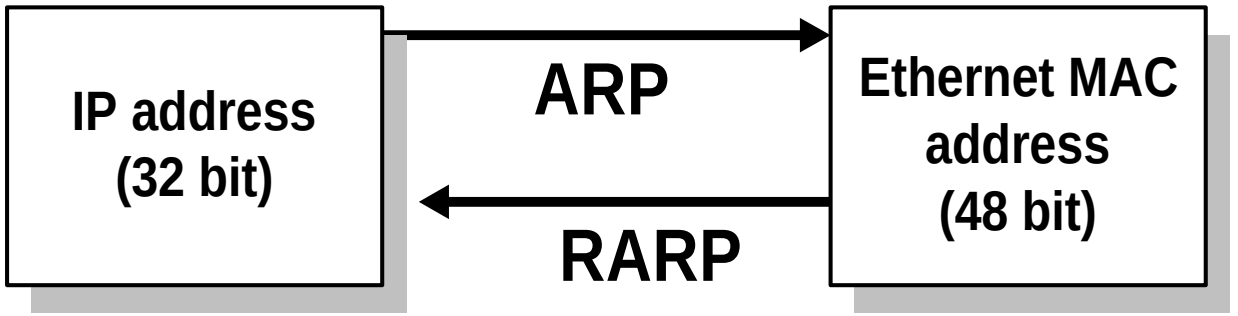
Network Layer Protocols:

ARP, IPv4, ICMPv4, IPv6, and ICMPv6

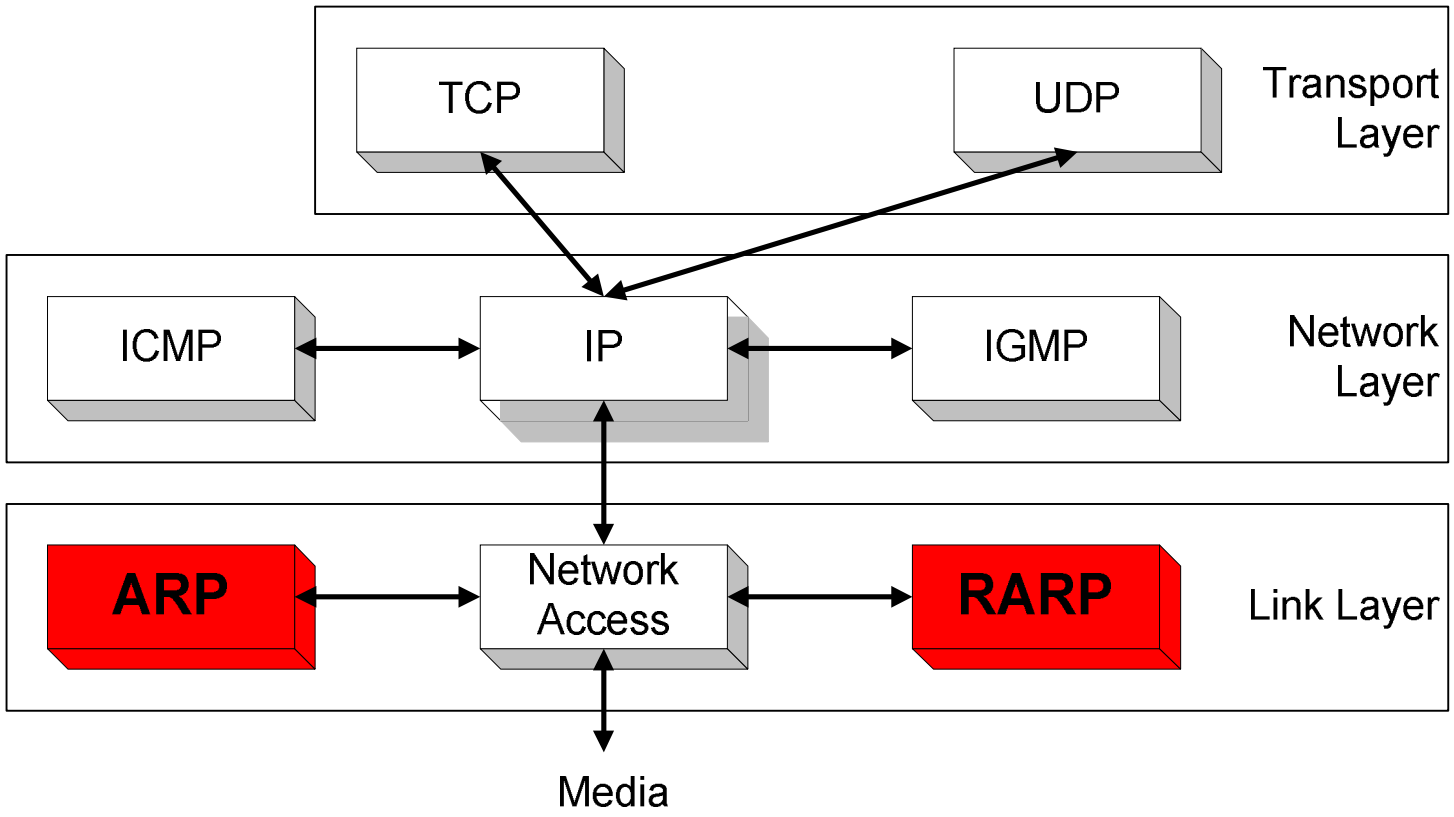
ARP- Address resolution protocol

RARP – Reverse Address resolution protocol

- Note:
  - The Internet is based on IP addresses
  - Data link protocols (Ethernet, FDDI, ATM) may have different (MAC) addresses
- The ARP and RARP protocols perform the translation between IP addresses and MAC layer addresses
- We will discuss ARP for broadcast LANs, particularly Ethernet LANs



ARP and RARP in ISO



ARP (address resolution protocol)

- Address resolution provides a mapping between two different forms of addresses
  - 32-bit IP addresses and whatever the data link uses
- ARP (address resolution protocol) is a protocol used to do address resolution in the TCP/IP protocol suite (**RFC826**)
- ARP provides a dynamic mapping from an IP address to the corresponding hardware address

Basic Idea

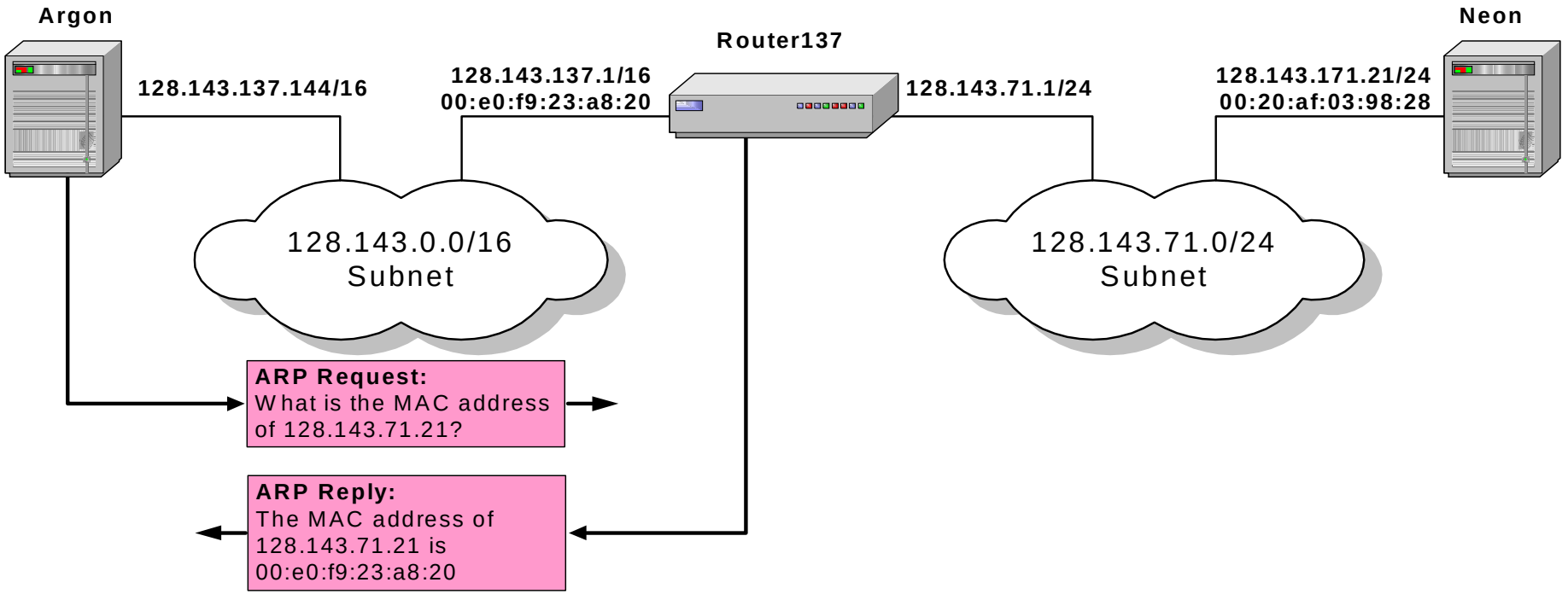
- ARP is required on multi-access channels and relies on the ability to broadcast
- The protocol is simple:
  - broadcast a packet containing the IP address of the destination machine
  - the machine with that address, or possibly a server, sends a reply containing the hardware address
  - upon receipt the hardware address is used to send the original packet

