Capítulo 3. Protocolos de soporte a IP

Redes de Ordenadores

2º Grado en Ingeniería en Tecnologías de Telecomunicación

Índice

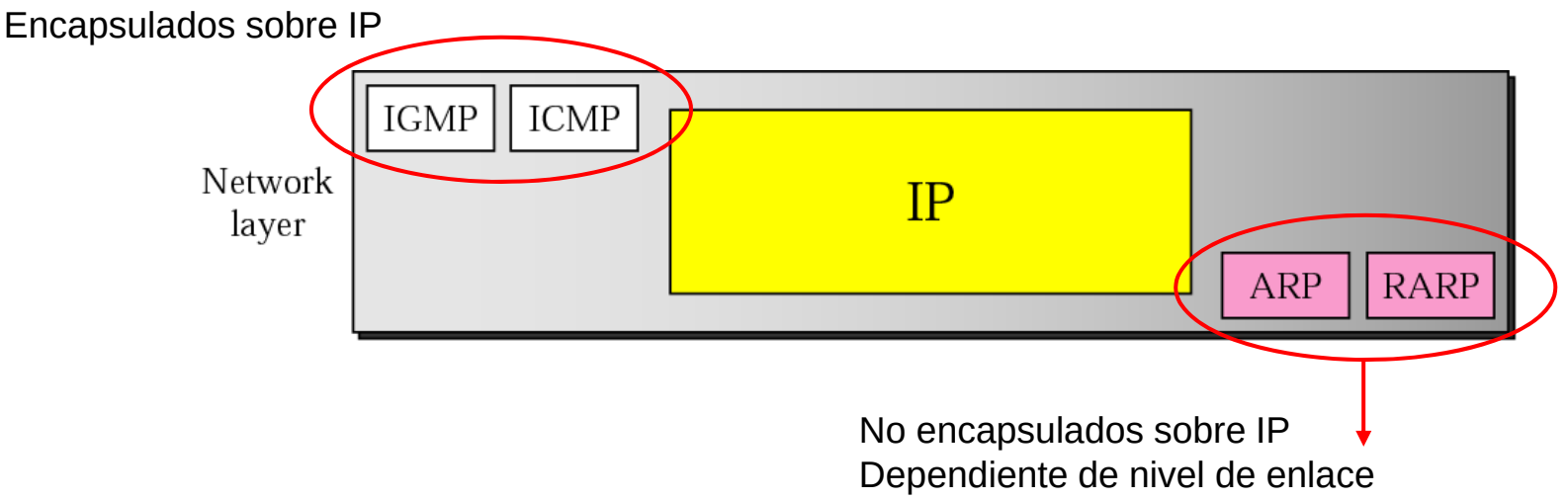
Índice hora 1

Objetivos

- Identificar la necesidad de un mecanismo automático de mapeo entre direcciones IP y direcciones MAC.
- Comprender las ventajas de los mecanismos de asignación automática de direcciones IP.

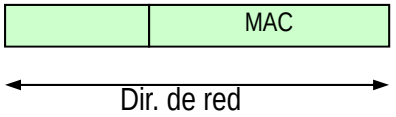
1 Introducción

- Para el correcto funcionamiento del protocolo IP se hace necesario utilizar una serie de protocolos complementarios:
  - ARP, RARP, DHCP - mapeo de direcciones físicas (MAC) con lógicas (IP).
  - ICMP - Notificación de problemas y errores. Supervisión del funcionamiento de la red.
  - IGMP - Gestión de grupos multicast.



2 ARP

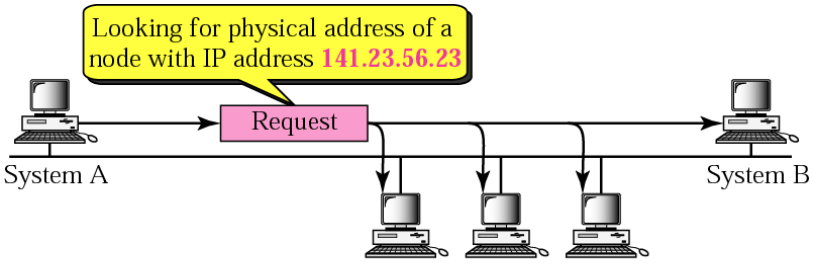
- Al enviar paquetes a una máquina normalmente sólo se conoce su dirección IP o nombre simbólico (DNS).
- Sin embargo, los datagramas IP se encapsulan sobre un nivel de enlace que necesita conocer las direcciones físicas de los equipos implicados.
- Necesidad de un mapeo IP → MAC que puede realizarse:
  - De forma estática, tener un fichero con todos los mapeos. Costosa su actualización para grandes redes.
  - Si la dirección de red es de mayor tamaño que la física se podría almacenar en ella, pero IP 32 bits y MAC habitualmente 48 bits (Ethernet, TokenRing, FDDI, etc.) por lo que no es posible.



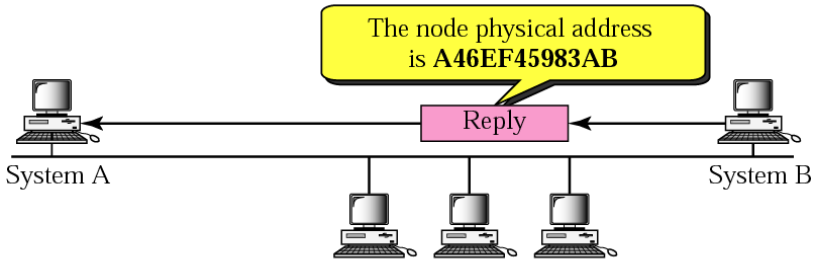
  - Protocolo dinámico que pregunte por la MAC de determinada IP cada vez que se necesite: *ARP*.

