Clase	Número	Longitud (bytes)	Nombre	Descripción
				dirección *IP* de la interfaz por donde lo re-envían.
0	9	Variable	Enrutamiento de Fuente Estricto (*Strict Source Routing*)	Listado de direcciones IP, escrito en origen, que se corresponde a las direcciones de *routers* por los que el datagrama con esta opción debe transitar obligatoriamente, con prohibición de procesamiento en otro que no se encuentre en el listado.
2	4	Variable	Sello de Tiempo (*Timestamp*)	Esta opción obliga a los *routers* que procesan el datagrama a escribir un sello de tiempo al momento del re-envío.
2	18	12	*Traceroute*	Para apoyo de la herramienta del mismo nombre.

9.3 Protocolo ARP (Address Resolution Protocol)

La comunicación entre clientes y servidores en Internet se facilita por el uso de nombres en lugar de direcciones IP. El usuario cliente conoce el nombre del sitio al que desea acceder y genera un mensaje de petición a la aplicación con la que desea comunicarse. Este mensaje debe ser encapsulado en un segmento TCP o un datagrama UDP, y luego en un paquete IP. Es decir que ese nombre debe traducirse de alguna manera a una dirección IP destino. Esta tarea la realiza un servicio denominado Servicio de Nombres de Dominio (DNS, Domain Name Service) de modo transparente para el usuario. Una vez obtenida la dirección IP del destino, se puede completar el armado del paquete IP, debiendo éste ser encapsulado en el formato que corresponda al nivel de enlace.

Se presenta entonces la necesidad algún mecanismo que ofrezca la dirección destino correspondiente a este nivel, por ejemplo una dirección MAC. Existe una gran diferencia en el significado de estas direcciones MAC, que sólo posee un alcance local, con respecto a las direcciones IP, cuyo alcance es global.

A modo de ejemplo, supongamos que un alumno, desde su casa, desea consultar material de estudio de Redes de Datos. En el navegador de su PC escribirá el nombre del servidor Web de la Facultad de Ingeniería: http://www.fi.mdp.edu.ar/electronica. Este servidor se encuentra conectado mediante una placa *Ethernet* a la red interna de la Facultad de Ingeniería. Aunque la cátedra le informara a cada alumno la dirección MAC del servidor, este dato no aportaría nada a una comunicación realizada desde fuera de la red de la Facultad de Ingeniería. Cuando el alumno, desde su computadora en casa, realice

el pedido de consulta, el servicio DNS de su propio proveedor le permitirá obtener la dirección IP del servidor Web destino pero, al momento de encapsular el mensaje a nivel de enlace, lo que interesa es dirigirlo al servidor de su propio proveedor de Internet, para que este realice el enrutamiento apropiado del pedido.

Se ha mencionado que el enrutamiento IP es del tipo salto a salto (*hop-by-hop*). Esto significa que, si el vínculo con el ISP funciona correctamente, será el *router* de éste el que conozca mediante la información almacenada en su Tabla de Enrutamiento, la dirección del siguiente *router* en el camino sobre la red desde la casa del alumno a la Facultad de Ingeniería. Es decir que el camino entre fuente y destino es una serie de saltos entre *routers* hasta llegar a destino final. En cada uno de estos saltos, hay una comunicación real a nivel de enlace, en la que importa conocer la dirección a nivel de enlace del *router* del siguiente salto. La dirección MAC del servidor Web sólo importa en la entrega final del mensaje, desde el *router* de entrada a la Facultad de Ingeniería a la ubicación del servidor dentro de esa red.

Dicho esto, se presentará primero un caso simplificado, en el que el alumno desea realizar la consulta pero ahora sentado frente a una máquina dentro de la Facultad, es decir, en la misma red que el servidor.

En cualquiera de los casos mencionados, se precisa un mecanismo que permita la traducción o relación entre direcciones IP y direcciones MAC. Este trabajo lo realiza el Protocolo de Resolución de Direcciones ARP, cuya aplicación es posible sólo en el caso de redes de difusión.

La Fig. 9.9 plantea la situación a resolver cuando ambos actores de la comunicación se encuentran en una misma red LAN, cuya numeración IP es 192.168.0.0. Supongamos que la máquina 1 desea comunicarse con la máquina 3 de la misma red. Ya se ha explicado cómo se puede obtener una dirección IP a partir de un nombre, ahora interesa entender el mecanismo que permite obtener una dirección MAC a partir de esa dirección IP.

