Name 1: Yoann Ponti
Name 2: Tristan Overney

COM-407: TCP/IP NETWORKING

LAB EXERCISES (TP) 0
BASIC CONFIGURATION AND IP SUITE:
PING(6), TRACEROUTE(6), NETSTAT, NSLOOKUP

September 22, 2015

Abstract

In this lab you will practice some networking commands that enable you to obtain information about Internet machines and about the connectivity and the paths between them.

1 ORGANIZATION OF THE TP AND USEFUL COMMANDS

1.1 TP REPORT

Type your answers in this document. We recommend you use Adobe Reader XI to open this PDF, as other readers (such as SumatraPDF, but also older versions of Adobe!) don't support saving HTML forms. That will be your TP report (one per group). When you finish, save the report and upload it on moodle. Don't forget to write your names on the first page of the report. **See on Moodle for the deadline.**

1.2 WIRESHARK

You will be using Wireshark to sniff packets. Since there are a lot of packets generated by the applications running on your machine, you may want to use filters. `http://wiki.wireshark.org/DisplayFilters`

2 THE IPV4 INTERNET

Connect to the Internet in IPv4 and disable any IPv6 connectivity. Then, in order to determine the following information:

- the IP address(es) of your machine `<my_ip>`,
- the netmask `<my_netmask>`, and
- the default gateway of your machine `<my_gateway>`.

In MacOS use

```
# ifconfig
# netstat -nr
```

In Linux use

```
# ifconfig
# route -n
```

or in Windows

```
> ipconfig /all
```

Q1/ List your findings here:

[A1.a] `<my_ip>=` 128.179.159.221
[A1.b] `<my_netmask>=` 0xfffff800
[A1.c] `<my_gateway>=` 128.179.152.1

Q2/ Is your IP address public or private? What does the netmask in IPv4 (or the prefix in IPv6) mean?

[A2] The address is public, indeed we can verify this by going to a webservice such as whatismyipaddress.com. This service return us the same ip address as the one seen using ifconfig. The netmask is used to differentiate between the network identifier and host identifier

Now, download Wireshark and install it on your computer. Start it (as administrator) and use the menu `Capture->Interfaces` to start capturing packets on the interface that you use for Internet connectivity.

Q3/ Do you see any packet captured with destination IP address of your default gateway?

[A3] No, the gateaway is an intermediary device and we shouldn't see any packets sent to it.

2.1 PING

PONG

The ping command uses the ICMP protocol to probe whether a host is up:

```
# ping <hostname>
```

Q4/ Start a new capture with Wireshark and then ping `www.facebook.com`. Observe the traffic generated by the ping command. Do you see only ICMP packets?. Stop the ping program and start it again after a couple of seconds. Is there a difference from the first captured packets? Explain.

[A4] No, the first run of the ping command also generate DNS traffic. Indeed, it first needs to " translate" www.facbook.com to an ip. Then ICMP traffic can be seen between our host and a server from facebook. At the second run, the DNS traffic is not seen, the ip address must have

Q5/ In a browser open `www.swisscom.ch`. Next, try pinging it. Explain.

[A5] The server doesn't respond to ping. It must have a router that drops the ICMP traffic meaning that is has disabled the ICMP echo replies.

2.2 TRACEROUTE AND NETSTAT

traceroute is a tool for displaying the route to a destination.

In MacOS and Linux:

```
# traceroute www.facebook.com
```

In Windows:

```
> tracert www.facebook.com
```

Q6/ Do you see more than one name/IP address at any of the hops? If so, why?

[A6] Yes, the 8th hop have 3 ips.
The 7th router has multiple routes toward the destination. Because traceroute don't rely on a single packet, each of them might take a different route. Which in turn will return us a different ip for the 8th router.

netstat is a tool for displaying TCP connections, routing table, interfaces and network statistics. Open a web browser, go to `lca.epfl.ch`, and leave the browser open for the moment.

Look at the active TCP connections.

```
# netstat -t -n
```

The `-n` switch prevents name resolving and makes netstat display results faster (but obviously without the names of the hosts).

