6. Capítulo 6: Protocolos de Red

El propósito de este capítulo es examinar los protocolos de la capa de red, principalmente el protocolo IP, el cual representa uno de los pilares sobre los cuales se asienta el encaminamiento de los datagramas que circulan en la gran autopista de la nube. En primer lugar, se revisarán los fundamentos sobre los que se basan los protocolos que permiten la interconexión de equipos en una red, como así también la interconexión entre ellas. El resto del capítulo estará dedicado a los protocolos estándar de interconexión de redes: IPv4 e IPv6, ICMP e IGMP.

6.1. Fundamentos de la interconexión de redes

La Tabla 6.1.1 muestra algunos de los términos más comúnmente utilizados y relacionados con la interconexión entre redes (internetworking). Un conjunto de redes interconectadas, desde el punto de vista del usuario, puede aparecer simplemente como una red más grande. Sin embargo, si cada una de las redes constituyentes retiene su identidad y se necesitan mecanismos especiales para la comunicación a través de múltiples redes, entonces a la configuración entera se le conoce como conjunto de redes (o una internet).

Tabla 6.1.1: Términos relacionados con la interconexión de redes

Red de comunicación
Un sistema que proporciona un servicio de transferencia de datos entre estaciones conectadas a la red.
Internet
Una colección de redes de comunicación interconectadas por puentes o dispositivos de encaminamiento.
Intranet
Una internet corporativa que proporciona las aplicaciones claves de Internet, especialmente el world wide web. Una intranet opera dentro de una organización con fines internos y puede existir aisladamente, como una internet autocontenida o puede tener enlaces a Internet.
Subred
Hace referencia a una red constituyente de una internet. Esto evita la ambigüedad dado que, desde el punto de vista del usuario, una internet completa es una sola red.
Sistema Final (ES)
Un dispositivo conectado a una de las redes de una internet que se utiliza para apoyar a las aplicaciones o servicios del usuario final.
Sistema Intermedio (IS)
Un dispositivo utilizado para conectar dos redes y permitir la comunicación entre sistemas finales conectados a diferentes redes.
Puente (bridge)
Un IS utilizado para conectar dos redes LAN que utilizan el mismo protocolo. Este no modifica el contenido del paquete ni incorpora nada al mismo. Opera en la capa 2 del modelo OSI
Dispositivo de encaminamiento (router)

Un IS utilizado para conectar dos redes que pueden o no ser similares. El dispositivo de encaminamiento utiliza un protocolo de internet presente en cada dispositivo de encaminamiento y en cada computador de la red. Opera en la capa 3 del modelo OSI.

Cada red constituyente de una internet permite la comunicación entre los dispositivos conectados a esa red; estos dispositivos se conocen como sistemas finales (ES, End Systems). Además, las redes se conectan por dispositivos denominados en los documentos ISO como sistemas intermedios (IS, Intermediate Systems). Los IS proporcionan caminos de comunicación y realizan las funciones de retransmisión y encaminamiento necesarias para que los datos se puedan intercambiar entre los dispositivos conectados en las diferentes redes de la internet.

Existen dos tipos de IS, los puentes y los dispositivos de encaminamiento, que son de particular interés. Las diferencias entre ellos se derivan de los protocolos utilizados para la lógica de la interconexión entre las redes. En esencia, un puente opera en la capa 2 de la arquitectura de 7 capas del modelo para la interconexión de sistemas abiertos (OSI) y actúa como un retransmisor de tramas entre redes parecidas; los puentes ya se examinaron en el apunte Notas acerca de redes y comunicaciones, Parte I. Un dispositivo de encaminamiento opera en la capa 3 de la arquitectura OSI y encamina los paquetes entre redes potencialmente diferentes. Tanto los puentes como los dispositivos de encaminamiento suponen que se usa el mismo protocolo en la capa superior.

Comenzaremos nuestro estudio de la interconexión de redes con una discusión de los principios subyacentes en varios enfoques de interconexión entre redes. Después examinaremos la técnica más importante para la interconexión entre redes: el dispositivo de encaminamiento no orientado a conexión. Tras ello se describe el protocolo para la interconexión más extendido, llamado sencillamente Protocolo Internet (del inglés Internet Protocol, IP). A continuación, se examina el protocolo de interconexión normalizado más reciente, conocido como IPv6.

Los requisitos globales para un sistema de interconexión entre redes son los que siguen a continuación:

1. Proporcionar un enlace entre redes. Como mínimo, se necesita una conexión física y de control del enlace.

2. Proporcionar el encaminamiento y entrega de los datos entre procesos en diferentes redes.

3. Proporcionar un servicio de contabilidad que realice un seguimiento de la utilización de las diferentes redes y dispositivos de encaminamiento, y mantenga información de estado.

4. Proporcionar los servicios mencionados de forma que no se requiera la modificación de la arquitectura de red de cualquiera de las redes interconectadas. Esto significa que el sistema de interconexión entre redes se debe acomodar a las diversas diferencias existentes entre las distintas redes. Algunas de estas diferencias son:

- ✓ Diferentes esquemas de direccionamiento: las redes pueden usar diferentes nombres y direcciones de los puntos finales y diferentes esquemas de

mantenimiento del directorio. Por tanto, se debe proporcionar un esquema de direccionamiento de red global, así como un servicio de directorio.

- ✓ Diferente tamaño máximo de paquete: puede que se necesite romper un paquete en unidades más pequeñas al pasar a otra red. Este proceso se denomina fragmentación.
- ✓ Diferentes mecanismos de acceso a la red: el mecanismo de acceso de la estación a la red podría ser diferente para estaciones de redes diferentes.
- ✓ Diferentes valores de expiración de los temporizadores: normalmente, un servicio de transporte orientado a conexión esperará la confirmación de una recepción correcta de datos hasta que un temporizador expira, en cuyo caso retransmitirá su bloque de datos. En general, se requieren valores grandes del temporizador para realizar una entrega satisfactoria a través de redes múltiples. Los procedimientos que establecen los valores en la interconexión de redes deben permitir una transmisión satisfactoria que evite retransmisiones innecesarias.
- ✓ Recuperación de errores: los procedimientos deben proporcionar un servicio que va desde no suministrar recuperación de errores hasta un servicio extremo a extremo (dentro de la red) seguro. El servicio de interconexión de redes no debería depender o no tendría que ser interferido por la naturaleza de la capacidad de recuperación de errores de las redes individuales.
- ✓ Informes de estado: las diferentes redes dan informes de estado y de rendimiento de distintas formas. Debe ser posible que el sistema de interconexión proporcione información de la actividad de interconexión a los procesos interesados y autorizados.
- ✓ Técnicas de encaminamiento: el encaminamiento dentro de la red puede depender de la detección de fallos y de las técnicas de control de congestión particulares de cada red. El sistema de interconexión entre redes debe ser capaz de coordinar estas técnicas para encaminar los datos adaptativamente entre las estaciones de las diferentes redes.
- ✓ Control de acceso del usuario: cada red tendrá su propia técnica de control de acceso de los usuarios (autorización para usar la red). Estas técnicas se deben solicitar por el sistema de interconexión según se necesite. Además, se podría requerir una técnica diferente de control de acceso a la interconexión entre redes.
- ✓ Conexión, sin conexión: las redes individuales pueden proporcionar un servicio orientado a conexión (por ejemplo, circuitos virtuales) o no orientados a conexión (datagramas). Es deseable que el servicio entre redes no dependa de la naturaleza del servicio de conexión de las redes individuales.

Funcionamiento no orientado a conexión

Mientras que el modo de funcionamiento orientado a conexión se corresponde con el mecanismo de circuito virtual de una red de conmutación de paquetes,

el modo de operación no orientado a conexión se corresponde con el mecanismo de datagramas de una red de conmutación de paquetes. Cada unidad de datos del protocolo de red se trata independientemente y se encamina desde el ES origen al ES destino a través de una serie de dispositivos de encaminamiento y redes. Para cada unidad de datos transmitida por A, A realiza una decisión sobre qué dispositivo de encaminamiento debería recibir la unidad de datos. La unidad de datos salta a través del conjunto de redes de un dispositivo de encaminamiento al siguiente hasta que alcanza la subred destino. En cada dispositivo de encaminamiento se toma una decisión de encaminamiento (independientemente para cada unidad de datos) relativa al siguiente salto. Así, diferentes unidades de datos pueden viajar por diferentes rutas entre el ES origen y destino.

Todos los ES y todos los dispositivos de encaminamiento comparten un protocolo de la capa de red común conocido genéricamente como protocolo de interconexión de redes. Dentro del proyecto internet de DARPA se desarrolló un protocolo Internet (IP) inicial, publicado como RFC 791, que ha llegado a ser un estándar de Internet. Existe la necesidad de disponer de un protocolo para acceder a cada red particular debajo de un protocolo de interconexión de redes. Así, normalmente hay dos protocolos en la capa de red operando en cada ES y dispositivo de encaminamiento: una subcapa superior que proporciona la función de interconexión y una capa inferior que proporciona el acceso a la red.

6.2. Funcionamiento de redes interconectadas en un esquema no orientado a conexión

IP proporciona un servicio no orientado a conexión, o datagrama, entre sistemas finales. El enfoque sin conexión tiene una serie de ventajas. Éstas son:

- ✓ Un sistema de interconexión sin conexión es flexible. Puede trabajar con una gran variedad de redes, algunas de las cuales serán también sin conexión. En esencia, IP requiere muy poco de las redes sobre las que actúa.
- ✓ Un servicio de interconexión sin conexión se puede hacer bastante robusto. Se puede utilizar el mismo argumento expuesto para un servicio de red datagrama frente a un servicio con circuitos virtuales (ya discutido en estas notas).
- ✓ Un servicio de interconexión sin conexión es el mejor servicio para un protocolo de transporte no orientado a conexión, ya que no impone información suplementaria innecesaria.

La Figura 6.2.1 muestra un ejemplo típico en el que se usa IP, donde dos LAN se interconectan mediante una red WAN de retransmisión de tramas. La figura muestra el funcionamiento del protocolo IP para los datos intercambiados entre el computador A en una LAN (red 1) y el computador B en otra LAN (red 2) a través de la WAN. La figura muestra la arquitectura del protocolo y el formato de la unidad de datos en cada etapa. Los sistemas finales y los dispositivos de encaminamiento deben compartir un protocolo de interconexión común. Además, los sistemas finales deben compartir el mismo protocolo que hay arriba de IP. Los dispositivos de encaminamiento intermedios sólo necesitan implementar hasta el protocolo IP.

El protocolo IP en A recibe bloques de datos desde las capas superiores del software en A para que los envíe a B. IP añade una cabecera (en el instante t1) especificando, entre otras cosas, la dirección global Internet de B. Esa dirección consta de dos partes lógicas: un identificador de la red y un identificador del sistema final. La combinación de la cabecera IP y los datos de la capa superior se llama unidad de datos del protocolo de interconexión (PDU, Protocol Data Unit), o simplemente un datagrama. El datagrama es posteriormente encapsulado con el protocolo de la LAN (cabecera LLC en el instante t2; cabecera y cola MAC en el instante t3) y enviado al dispositivo de encaminamiento, que elimina la cabecera LAN para leer la cabecera IP (t6). El dispositivo de encaminamiento, entonces, encapsula el datagrama con los campos del protocolo de retransmisión de tramas (t8) y lo transmite a través de la WAN a otro dispositivo de encaminamiento.

