

Para entender bien TCP/IP, hay que comprender completamente uno de sus protocolos más importantes: el Protocolo Internet, IP (Internet Protocol). IP es el bloque de interconexión de redes del resto de protocolos del Nivel Internet y superiores.

Introducción a IP

IP comprende el Nivel Internet del modelo DARPA y proporciona la funcionalidad de interconexión que hace posible la interconexión a gran escala como Internet. IP permanece desde que se formalizó en 1981 y se continuará usando en Internet durante años. Sólo recientemente se han tratado algunas dificultades de IP en una nueva versión denominada IP versión 6 (IPv6). La sorprendente longevidad de IP es un tributo a su original diseño.

Servicios de IP

IP ofrece los siguientes servicios a los protocolos de niveles superiores:

- **Protocolo de interconexión (Internetworking protocol).** IP es un protocolo de interconexión, también conocido como protocolo enrutable. La cabecera de IP contiene la información necesaria para el enrutamiento de un paquete, incluyendo las direcciones de origen y de destino. Una dirección de IP consta de dos componentes: una dirección de red y una dirección de nodo. La entrega entre redes, o enrutamiento, es posible gracias a la existencia de una dirección de red de destino. IP permite la creación de conjuntos de redes de IP, es decir, dos o más redes interconectadas mediante enrutadores de IP. La cabecera de IP también contiene un contador de saltos que se utiliza para limitar el número de enlaces por los que puede viajar un paquete antes de descartarlo.
- **Múltiples protocolos cliente.** IP es un transporte entre redes para los protocolos de niveles superiores. IP puede transportar distintos protocolos de los niveles superiores, pero cada paquete de IP sólo puede contener datos de un solo protocolo de nivel superior cada vez. Como cada paquete puede llevar uno de varios protocolos, debe existir un mecanismo para indicar a qué protocolo del nivel superior pertenecen los datos de un paquete, de manera que se puedan enviar al protocolo de nivel superior de destino apropiado. Siempre, tanto el cliente como el servidor, utilizan el mismo protocolo para un intercambio dado de datos. Por tanto, el paquete no necesita indicar distintos protocolos para el origen y para el destino. Ejemplos de protocolos de niveles superiores están otros protocolos del Nivel Internet como el Protocolo de mensajes de control de Internet, ICMP (Internet Control Message Protocol), y el Protocolo de administración de grupos de Internet, IGMP (Internet Group Management Protocol). Otros ejemplos son los protocolos del Nivel de Transporte como el Protocolo de control de transmisión, TCP (Transmission Control Protocol), y el Protocolo de datagramas de usuario, UDP (User Datagram Protocol).
- **Entrega de datagramas.** IP es un protocolo de datagramas que proporciona un servicio de entrega no fiable y sin conexión a los protocolos de niveles superiores. Sin conexión significa que no existe acuerdo entre los nodos de IP antes de enviar los datos, y que no se crea ni mantiene ninguna conexión lógica en el Nivel Internet. No fiable significa que IP envía un paquete sin secuencia y sin asentimientos de que ha llegado a su destino. La fiabilidad extremo a extremo es responsabilidad de los protocolos de niveles superiores como TCP.
- **Independencia del Nivel de interfaz de red.** En el Nivel Internet, IP se diseñó para ser independiente de las tecnologías de red presentes en el Nivel de interfaz de red. IP es independiente de los atributos del Nivel Físico de OSI como el cableado, la señalización y la velocidad. También es independiente de los atributos del Nivel de enlace de datos de OSI como el esquema de control de acceso al medio, el direccionamiento y el tamaño máximo de trama. IP usa direcciones de 32 bits independientes del esquema de direccionamiento usado

en el Nivel de interfaz de red.

- **Fragmentación y reensamblado.** Para admitir el máximo tamaño de trama de distintas tecnologías del Nivel de interfaz de red, IP permite la fragmentación de los datos cuando se envían por un enlace cuya MTU es menor que el tamaño de un datagrama. Los enrutadores, o hosts de reenvío, fragmentan los datos de IP, y esta fragmentación puede ocurrir múltiples veces. El host de destino reensambla los fragmentos para obtener los datos de IP enviados originalmente.
- **Extensible mediante las opciones de IP.** Cuando se requieren funciones que no están disponibles usando la cabecera estándar de IP, se pueden usar las opciones de IP. Estas opciones se añaden a la cabecera estándar para proporcionar funcionalidad como la capacidad de especificar una ruta que debe seguir un datagrama a través de una interred.
- **Tecnología de datagramas por conmutación de paquetes.** IP es un ejemplo de una tecnología de datagramas por conmutación de paquetes: cada paquete es un datagrama, un mensaje sin secuencia ni asentimiento que se reenvía por los conmutadores de la red de conmutación usando un esquema de direcciones con significado global. En el caso de IP, cada conmutador de la red de conmutación es un enrutador de IP, y el direccionamiento con significado global es la dirección de destino de IP. Esta dirección se examina en cada enrutador. El enrutador toma una decisión de enrutamiento independiente y reenvía el paquete. Como cada enrutador decide de manera independiente dónde reenviar el paquete, la ruta de un paquete desde un Nodo 1 hasta un Nodo 2 no es necesariamente la misma ruta que desde el Nodo 2 hasta el Nodo 1. Además, como cada paquete se conmuta de forma separada, cada uno puede llevar una ruta distinta desde el origen hasta el destino; y, debido a distintos retardos en el trayecto, cada paquete puede llegar en un orden distinto al que fue enviado.

El término conmutador se emplea como una generalización de dispositivo de reenvío y no significa un conmutador de Nivel 2 ni de Nivel 3. Un conmutador de Nivel 2 se suele usar en entornos Ethernet para segmentar el tráfico. Un conmutador de Nivel 3 es equivalente a un enrutador.

MTU de IP

Cada tecnología del Nivel de interfaz de red impone un tamaño máximo de trama que se puede enviar. El tamaño máximo de trama consiste en una cabecera, una cola y los datos. El tamaño máximo de trama para una tecnología del Nivel de interfaz de red dada se denomina la unidad máxima de transmisión (MTU). Para un paquete de IP, los datos del Nivel de interfaz de red es un datagrama de IP. Por tanto, el tamaño máximo de los datos se convierte en el tamaño máximo de un datagrama de IP. Es lo que se conoce como MTU de IP.

En un entorno con una mezcla de Protocolos del Nivel de interfaz de red puede ocurrir fragmentación cuando se cruza un enrutador de un enlace con una MTU de IP mayor a un enlace con una MTU de IP menor.

MTU de IP de tecnologías del Nivel de interfaz de red habituales	
Tecnología del Nivel de interfaz de red	MTU de IP
Ethernet (encapsulado Ethernet II)	1500
Ethernet (encapsulado SNAP de IEEE 802.3)	1492
Token Ring (4 y 16 Mbps)	Varía según el tiempo de retención de

	testigo
FDDI	4352
X.25	1600
Frame Relay	1600
ATM (IP clásico sobre ATM)	9180
MTU mínima	576

Datagrama de IP

Un datagrama de IP consta de una cabecera de IP y unos datos de IP.

