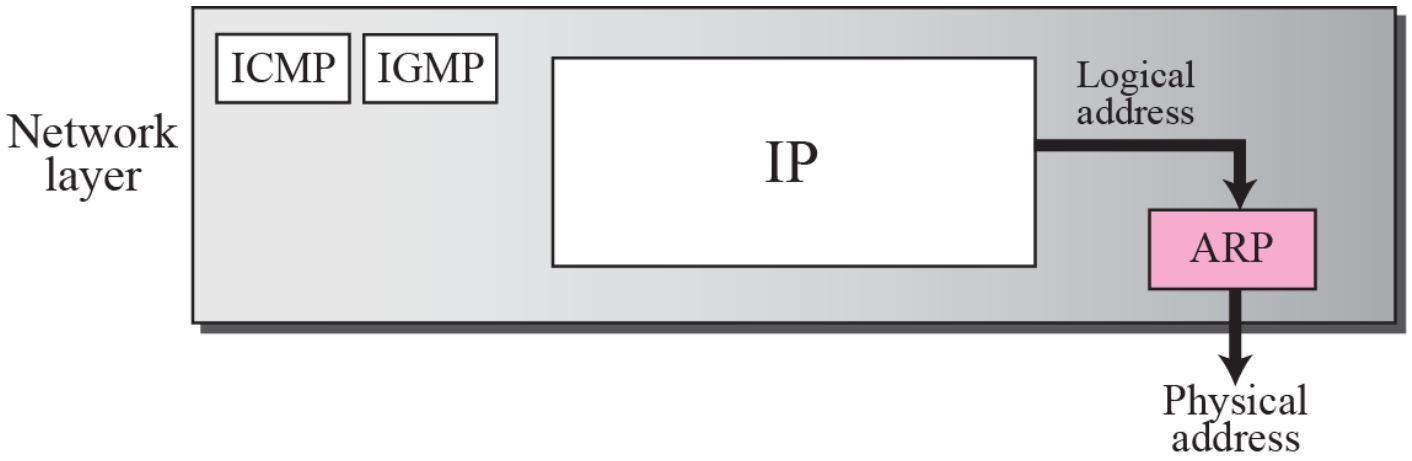
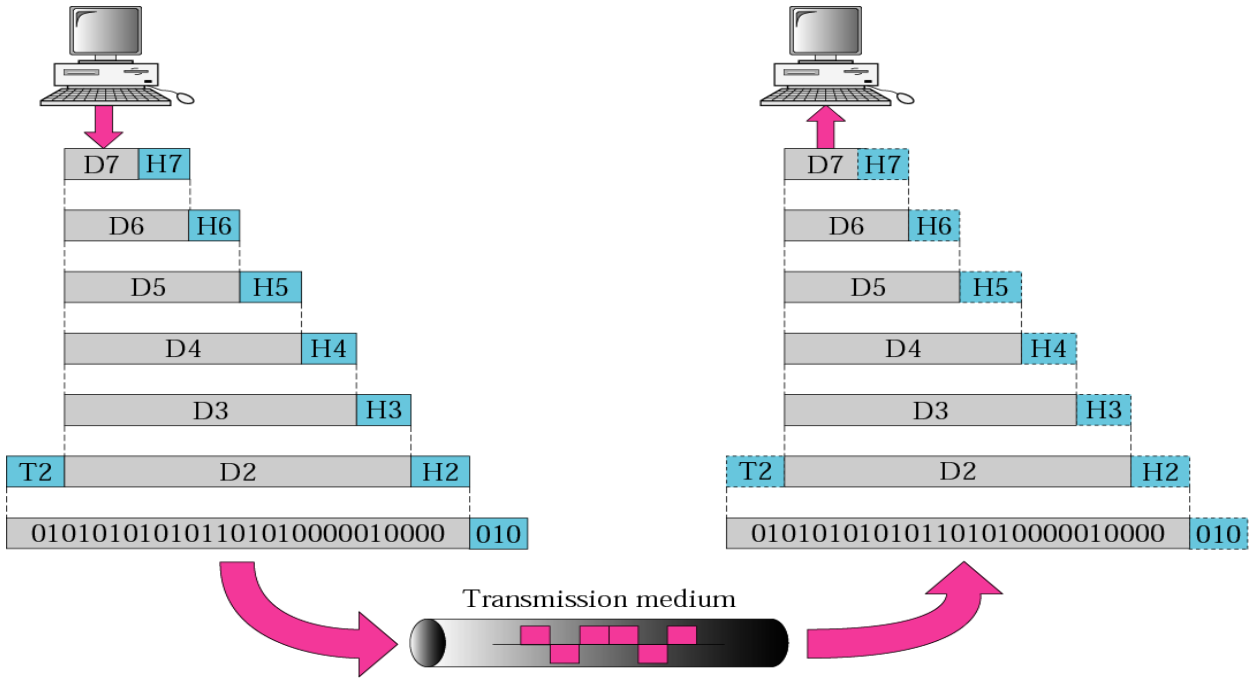
Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP)