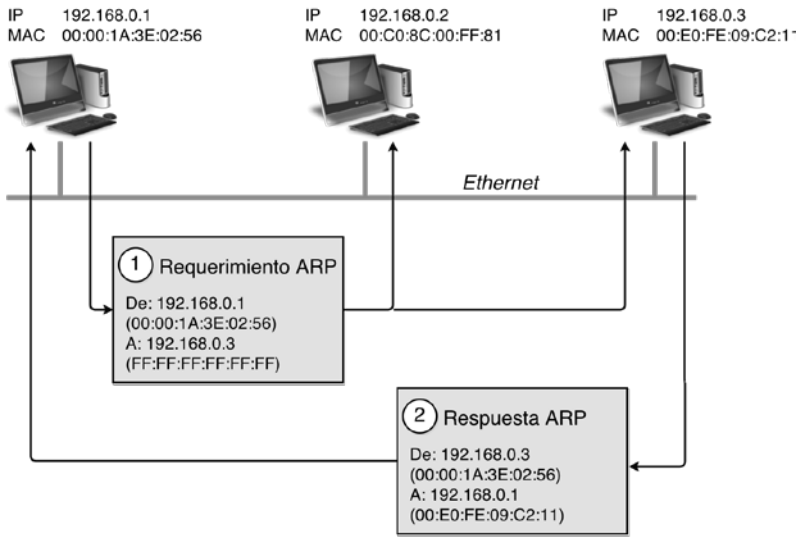

Figura 9.9 - Protocolo ARP.

La máquina 1 puede emitir un mensaje por *broadcast* a nivel de enlace que contenga la dirección IP destino, en este caso 192.168.0.3. Todos los dispositivos de la LAN pueden ver este mensaje, pero sólo la máquina 3 reconocerá su propia dirección en este mensaje y enviará su dirección MAC al interesado, en este caso 192.168.0.1 . Es decir que, a diferencia del requerimiento, la respuesta es por *unicast*. Complementariamente, la máquina 1, al recibir la respuesta, puede guardarla en memoria para futuras comunicaciones con la máquina 3. Esto es lo que se conoce como mecanismo de *caching*. Los datos que se guardan en la memoria se conocen como Cache ARP o Tabla ARP.

El cache ARP tiene la forma de una tabla, con pares de direcciones IP y MAC que se corresponden entre sí. Existe un cache de este tipo por cada interfaz de tipo *Ethernet* que posea cualquier dispositivo. Si una máquina posee más de una placa *Ethernet*, mantendrá una tabla por cada placa de red. Los datos no permanecen en la tabla por tiempo indefinido, sino que tienen un tiempo de vida, vencido el cual, se remueve la información. Esta remoción se hace para evitar que las tablas crezcan de manera indefinida y para dar mayor flexibilidad al esquema de resolución en caso de reemplazo de placas o cambios de direcciones IP. En general, las implementaciones ARP fijan un tiempo de vida por línea de entre 10 y 20 $minutos$.

El caché se carga no sólo en el dispositivo que inicia la resolución, sino también en el que es destinatario de la misma. Algunas implementaciones también cargan el caché con el mensaje de *broadcast*, aunque no sean destinatarios del requerimiento. Así pueden anexar la línea que caracteriza al dispositivo que inicia el requerimiento. Esto es posible debido a la información que cargan los mensajes del protocolo ARP.

Los mensajes ARP poseen un formato como el que se presenta en la Fig. 9.10. El primer campo, el de Tipo de Hardware (16 $bits$) lleva la codificación correspondiente a las redes *Ethernet*. El campo Tipo de Protocolo (16 $bits$) es complementario del anterior y se refiere al nivel de red, siendo el valor $0x800$ correspondiente a IPv4. El campo Longitud de la Dirección de Hardware (8 $bits$) llevará el valor 6 para *Ethernet*, en tanto que el campo Longitud de Dirección de Protocolo (8 $bits$) será 4 para IPv4. El campo Código de Operación (16 $bits$) sirve para distinguir entre preguntas (valor 1) y respuestas (valor 2).