- **Cabecera de IP.** La cabecera de IP es de tamaño variable entre 20 y 60 bytes, en incrementos de 4 bytes. Proporciona soporte para enrutamiento, identificación de datos, indicación de tamaño de la cabecera de IP y de los datos, fragmentación y opciones.
- **Datos de IP.** Los datos de IP son de tamaño variable, desde los 8 bytes (un datagrama de IP de 68 bytes con una cabecera de IP de 60 bytes) hasta los 65.515 bytes (un datagrama de IP de 65.535 bytes con una cabecera de IP de 20 bytes).

Cabecera de IP

Los campos de la cabecera de IP (versión 4) son los siguientes:

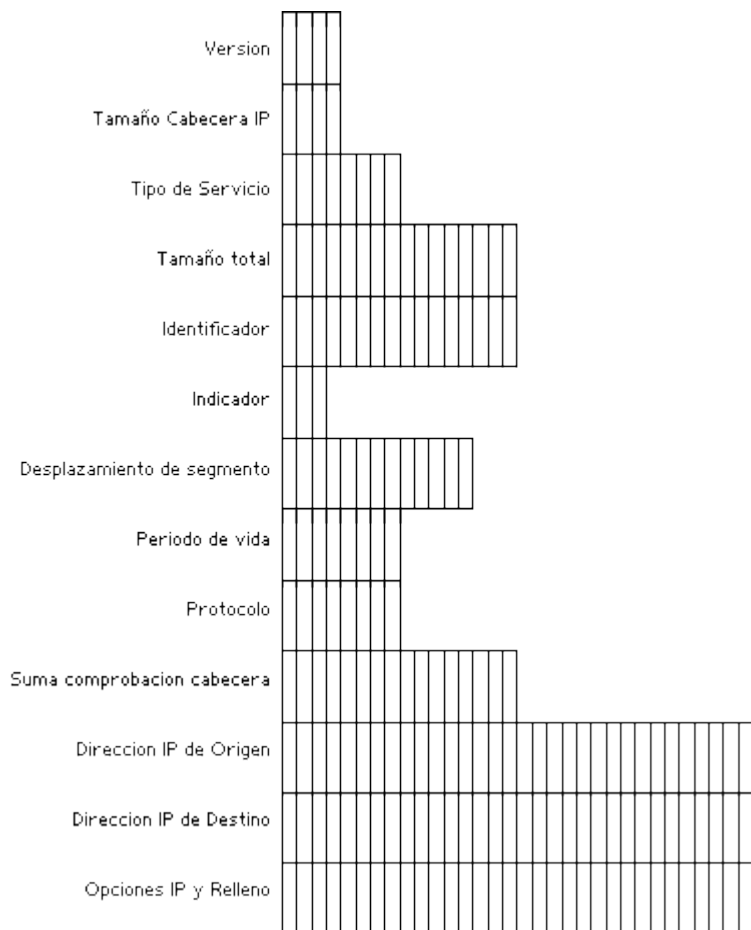
Versión

El campo Versión tiene 4 bits de tamaño y se usa para indicar la versión de la cabecera de IP. Un campo de 4 bits puede tener valores desde 0 hasta 15. La versión estándar que se usa hoy en redes corporativas a Internet es la versión 4, o IPv4. La siguiente versión de IP es la versión 6, o IPv6. El resto de valores para el campo Versión no están definidos ni se usan.

Tamaño de la cabecera

El campo Tamaño de la cabecera (Header Length) tiene 4 bits de tamaño y se usa para indicar el tamaño de la cabecera de IP. El número máximo que se puede representar con 4 bits es de 15. Por tanto, este campo no puede ser un contador de bytes. Indica el número de palabras de 32 bits, bloques de 4

bytes, de la cabecera de IP. La cabecera típica de IP no tiene opciones con un tamaño de 20 bytes. El tamaño más pequeño posible para tamaño de cabecera es 5 (0x5). Con el mayor número de opciones de IP, la mayor cabecera puede tener 60 bytes, lo que se indica con un tamaño de cabecera



de 15 (OxF).

Al usar un contador de bloques de 4 bytes indica que el tamaño de la cabecera de IP siempre ha de ser múltiplo de 4 bytes. Si hay opciones de IP que extiendan la cabecera, deben hacerlo en incrementos de 4 bytes. Si una opción de IP no tiene un tamaño de 4 bytes, se debe usar un relleno para que la cabecera siempre esté en la frontera de los 4 bytes.

Tipo de servicio

El campo Tipo de servicio, TOS (Type Of Service), tiene 8 bits de tamaño y se usa para indicar la calidad de servicio con que los enrutadores del conjunto de redes deben enviar ese datagrama. El campo TOS tiene subcampos a indicadores para indicar características de precedencia deseada, retardo, rendimiento, fiabilidad y coste.

En los 8 bits del campo TOS hay cinco campos para indicar distintas calidades de entrega del datagrama. El campo TOS lo establece el host emisor y los enrutadores no lo modifican. Todos los fragmentos de un datagrama de IP tienen el mismo TOS que el datagrama de IP original.

Normalmente, un host emisor envía un datagrama con un campo TOS con el valor 0x00: precedencia rutinaria, retardo normal, rendimiento normal, fiabilidad normal y coste normal. Los enrutadores suelen ignorar los valores del campo TOS y reenvían todos los datagramas como si estos campos no existiesen. Es lo que se conoce como enrutamiento TOSO. Sin embargo, los protocolos de enrutamiento modernos como OPSF y el IS-IS integrado admiten el cálculo de rutas para cada valor del campo TOS.

Los enrutadores y el protocolo de enrutamiento determinan cómo se interpretan los distintos valores del campo TOS. En una red configurada de forma apropiada, los paquetes con valores concretos de TOS se envían por rutas distintas. De esta forma se mejora el enrutamiento y la entrega eficiente en conjuntos de redes de IP multirruta. Por ejemplo, un conjunto de redes de IP podría tener una ruta para tráfico general, una para tráfico con pequeño retardo y otra para tráfico de alta fiabilidad. Cuando los hosts establecen distintas combinaciones de valores de TOS, los enrutadores pueden seleccionar entre dichas rutas.

El campo TOS se usa para calidad de servicio (QoS) en redes de IP.

- **Precedencia.** El campo Precedencia, de 3 bits de tamaño, se usa para indicar la importancia del datagrama. Por defecto el campo Precedencia se establece a 000 (Rutinario). Los valores de este campo son:
 - 000 Rutinario
 - 001 Prioritario
 - 010 Inmediato
 - 011 Flash
 - 100 Anulación de Flash
 - 101 CRÍTICO/ECP
 - 110 Control de Interred
 - 111 Control de Red
- **Retardo.** El campo Retardo es un indicador para indicar Retardo normal (=0) o Bajo retardo (=1). Si retardo está a 1, el enrutador de IP reenvía el datagrama de IP por la ruta que tiene el menor retardo. Una aplicación puede solicitar una ruta de bajo retardo cuando envía datos sensibles al tiempo, como voz o video digital, o tráfico interactivo, como una sesión de Telnet. De acuerdo con el indicador Retardo, el enrutador podría elegir un enlace WAN

terrestre sobre un enlace de satélite de mayor retardo, aunque el enlace de satélite tenga un mayor ancho de banda.

