Name 1:
Name 2:

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>`=
  [A1.b] `<my_netmask>`=
  [A1.c] `<my_gateway>`=

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

[A2]

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]

2.1 PING

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]

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

[A5]

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
```

3

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

[A6]

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]

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?

[A8]

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

[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

[A10]

5

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

[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:

```
swie12 (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 `swie12`. How does this differ from the usual DNS response observed in previous questions? Based on the observed difference, comment on how `traceroute` works.

[A12]

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

[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]

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]

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]

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]

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

[A18]

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

[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?

[A20]

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

[A21]