

- 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:

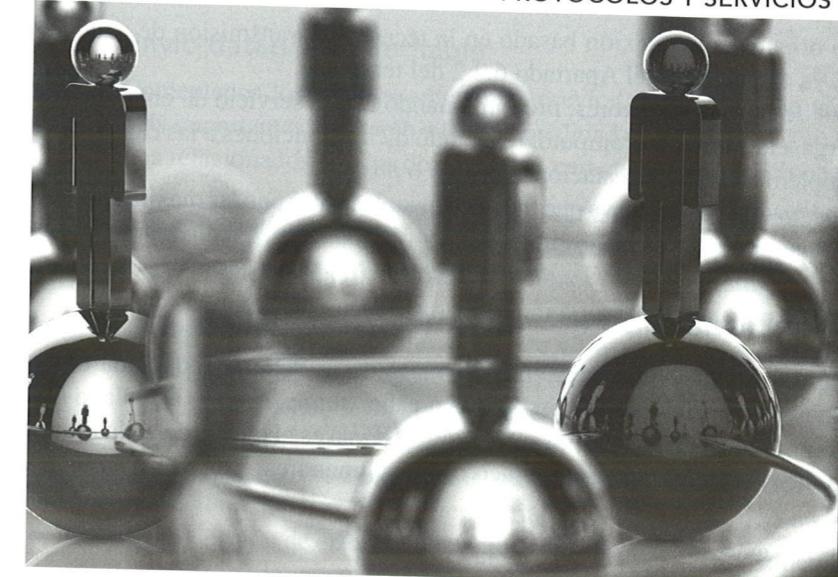
- a) Proponga una topología de red mixta cableada-inalámbrica, en la que los departamentos privados consiguen acceso externo mediante tecnología WiFi.
 - b) Especifique en la propia topología un direccionamiento de red público-privado mínimo para identificar adecuadamente todas las sub-redes de la configuración 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*. 3^a 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, 6^a 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>



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: direccional, 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

Para concluir el estudio del campo *TS* es de mencionar que este campo se usa en la práctica muy poco; de hecho, alternativamente en el RFC 2481 se propone una redefinición del mismo (en concreto los bits 6 y 7) para llevar a cabo la notificación explícita de congestión en conjunción con TCP.

- Con una longitud máxima permitida de 40 octetos, el campo *opciones* permite llevar a cabo algunas funciones de test y depuración. Cada opción especificada debe comenzar con el octeto indicado en la Figura 9.3(b). El primer bit, *copia*, indica si la opción en cuestión debe ser copiada en cada fragmento potencial del datagrama. Si este bit toma el valor 0, la opción solo se copiará en el primer fragmento y no en el resto.

Existen cuatro *clases* de opciones IPv4:

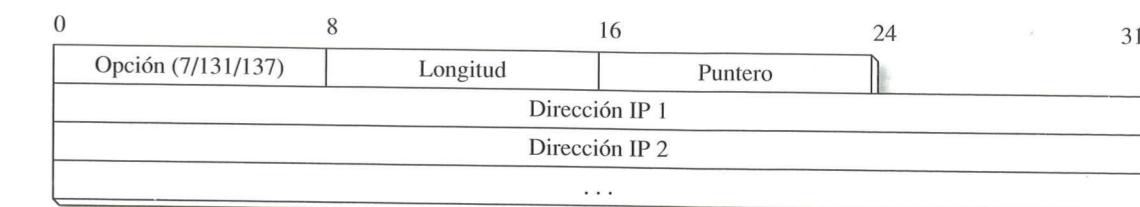
- 0 → Control de red o datagrama.
- 2 → Depuración y test.
- 1 y 3 → Reservados para uso futuro.

Las distintas opciones dentro de cada clase se diferencian entre sí mediante un *número*, siendo las más destacables las siguientes:

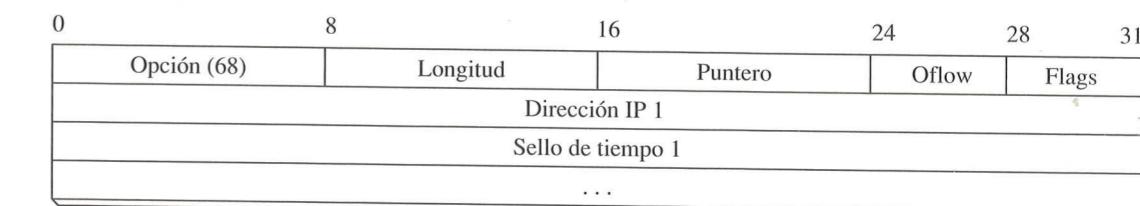
- a) *Registro de ruta*. Esta opción solicita que cada dispositivo de encaminamiento atravesado por el paquete especifique la dirección IP de la interfaz de salida dentro del mismo. Comenzando con el octeto mostrado en la Figura 9.3(b), con los subcampos *clase* = 0 y *número* = 7, el resto de campos de esta opción son los indicados en la Figura 9.4(a):
 - *Longitud*: número de octetos totales que forman la opción.
 - *Dirección IP i*: dirección IP de salida del *i*-ésimo dispositivo de encaminamiento atravesado por el paquete.
 - *Puntero*: próxima posición libre dentro del campo de opción *registro de ruta* en la que un nuevo dispositivo de encaminamiento almacenará su dirección.
- b) *Encaminamiento desde el origen*. Esta opción permite el encaminamiento del paquete siguiendo la ruta especificada por el emisor del mismo, según se discutió en el Apartado 6.3.4. De esta forma, cada dispositivo de encaminamiento se limitará a extraer la próxima dirección IP especificada a través del campo *puntero* (Figura 9.4(a)) y a retransmitir el paquete en consecuencia. El campo *puntero* será incrementado para cada nueva dirección IP accedida.
- c) Existen dos tipos de encaminamiento desde el origen: *estricto* (*clase* = 0, *número* = 9) y *flexible* (*clase* = 0, *número* = 3). Ambos con el campo *copia* a valor 1, en el primero se trata de seguir exactamente la secuencia de direcciones IP especificadas en el campo de opción correspondiente. En cambio, en el segundo se deja libertad a la subred para que entre cada dos direcciones IP indicadas en el paquete se puedan atravesar otras.

- c) *Sello de tiempo*. Esta opción es similar a la de registro de ruta, pero grabándose no solo la dirección IP de los dispositivos de encaminamiento atravesados por el paquete, sino también el instante en el que esto sucedió. Dicha marca de tiempo (Figura 9.4(b)) se expresa a través de 32 bits e indica los milisegundos transcurridos desde medianoche UTC.

Como en los casos anteriores, el campo *puntero* se incrementa consecuentemente en cada salto e indica la posición dentro del campo opción *sello de tiempo* en la que el siguiente dispositivo de encaminamiento debe grabar su dirección y el sello de tiempo correspondiente.



(a)



(b)

Figura 9.4. Formato de las opciones IP registro de ruta y encaminamiento desde el origen (a) y sello de tiempo (b).

Otros dos campos especificados en esta opción son los siguientes:

- *Flags*: de 4 bits de longitud, este campo indica la información a grabar por parte de los dispositivos de encaminamiento atravesados:
 - 0 → Grabar solo sello de tiempo.
 - 1 → Grabar dirección IP y sello de tiempo.
 - 3 → Las direcciones IP están especificadas por el emisor, de modo que un dispositivo de encaminamiento solo grabará el sello de tiempo si la siguiente dirección IP en la lista coincide con la suya.
- *Oflow*: campo de 4 bits utilizado para indicar el número de dispositivos de encaminamiento que no han podido grabar el sello de tiempo porque la longitud de la opción era demasiado pequeña.

Un comentario final acerca del campo *opciones* es que este no tiene forzosamente una longitud total múltiplo de 32 bits. Ello hace que se requiera un campo de *relleno* para, llegado el caso, completar la longitud del paquete hasta un múltiplo de 32 bits, haciendo así coherente el valor del campo *LC* del datagrama. Este campo indica, recordemos, el número de palabras de 32 bits de que consta la cabecera IP, dentro de la que se contabiliza el campo *opciones*. El campo *relleno* consiste en una secuencia de «todo ceros».

9.1.2. IPv6

Casi dos décadas después de la especificación formal de IPv4 apareció la versión 6 del protocolo IP: IPv6 (véase RFC 2460). Las características principales de este son:

- *Capacidades de direccionamiento extendidas*. En el caso de IPv6 se hace uso de direcciones IP de longitud 128 bits en lugar de las de 32 bits contempladas en IPv4.
- *Capacidad de etiquetado de flujo*. Cada paquete IPv6 se etiqueta con una marca identificativa del tráfico para el que el emisor desea, por ejemplo, una calidad de servicio dada.

— *Formato de cabecera simplificado y flexible.* Frente a la cabecera de formato fijo utilizada en IPv4, el datagrama IPv6 se desarrolla como una serie de cabeceras extendidas opcionales (véase Figura 9.5(a)). Esto proporciona una mayor simplicidad a la cabecera base, además de una mayor flexibilidad al protocolo, posibilitando su expansión natural a capacidades adicionales tales como nuevas tecnologías subyacentes o nuevas aplicaciones.

— *Autenticación y privacidad.* Como particularización de las cabeceras extendidas, hemos de destacar la existencia de unas específicas que permiten la provisión de seguridad en las transmisiones (véase Capítulo 12). Este nuevo aspecto de IP resulta de enorme interés actual en el contexto de las comunicaciones y la compartición de información.

El formato del paquete IPv6 es el indicado en la Figura 9.5(a), donde se muestra la disposición de las cabeceras extendidas tras la cabecera base. En relación a esta segunda, los campos que la componen son (Figura 9.5(b)):

- *Versión* (4 bits): para que los nodos intermedios puedan saber si se trata de un paquete IPv4 o IPv6, el primer campo del datagrama es, como en IPv4, el de versión. En el caso que nos ocupa el valor del campo será, obviamente, igual a 6.
- *Prioridad* (4 bits): campo que permite al origen indicar la prioridad deseada para sus paquetes, en relación a otros paquetes enviados. Los valores 0-7 se utilizan para el tráfico para el que el origen lleva a cabo control de congestión, y los valores 8-15 para el resto.
- *Etiqueta de flujo* (24 bits): todos los paquetes correspondientes a un mismo «flujo» serán transmitidos con las mismas direcciones IP origen y destino, la misma prioridad y la misma etiqueta de flujo. Esto permite a los nodos intermedios gestionar adecuadamente distintos flujos de datos, con diferentes requisitos de QoS (ver Apartado 7.2)
- *Longitud de datos* (16 bits): campo para indicar la longitud, en octetos, del campo de datos o *payload* del paquete.
- *Siguiente cabecera* (8 bits): identifica el tipo de cabecera de extensión que sigue inmediatamente a la fija de 40 octetos de IPv6. Si no existiese ninguna cabecera opcional tras la base, el valor de este campo sería 59.

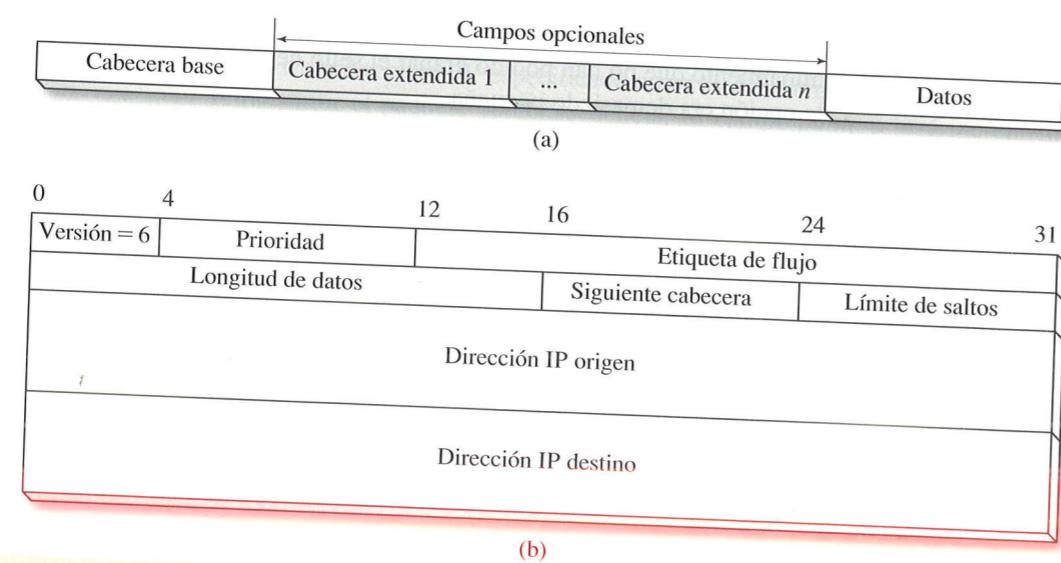


Figura 9.5. Formato general del paquete IPv6 (a) y campos de la cabecera base (b).

— *Límite de saltos* (8 bits): establece el número máximo de saltos permitido para un datagrama. Esto es, tiene la misma función que el campo TTL del paquete IPv4 pero expresado en saltos en lugar de en tiempo para reducir las necesidades de cómputo en los nodos intermedios. Así, cada nodo atravesado por el paquete decrementará este campo en 1, de manera que el paquete será descartado cuando el valor del campo sea 0.

— *Direcciones IP origen y destino* (128 bits cada una): como ya se ha indicado, las direcciones IPv6 son de 128 bits e identifican, como no puede ser de otro modo, las máquinas origen y destino del datagrama. Más adelante se profundiza en la nomenclatura general utilizada para este tipo de direccionamiento.

Tras la cabecera base, fija, en IPv6 pueden aparecer otros campos opcionales (Figura 9.5(a)) en lo que se denomina cabeceras de extensión, cuyo objetivo puede ser diverso (seguridad, fragmentación, etc.). Más adelante se discuten con más detalle estas cabeceras de extensión; antes de ello, sin embargo, veamos el direccionamiento utilizado en IPv6.

Direccionamiento IPv6

Como en el caso de IPv4, una dirección IPv6 es una etiqueta numérica que identifica una interfaz de red. En el caso de una dirección *unicast*, se trata de una interfaz específica conocida. En el caso de direcciones *IP multicast* (véase Capítulo 8) se identifica un grupo de dispositivos que participan de un mismo servicio. Es de mencionar que en IPv6 las direcciones *broadcast* se consideran un caso particular de las *multicast*.

Adicionalmente a estos tipos, IPv6 introduce un nuevo conjunto de direcciones conocidas como *anycast* (RFC 1546). Una dirección IP de este tipo identifica un grupo de interfaces de modo que un paquete *anycast* se envía a solo una de ellas, generalmente la más cercana.

Una dirección IPv6 se representa mediante ocho grupos de cuatro dígitos hexadecimales (expresados en letra minúscula), cada uno de los grupos representando en consecuencia 16 bits (2 octetos), y separados entre sí mediante el carácter «::» (véase RFC 2373). Ejemplo de todo lo anterior es la dirección IPv6 4ce2:0000:0000:28c9:82ea:dba9:07fa:0001.

