NAT: Network Address Translation

Private Network

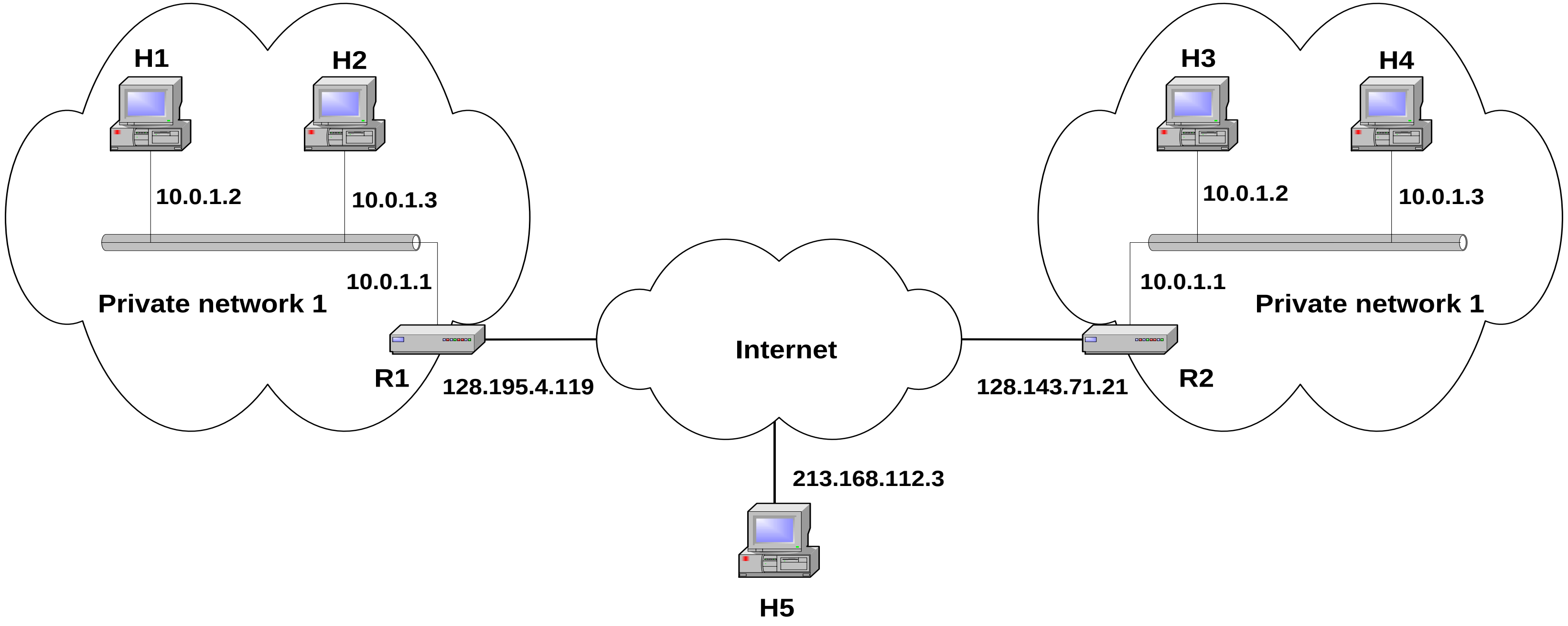
- *Private IP* network is an IP network that is not directly connected to the Internet

- IP addresses in a private network can be assigned arbitrarily.
  - Not registered and not guaranteed to be globally unique

- Generally, private networks use addresses from the following experimental address ranges **[RFC 1918]**
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Private Addresses

