**Operación de un Router**

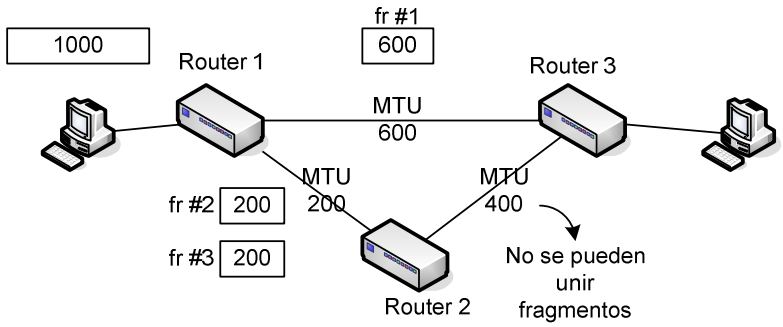
## 5.3 Segmentación y reensamblado

### 5.3.1 Introducción

En las redes de datos existen conexiones a nivel de enlaces muy variados, con protocolos diferentes y tamaños de información a transmitir muy disímiles. Por ejemplo las redes Ethernet emplean un tamaño de trama de 1518 bytes máximo, las redes ATM un tamaño de celdas de 53 bytes. La pregunta es como se hace para meter una trama Ethernet sobre una red ATM. Es aquí donde interviene en la operación la característica de sementaron.

Este tamaño máximo de información que puede transmitirse a nivel enlace datos se conoce como MTU **"Unidad Máxima de Transferencia"**

Dado el siguiente ejemplo, se observa claramente la imposibilidad de enviar una trama Ethernet de tamaño 1000 bytes sobre una red que emplea una MTU de 200 bytes y otra MTU de 600.




Por este motivo el router 1 debe fragmentar el datagrama original en dos fragmentos si ambos los enviara por la red con MTU de 600 bytes o formar 5 fragmentos si los enviara por la MTU de 200 bytes. En este ejemplo, enviamos un datagrama por la MTU de 600 bytes y enviamos dos datagramas por la MTU de 200 bytes. Como se puede apreciar cuando los dos datagramas de 200 bytes llegan el router 2, este no puede unirlos nuevamente ya que para hacer esta tarea requiere el fragmento 1 que va por otro camino.

De estos se deduce que la fragmentación siempre es decreciente, no habiendo inconvenientes en volver a armar los nuevos fragmentos, ya que se armaría en el destino la ultima fragmentación realizada, después seguirá con la inmediata anterior y así sucesivamente hasta llegar a la primera fragmentación realizada.

### 5.3.2 Ejemplo de Fragmentación en transmisión y reensamblado en recepción.

A continuación se muestra un ejemplo de fragmentación de un datagrama original y su correspondiente reensamblado en la recepción. Como se observa en la figura cada fragmento sigue caminos distintos lo que conlleva a que primero llegue el fragmento 2 y después el fragmento 1.

La fragmentación en la transmisión la realiza el router 1, ya que el tamaño máximo del datagrama original supera la MTU de 260 bytes fijada para

## Operación de un Router

la red de transmito. En la recepción el ordenamiento de los fragmentos se realiza en la capa de red, y se realiza en base al campo Offset y al bit de more como se indica en la figura 3. Ambos fragmentos se depositan en un buffer y en otra porción de memoria se van acomodando los fragmentos en función del campo Offset y a la longitud efectiva de datos. Siempre la longitud total incluye encabezado mas campo de datos, pero la segmentación o fragmentación se realiza sobre la longitud efectiva de los datos (no tiene en cuenta el encabezado).

