

CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-11
Wireshark Lab: Ethernet and ARP
April 2, 2025

Lab Instructions

- Mark your attendance in the attendance sheet before leaving the lab.
- Handle the lab resources with the utmost care.
- Please go through the following exercises in today's lab.
- It is recommended that you complete all the following exercises during the lab slot itself.
- If you face any difficulties, please feel free to seek help online or from your peers or TAs.
- After finishing all exercises, please carry your solutions with you (via email/pen drive) for future reference, and delete the files from the desktop.

Introduction

In this lab, we'll investigate the Ethernet protocol and the ARP protocol.

Part 0: Paste a screenshot of your system IP address, using ipconfig (on Windows) or ifconfig (on Mac and Linux), and fill out [this Google form](#) to submit the details of your system. The same system must be used to attempt all exercises of this lab.

Part-1: Capturing and analyzing Ethernet frames

Let's begin by capturing a set of Ethernet frames to study. To do this, of course, you'll need access to a wired Ethernet connection for your system.

Do the following:

1. First, make sure your browser's cache of previously downloaded documents is empty.
2. Start up Wireshark and enter the following URL into your browser:
`http://httpforever.com/`
3. Stop Wireshark packet capture.

Answer the following questions based on the Ethernet frame carrying the first HTTP GET request to the requested webpage:

1. What is the 48-bit Ethernet address of your computer?
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of `httpforever.com`? What device has this as its Ethernet address?
3. What is the hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET request? Which network-layer protocol does this correspond to?

4. What is the total size (in bytes) of the Ethernet frame encapsulating the HTTP GET request in Wireshark?
5. Is the Ethernet frame carrying the first HTTP GET request transmitted as a unicast, multicast, or broadcast frame? How can this be determined from the destination MAC address?

Answer the following questions based on the Ethernet frame carrying the first HTTP response from the requested webpage:

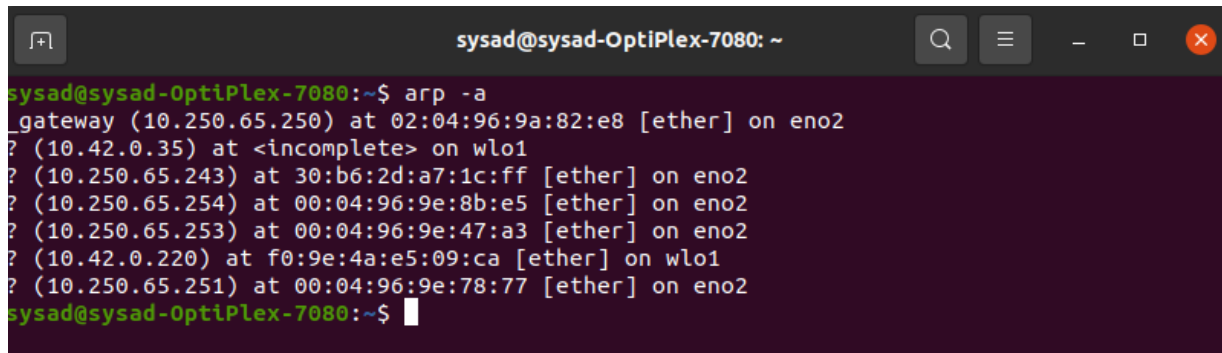
6. What is the value of the Ethernet source address? Is this the address of your computer, or `httpforever.com`? What device has this as its Ethernet address?
7. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” appear? After how many bytes in the HTTP does the “O” in “OK” appear?

Part-2: The Address Resolution Protocol

In this section, we’ll observe the ARP protocol in action.

Recall that the ARP protocol typically maintains a cache of IP-to-Ethernet address translation pairs on your computer. The *arp* command (in both DOS, MacOS and Linux) is used to view and manipulate the contents of this cache. Since the `arp` command and the ARP protocol have the same name, it’s understandably easy to confuse them. But keep in mind that they are different - the `arp` command is used to view and manipulate the ARP cache contents, while the ARP protocol defines the format and meaning of the messages sent and received, and defines the actions taken on ARP message transmission and receipt.

Let’s take a look at the contents of the ARP cache on your computer. In DOS, MacOS, and Linux, the “`arp -a`” command will display the contents of the ARP cache on your computer. So at the terminal, type “`arp -a`”. The results of entering this command are shown in the Figure below.

A terminal window titled 'sysad@sysad-OptiPlex-7080: ~' with a search icon, menu icon, and window control buttons. The terminal shows the command 'arp -a' and its output: 'gateway (10.250.65.250) at 02:04:96:9a:82:e8 [ether] on eno2', '? (10.42.0.35) at <incomplete> on wlo1', '? (10.250.65.243) at 30:b6:2d:a7:1c:ff [ether] on eno2', '? (10.250.65.254) at 00:04:96:9e:8b:e5 [ether] on eno2', '? (10.250.65.253) at 00:04:96:9e:47:a3 [ether] on eno2', '? (10.42.0.220) at f0:9e:4a:e5:09:ca [ether] on wlo1', and '? (10.250.65.251) at 00:04:96:9e:78:77 [ether] on eno2'. The prompt 'sysad@sysad-OptiPlex-7080:~\$' is visible at the bottom.

```
sysad@sysad-OptiPlex-7080:~$ arp -a
gateway (10.250.65.250) at 02:04:96:9a:82:e8 [ether] on eno2
? (10.42.0.35) at <incomplete> on wlo1
? (10.250.65.243) at 30:b6:2d:a7:1c:ff [ether] on eno2
? (10.250.65.254) at 00:04:96:9e:8b:e5 [ether] on eno2
? (10.250.65.253) at 00:04:96:9e:47:a3 [ether] on eno2
? (10.42.0.220) at f0:9e:4a:e5:09:ca [ether] on wlo1
? (10.250.65.251) at 00:04:96:9e:78:77 [ether] on eno2
sysad@sysad-OptiPlex-7080:~$
```

In order to observe your computer sending and receiving ARP messages, we'll need to clear the ARP cache, since otherwise your computer is likely to find a needed IP-Ethernet address translation pair in its cache and consequently not need to send out an ARP message.

Note: To delete the ARP cache on a Linux machine use the following command:

- `arp -a`: this lists all all the IP_Address.
- `sudo arp -d IP_Address`: You need to do this for all IPs in the above list.

Observing ARP in action

Answer the following questions based on the `ARP_Trace.pcapng`, which was captured on an interface with IP Address 10.0.0.1:

1. State the sender's MAC address.
2. Which target is the sender trying to connect to? Mention its IP and MAC addresses.
3. At what point does broadcasting occur in the ARP trace? Explain the reason for broadcasting.
4. List out all field values in the ARP request from the sender to the target.
5. List out all field values in the ARP reply from the target to the sender.
6. What are the differences between the ARP request and ARP reply field values?
7. Explain the presence of a Gratuitous ARP packet in the trace. What is its purpose?
8. What is the significance of the IP and MAC addresses in the Gratuitous ARP packet?
9. How many Gratuitous ARP packets are present in the trace corresponding to the sender's IP Address? Provide the packet number(s).
10. What is the sender and target MAC address in the Gratuitous ARP packet?

Submission Details

- Write your answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number, which contains all answers (with screenshots, if necessary).