Con objeto de simplificar la notación de las direcciones se permite la supresión de los 0 existentes en cada grupo. Así, la dirección ejemplo anterior quedaría 4ce2:0:0:28c9:82ea:dba9:7fa:1. También por simplicidad se acorta la dirección sustituyendo la secuencia de grupos «todo ceros» más larga por «::». En el caso anterior tendríamos 4ce2::28c9:82ea:dba9:7fa:1. En caso de que existiese más de una cadena de grupos «todo ceros» de la misma longitud, la sustitución se haría solo para la situada más a la izquierda. Por ejemplo, si tuviésemos la dirección 4ce2:0:0:28c9:0:0:7fa:1, la identificación final sería 4ce2::28c9:0:0:7fa:1.

Las direcciones *unicast* y *anycast* están compuestas usualmente, como sucede en IPv4, de dos partes lógicas: un prefijo de red de 64 bits usado para *routing* (véanse los protocolos de encaminamiento estudiados más adelante en este capítulo) y un identificador de interfaz de red (*o host*), también de 64 bits (Figura 9.6). Del grupo primero, los 16 bits menos significativos pueden utilizarse para identificar subredes dentro de una misma red. Frente a las direcciones anteriores, las *multicast* pueden tener distintos formatos dependiendo de la aplicación, si bien todas comienzan por el byte 11111111.

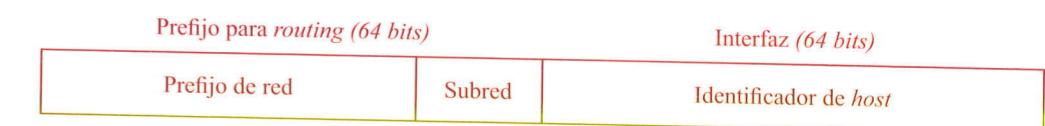


Figura 9.6. Formato general de direcciones *unicast* en IPv6.

Los rangos de direcciones de red se escriben en notación CIDR, de modo que, por ejemplo, la red 4ce2::28c9:0:0/96 comienza en la dirección 4ce2::28c9:0:0:0000:0000 y finaliza en la 4ce2::28c9:0:0:ffff:ffff. Por otro lado, a fin de facilitar el transitorio entre el direccionamiento IPv4 y el IPv6, el prefijo ::ffff:0:0/96 designa una dirección IPv4. Por ejemplo, la dirección IPv6 ::ffff:0:0:c0a8:10f correspondería a la IPv4 192.168.1.15. Adicionalmente a este hecho, está permitido escribir los 32 últimos bits de una dirección IPv6-IPv4 en la notación decimal con puntos. Así, la dirección anterior podría especificarse en IPv6 como ::ffff:0:0:192.168.1.15.

Cabe también mencionar la disposición de algunas direcciones *unicast* reservadas como son: ::/0, ruta por defecto; ::1/128, autobucle (*localhost*); ::/128, no especificada (p.e., un *host* iniciándose); y fc00::/7, comunicaciones locales. Del mismo modo, las direcciones *multicast* ff00::0/8 están reservadas para distintos usos y no pueden ser usadas para indicar grupos. También las 128 direcciones *anycast* más altas dentro de cada prefijo de subred (/64) están reservadas, lo que significa que tienen 57 bits a valor 1 seguidos de 7 bits que identifican la identidad *anycast*.

Para concluir esta breve discusión sobre el direccionamiento IPv6, hemos de hacer dos reseñas importantes. Por una parte, que una dirección puede tener un tiempo de uso limitado y que, frente al carácter habitual de direcciones únicas, estáticas en IPv4, una interfaz puede tener asociadas más de una dirección IPv6 y que estas pueden ser creadas temporalmente mediante cadenas aleatorias variables en el tiempo.

Por otro lado, comentar que si deseamos indicar una dirección IPv6 directamente en un enlace URL, esta ha de aparecer entre corchetes ('[]'). Por ejemplo, en el caso http://[2001:f8f:3400::34:47b9]:8080 estaríamos solicitando un recurso al puerto 8080 de la dirección 2001:f8f:3400::34:47b9.

Cabeceras de extensión

Como hemos mencionado con anterioridad, adicionalmente a la parte fija de la cabecera, IPv6 contempla la inclusión de una o más cabeceras opcionales a través de las cuales se posibilitan distintas funciones de interés. Son las denominadas cabeceras de extensión, encontrándose definidas en el RFC 2460 las siguientes, todas ellas con una longitud total múltiplo de 64 bits:

— *Fragmentación*. Como vimos en IPv4, las funciones de fragmentación y ensamblado son funciones necesarias para permitir la transmisión de paquetes de tamaño superior al soportado por las MTU asociadas a las rutas. Esto sigue siendo válido en IPv6 con la salvedad de que el proceso de fragmentación no se realiza en los nodos intermedios, sino exclusivamente en el origen. Para ello, previamente a la transmisión, el emisor debe llevar a cabo un procedimiento de *descubrimiento de MTU de ruta* en base al empleo del bit *DF* ya conocido de IP y protocolo ICMP (véase Apartado 9.2 más adelante), a fin de conocer la MTU mínima en la ruta hacia el destino. Fragmentados en consecuencia los paquetes de longitud mayor a la MTU mínima, estos se transmitirán hacia el destino en paquetes con la cabecera de extensión mostrada en la Figura 9.7(a). Los campos de esta cabecera son los siguientes:

- *Siguiente cabecera*: campo de 8 bits que indica el tipo de la siguiente cabecera extendida. Si no existiese ninguna más, es decir, si a continuación siguiese el campo *datos* del paquete IPv6, el valor del campo *siguiente cabecera* será 59.
- *Reservado*: campo a valor 0 ignorado en la recepción.
- *Desplazamiento*: campo de 13 bits que indica, en unidades de 8 octetos, la posición del fragmento respecto al inicio del paquete original sin fragmentar. Nótese la correspondencia de este campo con el homónimo visto para el paquete IPv4.

- *MF*: campo de 3 bits en el que los dos primeros toman el valor 0 y se indica a través del último que el fragmento en cuestión es (*MF* = 0) o no (*MF* = 1) el último de los que componen el datagrama original.
- *Identificación*: campo de 32 bits con el que se numera cada paquete del mensaje. Como en el caso de IPv4, todos los fragmentos correspondientes a un mismo datagrama tendrán el mismo valor de este campo. Obsérvese que la longitud de este campo en IPv4 era solo de 16 bits, permitiendo su ampliación al doble de bits una mejor adecuación de IPv6 a redes de alta velocidad y mensajes de gran tamaño.

De acuerdo con el RFC 1700, la cabecera de extensión de fragmentación se referencia con el valor 44 en el campo *siguiente cabecera* de la cabecera precedente a esta en el paquete IPv6.

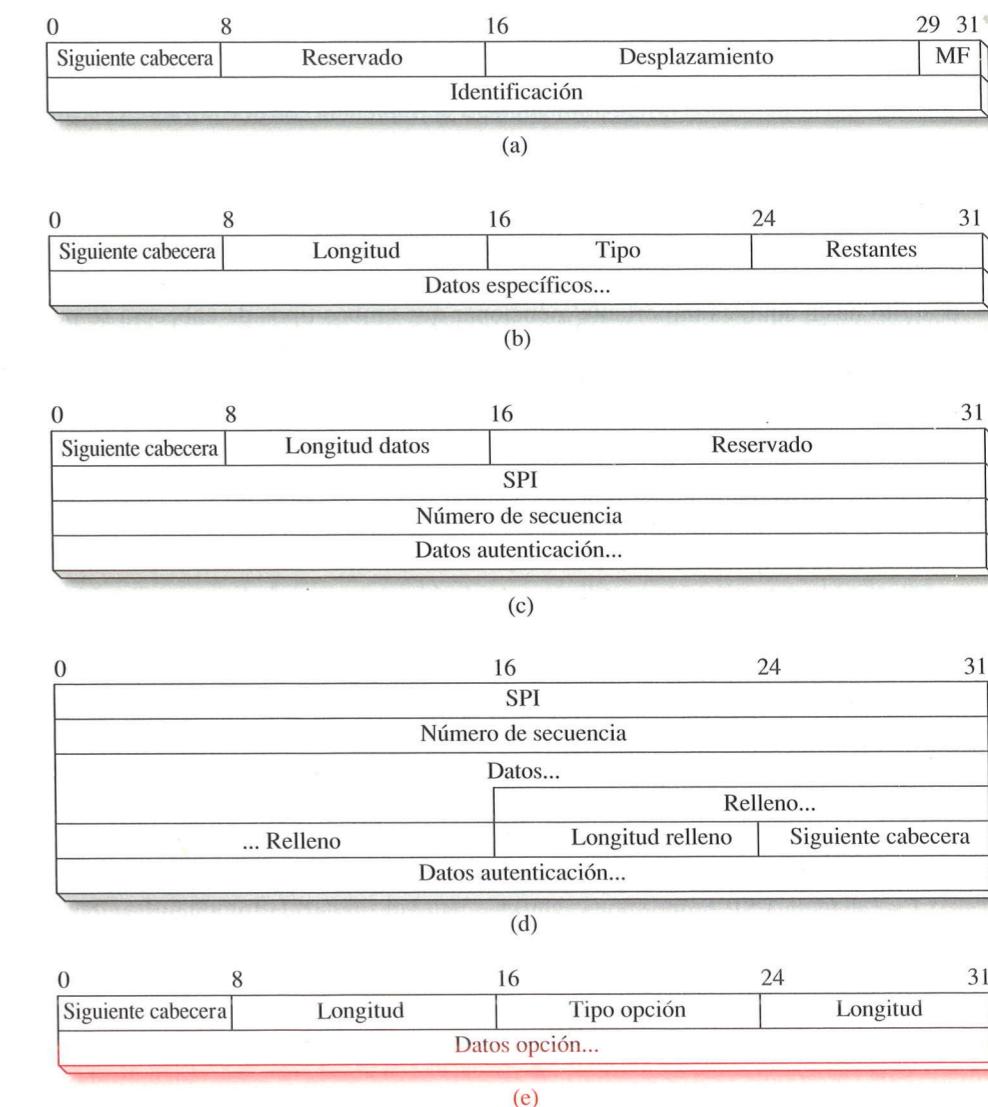


Figura 9.7. Cabeceras de extensión IPv6 de fragmentación (a), de encaminamiento (b), de autenticación (c), de encapsulado de seguridad (d) y genérica de opciones (e).

— *Encaminamiento.* Análoga a la opción de *encaminamiento desde el origen* o a la de *registro de ruta* en IPv4, esta cabecera IPv6 permite especificar por parte del origen la ruta a seguir por un paquete dado. El formato de esta cabecera es el mostrado en la Figura 9.7(b):

- *Siguiente cabecera:* indica el tipo de la siguiente cabecera extendida. Si no existiese ninguna más, esto es, si a continuación siguiese el campo datos del paquete IPv6, el valor del campo siguiente cabecera será 59.
- *Longitud:* longitud total de esta cabecera, en unidades de 8 octetos.
- *Tipo:* campo de 8 bits para indicar el tipo específico de encaminamiento (ver campo *datos específicos* más adelante o RFC para más detalles).
- *Restantes:* número de nodos intermedios que restan por visitar hasta llegar al destino.
- *Datos específicos:* campo de longitud variable definido por el tipo de encaminamiento. En el caso tipo = 0, el formato del campo *datos específicos* consiste en una lista de direcciones IP a visitar, precedida por 32 bits a valor 0.

La cabecera de extensión de encaminamiento se referencia con el valor 43 en el campo *siguiente cabecera* de la cabecera precedente a esta en el paquete IPv6. También cabe mencionar que esta opción está habitualmente deshabilitada en los routers por cuestiones de seguridad.

— *Autenticación y encapsulado de seguridad.* En los RFC 2402 y 2406 se describen, respectivamente, las cabeceras de extensión de autenticación (AH, «Authentication Header») y de encapsulado seguro de los datos (ESP, «Encapsulating Security Payload»). Aunque no se han descrito hasta aquí, es importante mencionar que ambos tipos de cabecera se pueden utilizar tanto en IPv4 como en IPv6.

Con la cabecera AH se permite la autenticación de un paquete y la comprobación de su integridad. Para ello, los campos de la cabecera de extensión directamente relacionados con esta función son los siguientes (Figura 9.7(c)):

- *SPI* («Security Parameters Index»): campo de 32 bits que, en combinación con la dirección IP de destino, identifica únicamente la asociación de seguridad para este paquete. Es decir, el conjunto de elecciones relacionadas con los algoritmos de cifrado, de resumen o hash y de autenticación a utilizar entre ambos extremos de la comunicación (véase Capítulo 12).
- *Número de secuencia:* valor monótonamente creciente a lo largo de la transmisión utilizado para la detección de paquetes duplicados. A través de esta técnica simple se intentan evitar ataques de repetición.
- *Datos autenticación:* campo de longitud variable que contiene el valor de comprobación de integridad y autenticación para este paquete. Algoritmos de autenticación empleados en el cálculo de este campo son DES (RFC 2405), MD5 (RFC 2403) y SHA-1 (RFC 2404) —véase Capítulo 12—.

La cabecera ESP proporciona confidencialidad, integridad y autenticación de los datos. Los campos de la cabecera ESP son los siguientes (Figura 9.7(d)):

- *SPI:* como en AH.
- *Número de secuencia:* como en AH.
- *Datos:* campo de longitud variable cuya naturaleza se especifica a través del campo *siguiente cabecera* existente más adelante; generalmente corresponde a una PDU de capa superior.
- *Relleno:* campo de longitud variable al que se recurre en caso de que el algoritmo de cifrado utilizado precise que la longitud del texto sea múltiplo de un cierto número de octetos.
- *Longitud relleno:* 8 bits para especificar la longitud del campo anterior.

- *Siguiente cabecera:* tipo de cabecera que sigue a esta en el paquete IPv6.
- *Datos de autenticación:* campo opcional donde se recogen los datos de autenticación o integridad en la forma descrita en el campo del mismo nombre de la cabecera AH anterior.

La cabecera de extensión de autenticación se referencia con el valor 51 en el campo *siguiente cabecera* de la cabecera precedente a esta en el paquete IP. Por su parte, la cabecera ESP se identifica mediante el valor 50 (ver RFC 1700). Como comentario adicional, decir que el uso de ambas cabeceras constituye el protocolo IPsec, ideado para proporcionar seguridad en las comunicaciones sobre IP (ver RFC 4301; Capítulo 12).

— *Otras opciones IPv6.* Adicionalmente a las cabeceras extendidas mencionadas, existen otras cuyo formato general es el indicado en la Figura 9.7(e). De entre ellas podemos destacar dos:

- *Salto-a-salto:* cabecera de referencia a valor 0 en el campo *siguiente cabecera* de la cabecera precedente, a través de la que se indican acciones a tomar por los dispositivos de encaminamiento atravesados en la ruta hacia el destino.
- *De destino:* frente a la anterior, esta opción especifica acciones que deben ser tomadas solo por el nodo destino del paquete.

