentación no publicada en los RFC puede encontrarse en las ya obsoletas series IEN («Internet Engineering Notes»).

8.3. Estructura y arquitectura de Internet

Como ya se ha comentado y según se desprende de lo expuesto en el apartado anterior, el término Internet se considera a lo largo del texto como sinónimo de TCP/IP, usándose en muchas ocasiones de forma indistinta.

En el Capítulo 1 ya se apuntó una visión conceptual de Internet, pudiendo verse esta como una gran red WAN cuya subred está compuesta por nodos de encaminamiento y (sub)redes (LAN y WAN) que los interconectan (Figura 8.3). En realidad, parte de las grandes infraestructuras de Internet están en manos de un conjunto de operadores que son los que las explotan comercialmente. Típicamente, el modelo de negocio de estos operadores consiste en el establecimiento de acuerdos de intercambio de tráfico entre ellos, lo que facilita la conectividad global. Para explicar y comprender la estructura de

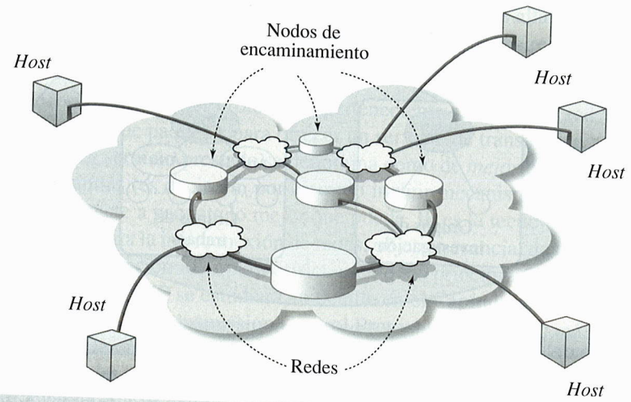


Figura 8.3. Estructura conceptual de Internet.

Internet es necesario definir los diferentes tipos de acuerdos que se establecen entre los diversos operadores de red:

1. *Acuerdos de peering*. Se trata de contratos establecidos entre dos operadores, mediante los que —sin que haya una contraprestación económica— se acuerda intercambiar un volumen de tráfico dado. Curiosamente, el acuerdo se define habitualmente en términos de velocidad de pico, y aunque no haya un beneficio monetario directo, generan un beneficio mutuo entre las partes: mayor cobertura, aumento de redundancia, más capacidad para cursar tráfico, mejores prestaciones, etc. Dentro de estos acuerdos se distingue entre *peering* público, cuando el intercambio se hace en capa 2 usando un conmutador (o *switch*) compartido en lo que se denomina puntos de acceso a la red (NAP, « Network Access Point»), y *peering* privado, el cual se realiza mediante un enlace punto a punto entre los operadores (puede que ubicados en un mismo edificio o dependencia).
2. *Acuerdos de tránsito*. A diferencia de los anteriores, en estos sí hay una contraprestación económica a cambio de que cierto operador permita a otro usar sus infraestructuras para cursar tráfico que vaya dirigido al propio operador o hacia un tercero.

Los dos tipos de contratos entre operadores identificados permiten hacer una clasificación —aceptada con bastante generalidad— de los operadores o redes troncales en Internet:

1. *Tier-1*: Son grandes operadores con infraestructuras gigantescas que se caracterizan porque para acceder a cualquier destino no necesitarían formalizar ningún contrato de tránsito con otro operador. Es decir, con solo acuerdos de *peering* pueden hacer llegar tráfico a cualquier destino en Internet. Aunque la definición no es del todo precisa, ya que es difícil conocer si un operador tiene o no acuerdos de tránsito, dentro de esta categoría se identifican del orden de 13 operadores (por ejemplo, AT&T, Deutsche Telekom, Level 3 Communications), siendo en su mayoría empresas norteamericanas.
2. *Tier-2*: Son operadores que aunque tienen acuerdos de *peering* con otros, necesitan acuerdos de tránsito para alcanzar algunas partes o redes de Internet. La mayor parte de los operadores son de este tipo.

3. *Tier-3*: Se trata de un operador que solo compra tránsito a otras redes. Esta y la anterior categoría se suelen denominar también (según el contexto) proveedores de acceso a Internet (ISP, «Internet Service Provider»).

Relacionado con su estructura de Internet, además de las entidades anteriores, el funcionamiento de Internet se basa en los denominados IXP («Internet eXchange Point»), también denominados puntos neutros o NAP. Esta denominación corresponde a infraestructuras (*switches*) a través de las que los ISP acuerdan intercambiar tráfico (con la ayuda del protocolo BGP, estudiado en Apartado 9.3.2). Su objetivo es reducir costes, pues al desplegar estos puntos de intercambio para cursar tráfico de un ISP a otro, se reduce la necesidad de contratar tránsito con terceros. Es interesante mencionar la existencia de algunos puntos neutros en España, tales como ESPANIX (http://www.espanix.net), CATNIX (http://www.catnix.net), GALNIX (http://www.galnix.net) y EuskoNIX (http://www.euskonix.com).

La arquitectura de Internet está directamente relacionada, como ya sabemos, con el modelo TCP/IP, cuyas capas constitutivas son las que se mostraron en la Figura 1.5 y que se reproducen en la Figura 8.4 para facilitar su visualización. Estas son:

1. *Aplicación:* Capa superior que implementa servicios de usuario tales como web, correo electrónico, transferencia de ficheros, etc.
2. *Transporte:* Capa extremo a extremo que involucra exclusivamente a los puntos finales de la transmisión y donde, básicamente, se adopta un modelo polarizado. Es decir, se ofrecen dos tipos de servicios: uno orientado a conexión fiable, a través del protocolo TCP (con control de conexión, de flujo, de errores y de congestión), y un servicio no orientado a conexión no fiable, mediante el empleo del protocolo UDP.
3. *Red:* Capa inferior donde se ofrece un servicio no orientado a conexión y no fiable mediante el protocolo IP. Este protocolo, a diferencia de los anteriores, opera salto a salto, es decir entre entidades separadas por una sola subred, y tiene como misiones principales la interconexión de las diferentes (sub)redes que componen Internet, así como el encaminamiento de los datos sobre ellas.

Como ya se ha mencionado, TCP/IP se caracteriza por ser independiente de la tecnología de red subyacente, pudiéndose implementar sobre cualquier red LAN o WAN existente. A modo de ejemplo, en la Figura 8.4 se muestra la implementación de este modelo sobre una red LAN genérica. Para hacer ello posible, se suele recurrir a protocolos específicos que llevan a cabo «funciones de interfaz» entre IP y la capa inferior sobre la que este protocolo (y en definitiva el modelo) se sustenta. Este es

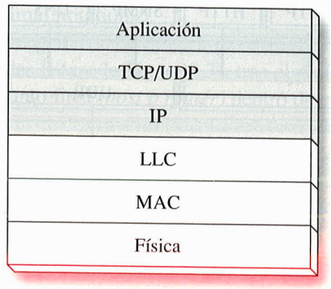


Figura 8.4. TCP/IP sobre una red LAN genérica.

el objetivo de protocolos como ARP y RARP, estudiados más adelante en este mismo capítulo, y del protocolo LLC, descrito en el Apartado 4.6. Aunque no se puede decir que ello implique una cuarta capa en la definición del modelo TCP/IP, sí es importante tener presente la existencia, por necesaria, de esta «interfaz».

El encapsulado realizado en la transmisión real en TCP/IP es el mismo que en cualquier otra red (ver Apartado 1.4 del texto): las diferentes unidades de datos van pasando de capa en capa de forma que la entidad correspondiente en cada una de ellas añade (en el emisor) o quita (en el receptor) la cabecera pertinente (Figura 8.5). No obstante, a diferencia de la rigidez que imponen las siete capas de OSI, en TCP/IP no se exige estrictamente tener que usar las cuatro capas del modelo. Por ejemplo, aunque no muy común, sería posible desarrollar aplicaciones que generen unidades de datos o mensajes para ser encapsulados directamente en IP, sin usar protocolo de transporte.