ARP

- ARP: Address Resolution Protocol.
- Paquete de petición ARP se manda a la dirección MAC de broadcast, todas las máquinas de la red lo oirán y la que tenga la IP solicitada contestará con su MAC en un paquete ARP de respuesta.



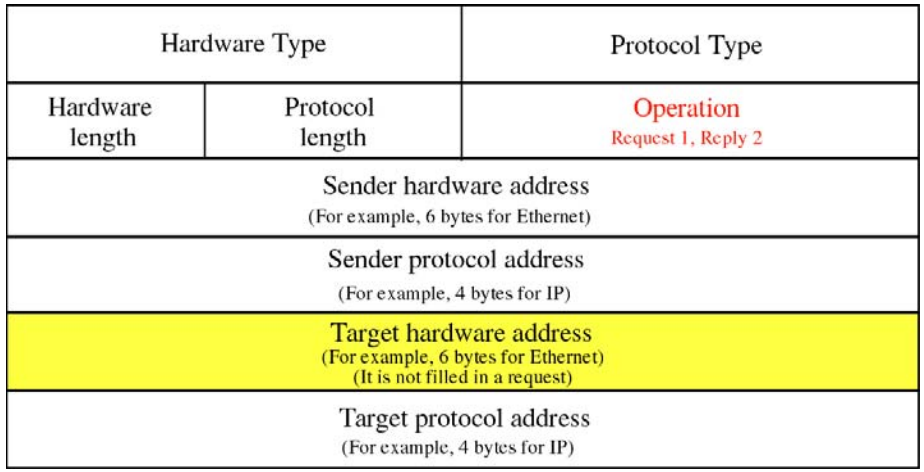
a. ARP request is broadcast



b. ARP reply is unicast

2.1 Cabecera ARP

- Campos cabecera ARP:
  - *Hw type (16bits)*: identifica la tecnología LAN. Para Ethernet 0x0001.
  - *Protocol type (16bits)*: identifica el protocolo de nivel de red. Para IPv4 0x0800.
  - *Hw length (8bits)*: tamaño (en bytes) de la dirección física. Para Ethernet es 6.
  - *Protocol length (8bits)*: tamaño (en bytes) de la dirección de red. Para IP es 4.
  - *Operation (16bits)*: 1 - ARP request, 2 - ARP reply.
  - *Sender/Target Hw Address*: campo de tamaño variable que contiene la dirección física del emisor/receptor.
  - *Sender/Target Protocol Address*: campo de tamaño variable que contiene la dirección de red del emisor/receptor.



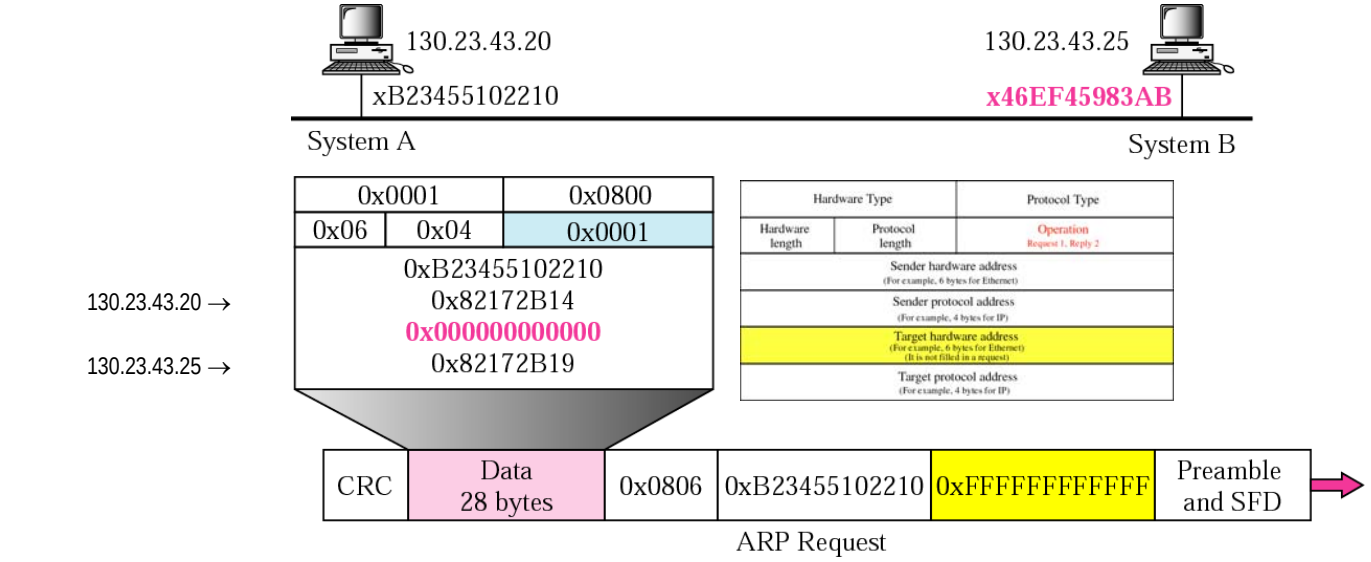
ARP, consideraciones

- ARP se encapsula directamente por encima del nivel de enlace.
  - Ethertype 0x0806
- ARP request es broadcast a nivel de enlace y el reply unicast.
- Los routers no reenvían broadcast de enlace y tampoco el ARP. Únicamente tiene sentido conocer la MAC de una máquina en la misma red. Para máquinas fuera de la red se hace necesario usar su dirección IP.
- El Target Hardware Address se coloca a 0's en el request.
- Se duplica información ya existente en la cabecera Ethernet (en algunos SOs por la dificultad de acceder a información de enlace).
- El receptor del request aprende a la vez la MAC del que hizo la petición de ARP.
- Tamaño paquete ARP en Ethernet/IP:

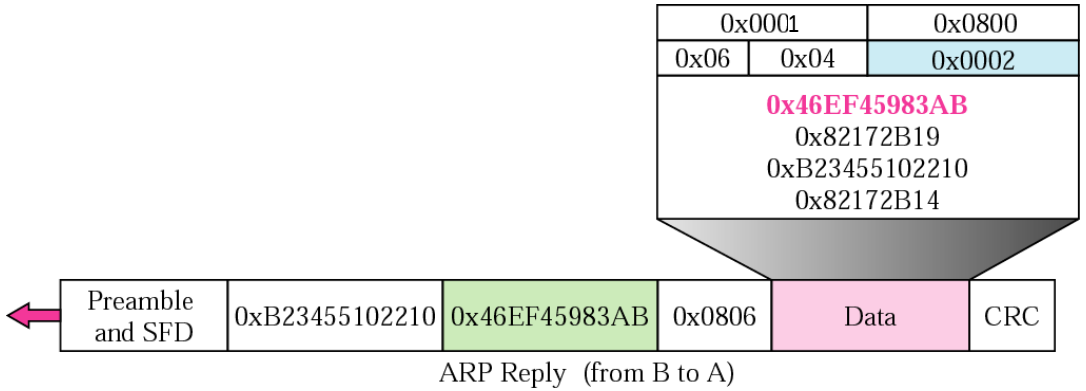
14 Ethernet + 28 ARP + 4 CRC = 46 bytes

< 64 bytes mínimo tamaño Ethernet (relleno hasta 64)

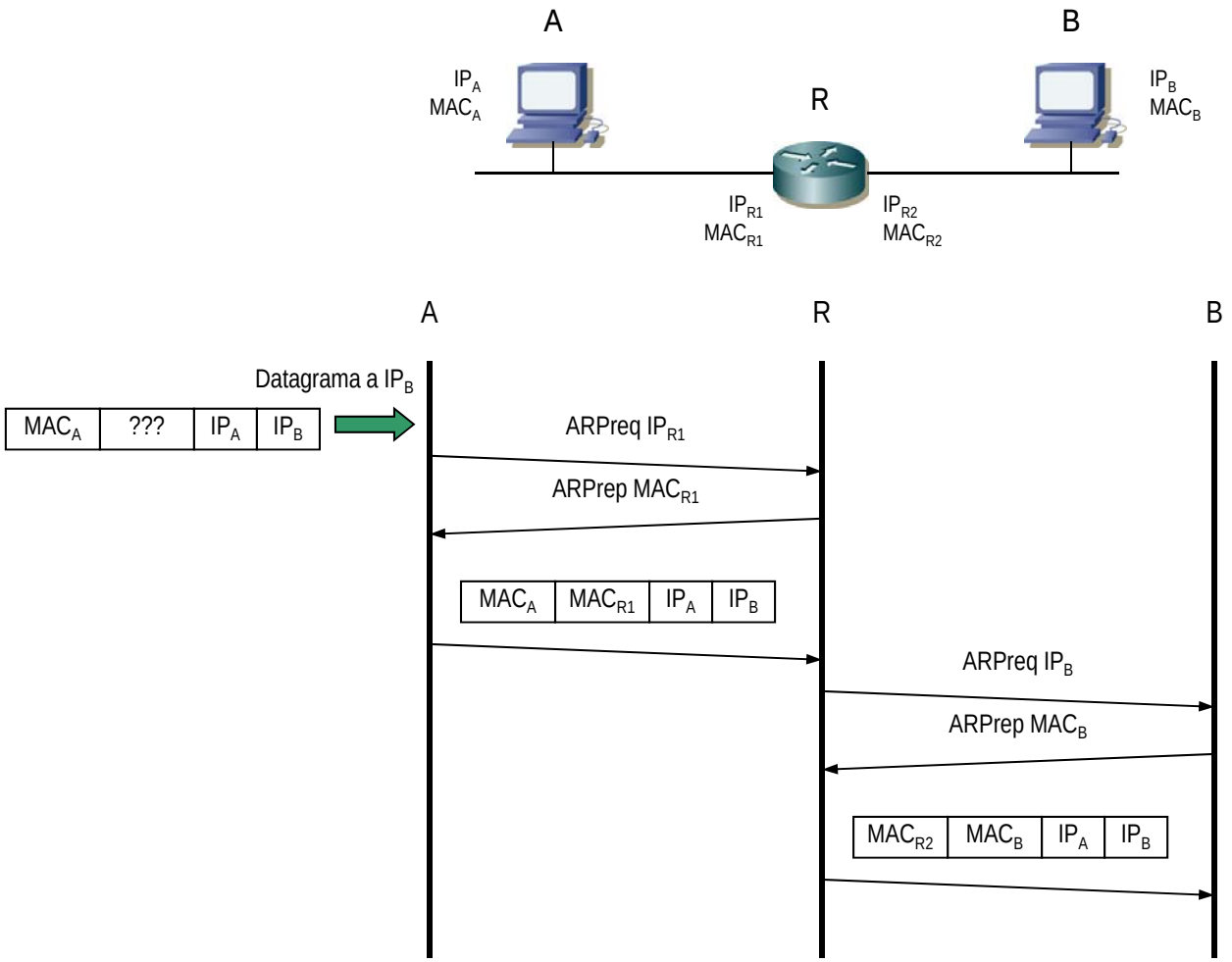
Ejemplo ARP



SFD (Start Frame Delimiter)