Los dos campos que siguen llevan escrita la Dirección de Hardware (48 $bits$) y la Dirección IP (32 $bits$) del transmisor del mensaje ARP. Los últimos dos campos se refieren al destinatario del mensaje y, en el caso de un requerimiento ARP, la parte de Dirección de Hardware del Target se rellena con "0", ya que se trata de la dirección que se pretende averiguar. En el campo Dirección de Protocolo del Target se carga la dirección IP por la que se pregunta. La respuesta también tiene cuatro direcciones que se escriben en orden inverso al del requerimiento, ya que se intercambian los roles entre transmisor y receptor del mensaje. En total, el mensaje tiene una longitud de 28 $bytes$ y viaja encapsulado en una trama *Ethernet*, cuya longitud mínima es de 64 $bytes$. Por este motivo, los mensajes ARP se rellenan con una serie de "0", hasta alcanzar la longitud mínima requerida.

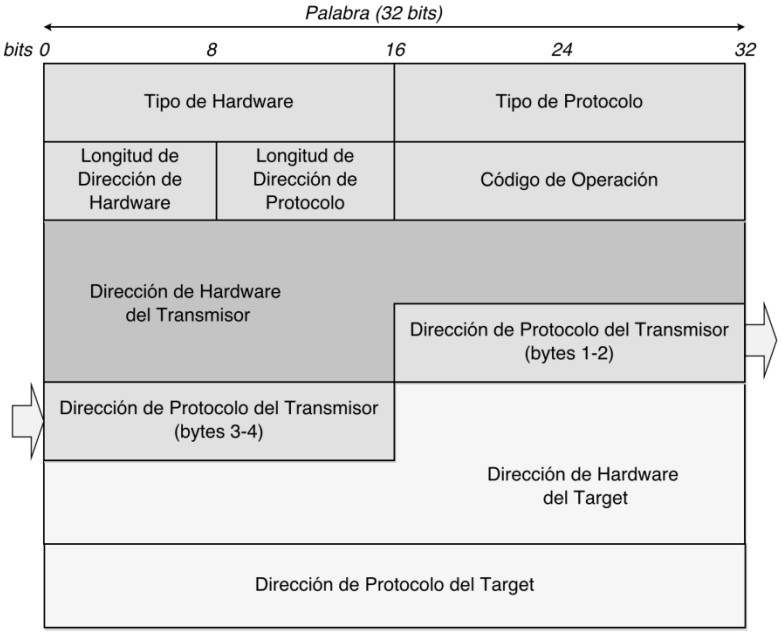

Figura 9.10 - Mensaje ARP.

Existen programas que permiten analizar los paquetes que circulan en una red. Estos programas, conocidos como husmeadores o *sniffers*, colocan a la placa de red en un modo de funcionamiento denominado promiscuo, en el cual la placa levanta todas las tramas que pasan por la red, aún las que no van dirigidas a ella.

A continuación se presenta un ejemplo de mensaje ARP encapsulado en *Ethernet*, levantado desde una red cableada con un *sniffer*:

Ethernet II	Src: 00:1f:d0:aa:bb:cc Dst: ff:ff:ff:ff:ff:ff Type: ARP (0x0806) Trailer: 000000000000000000000000000000000000
Address Resolution Protocol	Hardware type: Ethernet (0x0001) - Protocol type: IP (0x0800) - Hardware size: 6 - Protocol size: 4 - Opcode: request (0x0001) - Sender MAC address: 00:1f:d0:aa:bb:cc - Sender IP address: 192.168.0.1 - Target MAC address: 00:00:00:00:00:00 - Target IP address: 192.168.0.3

En este caso, la máquina con dirección IP $192.168.0.1$ y dirección MAC $00{:}\,1f{:}\,d0{:}\,aa{:}\,bb{:}\,cc$, pregunta a todos los dispositivos de la red LAN cuál es el que posee la dirección IP $192.168.0.3$. En la pregunta, la dirección MAC desconocida se rellena con ceros. En la respuesta este campo se completa y los dos pares de direcciones se presentan al revés que en la pregunta.

Restaría relacionar lo anteriormente explicado con una situación donde los actores se encontraran en distintas redes, como era el caso inicial de nuestro

alumno. Evidentemente, la funcionalidad ARP se desplegará por separado en cada enlace atravesado por el mensaje. De esta manera, en la red donde se encuentra la PC del alumno, su propio ARP generará un mensaje tratando de averiguar la MAC del *router* de salida. La información sobre la IP de dicho router la tomará desde su propia Tabla de Enrutamiento, ya que ese *router* es la puerta de salida o *gateway* a cualquier red diferente de la propia.