Como arquitectura que es, además del modelo de referencia, TCP/IP incluye la especificación de uno (o varios) protocolos para cada una de las capas, definiendo lo que se conoce como pila de protocolos TCP/IP (Figura 8.6). Entre los protocolos y servicios asociados más relevantes podemos destacar: IP, correspondiente a la capa de red, TCP y UDP, constitutivos de la capa de transporte, y los correspondientes a las aplicaciones de transferencia de ficheros (protocolo FTP), de correo electrónico (protocolo SMTP), de transferencia de hipertextos (protocolo HTTP) y el servicio de nombres de dominio (protocolo DNS).

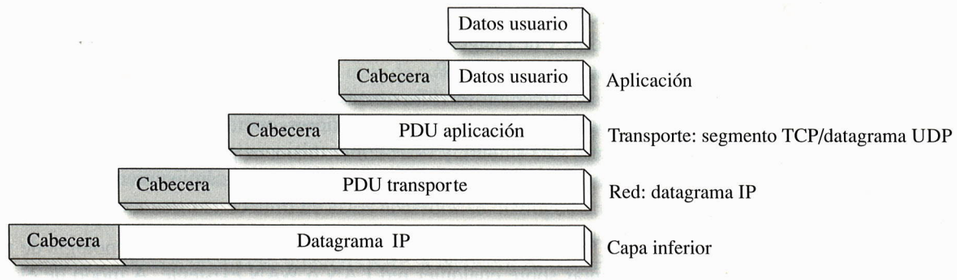


Figura 8.5. Encapsulado TCP/IP.

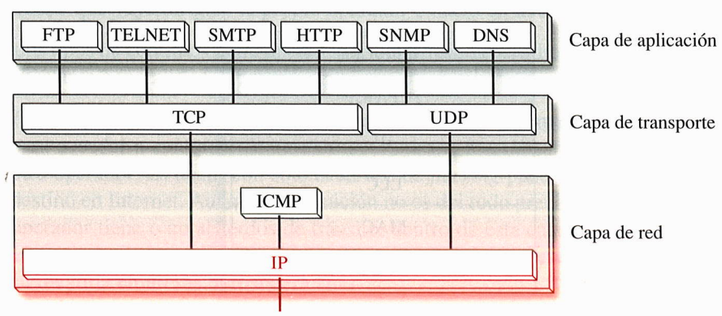


Figura 8.6. Pila de protocolos TCP/IP.

8.4. Direccionamiento Internet

Definimos direccionamiento como la metodología adoptada para identificar entidades en la arquitectura, esto es, entidades que pueden operar en cualquiera de las capas. Por lo general, cada capa adopta un esquema de direccionamiento propio, lo que se traduce en la inclusión de direcciones (origen y destino) en cada una de las cabeceras mostradas en la Figura 8.5.

De esta forma, las entidades o recursos en la capa de aplicación se direccionan mediante los así denominados localizadores universales de recursos (URL, «Universal Resource Locator»). Aunque otros formatos son igualmente posibles (como las direcciones de correo electrónico), típicamente un URL (por ejemplo http://www.ugr.es/index.html) corresponde formalmente a la sintaxis:

`[protocolo]://[dominio]/[directorio]/[recurso]`

En esta nomenclatura, el campo `[protocolo]={http|ftp|telnet|...}` identifica al protocolo necesario para acceder al recurso. Implícitamente, este campo está directamente relacionado con el direccionamiento de la capa de transporte, ya que cada protocolo tiene asociada una entidad de esta capa, la cual se direcciona mediante el número de puerto o sencillamente puerto. Este no es más que un número entero (típicamente de dos bytes) que identifica a la entidad que genera o consume (extremo a extremo) la información. Posteriormente, en el Capítulo 10 se estudiarán los puertos con más detalle.

En el URL también aparece el campo `[dominio]`, también denominado nombre de dominio. Implícitamente, con el dominio se está direccionando a la entidad IP que alberga al recurso en cuestión. El procedimiento para traducir un nombre de dominio a su correspondiente *dirección IP* es responsabilidad de uno de los servicios de la capa de aplicación más relevantes, eficaces y escalables que han sido responsables sin duda de buena parte del éxito de Internet: el servicio o sistema de nombres de dominio (DNS, «Domain Name System»), estudiado en el Capítulo 11.

Resumiendo, en la capa de aplicación se adoptan los URL, en transporte los puertos y en capa de red las direcciones IP. En capas inferiores, estrictamente no pertenecientes a la arquitectura, igualmente habrá un direccionamiento específico y dependiente de la tecnología física subyacente, como por ejemplo los 48 bytes usados para identificar entidades Ethernet en la capa MAC.

En lo que sigue nos centramos en el estudio y caracterización del direccionamiento en la capa IP. Una de las principales características de TCP/IP es su naturaleza universal o global. En este sentido, salvo el direccionamiento privado que será explicado más adelante, una dirección IP es unívoca y reconocida como válida en todo el mundo. En la versión 4 de IP (ver capítulo siguiente) se consideran direcciones IP de longitud 32 bits, las cuales, para hacer más cómodo su uso, se representan mediante cuatro octetos separados por puntos; por ejemplo, 150.214.60.53. Es la conocida como *notación decimal con puntos* («dotted-decimal notation»).

Las direcciones IP (con excepción de las direcciones clase D y E, explicadas más adelante) se dividen en tres partes bien diferenciadas (véase la Figura 8.7); tras el prefijo, una parte contiene el identificador de red y la otra identifica al punto final (*host o router*) dentro de esa red. Es decir, se adopta un direccionamiento relativo y jerarquizado en dos niveles (identificativo de red e identificador de *host*), lo que constituye una de las características propias de IP, y que significará (como más adelante explicaremos) una reducción en las tablas de encaminamiento. Nótese que en este contexto, en general, solo se habla de identificativo de *host* cuando en realidad se trata de una entidad IP genérica (que puede ser un *host* o un *router*).

Figura 8.7. Dirección genérica IPv4.

Dependiendo del prefijo, se definieron cinco clases de direcciones IP (RFC 1166), las cuales (excepto para las clases D y E) se diferencian por el número de bits dedicados para identificar a la red y al *host* (Figura 8.8):

— *Clase A*: 1 bit de prefijo (con valor 0 en este caso), 7 bits para red y 24 para *host*.
— *Clase B*: 2 bits de prefijo (con valores 10), 14 bits para red y 16 para *host*.
— *Clase C*: 3 bits de prefijo (con valores110), 21 bits para red y 8 para *host*.
— *Clase D*: con prefijo 1110, en este tipo de direcciones IP, no relativas ni jerárquicas, se usan 28 bits para especificar una dirección *multicast* correspondiente a un grupo de *hosts*.
— *Clase E*: direcciones que se reservaron para usos futuros y que comienzan con el prefijo 11110.

Según lo anterior, las direcciones de clase A se caracterizan por permitir pocas redes con un gran número de computadores, mientras que las de clase C permiten muchas redes con un número reducido de *hosts*. Más concretamente, los rangos de valores IP para cada una de las cinco clases de direcciones son, en primera instancia, los siguientes:

— *Clase A*: de 0.0.0.0 a 127.255.255.255, lo que significa un total de 128 redes posibles con un máximo de 16.777.216 *hosts* cada una de ellas.
— *Clase B*: de 128.0.0.0 a 191.255.255.255, es decir, 16.384 redes con 65.536 *hosts* cada una.
— *Clase C*: de 192.0.0.0 a 223.255.255.255, lo que permite un total de 2.097.152 redes con 256 *hosts*.
— *Clase D*: de 224.0.0.0 a 239.255.255.255
— *Clase E*: de 240.0.0.0 a 255.255.255.255

Así, por ejemplo, las direcciones utilizadas en la Universidad de Granada, 150.x.x.x, son, según lo anterior, de clase B. La definición de las clases implica por definición un tamaño fijo y predeterminado de las organizaciones a las que se les asignen. Para evitar esta rigidez, posteriormente se definieron las máscaras de redes estudiadas más adelante en el Apartado 8.7.