La cabecera de extensión *de destino* se referencia con el valor 60 en el campo *siguiente cabecera* de la cabecera precedente a esta en el paquete IPv6.

Como ejemplo de algunas de las acciones a que se refieren las opciones anteriores podemos mencionar entre otras: rechazo del paquete, rechazo del paquete y envío en respuesta al origen de un mensaje ICMP de problema de parámetros (véase Apartado 9.2.1).

Para concluir el estudio de las cabeceras extendidas de IPv6, hemos de decir que se recomienda que el orden en que aparezcan en el paquete (si es que lo hacen) tras la cabecera base fija sea el siguiente: *salto-a-salto, de destino* (para las opciones a procesar en el primer destino más los destinos subsiguientes listados en la cabecera de encaminamiento), *encaminamiento, fragmentación, autenticación, encapsulado de seguridad y de destino* (para las opciones a procesar solo por el destino final del paquete).

9.2. Mensajes de control de Internet: protocolo ICMP

En el RFC 792 se describe el *protocolo de mensajes de control de Internet* (ICMP, «Internet Control Message Protocol»). ICMP es, como IP, un protocolo de la capa de red, lo que no significa que sea una alternativa al mismo, sino, por el contrario, un complemento. Además, ICMP es usuario de IP, es decir, los mensajes ICMP se encapsulan dentro de los paquetes IP.

Según se desprende del estudio de IP, cada dispositivo de encaminamiento funciona de forma relativamente independiente del resto, de manera que todo el sistema funcionará adecuadamente si, y solo si, lo hacen todos los dispositivos que lo forman. Desafortunadamente, esto no ocurre en un sistema real. Así, encapsulado en el datagrama IP, cuyo campo *protocolo* tomará el valor 1 (ver RFC 1700), el protocolo ICMP define un conjunto de mensajes para informar o señalizar sobre determinadas situaciones tales como inaccesibilidad de un destino, expiración del tiempo de vida de un datagrama IP, etc. Además, ICMP define otros mensajes adicionales (como el de eco) para facilitar el diagnóstico de posibles problemas en la red.

Todos los mensajes ICMP comienzan con los siguientes tres campos de cabecera (los sombreados en la Figura 9.8), con una longitud total de 32 bits:

- *Tipo* (8 bits): indica el tipo del mensaje.
- *Código* (8 bits): identifica un subtipo dentro del tipo.

- *Comprobación* (16 bits): complemento a 1 de la suma complemento a 1 de las palabras de 16 bits que componen el mensaje ICMP, usado para el control de errores.

Los mensajes ICMP más relevantes son los siguientes (Tabla 9.1 y Figura 9.8):

- *Eco*. Utilizada para testar la accesibilidad de un destino dado, esta funcionalidad ICMP implica la consideración de dos mensajes, uno de solicitud de eco (*tipo* = 8, *código* = 0) y otro de respuesta (*tipo* = 0, *código* = 0).

Implementado a través del comando de usuario *ping*, un emisor genera un mensaje ICMP de solicitud de eco como el mostrado en la Figura 9.8(a), que será contestado mediante un mensaje de respuesta por el destinatario, en caso de estar accesible. El campo *opcional* contiene un conjunto de datos arbitrarios que el receptor deberá devolver al emisor en la respuesta. Los campos *identificador* y *secuencia* se utilizan para hacer corresponder solicitudes con respuestas. Como resultado, *ping* muestra por pantalla el tiempo consumido hasta el destino especificado.

- *Destino inalcanzable*. El mensaje ICMP tipo 3 (Figura 9.8(b)) se genera cuando el destino IP especificado en un datagrama dado no es accesible. Diversas pueden ser las causas que motiven esta inaccesibilidad, lo cual se especifica a través del campo *código* con los siguientes valores: 0 → red inalcanzable, 1 → host inalcanzable, 2 → protocolo inaccesible, 3 → puerto inaccesible, 4 → se precisa fragmentación y el bit DF está activo, 5 → fallo en ruta de origen, 6 → red destino desconocida, 7 → host destino desconocido, 8 → host origen aislado, 9 → comunicación prohibida con la red destino, 10 → comunicación prohibida con el *host* destino, 11 → red inaccesible por el tipo de servicio (campo *TS* en el paquete IP), 12 → *host* inaccesible por el tipo de servicio (campo *TS* en el paquete IP).

Dado que gran parte de los elementos mencionados anteriormente se especifican en la cabecera del protocolo IP o en el de nivel superior, el mensaje ICMP de *destino inalcanzable* incluye tanto la cabecera IP como parte de la PDU de la capa superior (a través de los 64 primeros bits del campo *datos* del datagrama IP) a fin de que el origen que generó el paquete al que se refiere el mensaje ICMP pueda realizar las comprobaciones oportunas.

- *Ralentización del origen* (del inglés «source quench»). El tipo de mensaje 4 consiste en una notificación explícita de congestión hacia atrás tal como se comentó en el Apartado 7.1.3. A través de este mensaje ICMP (Figura 9.8(c)), un dispositivo de encaminamiento comunica al *host* origen del paquete cuya cabecera y primeros 64 bits se especifican en el campo de datos del mensaje, que se está produciendo congestión en los recursos utilizados en su transmisión. Al recibir este mensaje, el *host* correspondiente debe reducir el flujo de emisión en la forma que se comentará en el Capítulo 10 (Apartado 10.3.5).

Tabla 9.1. Principales mensajes ICMP.

Campo tipo	Mensaje ICMP
8/0	Solicitud/respuesta de eco
3	Destino inalcanzable
4	Ralentización del origen
5	Redirección
11	Tiempo excedido
12	Problema de parámetros
13/14	Solicitud/respuesta de sello de tiempo
17/18	Solicitud/respuesta de máscara de red

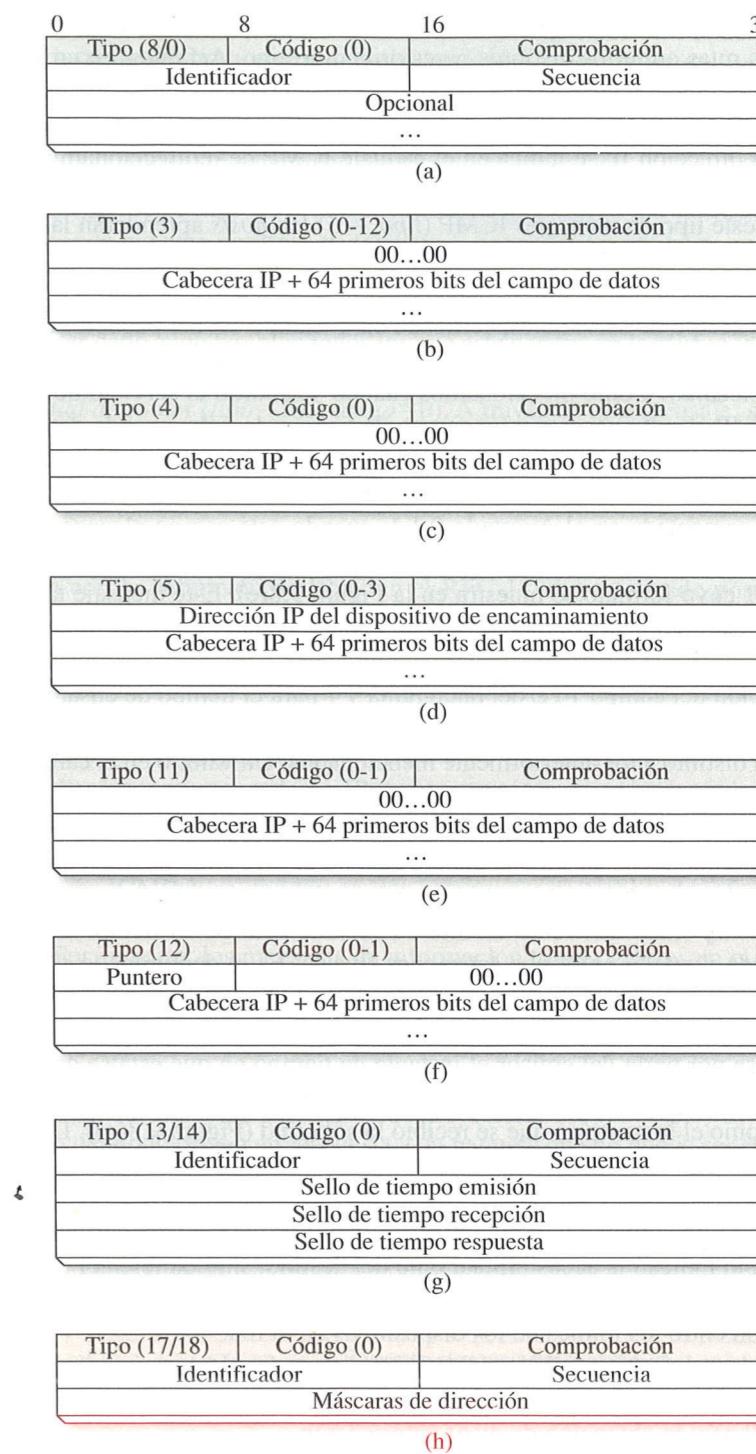


Figura 9.8. Formato de mensajes ICMP: (a) eco, (b) destino inalcanzable, (c) ralentización del origen, (d) redirección, (e) tiempo excedido, (f) problema de parámetros, (g) sello de tiempo y (h) máscara de red. (Nota: los campos sombreados corresponden a la cabecera ICMP).

- *Paquete demasiado grande (tipo=2, código=0)*. Mensaje enviado por un *router* cuando un paquete dado no pueda ser enviado por superar la MTU del enlace en cuestión.
 - *Tiempo excedido (tipo=3, código=0-1)*. Mensaje generado por un *router* hacia el origen de un paquete IPv6 que es descartado por haber alcanzado el campo *límite de saltos* el valor 0.
 - *Problema de parámetros (tipo=4, código=0-2)*. Mensaje motivado por la aparición de un problema al procesar algún campo del paquete.
- *Mensajes de información:*
- *Solicitud de eco (tipo=128, código=0)*. Como en ICMPv4.
 - *Respuesta de eco (tipo=129, código=0)*. Como en ICMPv4.
 - *Pertenencia a grupo (tipo=130-132, código=0)*. Mensajes usados para la notificación de información relacionada con la gestión de grupos *multicast* (véase IGMP en el Apartado 9.4.2).

A parte de los mensajes mencionados, existen otros valores de uso reservado tanto para los mensajes de error como los de información. Al igual que en ICMPv4, se incluyen mensajes para el descubrimiento y anuncio de *routers* y de las máscaras. También se incluyen funciones relacionadas con el descubrimiento de vecinos y agentes, de uso en el direccionamiento *anycast*. Por otro lado, en los RFC correspondientes se hace mención expresa a consideraciones adicionales acerca de la seguridad de las transmisiones sobre el protocolo ICMPv6. Se indica así la posible ocurrencia de ataques a este protocolo y el uso de las cabeceras AH y ESP en IP para la provisión de confidencialidad, integridad y autenticación.

9.3. Encaminamiento dinámico en Internet

Dado un datagrama IP, el proceso de encaminamiento seguido para su retransmisión en cada uno de los nodos intermedios de la subred es el siguiente:

1. Extracción de la dirección IP de destino especificada en el datagrama: IP_D .
2. Para cada entrada en la tabla de encaminamiento, consistente en un identificativo de red de destino, IP_N , y la máscara asociada, M_N , además del siguiente nodo en la ruta a seguir hasta dicha red, se procede como sigue:
 - a) Se realiza la operación lógica AND, bit a bit, entre IP_D y la máscara de red M_N , obteniéndose el identificativo de red IP_R . Es decir, $IP_R = (IP_D \text{ AND } M_N)$.
 - b) Si $IP_N = IP_R$, o lo que es lo mismo, si el identificativo de red correspondiente a la entrada coincide con el obtenido tras aplicar la máscara asociada a la dirección IP de destino del paquete, dicho paquete se encaminará como se indica en la tabla, tomando como dirección física (MAC) de destino la del siguiente dispositivo de encaminamiento en la ruta.
 - c) Si, por el contrario, $IP_N \neq IP_R$, se procede a consultar la siguiente entrada en la tabla.
3. Para evitar situaciones de error, la última entrada de la tabla de *routing* suele hacer referencia a una ruta por defecto sobre la que se enviarán aquellos paquetes para los que no se encuentre ninguna coincidencia previa en la tabla.

Obsérvese de lo expuesto que las direcciones IP origen y destino de los datagramas permanecen inalteradas a lo largo de la ruta; en cambio, las direcciones físicas de las tramas sobre los que se encapsulan varían salto a salto. Además, resulta relevante el orden de aparición de las entradas en la tabla de encaminamiento, aplicándose la primera de ellas con prefijo más largo que verifique $IP_N = IP_R$.

Haciendo referencia a los esquemas de establecimiento de las tablas de encaminamiento estudiados en el Capítulo 6 del texto, hemos de mencionar que en Internet se implementa un esquema adaptable, dinámico, de tipo distribuido jerárquico. Esto es, por una parte, los nodos se intercambian sus tablas periódicamente en el tiempo a fin de actualizar y adaptar la información de *routing* y, por otra, la red se divide en regiones de modo que la actualización de las tablas se realiza a dos niveles separados: intra-región e inter-región.

Cada una de las regiones en que se divide Internet se denomina *sistema autónomo* (Figura 9.9), consistente en un conjunto de subredes administradas por una única autoridad de forma que en dicho entorno se puede implementar un algoritmo de encaminamiento independientemente de los considerados en otros sistemas autónomos. Son los conocidos como *protocolos de encaminamiento interiores* o IGP («Interior Gateway Protocol»). Aparte del conocimiento que cada dispositivo de encaminamiento dentro de un sistema autónomo dado debe tener del mismo, deben conocerse las rutas entre sistemas autónomos a fin de establecer una conectividad completa de toda la red. Para ello, en cada sistema autónomo se establece al menos un dispositivo de encaminamiento encargado de encaminar el tráfico entrante/saliente al sistema autónomo. Estos dispositivos son los denominados *dispositivos de encaminamiento exterior o de frontera* ($R1$ y $R2$ en la Figura 9.9(b)). El encaminamiento entre sistemas autónomos también se establece siguiendo un esquema distribuido, en este caso mediante un algoritmo común a todos los *routers* frontera como es el algoritmo EGP («Exterior Gateway Protocol») o el más actual BGP («Border Gateway Protocol»).

9.3.1. Protocolos de encaminamiento interiores

En este apartado se presentan dos algoritmos IGP implementados para la actualización dinámica de las tablas de encaminamiento internas a un sistema autónomo dado. Estos son RIP y OSPF, de amplia adopción en Internet. Ambos, como se ha indicado anteriormente, presentan una característica común: son de naturaleza distribuida; es decir, la actualización de las tablas se realiza en base al intercambio periódico de las mismas entre nodos vecinos.