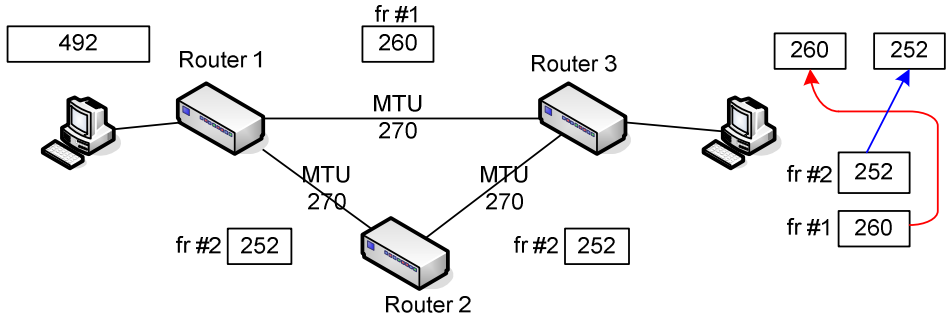
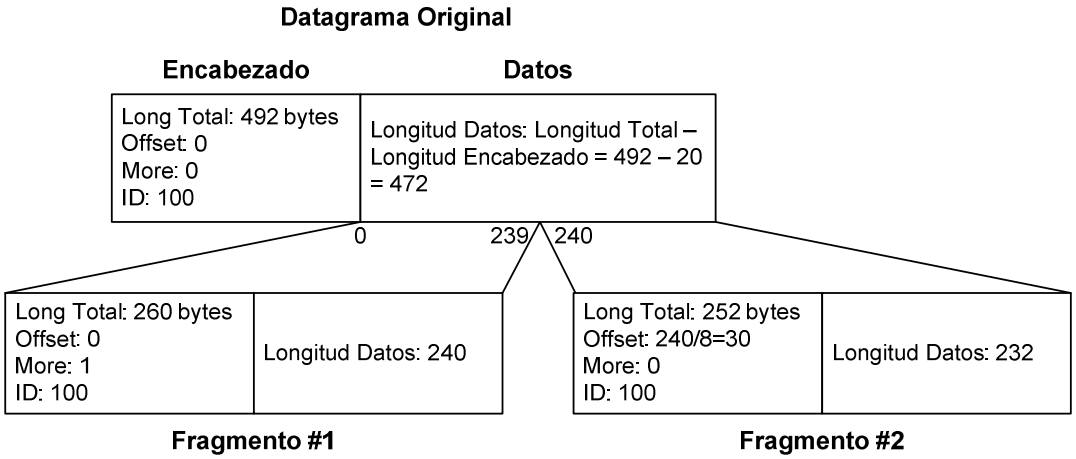



