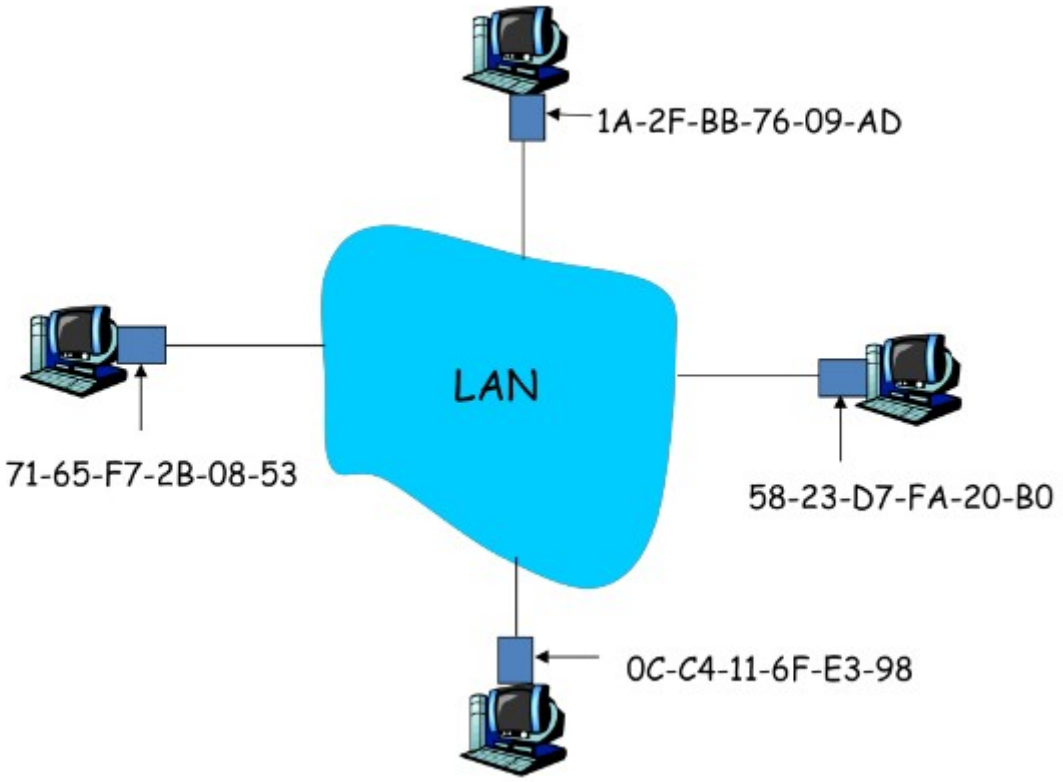
Lab#6: Address Resolution Protocol

You can read Kurose 5.4.

1. Intro

Every network interface card (NIC) has a 48-bit address called MAC address (aka physical address) represented by twelve hexadecimal digits, each byte represented by two digits.



Each computer will have an IP address associated with each network interface too. Most computers only have just one interface active at any time, so the idea of one computer means one IP address is accurate then.

The point now is how IP addresses and MAC addresses are related. Well, they are not. But given that MAC addresses are needed to send a datagram to the right destination, an IP address mapping to MAC address is needed. That is the purpose of the Address Resolution Protocol (or ARP). ARP provides the MAC address for a given IP address to any sender in the same subnet as the destination.

2. Traffic analysis

Wireshark software will be used for gathering ARP traffic so it can be studied in detail. But first lets have a look at our computer's configuration details.

Exercise#1. Using ifconfig find out how many network interface cards are installed in your computer.

1. Write down each card's MAC address and the corresponding IP address too.
2. Find out what type of technology is used for each network adapter.

For the next exercise the link layer information is where attention will be focused. Please note that ARP is not related to IP protocol at all. Though it is related to IP addresses, the information exchange it is purely based on the exchange of two link layer frames with an specific data format.

Exercise#2. Start a Wireshark capture (http-traffic capture filter this time) while you load www.uv.es main page on your browser.

1. What type of transport layer addressing is used?
2. What type of network layer addressing is used?
3. What type of link layer addressing is used? Whom is the destination MAC address?
4. What does Type field mean (on Ethernet header)? What is its value for captured traffic?

Our computer keeps a list of previously resolved MAC-to-IP mappings in memory. This way a new ARP is not needed for each IP datagram you want to send to a known destination. **arp** is a command you can use to access to that list.

Exercise#3. From a shell window run the command arp -a to list the content of the resolution cache. Write down the results. Which are the computers that appear on the list? How are they related with the previous exercise?

1. Now start a new Wireshark capture (no capture filter this time).
2. Now execute ping -c 1 158.42.180.62 and check againg the content of the ARP cache. What is the MAC address for that destination? You can stop the capture now.
3. Find the ARP request and reply within the capture (you can use display filter arp). Double-check that these frames do not include any TCP/IP known header.

Exercise#4. Now repeat a Wireshark while you ping to www.uji.es

1. Check if new entries appear now in your ARP cache. As you know, your computer performed a DNS query to resolve www.uji.es name. Why DNS server MAC address does not appear on your ARP cache?

ARP

2. What other MAC addresses are present on you ARP cache? Who they belong to?

Exercise#5. Repeat a capture with Wireshark while you do a ping broadcast (ping -b 158.42.171.255).

1. Check now the ARP cache. How many new entries have appeared? What computers are from?

2. Use the ARP display filter on Wireshark to show only ARP-related messages. Find one message that was querying for your own MAC address. What is the IP and MAC address of the requester? What is the destination MAC address of that frame? Who is answering it? What information is present in the response?

3. How many hosts have asked for your MAC address? Check if they are on your ARP cache too.

Exercise#6. Find out three MAC addresses of three other computers in the lab. You can combine the use of ping and arp commands (not need wireshark for that). Please note that ARP requests (and replies) happen regardless the destination computer drops ICMP's echo-request messages because of a firewall.

So you could use this was as an indication a computer is alive in your network even if it refuses to answer your ping commands.