Q7/ Identify the TCP connections opened by visiting the `lca.epfl.ch` webpage. Write them down and describe them here. Is there one, or are there several such connections? Why?

[A7]
```
tcp4       0      0  128.179.144.62.49253   104.16.22.35.80        ESTABLISHED
tcp4       0      0  128.179.144.62.49252   23.51.123.27.80        ESTABLISHED
tcp4       0      0  128.179.144.62.49251   52.49.139.252.443      ESTABLISHED
tcp4       0      0  128.179.144.62.49250   52.49.139.252.80       ESTABLISHED
tcp4       0      0  128.179.144.62.49249   128.178.50.12.80       ESTABLISHED
tcp4       0      0  128.179.144.62.49248   128.178.156.24.80      ESTABLISHED
tcp4       0      0  128.179.144.62.49247   128.178.156.24.80      ESTABLISHED
tcp4       0      0  127.0.0.1.6263         127.0.0.1.49246        ESTABLISHED
tcp4       0      0  127.0.0.1.49246        127.0.0.1.6263         ESTABLISHED
tcp4       0      0  128.179.144.62.49244   52.89.80.240.443       ESTABLISHED
```

3 NAMES IN THE INTERNET

Juliet: [...]
What's in a name? That which we call a rose
By any other name would smell as sweet.

W.S.

Replace your DNS servers by an inexisting IP address, say `1.2.3.4`. If you configured statically your DNS servers, don't forget to write them down somewhere.

Go to the `Properties` of your Internet connection. Click on Internet Protocol Version 4, `Properties`, choose `Use the following DNS server addresses`, and write `1.2.3.4`

Use the manual configuration in the network settings and set the DNS address to `1.2.3.4`

Switch to root mode using `su` and edit the `/etc/resolv.conf` file. Comment out the lines that begin with `nameserver` (precede them with the `#` character) and add one line `nameserver 1.2.3.4`

Q8/ Try pinging Facebook and observe the traffic with Wireshark. What happens?

Ping return us an error message: cannot resole www.facebook.com: Unknow host.
A DNS query to the server 1.2.3.4 is sent. Of course, without any reply. Because of this absence of a reply, the ping return us the error message.

[A8]

Q9/ Try pinging the IP address of Facebook that you discovered in Sections 2.1 and 2.2. Does it work?

Yes, it works because no dns resolution is needed.

[A9]

nslookup is a command-line tool for querying Domain Name System (DNS) name servers. Run `nslookup` with the address of the Google public DNS server.

```
# nslookup - 8.8.8.8
```

Q10/ In the > prompt, type `lca.epfl.ch`. Give the IPv4 and IPv6 addresses of `lca.epfl.ch`. Use `set type=A` for IPv4 or `set type=AAAA` for IPv6

IPv4 address: 128.178.156.24
IPv6 address: 2001:620:618:19c:1:80b2:9c18:1

[A10]

Q11/ Do you recognize the IPv4 address in the IPv6 address, or vice-versa?

128.178.156.24 in hexadecimal is 80.B2.9C.18.
The IPv6 addresse hold embedded the IPv4 address. (80b2:9c18)

[A11]

Restore now your initial DNS configuration.

Start a capture in `wireshark` and do a traceroute in IPv4 to `www.facebook.com`. Focus on the line:

```
swiel2 (192.33.209.33)  1.219 ms  0.968 ms  0.944 ms
```

Q12/ Look at the capture and identify the packet in which you see the name `swiel2`. How does this differ from the usual DNS response observed in previous questions? Based on the observed difference, comment on how `traceroute` works.

The DNS query issued is a reverse dns query. Indeed, it uses the domain suffix .in-addr.arpa.
It enable the traduction of an IPv4 address to a domain name.

[A12]

Q13/ Analyze the capture and comment on how `traceroute` find successive hops.

The traceroute command sends packets into the network and rely on the TTL field to map the path. Each time a packet goes through a router in direction of the destination the TTL value is deacresed by one. Once the value reach 0 the router drop the packet and send back a ICMP error message back to the host. This enable the host to get it's ip. Then to retrieve the name, a reverse DNS query is done.

