Los mensajes **eco** y **respuesta a eco** proporcionan un mecanismo para comprobar que la comunicación entre dos entidades es posible. El receptor de un mensaje de eco está obligado a devolver el mensaje en un mensaje de respuesta a eco. Al mensaje de eco se le asocia un identificador y un número de secuencia que coinciden con los de paquete de respuesta a eco. El identificador se puede utilizar como un punto de acceso al servicio, para identificar una sesión particular, y el número de secuencia se puede incrementar en cada petición de eco enviada.

Los mensajes **marca de tiempo** y **respuesta a marca de tiempo** proporcionan un mecanismo para muestrear las características en cuanto a retardo del conjunto de redes. El emisor de un mensaje marca de tiempo puede incluir un identificador y un número de secuencia en el campo parámetros e incluye el tiempo en el cual se envió el mensaje (marca de tiempo original). El receptor registra, en el mensaje respuesta, el tiempo en que recibió el mensaje y el tiempo en que transmitió el mensaje de respuesta. Si el mensaje marca de tiempo se envía usando un encaminamiento en el origen estricto, se pueden determinar las características de retardo de una ruta particular.

Los mensajes **petición de máscara de dirección** y **respuesta a máscara de dirección** son útiles en un entorno que incluya subredes. Los mensajes de petición y respuesta de máscara de dirección permiten a un computador conocer la máscara de dirección usada en la LAN a la que está conectado. El computador emite por difusión un mensaje de petición de máscara de dirección en la LAN. El dispositivo de encaminamiento en la LAN responde con un mensaje de respuesta a máscara de red que contiene la máscara de dirección.

18.5. IPv6

El Protocolo Internet (IP) ha sido el fundamento de Internet y virtualmente de todas las redes privadas de múltiples proveedores. Este protocolo está alcanzando el fin de su vida útil y se ha definido un nuevo protocolo conocido como IPv6 (IP versión 6) para, en última instancia, reemplazar a IP[4].

En primer lugar, examinaremos la motivación para desarrollar una nueva versión de IP y después analizaremos algunos de sus detalles.

IP DE NUEVA GENERACIÓN

El motivo que ha conducido a la adopción de una nueva versión ha sido la limitación impuesta por el campo de dirección de 32 bits en IPv4. Con un campo de dirección de 32 bits, en principio es posible asignar 2^{32} direcciones diferentes, alrededor de 4.000 millones de direcciones posibles. Se podría pensar que este número de direcciones era más que adecuado para satisfacer las necesidades en Internet. Sin embargo, a finales de la década de los ochenta se percibió que habría un problema y este problema empezó a manifestarse a comienzos de la década de los noventa. Algunas de las razones por las que es inadecuado utilizar estas direcciones de 32 bits son las siguientes:

- La estructura en dos niveles de la dirección IP (número de red, número de computador) es conveniente pero también es una forma poco económica de utilizar el espacio de direcciones. Una vez que se le asigna un número de red a una red, todos los números de computador de

[4] Se podría pensar que se han saltado varias versiones en este libro. La versión en uso de IP es actualmente la versión 4; las versiones previas de IP (de la 1 a la 3) fueron sucesivamente definidas y sustituidas hasta alcanzar IPv4. La versión 5 es el número asignado al protocolo de flujo (*stream protocol*), un protocolo de la capa internet orientado a conexión. De aquí el uso de la etiqueta versión 6.

ese número de red se asignan a esa red. El espacio de direcciones para esa red podría estar poco usado, pero en lo que concierne a la efectividad del espacio de direcciones, si se usa un número de red entonces se consumen todas las direcciones dentro de la red.

- El modelo de direccionamiento de IP requiere que se le asigne un número de red único a cada red IP independientemente de si la red está realmente conectada a Internet.
- Las redes están proliferando rápidamente. La mayoría de las organizaciones establecen LAN múltiples, no un único sistema LAN. Las redes inalámbricas están adquiriendo un mayor protagonismo. Internet misma ha crecido explosivamente durante años.
- El uso creciente de TCP/IP en áreas nuevas producirá un crecimiento rápido en la demanda de direcciones únicas IP (por ejemplo, el uso de TCP/IP para interconectar terminales electrónicos de puntos de venta y para los receptores de televisión por cable).
- Normalmente, se asigna una dirección única a cada computador. Una disposición más flexible es permitir múltiples direcciones IP a cada computador. Esto, por supuesto, incrementa la demanda de direcciones IP.

Por tanto, la necesidad de un incremento en el espacio de direcciones ha impuesto la necesidad de una nueva versión de IP. Además, IP es un protocolo muy viejo y se han definido nuevos requisitos en las áreas de configuración de red, flexibilidad en el encaminamiento y funcionalidades para el tráfico.

En respuesta a estas necesidades, el Grupo de Trabajo de Ingeniería de Internet (IETF) emitió una solicitud de propuestas para una nueva generación de IP (IPng) en julio de 1992. Se recibieron varias propuestas y en 1994 emergió el diseño final de IPng. Uno de los hechos destacados del desarrollo fue la publicación del RFC 1752, «La recomendación para el protocolo de nueva generación de IP», publicado en enero de 1995. El RFC 1752 describe los requisitos de IPng, especifica el formato de la PDU y señala las técnicas de IPng en las áreas de direccionamiento, encaminamiento y seguridad. Existen otros documentos Internet que definen los detalles del protocolo, ahora llamado oficialmente IPv6; éstos incluyen una especificación general de IPv6 (RFC 2460), un RFC que trata sobre la estructura de direccionamiento de IPv6 (RFC 2373) y una larga lista adicional.