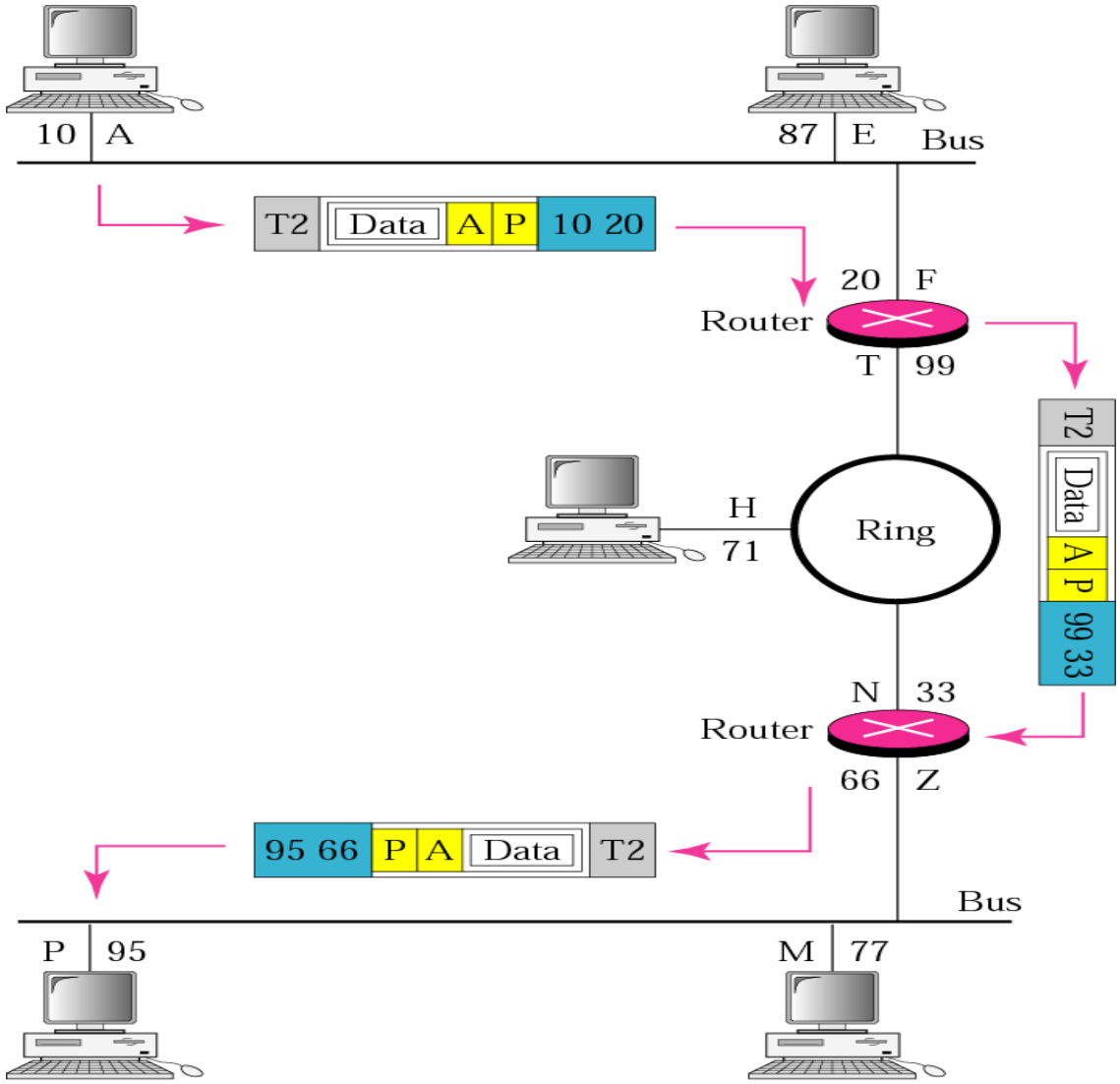


Network layer

Data link layer



Ipaddress : A, P
MAC address : 10, 95



8-1 ADDRESS MAPPING

Hosts and routers are recognized at the network level by their logical addresses.

It is called a *logical* address because it is usually implemented in software.

8-1 ADDRESS MAPPING

At the physical level, hosts and routers are recognized by their physical addresses.

Physical address is a local address.

- ✓ It should be unique locally, but not necessarily universally.
- ✓ called a *physical* address because it is usually (but not always) implemented in hardware.
- ✓ Examples of physical addresses are 48-bit MAC addresses in the Ethernet protocol, which are imprinted on the NIC installed in the host or router.

8-1 ADDRESS MAPPING

Delivery of a packet to a host or a router requires two levels of addressing: *logical* and *physical*.

Need to map a logical address to its corresponding physical address and vice versa.

These can be done using either *static* or *dynamic* mapping.

Static Mapping

Creating a table that associates a logical address with a physical address.

This has some limitations because physical addresses may change.

- A machine could change its NIC, resulting in a new physical address.
- In some LANs, such as LocalTalk, the physical address changes every time the computer is turned on.

To implement these changes, a static mapping table must be updated periodically.

Dynamic Mapping → ARP

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)
- Reverse Address Resolution Protocol (RARP).

ARP maps a logical address to a physical address;

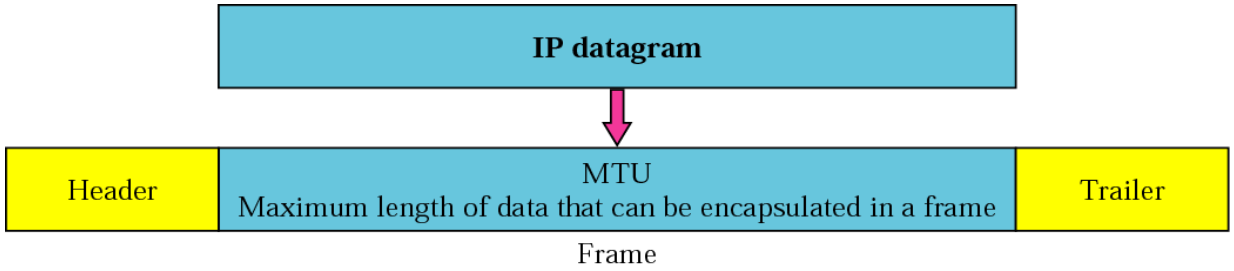
RARP maps a physical address to a logical address.

RARP is replaced with another protocol and therefore deprecated.

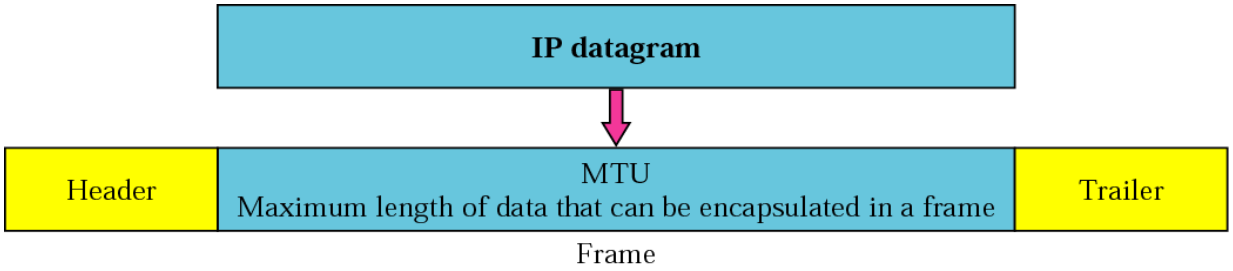
8-2 ADDRESS MAPPING

Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver.