ARP Cache

- Essential to the efficient operation of ARP is the maintenance of a cache on each host
- The cache maintains the recent IP to physical address mappings
- Each entry is aged (usually the lifetime is 20 minutes) forcing periodic updates of the cache
- ARP replies are often broadcast so that all hosts can update their caches

Proxy ARP

- **Proxy ARP:** Host or router responds to ARP Request that arrives from one of its connected networks for a host that is on another of its connected networks.



Gratuitous ARP

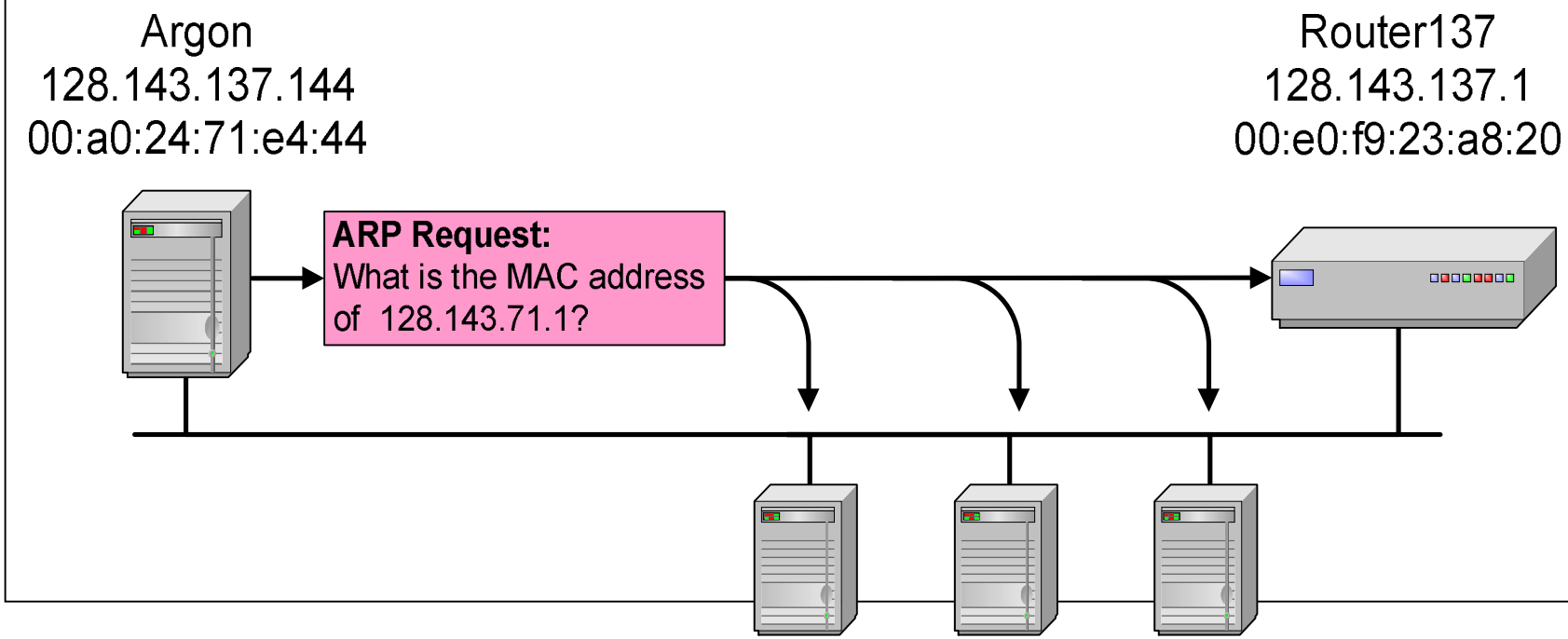
- Gratuitous ARP occurs when a host sends an ARP request looking for its own IP address
- This can happen at bootstrap time
- Gratuitous ARP provides two features
  - it lets a host determine if another host is already configured with the same IP address
  - if the host sending the gratuitous ARP has just changed its hardware address, the packet causes other hosts on the net to update their ARP cache entries