- **Rendimiento.** El campo Rendimiento es un indicador que indica Rendimiento normal (=0) o Alto rendimiento (=1). Si el campo Rendimiento está a 1, el enrutador de IP envía el datagrama por la ruta con mejor característica de rendimiento. Una aplicación puede solicitar un alto rendimiento cuando envía datos masivos. Según este indicador, el enrutador puede escoger un enlace de satélite de alto rendimiento sobre un enlace WAN terrestre de menor rendimiento, aunque el enlace terrestre presente un menor retardo.
- **Fiabilidad.** El campo Fiabilidad es un indicador que indica Fiabilidad normal (=0) o Alta fiabilidad (=1). Durante los períodos de congestión de un enrutador de IP, el campo Fiabilidad se usa para decidir qué datagramas de IP se descartan en primer lugar. Si el campo Fiabilidad está a 1, el enrutador de IP descarta estos datagramas en último lugar. Una aplicación puede solicitar una ruta de alta fiabilidad cuando envía datos sensibles al tiempo, por lo que no se deben descartar. Por ejemplo, con algunos métodos de envío de video digital, el video digitalizado se envía como dos tipos de paquetes: el tipo primario se usa para reconstruir la imagen base del video, y un tipo secundario que se usa para proporcionar una imagen de mayor resolución. En este caso, los paquetes primarios se envían con el campo Fiabilidad a 1 y los paquetes secundarios con este campo a 0. Si ocurre congestión en el enrutador, éste descarta primero los paquetes secundarios.
- **Coste.** El campo Coste es un indicador que indica Coste normal (=0) o Bajo coste (=1), donde coste indica coste monetario. Si el campo coste está a 1, el enrutador envía el datagrama de IP por la ruta que tiene el menor coste. Una aplicación puede solicitar la ruta de menor coste cuando envía datos que no son críticos. De acuerdo con el indicador Coste, el enrutador puede elegir un enlace terrestre de menor coste sobre un enlace de satélite de mayor coste, aunque el enlace terrestre tenga un menor ancho de banda.
- **Reservado.** El campo Reservado es el último bit y debe estar a 0. Los enrutadores lo ignoran cuando reenvían los datagramas de IP.

Configuración de TOS con PING.EXE

La utilidad PING de Microsoft Windows 2000 se puede usar con la opción <-v> para establecer el valor de TOS en los mensajes de Solicitud de eco de ICMP. Su sintaxis es la siguiente:

```
PING -v [valor de TOS] [dirección de IP o nombre de host]
```

El valor de TOS se expresa en decimal. Por ejemplo, para hacer un ping a 10.0.0.1 con un campo TOS con precedencia normal, retardo mínimo y mínimo coste monetario, use el siguiente comando:

```
PING -v 18 10.0.0.1
```

Tamaño total

El campo Tamaño total tiene 2 bytes y se usa para indicar el tamaño del datagrama de IP (cabecera de IP y datos de IP) en bytes. Con 16 bits, el tamaño máximo que se puede indicar es de 65.535 bytes. Para los datagramas de tamaño máximo, el tamaño total es el mismo que la MTU de IP para dicha tecnología del Nivel de interfaz de red.

Con el tamaño de cabecera y el tamaño total se puede determinar el tamaño de los datos: tamaño de los datos de IP (bytes) = tamaño total (bytes) - 4 * tamaño de la cabecera (palabras de 32 bits).

Identificación

El campo Identificación tiene 2 bytes de tamaño y se usa para identificar un paquete de IP concreto enviado entre un nodo emisor y el nodo de destino. El host emisor fija el valor del campo

Identificación que se incrementa en sucesivos datagramas de IP. Este campo se usa para identificar fragmentos de un datagrama de IP original.

Indicadores

El campo Indicadores consta de 3 bits y contiene los indicadores para la fragmentación. Un indicador se usa para indicar si el datagrama de IP es elegible para fragmentación y el resto indica si siguen más fragmentos o no a este fragmento de un datagrama de IP.

Desplazamiento de fragmento

El campo Desplazamiento de fragmento tiene 13 bits de tamaño y se usa para indicar el desplazamiento donde este fragmento empieza relativo a los datos de IP originales.

Período de vida

El campo Período de vida tiene 1 byte de tamaño y se usa para indicar cuántos enlaces puede atravesar este datagrama de IP antes de que un enrutador lo descarte. El campo Período de vida, TTL (Time to Live), se diseñó como un contador de tiempo, para indicar el número de segundos que el datagrama podía estar vivo en la Internet. Un enrutador de IP tenía que realizar un seguimiento del momento en que recibía el datagrama y el momento en que lo reenviaba. El TTL se decrementaba en el número de segundos que el paquete pasaba en el enrutador.

Sin embargo, el estándar más moderno (RFC 1812) especifica que los enrutadores decrementen el TTL en uno cuando reenvíen un datagrama de IP. Por tanto, el TTL es una cuenta inversa de enlaces. El host emisor fija el valor inicial de TTL, que actúa como una cuenta máxima de enlaces. El valor máximo limita el número que puede atravesar el datagrama y previene que esté indefinidamente dando vueltas.

Algunos aspectos adicionales del campo TTL son:

- Los enrutadores decrementan el TTL de los paquetes recibidos antes de consultar la tabla de enrutamiento. Si el TTL es 0, ese paquete se descarta y se envía un mensaje de ICMP Período expirado-TTL expirado en tránsito (Time Expired-TTL Expired In Transit) de vuelta al host emisor.
- Los hosts de destino no comprueban el campo TTL.
- Los hosts emisores deben enviar los datagramas de IP con un TTL mayor que 0. El valor exacto del campo TTL para los datagramas de IP enviados es el predeterminado del sistema operativo o el que especifique la aplicación. El valor máximo de TTL es 255.
- Un valor recomendado es el doble del diámetro del conjunto de redes. El diámetro es el número de enlaces entre los dos nodos más alejados del conjunto de redes.
- TTL es independiente de la métrica del protocolo de enrutamiento como la cuenta de saltos del Protocolo de información de enrutamiento (RIP) o el coste del Primero el camino más corto abierto (OSPF).

Se puede referir erróneamente a TTL como un contador de saltos cuando de hecho es un contador de enlaces. La diferencia es sutil pero importante. Una cuenta de saltos es el número de enrutadores que se cruzan para llegar a un destino. Una cuenta de enlaces es el número de enlaces del Nivel de interfaz de red que se cruzan para llegar a un destino. La diferencia entre cuenta de saltos y cuenta de enlaces es 1. Por ejemplo, si los hosts A y B están separados por cinco enrutadores, la cuenta de saltos es de 5, pero la cuenta de enlaces es de 6. Un datagrama de IP enviado desde el host A hasta el host B con un TTL de 5 será descartado por el quinto enrutador. Un datagrama de IP enviado desde el host A hasta el host B con un TTL de 6 llegará al host B.

Configuración de TTL con PING

Se puede usar la utilidad PING con la opción <-i> para establecer el valor de TTL en un mensaje de eco de ICMP. Su sintaxis es:

```
PING -i [valor TTL] [dirección de IP o nombre de host]
```

El valor de TTL se expresa en decimal. Por ejemplo, para hacer un ping a 10.0.0.1 con un campo TTL con el valor 7, use el siguiente comando:

```
PING -i 7 10.0.0.1
```

El valor predeterminado de TTL para los mensajes de eco de ICMP que envía PING es de 32.