IP datagram must be encapsulated in a frame to be able to pass through the physical network.



8-2 ADDRESS MAPPING



This means that the sender needs the physical address of the receiver.

ARP accepts a logical address from the IP protocol, maps the address to the corresponding physical address and pass it to the data link layer.

Figure 8.1 *Position of ARP in TCP/IP protocol suite*

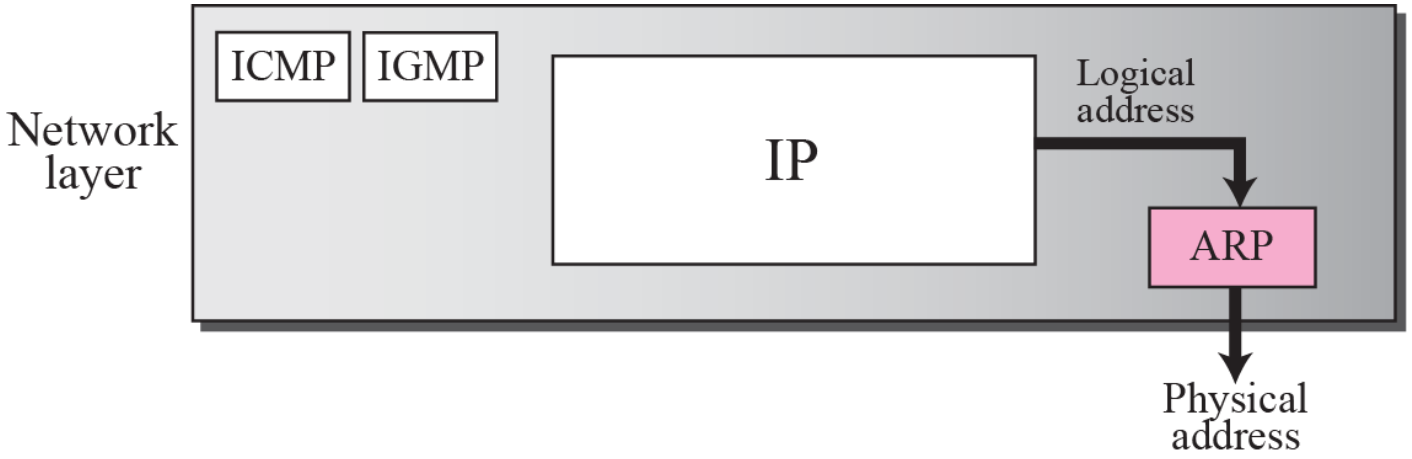


Figure 8.1 *Position of ARP in TCP/IP protocol suite*

Anytime a host, or a router, needs to find the physical address of another host or router on its network, it sends an ARP query packet.

Packet includes the physical and IP addresses of the sender and the IP address of the receiver.

Figure 8.1 *Position of ARP in TCP/IP protocol suite*

Because the sender does not know the physical address of the receiver, the query is broadcast over the network.

Figure 8.1 *Position of ARP in TCP/IP protocol suite*

Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.

The response packet contains the recipient's IP and physical addresses.

The packet is **unicast directly** to the inquirer using the physical address received in the query packet.

Figure 8.1 *Position of ARP in TCP/IP protocol suite*

The system on the (A) has a packet that needs to be delivered to another system (B) with IP address 141.23.56.23.

System A needs to pass the packet to its data link layer for the actual delivery, but it does not know the physical address of the recipient.

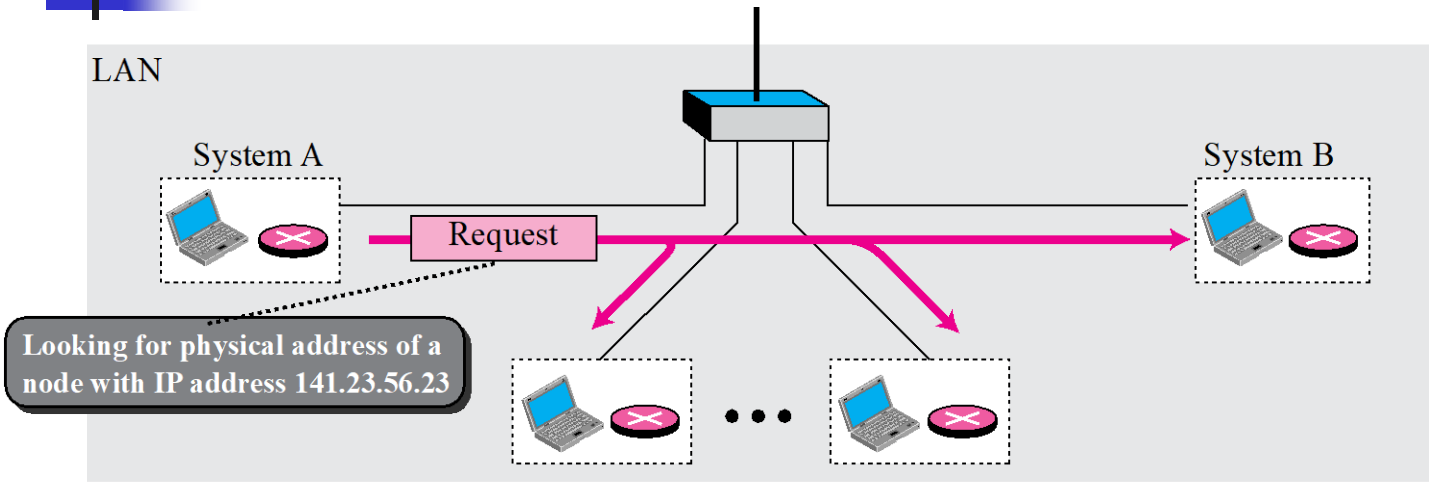
It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IP address of 141.23.56.23.

