# Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is one of the major protocol in the TCP/IP suit and the purpose of Address Resolution Protocol (ARP) is to map an **IPv4 address (32 bit Logical Address)** to the **physical address (48 bit MAC Address)**. Network Applications at the Application Layer use IPv4 Address to communicate with another device. But at the Data link layer, the addressing is **MAC address (48 bit Physical Address)**, and this address is burned into the network card permanently.

The purpose of Address Resolution Protocol (ARP) is to find out the **MAC address** of a device in your **Local Area Network (LAN)**, for the corresponding IPv4 address, which network application is trying to communicate.

## Static Mapping

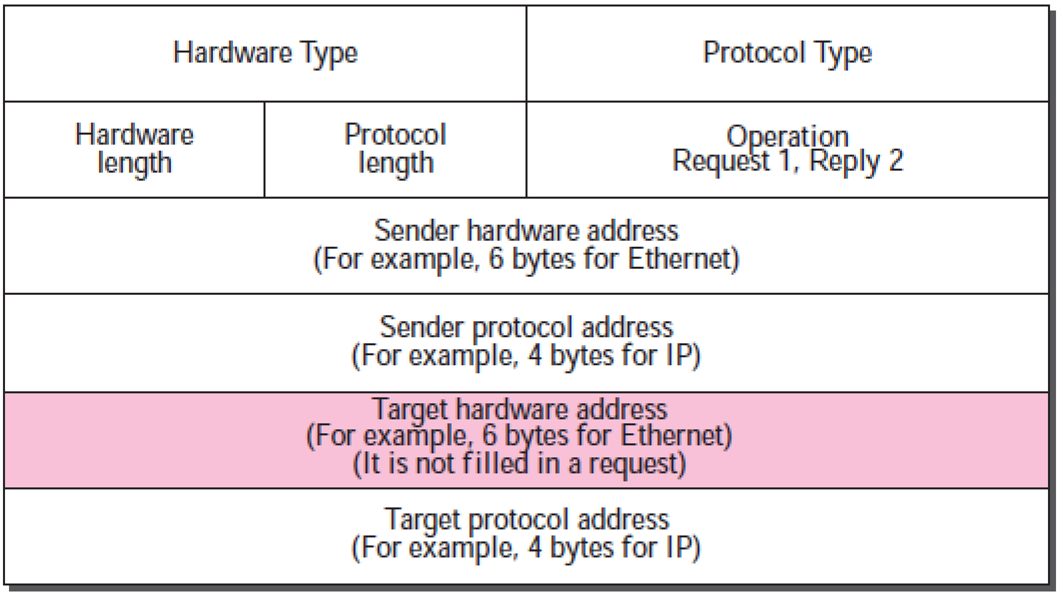
Static mapping means creating a table that associates a logical address with a physical address. This table is stored in each machine on the network. Each machine that knows, for example, the IP address of another machine but not its physical address can look it up in the table. This has some limitations because physical addresses may change in the following ways:

1. A machine could change its NIC, resulting in a new physical address.
2. In some LANs, such as LocalTalk, the physical address changes every time the computer is turned on.
3. A mobile computer can move from one physical network to another, resulting in a change in its physical address.

To implement these changes, a static mapping table must be updated periodically. This overhead could affect network performance.

## Dynamic Mapping

In dynamic mapping, each time a machine knows the logical address of another machine, it can use a protocol to find the physical address. Two protocols have been designed to perform dynamic mapping: Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP). ARP maps a logical address to a physical address; RARP maps a physical address to a logical address. Since RARP is replaced with another protocol and therefore ignored, we discuss only ARP protocol in this chapter.