Protocolo de información de encaminamiento (RIP)

La versión 1 del algoritmo RIP («Routing Information Protocol») se especifica en el RFC 1058, encontrándose en los RFC 1388, 1723 y 2453 revisiones sucesivas de la versión 2 del mismo. Aunque con una función propia de la capa de red, encaminamiento, RIP se implementa sobre UDP (ver capítulo

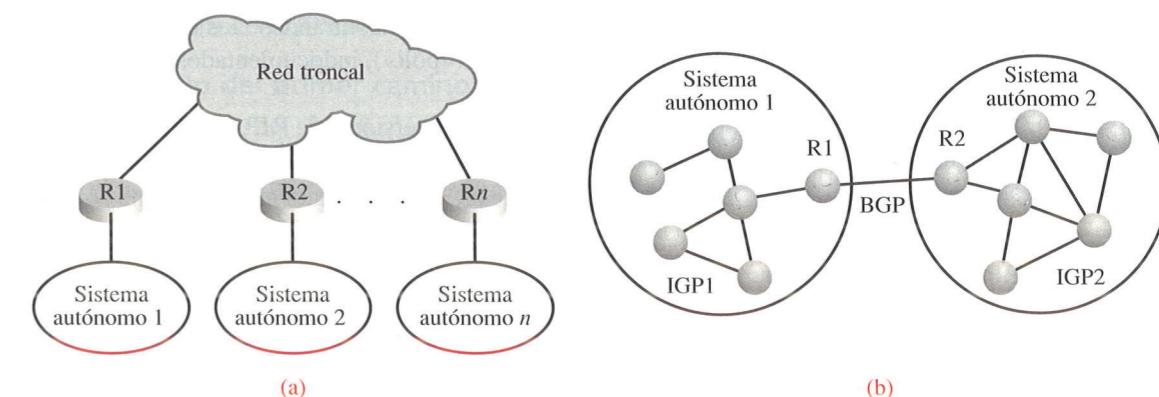


Figura 9.9. Visión conceptual de un sistema autónomo (a) y esquema de protocolos de encaminamiento interiores y exteriores (b).

$M = 1$. Además, cada mensaje estará numerado secuencialmente a través del campo *secuencia base de datos*.

- d) El campo de 1 bit S indica si el nodo emisor es el maestro ($S = 1$) o el esclavo ($S = 0$).
- e) El resto del paquete consta de una serie de piezas descriptoras de la base de datos correspondiente al estado de los enlaces. Cada una de estas piezas es lo que se llama *cabecera LSA* (HLSA, «Header Link Status Advertisement») y está compuesta por los campos indicados en la Figura 9.12(d):
 - *Edad del enlace*, en segundos, desde que este fue establecido.
 - *Opciones*, como en el apartado b) anterior
 - *Tipo de enlace*, el cual puede tomar cinco valores: 1 → de dispositivo de encaminamiento, 2 → de red, 3 → ruta a red, 4 → ruta a nodo frontera y 5 → a destino externo.
 - *Identificador* que describe la porción de Internet especificada por el enlace. Los posibles valores de este campo dependen del tipo de enlace de que se trate.
 - *Dirección del nodo notificador* que indicó la existencia de este enlace.
 - *Número de secuencia* del enlace para su ordenación e identificación, permitiendo, por ejemplo, la detección de LSA duplicados.
 - Suma de *comprobación* de los campos del LSA (ver mensaje tipo 4), incluyendo la cabecera excepto el campo *edad del enlace*.
 - *Longitud* en bytes del LSA (ver mensaje tipo 4) incluida la cabecera.

— Mensaje de *solicitud del estado del enlace* ($tipo = 3$). Mostrado en la Figura 9.13(a), este tipo de mensajes OSPF se envía por parte de un nodo para requerir información acerca de un conjunto

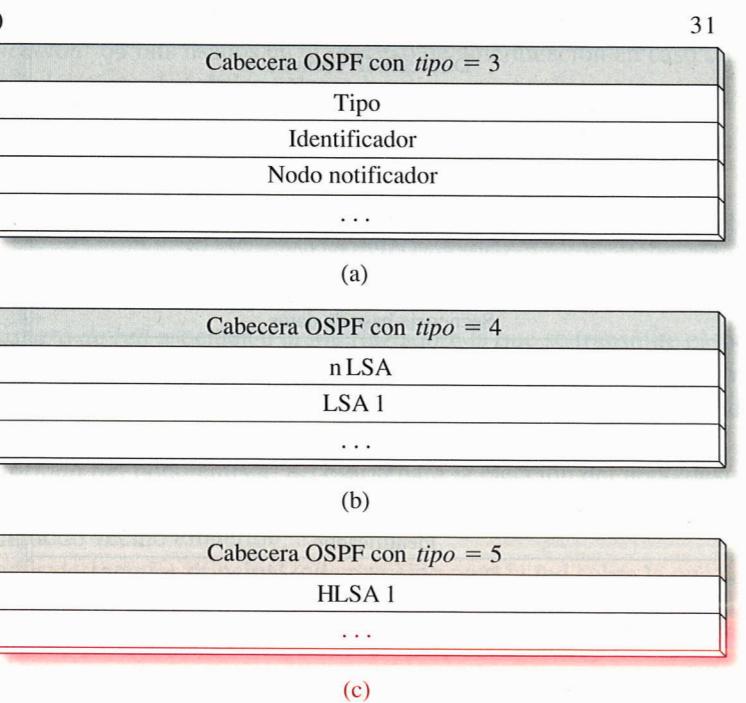


Figura 9.13. Mensajes OSPF solicitud del estado del enlace (a), actualización del estado del enlace (b) y confirmación del estado del enlace (c).

específico de enlaces (LSA). De cada uno de ellos se debe indicar su *tipo*, su *identificador* y el *nodo que lo notificó*.

- Mensaje de *actualización del estado del enlace* (*tipo* = 4). Enviado en respuesta al anterior, este mensaje indica el número de anuncios de estado contenidos (*nLSA*) y la lista de los mismos (Figura 9.13(b)). Cada uno de los LSA está compuesto por la cabecera HLSA, ya comentada y mostrada en la Figura 9.12(d), además de datos específicos dependientes del tipo de enlace de que se trate. Entre otros datos especificados (identificador, máscara, etc.), los más relevantes son: tipo de servicio y métrica o coste asociado al enlace (para más detalles, ver RFC 2328).
- Mensaje de *confirmación del estado del enlace*. Paquete utilizado para confirmar la recepción de un mensaje de actualización del estado del enlace. Como se indica en la Figura 9.13(c), este tipo de mensajes está compuesto por la cabecera OSPF con el campo *tipo* a valor 5 y una HLSA para cada LSA recibida en el paquete de actualización tipo 4.

Protocolos IGRP y EIGRP

Además de los protocolos de *routing* descritos, también merecen especial mención los propietarios de Cisco IGRP y EIGRP. El primero de ellos, *Interior Gateway Routing Protocol*, es, como RIP, un protocolo vector-distancia y fue desarrollado para solventar dos limitaciones de este para grandes redes: número máximo de saltos igual a 15 y uso de una sola métrica. En el caso de IGRP, el número máximo de saltos es 255 (100 por defecto) y se combinan varias métricas (ancho de banda, retardo, carga, MTU y fiabilidad) en una sola a través de una fórmula donde se hace uso de pesos para cada una de ellas.

Finalmente, comentar que la actualización de las tablas en IGRP se realiza por defecto cada 90 segundos y que se trata de un protocolo conforme a clase (*classful*), lo que significa que no se gestionan máscaras de subred. Esto es, si se trata de una red IP Clase A, los bits de red y *host* son los fijos ya conocidos: 7 y 24, respectivamente; 14 y 16 para Clase B; y 21 y 8 para Clase C.

Con posterioridad a IGRP, Cisco desarrolló el protocolo EIGRP («Enhanced Interior Gateway Routing Protocol»), el cual ha sustituido completamente al anterior. A diferencia de los protocolos previos, incluido IGRP, EIGRP se implementa directamente en la capa de red (es decir, sobre IP) y no en la de aplicación.

Las características principales de EIGRP son:

- Es conforme a CIDR y permite enmascaramiento variable (*classless*).
- Soporta balanceo de carga, en base a evitar bucles parciales y el uso de un algoritmo que calcula la cantidad de tráfico a enviar por cada camino.
- Permite usar diferentes *passwords* a lo largo del tiempo.
- Soporta autenticación MD5 entre los *routers*.
- El envío de la información de *routing* se refiere más bien a cambios en la topología y no tanto a tablas de encaminamiento completas.
- Realiza procesos de encaminamiento separados por protocolo (IP, IPv6, IPX, Apple Talk, etc.).

EIGRP implementa el algoritmo DUAL («Diffusing Update ALgorithm») para mejorar el encaminamiento en base a la eliminación de bucles en el entorno. Tres son las tablas usadas para el cálculo de las rutas:

- *Tabla de vecinos*: contiene información del conjunto de *routers* directamente conectados, disponiéndose una tabla distinta para cada protocolo posible. Cada entrada corresponde a un vecino, con la descripción de la interfaz de red y dirección, además de un contador para el intercambio periódico de paquetes *hello* para testar la accesibilidad del nodo en el tiempo.

- *Tabla de topología*: contiene una lista de las posibles redes de destino, junto con el coste asociado a la ruta y un «nodo sucesor» y un «nodo posible sucesor» para alcanzarla.
- *Tabla de rutas*: almacena las rutas reales a todos los destinos.

Como se ha indicado anteriormente, a diferencia de otros protocolos como RIP, EIGRP no se basa en el intercambio periódico de las tablas entre nodos vecinos, sino que se comunican los cambios habidos a lo largo del tiempo a partir de la definición de relaciones de vecindad.

9.3.2. Protocolo exterior BGP

A diferencia de como sucede en el encaminamiento interno, en el que cada sistema autónomo puede considerar un IGP independiente del resto (RIP, OSPF, EIGRP, etc.), el establecimiento de las rutas entre sistemas autónomos precisa de un algoritmo común implementado sobre los dispositivos de encaminamiento exteriores o frontera («border» en inglés). Inicialmente se especificó en el RFC 823 el protocolo GGP («Gateway-to-Gateway Protocol»), implementándose posteriormente el protocolo EGP («Exterior Gateway Protocol»), detallado en el RFC 904. A pesar del amplio uso que de este último protocolo se ha hecho, los problemas que a continuación se enuncian (ver RFC 1009) motivaron su sustitución por el *protocolo de pasarela frontera* (BGP, «Border Gateway Protocol»):

1. La conectividad global falla si un nodo frontera falla.
2. EGP solo establece una ruta para alcanzar cada sistema autónomo, no permitiendo balanceo de carga.
3. No interpreta ninguna de las métricas de distancia internas que aparecen en los mensajes de actualización de las tablas.

La última versión del protocolo BGP es la 4 (BGP-4), especificada en el RFC 1771 (actualizado por el RFC 4271). De forma análoga a EGP, el protocolo BGP presenta los siguientes tipos de mensajes:

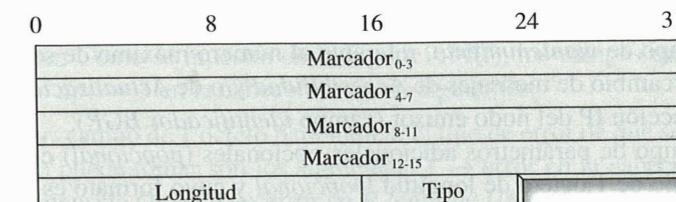
- *Adquisición de vecino*, a fin de establecer los nodos frontera entre los que se efectuará el intercambio de la información de encaminamiento.
- *Accesibilidad de vecino*, con objeto de testar la alcanzabilidad de los mismos.
- *Información de encaminamiento*, para proceder a la actualización de las tablas.

Cada uno de los mensajes BGP comienza con los siguientes tres campos de 19 octetos (Figura 9.14(a)):

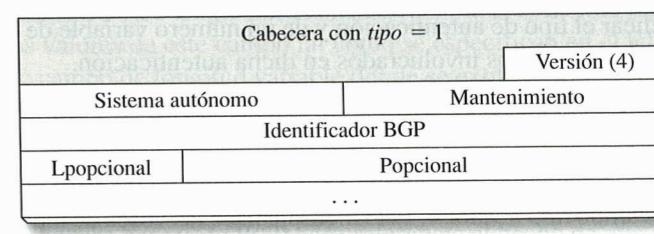
- *Marcador* (16 bytes): campo de autenticación que permite al destino verificar la identidad del emisor del mensaje.
- *Longitud* (2 bytes): indica el número de octetos que componen el mensaje BGP.
- *Tipo* (1 octeto): campo que indica el tipo de mensaje BGP de que se trata: 1 → *Apertura* (*Open*), 2 → *Actualización* (*Update*), 3 → *Notificación* (*Notification*) y 4 → *Accesibilidad* (*Keepalive*).

A continuación se comentan los cuatro tipos de mensajes BGP mencionados, según el orden seguido en su utilización:

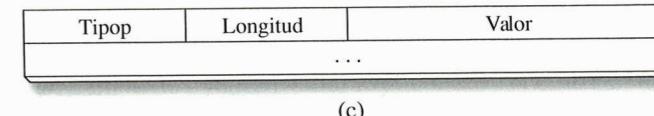
- *Apertura* (*Open*) (*tipo*=1). A través de este mensaje (Figura 9.14(b)) se solicita una relación de vecindad con un nodo frontera adyacente perteneciente a otro sistema autónomo. Con una longitud mínima de 29 octetos, en este mensaje se especifica:
 - a) Un campo de *versión* del protocolo BGP para la correcta interpretación de los campos que lo forman. La versión actual es la 4.



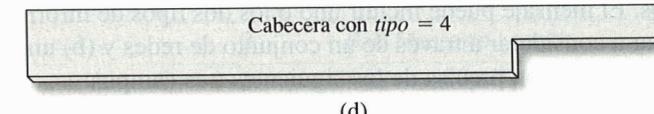
(a)



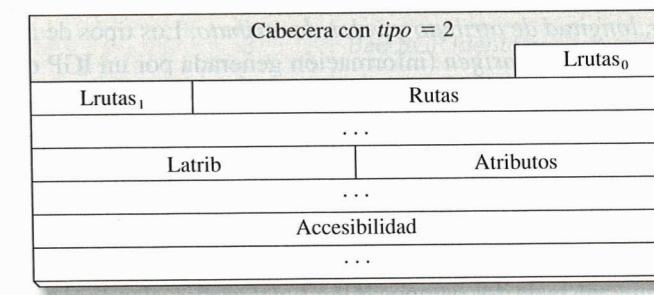
(b)



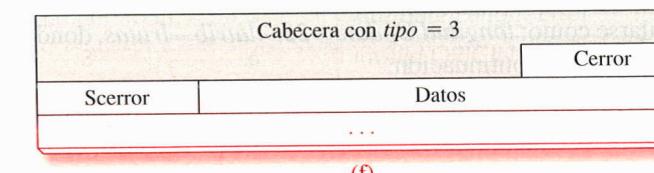
(c)



(d)



(e)



(f)

Figura 9.14. Cabecera BGP-4 (a) y mensajes Open (b), Keepalive (d), Update (e), y Notification (f). (c) corresponde al campo *popcional* en (b).