Respecto del direccionamiento IP hemos de destacar algunas situaciones particulares (ver RFC 1166) o convenciones aceptadas:

— red = 0 significa «esta red». Esta dirección no es válida como dirección IP, utilizándose solo en el proceso de arranque de un *host* o dispositivo.
— red = 0 y *host* = 0 equivale a decir «este *host*». No válida como dirección IP, esta, como la anterior, solo se utiliza en el arranque.

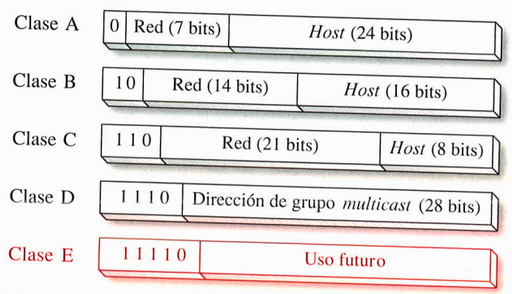
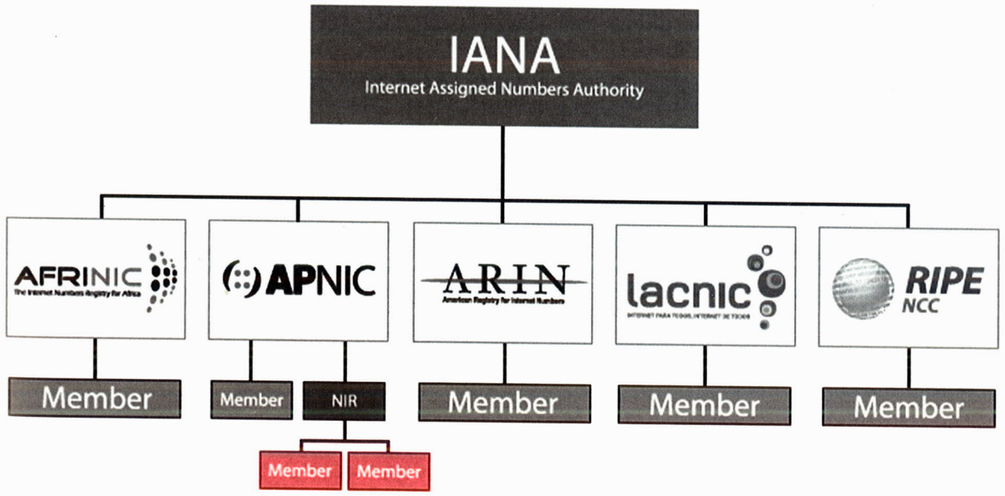


Figura 8.8. Clases de direcciones IPv4.

— *host* = 11...1 significa «difusión para la red indicada». No es válida como dirección IP de origen.
— red = 11...1 y *host* = 11...1 representa «difusión a la red local». Como la anterior, no es una dirección IP de origen válida.
— 127.x.x.x (generalmente 127.0.0.1) son direcciones reservadas denominadas de «autobucle». No deben aparecer nunca asignadas a una red.

Además de las direcciones y reglas anteriores, el IETF especificó un conjunto de direcciones IP denominadas privadas, las cuales son válidas como direcciones de origen y destino en una red corporativa (*intranet*) pero no en Internet (pública) como tal. Las direcciones privadas presentan como ventaja que al tener solo sentido dentro de las *intranets* (su ámbito por definición), el administrador puede usarlas y asignarlas bajo su criterio, sin necesidad de hacer una petición explícita a ningún organismo externo. Al contrario de lo que pasa con las direcciones públicas, las cuales se gestionan y asignan de una forma centralizada (aunque delegada en ocasiones). Con este fin se han reservado los rangos de direcciones privadas clase A de la 10.0.0.0 a la 10.255.255.255 (una subred), clase B de la 172.16.0.0 a la 172.31.255.255 (16 subredes) y por último 256 redes clase C que van desde la 192.168.0.0 a la 192.168.255.255.

Dado el carácter universal de las direcciones IP públicas, su asignación debe estar centralizada, como acabamos de mencionar. De ello se encarga el IANA («Internet Assigned Number Authority», http://www.iana.org), si bien hay que decir que este delega la asignación a su vez en entidades denominadas RIR («Regional Internet Registry»), Figura 8.9. En el Apartado 11.3, correspondiente al servicio DNS, se detallará en mayor profundidad esta cuestión. El RIR europeo es el RIPE NCC (http://www.ripe.net/), el cual también delega la asignación de las direcciones IP a entidades de ámbito nacional o LIR («Local Internet Registry»), listadas en https://www.ripe.net/membership/indices/ES.html para el caso de España.



Fuente: RIPE NCC.

Figura 8.9. Delegación de IANA en varios RIR.

Una última consideración importante acerca de las direcciones IP es que estas implican, para las clases A, B y C, un direccionamiento relativo; es decir, identifican un punto final en una red dada. Esto significa que si un *host* con dirección IP dada cambia su localización a otra red, deberemos asignarle una dirección IP distinta de la original. En definitiva, una dirección IP no está asociada a la entidad IP (*host* o *router*) sino más bien al punto de conexión en la red identificada. Por tanto, una entidad IP (*host*, *router*, etc.) debe tener asignadas tantas direcciones IP como conexiones o interfaces tenga, cada una con el identificativo que corresponda a la red con la que conecta a través de cada una de sus interfaces.

En la Figura 8.10 se muestra un ejemplo de asignación de direcciones IP a interfaces en una intranet con direccionamiento privado. Compuesta de tres redes LAN, a cada una de ellas se les ha asignado una dirección privada clase C del tipo 192.168.[1|2|3].x. A los *hosts* se les ha asociado una única dirección IP, mientras que a los dispositivos de encaminamiento R1 y R2, dado que tienen, respectivamente, 3 y 2 interfaces, se les han asignado otras tantas direcciones IP; una por cada red a la que se conectan. Por último, hemos de destacar el hecho de que una de las interfaces de R2 tiene una dirección clase B pública (150.214.60.100), a través de la cual se cursará tráfico desde y hacia Internet. En este sentido, R2 deberá implementar algún esquema de traducción de direcciones IP si deseamos que los distintos *hosts* de la intranet accedan a Internet haciendo uso de direcciones IP válidas (ver Apartado 8.8.).

8.5. Protocolos de resolución de direcciones

Como se ha mostrado en la Figura 8.5, los paquetes IP se deben encapsular en las PDU de la capa inferior. En el caso, por ejemplo, de una red local de tipo Ethernet el encapsulado se realizará sobre la trama LLC, que, a su vez, se encapsulará en la trama MAC correspondiente. Llegados a este punto, hemos de señalar que la transmisión sobre la red Ethernet precisa la especificación de las direcciones hardware de las estaciones origen y destino (ver Apartado 5.2.2), no la de sus direcciones IP. Será necesario, por tanto, arbitrar algún método para traducir las direcciones IP a direcciones físicas, y viceversa.