Una vez obtenida la MAC del *router* de salida, la PC del alumno podrá generar un mensaje de requerimiento de la página Web en cuestión que tendrá la particularidad de llevar como Dirección Destino IP la del servidor que aloja la página buscada, y como dirección MAC Destino la del *router* de salida de la red donde se encuentra el alumno cliente. Al reconocer el *router* su propia MAC en la trama, la levantará. Al leer la Dirección Destino IP, consultará en su propia Tabla de Enrutamiento y elegirá la interfaz apropiada de salida para la entrega del mensaje al siguiente *router* en el camino hacia el destino.

De compartir estos dos *routers* un enlace tipo LAN de difusión, se editará el requerimiento ARP para la dirección IP del *router* del próximo salto. Esta situación se repetirá en cada enlace de difusión que exista en el camino hacia el servidor Web. En cualquiera de estos enlaces, las direcciones fuente y destino IP del mensaje de requerimiento de la página Web se corresponderán con la fuente original del mensaje (la PC del alumno) y el destino final del mismo (la dirección IP de la máquina que aloja la página Web). El detalle a nivel de enlace, es que las direcciones irán variando entre fuente y destino, dentro de cada enlace particular. Recién cuando el mensaje llega al último *router*, en el ejemplo el *gateway* de la Facultad de Ingeniería, habrá un requerimiento ARP preguntando por la dirección IP del servidor Web. Sólo en la entrega final, la dirección IP y la dirección MAC destino del mensaje serán las del servidor. En este último tramo la dirección IP fuente es la de la PC del alumno, en tanto que la MAC fuente se corresponderá con la del *gateway* de la Facultad.

Como conclusión, cualquier mensaje que viaja a través de Internet, puede ir variando sus direcciones a nivel de enlace, pero nunca se cambian las direcciones IP origen y destino.

En la Fig. 9.11 se presenta un ejemplo de dos máquinas separadas por un *router*. La idea sería investigar los requerimientos ARP que serán necesarios para poder realizar un *ping* entre las dos máquinas A y B, separadas por el *router* R.

El comando *ping* se utiliza como herramienta para realizar pruebas de conexión. Sus mensajes se generan a partir del protocolo ICMP y se encapsulan en IP. En este ejemplo, no se presentarán los detalles de dichos mensajes, sólo se pretende hacer hincapié en los campos correspondientes a las direcciones, tanto a nivel MAC como a nivel IP. Es de destacar que el *router* de este ejemplo tiene interfaces sobre dos redes, por lo que posee dos direcciones MAC y debe ser configurado con una dirección IP diferente en cada interfaz.

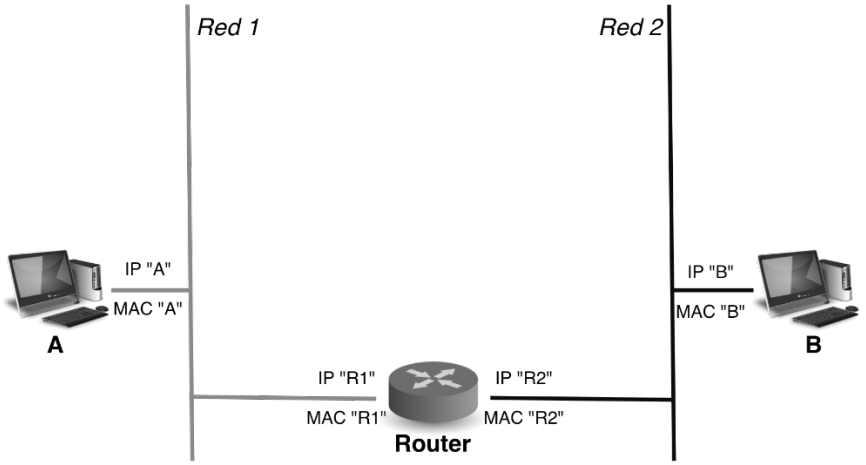

Figura 9.11 - Ping entre máquinas en distintas redes.

La Tabla 9.4 presenta un resumen de los mensajes intercambiados.

Tabla 9.4 – Mensajes intercambiados en un ping entre máquinas en distintas redes.