**Figura 1. Fragmentación y llegada fuera de orden de los fragmentos en la recepción.**

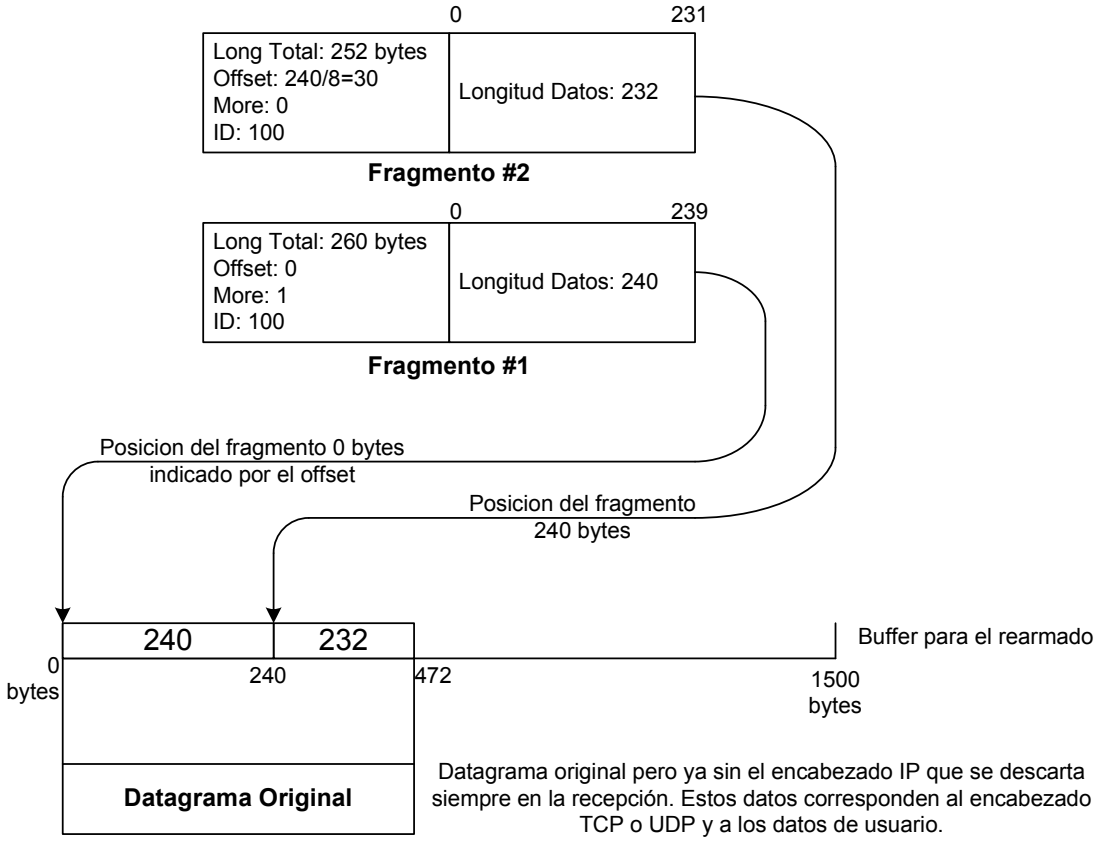
En la siguiente figura se muestra como el router 1 genera la fragmentación. Ambos fragmentos son los que viajan por la red de enrutadores hasta llegar al destino de manera desordenada, indicado de la forma




Durante el proceso de fragmentación en cada fragmento se copia gran parte de los campos del encabezado del datagrama original, en particular un campo que se conoce como identificador (ID). Esta campo permite reconocer que fragmentos son parte del mismo datagrama original, ya que todos esos fragmentos comparten el mismo ID que es único para cada datagrama transmitido por una PC.

**Operación de un Router**

El receptor almacena los fragmentos que poseen el mismo ID en una porción del buffer y usa otra porción de memoria buffer para rearmarlos siempre acomodando los fragmentos que tienen el mismo ID. Siempre el rearmado y el ordenamiento de los fragmentos se hace en la capa de red.




## 5.4 TTL

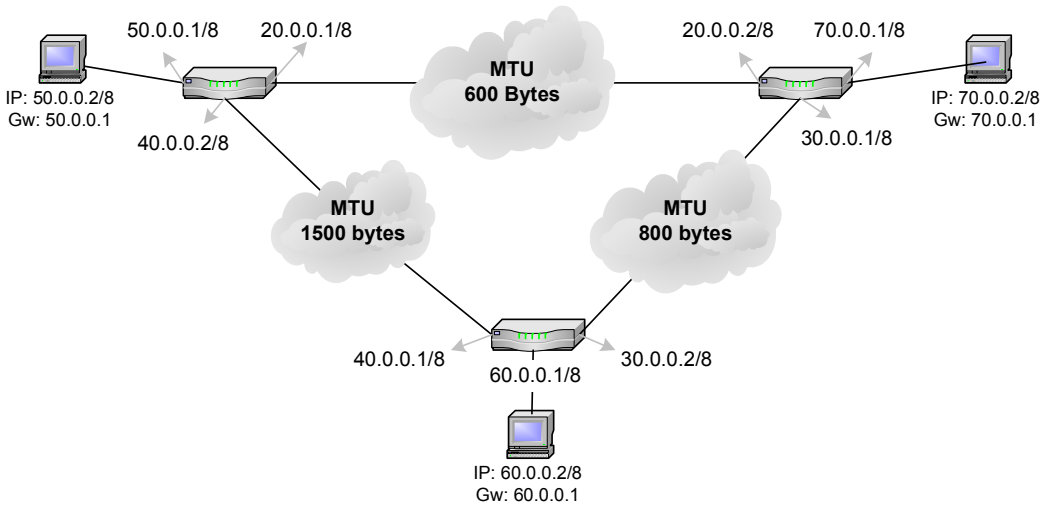
Es un contador de 8 bits que se decrementa en uno a medida que el datagrama va transitando por cada router. Cuando un router fija el contador a 0, este descarta el datagrama. Esto permite que un datagrama no quede circulando indefinidamente en la red cuando se dirige hacia un destino que no esta cargado explícitamente en la tabla de los routers que atraviesa el datagrama.

