Lab 5 – ARP

RES 841

October 2013

Introduction

1 Scope of the IP and MAC addresses

For this lab, we will work on the same topology as in TP_5a. In the TP_5a directory, you will find the same network as in the last lab, already configured. Once your network is started, check that all paths are well configured by sending `ping` requests between representative couples of stations, that belong to the same subnetwork and to different subnetworks. In this section, you will send packets from various sources to various destinations and notice how MAC and IP addresses change (or not).

1. Using `tcpdump -e -t` and maybe `wireshark`, capture the traffic that corresponds to a `ping` request between $A1$ and $A2$. What are the MAC and IP addresses of the source and of the destination? Which machines do these IP and MAC addresses identify?

2. Repeat the experience between $A1$ and $B1$, then between $Distant$ and $B1$. What do you notice on IP and MAC addresses? Explain.

3. Send now a `broadcast ping` request from $A1$ on subnet A while you capture the traffic on $A2$. What do you notice on the destination IP and MAC addresses in the request and in the answers?

4. Try now to emit a `ping` request from $A1$ to a non-existing machine that should belong to network A. Capture the emitted traffic on the second window of $A1$. What happens? Try now to emit a `ping` towards a non-existing machine that does not belong to $A1$'s network. Who sends the error message?

2 Address Resolution Protocol

You have noticed, in the previous exercise, that IP addresses in packets did not change from one end to the other end of the network (at least in the regular IP communication scenario), while the MAC addresses changed every time a router was crossed. IP addresses identify the true source and destination of data and MAC addresses are used to go from router to router. When a packet towards `A.B.C.D` arrives to a router, this router looks in its routing table to find the next router's IP address. It then encapsulates the IP packet into a new link layer frame, specifying the target router's MAC address and sends it on the link. It needs to determine the MAC address that corresponds to the router's IP address, which is the role of the ARP (*Address Resolution Protocol*) protocol. Note that ARP is not limited to a router's MAC address determination but it is used for all IP-Mac correspondences.

ARP catch some correspondences by looking at the received packets, but it essentially relies on a request-response mechanism. It maintains a table (called the ARP cache) that stores recent requests results.

1. Display the ARP cache of each machine using the `arp` command. The tables may be empty or not (depending on your last network activity). If they are not, you can remove entries using `arp -d`. You will note that, in this case, the table is not emptied but MAC addresses are considered invalid.

   The entries in this table expire after 3 minutes without any network activity. If you do not want to wait, you can crash, clean the temporary files and relaunch the lab.

@

2. From $A1$, send a single `ping` request to $A2$ (use `ping -c 1`). Display the ARP cache of $PC2$ and compare the displayed MAC address to the MAC address of `eth0` on $PC3$. Now display $PC3$'s ARP cache. What do you notice? Explain when each of these machines has learned the other one's addresses correspondence.

3. Try now, from $A2$ to ping $B1$. Look at the ARP cache of these two machines and the one of $R1$. Try to identify the entries that are relevant for this communication. Comment and explain the different entries.

4. Empty all the ARP caches by restarting the virtual network and avoid sending any network traffic before starting to capture the traffic. On router $R1$, start the capture with `tcpdump -e -t -i eth0`. Capture also the traffic on `eth0` interface of $A1$ and on `eth1` interface of $R1$.

5. From $B1$, send ping requests to $A1$. Identify the first ARP frames on the different machines (the one that happens before the first ICMP HELLO message). Represent graphically this exchange and explain the exchange.

6. Re-execute the `ping` command twice. Why isn't there any ARP exchange between these two requests?