This packet is received by every system on the physical network, but only system B will answer it.

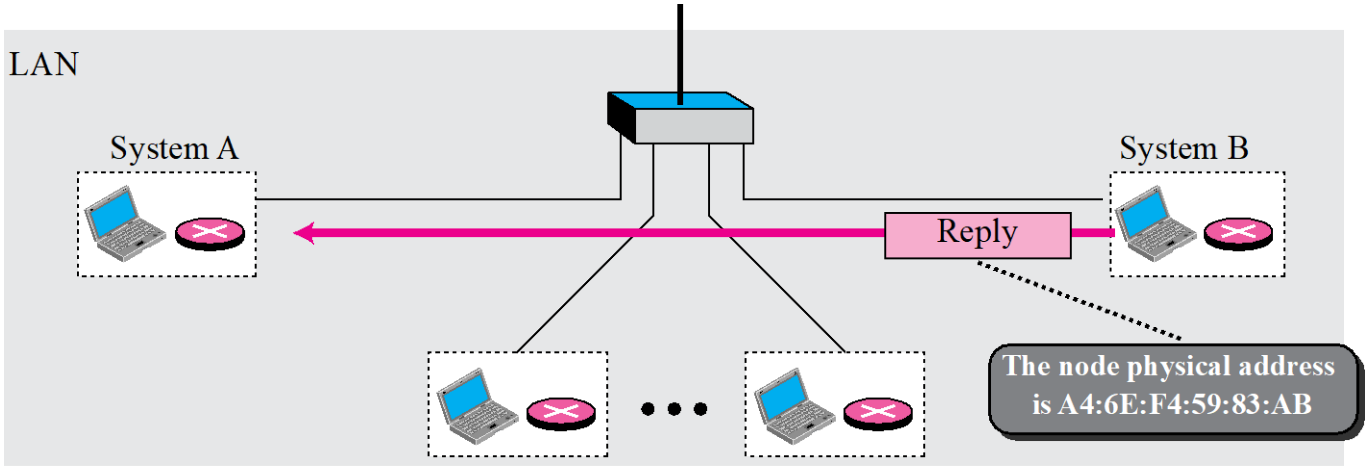
System B sends an ARP reply packet that includes its physical address.

Now system A can send all the packets it has for this destination using the physical address it received.

Figure 8.2 *ARP operation*



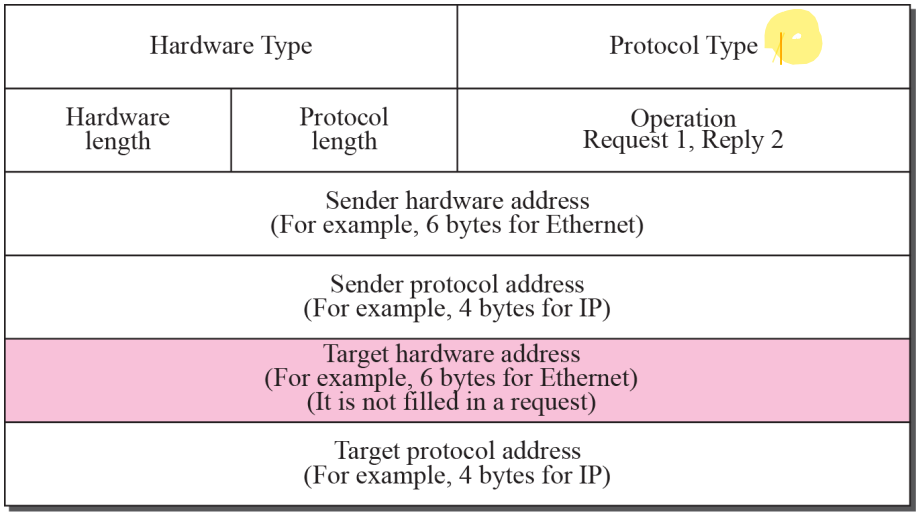
a. ARP request is broadcast



b. ARP reply is unicast

Figure 8.3 *ARP packet*

Packet Format



Hardware type. 16-bit field defining the type of network on which ARP is running. For Ethernet type is 1.

Protocol type. 16-bit field defining the protocol. For example, the value of this field for the IPv4 protocol is 0800_{16}. ARP can be used with any higher-level protocol.

Hardware length. 8-bit field defining the length of the physical address in bytes. For Ethernet, value is 6.

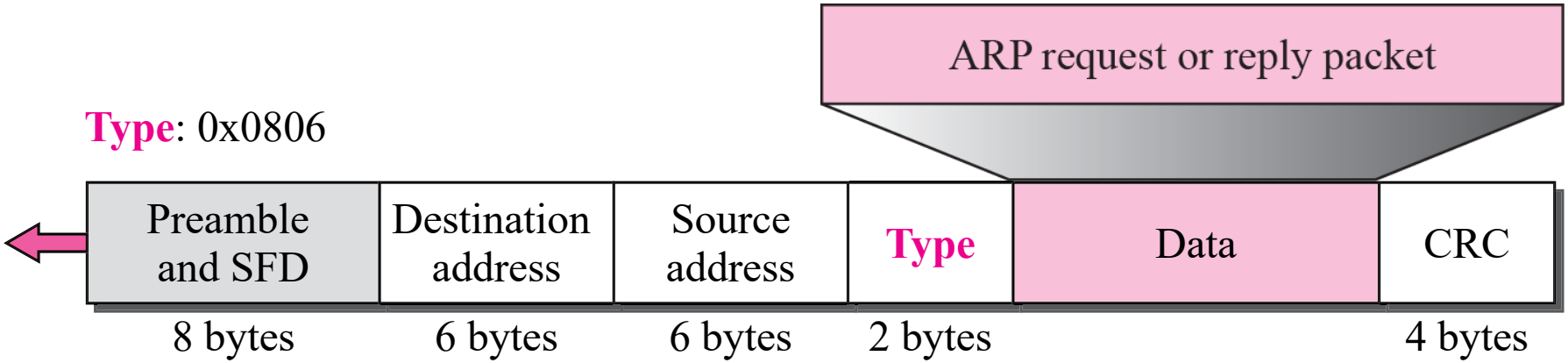
Protocol length. 8-bit field defining the length of the logical address in bytes. For the IPv4 value is 4.