<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td>Operation<br>Request 1, Reply 2</td></tr>
<tr><td colspan="3">Sender hardware address<br>(For example, 6 bytes for Ethernet)</td></tr>
<tr><td colspan="3">Sender protocol address<br>(For example, 4 bytes for IP)</td></tr>
<tr><td colspan="3">Target hardware address<br>(For example, 6 bytes for Ethernet)<br>(It is not filled in a request)</td></tr>
<tr><td colspan="3">Target protocol address<br>(For example, 4 bytes for IP)</td></tr>
</table>

Figure 1: ARP packet format

The fields in the Address Resolution Protocol (ARP) Message Format are:

Hardware Type: Hardware Type field in ARPMessage specifies the type of hardware used for the local network transmitting the Address Resolution Protocol (ARP) message. **Ethernet** is the common Hardware Type and he value for **Ethernet** is 1. The size of this field is 2 bytes.

Protocol Type: Each protocol is assigned a number used in this field. **IPv4** is 2048 (0x0800 in Hexa).

Hardware Address Length: Hardware Address Length in ARP Message is length in bytes of a **hardware (MAC) address**. **Ethernet MAC addresses** are 6 bytes long.

Protocol Address Length: Length in bytes of a **logical address (IPv4 Address)**. **IPv4 addresses** are 4 bytes long.

Opcode: Opcode field in ARP Message specifies the nature of the ARP message. 1 for ARP request and 2 for ARP reply.

Sender Hardware Address: Layer 2 (**MAC Address**) address of the device sending the message.

Sender Protocol Address: The **protocol address (IPv4 address)** of the device sending the message

Target Hardware Address: Layer 2 (**MAC Address**) of the intended receiver. This field is ignored in requests.

Target Protocol Address: The **protocol address (IPv4 Address)** of the intended receiver.