Este dispositivo de encaminamiento elimina los campos de retransmisión de tramas y recupera el datagrama, al cual se le incorporan los campos LAN apropiados de la LAN 2 y se envía a B.

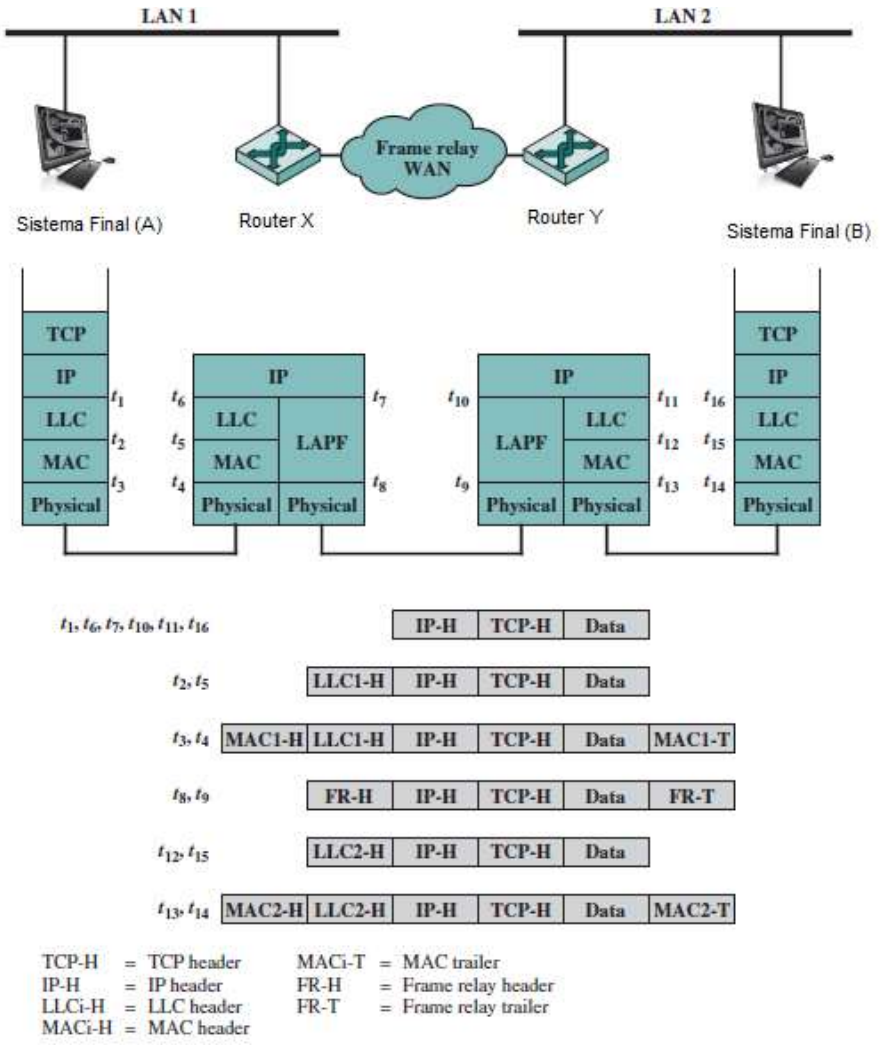

Figura 6.2.1: Ejemplo de operación del protocolo de internet

Se observa con más detalle este ejemplo. El sistema final A tiene que enviar un datagrama al sistema final B; el datagrama incluye la dirección internet de B. El módulo IP en A reconoce que el destino (B) está en otra subred. Por tanto, el primer paso es enviar los datos a un dispositivo de encaminamiento, en este caso al dispositivo de encaminamiento X. Para hacer esto, IP pasa el datagrama a la capa inferior (en este caso la capa LLC) con instrucciones para que se envíe al dispositivo de encaminamiento X. LLC pasa esta información a la capa MAC, que inserta la dirección de la capa MAC del dispositivo de encaminamiento en la cabecera MAC. Así, el bloque de datos transmitido en la LAN 1 incluye datos de una aplicación que está por encima de TCP, más la cabecera TCP, una cabecera IP, la cabecera LLC y la cabecera y cola MAC (tiempo t3 en la Figura 6.2.1).

A continuación, el paquete viaja a través de la red 1 hasta el dispositivo de encaminamiento X. Éste elimina los campos MAC y LLC y analiza el campo IP para determinar el destino último de los datos, en este caso B. El encaminador debe tomar ahora una decisión de encaminamiento.

Existen tres posibilidades:

- ✓ La estación destino B está conectada directamente a una de las redes a las que el dispositivo de encaminamiento está conectado. En este caso, el dispositivo de encaminamiento envía el datagrama directamente al destino.
- ✓ Se tienen que atravesar uno o más dispositivos de encaminamiento para alcanzar el destino. En este caso, se debe tomar una decisión de encaminamiento: ¿a qué dispositivo de encaminamiento se debe enviar el datagrama? En ambos casos 1 y 2, el módulo IP en el dispositivo de encaminamiento envía el datagrama a la capa inferior con la dirección de la red de destino. Hay que indicar que aquí se está hablando de una dirección de una capa inferior referente a esta red.
- ✓ El dispositivo de encaminamiento no conoce la dirección de destino. En este caso, el dispositivo de encaminamiento devuelve un mensaje de error a la fuente del datagrama.

En este ejemplo, los datos deben pasar a través del dispositivo de encaminamiento Y antes de alcanzar su destino. Por tanto, el dispositivo de encaminamiento X construye una nueva trama incorporando a la unidad de datos IP la cabecera y cola de retransmisión de tramas. La cabecera de retransmisión de tramas indica una conexión lógica con el dispositivo de encaminamiento Y; cuando esta trama llega al dispositivo de encaminamiento Y, se eliminan la cabecera y la cola. El dispositivo de encaminamiento determina que esta unidad de datos IP va dirigida a B, que está conectado directamente a la red a la cual está conectado el dispositivo de encaminamiento. Éste, por tanto, construye una trama con la dirección destino de la capa 2 de B y la envía en la LAN 2. Finalmente, los datos llegan a B, donde son eliminadas las cabeceras LAN e IP.

En cada dispositivo de encaminamiento, antes de que se reenvíen los datos, se podría necesitar fragmentar la unidad de datos para acomodarlos a la red de salida si en ésta hay un tamaño máximo de paquete inferior. La unidad de datos es partida en dos o más fragmentos, cada uno de los cuales constituirá una unidad de datos IP independiente. Cada nueva unidad de datos se integra en un paquete de la capa inferior y se coloca en cola para su transmisión. El dispositivo de encaminamiento podría también limitar la longitud de sus colas para cada red a la que está conectado para evitar que una red lenta perjudique a una rápida. Una vez que se alcanza el límite de la cola, las unidades de datos adicionales se descartan.

El proceso descrito antes continúa a través de tantos dispositivos de encaminamiento como necesite la unidad de datos para alcanzar su destino. Como con un dispositivo de encaminamiento, el sistema final destino recupera la unidad de datos IP a partir de los fragmentos obtenidos de la red.

Si ha habido fragmentación, el módulo IP en el sistema final destino almacena temporalmente los datos que llegan hasta que el bloque original de datos pueda ser totalmente reensamblado. Después, este bloque de datos se pasa a la capa superior del sistema final.

Este servicio ofrecido por un protocolo de interconexión es del tipo no fiable. Esto es, el protocolo de interconexión no garantiza que todos los datos se entreguen al destino ni que los datos que se entregan lleguen en el orden adecuado. Es responsabilidad de la capa superior (por ejemplo, TCP) tratar los errores que ocurran. Esta técnica proporciona un alto grado de flexibilidad.

Con esta forma de abordar el protocolo de interconexión, cada unidad de datos se pasa de dispositivo de encaminamiento a dispositivo de encaminamiento para ir de la fuente al destino. Puesto que la entrega no se garantiza, no hay ningún requisito particular de fiabilidad en cualquiera de las redes. Así, el protocolo funcionará con cualquier combinación de tipos de red. Ya que la secuencia de entrega no está garantizada, las unidades de datos sucesivas pueden seguir diferentes caminos a través del conjunto de redes. Esto le permite al protocolo reaccionar frente a la congestión y los fallos en las redes cambiando las rutas.

Aspectos a resolver en una interred no orientada a conexión

Una vez descripto brevemente el funcionamiento de una interconexión entre redes controlada por IP, se puede examinar algunas cuestiones de diseño con un mayor detalle. Éstas son:

- ✓ Encaminamiento.
- ✓ Tiempo de vida de los datagramas.
- ✓ Segmentación y reensamblado.
- ✓ Control de errores.
- ✓ Control de flujo.

Encaminamiento

El encaminamiento se efectúa por medio del mantenimiento de una tabla de encaminamiento en cada dispositivo de encaminamiento y en cada sistema final. En esta tabla se especifica, para cada red posible de destino, el siguiente dispositivo de encaminamiento al que se deberá enviar el datagrama internet.

La tabla de encaminamiento puede ser estática o dinámica. Una tabla estática puede contener rutas alternativas por si algún dispositivo de encaminamiento no está disponible. Una tabla dinámica es más flexible a la hora de enfrentarse a condiciones de error y congestión. En Internet, por ejemplo, cuando un dispositivo de encaminamiento se desconecta, todos sus vecinos emitirán un informe de estado, permitiendo a otros dispositivos de encaminamiento y estaciones que actualicen sus tablas de encaminamiento. Es posible utilizar un esquema similar para el control de congestión. Este último caso es particularmente importante a causa de las diferencias de capacidad entre las redes locales y las de área amplia. En el próximo capítulo se discute los protocolos de encaminamiento o ruteo.

Las tablas de encaminamiento también se pueden utilizar para ofrecer otros servicios de interconexión entre redes, como seguridad y prioridad. Por ejemplo, las redes individuales se podrían clasificar para gestionar datos de hasta un nivel de seguridad dado. El mecanismo de encaminamiento debe asegurar que a los datos de cierto nivel de seguridad no se les permita pasar a través de redes no acreditadas para gestionar tales datos.

Otra técnica de encaminamiento es el encaminamiento en el origen. La estación fuente especifica la ruta mediante la inclusión de una lista secuencial de dispositivos de encaminamiento en el datagrama. Esto, de nuevo, podría ser útil por motivos de seguridad o prioridad.

Finalmente, mencionaremos un servicio relacionado con el encaminamiento: el registro de la ruta. Para registrar la ruta, cada dispositivo de encaminamiento incorpora su dirección internet a una lista de direcciones que lleva el datagrama. Esta característica es útil con el objetivo de realizar operaciones de comprobación y depuración.

Tiempo de vida de los datagramas

Si se utiliza un encaminamiento dinámico o alternativo, existe la posibilidad de que un datagrama viaje indefinidamente a través del conjunto de redes. Esto no es aconsejable por dos razones. Primero, un datagrama circulando indefinidamente consume recursos. Segundo, como se verá cuando se analice el protocolo TCP, un protocolo de transporte depende de la existencia de un límite en la vida de un datagrama. Para evitar estos problemas, cada datagrama se puede marcar con un tiempo de vida. Una vez que ha transcurrido este tiempo de vida, el datagrama se descarta.