Analice el siguiente esquema y vera que si el destino es el IP 192.168.10.1, al aplicar la ruta por defecto en cada router el datagrama quedara circulando indefinidamente pasando de un router a otro. El datagrama circulara indefinidamente hasta que el TTL sea 0.

**Operación de un Router**

| Red | Mascara | Gateway |
|---|---|---|
| 0.0.0.0. | 0.0.0.0 | 20.0.0.2 |
| 50.0.0.0 | 255.0.0.0 | 50.0.0.1 |
| 20.0.0.0 | 255.0.0.0 | 20.0.0.1 |
| 40.0.0.0 | 255.0.0.0 | 40.0.0.2 |
| 60.0.0.0 | 255.0.0.0 | 40.0.0.1 |
| 30.0.0.0 | 255.0.0.0 | 40.0.0.1 |
| 70.0.0.0 | 255.0.0.0 | 20.0.0.2 |

| Red | Mascara | Gateway |
|---|---|---|
| 0.0.0.0. | 0.0.0.0 | 30.0.0.2 |
| 50.0.0.0 | 255.0.0.0 | 20.0.0.1 |
| 20.0.0.0 | 255.0.0.0 | 20.0.0.2 |
| 40.0.0.0 | 255.0.0.0 | 30.0.0.2 |
| 60.0.0.0 | 255.0.0.0 | 30.0.0.2 |
| 30.0.0.0 | 255.0.0.0 | 30.0.0.1 |
| 70.0.0.0 | 255.0.0.0 | 70.0.0.1 |




| Red | Mascara | Gateway |
|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 40.0.0.2 |
| 50.0.0.0 | 255.0.0.0 | 40.0.0.2 |
| 20.0.0.0 | 255.0.0.0 | 40.0.0.2 |
| 40.0.0.0 | 255.0.0.0 | 40.0.0.1 |
| 60.0.0.0 | 255.0.0.0 | 60.0.0.1 |
| 30.0.0.0 | 255.0.0.0 | 30.0.0.2 |
| 70.0.0.0 | 255.0.0.0 | 30.0.0.1 |

## 5.5 Control de Flujo

El control de flujo no se implementa en la cabecera del datagrama IP. Solo se hace control de flujo en la capa de transporte. El control de flujo es un mecanismo que permite regular el tráfico entre un transmisor rápido y un receptor mas lento en procesamiento, con el objetivo de no saturar al receptor y no perder información.

## 5.6 Control de Errores

El control de errores es un campo de la cabecera IP de 16 bits similar al CRC empleado en las tramas Ethernet. Se recalcula cada vez que algún router se cambia alguno de sus campos (por ejemplo, el Tiempo de Vida o se agrega información en el campo opciones). El método de cálculo, consiste en sumar en complemento a 1 cada palabra de 16 bits de la cabecera

(considerando valor 0 para el campo de suma de control de cabecera) y hacer el complemento a 1 del valor resultante.

## 5.7 Formato del datagrama IP


**Figura: Formato datagrama IP**

- **Versión**: 4 bits

Siempre vale lo mismo (**0100**). Este campo describe el formato de la cabecera utilizada. En la tabla se describe la versión 4.

- **Tamaño Cabecera (IHL)**: 4 bits

Longitud de la cabecera, en palabras de 32 bits. Su valor mínimo es de 5 para una cabecera correcta y el máximo de 15.