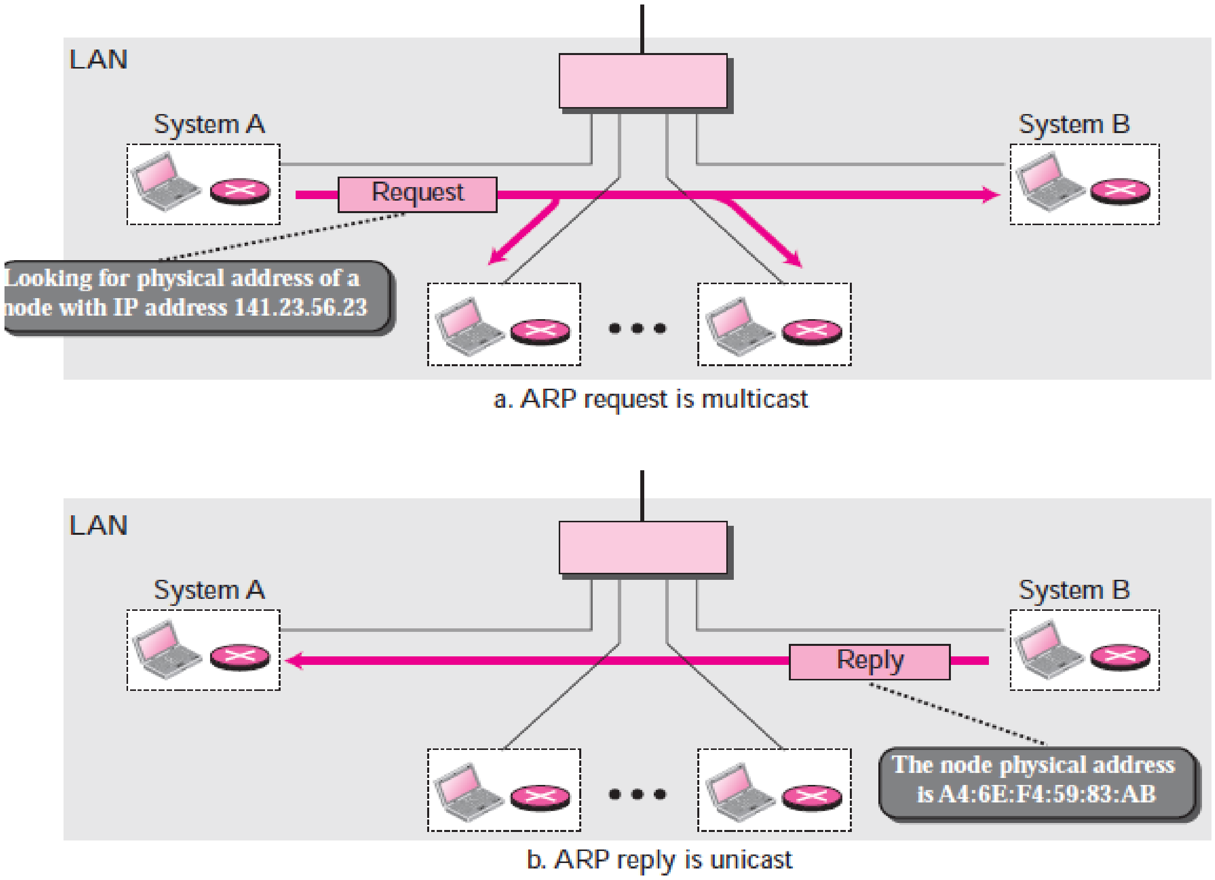

LAN
System A
System B
Request
Looking for physical address of a node with IP address 141.23.56.23
a. ARP request is multicast
LAN
System A
System B
Reply
The node physical address is A4:6E:F4:59:83:AB
b. ARP reply is unicast

Figure 2: ARP operation

## Encapsulation

An ARP packet is encapsulated directly into a data link frame. For example, in Figure 3 an ARP packet is encapsulated in an Ethernet frame. Note that the type field indicates that the data carried by the frame is an ARP packet.

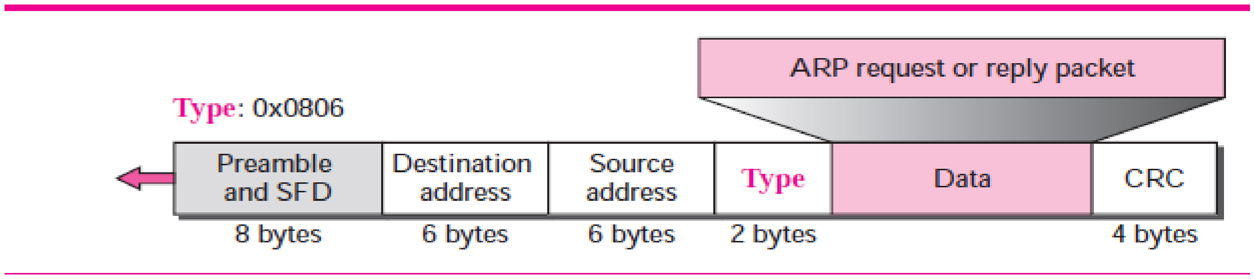


Figure 3: Encapsulation of ARP packet

## Operation

Let us see how ARP functions on a typical internet. First we describe the steps involved. Then we discuss the four cases in which a host or router needs to use ARP.

Steps Involved

These are seven steps involved in an ARP process:

1. The sender knows the IP address of the target. We will see how the sender obtains this shortly.
2. IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field is filled with 0s.
3. The message is passed to the data link layer where it is encapsulated in a frame using the physical address of the sender as the source address and the physical broadcast address as the destination address.
4. Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes the IP address.
5. The target machine replies with an ARP reply message that contains its physical address. The message is unicast.
6. The sender receives the reply message. It now knows the physical address of the target machine.
7. The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

## Four Different Cases

The following are four different cases in which the services of ARP can be used (see Figure 4).

❑ Case 1: The sender is a host and wants to send a packet to another host on the same network. In this case, the logical address that must be mapped to a physical address is the destination IP address in the datagram header.

❑ Case 2: The sender is a host and wants to send a packet to another host on another network. In this case, the host looks at its routing table and finds the IP address of the next hop (router) for this destination. If it does not have a routing table, it looks for the IP address of the default router. The IP address of the router becomes the logical address that must be mapped to a physical address.

❑ Case 3: The sender is a router that has received a datagram destined for a host on another network. It checks its routing table and finds the IP address of the next router. The IP address of the next router becomes the logical address that must be mapped to a physical address.