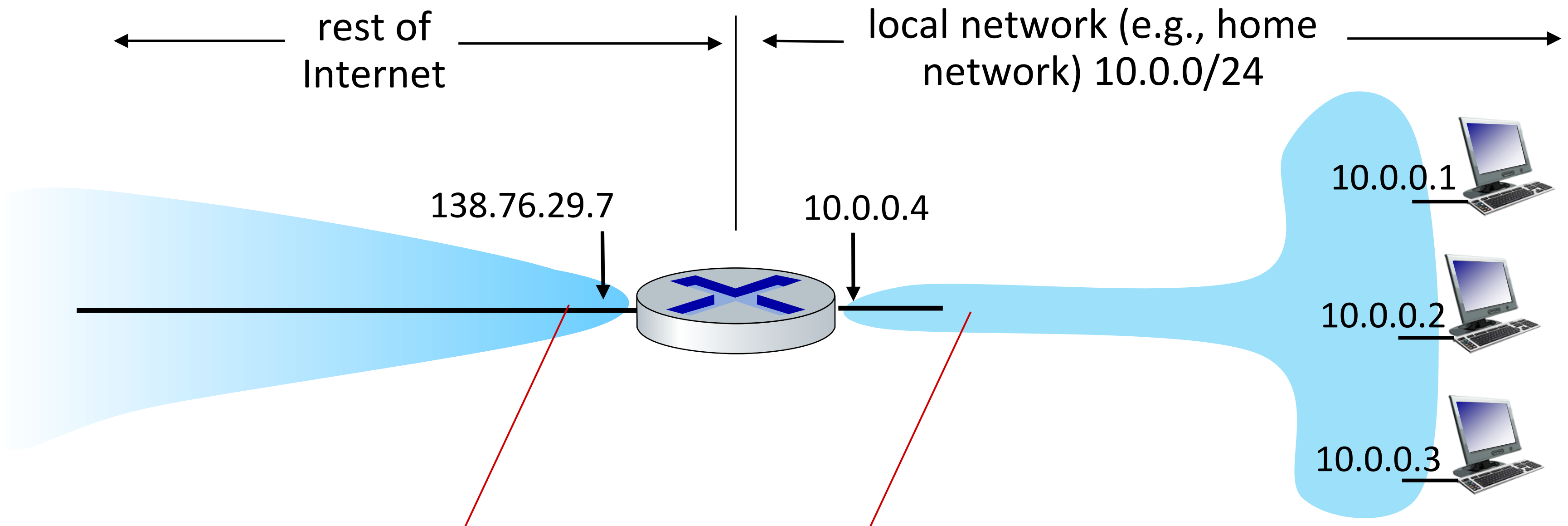


Network Address Translation (NAT)

- RFC 1631
- A short term solution to the problem of the shortage of IP addresses
  - Long term solution is IP v6
  - CIDR (Classless Inter Domain Routing) is a possible short term solution
  - NAT is another
- NAT is a way to conserve IP addresses
  - Can be used to hide a number of hosts behind a single IP address
  - Uses private addresses:
    - 10.0.0.0-10.255.255.255,
    - 172.16.0.0-172.32.255.255 or
    - 192.168.0.0-192.168.255.255

NAT: network address translation

NAT: all devices in local network share just one IPv4 address as far as outside world is concerned



all datagrams *leaving* local network have *same* source NAT IP address: 138.76.29.7, but *different* source port numbers

datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

NAT: network address translation

- all devices in local network have 32-bit addresses in a “private” IP address space (10/8, 172.16/12, 192.168/16 prefixes) that can only be used in local network
- advantages:
  - just one IP address needed from provider ISP for *all* devices
  - can change addresses of host in local network without notifying outside world
  - can change ISP without changing addresses of devices in local network
  - security: devices inside local net not directly addressable, visible by outside world

NAT: network address translation

implementation: NAT router must (transparently):

