

Computer Networks – Practical session #1

Basics

Baptiste Jonglez
M1 MOSIG

February 2020

When booting the computers, choose “FreeBSD”, and then login with:
Username: “root”
Password: “root./”

1 Introduction

1.1 Objective

In this first practical session, you will learn how to use the fundamental tools of networking. You will also explore basic networking concepts such as packets, protocols, encapsulation, addressing, routing, and *packet capture*.

1.2 FreeBSD

The computers you will use are running FreeBSD. BSD was one of the first operating system to implement IP networking, so it is considered to be a reference in this field.

If you have already used Linux or Mac OS X, the command-line interface is quite similar with some subtle differences.

2 Network interfaces

A *network interface* is a physical device that allows your computer to connect to a network. Depending on the technology of the network it connects to, the interface can be wired (Ethernet, fiber) or wireless (Wi-Fi, Bluetooth, 3G, 4G). A computer can have several network interfaces.

Q 1 — *Do you think your mobile phone has network interfaces? If so, how many interfaces does it have? Are they wired or wireless interfaces? What is the network technology they connect to?*



Open a terminal and run the `ifconfig` command. It displays a list of all the network interfaces on your computer.


Q 2 — *How many network interfaces are there on your computer according to `ifconfig`? What are their names?*

Q 3 — *Do you think that every interface in this list corresponds to a physical device? Are they wired or wireless interfaces?*

Q 4 — *Which interface seems to be currently active and usable? How did you tell the difference between an active and an inactive network interface?*

An IP address is a number that logically identifies a computer on a network. There are two versions of IP in use today: IPv4, for which addresses are written with decimal numbers (for instance `198.51.100.42`); and IPv6, where addresses are longer and written in hexadecimal (for instance `2001:db8:42:face:1234:abcd:696:cdcd`).


Q 5 — *Give all IP addresses that are configured on your computer according to `ifconfig`. How can your computer have several IP addresses?*

 Compare the IP addresses of your computer with your neighbour's computer.

Q 6 — *Are the IP addresses on your computer unique? For which interface? What can you deduce about these interfaces? Are they connected to the same network as your neighbour's computer?*


3 Testing connectivity

We will use the `ping` command to test connectivity to remote hosts. The mechanism used by `ping` is very simple: a request is sent to the remote host, who immediately sends a reply back to the sender.

 Try to `ping` the IP address of your neighbour. After a few seconds, use `Ctrl-c` to stop the command.

Q 7 — *What information does the `ping` command output? Give the minimum and average delay reported by `ping` and interpret its value.*

Q 8 — *How does `ping` measure the delay it reports? Explain the algorithm.*

 Try to `ping` two other hosts, `universiteparis2019.fr` and `www.columbia.edu`. Notice that `ping` translates the names into IP addresses.


Q 9 — *What are the average delays for these two hosts? How do you interpret the difference in delay compared to your neighbour's IP address?*

Q 10 — *Assuming that the delay you measured is only caused by the propagation time in a fiber, what is the approximate length of fiber between you and each of the three hosts you tried to `ping`? (The speed of light in a fiber is $2 \cdot 10^8 \text{ m} \cdot \text{s}^{-1}$). Does the result seem consistent with the probable geographical location of the hosts?*

4 Packet capture with Wireshark

Wireshark is a graphical tool that allows to capture packets from a network and analyze them. You may find Wireshark in the graphical menus. Otherwise, the most reliable way to launch Wireshark is to enter `wireshark` or `wireshark-gtk` in a terminal.

 Launch wireshark.


 Start a packet capture on the network interface connected to the school network. Then open your web browser and load a few web pages.


To start the capture, select “Interface List” in the main view (or click on the associated button in the toolbar near the top). You can then select one or more interfaces and start the capture.

You should have already determined which network interface is connected to the school network. If it is not the case, simply look at the packet counters: they should be increasing, since some network traffic is exchanged. The interface is usually named `igb0` or `em0`.

Q 11 — *During a packet capture, what does each line in the interface of Wireshark represent?*

Q 12 — *Which protocols can you see? Do you recognize the name of some protocols from the course? If so, which ones?*


 Use the “filter” box to only display DNS packets.

 Click on a DNS packet. Examine wireshark’s analysis of this packet (visible below the main table).

Q 13 — *According to wireshark, which protocols (in addition to DNS) are contained in this packet?*

Q 14 — *What is the total size of the packet? For each protocol except DNS, determine the size of the header and the size of the payload as seen by this protocol.*

Q 15 — *Draw a representation of the packet that shows the different layers of protocols in the packet. The name of each protocol should be clearly visible with the size of its header, as well as the size of the final payload.*

 Clear the display filter. While the packet capture is still running, `ping` the host `delos.imag.fr` for a few seconds. Then stop the packet capture to avoid filling up the memory of your computer.

Q 16 — *Looking at the packet capture, what is the name of the protocol used by `ping`? On top of which protocol does it run?*

Q 17 — *What are the source and destination addresses of the packet at the IP layer?*

Q 18 — *What are the values of the “Type” and “Code” field in the ICMP header? Can*

you guess the meaning of these fields?


Q 19 — Compare the request sent by `ping` and the reply sent by the remote host: which ICMP field has changed between these two packets?

Q 20 — Using Wireshark, compute the delay between a request and a reply and compare it with the delay reported by `ping`.

5 Understanding ARP


We will now look at the ARP protocol.

5.1 ARP table

 Clear the ARP table on your computer, using `arp -d -a`.

 Start a packet capture in Wireshark, and `ping` your neighbour's computer.

Q 21 — What ARP packets do you see in the capture? Do they occur before or after the packets generated by `ping`?

 While the packet capture is still running, stop the previous `ping`, wait several seconds, and `ping` the same computer again.

Q 22 — Do you see new ARP exchanges in the capture? Why?

It is possible to see the ARP table of the local computer by running:


```
# arp -n -a
```

Q 23 — Explain the notion of an “ARP table” and why it can also be called an “ARP cache”.

5.2 Local and remote networks

Q 24 — Analyze the previous packet capture: what is the Ethernet address of your neighbour's computer? Explain two different methods to obtain this address.

Q 25 — Similarly, find the Ethernet address of a third computer in the room: is it different from your neighbour's computer Ethernet address?

 Start a new packet capture and `ping universiteparis2019.fr`. Locate a query packet in the capture.

Q 26 — What is the destination Ethernet address of the query packet?

☞ Now ping `www.columbia.edu` instead, and locate again the corresponding query packet in the capture.

Q 27 — *What is the destination Ethernet address of the query packet? What do you notice? Is it different? Explain.*

☞ Display the routing table of your computer using `netstat -rn -f inet`

Q 28 — *Using this routing table, how can you explain the results you obtained in the four last questions?*

6 Traceroute

☞ Run the `traceroute` command towards several servers, for instance Columbia's web server.

Q 29 — *What does the output of `traceroute` show?*

Q 30 — *Considering again the `traceroute` towards `www.columbia.edu`, can you tell where your `traceroute` goes through a transatlantic fiber cable? That is, between which routers?*

Q 31 — *Using packet capture, explain how `traceroute` works: which packets it sends, which packets it receives in response and why, how it determines each hop, and how it measures latency. Beware, this is a difficult question!*

Q 32 — *Run `traceroute` towards `www.jami.net`. What happens beyond the 15th hop (or so)? Find a way to make `traceroute` work correctly in this case by changing its behaviour (using an option described in `man traceroute`).*