Encapsulation

An ARP packet is encapsulated directly into a data link frame.

Example shows ARP packet encapsulated in an Ethernet frame.

Type field indicates that the data carried by the frame is an ARP packet.



Operation

ARP functions on a typical internet.

- steps involved.
- Four cases in which a host or router needs to use ARP.

7 Steps Involved in an ARP Process

1. The sender knows the IP address of the target.

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. Target physical address field is filled with 0s.

3. 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. All machines except the one targeted drop the packet. The target machine recognizes the IP address.

5. Target machine replies with an ARP reply message that contains its physical address. The message is unicast.

6. Sender receives the reply message. Which contains the physical address of the target machine.

7. IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

Note

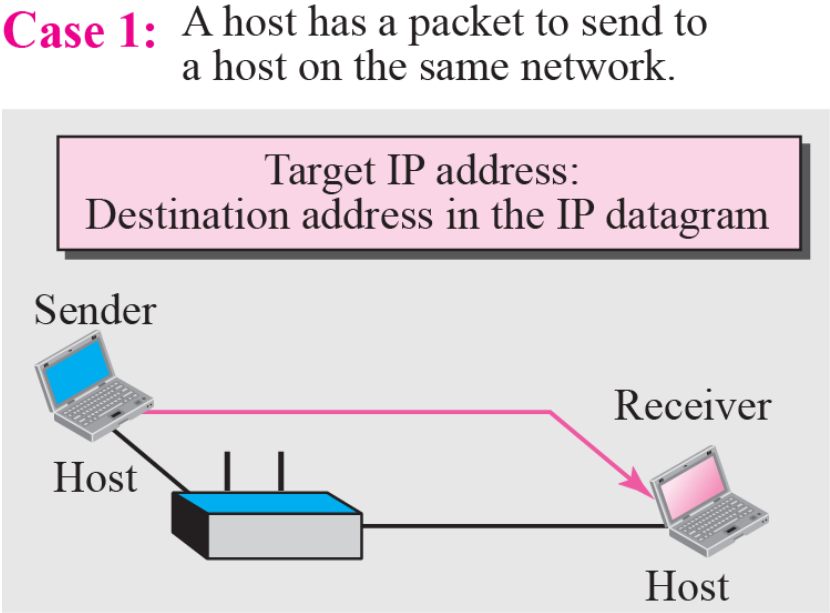
An ARP request is broadcast; an ARP reply is unicast.

Four Different Cases

Four different cases in which the services of ARP can be used.

Case 1:

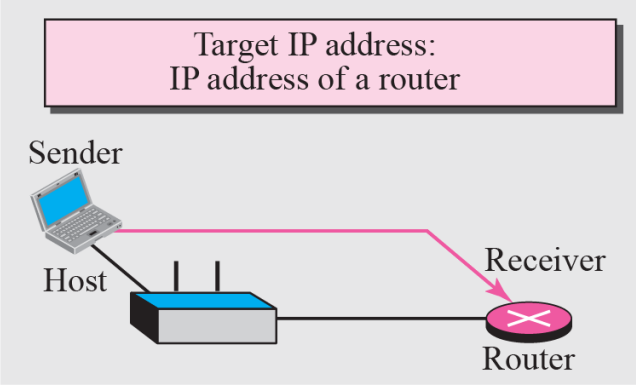
- Sender is a host and wants to send a packet to another host on the same network.
- In this case, the logical address that must be mapped to a physical address is the destination IP address in the datagram header.



Case 2:

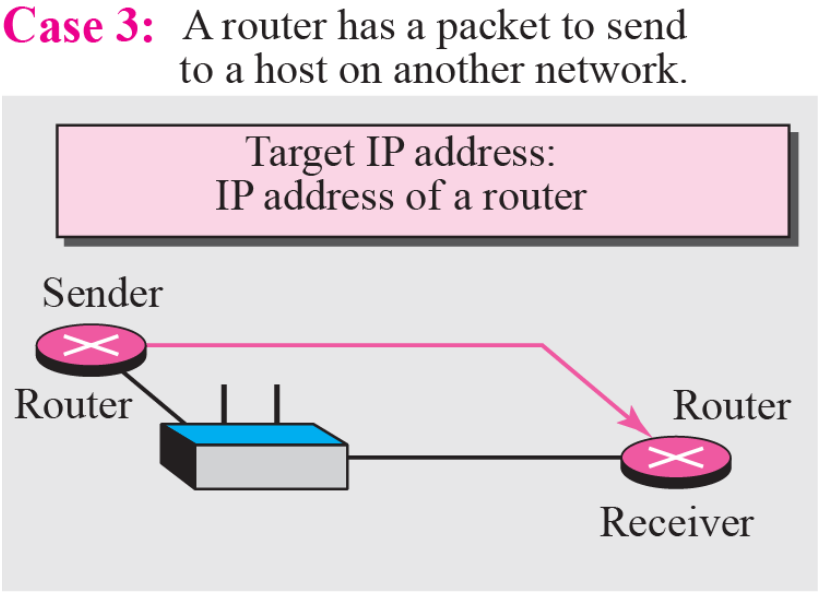
- Sender is a host and wants to send a packet to another host on another network.
- In this case, the host looks at its routing table and finds the IP address of the next hop (router) for this destination. If it does not have a routing table, it looks for the IP address of the default router.
- The IP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

Case 2: A host has a packet to send to a host on another network.



Case 3:

- 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.