Protocolo

El campo Protocolo tiene 1 byte y se usa para indicar el protocolo de nivel superior que contiene los datos de IP. El campo Protocolo es una indicación explícita del protocolo cliente. Algunos valores de este campo son 1 para ICMP, 6 para TCP y 17 (0x11) para UDP. Este campo actúa como una identificación de multiplexación de forma que los datos puedan atravesar los protocolos de nivel superior apropiados tras recibirse en el nodo de destino.

Las aplicaciones de Windows Sockets pueden referirse a los protocolos por su nombre. Los nombres de los protocolos se resuelven en números de protocolo mediante el archivo PROTOCOL que se encuentra en el directorio %SystemRoot%\system32\drivers\etc.

Suma de comprobación de cabecera

El campo Suma de comprobación de cabecera tiene 2 bytes y realiza una comprobación de integridad en el nivel de bit sólo de la cabecera de IP. Los datos de IP no se incluyen. Los datos deben incluir su propia suma de control para comprobar la integridad en el nivel de bit. El host emisor realiza una suma de comprobación inicial en el datagrama de IP enviado. Cada enrutador en la ruta entre el origen y el destino verifica el campo suma de comprobación de cabecera antes de procesar el paquete. Si la verificación falla, el enrutador descarta silenciosamente el datagrama de IP.

Como cada enrutador de la ruta entre el origen y el destino decrementa el TTL, la suma de comprobación de la cabecera cambia en todos los enrutadores.

Para calcular la suma de comprobación de la cabecera, a los valores de 16 bits de la cabecera se les hace el complemento a 1; a los bits que están a 0 se cambian a 1 y los bits que están a 1 se cambian a 0. Se suman todos los valores de 16 en complemento a 1 y a la suma resultado se vuelve a hacer el complemento a 1. El resultado se pone en el campo Suma de comprobación de la cabecera.

Para el cómputo de la suma de comprobación de todos los campos de la cabecera de IP, el valor de este mismo campo se pone a 0.

Dirección de origen

El campo Dirección de origen tiene 4 bytes y contiene la dirección de IP del host emisor, a no ser que un traductor de direcciones de red, NAT (Network Address Translator), esté traduciendo el datagrama de IP. Se usa un NAT para traducir entre direcciones privadas y públicas cuando se conectan a Internet.

Dirección de destino

El campo Dirección de destino tiene 4 bytes y contiene la dirección de IP del host de destino, a no ser que el datagrama de IP esté traduciendo un traductor de direcciones de red o se esté realizando un enrutamiento débil o estricto.

Opciones y Relleno

A la cabecera de IP se le pueden añadir Opciones y Relleno, pero se debe hacer en incrementos de 4 bytes de manera que el tamaño de la cabecera de IP se pueda indicar usando el campo Tamaño de cabecera.

Fragmentación

Cuando un host origen o un enrutador deben transmitir un datagrama de IP por un enlace cuya MTU es menor que el tamaño del datagrama de IP, hay que fragmentar el datagrama. Cuando ocurre la fragmentación de IP, los datos de IP se segmentan y cada segmento se envía con su cabecera de IP.

La cabecera de IP contiene la información requerida para reensamblar los datos de IP originales en el host de destino. Como IP es una tecnología de datagramas por conmutación de paquetes y los fragmentos pueden llegar en un orden distinto al que fueron enviados, hay que agrupar los fragmentos, usando el campo Identificación, secuenciarlos, usando el campo Desplazamiento de segmento, y delimitarlos, usando el campo Más fragmentos.

Las tecnologías de circuitos por conmutación de paquetes como X.25 y ATM sólo requieren la delimitación de fragmento/segmento. Por ejemplo, con ATM Nivel de adaptación 5, un datagrama de IP se segmenta en trozos de 48 bytes que se convierten en los datos de las celdas de ATM. ATM envía el flujo de celdas que componen el datagrama de IP y usa el tercer bit del campo Tipo de datos de la cabecera de ATM para indicar el final del flujo de celdas del datagrama.

Campos fragmentación

- **Identificación.** El campo Identificación se usa para agrupar todos los fragmentos de un datagrama. El host de origen establece el campo Identificación y este campo se mantiene durante el proceso de fragmentación. Este campo se pone incluso aunque no se permita la fragmentación de los datos de IP estableciendo el indicador No fragmentar.
- **Indicador No fragmentar.** El indicador No fragmentar, DF (Don't Fragment), se establece a 0 para permitir la fragmentación y a 1 para prohibirla. Por tanto, la fragmentación se producirá sólo si el indicador DF está a 0. Si se necesita fragmentar un datagrama de IP y el indicador DF está a 1, en enrutador descarta el datagrama y envía de vuelta al host de origen un mensaje de ICMP de destino inalcanzable-Fragmentación necesaria y se estableció DF, ICMP (Destination Unreachable-Fragmentation Needed And DF Set). La fragmentación es un proceso costoso para los enrutadores y para el host de destino. El indicador DF y el mensaje de ICMP de destino inalcanzable-Fragmentación necesaria y se especificó DF en el mecanismo por el que un nodo descubre la MTU de la ruta entre un origen y el destino, o Descubrimiento de la MTU de la ruta (Path MTU Discovery).
- **Indicador Más fragmentos.** El indicador Más fragmentos, MF (More Fragments), está a 0 si no existen más fragmentos que sigan a éste (éste es el último fragmento), y se pone a 1 si existen más fragmentos que sigan a éste (éste no es el último fragmento).
- **Desplazamiento de fragmento.** El campo Desplazamiento de fragmento indica la posición del fragmento relativa a los datos de IP originales. Este campo es un desplazamiento usado para dar orden durante el reensamblado, colocando los fragmentos que van llegando en el orden correcto para reconstruir los datos originales. Este campo tiene 13 bits de tamaño. Con un tamaño de datos de IP máximo de 65.515 bytes (la MTU de IP máxima de 65.535 menos la cabecera de IP mínima de 20 bytes), el campo Desplazamiento de fragmento no puede indicar un desplazamiento de bytes. Con 13 bits el máximo valor es de 8.191. El desplazamiento de fragmento debe ser de 16 bits de tamaño para indicar un desplazamiento de bytes.

Como se necesitan 16 bits para indicar el tamaño de datos de IP máximo y sólo se dispone de 13 bits en este campo, cada valor del desplazamiento del fragmento debe representar 3 bits. Por tanto, este campo se define en términos de bloques de 8 bytes, llamados bloques de fragmento.

Durante la fragmentación, los datos se dividen en fronteras de 8 bytes y en cada fragmento se sitúa el máximo número de bloques de fragmento de 8 bytes. El campo Desplazamiento de fragmento se establece para indicar el bloque de inicio de fragmento relativo al fragmento inicial de los datos. Para cada fragmento que se crea en un enrutador, se copia la cabecera original de IP y se cambian los siguientes campos:

- **Tamaño de la cabecera.** Puede cambiar o no dependiendo de las opciones presentes y si dichas opciones se copian en todos los fragmentos o sólo en el primero.
- **TTL.** Se decrementa en 1.
- **Tamaño total.** Cambia para reflejar la nueva cabecera de IP y el nuevo tamaño de los datos.
- **MF.** A 1 para el primero y los fragmentos centrales. A 0 para el último fragmento.
- **Desplazamiento de segmento.** Se fija para indicar la posición del fragmento en los bloques de fragmento relativo a los datos originales.
- **Suma de comprobación de la cabecera.** Se recalcula de acuerdo a los cambios realizados en los campos de la cabecera de IP.

