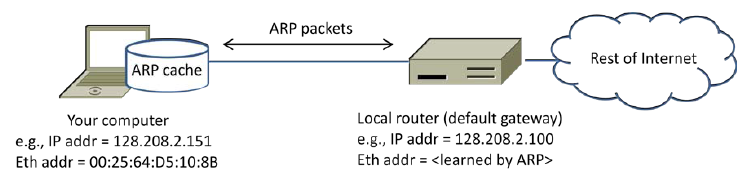
Lab Exercise – ARP

**Objective**

To see how ARP (Address Resolution Protocol) works. ARP is an essential glue protocol that is used to join Ethernet and IP. It is covered in §5.6.4 of your text. Review the text section before doing this lab.

**Network Setup**

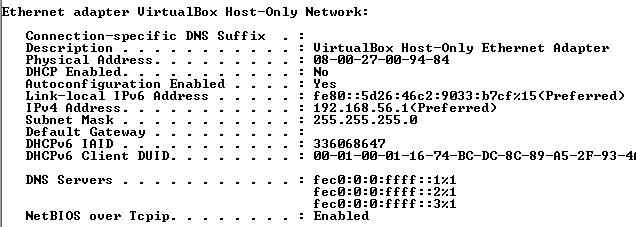
We want to observe the ARP protocol in action. Recall that ARP is used to find the Ethernet address that corresponds to a local IP address to which your computer wants to send a packet. A typical example of a local IP address is that of the local router or default gateway that connects your computer to the rest of the Internet. Your computer caches these translations in an ARP cache so that the ARP protocol need only be used occasionally to do the translation. The setup from the viewpoint of your computer is as shown in the example below.



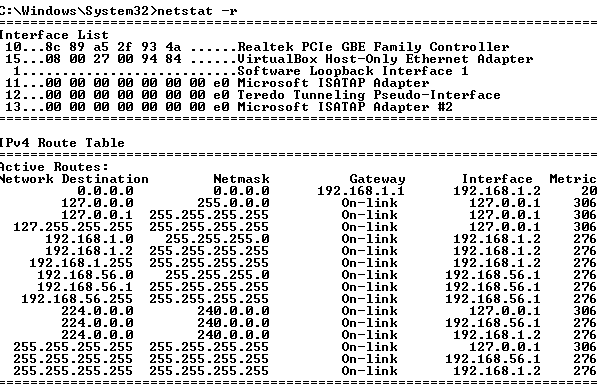
**Step 1: Capture a Trace**

*Proceed as follows to capture a trace of ARP traffic; alternatively, you may use a supplied trace.* To gath-er ARP packets, we will cause your computer to send traffic to the local router when it does not know the router’s Ethernet address – your computer will then use ARP to discover the Ethernet address.

1. *Find the Ethernet address of the main network interface of your computer with the* ifconfig / ipconfig *command*. You will want to know this address for later analysis. On Windows, bring up a command-line shell and type “ipconfig /all”. On Mac/Linux, bring up a command-line shell and type “ifconfig”. Among the output will be a section for the main interface of the computer (likely an Ethernet interface) and its Ethernet address. Common names for the in-terface are “eth0”, “en0”, or “Ethernet adapter”. Two examples are shown below, with our add-ed highlighting.



2. *Find the IP address of the local router or default gateway that your computer uses to reach the rest of the Internet using the* netstat */* route *command.* You should be able to use the netstat command (“netstat –r” on Windows, Mac and Linux, may require ctrl-C to stop). Alternatively, you can use the route command (“route print” on Windows, “route” on Linux, “route –n get default” on Mac). In either case you are looking for the gateway IP address that corresponds to the destination of default or 0.0.0.0. Two examples are shown be-low for netstat, with our added highlighting.



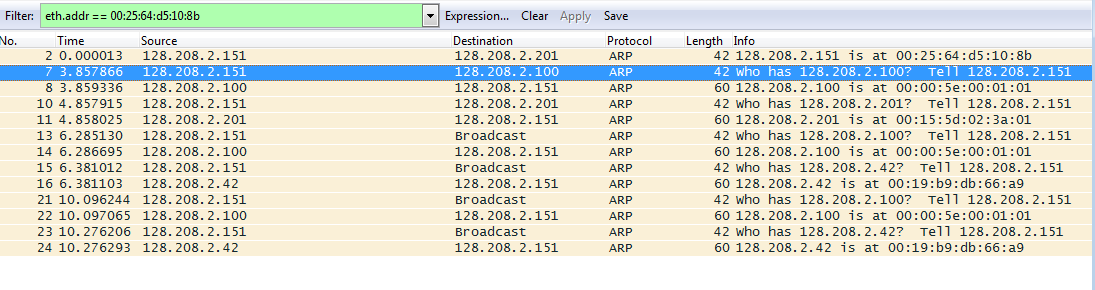
3. *Launch Wireshark and start a capture with a filter of* “arp”.

Since I am using the arp.pcap, I shall skip this step and 4-6.