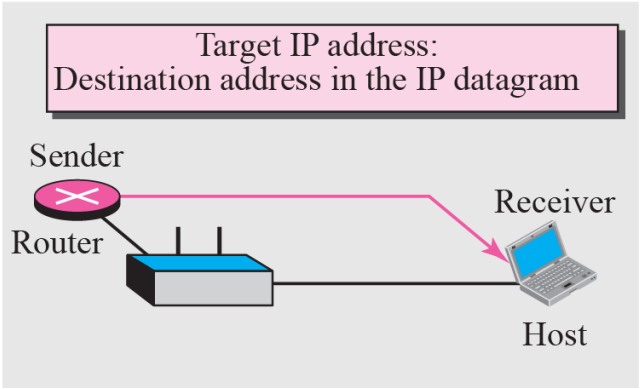


Case 4:

- Sender is a router that has received a datagram destined for a host in the same network.

- Destination IP address of the datagram becomes the logical address that must be mapped to a physical address.

Case 4: A router has a packet to send to a host on the same network.



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.
The two hosts are on the same Ethernet network.
Show the ARP request and reply packets encapsulated in Ethernet frames.

Hardware type: 0x0001
Protocol type: 0x0800

Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

Type: 0x0806

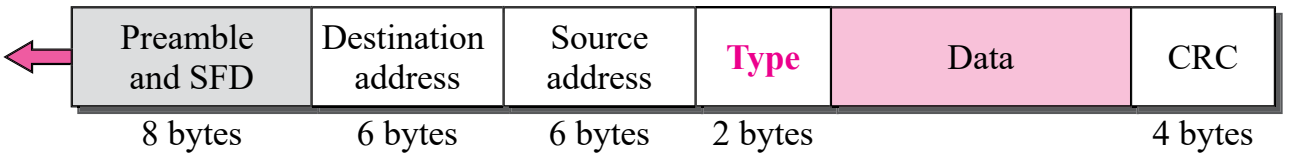


Figure 8.6 *Example 8.1*

IP addresses are shown in hexadecimal.

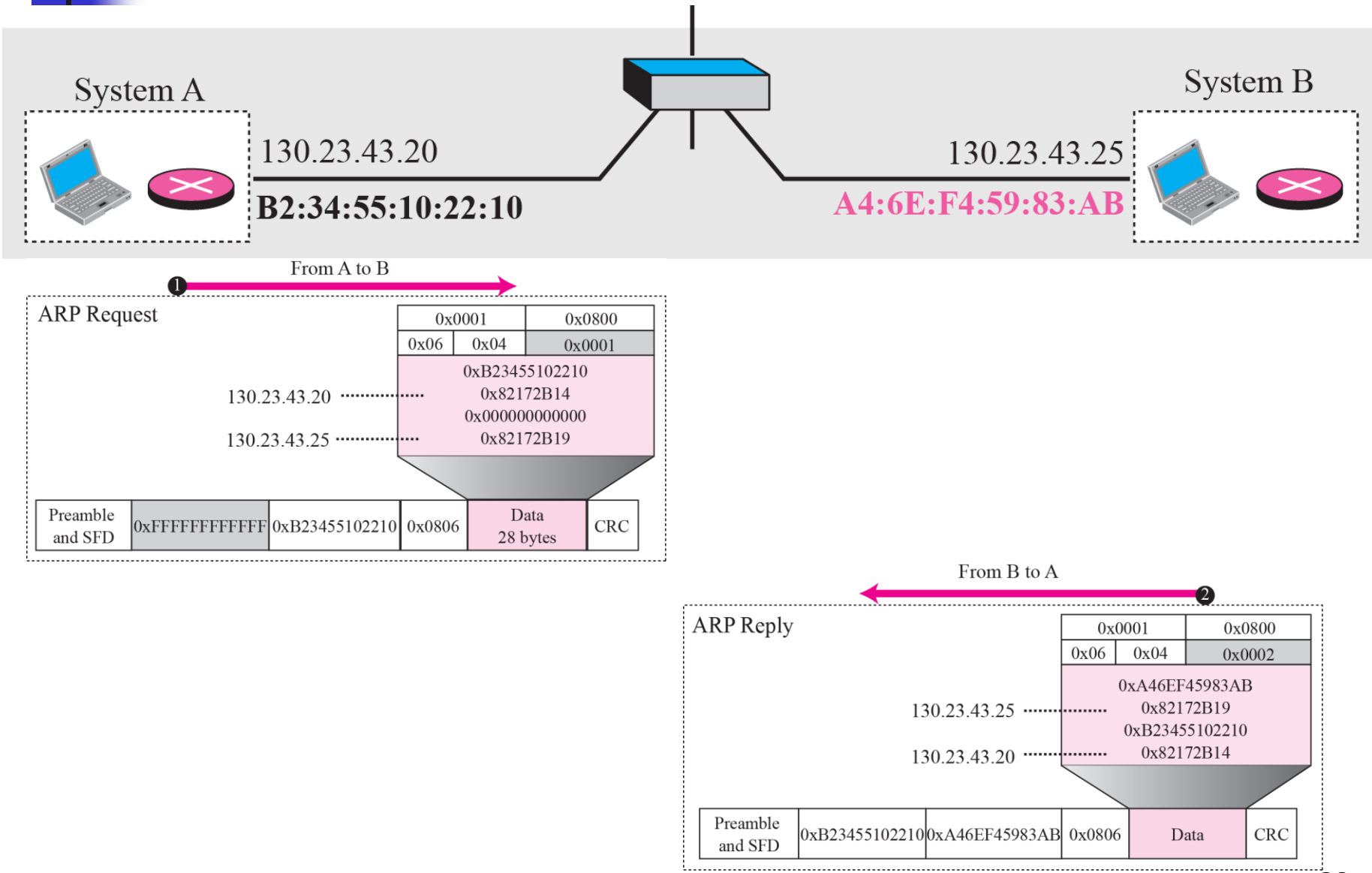


Figure 8.7 *Proxy ARP*

Proxy ARP

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.