❑ Case 4: The sender is a router that has received a datagram destined for a host in the same network. The destination IP address of the datagram becomes the logical address that must be mapped to a physical address.

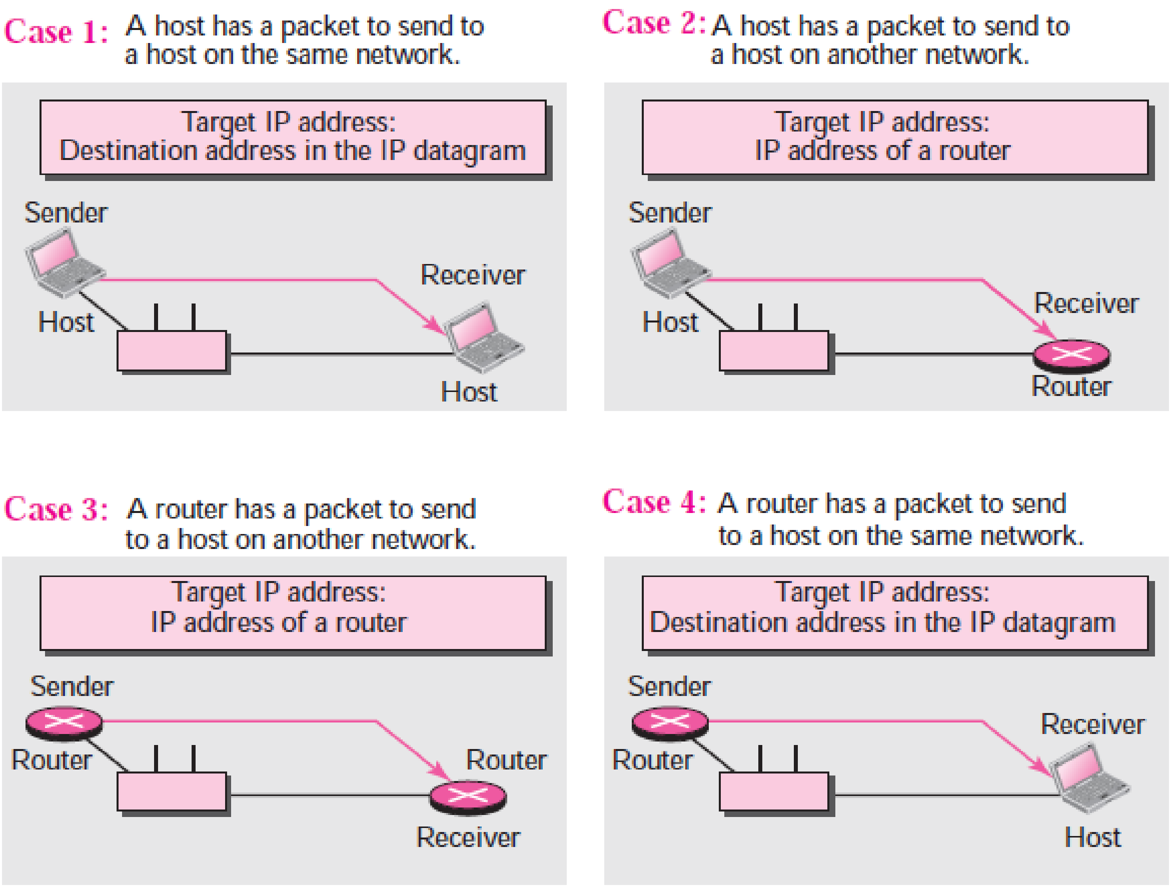

Case 1: A host has a packet to send to a host on the same network.
Target IP address: Destination address in the IP datagram
Sender
Host
Receiver
Host
Case 2: A host has a packet to send to a host on another network.
Target IP address: IP address of a router
Sender
Host
Receiver
Router
Case 3: A router has a packet to send to a host on another network.
Target IP address: IP address of a router
Sender
Router
Router
Receiver
Case 4: A router has a packet to send to a host on the same network.
Target IP address: Destination address in the IP datagram
Sender
Router
Receiver
Host

Figure 4: Four cases using ARP.