IPv6 incluye las siguientes mejoras sobre IPv4:

- **Un espacio de direcciones ampliado:** IPv6 utiliza direcciones de 128 bits en lugar de las direcciones de 32 bits de IPv4. Esto supone un incremento del espacio de direcciones en un factor de 2^{96}. Se ha señalado [HIND95] que esto permite espacios de direcciones del orden de 6×10^{23} por metro cuadrado de la superficie de la tierra. Incluso si la asignación de direcciones fuera muy ineficiente, este espacio de direcciones parece seguro.
- **Un mecanismo de opciones mejorado:** las opciones de IPv6 se encuentran en cabeceras opcionales separadas situadas entre la cabecera IPv6 y la cabecera de la capa de transporte. La mayoría de estas cabeceras opcionales no se examinan ni procesan por ningún dispositivo de encaminamiento en la trayectoria del paquete. Esto simplifica y acelera el procesamiento que realiza un dispositivo de encaminamiento sobre los paquetes IPv6 en comparación a los datagramas IPv4[5]. Esto también hace que sea más fácil incorporar opciones adicionales.
- **Autoconfiguración de direcciones:** esta capacidad proporciona una asignación dinámica de direcciones IPv6.

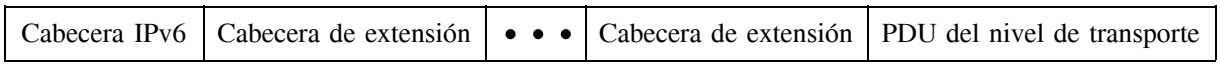
[5] La unidad de datos de protocolo para IPv6 se denomina paquete en lugar de datagrama, que es el término que se utiliza para las PDU de IPv4.

- **Aumento de la flexibilidad en el direccionamiento:** IPv6 incluye el concepto de una dirección monodifusión (*anycast*), mediante la cual un paquete se entrega sólo a un nodo seleccionado de entre un conjunto de nodos. Se mejora la escalabilidad del encaminamiento multidistribución con la incorporación de un campo de ámbito a las direcciones multidistribución.
- **Funcionalidad para la asignación de recursos:** en lugar del campo tipo de servicio de IPv4, IPv6 habilita el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el que el emisor solicita un tratamiento especial. Esto ayuda al tratamiento de tráfico especializado como el de vídeo en tiempo real.

Todas estas características se exploran en el resto de la sección, excepto las características de seguridad, que se discuten en el Capítulo 21.

ESTRUCTURA IPv6

Una unidad de datos del protocolo de IPv6 (conocida como paquete) tiene el formato general siguiente:



La única cabecera que se requiere se denomina simplemente cabecera IPv6. Ésta tiene una longitud fija de 40 octetos, comparados con los 20 octetos de la parte obligatoria de la cabecera IPv4 (*véase* Figura 18.6). Se han definido las siguientes cabeceras de extensión:

- **Cabecera de opciones salto a salto:** define opciones especiales que requieren procesamiento en cada salto.
- **Cabecera de encaminamiento:** proporciona un encaminamiento ampliado, similar al encaminamiento en el origen de IPv4.
- **Cabecera de fragmentación:** contiene información de fragmentación y reensamblado.
- **Cabecera de autenticación:** proporciona la integridad del paquete y la autenticación.
- **Cabecera de encapsulamiento de la carga de seguridad:** proporciona privacidad.
- **Cabecera de las opciones para el destino:** contiene información opcional para que sea examinada en el nodo destino.

El estándar IPv6 recomienda que, en el caso de que se usen varias cabeceras de extensión, las cabeceras IPv6 aparezcan en el siguiente orden:

1. Cabecera IPv6: obligatoria, debe aparecer siempre primero.
2. Cabecera de las opciones salto a salto.
3. Cabecera de las opciones para el destino: para opciones a procesar por el primer destino que aparece en el campo dirección IPv6 de destino y por los destinos subsecuentes indicados en la cabecera de encaminamiento.
4. Cabecera de encaminamiento.
5. Cabecera de fragmentación.
6. Cabecera de autenticación.
7. Cabecera de encapsulado de la carga de seguridad.

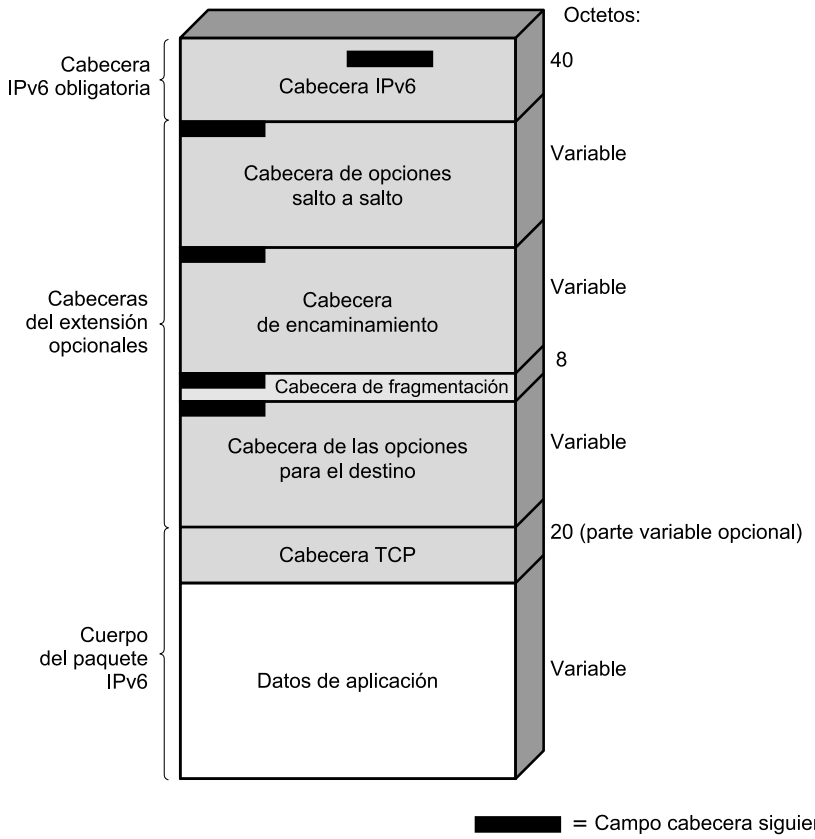


Figura 18.10. Paquete IPv6 con las cabeceras de extensión (conteniendo un segmento TCP).