Una forma sencilla de implementar esta función es usar un contador de saltos. Cada vez que un datagrama pasa a través de un dispositivo de encaminamiento, se

reduce en 1 (uno) el contador. Alternativamente, el tiempo de vida podría ser una medida de tiempo auténtica. Esto requiere que los dispositivos de encaminamiento conozcan de alguna manera el tiempo transcurrido desde que el datagrama o un fragmento cruzó por última vez un dispositivo de encaminamiento, para conocer cuánto tiene que reducir el campo de tiempo de vida. Esto requeriría algún mecanismo global de sincronización. La ventaja de usar una medida real de tiempo es que se puede utilizar en el algoritmo de reensamblado descrito a continuación.

Fragmentación y reensamblado

Las redes individuales en un conjunto de redes pueden especificar tamaños máximos de paquetes diferentes. Sería ineficiente e inmanejable tratar de imponer un tamaño de paquete uniforme a través de las redes. Así, ocurre que los dispositivos de encaminamiento pueden necesitar fragmentar los datagramas de entrada en unidades más pequeñas, llamadas segmentos o fragmentos, antes de transmitirlos en la red siguiente.

Si los datagramas se pueden fragmentar (quizá más de una vez) durante sus viajes, la cuestión que surge es dónde se deben reensamblar. La solución más fácil es realizar el reensamblado solamente en el destino. La principal desventaja de este método es que los fragmentos sólo se pueden hacer más pequeños a medida que los datos se mueven a través del conjunto de redes. Esto puede perjudicar la eficiencia de algunas redes. Por otra parte, si los dispositivos de encaminamiento intermedios pueden reensamblar, aparecen las siguientes desventajas:

1. Se requieren grandes memorias temporales en los dispositivos de encaminamiento y existe el riesgo de que todo el espacio de memoria temporal se use para almacenar datagramas parciales.
2. Todos los fragmentos de un datagrama deben pasar a través del mismo dispositivo de encaminamiento de salida. Esto imposibilita el uso del encaminamiento dinámico.

En IP, los fragmentos de los datagramas se reensamblan en el sistema final destino. La técnica de fragmentación de IP usa los siguientes campos en la cabecera IP:

- ✓ Identificador de la unidad de datos (ID).
- ✓ Longitud de los datos.
- ✓ Desplazamiento.
- ✓ Indicador de más datos.

El ID es un medio de identificar de forma única un datagrama originado en el sistema final. En IP, el ID consta de las direcciones fuente y destino, un identificador del protocolo que genera los datos (por ejemplo, TCP) y una identificación suministrada por el protocolo. La longitud de los datos indica la longitud del campo de datos de usuario,

expresado en octetos, y el campo desplazamiento es la posición de un fragmento de los datos de usuario en el campo de datos en el datagrama original, en múltiplos de 64 bits.

El sistema final origen crea un datagrama con una longitud de datos igual a la longitud entera del campo de datos, con desplazamiento = 0 y el indicador de más datos establecido a 0 (falso).

Para fragmentar un datagrama grande en dos piezas, un módulo IP en un dispositivo de encaminamiento realiza las siguientes tareas:

1. Crea dos nuevos datagramas y copia los campos de la cabecera del datagrama original en los datagramas nuevos.
2. Divide el campo de datos de usuario en dos porciones aproximadamente iguales con límites de 64 bits, situando una porción en cada datagrama nuevo. La primera porción debe ser un múltiplo de 64 bits (8 octetos).
3. Establece la longitud de datos del primer datagrama a la longitud de los datos insertados y establece a 1 (cierto) el indicador de más datos. El campo desplazamiento no se cambia.
4. Establece la longitud de datos del segundo datagrama a la longitud de los datos insertados, y añade la longitud de la primera porción de datos dividida por 8 al campo desplazamiento. El indicador de más datos permanece igual.

Para reensamblar un datagrama debe haber suficiente espacio de memoria temporal en el momento de reensamblar. Conforme los fragmentos con el mismo ID llegan, se insertan los campos de datos en la posición correcta en la memoria temporal hasta que el campo datos entero se reensambla, lo que se consigue cuando existe un conjunto contiguo de datos comenzando con un desplazamiento de cero y terminando con datos de un segmento con el indicador de más datos puesto a falso.

Una eventualidad con la que hay que enfrentarse es que uno o más fragmentos no hayan llegado: el servicio IP no garantiza la entrega. Se necesitan algunos métodos para decidir abandonar una tentativa de reensamblado con objeto de liberar espacio de memoria temporal. Comúnmente se utilizan dos técnicas:

- ✓ La primera asigna un tiempo de vida de reensamblado al primer segmento que llega. Éste se regula con un reloj en tiempo real local asignado por la función de reensamblado y decrementado mientras los fragmentos del datagrama original se van almacenando en la memoria temporal. Si el tiempo expira antes de completar el reensamblado, los fragmentos recibidos se descartan.
- ✓ Una segunda técnica consiste en hacer uso del tiempo de vida del datagrama, que es parte de la cabecera de cada uno de los fragmentos entrantes. El campo de vida es decrementado por la función de reensamblado. Como con la primera técnica, si el tiempo de vida expira antes de completar el reensamblado, los fragmentos recibidos se descartan.

Control de errores

El sistema de interconexión entre redes no garantiza la distribución satisfactoria de cada datagrama. Cuando un dispositivo de encaminamiento descarta un datagrama, éste debería intentar devolver alguna información al origen, si es posible. La entidad origen que usa el protocolo Internet puede emplear esta información para modificar su estrategia de transmisión y notificarlo a las capas superiores. Para informar que un datagrama específico ha sido descartado, se necesita algún medio de identificar datagramas.

Los datagramas se pueden descartar por una serie de razones, incluyendo la expiración del tiempo de vida, la existencia de congestión y de error en la suma de comprobación. En este último caso, no es posible realizar una notificación, ya que el campo de la dirección fuente puede haber sido dañado.

Control de flujo

El control de flujo en la interconexión permite a los dispositivos de encaminamiento y/o las estaciones receptoras limitar la razón a la cual se reciben los datos. Para un servicio no orientado a conexión como el que estamos describiendo, los mecanismos de control de flujo son limitados. La mejor aproximación parece ser enviar paquetes de control de flujo, solicitando una reducción del flujo de datos a otros dispositivos de encaminamiento y a las estaciones fuente. El protocolo ICMP implementa entre otras esa función.

6.3. Protocolo IP (Internet Protocol)

A continuación, se describe el protocolo IP versión 4, definido oficialmente en el RFC 791. Al momento de escribir estas notas existe una gran migración hacia IP versión 6 (principalmente como respuesta al faltante de direcciones IP públicas de la versión 4). Sin embargo, IPv4 está aún bastante vigente.

El protocolo Internet (IP) es parte del conjunto de protocolos TCP/IP y es el protocolo de interconexión de redes más utilizado. Como con cualquier protocolo estándar, IP se especifica en dos partes:

- ✓ La interfaz con la capa superior (por ejemplo, TCP), especificando los servicios que proporciona IP.
- ✓ El formato real del protocolo y los mecanismos asociados.

6.3.1. Servicios IP

Los servicios a proporcionar entre las capas de protocolos adyacentes (por ejemplo, entre IP y TCP) se expresan en términos de primitivas y parámetros. Una

primitiva especifica la función que se va a ofrecer y los parámetros se utilizan para pasar datos e información de control. La forma real de una primitiva depende de la implementación. Un ejemplo es una llamada a subrutina.

IP proporciona dos primitivas de servicio en la interfaz con la capa superior. La primitiva Send (envío) se utiliza para solicitar la transmisión de una unidad de datos. La primitiva Deliver (entrega) utiliza IP para notificar a un usuario la llegada de una unidad de datos. Los parámetros asociados a estas dos primitivas son los siguientes:

- ✓ Dirección origen: dirección global de red de la entidad IP que envía la unidad de datos.
- ✓ Dirección destino: dirección global de red de la entidad IP de destino.
- ✓ Protocolo: entidad de protocolo receptor (un usuario IP, como por ejemplo TCP))
- ✓ Indicadores del tipo de servicio: utilizado para especificar el tratamiento de la unidad de datos en su transmisión a través de los componentes de las redes.
- ✓ Identificador: utilizado en combinación con las direcciones origen y destino y el protocolo usuario para identificar de una forma única a la unidad de datos. Este parámetro se necesita para reensamblar e informar de errores.
- ✓ Indicador de no fragmentación: indica si IP puede fragmentar los datos para realizar el transporte.
- ✓ Tiempo de vida: medido en segundos.
- ✓ Longitud de los datos: longitud de los datos que se transmiten.
- ✓ Datos de opción: opciones solicitadas por el usuario IP.
- ✓ Datos: datos de usuario que se van a transmitir.

Hay que destacar que los parámetros: identificador, indicador de no fragmentación y tiempo de vida, los cuales se encuentran presentes en la primitiva Send, no lo están en la primitiva Deliver. Estos tres parámetros proporcionan instrucciones a IP que no son de la incumbencia del usuario IP destino.

El parámetro de opciones permite futuras extensiones y la inclusión de parámetros que normalmente no se invocan. Las opciones actualmente definidas son:

- ✓ Seguridad: permite que se incorpore una etiqueta de seguridad al datagrama.
- ✓ Encaminamiento en el origen: constituye una lista secuencial de direcciones de dispositivos de encaminamiento que especifica la ruta a seguir. El encaminamiento puede ser estricto (sólo los dispositivos de encaminamiento identificados pueden ser visitados) o débil (pueden visitarse otros dispositivos de encaminamiento intermedios).
- ✓ Registro de la ruta: se reserva un campo para registrar la secuencia de dispositivos de encaminamiento visitados por el datagrama.

- ✓ Identificación de la secuencia: identifica recursos reservados utilizados para un servicio de secuencia. Este servicio proporciona un tratamiento especial del tráfico volátil periódico (por ejemplo, voz).
- ✓ Marcas de tiempo: la entidad IP origen y algunos o todos los dispositivos de encaminamiento intermedios incorporan una marca temporal (con una precisión de milisegundos) a las unidades de datos conforme van pasando por ellos.

6.3.2. Protocolo IP

El protocolo entre entidades IP se describe mejor mediante la referencia al formato del datagrama IP mostrado en la Figura 6.3.2.1. Los campos son los siguientes:

- ✓ Versión (4 bits): indica el número de la versión del protocolo, para permitir la evolución del mismo; el valor es 4.
- ✓ Longitud de la cabecera Internet (IHL, Internet Header Length) (4 bits): longitud de la cabecera expresada en palabras de 32 bits. El valor mínimo es de cinco, correspondiente a una longitud de la cabecera mínima de 20 octetos.
- ✓ Tipo de servicio (8 bits): especifica los parámetros de fiabilidad, prioridad, retardo y rendimiento. Este campo se utiliza muy raramente; su interpretación ha sido sustituida recientemente. Los primeros 6 bits del campo son denominados ahora campo de servicios diferenciados (DS, Differentiated Services). Los 2 bits restantes están reservados para un campo de notificación explícita de congestión (ECN), actualmente en fase de estandarización. El campo ECN proporciona una señalización explícita de congestión de una manera similar a la discutida para retransmisión de tramas.
- ✓ Longitud total (16 bits): longitud total del datagrama, en octetos.
- ✓ Identificador (16 bits): un número de secuencia que, junto a la dirección origen y destino y el protocolo usuario, se utiliza para identificar de forma única un datagrama. Por tanto, el identificador debe ser único para la dirección origen del datagrama, la dirección destino y el protocolo usuario durante el tiempo en el que el datagrama permanece en la red.
- ✓ Indicadores (3 bits): solamente dos de estos tres bits están actualmente definidos. El bit de «más datos» se utiliza para la fragmentación y el reensamblado como se ha expuesto previamente.
- ✓ El bit de «no fragmentación» prohíbe la fragmentación cuando es 1. Este bit puede ser útil si se conoce que el destino no tiene capacidad de reensamblar fragmentos. Sin embargo, si este bit vale 1, el datagrama se descartará si se excede el tamaño máximo de una red en la ruta. Por tanto, cuando el bit vale 1, es aconsejable utilizar encaminamiento desde el origen para evitar redes con tamaño de paquete máximos pequeños.