Ejemplo ARP

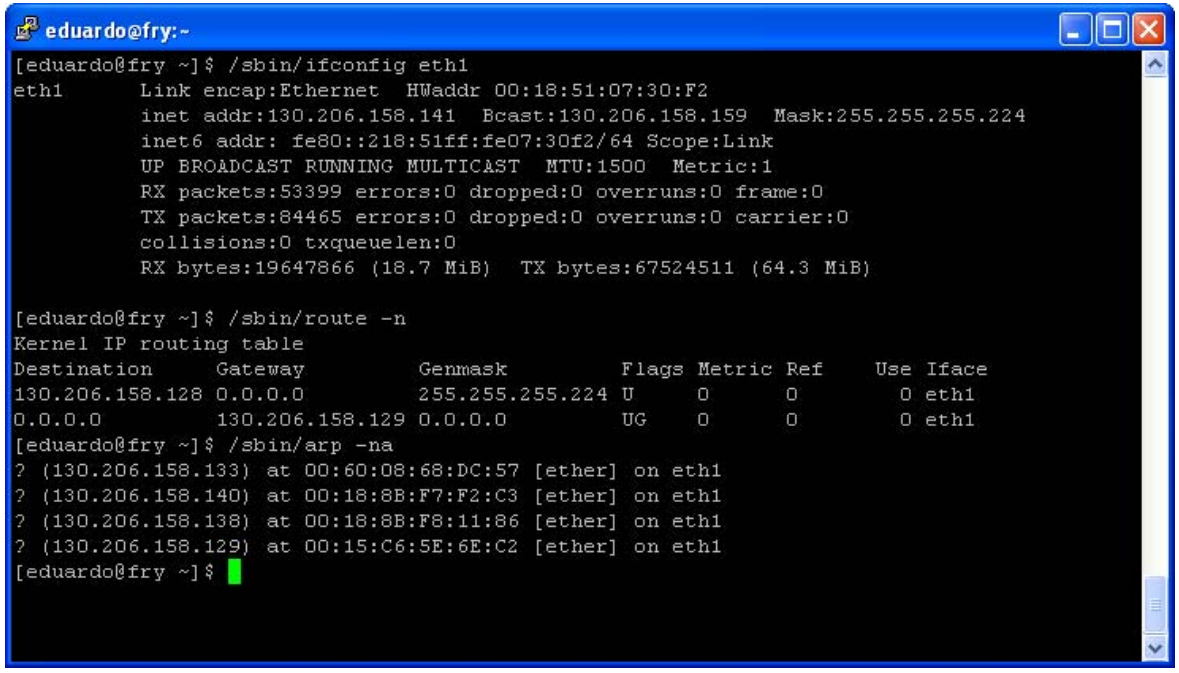

A
B
R
IP_A
MAC_A
IP_B
MAC_B
IP_R1
MAC_R1
IP_R2
MAC_R2
A
R
B
Datagrama a IP_B
MAC_A
???
IP_A
IP_B
ARPreq IP_R1
ARPrep MAC_R1
MAC_A
MAC_R1
IP_A
IP_B
ARPreq IP_B
ARPrep MAC_B
MAC_R2
MAC_B
IP_A
IP_B

2.2 Caché ARP

- La caché de ARP es una tabla con las direcciones MAC aprendidas recientemente, de forma que no sea necesario continuas peticiones ARP.
- Una tabla por interfaz (routers).
- Reside en memoria, por lo que comienza vacía con el arranque de la máquina.
- Las entradas se aprenden tanto de ARP request como reply.
- Las entradas envejecen y caducan por medio de temporizadores. Valores típicos de caducidad de 20 minutos.
  - ¿Qué ocurre si cambia la MAC de cierta IP?
- Los temporizadores se reinician cuando se ve un ARP request de esa máquina (broadcast).
- ARP flooding: cuando una máquina no contesta al ARP se recomienda reintentar 1 ARP/sg/destino, 3-5 reintentos.

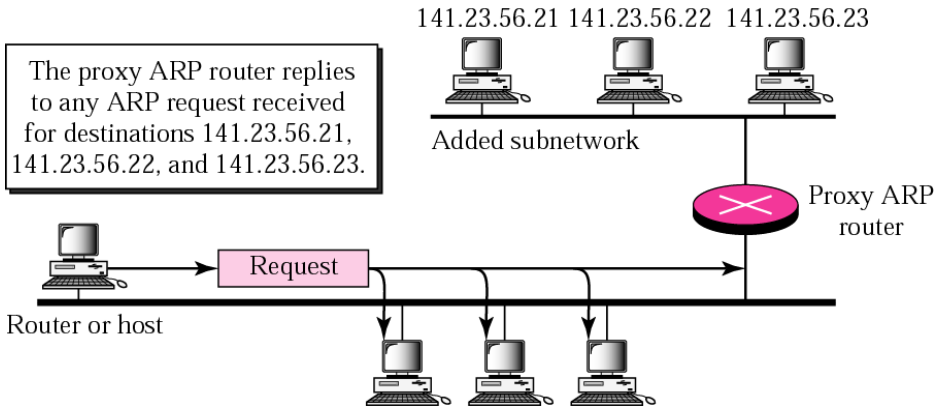
Caché ARP

- La solicitud de ARP se lanza siempre ante el envío de un paquete IP a un destino nuevo y se ha de guardar al menos el último paquete IP mientras se resuelve el ARP (puede costar un tiempo considerable por pérdida del ARP).
- Comando para mostrar la caché de ARP linux/windows: arp -a



2.3 Proxy ARP

- Los routers trabajan a nivel IP y no reenvían ARPs. Si 2 patas de un router están en la misma subred IP pero en 2 segmentos separados, puede interesar que conteste peticiones ARP de un segmento en nombre de máquinas del segundo segmento. Esto es el proxy ARP, promiscuous ARP o ARP hack.
- El router se hace pasar por las máquinas del segundo segmento respondiendo con su MAC a las peticiones ARP del primer segmento que mandan a IPs de máquinas del segundo segmento.