- b) El número de *sistema autónomo* del que forma parte el nodo emisor del mensaje.
- c) El tiempo de *mantenimiento*, referente al número máximo de segundos a considerar para el intercambio de mensajes de *Accesibilidad* y/o de *Actualización* entre vecinos.
- d) La dirección IP del nodo emisor (campo *identificador BGP*).
- e) Un campo de parámetros adicionales opcionales (*ipopcional*) cuya longitud se indica en el campo de 1 octeto de longitud *lpopcional* y cuyo formato es el que se especifica en la Figura 9.14(c).

Por el momento solo se considera un parámetro opcional (*tipop* = 1), el cual sirve para la autenticación del emisor y del receptor. El campo *valor* consta en este caso de 1 octeto para indicar el tipo de autenticación y de un número variable de bytes (*longitud-3*) correspondientes a los datos involucrados en dicha autenticación.

Si el nodo receptor de un mensaje *Open* acepta la relación de vecindad, deberá responder al emisor con un mensaje *Keepalive*.

- *Accesibilidad* (*Keepalive*). El mensaje *Keepalive* (Figura 9.14(d)) consiste solo en la cabecera BGP con el campo *tipo* a valor 4. Este mensaje hace las veces de mensaje *echo* y, como tal, sirve para testar la accesibilidad de los nodos vecinos. Si transcurre un tiempo igual al de mantenimiento especificado en el mensaje *Open* sin recibir un mensaje *Keepalive*, se concluye que el vecino identificado con anterioridad ha «muerto».

Además de para testar la accesibilidad, este mensaje BGP tipo 4 se utiliza como respuesta a un mensaje *Open*.

- *Actualización* (*Update*). A través de este mensaje BGP-4 tipo 2 (Figura 9.14(e)) se produce la actualización de las tablas de encaminamiento entre nodos pertenecientes a sistemas autónomos distintos. El mensaje puede incluir uno o los dos tipos de información siguientes: (a) una ruta particular a considerar a través de un conjunto de redes y (b) una lista de rutas a eliminar.

La primera situación precisa de los siguientes tres campos:

- a) *Latrib*: número de octetos de que consta el campo *atributos*.
- b) *Atributos*: lista de atributos aplicados a la ruta. Estos constan de 3 octetos: *tipo de atributo*, *longitud de atributo* y *valor de atributo*. Los tipos de atributos definidos son los siguientes: 1 → *origen* (información generada por un IGP o por BGP), 2 → *ruta_AS* (lista de sistemas autónomos atravesados por la ruta), 3 → *siguiente salto* (dirección IP del siguiente nodo frontera para alcanzar los destinos indicados), 4 → *multisalida* (indica varios puntos de salida hacia un sistema autónomo), 5 → *preferencia local* (indica una prioridad para una ruta interna al sistema autónomo), 6 → *agredado atómico* y 7 → *agregador* (utilizados para componer rutas con partes comunes).
- c) *Accesibilidad*: lista de direcciones IP correspondientes a los destinos alcanzables. Cada destino consta de dos campos: *longitud* y *prefijo*, siendo el primero un octeto para indicar la longitud del segundo.

Aunque el mensaje no la incluye, la longitud total del campo *accesibilidad* puede calcularse como: *longitud Update - 23 - latrib - lrutas*, donde el campo *lrutas* es como se especifica a continuación.

El segundo tipo de información que puede aparecer en un mensaje BGP *Update* es para la eliminación de rutas e involucra dos campos del paquete: *rutas*, de longitud variable y relativo a una lista de direcciones IP previamente anunciadas por este nodo y notificadas ahora para su borrado, y *lrutas*, de 2 octetos y cuyo fin es especificar la longitud del campo anteriormente mencionado. El formato del campo *rutas* es el mismo que el indicado anteriormente para el campo *accesibilidad*.

— *Notificación (Notification)*. Las posibles situaciones de error se indican con el mensaje BGP *Notification*. Como se muestra en la Figura 9.14(f), los campos que componen este mensaje, con campo *tipo* = 3 en la cabecera, son los siguientes:

- a) *Cerror*: campo de 1 octeto para indicar el tipo de error de que se trata. Los valores que este campo puede tomar son los siguientes: 1 → error en la cabecera del mensaje, 2 → error en el mensaje *Open*, 3 → error en el mensaje *Update*, 4 → expiración del tiempo de mantenimiento, 5 → error en la máquina de estados finitos correspondiente al procedimiento, 6 → cese.
- b) *Scerror*: campo de 1 byte para concretar aún más el tipo de error. En la Tabla 9.3 se indican los valores de este campo tal como se especifican en el RFC 1771.
- c) *Datos*: campo de longitud variable donde se explica la razón del error para su posible lectura por parte de un humano.

La longitud mínima del mensaje *Notificación*, incluida la cabecera, es de 21 octetos, caso en el cual se considera el campo *datos* de longitud nula.

Un último comentario acerca de BGP hace referencia al hecho de que estos mensajes no se encapsulan sobre datagramas IP, sino sobre segmentos TCP. En este sentido, BGP, como sucede con RIP y OSPF, es un protocolo propio de la capa de aplicación y no de la de red.

Tabla 9.3. Mensajes BGP de Notificación.

Campo <i>crror</i>	Campo <i>scrror</i>	Descripción
1	1	Connection Not Synchronized
	2	Bad Message Length
	3	Bad Message Type
2	1	Unsupported Version Number
	2	Bad Peer AS
	3	Bad BGP Identifier
	4	Unsupported Optional Parameter
	5	Authentication Failure
	6	Unacceptable Hold Time
3	1	Malformed Attribute List
	2	Unrecognized Well-known Attribute
	3	Missing Well-known Attribute
	4	Attribute Flags Error
	5	Attribute Length Error
	6	Invalid ORIGIN Attribute
	7	AS Routing Loop
	8	Invalid NEXT_HOP Attribute
	9	Optional Attribute Error
	10	Invalid Network Field
	11	Malformed AS_PATH

9.4. Encaminamiento multidestino en Internet

Un aspecto relevante a considerar en Internet, especialmente con la adopción de nuevos servicios del tipo multi-conferencia o video *streaming*, es el de las transmisiones multidestino o *multicast*. Es decir, envíos generados por un único origen pero simultáneamente destinados a varios receptores. Como ya se comentó en el Apartado 6.3.4, es patente la conveniencia de abordar la provisión de este tipo de servicios con comunicaciones distintas a las *unicast*. A modo de ejemplo sencillo, en la Figura 9.15 se muestra una situación en la que un emisor envía datos correspondientes a un mismo servicio a 3 destinos. Es evidente que, si bien es posible hacerlo, una transmisión *unicast* implicaría multiplicar innecesariamente el volumen de recursos (ancho de banda y *buffer* en los routers) involucrados en la provisión del servicio. El carácter «innecesario» viene derivado del hecho de que, como se observa en la figura, parte de los paquetes pueden ser «agrupados» para optimizar el uso de los recursos. Ello se consigue transmitiendo un solo paquete *multicast* en la parte de la ruta que sea común desde el origen a los posibles destinos y replicando el paquete desde el nodo a partir del cual las rutas a los posibles destinos diverjan.

Sobre este tipo de transmisiones son tres los aspectos principales a analizar. Por una parte, y frente al empleo ya conocido de direcciones IP *unicast*, cómo se puede identificar únicamente un grupo de destinos. Por otro lado, cómo se gestiona la creación y el mantenimiento de los grupos *multicast*, esto es, cómo se dan de alta y de baja puntos finales (destinos) de un cierto grupo. Por último, pero no menos importante, cómo se establecen las rutas *multicast* hacia los diferentes destinos.

Cada una de estas cuestiones se desarrolla en los siguientes apartados.

9.4.1. Direccionamiento IP *multicast*

La transmisión multidestino en IP es el equivalente en Internet del *multicast* y difusión hardware en las redes LAN (véase Apartado 5.2.2). En este sentido, la transmisión que da nombre al presente apartado permite el envío de datagramas IP a un conjunto más o menos amplio de *hosts* que constituyen un grupo; grupo que puede estar compuesto por miembros pertenecientes a redes físicas distintas. Como se estudió en el Apartado 8.4, las direcciones Clase D se utilizan para transmisiones multidestino IP

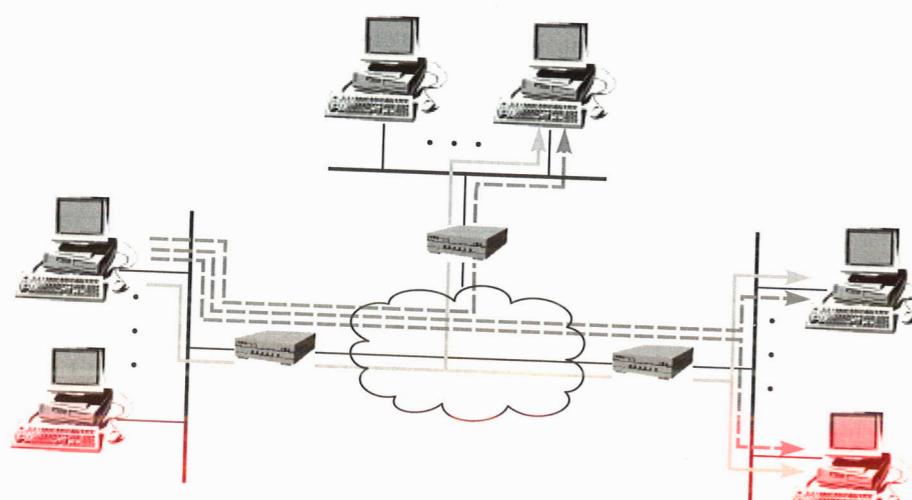


Figura 9.15. Ejemplo de transmisiones *multicast* (línea continua) frente a *unicast* (línea discontinua)

0	1	2	3	4	Identificador de grupo
1	1	1	0		

Figura 9.16. Direcciones IP Clase D multidestino.

(Figura 9.16), únicamente como direcciones destino y nunca como origen. El rango, por tanto, para estas direcciones es desde 224.0.0.0 a 239.255.255.255.

Es claro que, como se vio en el Capítulo 8 anterior, debe existir una correspondencia entre las direcciones IP multidestino y las direcciones hardware subyacentes, las cuales serán en este caso también multidestino. La conversión de direcciones multidestino IP a direcciones multidestino Ethernet se establece de la siguiente forma: *sustituir los correspondientes 23 bits menos significativos de la dirección multidestino Ethernet 01:00:5E:00:00:00 por los 23 bits menos significativos de la dirección IP*. Así, la dirección multidestino IP 224.10.8.21 se corresponderá con la dirección Ethernet multidestino 01:00:5E:10:08:21. Según se deduce de lo establecido, la no consideración de los 5 bits de dirección multidestino IP de posiciones 4 a 8 hace que la correspondencia entre ambos espacios de direcciones no sea única; es decir, varios grupos *multicast* IP pueden tener la misma dirección *multicast* Ethernet. Así por ejemplo, los grupos IP 224.10.8.21, 233.10.8.21 y 224.138.8.21 se corresponden con el mismo grupo Ethernet 01:00:5E:10:08:21. De todo ello se concluye que el software IP de una estación final debe filtrar la información recibida a fin de rechazar aquellos datagramas no solicitados.

Una vez aclarado el formato para las direcciones IP *multicast* y cómo estas se asocian a direcciones *multicast* físicas, una cuestión importante adicional es cómo se lleva a cabo la asignación de una dirección IP *multicast* dada a un conjunto de usuarios o grupo. En este punto, sin embargo, hay que matizar que una dirección *multicast* lo que realmente identifica es una fuente de datos, de manera que los destinatarios interesados en recibir estos deben indicarlo explícitamente (esto es, suscribirse al grupo) a sus respectivos nodos de acceso para que procedan a realizar el encaminamiento de la información correspondiente.

Aclarado ello, la asignación de una dirección *multicast* a una fuente dada se puede realizar de tres formas posibles:

- *Asignación estática*. El IANA («Internet Assigned Numbers Authority») tiene reservadas distintas direcciones IP *multicast* (<http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml>). Así, las direcciones 224.0.0.1 y 224.0.0.2 significan, respectivamente, envío a todos los *hosts* y a todos los nodos de una red; mientras que 224.0.0.9 significa «todos los routers RIP-2».
- *Relativa a dominio*. En el RFC 2365 se describe que el rango de direcciones 239.0.0.0 a 239.255.255.255 se asigna localmente a nivel de dominio, de manera que estas direcciones no pueden ser utilizadas entre dominios separados.
- *Asignación dinámica*. Para permitir un uso adecuado y flexible, dinámico según necesidad, del espacio de direcciones *multicast*, existen procedimientos automáticos de asignación bajo demanda. Estos se fundamentan en la arquitectura MALLOC («Multicast Address ALLOCation architecture») especificada en el RFC 2908 (actualizado a su vez por el RFC 6308).

Como se indica en la Figura 9.17, en la arquitectura MALLOC se definen dos niveles de actuación: inter-dominio e intra-dominio. El primero permite la asignación de rangos de direcciones para cada dominio, mientras que el segundo se refiere a una coordinación intra-domínio para la asignación final de direcciones *multicast*. Asimismo, para possibilitar una mayor escalabilidad de la solución se definen clientes y servidores de asignación. Los primeros solicitan una

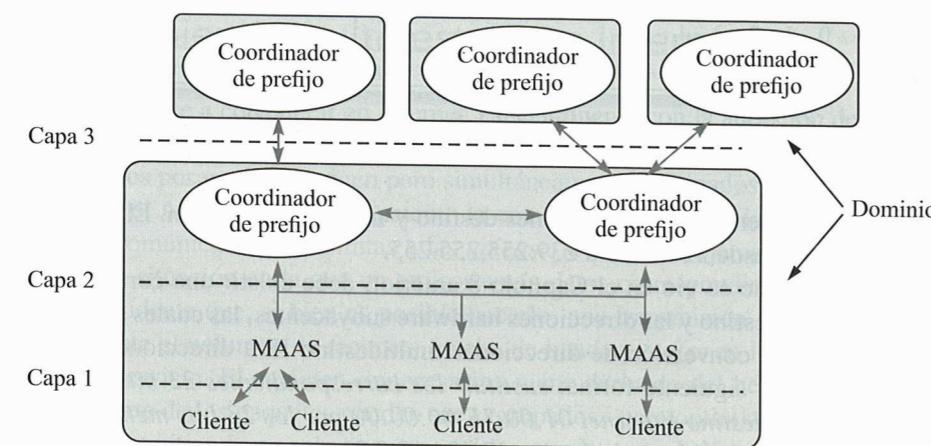


Figura 9.17. Arquitectura MALLOC.

dirección *multicast* como usuarios y los segundos, denominados MAAS («Multicast Address Allocation Server»), asignan y gestionan estas.