8. Cabecera de opciones para el destino: para opciones a procesar por el destino final del paquete.

La Figura 18.10 muestra un ejemplo de un paquete IPv6 que incluye un ejemplar de cada cabecera, excepto aquellas relacionadas con la seguridad. Obsérvese que la cabecera IPv6 y cada cabecera de extensión incluyen el campo cabecera siguiente. Este campo identifica el tipo de cabecera que viene a continuación. Si la siguiente cabecera es de extensión, entonces este campo contiene el identificador del tipo de esa cabecera. En caso contrario, este campo contiene el identificador del protocolo de la capa superior que está usando a IPv6 (normalmente un protocolo de la capa de transporte), utilizando el mismo valor que el campo protocolo de IPv4. En la Figura 18.10, el protocolo de la capa superior es TCP; por tanto, los datos de la capa superior transportados por el paquete IPv6 constan de una cabecera TCP seguida por un bloque de datos de aplicación.

A continuación, se examina la cabecera principal de IPv6 y después se examinan cada una de las extensiones.

CABECERA IPv6

La cabecera IPv6 tiene una longitud fija de 40 octetos, que consta de los siguientes campos (*véase* Figura 18.11):

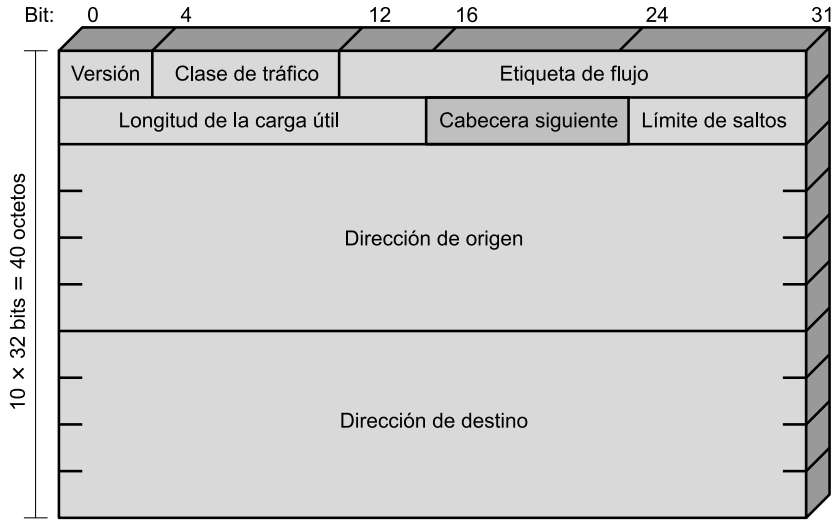


Figura 18.11. Cabecera IPv6.

- **Versión (4 bits):** número de la versión del protocolo Internet; el valor es 6.
- **Clase de tráfico (8 bits):** disponible para su uso por el nodo origen y/o los dispositivos de encaminamiento para identificar y distinguir entre clases o prioridades de paquete IPv6. Este campo se usa actualmente para los campos de ceros y ECN, como se describió para el campo tipo de servicio en IPv4.
- **Etiqueta de flujo (20 bits):** se puede utilizar por un computador para etiquetar aquellos paquetes para los que requiere un tratamiento especial en los dispositivos de encaminamiento dentro de la red; se discute después.
- **Longitud de la carga útil (16 bits):** longitud del resto del paquete IPv6 excluida la cabecera, en octetos. En otras palabras, representa la longitud de todas las cabeceras de extensión más la PDU de la capa de transporte.
- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6; se puede tratar tanto de una cabecera de extensión IPv6 como de una cabecera de la capa superior, como TCP o UDP.
- **Límite de saltos (8 bits):** el número restante de saltos permitidos para este paquete. El límite de saltos se establece por la fuente a algún valor máximo deseado y se decrementa en 1 en cada nodo que reenvía el paquete. El paquete se descarta si el límite de saltos se hace cero. Esto es una simplificación del procesamiento requerido por el campo tiempo de vida de IPv4. El consenso fue que el esfuerzo extra de contabilizar los intervalos de tiempo en IPv4 no añadía un valor significativo al protocolo. De hecho, y como regla general, los dispositivos de encaminamiento IPv4 tratan el campo tiempo de vida como un límite de saltos.
- **Dirección origen (128 bits):** dirección del productor del paquete.
- **Dirección destino (128 bits):** dirección de destino deseado del paquete. Puede que éste no sea en realidad el último destino deseado si está presente la cabecera de encaminamiento, como se explicará después.

Aunque la cabecera IPv6 es más grande que la parte obligatoria de la cabecera IPv4 (40 octetos frente a 20 octetos), contiene menos campos (8 frente a 12). Así, los dispositivos de encaminamiento tienen que hacer menos procesamiento por paquete, lo que agiliza el encaminamiento.