Address Translation with ARP

ARP Request:

Argon broadcasts an ARP request to all stations on the network:

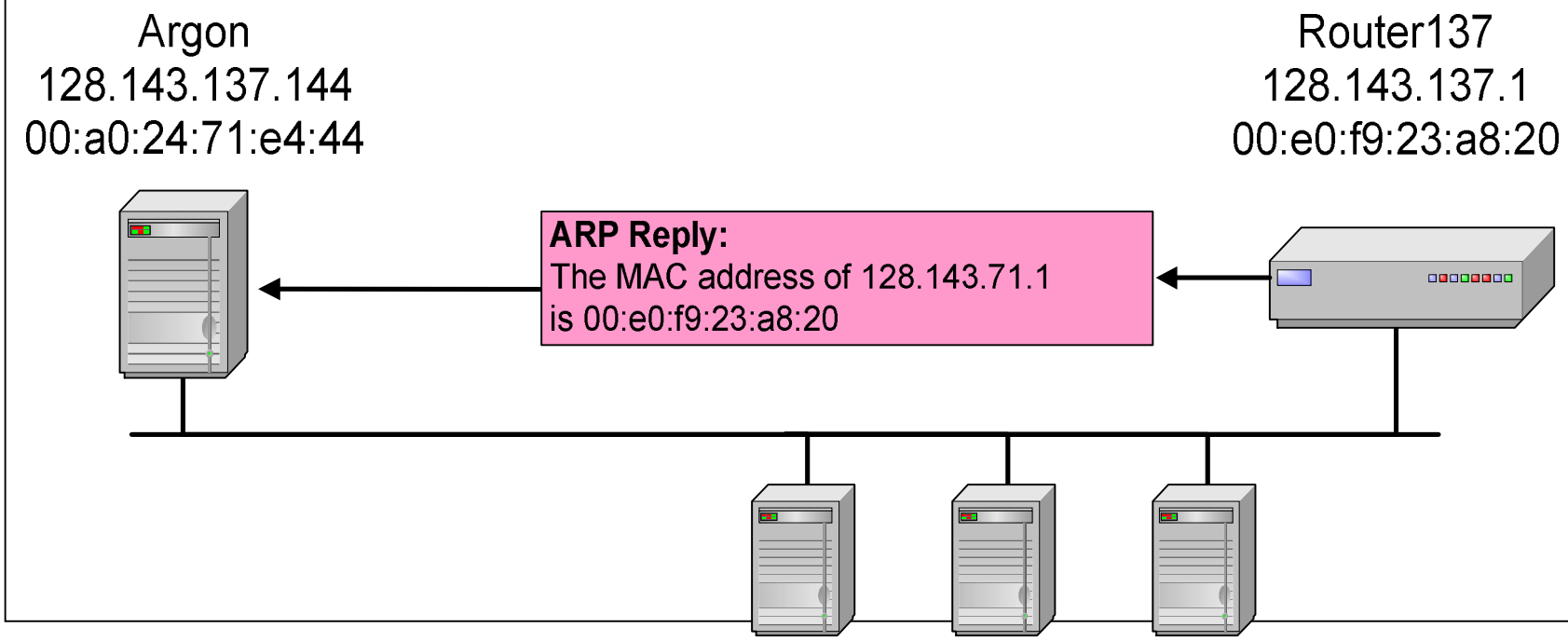
“What is the hardware address of Router137?”