Si bien son varios los protocolos existentes para llevar a cabo la asignación y gestión dinámica de direcciones *multicast*, dos de los más usados son MASC, tanto para inter-dominio como para coordinación intra-dominio, y MADCAP, para las interacciones cliente-MAAS.

Protocolo de asignación de direcciones *multicast* MASC

El protocolo MASC («Multicast Address-Set Claim protocol»), definido en el RFC 2909, está pensado tanto para relaciones intra-dominio como inter-dominio. Así, un nodo puede realizar las siguientes funciones y relaciones respecto de otro remoto (Figura 9.18):

- *Paritario intra-dominio*, como los nodos P4a y P4b en la Figura 9.18, diciéndose *P4a internal_peer P4b*.
- *Hijo*, como el caso del nodo C6a respecto del P4a en la Figura 9.18. En este caso se designan *C6a child P4a*.
- *Padre*, como el nodo T2a respecto del P4a en la Figura 9.18. En este caso se dice *T2a parent P4a*.

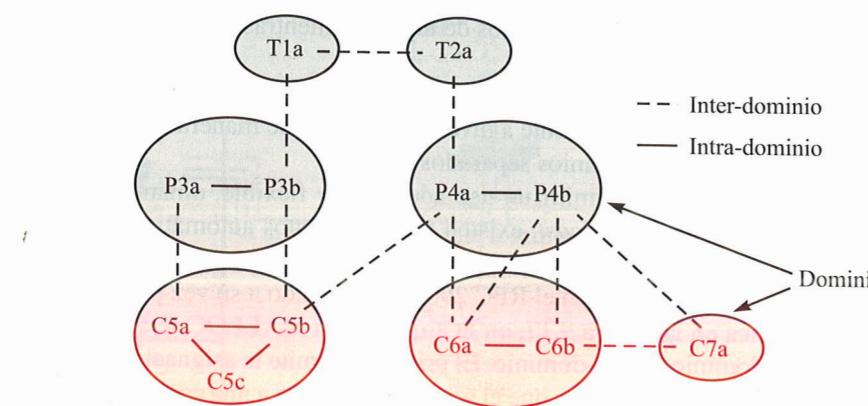


Figura 9.18. Ejemplo de topología jerárquica considerada en MASC.

- *Hermano o paritario inter-domino*, como T1a respecto de T2a en la Figura 9.18. En este caso se dice *T1a sibling T2a*.

A partir de lo anterior, los mensajes generados por un nodo dado se propagan hacia su padre, sus hermanos con el mismo parent y sus hijos. Los mensajes MASC están precedidos por la cabecera cuyo formato se indica en la Figura 9.19(a). De los campos que la componen es de destacar el campo *tipo*, a través del cual se indica el tipo concreto de mensaje MASC de que se trata⁵:

— *Open (tipo=0)*. Primer mensaje intercambiado para establecer una conexión TCP entre los nodos. De entre los campos que componen este mensaje (Figura 9.19(b)), son de destacar dos:

- *Rol*: papel del nodo emisor respecto del remoto (00→*internal_peer*; 01→*child*; 10→*sibling*; 11→*parent*).
- *Tiempo*: tiempo de intercambio de mensajes *Keepalive* para testar la accesibilidad (aproximadamente 4 minutos).

0	16	24	31		
Longitud					
Tipo					
Reservado					
(a)					
0	8	9	14	16	31
Longitud	0	Familia	Rol	Tiempo	
Identificador del dominio del emisor...					
Identificador del nodo MASC emisor...					
Identificador del dominio del parent...					
Parámetros opcionales...					
(b)					
0	16	24	31		
Longitud					
Tipo					
Reservado					
Reservado1	D	Familia	Rol	Reservado2	
Sello del tiempo de la solicitud					
Tiempo de vida de la solicitud					
Tiempo de tenencia (en <i>cache</i>) de la solicitud					
Identificador de dominio origen...					
Identificador de nodo origen...					
Dirección asociada al prefijo...					
Máscara...					
Parámetros opcionales...					
(c)					
0	1	8	16	31	
Código		Subcódigo	Datos		
(d)					

Figura 9.19. Cabecera de los mensajes MASC (a) y mensajes Open (b), Update (c) y Notification (d).

⁵ Notense las similitudes evidentes existentes con el protocolo BGP-4.

Tipo	Tiempo	Comprobación	31
Grupo			

Figura 9.21. Mensaje IGMP versión 2.

De modo análogo a ICMP, IGMP es parte integrante de la capa de red IP y se encapsula sobre dicho protocolo (campo *protocolo* del datagrama IP a valor 2). Especificado en su versión 2 en el RFC 2236 (versión 1 en RFC 1112 y versión 3 en RFC 3376), los mensajes IGMPv2 tienen el formato mostrado en la Figura 9.21. El significado de los distintos campos es el siguiente:

- *Tipo*: campo de 8 bits para especificar el tipo de mensaje IGMP de que se trata. Existen los siguientes cuatro tipos:
 - a) *Consulta de pertenencia a grupo* («Membership Query» o simplemente «Query»): con valor 11 en hexadecimal, existen dos subtipos de este mensaje diferenciados por el campo de 32 bits *grupo* (ver más adelante). El primero, llamado «General Query», sirve para preguntar acerca de la existencia de hosts en cualquiera de los grupos establecidos. El segundo subtipo, «Group-Specific Query», se utiliza para consultar sobre la existencia de hosts en un grupo *multicast* concreto.
 - b) *Informe de pertenencia* («Membership Report» o «Report»): mensaje de tipo 16 en hexadecimal, utilizado como respuesta a una consulta a través de «Query».
 - c) *Abandono de grupo* («Leave Group»): mensaje enviado por un host cuando abandona un grupo al que pertenecía. El valor hexadecimal del campo *tipo* para este mensaje es 17.
 - d) *Informe de pertenencia v1*: mensaje de *tipo* 12 en hexadecimal utilizado para compatibilidad con la versión 1 de IGMP.
- *Tiempo*: unidades de tiempo, en décimas de segundo, que expresan el intervalo máximo permitido para el envío de mensajes «Report». Este campo estará a valor 0 para todos los mensajes distintos de «Query», no considerándose por el receptor o receptores del paquete.
- *Comprobación*: campo de suma de comprobación del mensaje IGMP completo.
- *Grupo*: campo de 32 bits donde se indica la dirección del grupo multidestino IP. Este campo es el que diferencia los dos subtipos de mensajes «Query» existentes comentados anteriormente, siendo su valor 0 en el caso «General Query» y especificándose el grupo en cuestión para los mensajes «Group-Specific Query».

El procedimiento seguido por IGMP se basa en las siguientes tres premisas de funcionamiento:

1. Un nodo IGMP puede actuar o no como «consultante», o *querier* (es decir, emite mensajes «Query»).
2. Por defecto, debe existir un nodo «consultante» por cada red física, por lo que el estado natural de un nodo IGMP es el de «consultante».
3. Esto último es así a menos que el *router* IGMP detecte la existencia de otro «consultante» con menor dirección IP en la misma red, en cuyo caso pasa al estado de «no consultante» para dicha red.

A partir de estas premisas, el procedimiento IGMP seguido es el siguiente:

1. Cada nodo «consultante» debe transmitir periódicamente un mensaje «General Query» a cada una de las redes físicas a las que se encuentra conectado y de las que es «consultante».

2. Cuando un host interesado en un grupo recibe una consulta, establece un tiempo aleatorio de respuesta comprendido entre 0 y el valor especificado en el campo *tiempo* del «Query». De esta forma, cada vez que expira el temporizador asociado al contador, lleva a cabo la transmisión de un mensaje «Report» sobre la interfaz por donde ha recibido la consulta. Este informe se emite siempre y cuando no se detecte que otro host del grupo lo ha generado con anterioridad. En tal caso se reiniciará el contador.
3. Cada vez que un nodo recibe un informe relativo a un grupo dado por parte de un host, refresca un contador de vida asociado a dicho grupo. Por el contrario, si transcurrido un tiempo máximo no se recibe informe alguno acerca de un grupo dado, este se supondrá vacío y se eliminará, no transmiéndose con posterioridad mensajes «Query» referentes a dicho grupo.
4. Cuando un host se incorpora a un grupo, deberá emitir un mensaje «Group-Specific Report» para informar de este hecho si es el primero de la red en incorporarse a dicho grupo. Para evitar el potencial problema de que se pierda el mensaje, el host lo retransmitirá de forma espaciada una o dos veces.
5. Por su parte, cuando un host abandona un grupo emitirá un mensaje «Leave Group» hacia todos los nodos mediante la dirección 224.0.0.2. Esto es obligatorio si el host en cuestión fue el último de la red en responder a un «Query» para el grupo en cuestión.
6. Cuando un nodo «consultante» recibe un mensaje «Leave Group», emite un mensaje «Group-Specific Query» para ese grupo. Si no recibe respuesta dentro de un intervalo de tiempo dado actuará como se ha indicado en 3.

A partir del procedimiento descrito, en la Figura 9.22 se muestra el diagrama de estados de los nodos IGMP, tanto en su estado «consultante» como «no consultante», especificado en los RFC.

9.4.3. Algoritmos de encaminamiento multicast en Internet

Como hemos indicado al comienzo del subapartado anterior, IGMP no se implementa en los nodos intermedios de la red. Entonces, ¿cómo saben estos redireccionar adecuadamente la información correspondiente al servicio proporcionado hacia los routers finales, a los que se encuentran ligados los destinatarios que componen cada uno de los grupos *multicast* en un momento dado? La respuesta a esta cuestión viene de la mano de diversos protocolos de encaminamiento desarrollados específicamente para transmisiones *multicast*. Entre ellos cabe señalar DVMRP («Distance-Vector Multicast Routing Protocol», RFC 1075) y MOSPF («Multicast OSPF», RFC 1584), extensiones *multicast* de RIP y OSPF, respectivamente.

El principal inconveniente, sin embargo, de ambos protocolos es que son dependientes del esquema de encaminamiento usado en *unicast*. Así, si utilizamos DVMRP para *multicast*, debemos usar RIP para transmisiones *unicast*. Lo mismo sucede con MOSPF respecto de OSPF. Frente a ellos, el protocolo PIM («Protocol Independent Multicast») fue definido para evitar este tipo de dependencias, de manera que el protocolo a considerar a nivel *unicast* puede ser cualquiera de los disponibles. Seguidamente se describe PIM.

Protocolo PIM

El protocolo PIM tiene dos modos de funcionamiento: denso y disperso, los cuales hacen referencia a la cantidad (alta o baja) de grupos *multicast* existentes en el entorno de red. El primero de ellos, PIM-DM («PIM-Dense Mode»; RFC 3973), es el más simple de los dos, aunque resulta también menos escalable. Su operación básica es simple:

- Cuando un paquete *multicast* se recibe en un *router PIM* este lo difunde mediante inundaciones, evitándose la aparición de bucles usando la técnica *RPF*, ya vista en el Apartado 6.3.4.

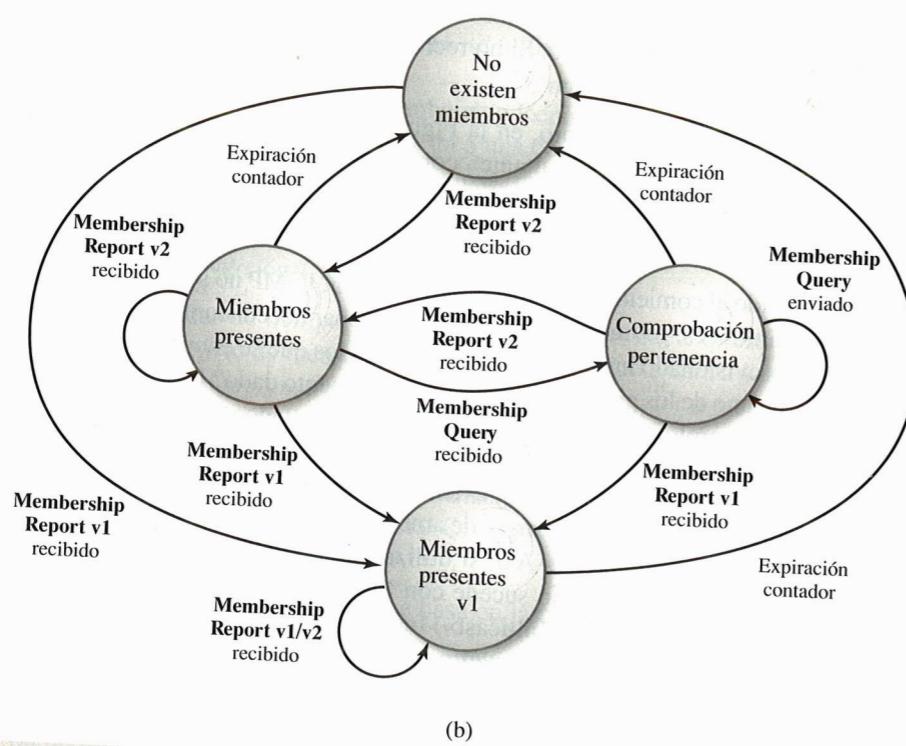
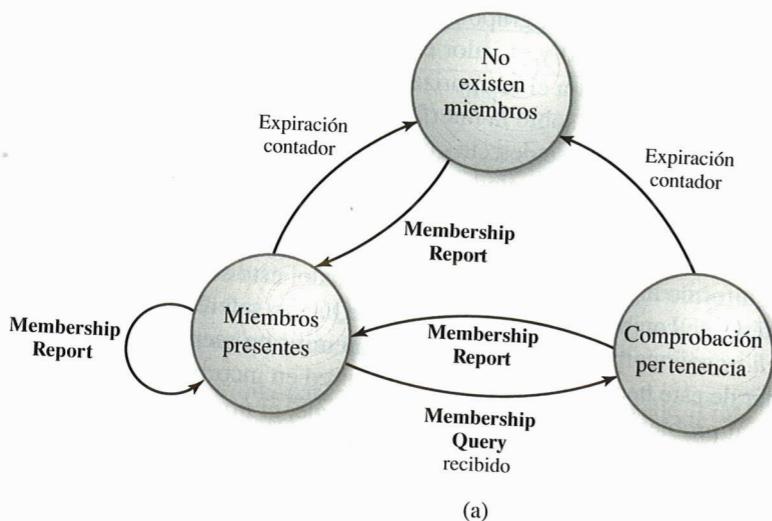


Figura 9.22. Diagrama de estados de los nodos IGMP en su función como «no consultante» (a) y como «consultante» (b).

- Implementando el algoritmo IGMP en los nodos terminales, estos pueden enviar hacia sus nodos «padre» mensajes de *poda* («prune» en inglés) en caso de no disponer de *hosts* usuarios por la red se construye tomando como punto raíz el origen o fuente de la información.

Estos mensajes pueden propagarse a su vez hacia arriba en el árbol para evitar transmisiones innecesarias. Es decir, si «debajo» de un cierto nodo no existe ningún otro con miembros de un grupo dado, aquel puede evitar la retransmisión de la información correspondiente (véase Figura 6.13).