Clase de tráfico

El campo de clase de tráfico de 8 bits permite a una fuente identificar las características en el tratamiento de tráfico que desea cada paquete en relación con otros paquetes procedentes de la misma fuente. Al igual que ocurrió con el campo TOS (Tipo de Servicio) de IPv4, la intención original del campo clase de tráfico ha sido suplantada. Actualmente, los primeros seis bits del campo clase de tráfico se denominan campo de servicios diferenciados (DS, *Differentiated Services*), discutidos en el Capítulo 19. Los 2 bits restantes se reservan para un campo de notificación explícita de congestión (ECN, *Explicit Congestion Notification*), encontrándose actualmente en proceso de estandarización. El campo ECN proporcionará un mecanismo para señalizar explícitamente la congestión de una manera similar a la que se discutió para retransmisión de tramas (*véase* Sección 13.5).

Etiqueta de flujo

El estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen particular a un destino particular (monodistribución o multidistribución) y para el que el origen desea un tratamiento especial por parte de los dispositivos de encaminamiento. Un flujo está unívocamente identificado por la combinación de una dirección origen, una dirección destino y una etiqueta de flujo de 20 bits distinta de cero. Así, todos los paquetes que van a formar parte del mismo flujo tienen asignada por el origen la misma etiqueta de flujo.

Desde el punto de vista del origen, un flujo será normalmente una secuencia de paquetes que se generan por una única aplicación en el origen y tienen los mismos requisitos del servicio de transferencia. Un flujo puede estar compuesto de una única conexión TCP o incluso de varias. Un ejemplo de este último caso es una aplicación de transferencia de ficheros, que podría tener una conexión de control y varias conexiones de datos. Una única aplicación puede generar un único flujo o varios flujos. Un ejemplo de este último caso es la conferencia multimedia, que podría tener un flujo para audio y otro para ventanas gráficas, cada una con diferentes requisitos de transmisión en términos de tasa de datos, retardo y variación del retardo.

Desde el punto de vista de los dispositivos de encaminamiento, un flujo es una secuencia de paquetes que comparten atributos que afectan a cómo deben ser tratados por el dispositivo de encaminamiento. Estos incluyen atributos de camino, asignación de recursos, requisitos sobre cómo descartar, contabilidad de paquetes transmitidos y atributos de seguridad. El dispositivo de encaminamiento puede tratar los paquetes de diferentes flujos de forma diversa, incluyendo la asignación de diferentes tamaños de memoria temporal, dando diferente precedencia en términos de reenvío y solicitando de las redes diferentes calidades de servicio.

Ninguna etiqueta de flujo tiene un significado especial. En consecuencia, el tratamiento especial que se ha de dar al flujo de paquetes se debe declarar de alguna forma. Por ejemplo, un origen podría negociar o solicitar a los dispositivos de encaminamiento un determinado tratamiento de forma anticipada por medio de un protocolo de control, o en el momento de la transmisión, mediante información insertada en alguna de las cabeceras de extensión del paquete, como puede ser en la cabecera de opciones de salto a salto. Como ejemplo de tratamiento especial que se podría solicitar están el de una calidad de servicio que sea diferente de la establecida implícitamente o alguna forma de servicio en tiempo real.

En principio, todos los requisitos de un usuario para un flujo particular se podrían definir en una cabecera de extensión incluida en todos los paquetes. Si queremos dejar el concepto de flujo abierto para incluir una gran variedad de requisitos, esta técnica de diseño daría lugar a cabeceras de paquete muy grandes. La alternativa, adoptada por IPv6, es la etiqueta de flujo, en la que los requisitos de flujo se definen antes de comenzar el flujo y se le asigna una única etiqueta. En este caso, el dispositivo de encaminamiento debe guardar la información sobre los requisitos de flujo de cada uno de los flujos.

Se aplican las siguientes reglas a las etiquetas de flujo:

1. Los computadores o dispositivos de encaminamiento que no soportan el campo de etiqueta de flujo deben poner a cero este campo cuando generan un paquete, no cambiar el campo cuando reenvían e ignorar el campo cuando reciben un paquete.
2. Todos los paquetes producidos en un origen dado con la misma etiqueta de flujo distinta de cero deben tener la misma dirección destino, dirección origen y el mismo contenido en las cabeceras de opciones salto a salto y de encaminamiento (si estas cabeceras están presentes). La intención es que un dispositivo de encaminamiento pueda decidir cómo encaminar y procesar el paquete simplemente buscando la etiqueta de flujo en una tabla, sin examinar el resto de la cabecera.
3. El origen asigna a cada flujo una etiqueta de flujo. Las etiquetas de flujo nuevas se deben elegir (pseudo)aleatoriamente y uniformemente en el rango de 1 a $2^{20} - 1$, teniendo en cuenta la restricción de que el origen no puede reutilizar una etiqueta de flujo para un flujo nuevo en el tiempo de vida del flujo existente. La etiqueta de flujo cero se reserva para indicar que no se está utilizando etiquetado en el flujo.