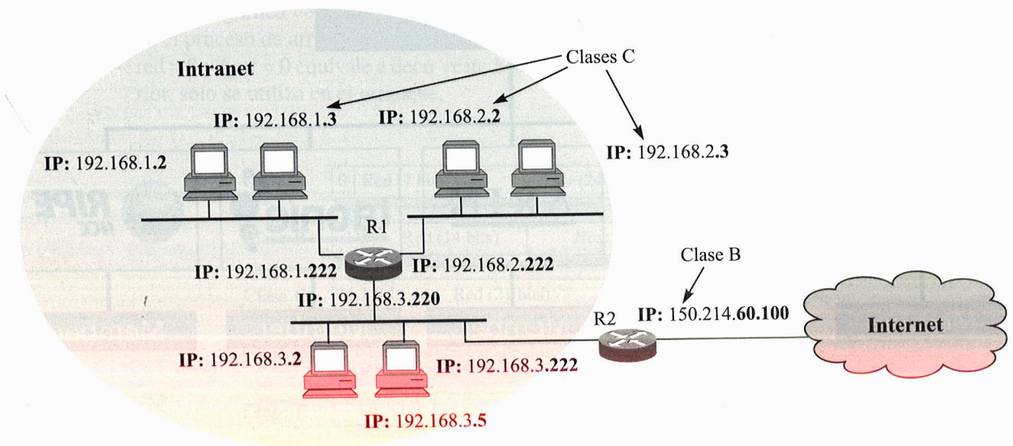


Figura 8.10. Ejemplo de asignación de direcciones IP.

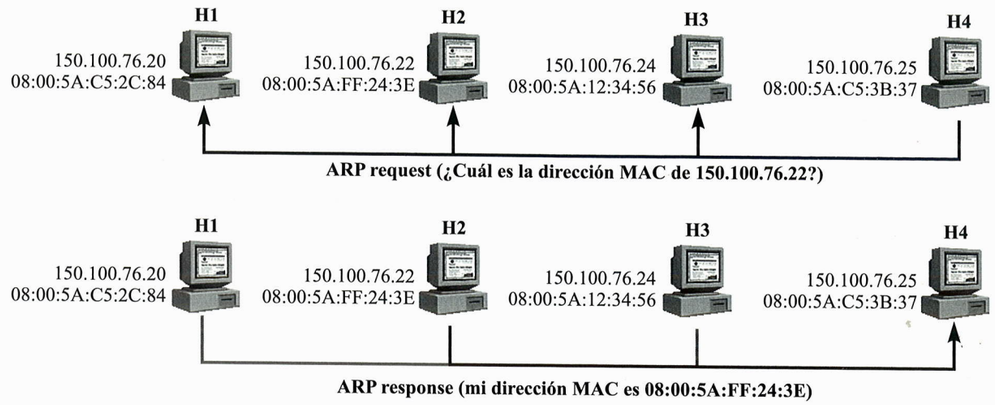


Figura 8.11. Solicitud y respuesta ARP.

El protocolo de resolución de direcciones ARP («Address Resolution Protocol», RFC 826) permite obtener la dirección física (o hardware) de un *host* a partir de su dirección IP. Pensemos en la configuración de red dada en la Figura 8.11. Si H4 desea comunicar con H1, pero no conoce su dirección Ethernet, sino solo la IP, procederá como sigue:

a) H4 difunde («broadcast») una consulta ARP a todos los *hosts* (dirección destino de trama MAC FF:FF:FF:FF:FF:FF —ver Apartado 5.2.2—) preguntando por la dirección IP 150.100.76.22 especificada en la solicitud.

b) El *host* poseedor de dicha dirección, H1 en nuestro caso, emitirá una respuesta ARP hacia el *host* origen, H4, indicando su dirección hardware.

Para mejorar las prestaciones del esquema ARP se puede hacer uso de una memoria *cache*. En la misma se almacenan resoluciones anteriores, tal que su consulta previa trata de evitar resoluciones correspondientes a parejas de dirección física-dirección IP ya conocidas.

Hay situaciones en las que es necesario el proceso contrario al anterior; es decir, obtener la dirección IP de un *host* a partir de su dirección hardware. Para ello se utiliza el *protocolo de resolución de direcciones contrario* (RARP, «Reverse Address Resolution Protocol» —RFC 903). Esta conversión se realiza, por ejemplo, por parte de *hosts* sin disco que arrancan remotamente y que, por tanto, no tienen dirección IP asignada estáticamente. Pensemos que H4 en la Figura 8.12 arranca de forma remota y precisa conocer su propia dirección IP. Los pasos seguidos en el proceso serían:

a) H4 difunde una consulta RARP a todos los *hosts* preguntando por la dirección IP del *host* cuya dirección hardware es la especificada en la consulta, la suya (Figura 8.12).

b) El *host* que conozca dicha información emitirá una respuesta RARP indicando la dirección IP solicitada. La respuesta puede ser múltiple (Figura 8.12), por lo que una posible solución para evitar una avalancha de envíos por parte de las estaciones que conozcan dicha información consistiría en planificar las respuestas aleatoriamente en el tiempo, de modo que una estación dada no responderá si detecta que otra lo ha hecho con anterioridad.

El formato de los paquetes ARP y RARP es el mostrado en la Figura 8.13. Los campos involucrados son los siguientes:

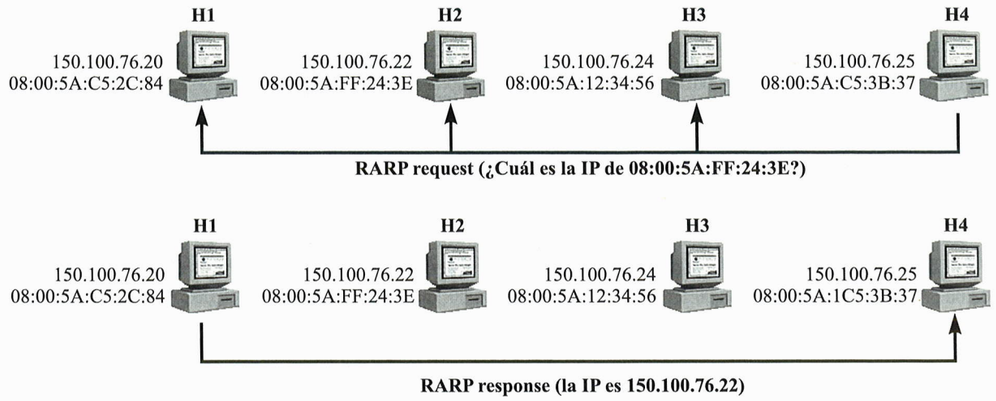


Figura 8.12. Solicitud y respuesta RARP.

— *Htipo:* Indica el tipo de direcciones hardware utilizadas. El valor de este campo es 1 en el caso de redes Ethernet[1].
— *Stipo:* Indica el tipo de direcciones lógicas, software, es decir del nivel superior utilizadas. En el caso de direcciones IP el valor de este campo es 0800 en hexadecimal.
— *Hlen:* Campo donde se indica el número de octetos de que constan las direcciones hardware; seis en el caso de direcciones Ethernet.
— *Slen:* Campo donde se indica el número de octetos de que constan las direcciones software; cuatro en el caso de tratarse de direcciones IP.
— *Operación:* Campo a través del que se indica el tipo de mensaje:

1 → Consulta ARP.
2 → Respuesta ARP.
3 → Consulta RARP.
4 → Respuesta RARP.

— *Hemisor:* Dirección hardware de la estación emisora del paquete. En la Figura 8.13 se ha supuesto que se trata de una dirección Ethernet de 6 octetos.
— *Semisor:* Dirección software de la estación emisora del paquete. En la Figura 8.13 se ha supuesto que se trata de una dirección IP de 4 octetos.
— *Hsol:* Dirección hardware de la estación por la que se pregunta. Este campo estará vacío en el caso de una consulta ARP, rellenándose por el receptor en la respuesta correspondiente. En la Figura 8.13 se ha supuesto que se trata de una dirección Ethernet de 6 octetos.
— *Ssol:* Dirección software de la estación por la que se pregunta. Este campo estará vacío en el caso de una consulta RARP, rellenándose por el receptor en la respuesta correspondiente. En la Figura 8.13 se ha supuesto que se trata de una dirección IP de 4 octetos.

[1] Los paquetes ARP y RARP intercambiados en un entorno Ethernet se identifican, respectivamente, mediante los valores hexadecimales 0806 y 8035 del campo *tipo* de las tramas MAC (sustitutivo del campo *longitud* en las tramas IEEE 802.3 —Figura 5.4—).