- Una vez podada una rama del árbol, esta se puede restablecer con posterioridad si apareciesen nuevos miembros del grupo. Ello se lleva a cabo mediante mensajes de *injerto* («graft» en inglés).

Como hemos indicado anteriormente, el protocolo PIM en su versión dispersa, PIM-SM («PIM-Sparse Mode») es más complejo que la versión densa. Definido originalmente en el RFC 2362 y actualizado a través del RFC 4601, la arquitectura funcional se muestra en la Figura 9.23. De ella hay que destacar la existencia de los siguientes elementos:

- Dominios PIM, esto es, entornos donde se implementa PIM.
- Dominios no PIM.
- Routers frontera multicast o MBR («Multicast Border Router»), los cuales permiten la interconexión de los tipos de dominios anteriores y, en suma, el encaminamiento *multicast*.
- Routers PIM designados (RD), puntos *rendezvous* (RP) y nodos *bootstrap*, involucrados en el desarrollo del encaminamiento *multicast* como se explica a continuación.

La transmisión en PIM-SM es como sigue (véase Figura 9.24):

- Para que un *router* reciba datos *multicast* debe indicarlo explícitamente a sus vecinos hacia arriba en el árbol. Para ello, los nodos intercambian mensajes PIM de *incorporación* («join») y *poda* («prune»). Estos, de modo análogo a como sucede en PIM-DM, se sustentan en el empleo de IGMP en los nodos hoja o finales.
- PIM-SM hace uso de árboles compartidos, pero tomando como punto raíz un nodo denominado *rendezvous* (RP) en lugar del origen de los datos como sucede en PIM-DM. Así, el RP es el encargado de hacer las transmisiones *multicast* hacia todos los receptores del correspondiente grupo dentro del dominio.

La existencia de los routers RP es anunciada a través de nodos especiales llamados *bootstrap*.

- Para enviar al RP, el origen u orígenes de la información encapsulan los datos en mensajes de control PIM y se envían en modo *unicast* al RP desde el nodo designado (RD) de la red local del origen.

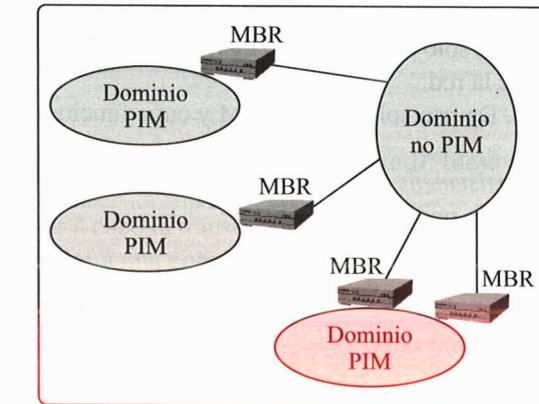


Figura 9.23. Arquitectura PIM-SM.

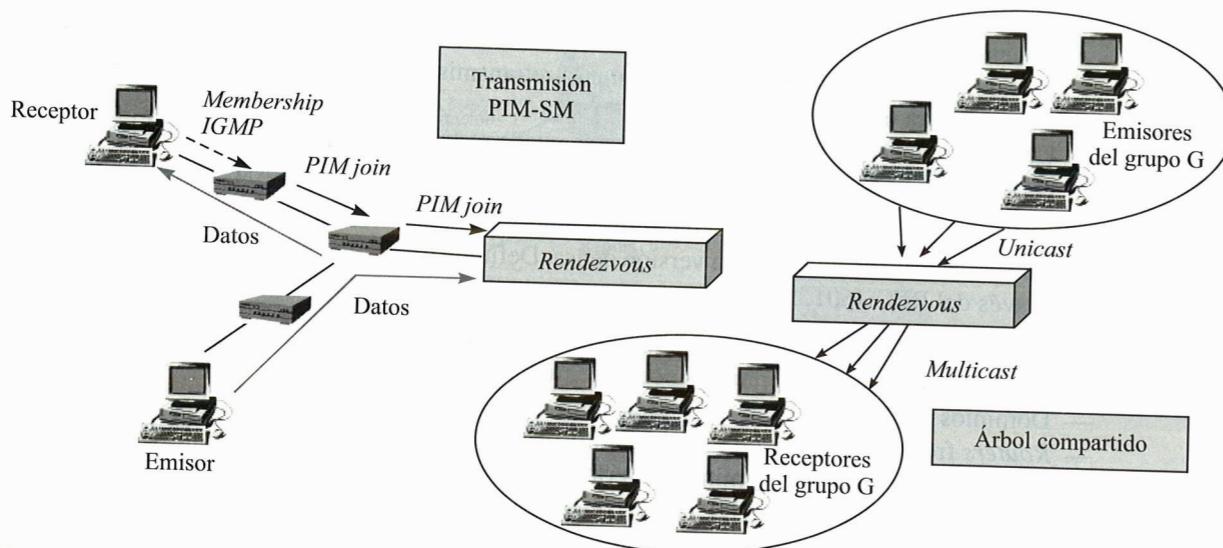


Figura 9.24. Funcionamiento operacional de PIM-SM.

El formato concreto de los mensajes PIM-SM es el indicado en la Figura 9.25, correspondiendo los campos sombreados a la cabecera. El más relevante de ellos desde el punto de vista de la funcionalidad pretendida es el campo *tipo*, el cual indica el tipo de mensaje PIM de que se trata. Los tipos disponibles en la versión 2 actual del protocolo son:

- *Hello* (*tipo*=0). Mensaje enviado periódicamente entre *routers* vecinos. El de dirección IP superior será el nodo designado o RD.
- *Register* (*tipo*=1). Mensaje sobre el que se encapsulan los datos enviados hacia los receptores de un grupo dado, y que se envía desde los RD al RP.
- *Register-Stop* (*tipo*=2). Contestación al mensaje anterior desde el RP para el control de flujo.
- *Join/Prune* (*tipo*=3). Incorporación/poda de nodos en el árbol de transmisión de la red.
- *Bootstrap* (*tipo*=4). Mensajes enviados mediante *multicast* al grupo ALL-PIM-ROUTERS (224.0.0.13) con información acerca del RP.
- *Assert* (*tipo*=5). Enviado a la dirección 224.0.0.13 para resolver la designación de RD.
- *Graft* (*tipo*=6). De uso solo en PIM-DM y cuya funcionalidad es el injerto de ramas en el árbol de transmisión sobre la red.
- *Graft-Ack* (*tipo*=7). De uso solo en PIM-DM y cuya funcionalidad es servir de confirmación al mensaje anterior.
- *Candidate-RP-Advertisement* (*tipo*=8). Mensaje enviado (*unicast*) periódicamente desde los RP candidatos hacia los nodos *bootstrap*.

0	5	8	16	31
Versión	Tipo	Reservado	Complicación	Mensaje...

Figura 9.25. Formato de mensaje PIM-SM.

Concluimos este apartado citando sin más la existencia de una tercera variante de PIM: PIM bidireccional (BIDIR-PIM), así como la disposición de algunos otros protocolos alternativos para llevar a cabo el encaminamiento *multicast* en Internet, como son MSDP («Multicast Source Discovery Protocol») y CBT («Core-Based Trees»). También es de mencionar el BGMP («Border Gateway Multicast Protocol») como protocolo *multicast* de tipo exterior, extensión de BGP.

RESUMEN

En este capítulo se ha abordado el estudio de las funciones propias de la capa de red en Internet. Como núcleo de la misma y soporte principal del resto de protocolos y servicios Internet se ha presentado el protocolo IP, el cual se caracteriza por ofrecer un servicio de transmisión datagrama no orientado a conexión y no fiable. A partir del formato del datagrama se ha comentado la capacidad de fragmentación y especificación de opciones IP.

Ante algunas evidentes limitaciones de la versión más conocida y usada de IP, IPv4, se ha discutido también su versión 6, IPv6. De ella se han destacado el direccionamiento extendido y las cabeceras de extensión, entre otros aspectos relevantes.

A pesar de la naturaleza de mejor esfuerzo demostrada por IP, se hace necesaria la implementación de procedimientos que permitan un cierto nivel de control de la subred para monitorizar el funcionamiento global de esta. Se ha introducido así el protocolo ICMP, el cual, encapsulado sobre IP, establece varios mensajes de control con los que se gestionan determinadas circunstancias que pueden presentarse en la transmisión de los datagramas. Como extensión al uso de IPv6, también se ha presentado la versión 6 de ICMP, ICMPv6.

Una cuestión de suma importancia en toda red se refiere al encaminamiento y actualización de las tablas por parte de los nodos intermedios. Presentado el concepto de sistema autónomo y el carácter distribuido jerárquico de los protocolos de encaminamiento en Internet, en el Apartado 9.3 se estudian tanto protocolos interiores, en particular RIP, OSPF y los propietarios de Cisco IGRP y EIGRP, como protocolos exteriores, en concreto BGP.

Para concluir el capítulo se han discutido las transmisiones *multicast* en Internet. Tres han sido las cuestiones a este respecto tratadas: gestión de direcciones *multicast*, gestión de grupos *multicast* y encaminamiento *multicast* sobre la subred. En lo concerniente a la primera se ha estudiado la arquitectura MALLOC, y los protocolos IGMP y PIM al respecto de la segunda y tercera cuestiones, respectivamente.

EJERCICIOS

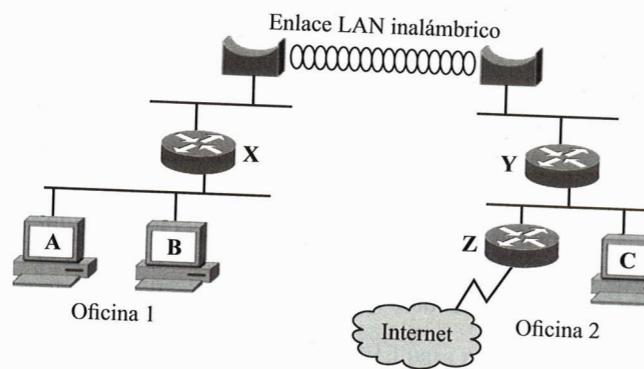
1. ¿Tendría sentido que el primer campo del paquete IP fuese otro distinto del de *versión*? Razone la respuesta.
2. Un nodo debe llevar a cabo la transmisión de un datagrama *N*, con un *payload* de longitud 1.500 bytes, correspondiente a una comunicación IP dada sobre una red de transporte con MTU igual a 1.200 octetos. Ante esta situación, ¿qué campos de la cabecera IP de los fragmentos será necesario modificar?
3. Un dispositivo de encaminamiento recibe un paquete que debe retransmitir sobre una red con MTU igual a 640 octetos. Si el paquete tiene una cabecera IP mínima y un campo de datos de 1.960 bytes, realice la fragmentación e indique los valores de los campos de la cabecera IP del paquete original y de cada fragmento según la siguiente tabla:

Paquete	Longitud cabecera	Longitud total	Protocolo	ID	MF	Offset
Original						
Fragmento 1						
...						

4. En el ejercicio anterior, ¿qué sucedería si el bit *DF* del paquete original estuviese especificado a valor 0?
5. Una empresa tiene dos oficinas (1 y 2) conectadas mediante un enlace LAN inalámbrico, como se ilustra en la figura inferior. Suponga que la empresa contrata una línea dedicada con un proveedor de Internet, el cual le ha asignado al *router* de acceso Z la dirección IP 192.169.15.6, con máscara de red de 30 bits. Suponga también que la empresa obtiene de su proveedor una dirección pública de red 150.214.60.0.

Utilizando las direcciones arriba mencionadas:

- Realice una asignación de las direcciones IP para los distintos equipos.
- Indique todas las tablas de encaminamiento.
- Indique qué haría si apareciera un nuevo grupo de ordenadores (D) en la oficina 1 con 70 nuevos usuarios.



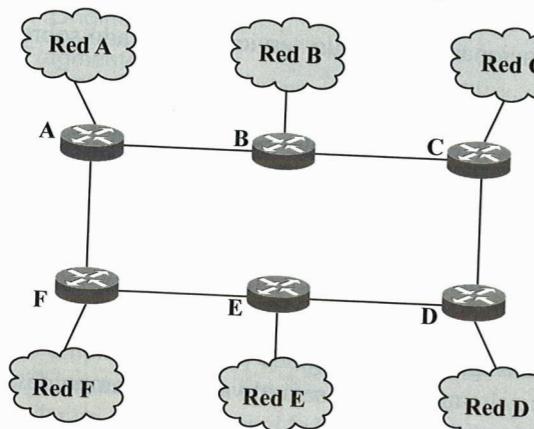
6. Se desea desplegar una red corporativa con acceso a Internet con las siguientes características básicas:
- Dos departamentos, cada uno con 5 equipos de trabajo, 1 servidor de ficheros y 1 impresora en red. Uno de los departamentos se encuentra ubicado en un edificio A y el otro en un edificio B separado 50 metros del primero.
 - Zona de servidores públicos: HTTP y DNS.
 - Aunque se usarán preferentemente direcciones privadas, también se dispone del rango de direcciones públicas 199.199.199.8/29 para la DMZ.
 - El *router* de acceso a Internet solo debe contener 4 entradas totales en su tabla de routing.
 - Proponga y dibuje una topología completa para la red pretendida.
 - Lleve a cabo una asignación de direcciones IP y máscaras asociadas.
 - Indique la tabla de encaminamiento del *router* de acceso a Internet.

7. La dirección IPv6 1080:0000:0000:002c:0000:0000:0000:417a ¿de qué tipo es, *unicast* o *multicast*? Especifíquela en formato abreviado.
8. Indique la dirección IPv4 10.214.23.3 en formato IPv6.
9. Ponga un ejemplo y explique el funcionamiento de un servicio sustentado sobre transmisiones *anycast*.
10. Frente a IPv4, en IPv6 es el emisor, y no los nodos intermedios, el encargado de fragmentar los paquetes IP. ¿Qué implicaciones tiene desde el punto de vista del origen? ¿Qué ventajas y desventajas presenta esta alternativa frente a la tradicional?
11. Supongamos que, de modo análogo al enunciado del Ejercicio 3, se dispone de 1.960 bytes de datos que transmitir sobre una topología de red con MTU mínima de 640 bytes. Responda a las siguientes cuestiones sobre el proceso de fragmentación si consideramos el uso del protocolo IPv6:
- Describa el proceso general de fragmentación seguido por el emisor.
 - ¿Cuántos datagramas IPv6 se generarán y cuál será el valor del campo *desplazamiento* de las cabeceras de extensión correspondientes?
 - ¿Cuál es el formato general de cada uno de los fragmentos desde el punto de vista de las cabeceras existentes?
12. La mayoría de los mensajes ICMP (p.e., *destino inalcanzable*, *tiempo excedido* y *problema de parámetros*) incluyen en el campo *datos*: «cabecera IP más los primeros 64 bits del campo *datos* del datagrama original». ¿Cuál es el objetivo de esta información?
13. El mensaje ICMP «*source quench*» se envía desde un *router* hacia el origen del paquete que motiva el mensaje. ¿Tendría sentido que estos mensajes fuesen destinados a un *router* o *routers* vecinos? Justifique la respuesta.
14. Suponga que un *host* dado envía un paquete IP sobre un cierto *router* hacia el destino pretendido. Si con posterioridad el *host* recibiese un mensaje ICMP de *tipo* = 5 y *código* = 0, ¿qué ocurriría?
15. Pruebe en su red de trabajo el comando *ping* y explique el resultado obtenido en relación a los mensajes ICMP involucrados. Repita el proceso con el comando *traceroute*.
16. El protocolo de encaminamiento RIP es susceptible de presentar el problema conocido como *cuenta al infinito*. ¿Es esta situación generalizable a otros protocolos IGP como, por ejemplo, OSPF? Justifique la respuesta.
17. Suponga que al *router* X en la red del Ejercicio 5 se le instala una tercera interfaz a una nueva red de dirección 150.214.70.0. Suponga también que el administrador opta por instalar el protocolo RIP en todos los equipos. Explique el funcionamiento de este protocolo de encaminamiento dinámico, identificando cada uno de los paquetes que aparecerían para llevar a cabo la actualización de las tablas de encaminamiento. (Nota: Haga las suposiciones que estime necesarias)

	ETH. ORIG.	ETH. DEST.	IP ORIG.	IP DEST.	DESCRIPCIÓN
1					
2					
3					
...					