Este último punto requiere alguna aclaración adicional. El dispositivo de encaminamiento debe mantener, presumiblemente en algún tipo de tabla, la información sobre las características de cada flujo activo que puede pasar por él. Para que sea capaz de reenviar los paquetes eficiente y rápidamente, la búsqueda en la tabla ha de ser eficiente. Una alternativa es tener una tabla con 2^{20} (alrededor de 16 millones) elementos, uno por cada etiqueta de flujo posible; esto impone una capacidad de memoria innecesaria en el dispositivo de encaminamiento. Otra alternativa es tener un elemento en la tabla por cada flujo activo y que incluya la etiqueta de flujo, lo que requiere que el dispositivo de encaminamiento busque en la tabla entera cada vez que le llega un paquete. Esto supone una carga de procesamiento innecesaria en el dispositivo de encaminamiento. En lugar de esto, la mayoría de los diseños de dispositivos de encaminamiento utilizan frecuentemente algún tipo de enfoque basado en una tabla de dispersión (*hash*). Con este enfoque se utiliza una tabla de tamaño moderado y a cada flujo se le asigna un elemento de la tabla utilizando una función de mezcla de la etiqueta de flujo. Esta función de mezcla podría ser simplemente extraer los bits menos significativos (por ejemplo, los 8 o 10 bits más bajos) de la etiqueta de flujo o algún cálculo sencillo con los 20 bits de la etiqueta de flujo. En cualquier caso, la eficiencia del planteamiento de funciones de dispersión normalmente depende de que las etiquetas de flujo estén distribuidas uniformemente en su rango posible (de aquí el requisito número 3 indicado anteriormente).

DIRECCIONES IPv6

Las direcciones IPv6 tienen una longitud de 128 bits. Las direcciones se asignan a interfaces individuales en los nodos, no a los nodos[6]. Una única interfaz puede tener múltiples direcciones

[6] En IPv6, un *nodo* es cualquier dispositivo que implemente IPv6; esto incluye a computadores y dispositivos de encaminamiento.

únicas. Cualquiera de las direcciones asociadas a las interfaces de los nodos se puede utilizar para identificar de forma única al nodo.

La combinación de direcciones largas y direcciones múltiples por interfaz permite una eficiencia mejorada del encaminamiento con respecto a IPv4. En IPv4, generalmente las direcciones no tienen una estructura que ayude al encaminamiento y, por tanto, un dispositivo de encaminamiento necesita mantener una gran tabla con rutas de encaminamiento. Una dirección internet más grande permite agrupar las direcciones por jerarquías de red, por proveedores de acceso, por proximidad geográfica, por institución, etc. Estas agrupaciones deben conducir a tablas de encaminamiento más pequeñas y a consultas más rápidas. El permitir múltiples direcciones por interfaz posibilita a un abonado que utiliza varios proveedores de acceso a través de la misma interfaz, tener direcciones distintas agrupadas bajo el espacio de direcciones de cada proveedor.

IPv6 permite tres tipos de direcciones:

- **Unidifusión (*unicast*):** un identificador para una interfaz individual. Un paquete enviado a una dirección de este tipo se entrega a la interfaz identificada por esa dirección.
- **Monodifusión (*anycast*):** un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección monodifusión se entrega a una de las interfaces identificadas por esa dirección (la más cercana, de acuerdo a la medida de distancia de los protocolos de encaminamiento).
- **Multidifusión (*multicast*):** un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección multidifusión se entrega a todas las interfaces identificadas por esa dirección.

CABECERA DE OPCIONES SALTO A SALTO

La cabecera de opciones salto a salto transporta información opcional que, si está presente, debe ser examinada por cada dispositivo de encaminamiento a lo largo de la ruta. Esta cabecera contiene los siguientes campos (*véase* Figura 18.12a):

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Longitud de la cabecera de extensión (8 bits):** longitud de la cabecera en unidades de 64 bits, sin incluir los primeros 64 bits.
- **Opciones:** campo de longitud variable que consta de una o más definiciones de opción. Cada definición se expresa mediante tres subcampos: tipo de opción (8 bits), que identifica la opción; longitud (8 bits), que especifica la longitud en octetos del campo de datos de la opción; y datos de opción, que es una especificación de la opción de longitud variable.

En realidad, se utilizan los cinco bits menos significativos del campo tipo de opción para especificar una opción particular. Los bits más significativos indican la acción que tiene que realizar un nodo que no reconoce el tipo de opción, de acuerdo a:

- 00—ignorar esta opción y continuar procesando la cabecera.
- 01—descartar el paquete.
- 10—descartar el paquete y enviar un mensaje ICMP de problema de parámetro a la dirección origen del paquete, indicando el tipo de opción no reconocida.