- ✓ Desplazamiento del fragmento (13 bits): indica el lugar donde se sitúa el fragmento dentro del datagrama original, medido en unidades de 64 bits. Esto implica que todos los fragmentos excepto el último contienen un campo de datos con una longitud múltiplo de 64 bits.
- ✓ Tiempo de vida (8 bits): especifica cuánto tiempo, en segundos, se le permite a un datagrama permanecer en la red. Cada dispositivo de encaminamiento que procesa el datagrama debe reducir este campo al menos en una unidad, de forma que el tiempo de vida es de alguna forma similar a una cuenta de saltos.
- ✓ Protocolo (8 bits): identifica el protocolo de la capa de red inmediatamente superior que va a recibir el campo de datos en el destino; así, este campo sirve para identificar el siguiente tipo de cabecera presente en el paquete después de la cabecera IP.
- ✓ Suma de comprobación de la cabecera (16 bits): un código de detección de errores aplicado solamente a la cabecera. Ya que algunos campos de la cabecera pueden cambiar durante el viaje (por ejemplo, el tiempo de vida y los campos relacionados con la segmentación), este valor se verifica y recalcula en cada dispositivo de encaminamiento. El campo suma de comprobación es el complemento a uno de la suma complemento a uno de todas las palabras de 16 bits en la cabecera. Por motivos de cálculo, este campo se inicializa a sí mismo a un valor de todo cero.
- ✓ Dirección de origen (32 bits): codificada para permitir una asignación variable de bits para especificar la red y el sistema final conectado a la red especificada, como se discute posteriormente.
- ✓ Dirección destino (32 bits): igual que el campo anterior.
- ✓ Opciones (variable): contiene las opciones solicitadas por el usuario que envía los datos.
- ✓ Relleno (variable): se usa para asegurar que la cabecera del datagrama tiene una longitud múltiplo de 32 bits.
- ✓ Datos (variable): el campo de datos debe tener una longitud múltiplo de 8 bits. La máxima longitud de un datagrama (campo de datos más cabecera) es de 65.535 octetos.

Figura 6.3.2.1: Cabecera protocolo IP

6.3.3. Direcciones IP

Los campos dirección origen y destino en la cabecera IP contienen cada uno una dirección internet global de 32 bits que, generalmente, consta de un identificador de red y un identificador de computador.

Clases de red

La dirección está codificada para permitir una asignación variable de bits para especificar la red y el computador, como se muestra en la Figura 6.3.3.1. Este esquema de codificación proporciona flexibilidad al asignar las direcciones a los computadores y permite una mezcla de tamaños de red en un conjunto de redes. Existen tres clases principales de redes que se pueden asociar a las siguientes condiciones:

- ✓ Clase A: pocas redes, cada una con muchos computadores.
- ✓ Clase B: un número medio de redes, cada una con un número medio de computadores.
- ✓ Clase C: muchas redes, cada una con pocos computadores.

En un entorno particular, podría ser mejor utilizar todas las direcciones de una misma clase. Por ejemplo, en un conjunto de redes de una entidad, consistente en un gran número de redes de área local departamentales, podría ser necesario usar direcciones de clase C exclusivamente. Sin embargo, el formato de las direcciones es tal que es posible mezclar las tres clases de direcciones en el mismo conjunto de redes; esto es lo que se hace en el caso de la misma Internet. En el caso de un conjunto de redes formado por pocas redes grandes, muchas redes pequeñas y algunas redes de tamaño mediano, es apropiado utilizar una mezcla de clases de direcciones.

Las direcciones IP se escriben normalmente en lo que se llama notación punto decimal, utilizando un número decimal para representar cada uno de los octetos de la dirección de 32 bits. Por ejemplo, la dirección IP 11000000 11100100 00010001 00111001 se escribe como 192.228.17.57.

Obsérvese que todas las direcciones de red de clase A empiezan con un 0 binario. Las direcciones de red con el primer octeto puesto a 0 (en binario 00000000) o que sea 127 (en binario 01111111) están reservadas. Por tanto, existen 126 números de red potenciales de clase A en los cuales su primer octeto en formato punto decimal está en el rango de 1 a 126. Las direcciones de red de clase B comienzan con un número binario 10, de forma que su primer número decimal está entre 128 y 191 (en binario entre 10000000 y 10111111). El segundo octeto también forma parte de la dirección de clase B, de forma que existen 2^{14}=16.384 direcciones de clase B. Para las direcciones de clase C, el primer número decimal va de 192 a 223 (de 11000000 a 11011111). El número total de direcciones de clase C es de 2^{21}=2.097.152.

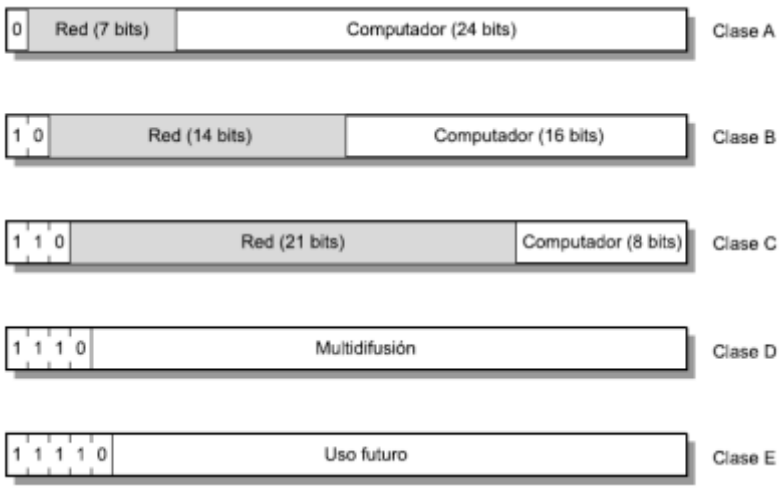

Figura 6.3.3.1: Formato de una dirección IP

Subredes y máscaras de subred

El concepto de subred fue introducido como una solución para el siguiente problema. Considere un conjunto de redes que incluye una o más WAN y un determinado número de sitios, cada uno de ellos con un determinado número de LAN. Nos gustaría tener una complejidad arbitraria de estructuras de LAN interconectadas dentro de la organización, aislando al resto del conjunto de redes frente a un crecimiento explosivo en el número de redes y la complejidad en el encaminamiento. Una solución a este problema es asignar a todas las LAN en un sitio un único número de red.

Desde el punto de vista del resto del conjunto de redes, existe una única red en ese sitio, lo cual simplifica el direccionamiento y el encaminamiento. Para permitir que los dispositivos de encaminamiento internos al sitio funcionen correctamente, a cada LAN se le asigna un número de subred. La parte computador en la dirección internet se divide en un número de subred y un número de computador para acomodar este nuevo nivel de direccionamiento.

Dentro de una red dividida en subredes, los dispositivos de encaminamiento locales deben encaminar sobre la base de un número de red extendido consistente en la porción de red de la dirección IP y el número de subred. Las posiciones a nivel de bit que contienen este número de red extendido se indican mediante la máscara de dirección. El uso de esta máscara de dirección permite a un computador determinar si un datagrama de salida va destinado a otro computador en la misma LAN (entonces se envía directamente) o a otra LAN (se envía a un dispositivo de encaminamiento).

Se supone que se utiliza algún otro medio (por ejemplo, mediante la configuración manual) para crear las máscaras de dirección y darlas a conocer a los dispositivos de encaminamiento locales.

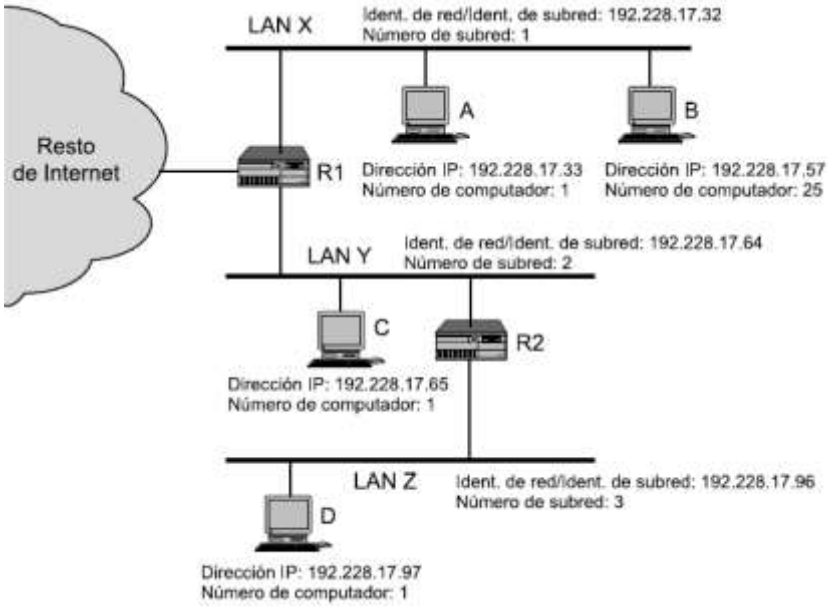

Figura 6.3.3.2: Uso de direcciones IP en subredes

La Tabla 6.3.3.3a muestra los cálculos que se realizan con la utilización de una máscara de subred. Obsérvese que el efecto de la máscara de subred es borrar la parte del campo de computador que indica el computador real en una subred. Lo que permanece es el número de red y el número de subred. La Figura 6.3.3.2 muestra un ejemplo de utilización de subredes. La figura muestra un complejo local consistente en tres LAN y dos dispositivos de encaminamiento. Para el resto del conjunto de redes este complejo es una red única con una dirección de clase C de la forma 192.228.17.x, donde los tres octetos más a la izquierda son el número de red y el octeto más a la derecha contiene un número de computador x. Ambos dispositivos de encaminamiento R1 y R2 se configuran con una máscara de subred con el valor 255.255.255.224 (véase la Tabla 6.3.3.4a). Por ejemplo, si un datagrama con una dirección destino 192.228.17.57 llega a R1 desde el resto del conjunto de redes o desde la LAN Y, R1 aplica la máscara de subred para determinar que esta dirección hace referencia a una dirección de la subred 1, la cual es la LAN X, y si es así enviarlo a la LAN X. De forma similar, si llega un datagrama con esa dirección destino a R2 desde la LAN Z, R2 aplica la máscara y determina a partir de su base de datos que el datagrama destinado a la subred 1 se debe enviar a R1. Los computadores también utilizan la máscara de subred para tomar decisiones de encaminamiento.