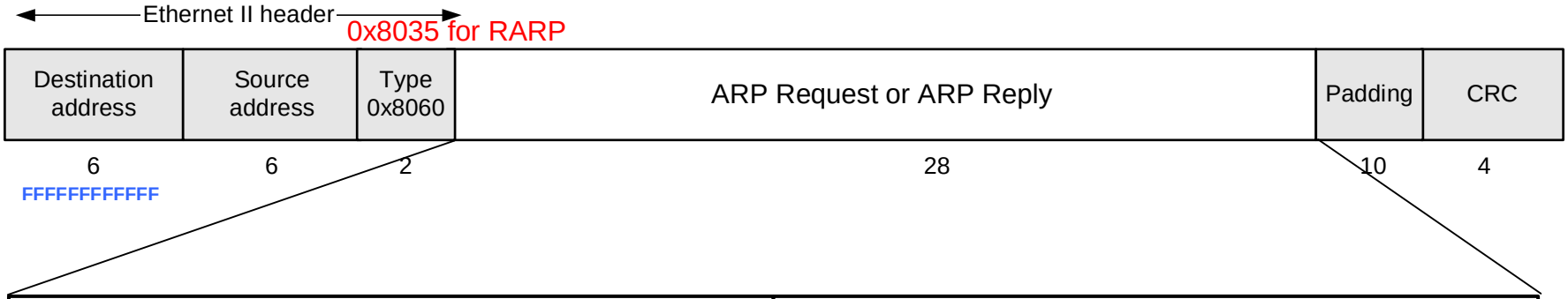
Address Translation with ARP

ARP Reply:

Router 137 responds with an ARP Reply which contains the hardware address



ARP Packet Format



Hardware type (2 bytes) — 1 for Ethernet	Protocol type (2 bytes) — 0800H fpr IP
Hardware address length (1 byte) / Protocol address length (1 byte)	Operation code (2 bytes) — 1 request; 2 reply; 3/4 RAPR req/Reply
Source hardware address*	6 bytes for Ethernet MAC address
Source protocol address*	4 for IP address
Target hardware address*	6 bytes for Ethernet MAC address
Target protocol address*	4 for IP address

* Note: The length of the address fields is determined by the corresponding address length fields

Example

- *ARP Request from Argon:*

Source hardware address:	00:a0:24:71:e4:44
Source protocol address:	128.143.137.144
Target hardware address:	00:00:00:00:00:00
Target protocol address:	128.143.137.1

- *ARP Reply from Router137:*

Source hardware address:	00:e0:f9:23:a8:20
Source protocol address:	128.143.137.1
Target hardware address:	00:a0:24:71:e4:44
Target protocol address:	128.143.137.144