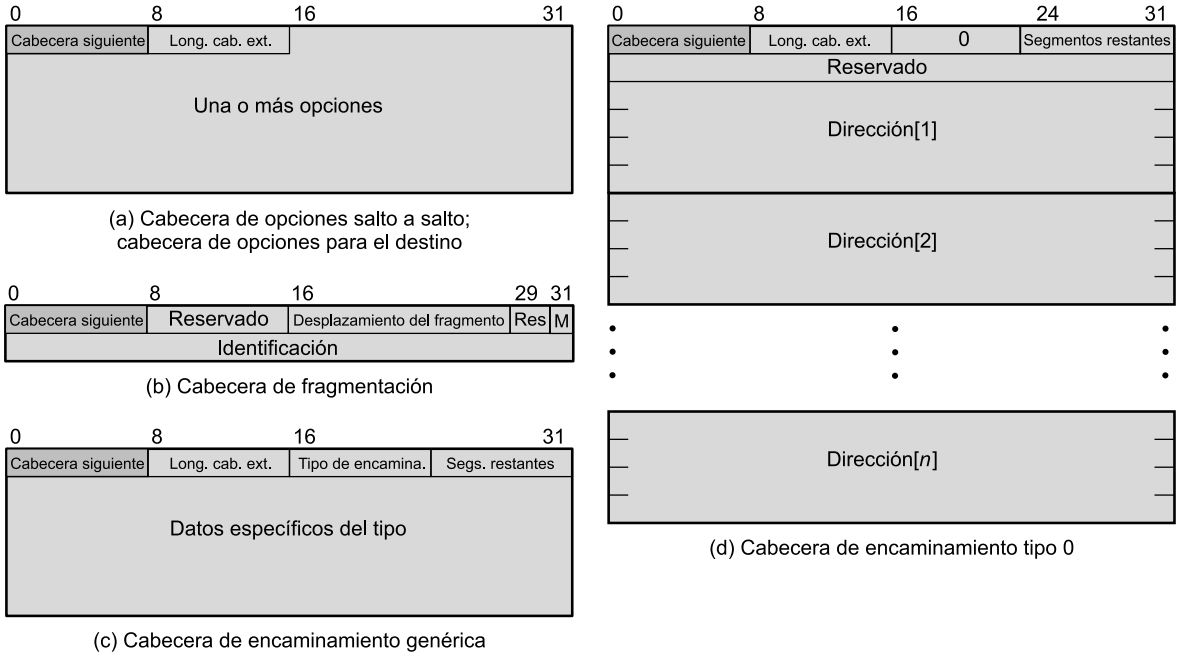


Figura 18.12. Cabecera de extensión IPv6.

- 11—descartar el paquete y, solamente si la dirección destino del paquete no es una dirección multidifusión, enviar un mensaje ICMP de problema de parámetro a la dirección origen del paquete, indicando el tipo de opción no reconocida.

El tercer bit indica si el campo de datos de la opción no cambia (0) o si puede cambiar (1) en el camino desde el origen al destino. Los datos que pueden cambiar se deben excluir de los cálculos de autentificación, como se discutirá en el Capítulo 21.

Estas convenciones para el campo del tipo de opción también se aplican a la cabecera de opciones en el destino.

Hasta ahora se han especificado cuatro opciones salto a salto:

- **Relleno1:** utilizada para insertar un byte de relleno dentro de la zona de opciones de la cabecera.
- **RellenoN:** utilizada para insertar N bytes ($N \geqslant 2$) de relleno dentro de la zona de opciones de la cabecera. Las dos opciones de relleno aseguran que la cabecera tiene una longitud múltiplo de 8 bytes.
- **Carga útil Jumbo:** se utiliza para enviar paquetes con una carga útil mayor de 65.535 octetos. El campo de datos de esta opción tiene una longitud de 32 bits y da la longitud del paquete en octetos, excluyendo la cabecera IPv6. Para estos paquetes, el campo de longitud de la carga en la cabecera IPv6 debe estar a cero y no puede haber cabecera de fragmentación. Con esta opción, IPv6 permite tamaños de paquete de hasta 4.000 millones de octetos. Esto facilita la transmisión de paquetes de vídeo grandes y posibilita que IPv6 haga el mejor uso de la capacidad disponible sobre cualquier medio de transmisión.

- **Alerta al dispositivo de encaminamiento:** informa al dispositivo de encaminamiento que el contenido de este paquete es de interés para el dispositivo de encaminamiento y para tratar adecuadamente cualquier información de control. La ausencia de esta opción en un datagrama IPv6 informa al dispositivo de encaminamiento que el paquete no contiene información necesaria para el dispositivo de encaminamiento y, por tanto, puede encaminarlo de forma segura sin ningún análisis adicional. A los computadores que originan paquetes IPv6 se les obliga a que incluyan esta opción en ciertas circunstancias. El motivo de esta opción es proporcionar un apoyo suficiente a protocolos como RSVP (*véase* Capítulo 19) que generan paquetes que necesitan ser examinados por dispositivos de encaminamiento intermedios por motivos de control de tráfico. En lugar de requerir a los dispositivos de encaminamiento intermedios que analicen en detalle la cabecera de extensión, esta opción alerta al dispositivo de encaminamiento cuando se requiere esta atención.

CABECERA DE FRAGMENTACIÓN

En IPv6, la fragmentación sólo puede ser realizada por el nodo origen, no por los dispositivos de encaminamiento a lo largo del camino del paquete. Para obtener todas las ventajas del entorno de interconexión, un nodo debe ejecutar un algoritmo de obtención de la ruta, lo que permite conocer la unidad máxima de transferencia (MTU, *Maximum Transfer Unit*) permitida por cada red en la ruta. Con este conocimiento, el nodo origen fragmentará el paquete, según se requiera, para cada dirección de destino dada. Si no se ejecuta este algoritmo, el origen debe limitar todos los paquetes a 1.280 octetos, que debe ser la mínima MTU que permitan las redes.

La cabecera de fragmentación contiene los siguientes campos (*véase* Figura 18.12b):

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Reservado (8 bits):** reservado para usos futuros.
- **Desplazamiento del fragmento (13 bits):** indica dónde se sitúa en el paquete original la carga útil de este fragmento. Se mide en unidades de 64 bits. Esto implica que los fragmentos (excepto el último) deben contener un campo de datos con una longitud de múltiplo de 64 bits.
- **Reservado (2 bits):** reservado para usos futuros.
- **Indicador M (1 bit):** 1 = más fragmentos; 0 = último fragmento.
- **Identificación (32 bits):** utilizado para identificar de forma única el paquete original. El identificador debe ser único para la dirección origen y dirección destino durante el tiempo que el paquete permanece en Internet. Todos los fragmentos con el mismo identificador, dirección origen y dirección destino son reensamblados para recuperar el paquete original.

El algoritmo de fragmentación es el mismo que el descrito en la Sección 18.3.