- **Tipo de Servicio**: 8 bits

Indica una serie de parámetros sobre la calidad de servicio deseada durante el tránsito por una red. Algunas redes ofrecen prioridades de servicios, considerando determinado tipo de paquetes "más importantes" que otros (en particular estas redes solo admiten los paquetes con prioridad alta en momentos de sobrecarga). Estos 8 bits se agrupan de la siguiente manera. Los 5 bits de menos peso son independientes e indican características del servicio:

  - **Bit 0**: sin uso, debe permanecer en 0.
  - **Bit 1**: 1 costo mínimo, 0 costo normal.
  - **Bit 2**: 1 máxima fiabilidad, 0 fiabilidad normal.
  - **Bit 3**: 1 máximo rendimiento, 0 rendimiento normal.
  - **Bit 4**: 1 mínimo retardo, 0 retardo normal.

Los 3 bits restantes están relacionados con la prioridad de los mensajes, un indicador adjunto que indica el nivel de urgencia basado en

## Operación de un Router

el sistema militar de precedencia. La urgencia que estos estados representan aumenta a medida que el número formado por estos 3 bits lo hace y responden a los siguientes nombres.

- 000: De rutina.
- 001: Prioritario.
- 010: Inmediato.
- 011: Relámpago.
- 100: Invalidación relámpago.
- 101: Procesando llamada crítica y de emergencia.
- 110: Control de trabajo de Internet.
- 111: Control de red.

- **Longitud Total**: 16 bits

Es el tamaño total, en bytes, del datagrama, incluyendo el tamaño de la cabecera y el de los datos. El tamaño mínimo de los datagramas usados normalmente es de 576 octetos (64 de cabeceras y 512 de datos). Una máquina no debería enviar datagramas menores o mayores de ese tamaño a no ser que tenga la certeza de que van a ser aceptados por la máquina destino.

En caso de fragmentación este campo contendrá el tamaño del fragmento, no el del datagrama original.

- **Identificador**: 16 bits

Identificador único del datagrama. Se utilizará, en caso de que el datagrama deba ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro. El originador del datagrama debe asegurar un valor único para la pareja origen-destino y el tipo de protocolo durante el tiempo que el datagrama pueda estar activo en la red. El valor asignado en este campo debe ir en formato de red.

- **Flags**: 3 bits

Actualmente utilizado sólo para especificar valores relativos a la fragmentación de paquetes:

- **bit 2**: Reservado; debe ser 0
- **bit 1**: 0 = Fragmentable, 1 = No Fragmentable (DF)
- **bit 0**: 0 = Último Fragmento, 1 = Fragmento Intermedio (le siguen más fragmentos) (MF)

La indicación de que un paquete es fragmentable debe ser tenida en cuenta bajo cualquier circunstancia. Si el paquete necesitara ser fragmentado, no se enviará.

- **Offset**: 13 bits

En paquetes fragmentados indica la posición, en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama original. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0.

## Operación de un Router

- **Tiempo de Vida (TTL)**: 8 bits

Indica el máximo número de enrutadores que un paquete puede atravesar. Cada vez que algún nodo procesa este paquete disminuye su valor en 1 como mínimo, una unidad. Cuando llegue a ser 0, el paquete será descartado.

- **Protocolo**: 8 bits

Indica el protocolo de las capas superiores al que debe entregarse el paquete Vea Números de protocolo IP para comprender como interpretar este campo. Si el datagrama transporte en su parte de datos TCP indicara este campo el valor $\mathbf{0x06_H}$ y si transporta UDP este valor indicara el $\mathbf{0x11_H}$.

- **Suma de Control de Cabecera**: 16 bits

Se recalcula cada vez que algún nodo cambia alguno de sus campos (por ejemplo, el Tiempo de Vida). El método de cálculo -intencionadamente simple- consiste en sumar en complemento a 1 cada palabra de 16 bits de la cabecera (considerando valor 0 para el campo de suma de control de cabecera) y hacer el complemento a 1 del valor resultante.

- **Dirección IP de origen**: 32 bits

Es la dirección IP de la estación de trabajo o dispositivo de red que emite el datagrama. Entre el origen y el destino siempre se mantiene la misma dirección IP de origen.