**Step 2: Inspect the Trace**

Now we can look at an ARP exchange! Since there may be many ARP packets in your trace, we’ll first narrow our view to only the ARP packets that are sent directly from or to your computer.

*Set a display filter for packets with the Ethernet address of your computer.* You can do this by entering an expression in the blank “Filter:” box near the top of the Wireshark window and clicking “Apply”. The filter to enter depends on your Ethernet address. For example, if your Ethernet address is 01:02:03:04:05:06 then enter a filter expression of “eth.addr==01:02:03:04:05:06”. Note the double equal sign. If you are using the supplied trace, it comes with an additional text file giving the Ethernet address and default gateway IP address. After applying this filter your capture should look something like the figure below, in which we have expanded the ARP protocol details.

****

*Find and select an ARP request for the default gateway and examine its fields.* There are two kinds of ARP packets, a request and a reply, and we will look at each one in turn. The Info line for the request will start with “Who has …”. You want to look for one of these packets that asks for the MAC address of the default gateway, e.g., “Who has xx.xx.xx.xx …” where xx.xx.xx.xx is your default gateway. You can click on the + expander or icon for the Address Resolution Protocol block to view the fields:

* Hardware and Protocol type are set to constants that tell us the hardware is Ethernet and the protocol is IP. This matches the ARP translation from IP to Ethernet address.
* Hardware and Protocol size are set to 6 and 4, respectively. These are the sizes of Ethernet and IP addresses in bytes.
* The opcode field tells us that this is a request.
* Next come the four key fields, the sender MAC (Ethernet) and IP and the target MAC (Ethernet) and IP. These fields are filled in as much as possible. For a request, the sender knows their MAC and IP address and fills them in. The sender also knows the target IP address – it is the IP ad-dress for which an Ethernet address is wanted. But the sender does not know the target MAC address, so it does not fill it in.

*Next, select an ARP reply and examine its fields*. The reply will answer a request and have an Info line of the form “xx.xx.xx.xx is at yy:yy:yy:yy:yy:yy”:

* The Hardware and Protocol type and sizes are as set as before.
* The opcode field has a different value that tells us that this is a reply.
* Next come the four key fields, the sender MAC (Ethernet) and IP and the target MAC (Ethernet) and IP just as before. These fields are reversed from the corresponding request, since the old target is the new sender (and vice versa). The fields should now be all filled in since both com-puters have supplied their addresses.

**Step 3: ARP request and reply**

*To show your understanding of an ARP exchange, draw a figure that shows the ARP request and reply packets sent between your computer and the default gateway. Make it for the case we examined of your computer doing an ARP for the default gateway. Label one packet the request and the other the reply. Give the sender and target MAC and IP addresses for each packet; you can use Wireshark to inspect the packets to get these values. Finally, circle the sought after Ethernet address on your drawing to show where it comes from in the exchange.*

**Turn-in**: Hand in your drawing of the ARP exchange.

**Request**

*Sender IP address: (128.208.2.151)*

*Sender MAC address:* (00:25:64:d5:10:8b)

*Target IP address* (128.208.2.100)

*Target MAC address:*

*???*

*[128.208.2.100 (00:00:5e:00:01:01)]*

Target

Host

**Reply**

*Sender IP address: (128.208.2.100)*

*Sender MAC address:* (00:00:5e:00:01:01)

Target IP address: (128.208.2.151)

Target MAC address: (00:25:64:d5:10:8b)

**Step 4: Details of ARP over Ethernet**

*To look at further details of ARP, examine an ARP request and ARP reply to answer these questions:*

1. *What opcode is used to indicate a request? What about a reply?*

Opcode 1 indicates a request, opcode 2 indicates a reply

2. *How large is the ARP header for a request? What about for a reply?*

Both ARP request and ARP reply have a header of size 28 bytes.

3. *What value is carried on a request for the unknown target MAC address?*

The sender’s IP address.

ARP packets are carried in Ethernet frames, and the values of the Ethernet header fields are chosen to support ARP. For instance, you may wonder how an ARP request packet is delivered to the target com-puter so that it can reply and tell the requestor its MAC address. The answer is that the ARP request is (normally) broadcast at the Ethernet layer so that it is received by all computers on the local network including the target. Look specifically at the destination Ethernet address of a request: it is set to ff:ff:ff:ff:ff:ff, the broadcast address. So the target receives the request and recognizes that it is the intended recipient of the message; other computers that receive the request know that it is not meant for them. Only the target responds with a reply. However, anyone who receives an ARP packet can learn a mapping from it: the sender MAC and sender IP pair.

*Examine an ARP request and reply to answer these questions:*

4. *What Ethernet Type value which indicates that ARP is the higher layer protocol?*

5. *Is the ARP reply broadcast (like the ARP request) or not?*

I believe that it is the same in nature. It is a message sent to all in response to a previous message. If a computer isn’t the intended receiver, or expecting that kind of reply it just ignores it.

**Turn-in**: Hand in your answers to the above questions.