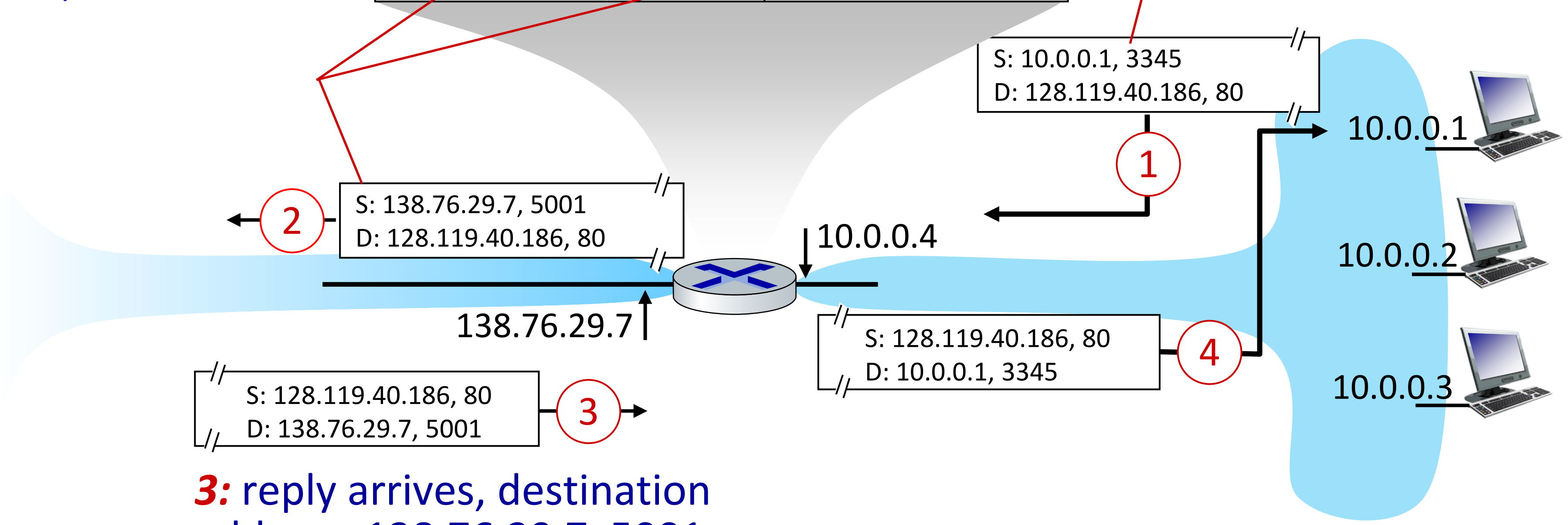
- outgoing datagrams: replace (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)
  - remote clients/servers will respond using (NAT IP address, new port #) as destination address
- remember (in NAT translation table) every (source IP address, port #) to (NAT IP address, new port #) translation pair
- incoming datagrams: replace (NAT IP address, new port #) in destination fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

NAT: network address translation

2: NAT router changes datagram source address from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

NAT translation table	
WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
……	……

1: host 10.0.0.1 sends datagram to 128.119.40.186, 80



3: reply arrives, destination address: 138.76.29.7, 5001

Concerns about NAT

- **Performance:**
  - Modifying the IP header by changing the IP address requires that NAT boxes recalculate the IP header checksum
  - Modifying port number requires that NAT boxes recalculate TCP checksum

- **End-to-end connectivity:**
  - NAT destroys universal end-to-end reachability of hosts on the Internet.
  - A host in the public Internet often cannot initiate communication to a host in a private network.
  - The problem is worse, when two hosts that are in a private network need to communicate with each other.
- **but NAT is here to stay:**
  - extensively used in home and institutional nets, 4G/5G cellular nets

Address Resolution Protocol (ARP)

Address Mapping Cont..

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

- **We need to be able to map a logical address to its corresponding physical address and vice versa.**

- **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.**

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

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

- **A mapping corresponds a logical address to a physical address. 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.**