El campo Identificación no cambia en ningún fragmento.

Fragmentación de un fragmento

Es posible que los fragmentos se vuelvan a fragmentar. En este caso, cada fragmento se fragmenta para casar con la MTU del enlace al que se va a reenviar. El proceso de fragmentar un fragmento es un poco distinto de fragmentar el datagrama de IP original. La diferencia es cómo se establece el indicador MF.

Cuando se fragmenta un fragmento, el indicador MF es siempre 1, excepto cuando el fragmento de un fragmento es el último fragmento del último fragmento.

- Si un enrutador de IP fragmenta un fragmento anterior que sea el primero 0 uno intermedio, todos los fragmentos tendrán su indicador MF a 1.
- Si un enrutador de IP fragmenta un fragmento anterior que era el último, todos los fragmentos excepto el último tendrán su indicador MF a 1.

Por tanto, independientemente de cuantas veces se fragmente un datagrama de IP, sólo uno de los fragmentos tendrá su indicador MF a 0, indicando que es el último fragmento del datagrama de IP original.

Evitando la fragmentación

Aunque la fragmentación permite que los nodos de IP se conecten independientemente de las distintas MTU en los segmentos de red intermedios y sin intervención del usuario, el fragmentado y reensamblado es un proceso relativamente costoso, tanto en los enrutadores, o host de reenvío, como en el host de destino. En la Internet actual, la fragmentación se desaconseja; los enrutadores de Internet están suficientemente ocupados con el reenvío de tráfico de IP.

Se puede evitar la fragmentación tomando una de las siguientes medidas:

- Establezca el indicador DF a 1 en todos los datagramas enviados.

- Descubra la MTU de IP que admiten todos los enlaces en la ruta desde el origen al destino (la MTU de la ruta).

Configuración de DF con PING

Se puede usar la utilidad PING con la opción <-f> para establecer el indicador DF a 1 en los mensajes de eco de ICMP. La sintaxis es:

```
PING -f [dirección de IP o nombre de host]
```

Por ejemplo, para hacer un ping a 10.0.0.1 y establecer DF a 1:

```
PING -f 10.0.0.1
```

El valor del indicador DF predeterminado para los mensajes de eco de ICMP que envía PING es 0 (se permite la fragmentación).

Configuración del Tamaño de datos con PING

Se puede usar la utilidad PING con la opción <-l> para establecer el tamaño de los datos de ICMP en los mensajes de eco de ICMP. La sintaxis es:

```
PING -l [tamaño de los datos] [dirección de IP o nombre de host]
```

El valor del tamaño se expresa en decimal.

Por ejemplo, para hacer ping a 10.0.0.1 con un tamaño de datos de ICMP de 5000:

```
PING -l 5000 10.0.0.1
```

El tamaño predeterminado de los datos de ICMP que envía PING es 32.

El tamaño de los datos de ICMP no es el mismo que el de los datos de IP debido a que los mensajes de eco incluyen una cabecera de ICMP de 8 bytes. Por tanto, para calcular el tamaño de los datos de IP, añada 8 al tamaño de los datos de ICMP. Para calcular el tamaño del datagrama de IP, añada 20 al tamaño de los datos de IP. Para hacer ping con un eco del tamaño máximo que permita la tecnología de la Interfaz de red, reste 28 de la MTU de IP. Por ejemplo, para hacer ping con el tamaño máximo en una red Ethernet, que tiene una MTU de IP de 1500, el comando PING sería:

```
PING -l 1472 10.0.0.1
```

Uso de PING para crear paquetes con fragmentación fuente

Se puede usar la utilidad PING de Windows 2000 con la opción <-l> para producir paquetes con fragmentación fuente. Hacer ping con un tamaño de datos de ICMP mayor que [MTU de IP-28] bytes genera paquetes fragmentados. Por ejemplo, hacer ping desde un nodo Ethernet con un tamaño de 1472 o menor no producirá paquetes fragmentados. Si se hace con un tamaño mayor de 1472 se producirán paquetes fragmentados.

Fragmentación y entornos de puentes de traducción

Los puentes de traducción es el mecanismo de interconexión de dos tecnologías de Interfaz de red diferentes en la misma red mediante un dispositivo de Nivel 2 como un puente o un conmutador. Un uso habitual de los puentes de traducción es conectar un segmento de Ethernet con otro Token Ring. En las redes modernas, este tipo de puentes se tienen con conmutadores que conectan nodos de Ethernet a 10 ó 100 Mbps a servidores en los puertos de alta velocidad. Las tecnologías de puertos de alta velocidad incluyen FDDI, Gigabit Ethernet y ATM.

El obstáculo más serio para los puentes de traducción es la diferencia en las MTU entre las distintas tecnologías del Nivel de interfaz de red. Como no existe un enrutador en medio, no se puede confiar la fragmentación ni en el proceso de descubrimiento de la MTU de la ruta para las distintas MTU. Un puente de traducción no tiene la capacidad de fragmentar. Las tramas mayores que la MTU del

enlace donde se han de reenviar serán descartadas silenciosamente por el puente.

Cuando se establece una conexión de TCP, ambos nodos se comunican la MTU en forma de opción del Tamaño máximo de segmento, MSS (Maximum Segment Size), de TCP. Tras recibir cada uno el MSS de TCP del otro, ambos nodos llegan al acuerdo de enviar segmentos de TCP del menor MSS del de los dos nodos. Sin embargo, a pesar de esta negociación de MTU, una comunicación apropiada entre todos los nodos de un entorno de puentes de traducción puede requerir la modificación de la MTU de IP de nodos concretos.

Si tenemos dos conmutadores de Ethernet conectados por una red troncal Ethernet. En cada conmutador Ethernet se encuentra un puerto conectado a un anillo FDDI que contiene servidores de aplicación. Cuando los servidores en el mismo anillo se comunican unos con otros, pueden enviar paquetes con una MTU de FDDI de 4.352 bytes. Cuando un nodo de Ethernet en uno de los conmutadores usa TCP para conectarse con un servidor de aplicaciones en un anillo de FDDI, la opción MSS de TCP reduce la MTU de TCP, basada en datagramas, a 1.500.

Sin embargo, considere la comunicación entre servidores de aplicaciones en distintos anillos de FDDI. Al crear la conexión TCP, cada servidor negocia un MSS de TCP basado en FDDI. Por tanto, los conmutadores de Ethernet descartarán silenciosamente los datagramas de IP de tráfico TCP enviados entre los servidores de los distintos anillos que tengan un tamaño superior a 1.500 bytes.

La solución a este problema es configurar manualmente la MTU de IP de los servidores de aplicación con la menor MTU de IP de todos los enlaces dentro de la red con puentes de traducción.