La máscara de subred por defecto para una clase de direcciones dada es una máscara nula (Tabla 6.3.3.4b), que produce el mismo número de red y de computador que en el caso de una dirección sin subredes.

Tabla 6.3.3.3: Direcciones IP y máscaras de subred

(a) Representaciones punto decimal y binaria de las direcciones IP y las máscaras de subred

	Representación binaria	Punto decimal
Dirección IP	11000000.11100100.00010001.00111001	192.228.17.57
Máscara de subred	11111111.11111111.11111111.11100000	255.255.255.224
Operación AND bit-a-bit de la dirección y la máscara (número de red/subred resultante)	11000000.11100100.00010001.00100000	192.228.17.32
Número de subred	11000000.11100100.00010001.001	1
Número de computador	00000000.00000000.00000000.00011001	25

(b) Máscaras de subred por defecto

	Representación binaria	Punto decimal
Máscara de clase A por defecto	11111111.00000000.00000000.00000000	255.0.0.0
Ejemplo de máscara de clase A	11111111.11000000.00000000.00000000	255.192.0.0
Máscara de clase B por defecto	11111111.11111111.00000000.00000000	255.255.0.0
Ejemplo de máscara de clase B	11111111.11111111.11111000.00000000	255.255.248.0
Máscara de clase C por defecto	11111111.11111111.11111111.00000000	255.255.255.0
Ejemplo de máscara de clase C	11111111.11111111.11111111.11111100	255.255.255.252

VLSM (Máscara de longitud variable, Variable Length Subnet Mask)

La subdivisión en subredes, o el uso de una Máscara de subred de longitud variable (VLSM), fue diseñada para maximizar la eficiencia del direccionamiento. Al identificar la cantidad total de hosts que utiliza la división tradicional en subredes, se asigna la misma cantidad de direcciones para cada subred.

Si todas las subredes tuvieran los mismos requisitos en cuanto a la cantidad de hosts, estos bloques de direcciones de tamaño fijo serían eficientes. Sin embargo, esto no es lo que suele suceder.

A diferencia del subneteo (subnetting) que genera una máscara común (fija) y cantidad de hosts iguales a todas las subredes, el proceso de VLSM toma una dirección de red o subred y la divide en subredes más pequeñas adaptando las máscaras según las necesidades de hosts de cada subred, generando una máscara diferente para las distintas subredes de una red. Esto permite no desaprovechar un gran número de direcciones, sobre todo en los enlaces seriales.

Hay varios factores a tener en cuenta a la hora de subnetear y trabajar con VLSM:

- ✓ El uso de VLSM solo es aplicable con los protocolos de enrutamiento sin clase (classless) RIPv2, OSPF, EIGRP, BGP4 e IS-IS.
- ✓ Al igual que en el subneteo, la cantidad de subredes y hosts está supeditada a la dirección IP de red o subred que nos otorguen.
- ✓ Es imposible comprender el proceso de obtención de VLSM si no se conoce fluidamente el proceso de subneteo común.

Para comprender su aplicación, se supone que se brinda un servicio de internet internacional y que LACNIC nos vendió el paquete de direcciones IP de red

53.0.0.0/8. Utilizando subneteo con VLSM se venderán bloques de direcciones a diferentes ISP´s locales, de acuerdo a la Tabla 6.3.3.4, para que ellos a su vez distribuyan las mismas.

Tabla 6.3.3.4: Requerimientos de direcciones IP públicas

Proveedores ISP	Cantidad de Direcciones Solicitadas
ISP 1	2.000.000
ISP 2	1.000.000
ISP 3	4.000.000
ISP 4	3.000.000
ISP 5	500.000

Con los requerimientos descriptos, se concluye que debemos entregar 10.500.00 direcciones. De esta forma se debe comprobar si el bloque asignado puede cubrir ese número de direcciones: al usar 8 bit para la máscara, quedan disponibles 2^{24} direcciones posibles, o sea un total 16.777.216 de direcciones. Se puede cubrir la necesidad.

Luego se debe ordenar de mayor a menor los requerimientos expresados en notación módulo 2:

1. 2^{23} = 8.388.608 Direcciones
2. 2^{22} = 4.194.304 Direcciones (para el ISP 3 y el ISP 4)
3. 2^{21} = 2.097.152 Direcciones (para el ISP 1)
4. 2^{20} = 1.048.576 Direcciones (para el ISP 2)
5. 2^{19} = 524.288 Direcciones (para el ISP 5)

Se comienza con el ISP 3 (el de mayor requerimiento):

La máscara de red adaptada, que va a quedar 255.192.0.0 = /10, permite 4 subredes (2^2 = 4) con 4.194.304 direcciones (2^{22} = 4.194.304) cada una. Figura 6.3.3.5

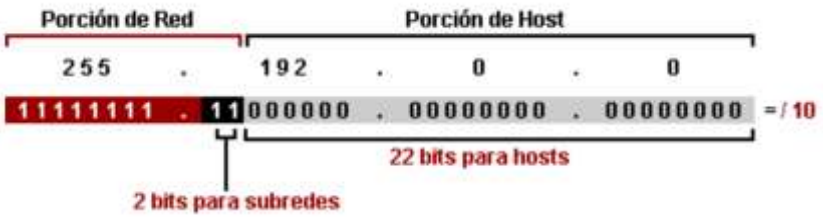

Figura 6.3.3.5: Red 255.192.0.0/10

Así se obtiene la "Subred 0" que es la 64.0.0.0 /10 y que va a ser para el ISP 3. Ahora se deben calcular las otras subredes que se generaron. Para obtener el "salto" entre subredes le restamos al número 256 el número de la máscara de subred adaptada: 256 - 192 = 64 y obtenemos las subredes restantes. Tabla 6.3.3.6

Tabla 6.3.3.6: Subredes a partir de la /10

Subred	Desde	Hasta	Direcciones		ISP	Máscara
0	64.0.0.0	64.63.255.255	4.194.304		3	/10
1	64.64.0.0	64.127.255.255	4.194.304		-	/10
2	64.128.0.0	64.191.255.255	4.194.304		-	/10
3	64.192.0.0	64.255.255.255	4.194.301		-	/10

Para el ISP 4 se sigue el mismo razonamiento, por lo tanto, si se vendió la subred 0 al ISP 3, se va a vender toda la subred 1 al ISP 4 (requirió 3.000.000 de direcciones).

A la hora de encontrar el bloque de datos para el ISP 1 (2.000.000 de direcciones), se hace lo siguiente:

Se utiliza la "Subred 3" cuya dirección IP es 64.128.0.0 /10. Se toma la máscara de red y se convierte a binario. Ya en binario la máscara, se busca en la tabla cuantos bits "0" son necesarios para obtener un mínimo de 2.000.000 direcciones. Con 21 bits "0" obtenemos 2.097.152 direcciones (2^{21} = 2.097.152), entonces el bit "0" restante se lo roba a la porción de host y se lo reemplaza por un bit "1". Figura 6.3.3.7

Figura 6.3.3.7: Red 64.128.0.0/10

La máscara 255.224.0.0 = /11, permite 2 subredes (2^1 = 2) con 2.097.152 direcciones (2^{21} = 2.097.152) cada una.

Así la dirección IP 64.128.0.0 /11 con 2.097.152 direcciones va a ser la dirección de la Red para el ISP 1. Como a esta red se la obtuvo a partir de la "Subred 2", se llamará "Subred 2A" y la otra subred generada se llamará "Subred 2B".

Se debe observar que el "salto" entre las subredes: 256 - 224 = 32, entonces la dirección de la "Subred 2B" va a ser 64.160.0.0 /11. Tabla 6.3.3.8

Tabla 6.3.3.8: Redes con máscara /10, /11 y /12

Subred	Desde	Hasta	Direcciones	ISP	Máscara
0	64.0.0.0	64.63.255.255	4.194.304	3	/10
1	64.64.0.0	64.127.255.255	4.194.304	4	/10
2A	64.128.0.0	64.159.255.255	2.097.152	1	/11
2B	64.160.0.0	64.191.255.255	2.097.152	-	/11
3	64.192.0.0	64.255.255.255	4.194.301	-	/10

Es el momento de encontrar el bloque de datos para el ISP 2 (1.000.000 de direcciones):

Se utilizará la "Subred 2B" que es la 64.160.0.0 /11 que permite 2.097.152 direcciones cuya máscara en binario es /21.

Para obtener el 1.000.000 de direcciones se observa en la tabla que necesitamos 20 bits en la porción de host (2^{20} = 1.048.576). Tenemos 21 bits en la porción de host, en consecuencia, se convertirá el bit "0" restante en un bit "1" y se hace parte de la porción de red. Figura 6.3.3.9

Figura 6.3.3.9: Selección de la red "Subred 2B"

La máscara 255.240.0.0 = /12, permite 2 subredes (2^1 = 2) con 1.048.576 direcciones cada una. Entonces la dirección de la "Subred 2B" 64.160.0.0 /12 con 1.048.576 direcciones va a ser la dirección del ISP 2. La otra subred creada la vamos a llamar "Subred 2C".

Para obtener el "salto" entre las subredes: 256 - 240 = 16, entonces la dirección de la "Subred 2C" va a ser 64.176.0.0 /12. Tabla 6.3.3.10

Tabla 6.3.3.10: Determinación de la red "Subred 2C"

Subred	Desde	Hasta	Direcciones	ISP	Máscara
0	64.0.0.0	64.63.255.255	4.194.304	3	/10
1	64.64.0.0	64.127.255.255	4.194.304	4	/10
2A	64.128.0.0	64.159.255.255	2.097.152	1	/11
2B	64.160.0.0	64.175.255.255	1.048.152	2	/12
2C	64.176.0.0	64.191.255.255	1.048.576	-	/12
3	64.192.0.0	64.255.255.255	4.194.301	-	/10

Para resolver el requerimiento del ISP 5 (500.000 de direcciones) se sigue el mismo procedimiento, dividiendo el bloque de direcciones a partir de la "Subred C". El resultado final es el siguiente (Tabla 6.3.3.11):

Tabla 6.3.3.11: Todas las subredes con máscara variable

Subred	Desde	Hasta	Direcciones	ISP	Máscara
0	64.0.0.0	64.63.255.255	4.194.304	3	/10
1	64.64.0.0	64.127.255.255	4.194.304	4	/10
2A	64.128.0.0	64.159.255.255	2.097.152	1	/11
2B	64.160.0.0	64.175.255.255	1.048.152	2	/12

2C	64.176.0.0	64.183.255.255	524.288	5	/13
2D	64.184.0.0	64.191.255.255	524.288	-	/13
3	64.192.0.0	64.255.255.255	4.194.301	-	/10

CIDR (Direccionamiento IP sin clases, Classless Inter-Domain Routing)

El protocolo CIDR, Classless Inter-Domain Routing (Encaminamiento inter-dominios sin clases), se introdujo en 1993. Este protocolo permite un uso más eficiente de las cada vez más escasas direcciones IPv4. CIDR usa máscaras de subred de longitud variable (VLSM) para asignar direcciones IP a subredes de acuerdo a las necesidades de cada subred.

Además, con el objetivo de reducir las tablas de rutas de los nodos principales de Internet, permite la "agregación de rutas". Por agregación de rutas se entiende sustituir en las tablas de un router las múltiples entradas de un conjunto de redes contiguas (que comparten la primera parte de la dirección y la misma pasarela) por una única dirección IP que englobe a todas las rutas hacia esas redes.