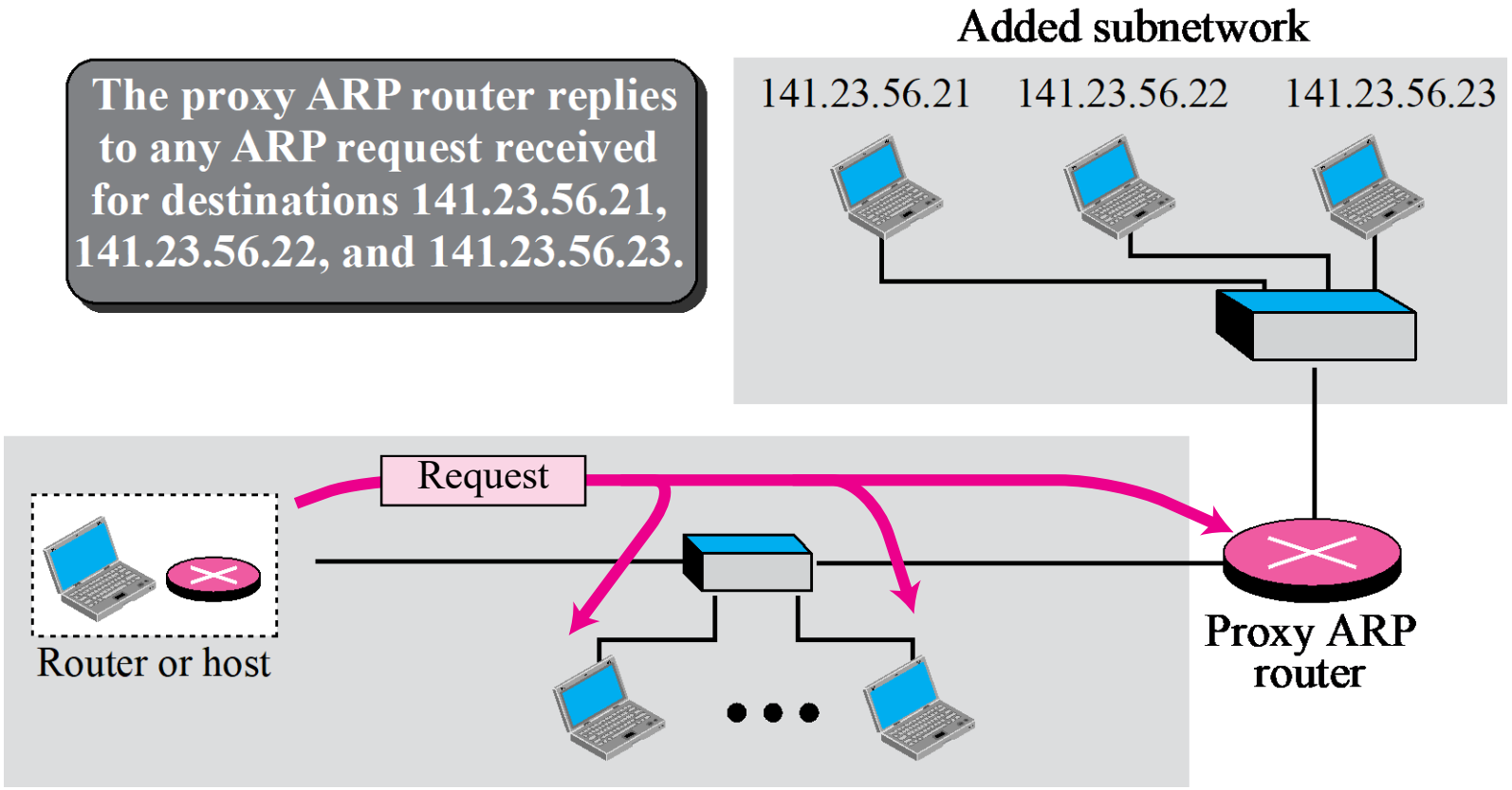
After the router receives the actual IP packet, it sends the packet to the appropriate host or router.

Proxy ARP

When it receives an ARP request with a target IP address that matches the address of one of its protégés (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.

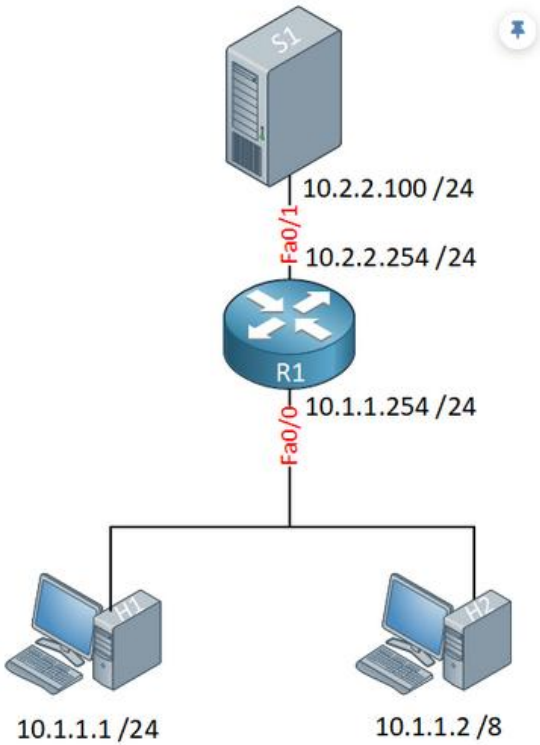
When the router receives the IP packet, it sends the packet to the appropriate host.