Proxy ARP

- Cuando el router reciba el paquete dirigido a su MAC pero a una IP del segundo segmento lo reenviará como es habitual.
- Ambos segmentos deben pertenecer a la misma red IP: direcciones IP de las máquinas dentro de la misma red. Se hace necesario por tanto una configuración en el router para indicarle las direcciones IP existentes en cada segmento o dividir la red IP en dos subredes IP diferenciables por el router.
- Ventaja:
  - Bloquea el tráfico de broadcast.
  - Disminuye el tráfico de ARP: una petición de ARP no inunda ambos segmentos, tan sólo uno.
  - Aisla ambos segmentos aunque pertenezcan a la misma red de forma transparente. Útil por ejemplo en implementaciones antiguas de TCP/IP con alguna incompatibilidad, por ejemplo sin soporte de subnetting.

2.4 Gratuitous ARP

- Consiste en lanzar periódicamente un ARP request solicitando la MAC de la IP de la propia máquina para:
  - Comprobar si hay otra máquina en la misma LAN que está utilizando su misma IP. No es admisible duplicidades de máquinas con la misma IP y se podría producir un mal funcionamiento de la red.
  - Actualizar la caché de ARP del resto de máquinas de la red que ya tuvieran esa entrada almacenada.

3 Asignación automática de direcciones IP

- El proceso de configuración manual de la información de red para máquinas de una red mediana o grande se convierte en un problema grave de gestión
  - Control de altas/bajas
  - Evitar direcciones IP duplicadas
  - Reparto eficiente del direccionamiento (multiplexación)
- Se hace necesario, por tanto, un proceso que permita asignar automáticamente la información de red a una máquina en su arranque.
  - Esa información podrá cambiar de un arranque al siguiente
  - Esa información no podrá ser secuestrada por la máquina de forma indefinida (si se apaga por ejemplo)

3.1 RARP

- Reverse Address Resolution Protocol.
- Permite el proceso inverso al ARP: obtención de la dirección IP de la máquina conociendo su dirección MAC.
- Un servidor de RARP contiene el mapeo IP-MAC de todas las máquinas de la red. El RARP request es *broadcast* para llegar a todas las máquinas, pero sólo contesta el servidor RARP de forma *unicast*.
- La cabecera es como la de ARP cambiando sólo el campo de operación:
  - 3: RARP request,
  - 4: RARP reply.
- Utilidad: asignación dinámica de dirección IP a una máquina en función de su MAC. Funcionalidad muy limitada en la actualidad porque la configuración de red va más allá de las dirección IP: máscara, router por defecto, servidores de DNS, etc.

3.2 BOOTP/DHCP

- Protocolos que proveen esas funcionalidades añadidas:
  - BOOTP, Bootstrap Protocol
    - Sobre UDP, puertos 67(servidor)-68(cliente).
    - Solicitud sobre paquete con IP destino broadcast.
    - Permite especificar la máscara, router por defecto, DNS e incluso un fichero con código de arranque para la máquina (descargable vía TFTP).
    - Mapeo fijo IP-MAC en el servidor.
  - DHCP, Dynamic Host Configuration Protocol
    - Como BOOTP pero permite la asignación de direcciones IP temporales o no asignadas a priori a una dirección MAC.
    - ¿Cómo comunicarse con un protocolo que usa IP sin tener todavía asignada dirección IP en la máquina?

DHCP solicitud inicial

DHCP client
MAC = a

- xid: ID transacción
- ciaddr: dirección IP cliente
- yiaddr: dirección IP asignada
- serverID: dirección IP servidor

DHCP server
MAC = b, IP = c
IP pool = {x,y,z}

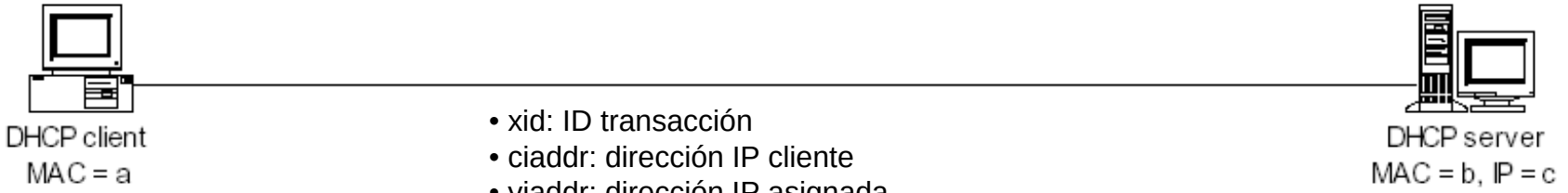
DHCPDISCOVER (src MAC = a, dst MAC = 0xffffffffffff, src IP = 0.0.0.0, dst IP = 255.255.255.255, src port = 68, dst port = 67, xid = n, ciaddr = 0.0.0.0)

DHCPOFFER (src MAC = b, dst MAC = 0xffffffffffff, src IP = c, dst IP = 255.255.255.255, src port = 67, dst port = 68, xid = n, ciaddr = 0.0.0.0, yiaddr = x, server ID = c, lease time = 3600 seconds, netmask = 255.255.255.0)