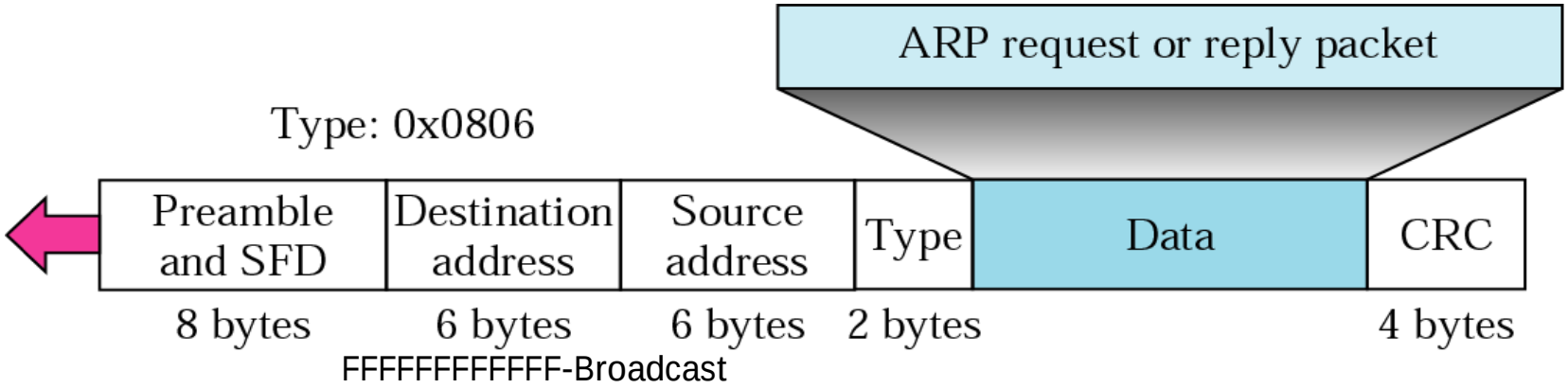
ARP Cache

- Since sending an ARP request/reply for each IP datagram is inefficient, hosts maintain a cache (ARP Cache) of current entries. The entries expire after 20 minutes.

- Contents of the ARP Cache:

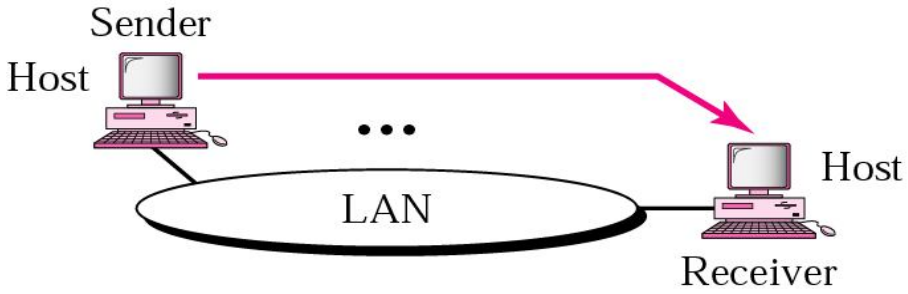
  (128.143.71.37) at 00:10:4B:C5:D1:15 [ether] on eth0
  (128.143.71.36) at 00:B0:D0:E1:17:D5 [ether] on eth0
  (128.143.71.35) at 00:B0:D0:DE:70:E6 [ether] on eth0
  (128.143.136.90) at 00:05:3C:06:27:35 [ether] on eth1
  (128.143.71.34) at 00:B0:D0:E1:17:DB [ether] on eth0
  (128.143.71.33) at 00:B0:D0:E1:17:DF [ether] on eth0

Encapsulation of ARP packet

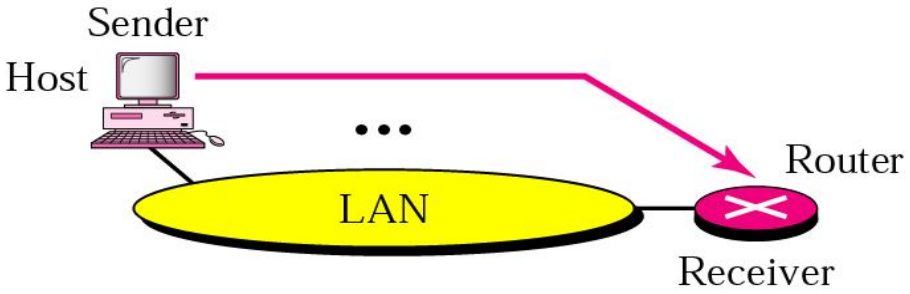


0x0806 = ARP Message

Four cases using ARP

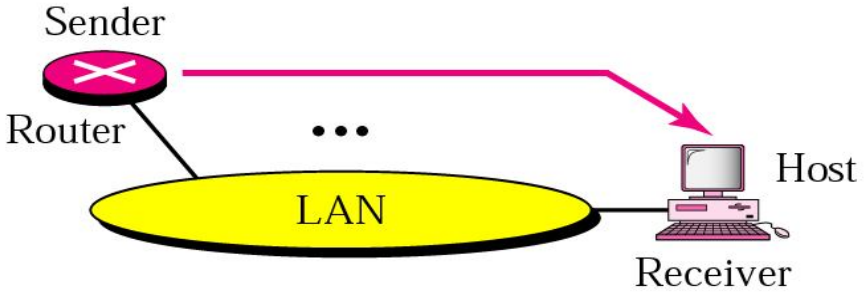


Case 1. A host has a packet to send to another host on the same network.