- **Dirección IP de destino**: 32 bits

Es la dirección IP de la estación de trabajo o dispositivo de red que recibe el datagrama. Entre el destino y el origen siempre se mantiene la misma dirección IP de destino.

- **Opciones**: Variable

Aunque no es obligatoria la utilización de este campo, cualquier nodo debe ser capaz de interpretarlo. Puede contener un número indeterminado de opciones, detalladas brevemente a continuación:

  - **Final de Lista de Opciones:**

    Se usa al final de la lista de opciones, si ésta no coincide con el final de la cabecera IP.

  - **Ninguna Operación (NOP)**:

    Se puede usar para forzar la alineación de las opciones en palabras de 32 bits.

## Operación de un Router

- **Seguridad**:

  Especifica niveles de seguridad que van desde "No Clasificado" hasta "Máximo Secreto", definidos por la Agencia de Seguridad de la Defensa (de EE.UU.).

- **Enrutado desde el Origen (abierto) y Registro de Ruta (LSSR)**:

  Esta opción provee el mecanismo para que el originador de un datagrama pueda indicar el itinerario que ha de seguir a través de la red y para registrar el camino seguido. Los Datos de Opción consisten en un puntero (un octeto) y una lista de direcciones IP (4 octetos cada una) que se han de alcanzar ("procesar"):

  El puntero indica la posición de la siguiente dirección de la ruta, dentro de la Opción; así, su valor mínimo es de 4. Cuando un nodo de Internet procesa la dirección de la lista apuntada por el puntero (es decir, se alcanza esa dirección) incrementa el puntero en 4, y redirige el paquete a la siguiente dirección. Si el puntero llega a ser mayor que el Tamaño de Opción significa que la información de ruta se ha procesado y registrado completamente y se redirigirá el paquete a su dirección de destino.

  Si se alcanza la dirección de destino antes de haber procesado la lista de direcciones completa (el puntero es menor que el Tamaño de Opción) la siguiente dirección de la lista reemplaza a la dirección de destino del paquete y es a su vez reeemplazada por la dirección del nodo que está procesando el datagrama ("Ruta Registrada"), incrementando, además, el puntero en 4.

  Utilizando este método de sustituir la dirección especificada en origen por la Ruta Registrada se asegura que el tamaño de la Opción (y de la cabecera IP) no varía durante su recorrido por la red.

  Se considera que la ruta especificada por el originador es "abierta" porque cualquier nodo que procesa el paquete es libre de dirigirlo a la siguiente dirección siguiendo cualquier otra ruta intermedia.

  Sólo puede usarse una vez en un datagrama, y, en caso de fragmentación, la opción se copiará a los paquetes resultantes.

- **Enrutado desde el Origen (estricto) y Registro de Ruta (SSRR)**:

  Exactamente igual que LSSR, excepto en el tratamiento que los nodos harán de este datagrama. Al ser la ruta especificada "estricta", un nodo debe reenviar el paquete directamente a la siguiente dirección, es decir, no podrá redireccionarlo por otra red.

- **Registro de Ruta**:

  Mediante el uso de esta Opción se puede registrar el itinerario de un datagrama. Los Datos de Opción consisten en un puntero (un octeto) y un espacio relleno de ceros que contendrá la Ruta Registrada para el paquete.

**Operación de un Router**

Cuando un nodo recibe un paquete en el que está presente esta opción, escribirá su dirección IP en la posición indicada por el puntero, siempre que ésta sea menor que el Tamaño de Opción, e incrementará el puntero en 4.

Es preciso que el espacio reservado para la Ruta Registrada tenga una longitud múltiplo de 4; si al intentar grabar su dirección un nodo detecta que existe espacio libre pero es menor de 4 octetos, el paquete no se reenvía (se pierde) y se notifica el error, mediante ICMP, al originador del datagrama.

Esta Opción no se copia en caso de fragmentación, y sólo puede aparecer una vez en un paquete.