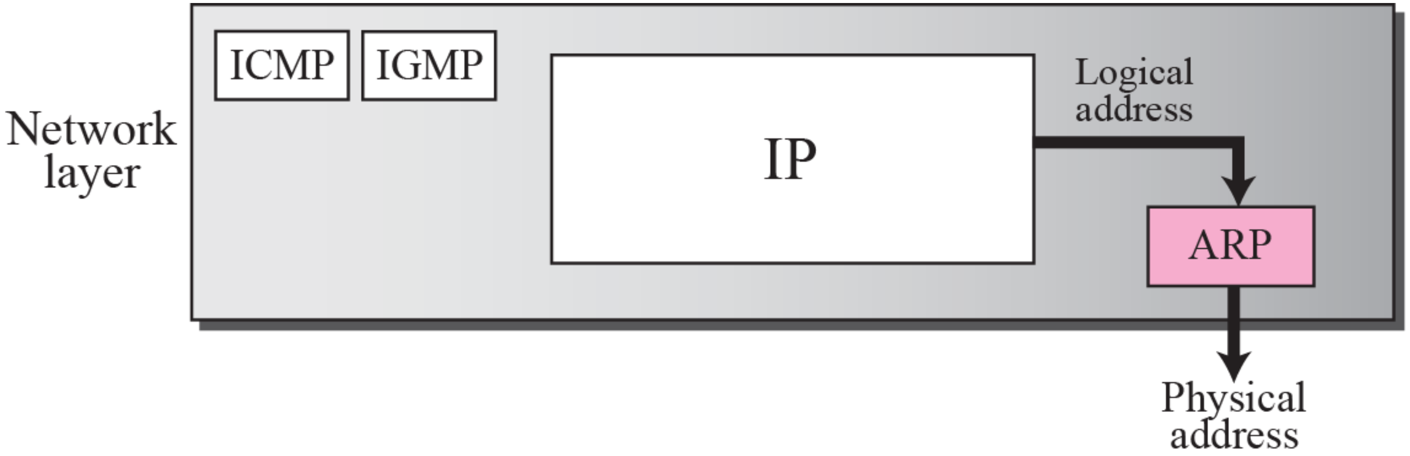
Logical and Physical addresses

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : iitbhilai.ac.in
   Description . . . . . . . . . . . : Qualcomm QCA9377 802.11ac Wireless Adapter
   Physical Address. . . . . . . . . : B0-68-E6-82-D9-8D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::80d1:147e:1fc0:c043%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.3.54.107(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.192.0
   Lease Obtained. . . . . . . . . . : 29 September 2020 09:39:45
   Lease Expires . . . . . . . . . . : 29 September 2020 18:28:38
   Default Gateway . . . . . . . . . : 10.3.0.1
   DHCP Server . . . . . . . . . . . : 10.1.72.7
   DHCPv6 IAID . . . . . . . . . . . : 162556134
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-F3-49-C3-D8-D0-90-5B-50-B5
   DNS Servers . . . . . . . . . . . : 192.168.10.87
                                       192.168.10.72
```

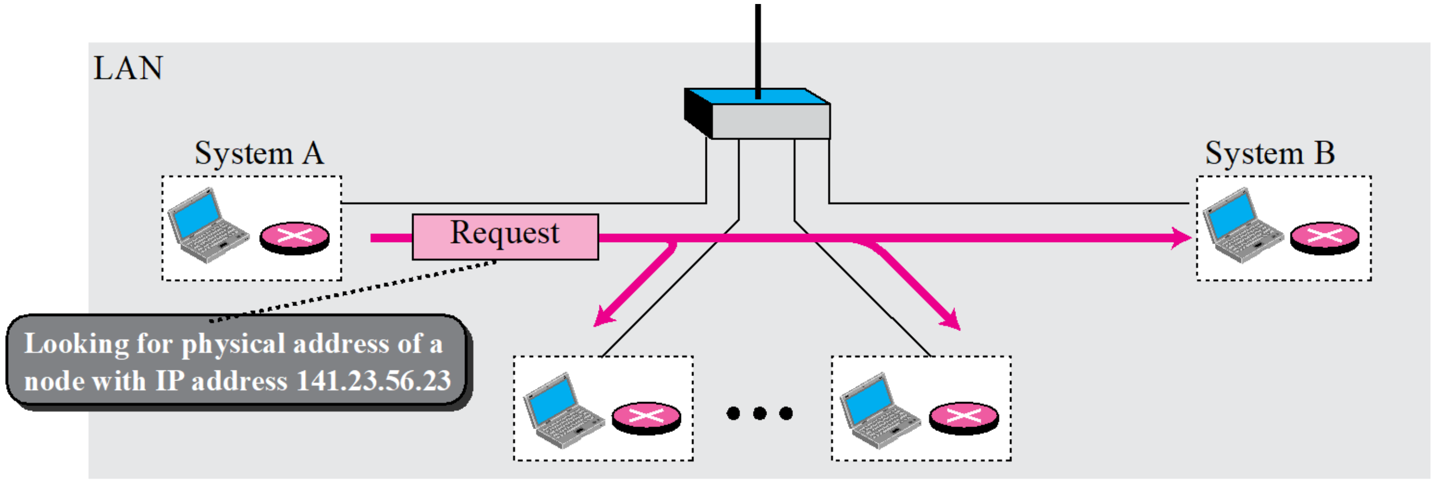
ARP Cache