0	8	16 … 31
Htipo		Stipo
Hlen	Slen	Operación
Hemisor (bytes 0-3)		
Hemisor (bytes 4-5)		Semisor (bytes 0-1)
Semisor (bytes 2-3)		Hsol (bytes 0-1)
Hsol (bytes 2-5)		
Ssol (bytes 0-3)		

Figura 8.13. Formato de los paquetes ARP y RARP para la conversión de direcciones IP a direcciones Ethernet, y viceversa.

Antes de finalizar este apartado, comentar que los diferentes sistemas operativos (por ejemplo, Microsoft Windows y las diversas variantes Linux) ofrecen el comando `arp` para interaccionar con la *cache* de ARP/RARP. Para más detalles sintácticos y de funcionalidad consultar las correspondientes páginas de manual o ayuda.

8.6. Debilidades del direccionamiento IP

El esquema de direccionamiento IP establece una relación unívoca entre una red física y el identificativo de red IP asociado, reservando el resto de los bits de la dirección IP para indicar un *host* dentro de la red. Si bien la principal ventaja del carácter jerárquico de dicho esquema reside en el menor tamaño de las tablas de encaminamiento requeridas en los nodos intermedios, (consistentes en una entrada por cada red de destino en lugar de por cada *host*), también presenta un importante inconveniente motivado por el vertiginoso crecimiento de Internet en los últimos años: la continua aparición de nuevas redes de pequeño tamaño, lo cual está provocando que comience a quedar exhausto el espacio IP (en su versión 4; ver capítulo siguiente), en especial por lo que respecta a los identificativos de red disponibles. ¿Cómo reducir el número de direcciones de red asignadas sin afectar al esquema de direccionamiento original? Algunas soluciones han sido propuestas al respecto.

La solución más inmediata a este problema pasa por ampliar el número de bits utilizado en las direcciones IP. Esto es lo que hace la versión 6 de IP (ver Apartado 9.1.2), en la que se consideran 128 bits en lugar de los 32 hasta ahora comentados. No obstante, hay que decir que, el despliegue de IPv6 está siendo mucho más lento de lo que inicialmente se podía prever, por lo que se han propuesto otras soluciones alternativas y transitorias, en ocasiones complementarias entre sí. Las dos más utilizadas, son las siguientes:

1. Compartir un mismo prefijo de red IP por parte de varias redes físicas diferentes, rompiendo con la correspondencia unívoca red física-identificativo de red.
2. Mejor aprovechamiento del espacio de direcciones IP mediante técnicas que eviten la rigidez impuesta por las diferentes clases de direcciones IP disjuntas.

Dentro de la primera de las soluciones planteadas se encuentra el procedimiento conocido como *ARP promiscuo* o *sustituto* («proxy» en inglés). En la Figura 8.14 se ilustra la situación mediante un ejemplo. El puente R, que implementa el esquema ARP sustituto posibilita que todos los *hosts* de la red LAN2 compartan el mismo prefijo o identificativo de red IP asociado a la red LAN1, IPN_1, y, por

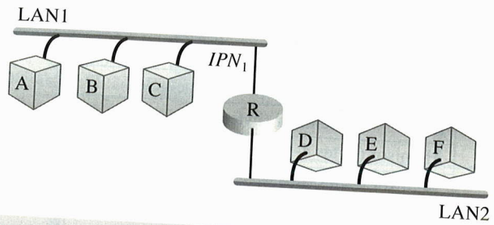


Figura 8.14. Esquema ARP promiscuo, implementado en R, gracias al cual las estaciones de LAN2, D, E y F, comparten el identificativo de red de LAN1, IPN1.

tanto, compartido con los *hosts* A, B y C, mediante un simple esquema de multiplexación en el que, por supuesto, R debe llevar a cabo un control exhaustivo de las transmisiones efectuadas desde y hacia D, E y F. En resumen, R miente sobre las asociaciones dirección física-dirección de red IP de dichos *hosts*.

La ruptura de la correspondencia uno a uno entre red física-red IP se puede realizar también con *dispositivos de encaminamiento transparentes*. Su adopción en un entorno como el mostrado en la Figura 8.15 posibilitaría la conexión de los *hosts* de la red LAN a la red WAN, de forma que estos pasarían a compartir el mismo esquema de direccionamiento que el utilizado en esta última red. Así, para el resto de dispositivos en la red WAN no resultaría visible ni el dispositivo transparente ni la LAN como tal, siendo los *hosts* A, B y C unas estaciones más de la red de área amplia. Por tanto, si esta utilizase, por ejemplo, direcciones IP de clase A, los *hosts* A, B y C en LAN también podrán utilizar dicha clase de direcciones. Esta aproximación tiene como desventaja que al compartir el mismo prefijo de red, el dispositivo de interconexión no aísla tráficos entre las dos o más subredes interconectadas.

8.7. Máscaras de red

Para paliar las dificultades apuntadas que presenta el direccionamiento IP, además del ARP promiscuo y del uso de los dispositivos de encaminamiento transparentes, se han propuesto otras aproximaciones. El objetivo es evitar la rigidez que imponen los tamaños fijos y preestablecidos de las tres clases A, B y C, ya que no todas las instituciones (y en definitiva sus redes) se adecuan a uno de los tres tamaños preestablecidos para cada una de las clases, lo que significa que en ciertos casos se desaprovecha el espacio de direcciones. Por ejemplo, si a una red con 12.000 direcciones IP le asignáramos una clase B, se estarían desaprovechando más de 50.000 direcciones. La alternativa sería asignar a la

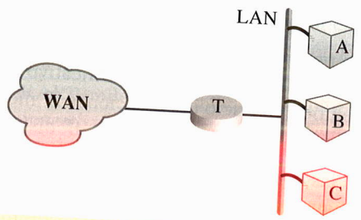


Figura 8.15. Dispositivo de encaminamiento transparente y extensión de cobertura de una red WAN.

red del ejemplo anterior un conjunto de redes clase C, pero esto implicaría aumentar la complejidad de las tablas de enrutamiento.

En definitiva, se necesita un mejor y más flexible aprovechamiento del espacio de direcciones. Para ello, además de la posibilidad de elegir direcciones IP privadas, ya explicada con anterioridad, se definen las máscaras de red. Una máscara de red no es más que un patrón de 32 bits en el que valdrán 1 los bits cuyas posiciones coincidan con posiciones pertenecientes al identificativo de red, siendo el resto 0. De esta forma, una máscara flexibiliza la definición de qué bits pertenecen al identificativo de red y cuáles corresponden al identificativo de *host* para una dirección IP dada (al margen de la clase específica de esta), sin más que hacer una operación lógica AND entre esta dirección IP y su máscara.

Las máscaras se representan con la misma la notación decimal con puntos que las direcciones IP. Por ejemplo 255.255.255.0 significa que los tres primeros octetos de la dirección IP son de red, mientras que solo el último byte corresponde al identificativo de host; es decir, la dirección IP efectiva considerada es de clase C, independientemente de la clase de dirección IP original. Por ejemplo, en la Universidad de Granada se consideran direcciones IP del tipo 150.214.x.x, es decir, clase B, pero, en cambio, las máscaras generalmente utilizadas son 255.255.255.0, o sea, las direcciones IP efectivas son de clase C. Esto permite, como hemos dicho antes, una mejor estructuración/organización de los *hosts* en subredes y un mejor aprovechamiento del espacio de direcciones global.

Otra notación habitual para las máscaras consiste en representarlas como */N*, dónde N es el número de bits a valor 1 en la máscara. Por ejemplo, la máscara 255.255.255.0 se nota igualmente como /24. Volviendo al ejemplo anterior, la notación 150.124.x.x/24 significa que los 3 primeros octetos (24 bits) de la dirección IP considerada (clase B) son de red, mientras que solo el cuarto octeto (8 bits) identifica al *host*. En este caso, está implícito que todos los bits 1 de la máscara son consecutivos y siempre en las posiciones más significativas, lo cual es lo recomendado (aunque no obligatorio).