## Example 8.1

A host with IP address 130.23.43.20 and physical address B2:34:55:10:22:10 has a packet to send to another host with IP address 130.23.43.25 and physical address A4:6E:F4:59:83:AB (which is unknown to the first host). The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

## Solution

Figure 5 shows the ARP request and reply packets. Note that the ARP data field in this case is 28 bytes, and that the individual addresses do not fit in the 4-byte boundary. That is why we do not show the regular 4-byte boundaries for these addresses. Also note that the IP addresses are shown in hexadecimal. For information on binary or hexadecimal notation see Appendix B.

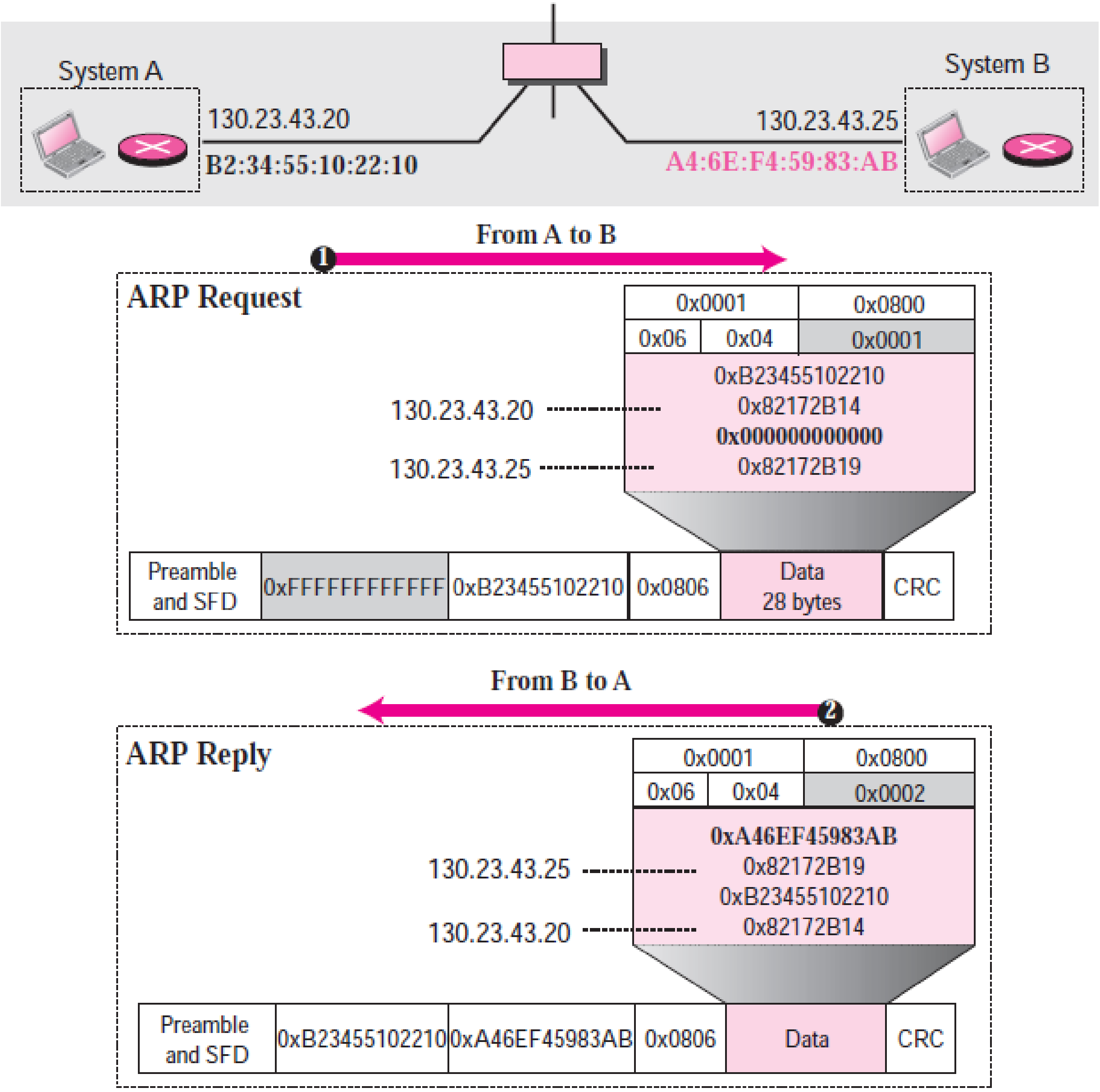


Figure 5: Example 8.1.