```
C:\Users\Anand>arp -a

Interface: 10.3.54.107 --- 0x9
  Internet Address      Physical Address      Type
  10.3.0.1              00-00-0c-07-ac-cd     dynamic
  10.3.52.151           a4-fc-77-04-20-43     dynamic
  10.3.58.183           00-28-f8-93-47-7a     dynamic
  10.3.63.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

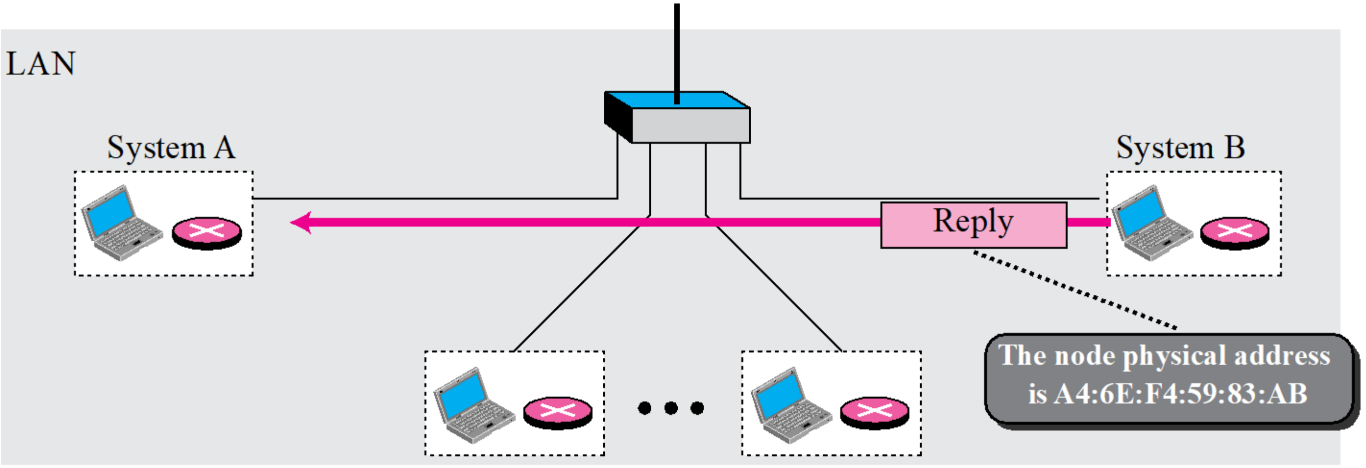
Position of ARP in TCP/IP protocol suite



ARP operation



a. ARP request is broadcast

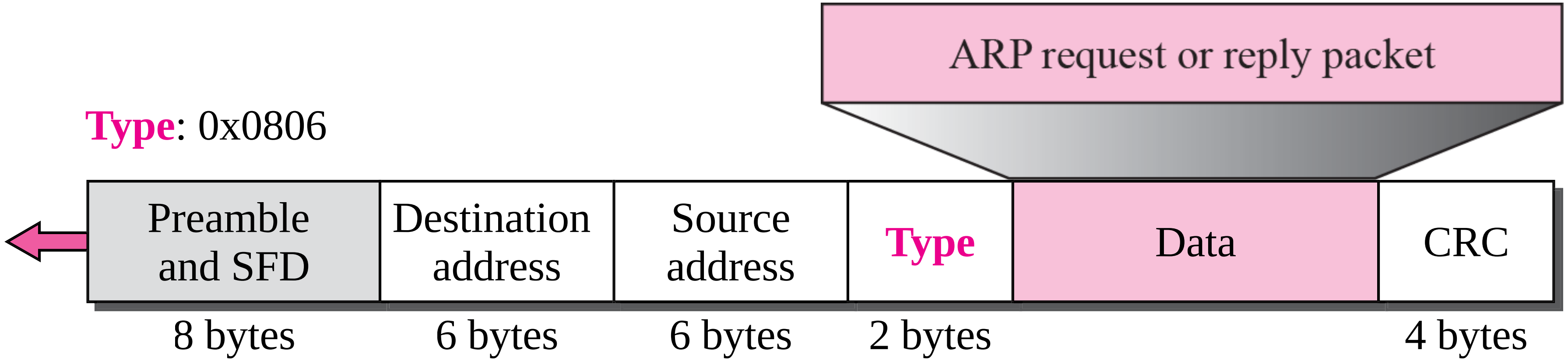


b. ARP reply is unicast

ARP packet

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)			