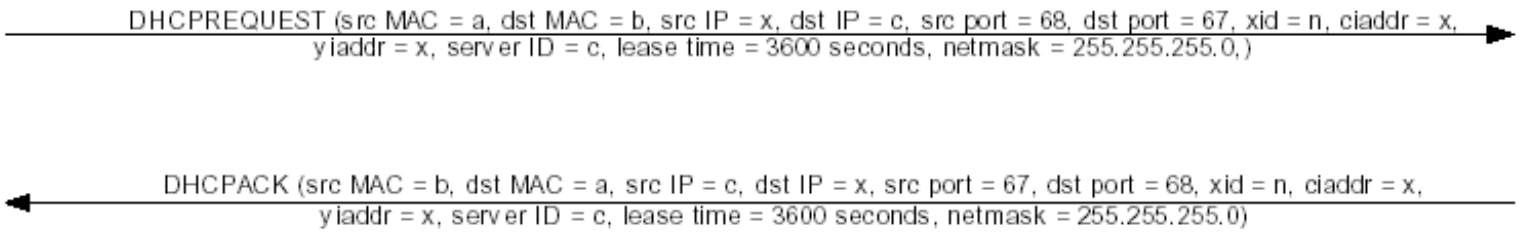
DHCPREQUEST (src MAC = a, dst MAC = 0xffffffffffff, src IP = 0.0.0.0, dst IP = 255.255.255.255, src port = 68, dst port = 67, xid = n+1, ciaddr = 0.0.0.0, yiaddr = x, server ID = c, lease time = 3600 seconds, netmask = 255.255.255.0, requested IP address = x)

DHCPACK (src MAC = b, dst MAC = 0xffffffffffff, src IP = c, dst IP = 255.255.255.255, src port = 67, dst port = 68, xid = n+1, ciaddr = 0.0.0.0, yiaddr = x, server ID = c, lease time = 3600 seconds, netmask = 255.255.255.0)

DHCP renovación



- xid: ID transacción
- ciaddr: dirección IP cliente
- yiaddr: dirección IP asignada
- serverID: dirección IP servidor



DHCP opciones

Table 8-1 DHCP Options

Tag	Name	Length	Meaning
0	Pad	0	None
1	Subnet Mask	4	Subnet mask value
2	Time Offset	4	Time offset in seconds from UTC
3	Router	N	N/4 router addresses
4	Time Server	N	N/4 time server addresses
5	Name Server	N	N/4 IEN-116 server addresses
6	Domain Server	N	N/4 DNS server addresses
7	Log Server	N	N/4 logging server addresses
8	Quotes Server	N	N/4 quotes server addresses
9	LPR Server	N	N/4 printer server addresses
10	Impress Server	N	N/4 Impress server addresses
11	RLP Server	N	N/4 RLP server addresses
12	Hostname	N	Hostname string
13	Boot File Size	2	Size of boot file in 512-byte chunks
14	Merit Dump File	N	Client to dump and name the file to dump it to
15	Domain Name	N	DNS domain name of the client
16	Swap Server	N	Swap server address
17	Root Path	N	Path name for root disk
18	Extension File	N	Path name for more BOOTP info
19	Forward On/Off	1	Enable/disable IP forwarding
20	SrcRte On/Off	1	Enable/disable source routing
21	Policy Filter	N	Routing policy filters
22	Max DG Assembly	2	Max datagram reassembly size
23	Default IP TTL	1	Default IP Time to Live
24	MTU Timeout	4	Path MTU aging timeout
25	MTU Plateau	N	Path MTU plateau table
26	MTU Interface	2	Interface MTU size
27	MTU Subnet	1	All subnets are local
28	Broadcast Address	4	Broadcast address
29	Mask Discovery	1	Perform mask discovery
30	Mask Supplier	1	Provide mask to others
31	Router Discovery	1	Perform router discovery
32	Router Request	4	Router solicitation address
33	Static Route	N	Static routing table
34	Trailers	1	Trailer encapsulation

Table 8-1 DHCP Options (continued)