## Proxy ARP

A technique called proxy ARP is used to create a subnetting effect. A proxy ARP is an ARP that acts on behalf of a set of hosts. Whenever a router running a proxy ARP receives an ARP request looking for the IP address of one of these hosts, the router sends an ARP reply announcing its own hardware (physical) address. After the router receives the actual IP packet, it sends the packet to the appropriate host or router. Let us give an example. In Figure 6, the ARP installed on the right-hand host will answer only to an ARP request with a target IP address of 141.23.56.23.

However, the administrator may need to create a subnet without changing the whole system to recognize subnetted addresses. One solution is to add a router running a proxy ARP. In this case, the router acts on behalf of all of the hosts installed on the subnet. When it receives an ARP request with a target IP address that matches the address of one of its protected (141.23.56.21, 141.23.56.22, and 141.23.56.23), it sends an ARP reply and announces its hardware address as the target hardware address. When the router receives the IP packet, it sends the packet to the appropriate host.

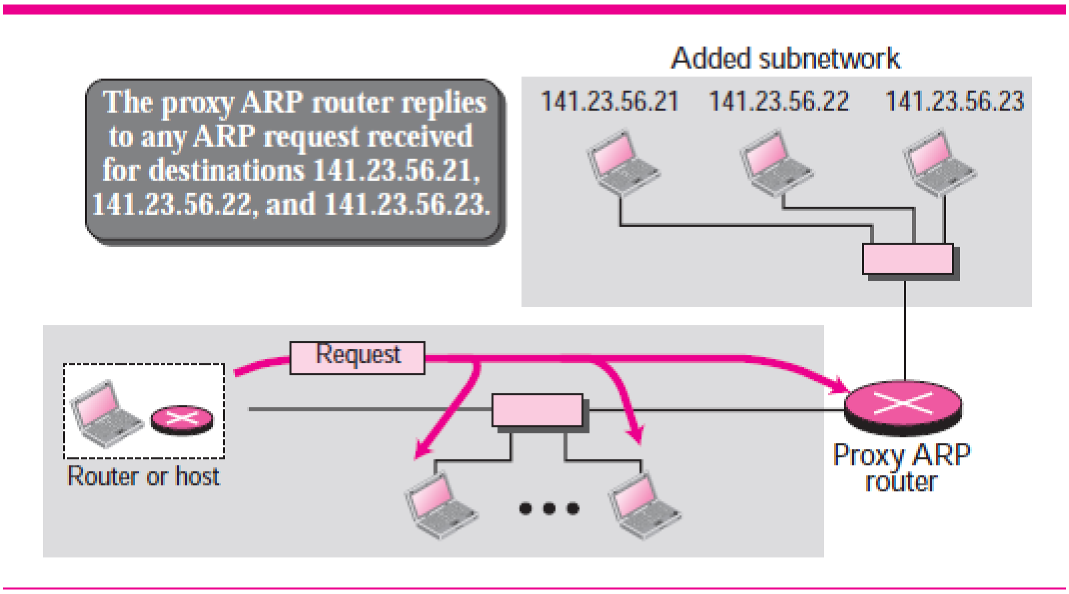

The proxy ARP router replies to any ARP request received for destinations 141.23.56.21, 141.23.56.22, and 141.23.56.23.
Added subnetwork
141.23.56.21
141.23.56.22
141.23.56.23
Request
Router or host
Proxy ARP router

Figure 6: Proxy ARP