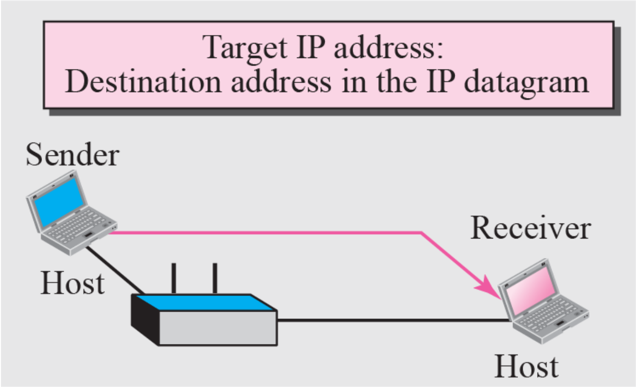
Encapsulation of ARP packet



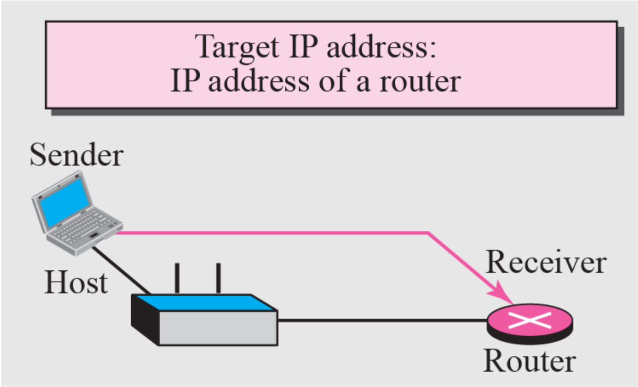
An ARP request is broadcast; an ARP reply is unicast.

Four cases using ARP

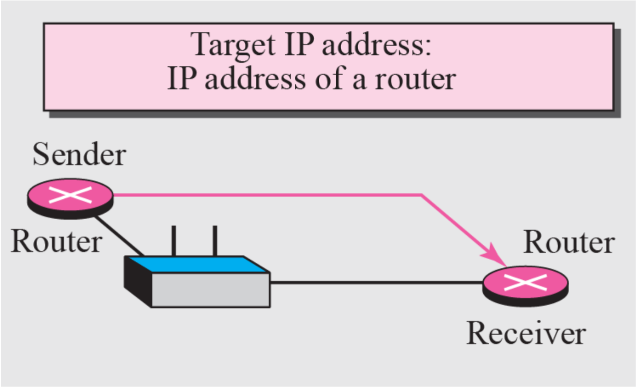
Case 1: A host has a packet to send to a host on the same network.



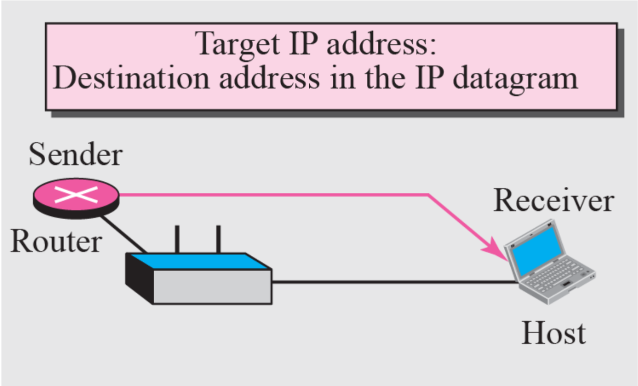
Case 2: A host has a packet to send to a host on another network.



Case 3: A router has a packet to send to a host on another network.