Las 3 clases A, B, C, definen implícitamente y de forma estática qué posiciones corresponden a los identificativos de red y *host*. Con las máscaras podemos flexibilizar esta asignación; así dada una IP perteneciente a una clase en particular, nos encontramos con dos posibilidades (Figura 8.16):

1. que la máscara «robe» bits del identificativo de host, desplazando la separación hacia la derecha, creando sub-redes o
2. que la máscara ceda bits al identificativo de host, desplazando la separación hacia la izquierda, creando una súper-red.

Esta técnica de creación de súper-redes y sub-redes se denomina CIDR («Classless InterDomain Routing»), la cual está especificada en el RFC 4632. Además de un mejor aprovechamiento del espacio de direcciones IP, CIDR permite simplificar el tamaño de las tablas de encaminamiento (explicadas en el Capítulo 9).

8.7.1. Asignación de sub-redes

La creación de sub-redes permite simplificar las tablas de encaminamiento, ya que si asignamos adecuadamente varias sub-redes a partir de una dirección IP dada, todas ellas podrán ser identificadas como una única entrada en la tabla de los *router* externos (como por ejemplo desde los *routers* en

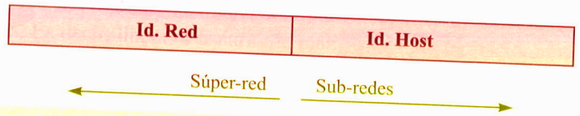


Figura 8.16. Máscaras para la creación de súper-red o sub-redes.

Internet para el escenario mostrado en la Figura 8.17). En este caso, se ha optado por dividir la dirección clase B (140.16.0.0) en cuatro sub-redes (Figura 8.18), usando la máscara 255.255.192.0, o lo que es lo mismo, /18.

Se asignan tres de las subredes (dejando la cuarta para el posible despliegue de una sub-red futura) tal y como se muestra en la Figura 8.17. En este caso, las tres subredes de la intranet podrán ser identificadas de una forma compacta y con una única entrada, desde los *routers* externos a la intranet, con la dirección 140.16.0.0/16. Obsérvese que en este caso, dada la máscara /18, cada una de las 4 sub-redes podrá albergar hasta 2^{14} direcciones IP, con los rangos mostrados en la siguiente tabla:

Bits de la subred	Subred	Máscara	Rango de direcciones IP (214)
00	140.16.0.0	255.255.192.0 o /18	140.16.0.0-140.16.63.255
01	140.16.64.0	255.255.192.0 o /18	140.16.64.0-140.16.127.255
10	140.16.128.0	255.255.192.0 o /18	140.16.128.0-140.16.191.255

8.7.2. Asignación de súper-redes: CIDR

Alternativamente, como se ha dicho, si desplazamos la máscara hacia la izquierda (Figura 8.16) podemos agrupar varias redes de una clase dada en una súper-red. Esto ayuda definitivamente a paliar el desaprovechamiento de direcciones. Así, si tuviéramos una red con necesidad de 2.000 direcciones IP, asignarle una clase B implicaría desaprovechar más de 60.000 direcciones. Por el contrario, para hacer un mejor aprovechamiento de direcciones, podríamos agrupar 8 redes clase C, convenientemente elegidas y asignarlas a esa red. Concretamente, usando una máscara /21 (lo que equivale a 255.255.248.0) sobre direcciones clase C, se definiría por ejemplo la súper-red 200.100.16.0/21, lo que correspondería a agrupar las 8 redes clase C que van desde la 200.100.16.0/24 a la 200.100.23.0/24. De esta manera, la asignación de la súper-red 200.100.16.0/21 serviría para cubrir las 2.000 direcciones necesitadas, pero desperdiciaría muchas menos en comparación con asignar una clase B a esta red.

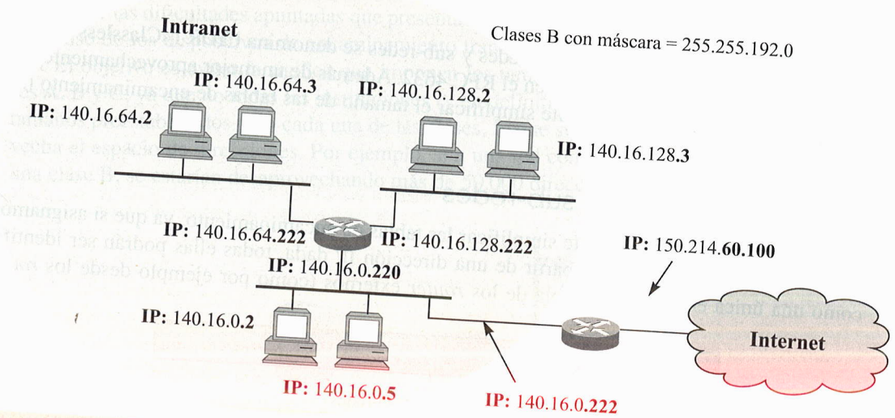


Figura 8.17. Escenario para la asignación de sub-redes.

255	-	255	192		-	0
11111111	-	11111111	11	000000	-	00000000
140	-	16	→	Id. de host		

Figura 8.18. Ejemplo de 4 sub-redes para una dirección clase B.

En relación a la capacidad de CIDR para simplificar el tamaño de las tablas de encaminamiento, nótese que en el ejemplo de asignación anterior las 8 redes clase C, es decir la súper-red 200.100.16.0/21, se podrían agrupar necesitando solo una entrada o fila en las tablas de encaminamiento.

8.8. Traducción de direcciones de red

Además de las máscaras de red, un mecanismo ampliamente utilizado para mejorar el aprovechamiento del espacio de direcciones IP es el conocido como *traducción de dirección de red* o, simplemente, NAT («Network Address Translation»). Especificado originalmente en el RFC 1631 y actualizado a través del RFC 3022, NAT permite, en su forma tradicional, la traducción o conversión de un conjunto de *m* direcciones IP (normalmente privadas) a uno de *n* direcciones IP (normalmente públicas). ¿En qué contexto tiene sentido un proceso de este tipo? Típicamente en las siguientes situaciones:

— Cuando se dispone de un número de direcciones IP públicas inferior al número de *hosts* existente. Este caso corresponde, por ejemplo, a la conexión a Internet de una red privada del tipo de la mostrada en la Figura 8.10. En ella, será responsabilidad del *router* R2 la asignación de direcciones IP válidas para posibilitar el acceso de los *hosts*, con direcciones privadas del tipo 192.18.[1|2|3].x, a Internet.

— Cuando se quiere mejorar la seguridad en una red, de forma que los *hosts* del exterior no tengan acceso directo a las direcciones IP internas.

Un esquema NAT puede ser estático o dinámico. En el primer caso sucede que $m,n \geqslant 1$ y $m = n$; es decir, los dos conjuntos de direcciones, privadas y públicas, disponen del mismo número de direcciones IP, llevándose a cabo una conversión fija entre ambos espacios. Por su parte, en un esquema NAT dinámico, $m \geqslant 1$ y $m \geqslant n$, o lo que es lo mismo, el conjunto de direcciones públicas de que se dispone suele ser inferior al de las privadas. Un caso particular relevante de este último esquema es aquel en el que $m \geqslant 1$ y $n = 1$, situación que se conoce con el nombre de *enmascaramiento* («masquerading» en inglés) y que correspondería, por ejemplo, al hecho de que R2 en la Figura 8.10 utilizase como espacio IP de origen el de las direcciones intranet y como conjunto de direcciones IP final una única, la de valor 150.214.60.100. El esquema de enmascaramiento recibe también el nombre de NAPT («Network Address Port Traslation»), debido al hecho de que un dispositivo de encaminamiento NAT permite varias conexiones mediante un proceso de multiplexación sobre puertos disponibles (ver Apartados 10.2 y 10.3).