Para hacer posible la implementación de la agregación de rutas se requiere un direccionamiento más flexible que no tenga en cuenta el concepto de clases IP. Para ello CIDR permite utilizar máscaras a nivel de bit, que ya no están limitadas a la estructura de las clases. La máscara derivada de las clases se denomina ahora "máscara natural" o "por omisión".

Aunque en los comienzos de Internet, cuando las direcciones IP se adjudicaban según eran solicitadas y sin ningún tipo de organización, las direcciones contiguas podían pertenecer a usuarios en localizaciones geográfica muy distantes. En cambio, hoy en día se asignan bloques continuos a grandes proveedores de Internet o proveedores de tránsito (Internet troncal). Éstos a su vez destinan porciones de rangos contiguos a sus clientes, que son los proveedores regionales, y éstos a los proveedores locales, que dan finalmente acceso a los usuarios particulares. De esta manera, la asignación de direcciones en Internet refleja la situación geográfica y su topología. Por lo que es útil usar la agregación de rutas.

Por ejemplo, el rango de direcciones IP $\{194.0.0.0 - 195.255.255.255\}$ pertenece a Europa. Por tanto, la red 195.4.12.0 y la red 195.4.13.0 se alcanzan a través de los mismos routers intermedios. Sin embargo, mientras las direcciones 195.4.12.0 y 195.4.13.0 se interpreten como direcciones de clase C, requieren el uso de entradas independientes en las tablas de los routers. Para agregar las rutas a las redes 195.4.12.0 y 195.4.13.0 se utiliza ahora la máscara 255.255.0.0 y una única dirección IP, la 195.4.0.0, que incluye todas las direcciones del rango $\{194.4.0.0 - 195.4.255.255\}$. En realidad, se está creando una dirección de red mayor como si fuera de clase B dentro del "espacio de direcciones" correspondiente a la clase C. Esta forma de crear redes mayores que las impuestas por las clases se denomina "supernetting" (Figura 6.3.3.12).

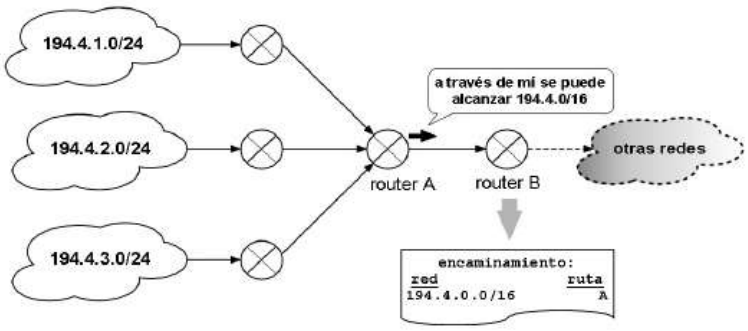

Figura 6.3.3.12: Reducción de entradas en las tablas de ruteo con CIDR

Los beneficios de aplicar "supernetting" usando CIDR se detallan a continuación:

- ✓ Hace más pequeñas las tablas de enrutamiento.
- ✓ Esto hace que las búsquedas en la tabla sean más rápidas.
- ✓ Vuelve más legible la información.
- ✓ Oculta información específica acerca de las redes sumarizadas.
- ✓ Las redes más pequeñas incluidas pueden caerse sin que esto afecte a la publicación del sumario.
- ✓ Los protocolos de enrutamiento dinámico pueden evitar consumir ancho de banda para las actualizaciones.

6.4. Protocolo ARP (Protocolo de Resolución de Direcciones, Address Resolution Protocol)

El protocolo ARP permite encontrar cuál es la dirección MAC correspondiente a una dirección IP. Para lograr el objetivo, el proceso consta de 4 pasos (Figura 6.4.1):

- ✓ ARP: solicitud. La computadora origen (la que requiere enviar la información) envía una trama de 'Petición ARP' a todas las máquinas de la red vía un broadcast. La solicitud contiene la IP del equipo del cual se requiere su MAC. Solo la computadora que tenga tal dirección IP, continuará con la siguiente etapa.
- ✓ ARP: verificación. El protocolo ARP de la computadora destino verifica quién es el equipo solicitante y registra sus datos (MAC e IP) para enviarle la información que requiere.
- ✓ ARP: respuesta. La computadora destino emite, para el equipo solicitante, una trama de 'Respuesta ARP' incorporando su dirección MAC e IP.
- ✓ ARP: registro. La computadora origen recibe la respuesta y guarda el resultado en una tabla, pudiendo emitir a partir de entonces datagramas IP.

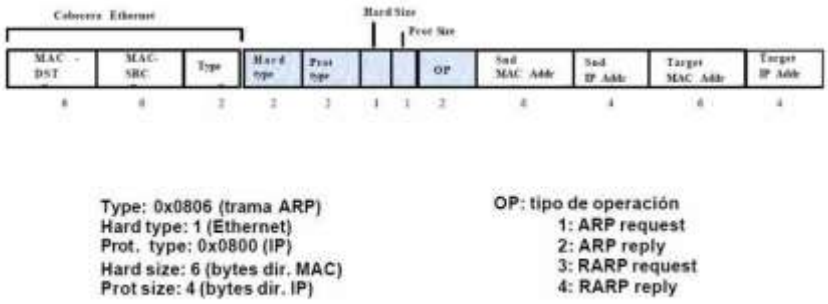

Figura 6.4.1: Trama ARP

6.5. Protocolo ICMP (Protocolo de Mensajes de Control de Internet, Internet Control Message Protocol)

El estándar IP especifica que una implementación que cumpla las especificaciones del protocolo debe también implementar ICMP (RFC 792). ICMP proporciona un medio para transferir mensajes desde los dispositivos de encaminamiento y otros computadores a un computador. En esencia, ICMP proporciona información de realimentación sobre problemas del entorno de la comunicación.

Algunas situaciones donde se utiliza son: cuando un datagrama no puede alcanzar su destino, cuando el dispositivo de encaminamiento no tiene la capacidad de almacenar temporalmente para reenviar el datagrama y cuando el dispositivo de encaminamiento indica a una estación que envíe el tráfico por una ruta más corta. En la mayoría de los casos, el mensaje ICMP se envía en respuesta a un datagrama, bien por un dispositivo de encaminamiento en el camino del datagrama o por el computador destino deseado.

Aunque ICMP está, a todos los efectos, en el mismo nivel que IP en el conjunto de protocolos TCP/IP, es un usuario de IP. Cuando se construye un mensaje ICMP, éste se pasa a IP, que encapsula el mensaje con una cabecera IP y después transmite el datagrama resultante de la forma habitual. Ya que los mensajes ICMP se transmiten en datagramas IP, no se garantiza su entrega y su uso no se puede considerar fiable.

La Figura 6.5.1 muestra el formato de varios tipos de mensajes ICMP. Todos los mensajes ICMP empiezan con una cabecera de 64 bits que consta de los siguientes campos:

- ✓ Tipo (8 bits): especifica el tipo de mensaje ICMP.
- ✓ Código (8 bits): se usa para especificar parámetros del mensaje que se pueden codificar en uno o unos pocos bits.
- ✓ Suma de comprobación (16 bits): suma de comprobación del mensaje ICMP entero. Se utiliza el mismo algoritmo de suma de comprobación que en IP.

- ✓ Parámetros (32 bits): se usa para especificar parámetros más largos.

A estos campos les siguen generalmente campos de información adicional que especifican aún más el contenido del mensaje. En aquellos casos en los que un mensaje ICMP se refiere a un datagrama previo, el campo de información incluye la cabecera IP entera más los primeros 64 bits del campo de datos del datagrama original. Esto permite al computador origen emparejar el mensaje ICMP que llega con el datagrama anterior. La razón de incorporar los primeros 64 bits del campo de datos es que permite al módulo IP en el computador determinar qué protocolo o protocolos del nivel superior estaban implicados. En particular, los primeros 64 bits incluirían una porción de la cabecera TCP u otra cabecera del nivel de transporte.

El mensaje destino inalcanzable cubre un cierto número de situaciones. Un dispositivo de encaminamiento puede devolver este mensaje si no sabe cómo alcanzar la red destino. En algunas redes, un dispositivo de encaminamiento conectado a una de estas redes puede ser capaz de determinar si un computador es inalcanzable y devolver este tipo de mensaje. El propio computador de destino puede devolver este mensaje si el protocolo de usuario o algún punto de acceso al servicio de un nivel superior no están alcanzables. Esto puede ocurrir si el correspondiente campo en la cabecera IP no tiene el valor correcto. Si el datagrama especifica una ruta dada por la fuente que no se puede usar, se devolverá un mensaje. Finalmente, si un dispositivo de encaminamiento debe fragmentar un datagrama, pero el indicador de no fragmentación está establecido, se devuelve también el mensaje *"destino inalcanzable".*

El mensaje de ralentización del origen proporciona una forma rudimentaria de control de flujo. Este mensaje lo pueden enviar tanto un dispositivo de encaminamiento como un computador destino a un computador origen solicitando que reduzca la tasa a la que envía el tráfico al destino. Cuando se recibe este tipo de mensaje, un computador origen debe disminuir la tasa de datos a la que envía el tráfico al destino especificado hasta que no reciba más mensajes de ralentización del origen. El mensaje de ralentización del origen lo puede generar tanto un dispositivo de encaminamiento como un computador que deba descartar datagramas debido a que su memoria temporal está llena. En este caso, el dispositivo de encaminamiento o el computador enviará un mensaje de ralentización del origen por cada datagrama que se descarta. Además, un sistema se puede anticipar a la congestión y enviar este tipo de mensaje cuando su memoria esté a punto de llegar a su capacidad máxima. En ese caso, el datagrama referido en el mensaje de ralentización del origen podrá ser entregado correctamente. Así, la recepción de un mensaje de ralentización no implica la entrega o la no entrega del datagrama correspondiente.

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.

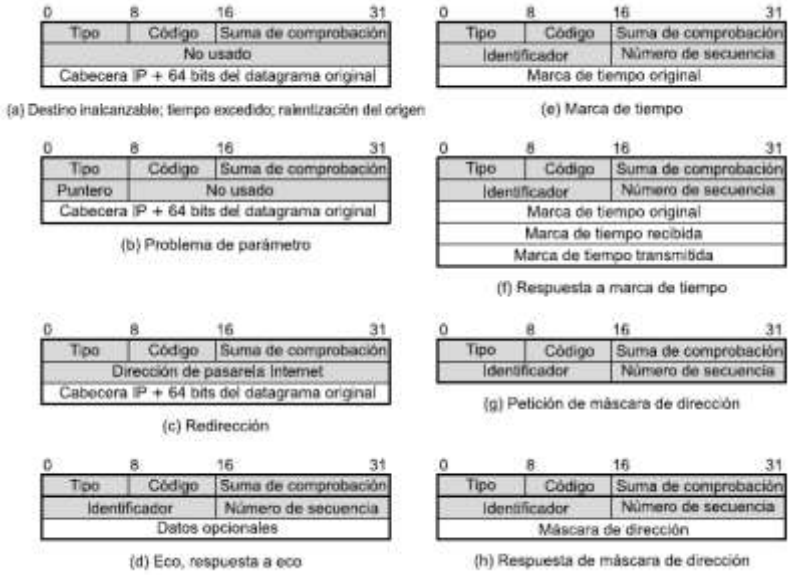

Figura 6.5.1: Formatos de datagrama ICMP

6.6. Protocolo IGMP (Protocolo de Administración de Grupos de Internet, Internet Group Management Protocol

Las estaciones y encaminadores utilizan el protocolo de gestión de grupos de Internet (IGMP, Internet Group Management Protocol), definido en el RFC 3376, para intercambiar información sobre la pertenencia a los grupos de multidifusión en una LAN. IGMP aprovecha la naturaleza de difusión de las LAN para proporcionar una técnica eficiente para el intercambio de información entre múltiples estaciones y encaminadores. En general, IGMP ofrece dos funciones principales:

1. El envío de mensajes desde las estaciones a los encaminadores para subscribirse y para abandonar grupos de multidifusión definidos por una dirección de multidifusión dada.