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



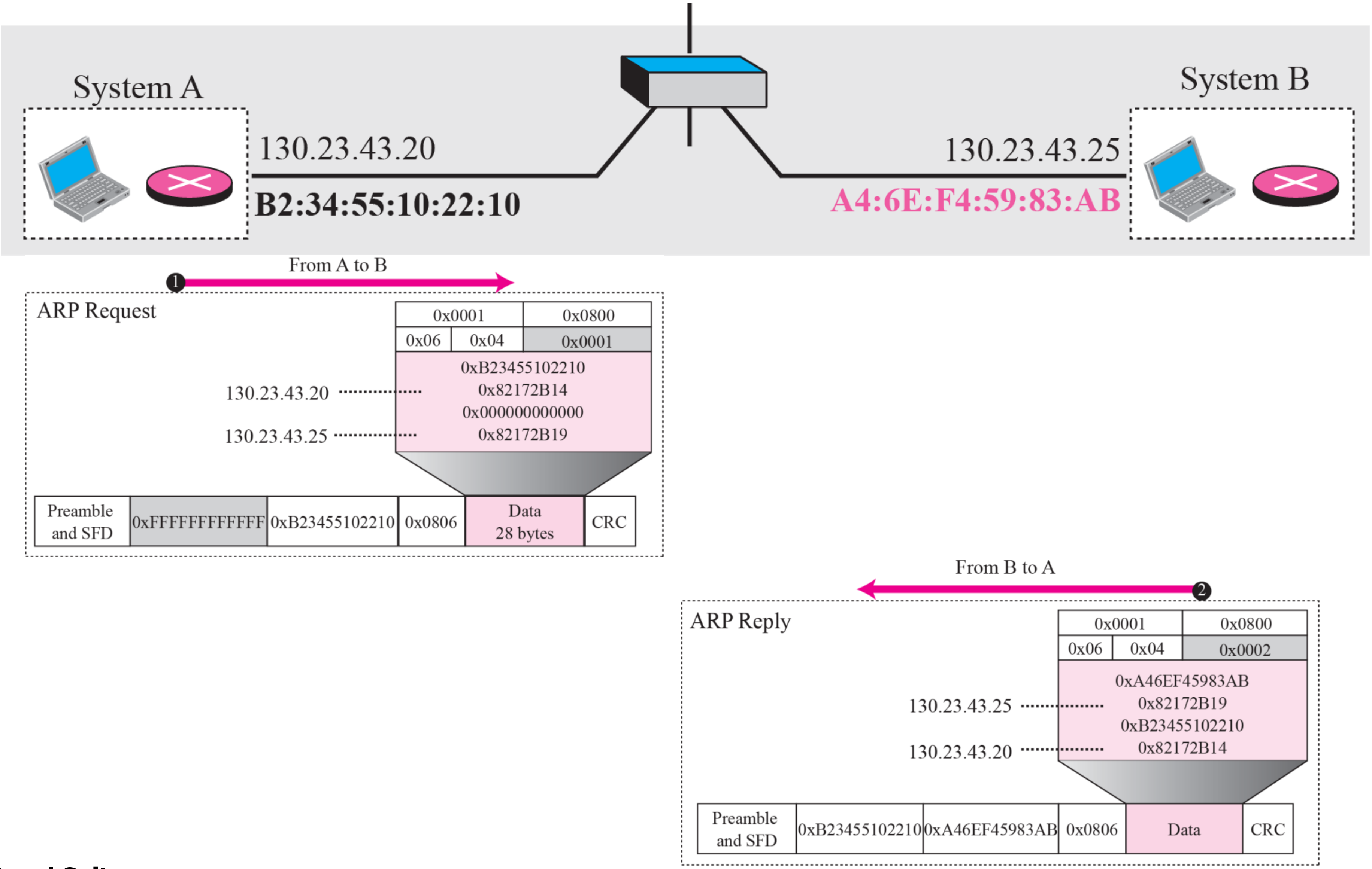
Example

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.

Solution

Figure 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.

Example


System A
System B
130.23.43.20
B2:34:55:10:22:10
130.23.43.25
A4:6E:F4:59:83:AB
From A to B
ARP Request
0x0001
0x0800
0x06
0x04
0x0001
0xB23455102210
0x82172B14
0x000000000000
0x82172B19
130.23.43.20
130.23.43.25
Preamble and SFD
0xFFFFFFFFFFFF
0xB23455102210
0x0806
Data 28 bytes
CRC
From B to A
ARP Reply
0x0001
0x0800
0x06
0x04
0x0002
0xA46EF45983AB
0x82172B19
0xB23455102210
0x82172B14
130.23.43.25
130.23.43.20
Preamble and SFD
0xB23455102210
0xA46EF45983AB
0x0806
Data
CRC