CABECERA DE ENCAMINAMIENTO

La cabecera de encaminamiento contiene una lista de uno o más nodos intermedios por los que se pasa en el camino del paquete a su destino. Todas las cabeceras de encaminamiento comienzan con un bloque de 32 bits consistente en 4 campos de 8 bits, seguido por datos de encaminamiento específicos al tipo de encaminamiento dado (*véase* Figura 18.12c). Los cuatro campos de 8 bits son los siguientes:

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Longitud de la cabecea de extensión (8 bits):** longitud de esta cabecera en unidades de 64 bits, sin incluir los primeros 64 bits.
- **Tipo de encaminamiento (8 bits):** identifica una variante particular de cabecera de encaminamiento. Si un dispositivo de encaminamiento no reconoce el valor del tipo de encaminamiento, debe descartar el paquete.
- **Segmentos restantes (8 bits):** número de segmentos en la ruta que quedan; esto es, el número de nodos intermedios explícitamente contenidos en la lista que se visitarán todavía antes de alcanzar el destino.

El único formato de cabecera de encaminamiento definido en el RFC 2460 es el de la cabecera de encaminamiento tipo 0 (*véase* Figura 18.12d). Cuando se utiliza una cabecera de encaminamiento tipo 0, el nodo origen no sitúa la dirección del último destino en la cabecera IPv6. En lugar de eso, esa dirección es la última de la lista en la cabecera de encaminamiento (Dirección[*n*], en la Figura 18.12d), y la cabecera IPv6 contiene la dirección destino del primer dispositivo de encaminamiento deseado en el camino. La cabecera de encaminamiento no se examina hasta que el paquete llega al nodo identificado por la cabecera IPv6. En ese punto, el paquete IPv6 y el contenido de la cabecera se actualizan y el paquete se reenvía. La actualización consiste en situar la siguiente dirección a visitar en la cabecera IPv6 y decrementar el campo segmentos restantes en la cabecera de encaminamiento.

CABECERA DE OPCIONES PARA EL DESTINO

La cabecera de opciones para el destino lleva información opcional que, si está presente, se examina por el nodo destino del paquete. El formato de esta cabecera es el mismo que la cabecera de opciones salto a salto (*véase* Figura 18.12a).

18.6. LECTURAS Y SITIOS WEB RECOMENDADOS

[RODR02] proporciona un tratamiento completo y claro de todos los temas tratados en este capítulo. En [COME01] y [STEV94] se puede encontrar un buen estudio sobre interconexión entre redes y sobre IPv4. [HUIT98] es una descripción técnica de varios RFC que integran juntos la especificación de IPv6; el libro proporciona una discusión sobre el propósito de varias características y el funcionamiento del protocolo. En [KESH98] se proporciona un instructivo repaso a la funcionalidad presente y futura de los dispositivos de encaminamiento.

COME01 Comer, D. *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture.* Upper Saddle River, NJ: Prentice Hall, 2001.

HUIT98 Huitema, C. *IPv6: The New Internet Protocol.* Upper Saddle River, NJ: Prentice Hall, 1998.

KESH98 Keshav, S., y Sharma, R. «Issues and Trends in Router Design.» *IEEE Communications Magazine*, mayo 1998.

RODR02 Rodriguez, A., *et al*., *TCP/IP Tutorial and Technical Overview*. Upper Saddle River: NJ: Prentice Hall, 2002.

STEV94 Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols.* Reading, MA: Addison-Wesley, 1994.

SITIOS WEB RECOMENDADOS

- **IPv6:** información sobre IPv6 y temas relacionados.
- **Página de información sobre IPv6:** incluye material introductorio, noticias sobre desarrollos recientes de productos IPv6 y enlaces relacionados.
- **Foro IPv6:** se trata de un consorcio de fabricantes que promociona productos relacionados con IPv6. Incluye una serie de documentos introductorios y artículos.

18.7. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

clase de tráfico
difusión
dispositivo de encaminamiento
fragmentación
interconexión de redes
internet
intranet
IPv4
IPv6
máscara de subred
monodifusión
multidifusión
protocolo de mensajes de control de internet (ICMP)
protocolo Internet (IP)
reensamblado
segmentación
sistema final
sistema intermedio
subred
tiempo de vida del datagrama

CUESTIONES DE REPASO

18.1. Dé algunas razones para usar fragmentación y reensamblado.

18.2. Enumere los requisitos de un mecanismo de interconexión de redes.

18.3. ¿Cuáles son los pros y los contras de limitar el reensamblado a los sistemas finales en lugar de permitirlo en los dispositivos de encaminamiento?

18.4. Explique la función de los tres indicadores en la cabecera de IPv4.

18.5. ¿Cómo se calcula la suma de comprobación de la cabecera de IPv4?

18.6. ¿Qué diferencia existe entre los campos clase de tráfico y etiqueta de flujo en la cabecera de IPv6?

18.7. Explique brevemente los tres tipos de direcciones IPv6.

18.8. ¿Cuál es el propósito de cada uno de los tipos de cabeceras presentes en IPv6?

EJERCICIOS

18.1. En la discusión sobre IP, se mencionó que el *identificador*, el *indicador de no fragmentar* y el *tiempo de vida* se hallan presentes en la primitiva *Send* pero no en la primitiva

Deliver, ya que esos parámetros no son competencia de IP. Indique, para cada una de estas primitivas, si es competencia de la entidad IP en el origen, de la entidad IP en cada dispositivo de encaminamiento intermedio o de la entidad IP en el sistema final destino. Justifique su respuesta.

18.2. ¿Cuál es la información suplementaria de la cabecera en el protocolo IP?

18.3. Describa algunas circunstancias en las que sería deseable utilizar encaminamiento en el origen en lugar de dejar a los dispositivos de encaminamiento que realicen la decisión de encaminamiento.