[A13]

4 THE IPV6 INTERNET

Now let's examine the situation when only IPv6 connectivity is present.

Find an access to an IPv6 network and disable IPv4 on your machine. IPv6 access is provided in INF019 via a wireless access point, or on the PCs in the room via a wired connection.

Use wireshark to observe the traffic. On your computer type

```
# ping6 www.facebook.com
```

Q14/ Describe some differences in the observed traffic compared to the IPv4 case. Write the average RTT you get and compare it with the IPv4 case. Explain the differences if any.

[A14] Difference can be seen in the packet captured by wireshark. Indeed they differe in their length and protocol used. The RTT is around 23ms for both IPv4 and IPv6 even though in the case of IPv6 we have some ping with a RTT of more than 100ms. This comes probably from the fact that IPv6 packets takes different paths than IPv4 packets or that during the two experiments the congestion did change.

Repeat the test with the `traceroute` command from Section 2. Use:

In Linux or MacOS:

```
# traceroute6 www.facebook.com
```

In Windows:

```
> tracert -6 www.facebook.com
```

Q15/ Write the result. Does the path to Facebook in the IPv6 Internet cross the same routers as in IPv4?

[A15] IPv6:
traceroute6 to star-mini.c10r.facebook.com (2a03:2880:f11b:83:face:b00c::25de) from 2002:80b2:9c51::ffff:1df, 64 hops max, 12 byte packets
1 2002:80b2:9c51::cccc:1 12.354 ms 15.409 ms 1.046 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 po4.msw1ad.01.ams3.tfbnw.net 2485.309 ms 1015.455 ms
po4.msw1ab.01.ams3.tfbnw.net 1018.516 ms
11 edge-star-mini6-shv-01-ams3.facebook.com 1014.328 ms 1063.317 ms 1092.630 ms

Now, open the web browser (new window), go to `lca.epfl.ch`.

Q16/ Do you notice a difference between two versions of `lca.epfl.ch` pages? Can you imagine by which mechanism such a difference may occur ?
Hint: Which device (default gateway, intermediate routers, the web server, etc) do you think is in charge of displaying the web content for IPv4 if you are connected to an IPV4 network or for IPv6 otherwise?

[A16] A green lock at the bootom of the page which is not present in the version loaded using IPv4. Also the "route widgets" is not loaded. The widgets must be served from a IPv4 only server. Now for the lock, the server knows from which network the request arrives. It is then just a question of running a script or serving a different version of the HTML. The others systems

Look at the active connections.

```
# netstat -t -n
```

Q17/ Compare the output that is related to `lca.epfl.ch` with the one that you wrote down for IPv4. Comment about it

[A17] As before there is a certain amount of tcp connection. But now instead of ipv4 addresses they are ipv6 addresses. Some addresse are not present such as the one serving the route widgets because is not IPv6 compatible.

Q18/ Try pinging `www.swisscom.ch` again. Did it work? Explain.

[A18] It now works which means that IPv4 and IP6 configurations are different on the interface serving swisscom.ch website.

5 IPv4 AND IPv6

Let's see what happens when both IPv4 and IPv6 Internet connectivities are present. Stay connected in IPv6, but enable IPv4.
From your computer do a traceroute in IPv4 and IPv6 to `www.switch.ch`

Q19/ Does it work in both cases?. Write down any difference in the traceroutes

Traceroute works in both case but no intermediary routers did respond in the IPv6 case. We can see a difference in the number of hops, 6 for IPv4 and 10 for IPv6.

[A19]

Now, start a new `Wireshark` capture, open a browser and type `www.switch.ch`.

Q20/ Check the capture in Wireshark, your connection to the webpage is done in IPv4 or in IPv6?

The connection is done using IPv4. But we obtain two DNS reply to the DNS query. Indeed we receive one for the IPv4 address and one for the IPv6

[A20]

Q21/ Explain how do you think your machine could decide whether it uses IPv4 or IPv6.

Based on DNS for example. If there is a AAAA record and A record, we could first try to connect using IPv6. If only a A record is present, directly connect using IPv4.

[A21]