- **Relleno**: Variable

Utilizado para asegurar que el tamaño, en bits, de la cabecera es un múltiplo de 32. El valor usado es el 0.

## 5.8 ICMP

El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas en inglés de Internet Control Message Protocol) es un protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o estación de trabajo no puede ser localizado.

ICMP no es utilizado directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta ping y traceroute, que envían mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa.

### 5.8.1 Formato basico del ICMP

ICMP es parte del conjunto de protocolos IP tal cual y como se definió en la RFC 792. Los mensajes ICMP son comúnmente generados en respuesta a errores en los datagramas de IP o para diagnóstico y ruteo. La versión de ICMP para IPv4 también es conocida como ICMPv4.

IPv6 tiene su protocolo equivalente ICMPv6. Los mensajes ICMP son construidos en el nivel de capa de red. IP encapsula el mensaje ICMP apropiado con una nueva cabecera IP (para obtener los mensajes de respuesta desde el host original que envía), y transmite el datagrama resultante de manera habitual.

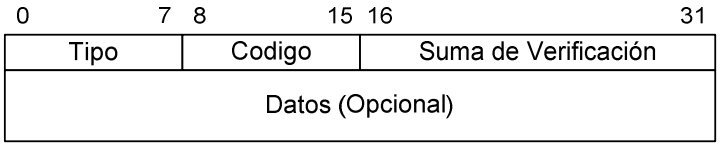
Por ejemplo, cada router que reenvía un datagrama IP tiene que disminuir el campo de tiempo de vida (TTL) de la cabecera IP en una unidad; si el TTL llega a 0, un mensaje ICMP "Tiempo de Vida se ha excedido en transmitirse" es enviado a la fuente del datagrama. Cada mensaje ICMP es encapsulado directamente en un solo datagrama IP y por tanto no garantiza la entrega del ICMP. Aunque los mensajes ICMP son contenidos dentro de datagramas estándar IP, los mensajes ICMP se procesan como un caso especial del procesamiento normal de IP, algo así como el procesamiento de un sub-protocolo de IP. En muchos casos es necesario inspeccionar el contenido del

## Operación de un Router

mensaje ICMP y entregar el mensaje apropiado de error a la aplicación que generó el paquete IP original, aquel que solicitó el envío del mensaje ICMP.

La utilidad del protocolo ICMP es controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, etc. Es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado.

Muchas de las utilidades de red comunes están basadas en los mensajes ICMP. El comando **"traceroute"** está implementado transmitiendo datagramas UDP con campos especiales TTL IP en la cabecera, y buscando los mensajes de "Tiempo de Vida en tránsito" y "Destino inalcanzable" generados como respuesta. La herramienta ping está implementada utilizando los mensajes "Echo request" y "Echo reply" de ICMP. A continuación se muestra el formato basico de un mensaje ICMP donde se compone de una campo tipo y dentro de cada tipo existen también mensajes particulares.




Algunos ejemplos de envío y recepción de mensajes de control permitidos:

0 - Echo Reply
1 - Reservado
2 - Reservado
3 - Destination Unreachable
4 - Source Quench
5 - Redirect Message
6 - Dirección Alterna de Host
7 - Reservado
8 - Echo Request
9 - Anuncio de Router
10 - Solicitud de Router
11 - Tiempo Excedido
12 - Problema de Parámetro
13 - Marca de tiempo
14 - Respuesta de Marca de tiempo
15 - Petición de Información
16 - Respuesta de Información
17 - Petición de Máscara de Dirección
18 - Respuesta de Máscara de Dirección
19 - Reservado para seguridad
20-29 - Reservado para experimentos de robustez
30 - Traceroute
31 - Error de Conversión de Datagrama
32 - Redirección de Host Móvil
33 - IPv6
34 - Petición de Registro de Móvil
35 - Respuesta de registro de Móvil
36 - Petición de Nombre de Dominio
37 - Respuesta de Nombre de Dominio
38 - SKIP Protocolo de Algoritmo de Descubrimiento
39 - Photuris, Fallas de Seguridad
40-255 - Reservado