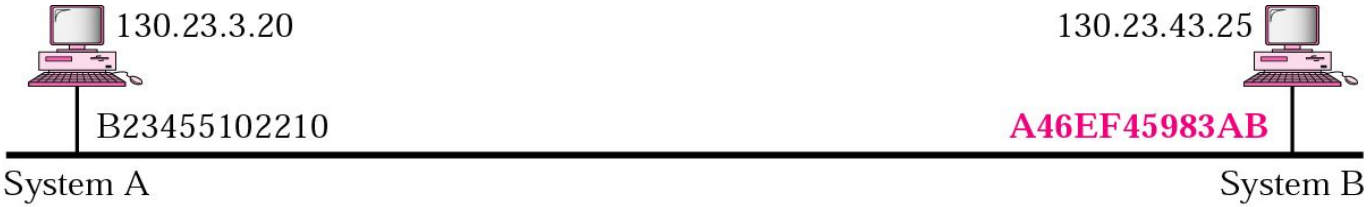
Case 2. A host wants to send a packet to another host on another network.
It must first be delivered to the appropriate router.

Case 3. A router receives a packet to be sent to a host on another network.
It must first be delivered to the appropriate router.

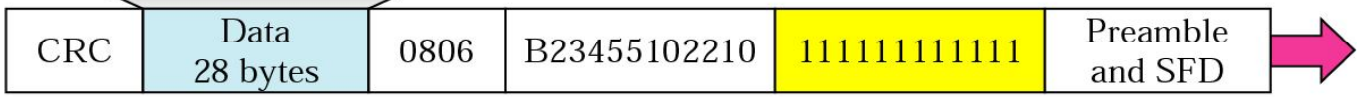


Case 4. A router receives a packet to be sent to a host on the same network.

Example 1



0001		0800
06	04	0001
B23455102210		
130.23.3.20		
000000000000		
130.23.43.25		



ARP Request (from A to B)

A host with IP address 130.23.3.20 and physical address B23455102210 has a packet to send to another host with IP address 130.23.43.25 and physical address A46EF45983AB.

0002		0800
06	04	0002
A46EF45983AB		
130.23.43.25		
B23455102210		
130.23.3.20		

ARP Reply (from B to A)

Issues

- Many people ARP to be a dangerous protocol
  - a bogus host can issue a gratuitous ARP and change cache entries
  - a bogus host can send replies giving its own hardware address (instead of the target)
- Broadcasting can be expensive
  - excessive use of bandwidth
  - CPU costs

Things to know about ARP

- What happens if an ARP Request is made for a non-existing host?

  Several ARP requests are made with increasing time intervals between requests. Eventually, ARP gives up.

- On some systems (including Linux) a host periodically sends ARP Requests for all addresses listed in the ARP cache. This refreshes the ARP cache content, but also introduces traffic.

- Gratuitous ARP Requests: A host sends an ARP request for its own IP address:
  - Useful for detecting if an IP address has already been assigned.

Vulnerabilities of ARP

1. Since ARP does not authenticate requests or replies, ARP Requests and Replies can be forged
2. ARP is stateless: ARP Replies can be sent without a corresponding ARP Request
3. According to the ARP protocol specification, a node receiving an ARP packet (Request or Reply) must update its local ARP cache with the information in the source fields, if the receiving node already has an entry for the IP address of the source in its ARP cache. (This applies for ARP Request packets and for ARP Reply packets)

Typical exploitation of these vulnerabilities:

- A forged ARP Request or Reply can be used to update the ARP cache of a remote system with a forged entry (ARP Poisoning)
- This can be used to redirect IP traffic to other hosts

RARP (Reverse Address Resolution Protocol)

- It used to require the Ethernet address of the IP address.
- The principle of RARP is for the diskless system to read its unique hardware address from the interface card and send an RARP request asking for someone to reply with the diskless system's IP address.