Un esquema utilizado también en el mismo contexto que NAT es el de asignación dinámica de direcciones IP a través del protocolo DHCP («Dynamic Host Configuration Protocol», RFC 2131). Como su nombre indica, este protocolo facilita la configuración automática de direcciones IP y otras cuestiones relacionadas. Es decir, libera al usuario de realizar una configuración manual de los equipos finales. DHCP es una aplicación cliente-servidor que consta de dos componentes: un protocolo para el envío de parámetros de configuración específicos del *host* y un mecanismo para la reserva de direcciones de red para *hosts*. Por lo que respecta a la segunda cuestión, DHCP soporta tres mecanismos distintos de reserva de direcciones IP: (a) automático, donde se asigna una dirección permanente a un cliente que lo

solicita; (b) dinámico, donde la asignación realizada es temporal por un tiempo limitado; y (c) manual, en el que la asignación es realizada por el administrador, limitándose DHCP a comunicarla al cliente. Una red dada usará uno o más de estos mecanismos dependiendo de las políticas fijadas por el administrador. En todo caso, es el esquema de reserva dinámica el que resulta adecuado para: (1) llevar a cabo la asignación de una dirección IP a un cliente que se conecta temporalmente a la red, o (2) compartir un conjunto de direcciones IP entre una serie de clientes que no precisan el empleo de direcciones permanentes.

RESUMEN

En este primer tema de la segunda parte del texto se ha introducido Internet a partir del modelo TCP/IP. Presentadas someramente su génesis y evolución, seguidamente se ha comentado su estructura, su arquitectura y algunos de los protocolos que la forman.

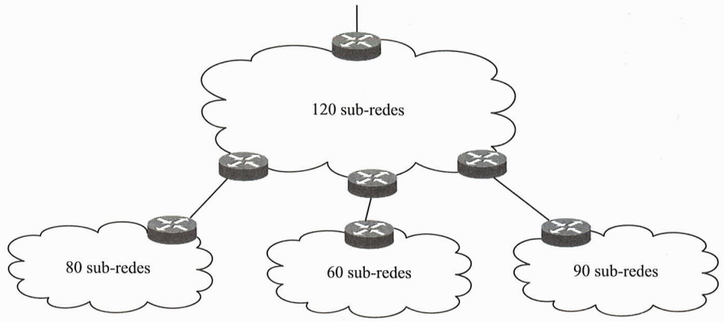
Una cuestión básica en el estudio de Internet es la relativa a las direcciones IP. Respecto de ellas, se han presentado las distintas clases existentes, los algoritmos de resolución ARP y RARP, así como distintas técnicas que permiten mejorar el uso del espacio de direcciones, en la actualidad prácticamente exhausto para la versión 4 de IP. A este último respecto hemos de destacar el empleo de CIDR y las máscaras de red para la creación de sub-redes y súper-redes, así como la implementación de esquemas de traducción de direcciones de red.

En los temas que siguen se lleva a cabo el estudio de las distintas capas y protocolos Internet (o TCP/IP).

EJERCICIOS

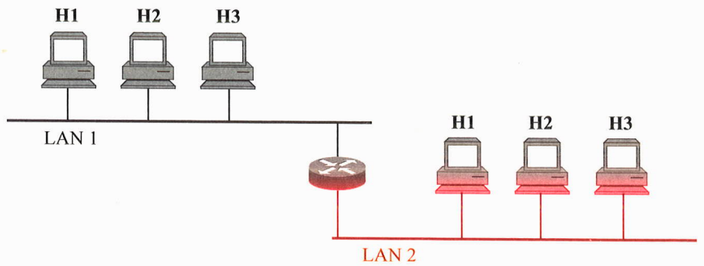
1. Identifique algunos servicios de la capa de aplicación en Internet que sean escalables. Justifique su respuesta.
2. Según el principio de modularidad o acoplamiento débil: funciones distintas deben estar en capas distintas. Adoptar esta aproximación, ¿impide tener una visión de conjunto en Internet que proporcione soluciones más eficaces?
3. Hay protocolos de encaminamiento que se ejecutan en los *routers* usando los servicios de transporte TCP o UDP. ¿Vulnera este hecho el principio de diseño de Internet según el cual la complejidad se debe situar en los extremos? Justifique la respuesta. Ponga ejemplos, si los hubiere, de otros protocolos que vulneren este principio.
4. Dibuje gráficamente cómo sería una posible topología que conectara dos redes de usuario (LAN) que acceden a Internet a través de dos operadores distintos *tier-2* que no tienen un punto neutro en común. Identifique el tipo de acuerdos que deben tener los operadores entre sí, o con un tercero. ¿Y si fueran operadores tipo *tier-1*?
5. Discuta las ventajas e inconvenientes que tienen los URL y las direcciones IP para facilitar la movilidad de recursos y de entidades de red.
6. Identifique la clase de dirección de las direcciones IP siguientes: 201.158.20.165, 129.176.32.24, 14.169.128.50, 150.214.35.1, 250.9.96.24.
7. Una universidad tiene 150 LAN con 100 computadoras cada una. Supuesto que se dispone de una dirección de clase B:
   a) Diseñe un esquema de direccionamiento en subred apropiado.
   b) Diseñe un esquema de direccionamiento CIDR apropiado.

8. Una organización pequeña tiene asignada una dirección de clase C para siete redes con 24 computadoras cada una. ¿Cuál es la máscara de subred apropiada?
9. Una red tiene una máscara de subred igual a 255.255.255.240.0. ¿Cuál es el número máximo de *hosts* de dicha subred?
10. Una organización obtiene una dirección 193.1.1.0/24. Si se necesitan 6 sub-redes con 25 *hosts* cada una, identifique la lista de todas las posibles sub-redes.
11. Para una dirección IP 172.16.10.40 y máscara asociada 255.255.255.240, conteste las siguientes cuestiones:
    a) ¿Cual es el identificativo de la sub-red?
    b) ¿Cuál es la dirección de *broadcast*?
    c) ¿Qué rango de direcciones IP se dispone para asignar a *hosts*?
12. Identifique las direcciones IP y sub-redes que hay en la dirección CIDR 198.31.168.0/21.
13. En el escenario de la figura inferior, diseñe una asignación de direcciones IP si dispone del rango150.55.0.0/16. ¿Cuántos *hosts* se pueden asignar en cada una de las sub-redes?

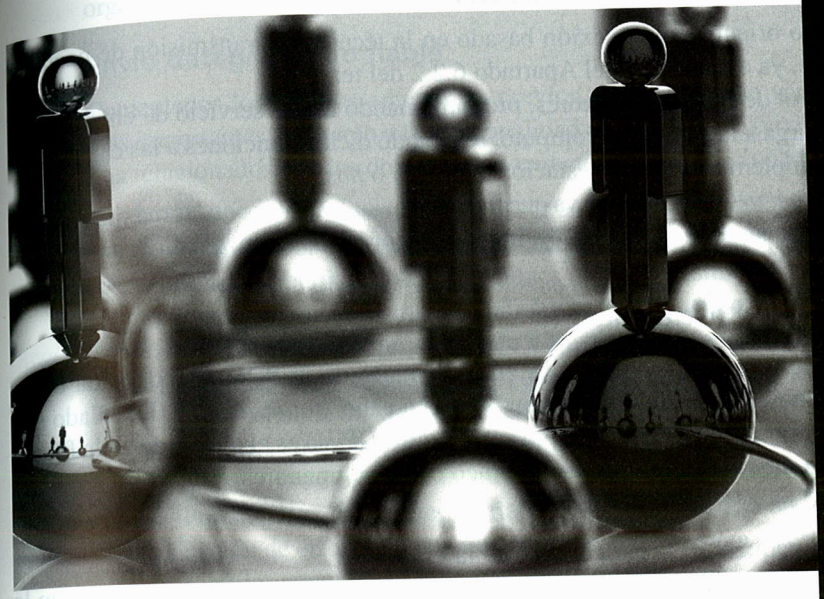


14. En el escenario de la figura inferior, suponga que H1 usa el protocolo ARP para obtener la dirección IP del *host* H5. Suponiendo que todos los dispositivos se acaban de iniciar, muestre los mensajes intercambiados y explique qué ocurrirá.