2. La comprobación periódica de los encaminadores sobre qué grupos de multidifusión interesan a qué estaciones.

Formato del mensaje IGMP

Todos los mensajes de IGMP se transmiten en datagramas IP. La versión actual define dos tipos de mensajes: *"consulta de pertenencia a grupo"* e *"informe de pertenencia a grupo"*.

Los mensajes de consulta de pertenencia a grupo (Membership Query) los envían los encaminadores de multidifusión. Existen tres subtipos: una consulta general, empleada para descubrir qué grupos tienen miembros en una red conectada al encaminador, una consulta de grupo específico, utilizada para averiguar si un grupo

determinado tiene algún miembro en una red conectada al encaminador, y una consulta de grupo y fuente específicos, utilizado para averiguar si alguno de los dispositivos conectados desea recibir los paquetes enviados a una dirección de multidifusión especificada, desde alguna de las fuentes especificadas en una lista. La Figura 6.6.1(a) muestra el formato del mensaje, que se compone de los siguientes campos:

- ✓ Tipo: indica el tipo de este mensaje.
- ✓ Tiempo de respuesta máximo: especifica el tiempo máximo de respuesta tolerado antes de enviar un informe de respuesta en unidades de 1/10 segundos.
- ✓ Suma de comprobación: un código de detección de errores, calculado como el complemento a uno de la suma de todas las palabras de 16 bits del mensaje. A efectos de cálculo, el campo de suma de comprobación se inicializa a cero. Éste es el mismo algoritmo de suma de comprobación que el calculado en IPv4.
- ✓ Dirección de grupo: cero para un mensaje de consulta general. Una dirección IP de grupo de multidifusión válida cuando se envía una consulta de grupo específico, o una consulta de grupo y fuente específicos.
- ✓ Indicador S: cuando su valor es uno, indica a todos los encaminadores de multidifusión que lo reciban que deben suprimir las actualizaciones habituales del temporizador que realizan tras recibir una consulta.
- ✓ Indicador de robustez del solicitante, o QRV (Querier's Robutness Variable): si su valor es distinto de cero, el campo QRV contiene el valor RV utilizado por el solicitante (es decir, el emisor de la consulta). Los encaminadores adoptan como su propio valor de RV el valor del RV de la consulta más recientemente recibida, a menos que haya sido cero, en cuyo caso los receptores utilizan un valor por defecto o un valor estático de configuración. El RV impone el número de veces que una estación retransmitirá un informe para asegurar que todos los encaminadores de multidifusión conectados lo reciben.
- ✓ Intervalo de consulta del consultante, o QQIC (Querier's Querier Interval Code): especifica el valor de QI empleado por el consultante, que es un temporizador para enviar múltiples consultas. Los encaminadores que no son consultantes en ese momento adoptan como valor propio de QI el valor de QI de la consulta más recientemente recibida, a menos que fuera cero, en cuyo caso usan el valor de QI por defecto.
- ✓ Número de fuentes: especifica cuántas direcciones de fuentes hay en la consulta. Este valor es diferente a cero sólo para la consulta de grupo y fuente específicos.
- ✓ Direcciones de fuentes: si el número de fuentes es N, entonces hay N direcciones de unidifusión de 32 bits adjuntas al mensaje.

Un mensaje de informe de pertenencia a grupo (Membership Report) se compone de los siguientes campos (Figura 6.6.1(b)):

- ✓ Tipo: indica el tipo de este mensaje.

- ✓ Suma de comprobación: un código de detección de errores, calculado como el complemento a uno de la suma de todas las palabras de 16 bits del mensaje.
- ✓ Número de entradas de grupo: especifica cuántas entradas de grupo están presentes en el informe.
- ✓ Entradas de grupo: si el número de entradas es M, entonces hay M direcciones de unidifusión de 32 bits adjuntas al mensaje.

Una entrada de grupo incluye los siguientes campos:

- ✓ Tipo de entrada: define el tipo de la entrada, como se describe posteriormente.
- ✓ Longitud de datos auxiliares: indica la longitud del campo de datos auxiliares, en palabras de 32 bits.
- ✓ Número de fuentes: especifica cuántas direcciones de fuentes hay en esta entrada.
- ✓ Dirección de multidifusión: la dirección IP de multidifusión a la que concierne la entrada.
- ✓ Direcciones de las fuentes: si el número de fuentes es N, entonces hay N direcciones de unidifusión de 32 bits adjuntas al mensaje.
- ✓ Datos auxiliares: información adicional concerniente a esta entrada. Actualmente, no existen valores definidos para los datos auxiliares.

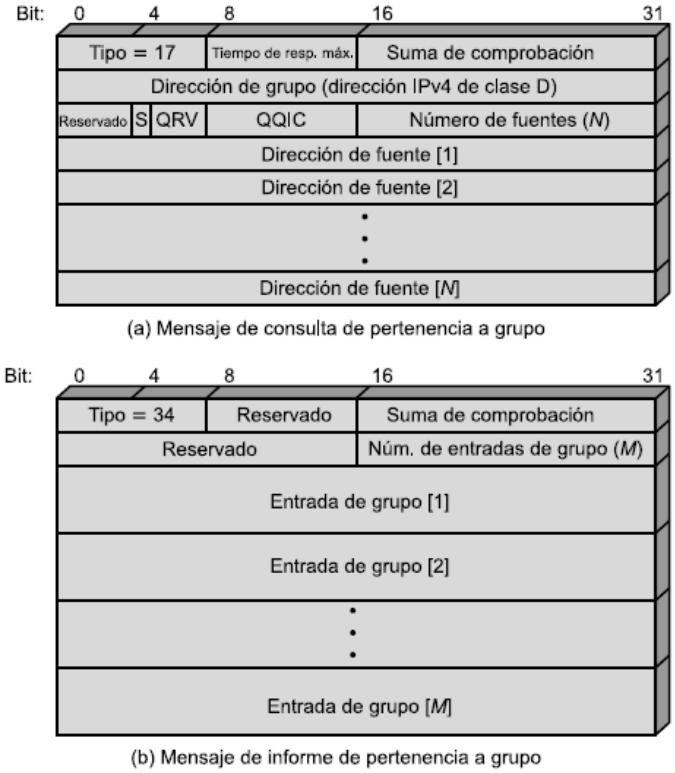

Figura 6.6.1: Formato de mensaje IGMP v3

Funcionamiento IGMP

El objetivo de que un computador utilice IGMP es darse a conocer como un miembro del grupo con una dirección de multidifusión concreta a otros computadores de la LAN y a todos los dispositivos de encaminamiento de la LAN. IGMPv3 introduce en las estaciones la capacidad de señalizar su pertenencia a un grupo con la posibilidad de filtrar fuentes. Una estación puede indicar que quiere recibir tráfico de todas las fuentes que envíen a un grupo exceptuando algunas fuentes específicas (a lo que se denomina modo EXCLUSIVO), o que quiere recibir tráfico sólo de algunas fuentes concretas de las que envían al grupo (modo INCLUSIVO). Para unirse a un grupo, una estación envía un mensaje IGMP de informe de pertenencia a grupo, en el que el campo de dirección de grupo sea la dirección de multidifusión del grupo. Este mensaje se envía en un datagrama IP con la misma dirección de multidifusión destino. En otras palabras, el campo de dirección de grupo del mensaje IGMP y el campo de dirección de destino de la cabecera del datagrama IP son el mismo. Todas las estaciones que sean en ese momento miembros de este grupo de multidifusión reciben el mensaje y descubren así la existencia del nuevo miembro del grupo. Cada dispositivo de encaminamiento conectado a la LAN debe atender todas las direcciones IP de multidifusión para poder recibir todos los informes.

IGMP se definió para operar con IPv4 y hace uso de direcciones de 32 bits. Las redes IPv6 requieren la misma funcionalidad. En lugar de definir una versión separada de IGMP para IPv6, su funcionalidad se ha incorporado en la nueva versión del protocolo de mensajes de control de Internet (ICMPv6). ICMPv6 incluye toda la funcionalidad de ICMPv4 e IGMP. Para dar soporte a la multidifusión, ICMPv6 incluye un mensaje de consulta de pertenencia a grupo y un mensaje de informe de pertenencia a grupo, que se utilizan en la misma forma que en IGMP.

6.7. IP de nueva generación: IPv6

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 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, receptores de televisión por cable, sensores de IoT, entre otros).
- ✓ 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.

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 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. Esto también hace que sea más fácil incorporar opciones adicionales.

- ✓ Autoconfiguración de direcciones: esta capacidad proporciona una asignación dinámica de direcciones IPv6.
- ✓ 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 multidifusión (multicast) con la incorporación de un campo de ámbito a las direcciones multicast.
- ✓ 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.

Cabecera IPv6

La cabecera IPv6 tiene una longitud fija de 40 octetos, que consta de los siguientes campos (Figura 6.7.1):

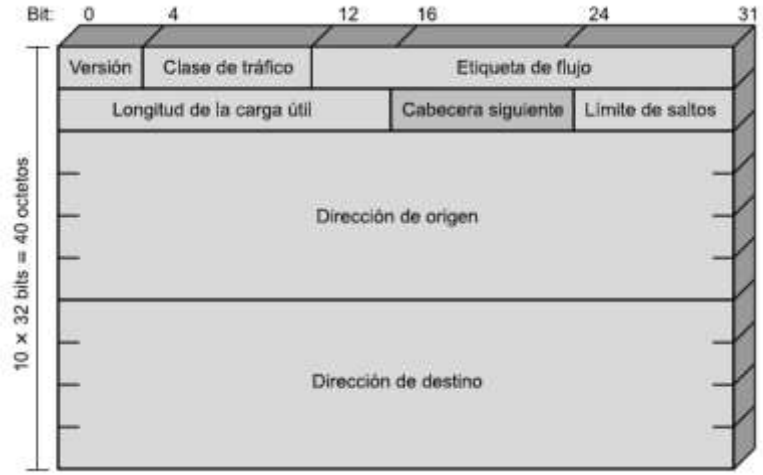

Figura 6.7.1: Cabecera paquete IPv6

- 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

- 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 reduce 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.

Direcciones IPv6

Las direcciones son representadas como una serie de campos de 16 bits, hexadecimales, separados por dos puntos (:) en el formato x:x:x:x:x:x:x:x. Un doble dos puntos (::), se permite uno solo por dirección, puede ser usado para comprimir sucesivos campos hexadecimales de ceros.