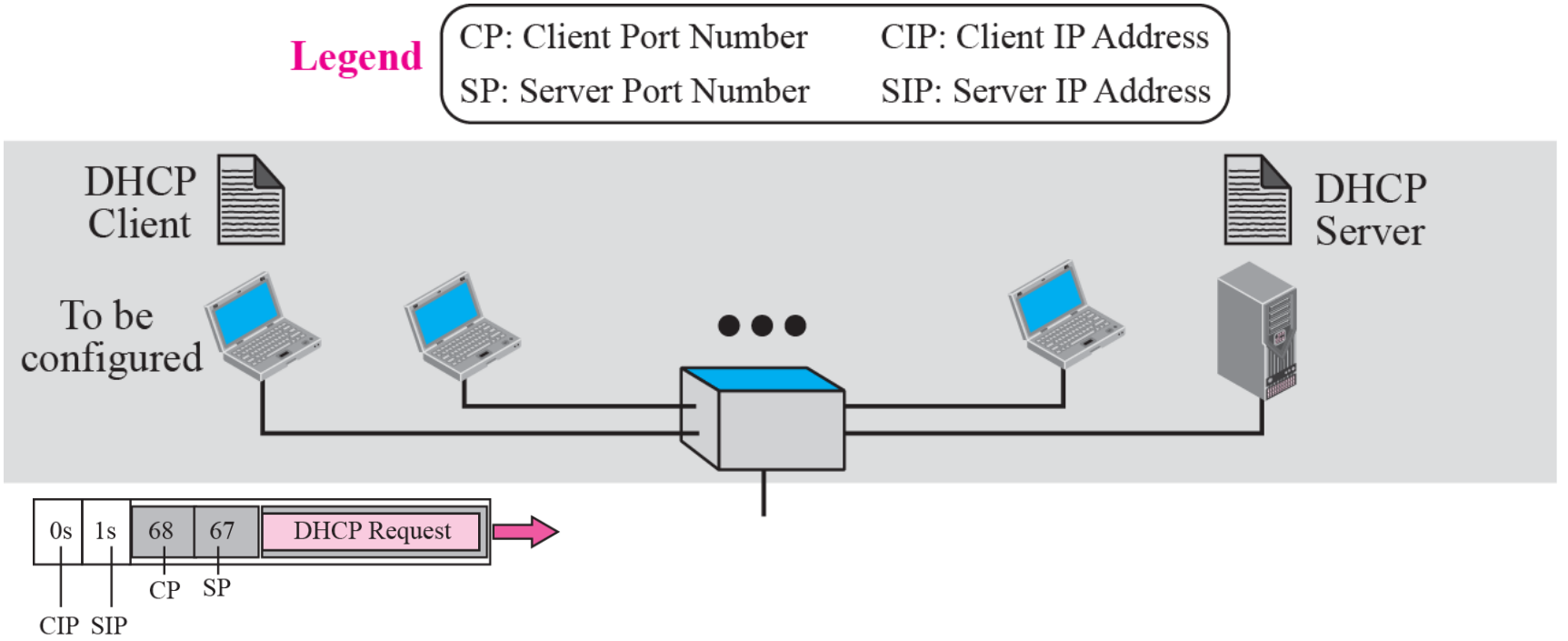
Tag	Name	Length	Meaning
35	ARP Timeout	4	ARP cache timeout
36	Ethernet	1	Ethernet encapsulation
37	Default TCP TTL	1	Default TCP Time to Live
38	Keepalive Time	4	TCP keep-alive interval
39	Keepalive Data	1	TCP keep-alive garbage
40	NIS Domain	N	NIS domain name
41	NIS Servers	N	NIS server addresses
42	NTP Servers	N	NTP server addresses
43	Vendor Specific	N	Vendor-specific information
44	NETBIOS Name Srv	N	NETBIOS name servers
45	NETBIOS Dist Srv	N	NETBIOS datagram distribution
46	NETBIOS Node Type	1	NETBIOS node type
47	NETBIOS Scope	N	NETBIOS scope
48	X Window Font	N	X Window font server
49	X Window Manager	N	X Window display manager
50	Address Request	4	Requested IP address
51	Address Time	4	IP address lease time
52	Overload	1	Overload "sname" or "file"
53	DHCP Msg Type	1	DHCP message type
54	DHCP Server Id	4	DHCP server identification
55	Parameter List	N	Parameter request list
56	DHCP Message	N	DHCP error message
57	DHCP Max Msg Size	2	DHCP maximum message size
58	Renewal Time	4	DHCP renewal time (T1)
59	Rebinding Time	4	DHCP rebinding time (T2)
60	Vendor Class ID	N	Vendor class Identifier
61	Client ID	N	Client Identifier
62	NetWare/IP Domain	N	NetWare/IP domain name
63	NetWare/IP Option	N	NetWare/IP sub options
64	NIS-Domain-Name	N	NIS+ v3 client domain name
65	NIS-Server-Addr	N	NIS+ v3 server addresses
66	Server-Name	N	TFTP server name
67	Bootfile-Name	N	Boot filename
68	Home-Agent-Addrs	N	Home agent addresses
69	SMTP-Server	N	Simple Mail server addresses

Table 8-1 DHCP Options (continued)

Tag	Name	Length	Meaning
70	POP3-Server	N	Post Office server addresses
71	NNTP-Server	N	Network News server addresses
72	WWW-Server	N	WWW server addresses
73	Finger-Server	N	Finger server addresses
74	IRC-Server	N	Chat server addresses
75	StreetTalk-Server	N	StreetTalk server addresses
76	STDA-Server	N	ST Directory Assistance addresses
77	User-Class	N	User class information
78	Directory Agent	N	Directory agent information
79	Service Scope	N	Service location agent scope
80	Naming Authority	N	Naming authority
81	Client FQDN	N	Fully qualified domain name
82	Agent Circuit ID	N	Agent circuit ID
83	Agent Remote ID	N	Agent remote ID
84	Agent Subnet Mask	N	Agent subnet mask
85	NDS Servers	N	Novell Directory Services
86	NDS Tree Name	N	Novell Directory Services
87	NDS Context	N	Novell Directory Services
88	IEEE 1003.1 POSIX	N	IEEE 1003.1 POSIX time zone
89	FQDN	N	Fully qualified domain name
90	Authentication	N	Authentication
91	Vines TCP/IP	N	Vines TCP/IP server option
92	Server Selection	N	Server selection option
93	Client System	N	Client system architecture
94	Client NDI	N	Client network device interface
95	LDAP	N	Lightweight Directory Access Protocol
96	IPv6 Transitions	N	IPv6 transitions
97	UUID/GUID	N	UUID/GUID-based Client Identifier
98	User-Auth	N	Open Group's user authentication

"N" in length column represents a variable number.

