

Universidad de León
Bachelor Degree on Computer Engineering
Course on Computer Networks

Practice on the ARP Protocol

All rights reserved © 2013-2021 by José María Foces Morán and José María Foces Vivancos

Reference documentation for this practice

- The following practice document contains technical information about the ARP protocol that can be used as an introduction to ARP.

<http://paloalto.unileon.es/cn/labs/CN-IP-ARP-ICMP.pdf>

- In addition, you may wish to skim the following presentation about ARP:

<http://paloalto.unileon.es/cn/labs/CN-IP-ARP-ICMP-DHCP.pdf>

Exercises for practice

1. Connect to your account in paloalto.unileon.es (ssh -p 50500 ...)

```
$ ssh -p 50500 <login name>@paloalto.unileon.es
```

2. We need that you *jump* into two hosts from Lab B6 after logging into the remote lab. Select two ready hosts from VLAN 30 or VLAN 50; check connectivity with ping as in the following command:

```
$ ping 192.168.50.102
```

Check another host from that same VLAN:

```
$ ping 192.168.50.103
```

Check with other IPs from the same VLAN if you receive echo from neither. You may check 192.168.50.100, 192.168.50.101, etc. You can discover other ready hosts in 192.168.30.[100, 101, ...].

3. Let's use the convention of calling each host H_{102} and H_{103} , respectively. Assuming that you did receive echo as much from 192.168.50.102 as from 192.168.50.103, open two sessions on H_{102} and another one on H_{103} . In all of them, use the habitual administrator

4. To be done at H₁₀₂:

- a. Get the current contents of the arp table by submitting the following arp command:

```
$ arp -a
```

Observe the listing of IP to MAC mappings.

- b. Clear the arp table entry corresponding to host H₁₀₃:

```
$ su
Password:
# arp -d 192.168.50.103
# arp -a
```

The preceding command should print no mapping to IP address 192.168.50.103, at this time.

- c. Before proceeding to capturing ARP messages with tcpdump, check again the current contents of the arp table of host H₁₀₃. The listing should contain no mapping for resolution for H₁₀₃:

```
[internal 11] $ arp -a
```

Now, host H₁₀₂ *doesn't know* about the MAC address corresponding to H₁₀₃, thus, if you send a **ping to H₁₀₃**, before sending the first ICMP Echo request packet, H₁₀₂ host will have to find out the MAC of H₁₀₃. Resolving this MAC entails using the ARP protocol.

First, your host will send an ARP REQUEST to the broadcast address, afterwards host H₁₀₃ will respond with an ARP REPLY containing the MAC of the NIC used by H₁₀₃ for sending the ARP REPLY.

To check that host H₁₀₂ receives the ARP REPLY; you'll have to run tcpdump, as in the following command. Select the right NIC in H₁₀₂, usually eno1 is ok in many hosts in Lab B6:

```
# tcpdump -i eno1 -n -ex -XX -vvv arp or icmp
```

- d. Now, from your second session on H₁₀₂, send a ping to 192.168.50.103 that sends 3 echo packets:

```
$ ping -c 3 192.168.50.103
```

5. **Document and explain** the results that you have obtained, as much in H₁₀₂ as in H₁₀₃. If necessary, repeat all the steps if some results are not what you expected; maybe you want to change the *experiment* somehow so that you better understand some aspect of this practice or the lecture. If you need some explanation about ARP, read the practice and the presentation referenced above.
6. Speculate or explain why some ARP requests go *unicast* instead of *broadcast*.
7. What is *gratuitous ARP*? Explain it briefly.
8. Create a scenario to observe Gratuitous ARP; explain your solution and interpret the results that you have obtained. VLANs 10, 30, 40 and 50 use a DHCP server that can help you with this exercise. Most of the PCs connected to those VLANs boot with DHCP, so they must send a Gratuitous ARP after accepting the IP address granted by the DHCP server.