En IPv6 no existen las direcciones broadcast, su función es sustituida por las direcciones multicast. Existe una dirección de loopback (::1) similar a la de IPv4, y se agrega un nuevo tipo de dirección: la dirección no especificada(::), que indica la ausencia de una dirección IPv6. Esta dirección no debe ser asignada a ninguna interface ni debe ser usada como dirección destino en un paquete IPv6.

Las direcciones se asignan a las interfaces, pueden tener más de una dirección asignada, y no a los nodos. En IPv6, el concepto de máscara de red, es reemplazado por el concepto de prefijo. Éste es un número decimal que indica cuantos bits contiguos de más alto orden son usados para identificar la porción de red de la dirección. Una dirección IPv6 está compuesta de la siguiente manera (Figura 6.7.2):

dirección IPv6 / prefijo

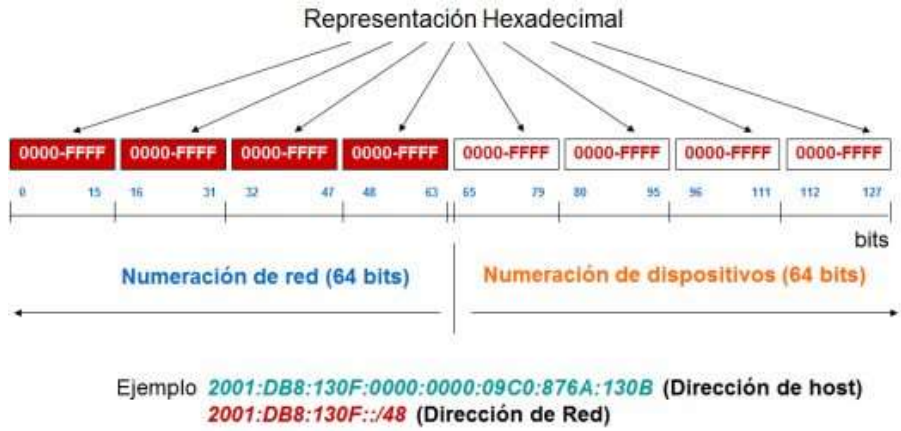

Figura 6.7.2: Representación de una dirección IP v6

Distintas formas de representar una dirección IPv6 se detallan a continuación:

2031:0000:130F:0000:0000:09C0:876A:130B

Podría representarse como 2031:0:130F::9C0:876A:130B

No podría ser 2031::130F::9C0:876A:130B

FF01:0:0:0:0:0:0:1 o lo que es igual a FF01::1

0:0:0:0:0:0:0:1 o lo que es igual a ::1

0:0:0:0:0:0:0:0 o lo que es igual a ::

Existen 3 tipos de direcciones:

- ✓ **Unicast:** Una dirección unicast es una dirección para una sola interface. Un paquete enviado a una dirección unicast es entregado, solamente, a la interface indicada por esa dirección. Las direcciones unicast IPv6 son similares a las direcciones IPv4 con CIDR (Classless Inter-Domain Routing). Los siguientes son algunos tipos de direcciones unicast:
  - ✓ **Aggregatable Global Address (Dirección global agregable)**

    Estas direcciones son utilizadas para el tráfico IPv6 a través de la Internet IPv6. Son similares a las direcciones unicast públicas utilizadas en IPv4 para comunicarse en Internet. Representan la parte más importante de la arquitectura de direcciones de IPv6. La Figura 6.7.3 muestra su estructura:

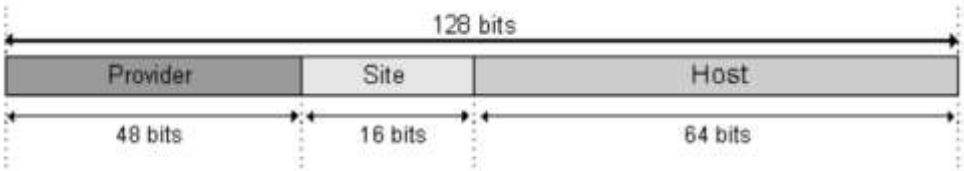

Figura 6.7.3: Aggregable Global Address

Provider: representa el prefijo de 48 bits cedido a una organización por algún proveedor autorizado.

Site: con un /48 cedido a una organización, ésta puede manejar hasta 65.535 subredes diferentes. El sitio usa estos bits para subnetting.

Host: esta parte, que representa los 64 bits de más bajo orden de la dirección, se llama Interface ID. Identifica una interface en un enlace. Debe ser único en ese enlace.

- ✓ **Unique Local Address (Dirección local exclusiva)**

Sustituyen a las direcciones locales del sitio (conjunto de redes de la organización) definidas en las especificaciones iniciales de IPv6 y cuya utilización ha sido desaconsejada en la especificación RFC 3879 del protocolo (Figura 6.7.4).

Las direcciones locales exclusivas equivalen al espacio de direcciones privadas de IPv4 (10.0.0.0/8, 172.16.0.0/16 - 172.31.0.0/16 y 192.168.0.0/24 - 192.168.255.0/24). Los encaminadores IPV6 no deben reenviar tráfico dirigido a direcciones locales fuera de la organización, por lo que las direcciones locales exclusivas no son accesibles desde las redes de otras organizaciones. Así pues, las redes privadas que no tienen una conexión directa a Internet pueden utilizar direcciones locales exclusivas.

En IPv6 un mismo nodo puede utilizar al mismo tiempo una dirección local exclusiva y una dirección global agregable. A diferencia de las direcciones locales del enlace, las direcciones locales exclusivas no se configuran automáticamente y se deben asignar mediante procesos de configuración de direcciones con control de estado (mediante servicios de asignación de configuración IP como DHCP) o sin control de estado (mediante procesos de configuración automática).

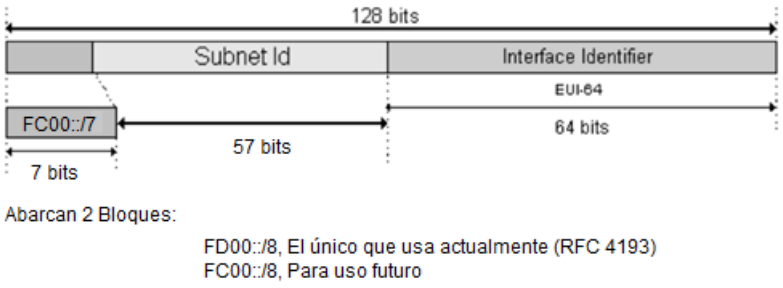

Figura 6.3.7.4: Unique Local Address

- ✓ **Link Local Address (Dirección local del enlace)**

Estas direcciones, identificadas por el FP = 1111 1110 10, son usadas para la autoconfiguración de direcciones, en funciones del Neighbor Discovery y

cuando no existe un router en el link. El prefijo para una dirección de link-local es FE80::/10 (Figura 6.7.5)

Cuando en una interface se habilita IPv6, la dirección de link-local es la primera dirección que se auto configura. Un nodo IPv6, no puede, no tener una dirección de este tipo asignada. Son similares a las direcciones APIPA en IPv4 (169.254.1.0 a 169.254.254.255)

El alcance de estas direcciones es el link. Un router nunca debería reenviar un paquete con una dirección de link-local, como dirección origen o destino, más allá del mismo.

Figura 6.7.5: Link Local Address

- ✓ **Anycast Address**

Identifica a un conjunto de interfaces, de tal manera, que al enviar un paquete a una dirección anycast es entregado a un solo miembro de ese grupo.

Estas direcciones son tomadas del espacio de direcciones unicast, es decir, que son sintácticamente indistinguibles una de las otras. Cuando se asignan a una interface se debe indicar explícitamente que la dirección es de tipo anycast.

- ✓ **Multicast Address**

Identifica a un conjunto de interface, de tal modo, que un paquete enviado a una dirección multicast es entregado a todas las interfaces del grupo. Se identifican por el FP (Format Prefix) = 1111 1111, por lo cual, comienzan con el prefijo FF00::/8. El campo Flags indica si una dirección multicast es permanente (0) o si es temporal (1). El campo Scope limita el alcance de un grupo multicast. (Figura 6.7.6).

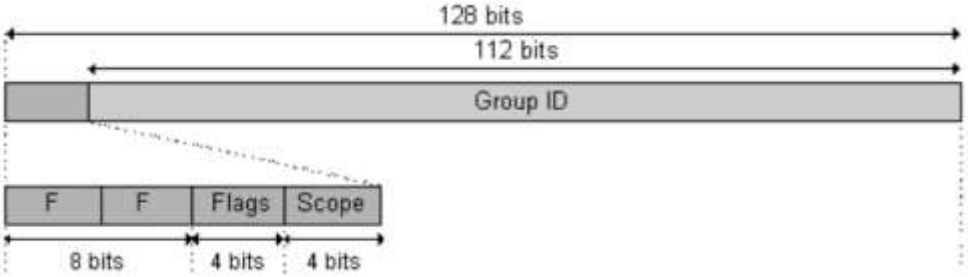

Figura 6.7.6: Direcciones IPv6 multicast

Entre las direcciones multicast asignadas (permanentes) se encuentran:

• FF02::1/8 (dirección multicast de todos los nodos del link-local)

• FF02::2/8 (dirección multicast de todos los routers del link-local).

Existe otro tipo de dirección multicast, utilizada por el Neighbor Discovery, que es la dirección multicast de nodo solicitado. Esta dirección permite, a los nodos, un eficiente método de consulta durante el proceso de resolución de direcciones.

El prefijo de este tipo de direcciones es FF02:0:0:0:0:1:FFxx:xxxx/104, donde los últimos 24 bits son los últimos 24 bits de la dirección unicast o anycast que se está intentando resolver. Son utilizadas en los mensajes Neighbor Solicitation del Neighbor Discovery. El siguiente gráfico 6.7.7 muestra la estructura de este tipo de direcciones:

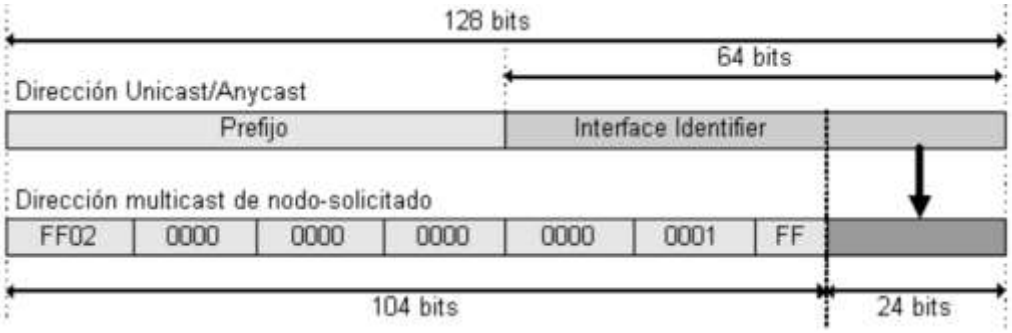

Figura 6.7.7: Dirección multicast de nodo solicitado

Todos los nodos (hosts y routers) se deben unir a las siguientes direcciones multicast:

- ✓ FF02::1/8
- ✓ FF02:0:0:0:0:1:FFxx:xxxx

Además, los routers se deben aceptar los mensajes enviados a la dirección FF02::2/8. Una interface su puede unir a más de una dirección multicast.