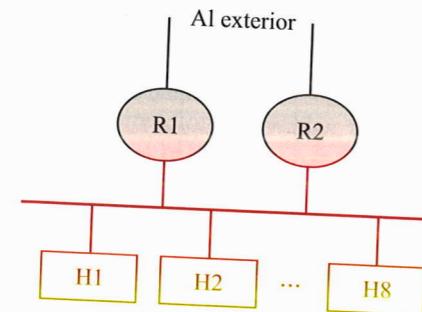
18. Los *routers* de la figura adjunta tienen definidas las rutas a las redes que tienen conectadas directamente. El administrador de la red decide utilizar en dichos *routers* el protocolo RIP (en las

interfaces hacia otros routers) y activa dicho servicio siguiendo la secuencia temporal indicada a la derecha de la figura (en segundos).

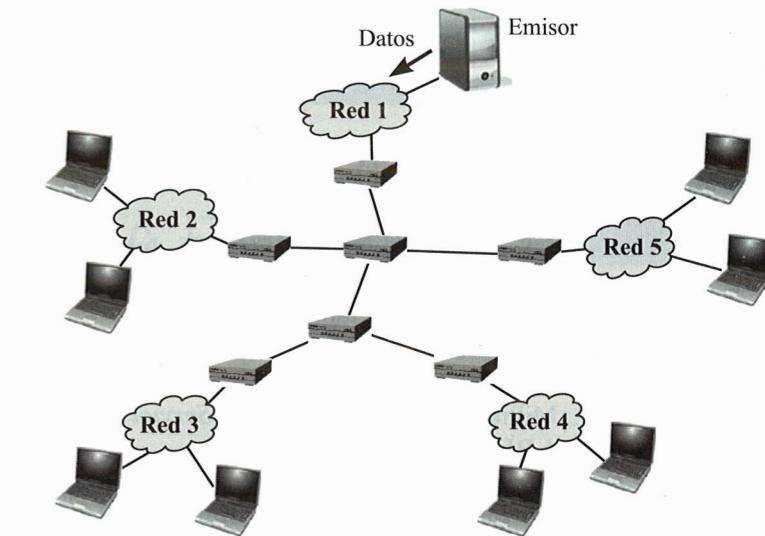


- $t = t_0$ → Activación RIP en router A
- $t = t_0 + 5$ → Activación RIP en router B
- $t = t_0 + 10$ → Activación RIP en router C
- $t = t_0 + 15$ → Activación RIP en router D
- $t = t_0 + 20$ → Activación RIP en router E
- $t = t_0 + 25$ → Activación RIP en router F

- a) Explique el funcionamiento del protocolo de encaminamiento dinámico RIP mediante la descripción de los mensajes intercambiados entre los routers (indique origen/destino del mensaje, redes conocidas por el receptor tras recibir el mensaje, coste para alcanzar cada red y cuál es el primer router en la ruta hacia dicha red) hasta que las rutas se mantienen estable.
- Suponga que solo se utilizan actualizaciones periódicas y que el primer mensaje periódico enviado por cada router es a los 30 segundos de haber arrancado el servicio RIP. Incluya en la descripción solo la accesibilidad a las redes A, B, C, D, E y F.
- b) ¿Cuál es el tiempo total transcurrido hasta que la situación de toda la red se ha estabilizado (desde el instante t_0)?
19. A través del campo TTL del datagrama IP se especifica el tiempo de vida máximo permitido para el paquete; sin embargo, dicho campo se suele especificar a valor 1 en transmisiones multicast. Justifique razonadamente el motivo de este hecho.
20. En relación al protocolo IGMP:
- Identifique y explique todos los contadores necesarios en un router «consultante».
 - Identifique y explique todos los contadores en un host miembro de 2 grupos multicast distintos.
21. Disponemos de una red con la topología indicada en la figura adjunta y en la que tanto los hosts como los nodos R1 y R2 implementan el protocolo IGMP. Supuesta la existencia de los grupos multicast 224.135.22.4 y 224.7.22.4 por parte de R1 y R2,



- a) ¿Qué dispositivo/s emitiría/n el mensaje MQ «¿quién quiere formar parte de un grupo multicast?»? ¿Sería este mensaje de tipo GMQ o SGMQ?
- b) Los hosts H1, H3 y H5 están interesados en formar parte del grupo 224.135.22.4, mientras que solo el host H7 quiere pertenecer a 224.7.22.4. Indique los mensajes MR enviados en respuesta al MQ de a), contemplando los temporizadores involucrados.
- c) ¿Cómo abandonaría el host H3 el grupo al que está suscrito?
22. Suponga la infraestructura de red inferior, donde se dispone de un emisor multicast y se implementan los algoritmos PIM-DM e IGMP. Explique los mensajes intercambiados y el árbol de transmisión en las siguientes situaciones temporales:
- Inicialmente, ningún host en la red desea recibir información del grupo.
 - En t_0 , un host de Red 3 se incorpora al grupo para recibir la información correspondiente.
 - Posteriormente, en t_1 un host de Red 4 solicita la incorporación.
 - En t_2 el segundo host de Red 4 se incorpora también.
 - En t_3 el host de Red 3 se da de baja del grupo.
 - En t_4 uno de los hosts de Red 4 se da de baja del grupo.

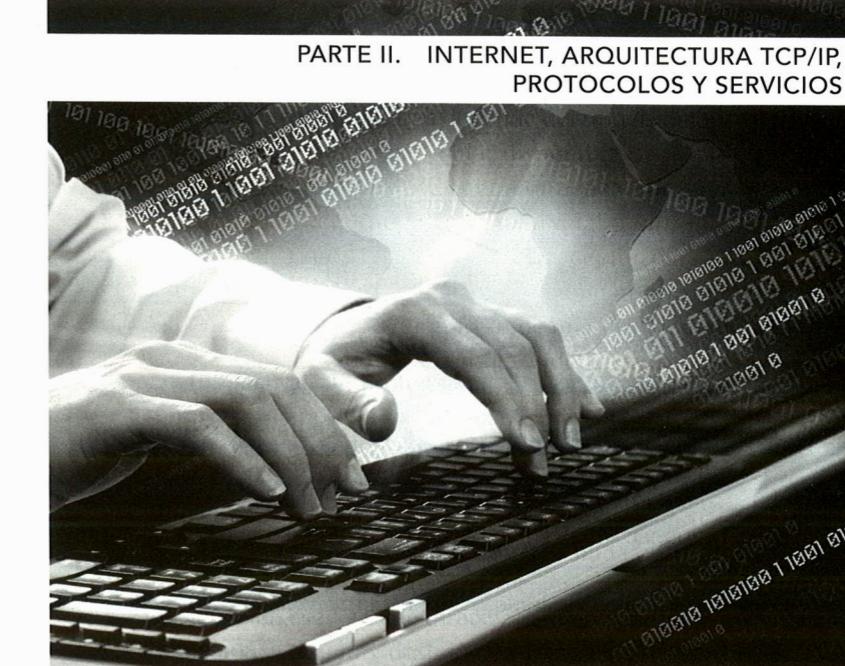


23. Tal como se ha indicado en el tema, una posibilidad para dar a conocer la dirección del grupo multicast del ejercicio anterior es hacerlo mediante el protocolo SAP. Consulte el RFC correspondiente y describa el proceso asociado.

BIBLIOGRAFÍA

- Adams, A.; Nicholas, J.; Siadak, W.: *Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)*. RFC 3973. Enero, 2005.
- Almquist, P.: *Type of Service in the Internet Protocol Suite*. RFC 1349. Julio, 1992.
- Braden, R.T.; Postel, J.: *Requirements for Internet Gateways*. RFC 1009. Junio, 1987.
- Comer, D.E.: *Internetworking with TCP/IP. Volume I: Principles, Protocols and Architecture*. 3.^a edición. Prentice Hall, 1995.
- Conta, A.; Deering, S.: *Internet Control Message Protocol (ICMP) for the Internet Protocol Version 6 (IPv6)*. RFC 1885. Diciembre, 1995.

- Deering, S.E.: *Host Extensions for IP Multicasting*. RFC 1112. Agosto, 1989.
- Deering, S.: *ICMP Router Discovery Messages*. RFC 1256. Septiembre, 1991.
- Deering, S.; Hinden, R.: *Internet Protocol, Version 6 (IPv6). Specification*. RFC 2460. Diciembre, 1998.
- Fenner, W.: *Internet Group Management Protocol, Version 2*. RFC 2236. Noviembre, 1997.
- Fenner, B.; Handley, M.; Holbrook, H.; Kouvelas, I.: *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*. RFC 4601. Agosto, 2006.
- Hanna, S.; Patel, B.; Shah, M.: *Multicast Address Dynamic Client Allocation Protocol (MADCAP)*. RFC 2730. Diciembre, 1999.
- Hedrick, C.L.: *Routing Information Protocol*. RFC 1058. Junio, 1988.
- Hinden, R.M.; Sheltzer, A.: *DARPA Internet gateway*. RFC 823. Septiembre, 1982.
- Hinden, R.; S. Deering.: *IP Version 6 Addressing Architecture*. RFC 2373. Julio, 1998.
- Kent, S.; Atkinson, R.: *IP Authentication Header*. RFC 2402. Noviembre, 1998.
- Kent, S.; Atkinson, R.: *IP Encapsulating Security Payload (ESP)*. RFC 2406. Noviembre, 1998.
- Kent, S.; Seo, K.: *Security Architecture for the Internet Protocol*. RFC 4301. Diciembre 2005.
- Kurose, J.F.; Ross, K.W.: *Computer Networking. A Top-Down Approach*. Addison Wesley, 2013. 6.^a edición.
- Madson, C.; Glenn, R.: *The Use of HMAC-MD5-96 within ESP and AH*. RFC 2403. Noviembre, 1998.
- Madson, C.; Glenn, R.: *The Use of HMAC-SHA-1-96 within ESP and AH*. RFC 2404. Noviembre, 1998.
- Madson, C.; Doraswamy, N.: *The ESP DES-CBC Cipher Algorithm with Explicit IV*. RFC 2405. Noviembre, 1998.
- Malkin, G.: *RIP Version 2*. RFC 2453. Noviembre, 1998.
- Meyer, D.: *Administratively Scoped IP Multicast*. RFC 2365. Julio, 1998.
- Mills, D.L.: *Exterior Gateway Protocol Formal Specification*. RFC 904. Abril, 1984.
- Moy, J.: *OSPF Specification*. RFC 1131. Octubre, 1989.
- Moy, J.: *Multicast Extensions to OSPF*. RFC 1584. Marzo, 1994.
- Moy, J.: *OSPF Version 2*. RFC 2328. Abril, 1998.
- Partridge, C.; Mendez, T.; Milliken, W.: *Host Anycasting Service*. RFC 1546. Noviembre, 1993.
- Postel, J.: *Internet Protocol*. RFC 791. Septiembre, 1981.
- Postel, J.: *Internet Control Message Protocol*. RFC 792. Septiembre, 1981.
- Radoslavov, P.; Estrin, D.; Govindan, R.; Handley, M.; Kumar, S.; Thaler, D.: *The Multicast Address-Set Claim (MASC) Protocol*. RFC 2909. Septiembre, 2000.
- Ramakrishnan, K.; Floyd, S.: *A Proposal to Add Explicit Congestion Notification (ECN) to IP*. RFC 2481. Enero, 1999.
- Rekhter, Y.; Li, T.: *A Border Gateway Protocol 4 (BGP-4)*. RFC 1771. Marzo, 1995.
- Reynolds, J.; Postel, J.: *Assigned Numbers*. RFC 1700. Octubre, 1994.
- Stallings, W.: *Comunicaciones y Redes de Computadores*. Pearson Educación, 2004. 7.^a edición.
- Stevens, W.R.: *TCP/IP Illustrated, Vol. 1. The Protocols*. Ed. Addison Wesley, 2000.
- Thaler, D.; Handley, M.; Estrin, D.: *The Internet Multicast Address Allocation Architecture*. RFC 2908. Septiembre 2000.
- Waitzman, D.; Partridge, C.; Deering, S.E.: *Distance Vector Multicast Routing Protocol*. RFC 1075. Noviembre, 1988.



PROTOCOLOS EXTREMO A EXTREMO

10.1. Introducción

Continuando con el estudio de la arquitectura TCP/IP, tras la presentación de la capa de red y de sus protocolos, en este capítulo abordaremos las funciones propias de la capa de transporte, considerando especialmente las soluciones adoptadas en los protocolos asociados. De igual manera a como sucede en el modelo OSI, la capa de transporte en TCP/IP es la primera de las capas denominadas extremo a extremo (Figura 10.1). Esto es, involucra directamente a las estaciones finales o *hosts* y no a los dispositivos intermedios de la subred (ver Capítulo 1). El diseño de esta capa, como comprobaremos en el capítulo, adopta el principio de diseño de situar la complejidad en los extremos (ver Apartado 8.1).

A diferencia de lo que ocurre en la capa de red, donde solo existe el protocolo IP para llevar a cabo las funcionalidades de direccionamiento y encaminamiento, para la capa de transporte se adopta una aproximación polarizada en la que se especifican dos alternativas: UDP y TCP. El primer protocolo se caracteriza por ofrecer, al igual que IP, un servicio no fiable y no orientado a conexión. Por el contrario, TCP ofrece un servicio orientado a conexión que incluye el control de flujo, control de errores y control de congestión.

En el siguiente apartado se explica el protocolo UDP. Frente a este, con una complejidad mucho mayor, en el apartado tercero se estudian los servicios ofrecidos por TCP. Además, en ese mismo apartado se consideran las variantes o «sabores» de TCP más relevantes. Nuestro estudio también incluye un modelado analítico de TCP, tanto en latencia como en tasa o velocidad de transmisión, que permitirá