Mensaje Número	**Tipo**	**Contenido**
1	ARP Req.	***ETHERNET HEADER*:** SRCMAC: MACA. DSTMAC: FF:FF:FF:FF:FF:FF. TYPE: ARP. ***ARP HEADER*:** ARP REQUEST. SENDERMAC: MACA. SENDERIP: IPA. TARGETMAC: 00:00:00:00:00:00. TARGETIP: IPR1
2	ARP Rta.	***ETHERNET HEADER*:** SRCMAC: MACR1. DSTMAC: MACA. TYPE: ARP. ***ARP HEADER*:** ARP REPLY. SENDERMAC: MACR1. SENDERIP: IPR1. TARGETMAC: MACA. TARGETIP: IPA
3	Ping Req.	***ETHERNET HEADER*:** SRCMAC: MACA. DSTMAC: MACR1. TYPE: IP. ***IP HEADER*:** SOURCE IP: IPA. DESTIP: IPB. DATA: ECHO REQUEST
4	ARP Req.	***ETHERNET HEADER*:** SRCMAC: MACR2. DSTMAC: FF:FF:FF:FF:FF:FF. TYPE: ARP. ***ARP HEADER*:** ARP REQUEST. SENDERMAC: MACR2. SENDERIP: IPR2. TARGETMAC: 00:00:00:00:00:00. TARGETIP: IPB
5	ARP Rta.	***ETHERNET HEADER*:** SRCMAC: MACB. DSTMAC: MACR2. TYPE: ARP. ***ARP HEADER*:** ARP REPLY. SENDERMAC: MACB. SENDERIP: IPB. TARGETMAC: MACR2. TARGETIP: IPR2

Mensaje Número	Tipo	Contenido
6	Ping Req.	***ETHERNET HEADER*:** SRCMAC: MACR2. DSTMAC: MACB. TYPE: IP. ***IP HEADER*:** SOURCE IP: IPA. DESTIP: IPB. DATA: ECHO REQUEST.
7	Ping Rta.	***ETHERNET HEADER*:** SRCMAC: MACB. DSTMAC: MACR2. TYPE: IP. ***IP HEADER*:** SOURCE IP: IPB. DESTIP: IPA. DATA: ECHO REPLY
8	Ping Rta.	***ETHERNET HEADER*:** SRCMAC: MACR1. DSTMAC: MACA. TYPE: IP. ***IP HEADER*:** SOURCE IP: IPB. DESTIP: IPA. DATA: ECHO REPLY.

9.4 Protocolo ICMP (Internet Control Message Protocol)

ICMP, el Protocolo de Mensajes de Control de Internet, fue ideado para reportar situaciones de error a los dispositivos de transmisión y proveer mecanismos de testeo de presencia de equipos receptores, funcionalidades con las que el protocolo original IP no fue dotado. Se trata de un protocolo muy básico, implementado mediante un conjunto de mensajes que comparten un mismo formato.

Como se ha explicado, IP es un protocolo de red cuyo mecanismo de entrega es del tipo sin conexión, no confiable y sin mensajes de reconocimiento (ACK). Esto significa que no hay seguridad en la entrega de los paquetes. Prácticamente toda la confiabilidad necesaria para algunos tipos de aplicaciones descansa en TCP. Esta ausencia de confiabilidad a nivel de red se trató de suplir por medio de ICMP, cuyos mensajes se encapsulan en paquetes IP. A pesar de este encapsulado, que conduciría a ubicar el protocolo a nivel de transporte, por encima de IP, el estándar RFC 792 lo coloca al mismo nivel que IP, pero como una entidad separada.

Existen dos versiones del protocolo: ICMPv4 descripto en la RFC 792 para IPv4 e ICMPv6 descripto en la RFC 2463 para IPv6. A su vez, existen otros protocolos que definen sus propios mensajes basados en ICMP, tales como el que desarrolla la funcionalidad de *Traceroute* o el que especifica los mensajes de descubrimiento de *routers*.

En términos generales, ICMP ofrece un mecanismo para la detección de errores, que sólo pueden ser reportados al dispositivo origen del datagrama, debido a que en el paquete IP sólo figuran las direcciones IP fuente y destino. Por su parte, el receptor del mensaje ICMP no tiene obligación de responder o de tomar alguna precaución. Sólo se lo notifica.

La Tabla 9.5 presenta un listado de los mensajes ICMP definidos para la versión 4. Todos ellos son reconocidos por el número "1" presente en el campo Protocolo del encabezado IP que los encapsula. Los mensajes se pueden generar