Si establecemos la MTU de IP de los servidores de aplicación en los anillos de FDDI en 1.500, los puentes de traducción pueden enviar datagramas de IP entre los anillos FDDI. El cambio de la MTU de los servidores de aplicación significa que cuando envíen paquetes a servidores de aplicación en el mismo anillo, los paquetes se enviarán con una MTU tan reducida como 1.500, con menor eficiencia que cuando la MTU de FDDI predeterminada era de 4.352. Sin embargo, es preferible una menor eficiencia entre los servidores del mismo anillo que no tener ninguna entre servidores de distintos anillos.

Opciones de IP

Las opciones de IP son campos adicionales que se añaden a la cabecera estándar de 20 bytes de IP. Aunque no se requiere que las opciones existan en todas las cabeceras de IP, se requiere la capacidad de procesar los campos de opción de IP. Las opciones de IP se usan muy infrecuentemente con objeto de prueba de la red.

El tamaño de la parte opciones de IP de la cabecera de IP variará en tamaño según las opciones de IP que se usen. Las distintas opciones también varían en tamaño, desde un único byte hasta múltiples cantidades de 4 bytes. Recuerde que el máximo tamaño de la cabecera de IP que se puede indicar en el campo Tamaño de la cabecera es de 60 bytes. Con una cabecera estándar de IP de 20 bytes se dejan 40 bytes para opciones de IP.

Copia

El campo Copia es de un bit y se usa cuando un enrutador o un host de envío debe fragmentar un datagrama de IP. Cuando este campo vale 0, se debe copiar la opción de IP sólo en el primer fragmento. Cuando este campo vale 1, la opción se debería copiar en todos los fragmentos.

Clase de opción

El campo Clase de opción tiene dos bytes y se usa para indicar la clase general de la opción. Las clases de opción definidas, son:

- 0 Control de la red.

- 1 Reservado para uso futuro.
- 2 Depuración y medidas.
- 3 Reservado para uso futuro.

Número de opción

El campo Número de opción tiene 5 bits y se usa para indicar una opción concreta dentro de la clase de opción. Cada clase de opción puede tener hasta 32 números de opción distintos. En la tabla se listan las clases y los números de opción para equipos no militares.

Clases y números de opción		
Clase de opción	Número de opción	Descripción
0	0	Fin de la lista de opciones. Opción de 1 byte que se usa para indicar el fin de una lista de opciones.
0	1	No operación. Opción de 1 byte que se usa para alinear los bytes de una lista de opciones.
0	3	Enrutamiento fuente débil. Una opción de longitud variable que se usa para enrutar un datagrama por una ruta especificada donde se pueden decidir rutas alternativas.
0	7	Registro de ruta. Una opción de tamaño variable que se usa para trazar una ruta a través de un conjunto de redes de IP.
0	9	Enrutamiento fuente estricto. Una opción de tamaño variable que se usa para especificar una ruta donde no se pueden decidir rutas alternativas.
0	20	Alerta al enrutador de IP. Una opción de tamaño fijo que se usa para informar al enrutador que se necesita procesamiento adicional del datagrama.
2	4	Marca de tiempo de Internet. Una opción de tamaño variable que se usa para registrar una serie de marcas de tiempo en cada salto.

Fin de la lista de opciones

Código de opción 00000000

La opción Fin de la lista de opciones siempre es un byte que se usa al final de las opciones de IP cuando éstas no coinciden en la frontera de 4 bytes. Esta opción sólo se utiliza al final de todas las opciones, no al final de cada una de ellas.

No operación

Código de opción 00000001

La opción No operación siempre es un único byte y se usa entre las opciones de IP cuando una opción no casa en un múltiplo de 4 bytes.

Registro de ruta

Código de opción 00000111
Tamaño de la opción
Puntero a la siguiente ranura
Primera dirección de IP
Segunda dirección de IP

La opción Registro de ruta es una opción de tamaño variable que se usa para registrar las direcciones de IP de las interfaces lejanas de los enrutadores que atraviesan por el conjunto de redes de IP. La interfaz lejana es la interfaz del enrutador por la que se reenvía el datagrama de IP. Se presupone que la interfaz lejana es la más lejana respecto al host emisor.

Según se reenvía el datagrama de un enrutador a otro, cada enrutador añade su dirección de IP a la lista; cada enrutador modifica también el campo Puntero a la siguiente ranura. Se registra la ruta desde el host de origen hasta el host de destino. Para obtener la ruta completa debe haber suficiente sitio en la cabecera de opciones de Registro de ruta. Al contrario que en el enrutamiento fuente de Token Ring, el número de ranuras para direcciones de IP especifica el host emisor y se establece en la cabecera de IP.

La opción Registro de ruta tiene los siguientes campos:

- **Código de opción.** Se establece a 7 (Bit de copia=0, Clase de opción=0, Número de opción=7).
- **Tamaño de la opción.** Se establece por el host emisor al número de bytes de la opción Registro de ruta.
- **Puntero a la siguiente ranura.** Indica el desplazamiento al byte (desde 1) dentro de la opción Registro de ruta de la siguiente dirección de IP libre. El valor mínimo del puntero es de 4.
- **Primera dirección de IP, Segunda dirección de IP.** Indica la dirección de IP de la interfaz lejana de los enrutadores. Con un máximo de 40 bytes en la parte de opciones de IP de la cabecera de IP hay espacio suficiente para un máximo de nueve direcciones de IP.

Procesado del Registro de ruta

Un enrutador de IP que recibe un datagrama de IP con la opción Registro de ruta compara los campos Tamaño de opción y Puntero a la siguiente ranura. Si el campo Puntero a la siguiente ranura es menor que el campo Tamaño de opción, queda espacio para direcciones de IP. El enrutador registra la dirección de IP de la interfaz que reenvía el datagrama en el siguiente campo dirección de IP disponible; el enrutador también actualiza el campo Puntero a la siguiente ranura sumándole 4. Si el valor del campo Puntero a la siguiente ranura es mayor que el campo Tamaño de opción, ya se han usado todas las ranuras para direcciones de IP por enrutadores previos. El enrutador reenvía el datagrama sin modificar la opción Registro de ruta.

Ambos hosts, deben acordar que se procesará la información de la opción Registro de ruta en los datagramas que se envían. Si uno de ellos no está de acuerdo, la información de la opción Registro de ruta se ignora tras recibirlo y no se devuelven los datagramas de IP con la opción Registro de ruta.

Como el tamaño de la opción Registro de ruta no es un múltiplo de 4 bytes, se debe añadir una opción Fin de opciones (si no hay más opciones) o una opción No operación (si hay más opciones) para asegurar que la cabecera de IP es de un tamaño múltiplo de 4 bytes.

Configuración de la opción Registro de ruta con PING

Se puede usar la utilidad PING con la opción <-r> para añadir la opción Registro de ruta y

establecer el número de ranuras para direcciones de IP de la opción dentro de un mensaje de eco de ICMP. Su sintaxis es:

```
PING -r [ranuras para direcciones de IP] [dirección de IP o nombre de host]
```

donde el valor de ranuras para direcciones de IP se expresa en decimal.

Por ejemplo, para hacer ping a 10.0.0.1 con siete ranuras para direcciones de IP, use el comando:

```
PING -r 7 10.0.0.1
```

Enrutamiento fuente débil y estricto

El proceso de enrutamiento de IP en los enrutadores se realiza mediante la comparación de la dirección de IP de destino con las entradas de una tabla local de enrutamiento. Cada enrutador realiza una decisión de reenvío. Sin embargo, a veces es necesario especificar la ruta que debe seguir un datagrama de IP independientemente de las entradas de la tabla de enrutamiento del enrutador. Si la ruta se especifica antes de que el host emisor envíe el datagrama; es lo que se conoce como enrutamiento fuente.