    Suponga ahora que las LAN 1 y 2 comparten el mismo prefijo de red y con la misma máscara. ¿Qué mensajes aparecerían en estas circunstancias?



15. Se desea desplegar una red de comunicaciones IP con acceso Internet, con las siguientes especificaciones básicas:



CAPÍTULO 9

PROTOCOLOS PARA LA INTERCONEXIÓN DE REDES

9.1. Protocolo Internet: IP
9.2. Mensajes de control de Internet: protocolo ICMP
9.3. Encaminamiento dinámico en Internet
9.4. Encaminamiento multidestino en Internet

Tras la introducción a Internet realizada en el capítulo anterior, en este se da comienzo al estudio detallado de la arquitectura de red en que se basa aquella: TCP/IP. Siguiendo la metodología de la primera parte del texto, el presente capítulo se centra en la descripción de los servicios implementados en la más baja de las capas de TCP/IP, la de red, a través del estudio de los protocolos desarrollados y adoptados al efecto.

Comenzando por el más importante de ellos, y que constituye el núcleo de esta arquitectura, IP, tras él se presentarán otros protocolos de gran transcendencia como ICMP, orientado al control de ciertas eventualidades y situaciones en la subred, y RIP, OSPF y BGP, cuyo fin es la actualización dinámica de las tablas de encaminamiento de los *routers*.

Asimismo, se estudiarán las transmisiones *multicast* en Internet desde tres perspectivas: direccionamiento, gestión de grupos y encaminamiento. En relación a cada una de ellas se discutirán, respectivamente, la arquitectura MALLOC, el protocolo IGMP y el protocolo PIM.

9.1. Protocolo Internet: IP

Como se comentó a partir de la Figura 8.5, la PDU de la capa de red se encapsula en el campo de datos de la PDU de la capa inferior (típicamente una trama de enlace) sobre la que se implementa la arquitectura TCP/IP. El protocolo de la capa red en TCP/IP es el conocido como protocolo Internet o IP

— Zona de servidores públicos, con 1 servidor Web y 1 servidor FTP.
— Zona departamental pública, con 3 puestos de trabajo con acceso externo sin restricciones y servicio de impresión interno.
— Dos zonas departamentales privadas, con acceso externo limitado al servicio HTTP y servidores de ficheros de acceso exclusivo interno. Además, cada departamento contará con 8 puestos de trabajo.

En esta situación, responda a las siguientes cuestiones:

a) Proponga una topología de red mixta cableada-inalámbrica, en la que los departamentos privados consiguen acceso externo mediante tecnología WiFi.
b) Especifique en la propia topología un direccionamiento de red público-privado mínimo para identificar adecuadamente todas las sub-redes de la configuración propuesta.

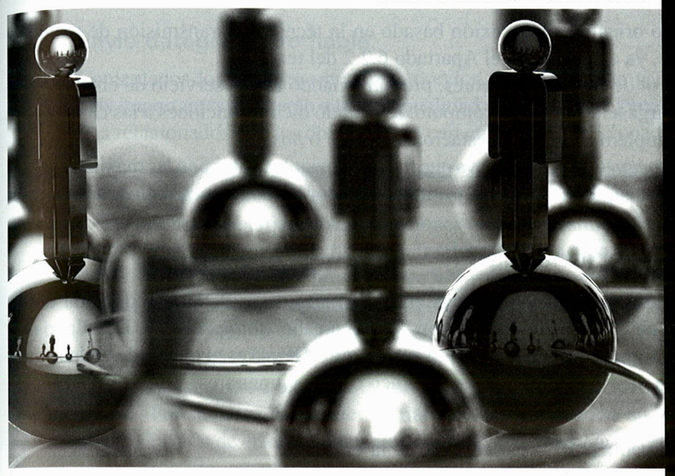
16. Dado una aplicación situada en una entidad IP dentro de una intranet privada que está conectada a Internet través de un *router* de acceso con enmascaramiento, desarrolle y explique un procedimiento para que cualquier otra aplicación desde Internet pueda contactar con la aplicación de la intranet (desde fuera a dentro). *Pista: utilice un servidor externo.*

BIBLIOGRAFÍA Y SITIOS WEB

Bradley, T.; Brown, C.; Malis, A.: *Inverse Address Resolution Protocol*. RFC 2390. Septiembre, 1998.
Comer, D. E.: *Internetworking with TCP/IP. Volume I: Principles, Protocols and Architecture*. 3ª edición. Prentice Hall, 1995.
Droms, R.: *Dynamic Host Configuration Protocol*. RFC 2131. Marzo, 1997.
Finlayson, R.; Mann, T.; Mogul, J.C.; Theimer, M.: *Reverse Address Resolution Protocol*. RFC 903. Junio, 1984.
V. Fuller, T. Li: «*Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*». RFC 4632, Agosto 2006.
Kirkpatrick. S.; Stahl, M.K.; Recker, M.: *Internet Numbers*. RFC 1166. Julio, 1990.
Kurose, J. F.; Ross, K.W.: *Computer Networking. A Top-Down Approach Featuring the Internet*. Addison Wesley, 6a. edición, 2012.
Plummer, D. C.: *Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware*. RFC 826. Noviembre, 1982.
Srisuresh, P; Egevang, K.: *Traditional IP Network Address Translator (Traditional NAT)*. RFC 3022. Enero, 2001.
Stevens, W. R.: *TCP/IP Illustrated, Vol. 1. The Protocols*. Ed. Addison Wesley, 2000.

Adicionalmente a los textos citados, existen diversos sitios web que resultan básicos en la búsqueda de información relacionada con Internet. Algunos de los más importantes, mencionados a lo largo de este tema, son los siguientes:

http://www.iab.org
http://www.iana.net
http://www.ietf.org
http://www.internic.org
http://www.irtf.org
http://www.isoc.org
http://www.rfc-editor.org



CAPÍTULO 9

PROTOCOLOS PARA LA INTERCONEXIÓN DE REDES

9.1. Protocolo Internet: IP
9.2. Mensajes de control de Internet: protocolo ICMP
9.3. Encaminamiento dinámico en Internet
9.4. Encaminamiento multidestino en Internet

Tras la introducción a Internet realizada en el capítulo anterior, en este se da comienzo al estudio detallado de la arquitectura de red en que se basa aquella: TCP/IP. Siguiendo la metodología de la primera parte del texto, el presente capítulo se centra en la descripción de los servicios implementados en la más baja de las capas de TCP/IP, la de red, a través del estudio de los protocolos desarrollados y adoptados al efecto.

Comenzando por el más importante de ellos, y que constituye el núcleo de esta arquitectura, IP, tras él se presentarán otros protocolos de gran transcendencia como ICMP, orientado al control de ciertas eventualidades y situaciones en la subred, y RIP, OSPF y BGP, cuyo fin es la actualización dinámica de las tablas de encaminamiento de los *routers*.

Asimismo, se estudiarán las transmisiones *multicast* en Internet desde tres perspectivas: direccionamiento, gestión de grupos y encaminamiento. En relación a cada una de ellas se discutirán, respectivamente, la arquitectura MALLOC, el protocolo IGMP y el protocolo PIM.

9.1. Protocolo Internet: IP

Como se comentó a partir de la Figura 8.5, la PDU de la capa de red se encapsula en el campo de datos de la PDU de la capa inferior (típicamente una trama de enlace) sobre la que se implementa la arquitectura TCP/IP. El protocolo de la capa red en TCP/IP es el conocido como protocolo Internet o IP