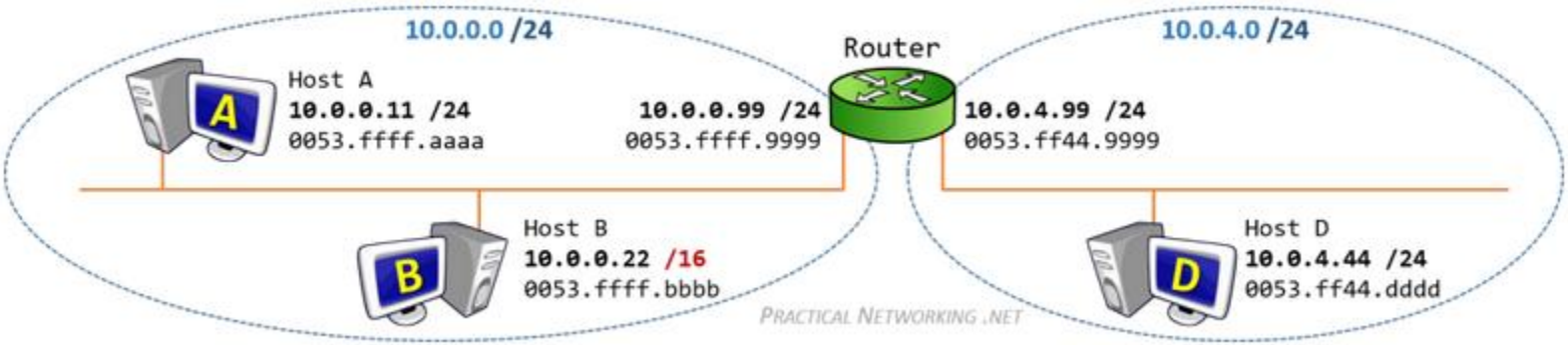
Figure 8.7 *Proxy ARP*



when a host is speaking to another host on the same IP network, the target for the ARP request is the other host's IP address.

If a host is speaking to another host on a different IP network, the target for the ARP request will be the Default Gateway's IP address.


S1
10.2.2.100 /24
Fa0/1
10.2.2.254 /24
R1
10.1.1.254 /24
Fa0/0
H1
H2
10.1.1.1 /24
10.1.1.2 /8


10.0.0.0 /24
Router
10.0.4.0 /24
Host A
10.0.0.11 /24
0053.ffff.aaaa
10.0.0.99 /24
0053.ffff.9999
10.0.4.99 /24
0053.ff44.9999
Host B
10.0.0.22 /16
0053.ffff.bbbb
Host D
10.0.4.44 /24
0053.ff44.dddd
PRACTICAL NETWORKING .NET

https://www.practicalnetworking.net/series/arp/proxy-arp/

https://networklessons.com/cisco/ccie-routing-switching/proxy-arp-explained

Cache Table

A sender usually has more than one IP datagram to send to the same destination.

It is inefficient to use the ARP protocol for each datagram destined for the same host or router.

The solution is the cache table.

However, as space in the cache table is very limited, mappings in the cache are not retained for an unlimited time.

Cache Table (contd)

The cache table is implemented as an array of entries. Each entry contains the following fields:

State. This column shows the state of the entry. It can have one of three values: *FREE, PENDING,* or *RESOLVED*.

- The FREE state means that the time-to-live for this entry has expired. The space can be used for a new entry.
- The PENDING state means a request for this entry has been sent, but the reply has not yet been received.
- The RESOLVED state means that the entry is complete. The entry now has the physical (hardware) address of the destination. The packets waiting to be sent to this destination can use the information in this entry.

Table 8.5 *Original cache table used for examples*

State	*Queue*	*Attempt*	*Time-Out*	*Protocol Addr.*	*Hardware Addr.*
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
F					
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

The ARP output module receives an IP datagram with the destination address 114.5.7.89.

It checks the cache table and finds that an entry exists for this destination with the RESOLVED state (R in the table).

It extracts the hardware address, which is 457342ACAE32, and sends the packet and the address to the data link layer for transmission.

The cache table remains the same.

Example 8.3

Table 8.5 *Original cache table used for examples*

State	Queue	Attempt	Time-Out	Protocol Addr.	Hardware Addr.
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
F					
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

Twenty seconds later, the ARP output module receives an IP datagram (from the IP layer) with the destination address 116.1.7.22.
It checks the cache table and does not find this destination in the table. The module adds an entry to the table with the state PENDING and the Attempt value 1.
It then sends an ARP request to the data link layer for this destination.

Table 8.6 *Updated cache table for Example 8.3*

State	Queue	Attempt	Time-Out	Protocol Addr.	Hardware Addr.
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	23	1		116.1.7.22	
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

Example 8.4

Table 8.6 *Updated cache table for Example 8.3*

State	Queue	Attempt	Time-Out	Protocol Addr.	Hardware Addr.
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	23	1		116.1.7.22	
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

Fifteen seconds later, the ARP input module receives an ARP packet with target protocol (IP) address 188.11.8.71.

The module checks the table and finds this address. It changes the state of the entry to RESOLVED and sets the time-out value to 900.

The module then adds the target hardware address (E34573242ACA) to the entry. Now it accesses queue 18 and sends all the packets in this queue, one by one, to the data link layer.

Table 8.7 *Updated cache table for Example 8.4*

State	Queue	Attempt	Time-Out	Protocol Addr.	Hardware Addr.
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	23	1		116.1.7.22	
R	9		60	19.1.7.82	4573E3242ACA
R	18		900	188.11.8.71	E34573242ACA

Example 8.5

Table 8.7 *Updated cache table for Example 8.4*

State	Queue	Attempt	Time-Out	Protocol Addr.	Hardware Addr.
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	23	1		116.1.7.22	
R	9		60	19.1.7.82	4573E3242ACA
R	18		900	188.11.8.71	E34573242ACA

Twenty-five seconds later, the cache-control module updates every entry. The time-out values for the first 3 resolved entries are decremented by 60. The time-out value for the last resolved entry is decremented by 25. The state of the next-to-the last entry is changed to FREE because the time-out is zero. For each of the three pending entries, the value of the attempts field is incremented by one. After incrementing, the attempts value for one entry (the one with IP address 201.11.56.7) is more than the maximum; the state is changed to FREE, the queue is deleted, and an ICMP message is sent to the original destination.

Table 8.8 *Updated cache table for Example 8.5*

State	Queue	Attempt	Time-Out	Protocol Addr.	Hardware Addr.
R	5		840	180.3.6.1	ACAE32457342
P	2	3		129.34.4.8	
F					
R	8		390	114.5.7.89	457342ACAE32
P	12	2		220.55.5.7	
P	23	2		116.1.7.22	
F					
R	18		875	188.11.8.71	E34573242ACA

END