Por ejemplo, en un conjunto de redes de IP multirruta, donde existe más de una ruta entre distintos conjuntos de redes de IP, los enrutadores seleccionan la mejor de ellas según una métrica de menor coste. Una vez el enrutador ha determinado todas las mejores rutas, las rutas de mayor coste no se usan a no ser que la topología de las redes cambie. Para comprobar que las rutas de mayor coste contienen enlaces válidos, se debe utilizar enrutamiento fuente.

El enrutamiento fuente en IP se realiza especificando las direcciones de IP de las interfaces cercanas de los enrutadores deseados entre el origen y el destino. En cada trayecto del viaje, la dirección de IP de destino de la cabecera de IP se establece a la dirección de IP de la siguiente interfaz cercana del siguiente enrutador. IP admite tanto enrutamiento fuente débil como estricto. En el enrutamiento fuente débil la siguiente dirección de IP de un enrutador no tiene por qué ser un enrutador vecino; puede encontrarse varios saltos más allá. En el enrutamiento fuente estricto, la dirección de IP del siguiente enrutador debe ser un enrutador vecino (a un solo salto).

El enrutamiento fuente de IP también registra la ruta de la misma forma que la opción Registro de ruta. En cada paso del trayecto se registra la dirección de IP de la interfaz de cada enrutador que realiza el reenvío del datagrama de IP.

Opción Enrutamiento fuente estricto

Código	de	opción	10001001	
Tamaño	de	la	opción	
Puntero	a	la	siguiente	ranura
Primera		dirección	de	IP
Segunda	dirección de IP			

La opción de enrutamiento fuente estricto tiene los siguientes campos:

- **Código de opción.** Se establece a 137 (Bit de copia=1, Clase de opción=0, Número de opción=9).
- **Tamaño de la opción.** Se establece por el host emisor al número de bytes de la opción Enrutamiento fuente estricto.
- **Puntero a la siguiente ranura.** Indica el desplazamiento al byte (desde 1) dentro de la siguiente opción Enrutamiento fuente estricto del enrutador. El valor mínimo del campo Puntero a la siguiente ranura es de 4. El campo Puntero a la siguiente ranura se usa también de la misma manera que la opción Registro de ruta para determinar la posición de la siguiente ranura para la dirección de IP donde registrar la ruta.

- **Primera dirección de IP.** Segunda dirección de IP. Las establece el host emisor a la serie de sucesivos enrutadores de destino en el caso de enrutamiento fuente estricto; también las establecen los enrutadores de IP con las direcciones de las interfaces de reenvío. Con un máximo de 40 bytes en la parte de opciones de IP de la cabecera de IP hay espacio suficiente para un máximo de nueve direcciones de IP.

Cuando un host emisor envía un datagrama de IP con la opción enrutamiento fuente estricto, el host emisor:

1. Establece el valor del Puntero a la siguiente ranura en 4.
2. Sitúa en la primera dirección de IP en el enrutamiento fuente estricto en el campo dirección de IP de destino de la cabecera de IP.

Cuando un enrutador de IP recibe un datagrama de IP con la opción Enrutamiento fuente estricto, compara los campos Tamaño de opción y Puntero a la siguiente ranura. Si el campo Puntero a la siguiente ranura es menor que el campo Tamaño de opción, el enrutador:

1. Suma 4 al valor del campo Puntero a la siguiente ranura.
2. Sustituye la dirección de IP de destino por la dirección de IP que está registrada en la siguiente ranura, según el nuevo valor del campo Puntero a la siguiente ranura.
3. Registra la dirección de IP de la interfaz de reenvío en la ranura anterior.

Si la dirección de IP de destino no se alcanza usando una red conectada directamente, la dirección de IP de un enrutador o host vecino, el datagrama de IP se descarta y se envía de vuelta al host emisor un mensaje de ICMP de Destino inalcanzable-Error en la ruta fuente.

Si el valor del campo Puntero a la siguiente ranura es mayor que el valor del campo Tamaño de opción, el datagrama de IP ha llegado a su destino final.

Como el tamaño de la opción Enrutamiento fuente estricto no es múltiplo de 4 bytes, se debe añadir una opción de Fin de opciones (si no hay más opciones) o una opción de No operación (si hay más opciones tras la opción de Enrutamiento fuente estricto) para asegurar que la cabecera de IP tiene un tamaño múltiplo de 4 bytes. de opciones.

Configuración de la opción Enrutamiento fuente estricto con PING

Se puede usar la utilidad PING de Windows 2000 con la opción <-k> para añadir la opción de Enrutamiento fuente estricto. La utilidad PING también se puede usar para establecer las direcciones de IP de los sucesivos enrutadores y del destino final en los mensajes de Eco de ICMP. Su sintaxis es:

```
PING -k [dirección de IP del primer salto] [dirección de IP del
segundo salto] ... [dirección de destino de IP]
```

Por ejemplo, para hacer ping a 10.0.0.1 a través de las interfaces de enrutadores vecinos 192.168.1.1 y 192.168.2.1, use el siguiente comando:

```
PING -k 192.168.1.1 192.168.2.1 10.0.0.1
```

Opción de Enrutamiento fuente débil

Código	de	opción	10000011
Tamaño	de	la	opción
Puntero	a	la	siguiente
Primera		dirección	de
Segunda		dirección de IP	IP

La opción Enrutamiento fuente débil tiene los siguientes campos:

- **Código de opción.** Se establece a 131 (Bit de copia=1, Clase de opción=0, Número de opción=3).
- **Tamaño de la opción.** Se establece por el host emisor al número de bytes de la opción Enrutamiento fuente débil.
- **Puntero a la siguiente ranura.** Indica el desplazamiento al byte (desde 1) dentro de la siguiente opción Enrutamiento fuente débil del enrutador. El valor mínimo del campo Puntero a la siguiente ranura es de 4. El campo Puntero a la siguiente ranura se usa también de la misma manera que la opción Registro de ruta para determinar la posición de la siguiente ranura para la dirección de IP donde registrar la ruta.
- **Primera dirección de IP.** Segunda dirección de IP. Las establece el host emisor a la serie de sucesivos enrutadores de destino en el caso de enrutamiento fuente débil; también las establecen los enrutadores de IP con las direcciones de las interfaces de reenvío. Con un máximo de 40 bytes en la parte de opciones de IP de la cabecera de IP hay espacio suficiente para un máximo de nueve direcciones de IP.

Cuando un host emisor envía un datagrama de IP con la opción Enrutamiento fuente débil, este host:

1. Establece el valor del campo Puntero a la siguiente ranura en 4.
2. Sitúa la primera dirección de IP de la ruta fuente débil en la dirección de IP de destino de la cabecera de IP.