Reverse Address Resolution Protocol

- When a system boots, it typically gets its IP address from a file
- How does a system, without a disk, get its IP address?
- Since each system has a unique hardware address, that hardware address can be used to lookup the corresponding IP address
- RARP (RFC903) does exactly that

RARP Packet Format

- The format is exactly the same as ARP except some of the numbers change
- The RARP request is broadcast and the reply is sent to the requester
- Unlike ARP, designated RARP server(s) that handles RARP requests

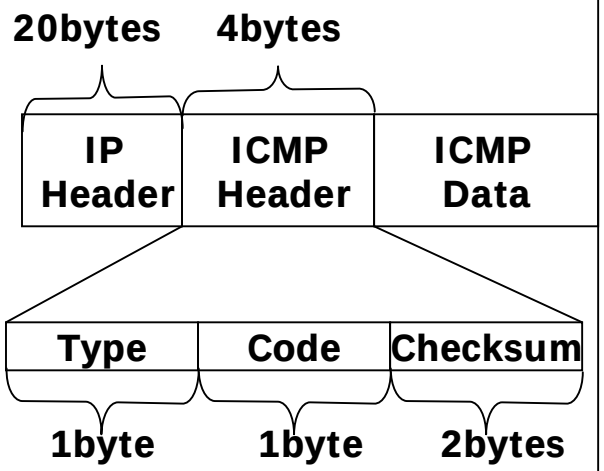
ICMP
Internet Control Message Protocol

- ICMP is a protocol used for exchanging control messages.
- ICMP uses IP to deliver messages.
- ICMP messages are usually generated and processed by the IP software, not the user process.

ICMP : Internet Control Message Protocol

- IP has no error reporting. (What happen if something go wrong?)
  - If router must to discard a datagram because it cannot find the final dest
  - A host sometimes needs to determine if router or another host is alive
- The ICMP has been design to compensate these deficiencies.
- It is a companion to the IP
- Used to report problems with delivery of IP Datagrams within an IP network
- Used by Ping, Tracerout commands

ICMP Message

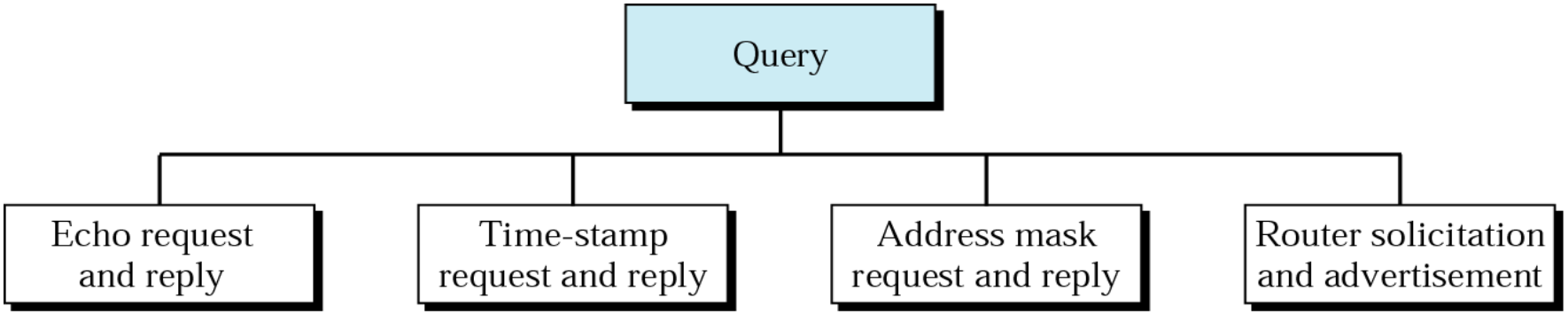


Types and Codes

- Echo Request (type=8, code=0)
- Echo Reply(type=0, code=0)
- Destination Unreachable(type=3, code=0)
- Time Exceeded(type=11, code=0) : Time-to-Live =0

Query messages

There is no flow control or congestion control mechanism in IP.



ICMP Message Types **Error-reporting messages**

- Echo Request
- Echo Response
- Destination Unreachable
- Redirect
- Time Exceeded
- Redirect (route change)
- there are more ...