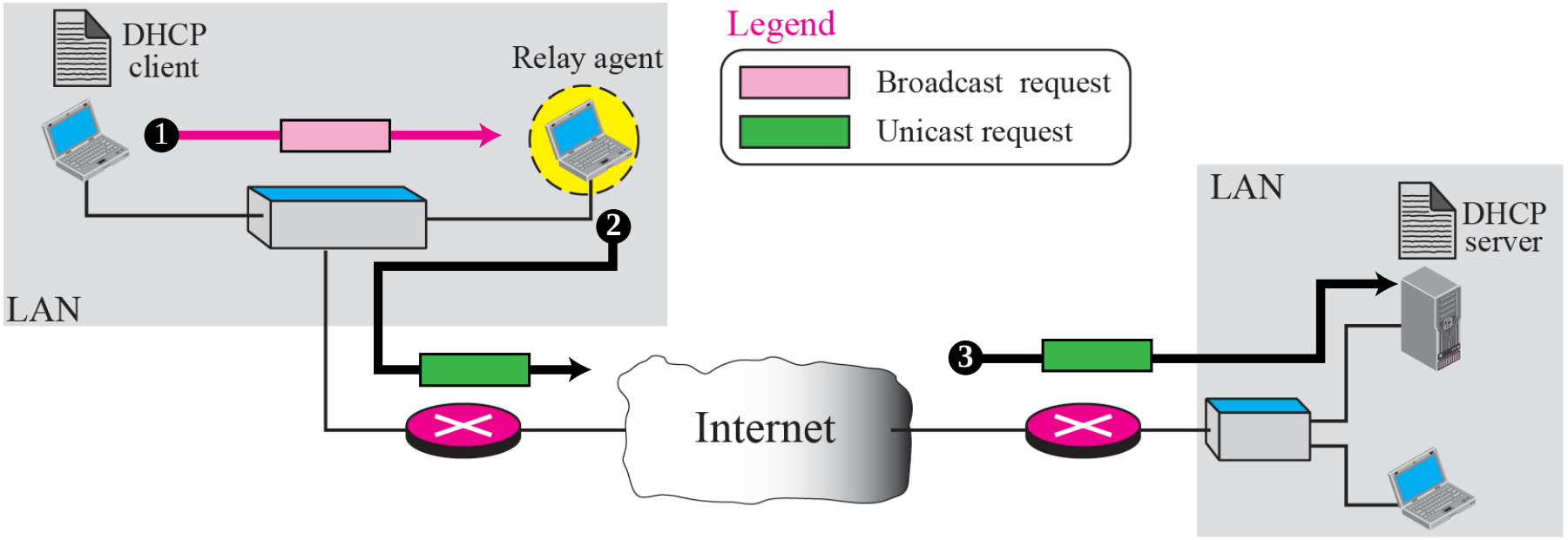
DHCP servidor en la misma red



- La respuesta puede ser broadcast o unicast a nivel de enlace (se conoce la MAC del cliente)

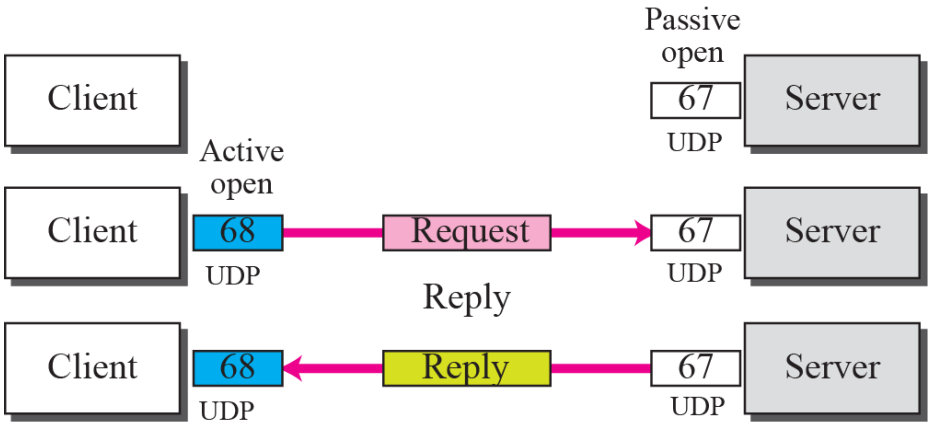
DHCP servidor en distinta red

- El relay agent puede ser una máquina, un switch o un router de la red.
  - Reenvía la solicitud a la IP del servidor DHCP que conoce a priori (unicast)
  - Un campo de la cabecera DHCP contiene la IP del relay agent
  - La respuesta vuelve al relay que lo vuelca unicast/broadcast a la red



DHCP puerto fijo de cliente

- Como las respuestas pueden ser broadcast, al elegir un puerto efímero para el cliente DHCP podría colisionar con otro cliente (de otro servicio) de otra máquina en el mismo puerto que recibiría los mismos paquetes.



Resumen

- ARP
  - Protocolo encapsulado por encima de nivel de enlace.
  - Permite preguntar (broadcast) por la dirección MAC de una dirección IP determinada.
  - Caché de ARP, para mapeos IP-MAC realizados recientemente
- DHCP
  - Protocolo encapsulado por encima de nivel de transporte UDP
  - Protocolo para la asignación automática de direcciones IP de forma no permanente
    - Pool de direcciones IP a repartir entre las máquinas conectadas en cada momento
  - Además de dirección IP provee máscara, router por defecto, servidores DNS, etc.

Referencias

- [Forouzan]
  - Capítulo 8, secciones 8.1-8.2 “Address mapping”, “The ARP protocol”
  - Capítulo 18, secciones 18.1-18.2 “Introduction”, “DHCP operation”
- [Stevens]
  - Capítulo 4 “ARP: Address Resolution Protocol”
  - Capítulo 5 “RARP: Reverse Address Resolution Protocol”
  - Capítulo 16 “BOOTP: Bootstrap Protocol”