Cuando un enrutador de IP recibe un datagrama de IP con la opción Enrutamiento fuente débil, compara los campos Tamaño de opción y Puntero a la siguiente ranura. Si el valor del campo Puntero a la siguiente ranura es menor que el valor del campo Tamaño de opción, el enrutador:

1. Suma 4 al valor del campo Puntero a la siguiente ranura.
2. Sustituye la dirección de IP de destino de la cabecera de IP por la dirección que se encuentra registrada en la siguiente ranura, de acuerdo con el nuevo valor del campo Puntero a la siguiente ranura.
3. Registra la dirección de IP de la interfaz de reenvío en la ranura anterior.

Si el valor del campo Puntero a la siguiente ranura es mayor que el valor del campo Tamaño de opción, el datagrama de IP ha llegado a su destino final.

Como el tamaño de la opción Enrutamiento fuente débil no es múltiplo de 4 bytes, se debe añadir una opción Fin de opciones (si no hay más opciones) o una opción No operación (si hay más opciones) para asegurar que el tamaño de la cabecera de IP sea múltiplo de 4 bytes.

Configuración de la opción Enrutamiento fuente débil con PING

Se puede usar la utilidad PING de Windows 2000 con la opción <-j> para añadir la opción Enrutamiento fuente débil. Además, se usa para establecer las direcciones de IP de los sucesivos enrutadores y el destino final de los mensajes de Eco de ICMP. Su sintaxis es:

```
PING -j [dirección de IP del primer salto] [dirección de IP del
segundo salto] ... [dirección de IP de destino]
```

Por ejemplo, para hacer ping a 10.0.0.1 a través de las interfaces de enrutadores vecinos 192.168.1.1 y 192.168.2.1, use el siguiente comando:

```
PING -j 192.168.1.1 192.168.2.1 10.0.0.1
```

Alerta al enrutador de IP

Código de opción de opción 10010100

Tamaño de opción 00000100
Valor

La Alerta al enrutador de IP se usa para indicar a los enrutadores de IP que se requiere un procesamiento adicional de los datagramas de IP, incluso aunque el datagrama de IP no vaya dirigido a dicho enrutador. La opción Alerta al enrutador de IP se usa por el Protocolo de reserva de recursos (RSVP) y el Protocolo de administración de grupos de Internet (IGMP) versión 2. Por ejemplo, cuando un enrutador recibe un datagrama de IP con la opción Alerta al enrutador de IP, observa el campo Protocolo de IP para ver si los datos necesitan un procesamiento adicional antes de realizar la decisión de reenvío.

Esta opción tiene los siguientes campos:

- **Código de opción.** Se establece en 148 (Bit de copia=1, Clase de opción=0, Número de opción=20).
- **Tamaño de opción.** Se establece en un tamaño fijo de 4.
- **Valor.** Campo de 2 bytes con valor 0. El resto de valores está reservado. El valor 0 indica que el enrutador debe examinar el paquete.

Marcas de tiempo de Internet

Código de opción 01000100
Tamaño de opción
Puntero a la siguiente ranura
Desbordamiento
Indicador
Primera dirección de IP
Segunda dirección de IP

La opción Marca de tiempo se usa para registrar el momento en que llega un datagrama de IP a cada enrutador de IP en la ruta desde el host de origen hasta el de destino. La opción Marca de tiempo es similar a la opción Registro de ruta en que el nodo emisor crea entradas en blanco en la cabecera de IP que los enrutadores rellenan según el paquete viaja a través de un conjunto de redes de IP. Cada entrada consiste en la dirección de IP del enrutador y una marca de tiempo, un entero de 32 bits para indicar el número de milisegundos desde medianoche, en tiempo universal. Si no se usa tiempo universal, el bit de mayor orden del campo se pone a 1.

La opción Marca de tiempo de Internet tiene los siguientes campos:

- **Código de opción.** Se establece en 68 (Bit de copia=0, Clase de opción=2, Número de opción=4).
- **Tamaño de opción.** Lo establece el host emisor al número de bytes de la opción Marca de tiempo de Internet.
- **Puntero a la siguiente ranura.** Indica el desplazamiento al byte (desde 1) dentro de la siguiente opción Marca de tiempo de Internet de la siguiente ranura para el registro de la dirección de IP y la marca de tiempo. El valor mínimo del campo Puntero a la siguiente ranura es de 5.
- **Desbordamiento.** Lo establecen los enrutadores para indicar el número de enrutadores que fueron capaces de registrar su dirección de IP y su marca de tiempo.
- **Indicadores.** Los establece el host emisor para indicar el formato de las ranuras Dirección de IP/Marca de tiempo. Si Indicadores = 0, se omite la dirección de IP. De esta forma se pueden registrar hasta nueve marcas de tiempo. Si Indicadores = 1, se registra la dirección de IP, lo que permite registrar cuatro pares de dirección de IP/marca de tiempo. El formato

de la opción de Marca de tiempo de Internet que se muestra presupone que Indicadores = 1. Si Indicadores = 3, el nodo emisor especifica las direcciones de IP de los enrutadores sucesivos: se registra una marca de tiempo sólo si coincide la dirección de IP de la ranura con la del enrutador.

- **Primera Dirección de IP.** Primera marca de tiempo. Los enrutadores registran las direcciones de IP y marcas de tiempo de los enrutadores atravesados (Indicadores = 1), o especificados (Indicadores = 3).

Cuando un host emisor envía un datagrama de IP con la opción de Marca de tiempo, este host emisor:

1. Establece el valor del campo Puntero a la siguiente ranura a 5.
2. Para la ruta especificada (Indicadores = 3), sitúa la serie de direcciones de IP en la opción Marca de tiempo de Internet.

Cuando un enrutador recibe un datagrama de IP con esta opción, compara los campos Tamaño de opción y Puntero a la siguiente ranura. Si el valor de Puntero a la siguiente ranura es menor que el valor del campo Tamaño de opción:

- Si Indicadores = 3, el enrutador sustituye la dirección de IP de destino de la cabecera de IP por la dirección de IP registrada en la siguiente ranura, de acuerdo al campo Puntero a la siguiente ranura.
- Si Indicadores = 1 o Indicadores = 3, el enrutador registra la dirección de IP de la interfaz en la que se recibió el datagrama de IP en la misma ranura.
- Si Indicadores = 0, el enrutador registra la marca de tiempo y suma 4 al campo Puntero a la siguiente ranura. Si Indicadores = 1, el enrutador registra la marca de tiempo tras la dirección de IP y suma 8 al campo Puntero a la siguiente ranura. Si Indicadores = 3, el enrutador sustituye la dirección de IP y suma 4 al campo Puntero a la siguiente ranura.

Si el valor del campo Puntero a la siguiente ranura es mayor que el valor del campo Tamaño de opción, el enrutador incrementa el campo Desbordamiento. Si el campo Desbordamiento vale 15 antes de incrementarlo, se envía un mensaje de Problema de los parámetros de ICMP de vuelta al host de origen.

Configuración de la opción Marcas de tiempo de Internet con PING

Se puede usar la utilidad PING de Windows 2000 con la opción <-s> para enviar un mensaje de Eco de ICMP con marcas de tiempo. Su sintaxis es:

```
PING -s [ranuras] [dirección de IP de destino]
```

Por ejemplo, para hacer ping a la dirección de IP 10.0.0.1 usando marcas de tiempo de Internet con tres ranuras, use el siguiente comando:

```
PING -s 3 10.0.0.1
```