18.4. A causa de la fragmentación, un datagrama IP puede llegar en varios trozos, no necesariamente en el orden adecuado. La entidad IP en el sistema final receptor debe acumular estos fragmentos hasta que se reconstruya el datagrama original.

a) Considere que la entidad IP crea una memoria temporal para reensamblar el campo de datos del datagrama original. Conforme se va realizando el reensamblado, la memoria temporal contendrá bloques de datos y zonas vacías («agujeros») entre los bloques de datos. Describa un algoritmo para reensamblar datagramas basado en este concepto.

b) Para el algoritmo de la parte (a) es necesario hacer un seguimiento a los agujeros. Describa un mecanismo sencillo para hacer esto.

18.5. Un datagrama de 4.480 octetos se va a transmitir y se necesita fragmentar ya que va a pasar por una red Ethernet con un campo máximo de carga útil de 1.500 octetos. Muestre los valores de los campos longitud total, indicador de más segmentos y desplazamiento de fragmento en cada uno de los fragmentos resultantes.

18.6. Se necesita que la suma de comprobación de IP se recalcule en los dispositivos de encaminamiento a causa de los cambios en la cabecera IP, como el que ocurre en el campo tiempo de vida. Es posible recalcular esta suma desde cero. Sugiera un procedimiento que suponga menos cálculos. *Sugerencia:* suponga que el valor en el octeto k es cambiado por Z = valor_nuevo – valor_viejo; considere el efecto de este cambio en la suma de comprobación.

18.7. Se va a segmentar un datagrama. ¿Qué opciones del campo de opción se necesitan copiar en la cabecera de cada fragmento y cuáles se necesitan copiar sólo en el primer fragmento? Justifique el tratamiento de cada opción.

18.8. Un mensaje de la capa de transporte, que contiene 1.500 bits de datos y 160 bits de cabecera, se envía a la capa internet, la cual incorpora otros 160 bits de cabecera. El resultado se transmite a través de dos redes que utilizan cada una 24 bits de cabecera de paquete. La red destino tiene un tamaño de paquete máximo de 800 bits. ¿Cuántos bits, incluyendo cabeceras, se entregan al protocolo de la capa de red en el destino?

18.9. Se va a utilizar la arquitectura sugerida por la Figura 18.2. ¿Qué funciones se deberían añadir a los dispositivos de encaminamiento para aliviar algunos de los problemas causados por la desigualdad entre redes locales y de transporte a larga distancia?

18.10. ¿Debería existir una relación entre la interconexión entre redes y el encaminamiento interno de red? ¿Por qué sí o por qué no?

18.11. Compare los campos individuales de la cabecera IPv4 con los de la cabecera IPv6. Compare las posibilidades proporcionadas por cada uno de los campos de IPv4 con los de IPv6.

18.12. Justifique el orden recomendado de las cabeceras de extensión de IPv6 (por ejemplo, ¿por qué va primero la cabecera de opciones salto-a-salto?, ¿por qué la cabecera de encaminamiento está antes que la cabecera de fragmentación?, y así hasta la cabecera final).

18.13. El estándar IPv6 afirma que si un paquete con una etiqueta de flujo distinta de cero llega a un dispositivo de encaminamiento y éste no tiene información para esa etiqueta de flujo, el dispositivo de encaminamiento debería ignorar la etiqueta de flujo y reenviar el paquete.

a) ¿Cuáles son las desventajas de tratar este evento como un error, descartar el paquete y enviar un mensaje ICMP?

b) ¿Existen situaciones en las que encaminar el paquete como si su etiqueta de flujo fuera cero causará un resultado erróneo? Explíquelo.

18.14. El mecanismo de flujo de IPv6 supone que el estado asociado con una etiqueta de flujo dada se almacena en los dispositivos de encaminamiento. Por tanto, éstos saben cómo tratar los paquetes que llevan esa etiqueta de flujo. Un requisito de diseño es eliminar en los dispositivos de encaminamiento las etiquetas de flujo que no se van a utilizar más (etiquetas de flujo obsoletas).

a) Suponga que una fuente siempre envía un mensaje de control a todos los dispositivos de encaminamiento afectados suprimiendo una etiqueta de flujo cuando el origen acabe con ese flujo. En este caso, ¿cómo podría persistir una etiqueta de flujo antigua?

b) Sugiera mecanismos del origen y de los dispositivos de encaminamiento para superar el problema de las etiquetas de flujo antiguas.

18.15. Una cuestión que se plantea es qué paquetes generados por un origen deberían llevar etiquetas de flujo IPv6 distintas de cero. Para algunas aplicaciones, la respuesta es obvia. Los intercambios pequeños de datos deberían tener una etiqueta de flujo cero, ya que no merece la pena crear un flujo para unos pocos paquetes. Los flujos en tiempo real deberían tener una etiqueta de flujo; estos flujos fueron la causa primera de que se crearan etiquetas de flujo. Una cuestión más difícil es qué hacer con entidades paritarias que están enviando una gran cantidad de tráfico con el mejor esfuerzo (por ejemplo, las conexiones TCP). Describa un caso para asignar una única etiqueta de flujo a cada conexión TCP de gran duración. Describa un caso para no hacer esto.

18.16. Las especificaciones originales de IPv6 combinaban los campos de etiqueta de flujo y prioridad en un solo campo de etiqueta de flujo de 28 bits. Esto permitía a los flujos redefinir la interpretación de los diferentes valores de prioridad. Sugiera una razón por la que la especificación final incluye un campo de prioridad en un campo distinto.

18.17. Para el encaminamiento IPv6 tipo 0, especifique el algoritmo para actualizar las cabeceras IPv6 y de encaminamiento en los nodos intermedios.