Name 1:	FURKAN KARAKAS
Name 2:	ONUR VEYISOGLU

COM-407: TCP/IP NETWORKING

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

September 18, 2019
Deadline: September 25, 2019 at 23.55 PM

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. You will also learn to use a GUI-based packet capture/inspection tool called Wireshark. Optionally, in research exercises, you will use tshark (command-line version of Wireshark) for packet capture/inspection.

1 ORGANIZATION OF THE 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.

2 The IPv4 Internet And Network Packet Inspection

2.1 Ifconfig

Connect to the Internet in IPv4 and disable IPv6 connectivity, if needed.

To disable IPv6:

On MacOSX, you can execute the following command from the *Terminal* app

```
# networksetup -setv6off "InterfaceName"
```

If you do not know the InterfaceName, you can use the following command

```
# networksetup -listallnetworkservices
```

On Red Hat-based Linux, following commands can be used from the *Terminal* app

```
# sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1
# sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1
```

On Debian-based Linux, add the following in `/etc/sysctl.conf` file and reboot the machine.

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

On Windows, Click Start, and then click Control Panel. Click Network and Sharing Center. In the View your active networks area, click Local Area Connection, and then click Properties. On the Networking tab, clear the Internet Protocol Version 6 (TCP/IPv6) check box, and then click OK.

After disabling the IPv6 connectivity, we now want 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 following commands in *Terminal* app

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

In Linux use following commands in *Terminal* app

```
# ip addr show
# ip route show
```

or in Windows use following commands in *powershell* app

```
> ipconfig /all
```

Q1/ List your findings here:

[A1.a] <my_ip>= 128.179.185.26
[A1.b] <my_netmask>= 255.255.248.0
[A1.c] <my_gateway>= 128.179.184.1

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

[A2] It is public since it is not in the range of private IPs reserved by IANA. It is a mask that is consisting of 32 bits and used for dividing your net into subnets and it shows all available host addresses in that network. In this case, the binary representation of 248 is 11111000, and the

2.2 Network packet inspection. Wireshark

We need to see or inspect the packets leaving or coming to our computer or other computers for various reasons. These reasons vary depending on the person and his motivations. For example, network administrators need this for troubleshooting network-related problems, software developers for debugging network-related code and network protocol implementations, and security engineers for analyzing the network traffic for security purposes. In general, we all can use these tools to understand how machines actually communicate with each other, i.e., to understand the internals of the network protocols.

There exists many tools for network packet inspection. Under the hood, all these tools use packet capture libraries such as libpcap, winpcap or npcap but they differ in the way users can interface with them and the features they provide. For example, Wireshark is a powerful sniffer which can decode lot of protocols. It provides a nice GUI for make usage more user friendly.

Since there are a lot of packets generated by the applications running on your machine, you may want to use filters, for more details see
`http://wiki.wireshark.org/DisplayFilters`. Please note that there are two types of filters: *capture* and *display*. Capture filters are used to selectively capture the traffic whereas with display filters, you capture all the traffic but the traffic is displayed as per the filter rules.

Now, download Wireshark and install it on your computer. (Note that, if you are using Windows, it will require to install npcap library. While installation process, you do not need to install the npcap loopback adapter). Start it (as administrator) and use the menu `Capture->Interfaces` to start capturing packets on the interface that you are currently using for the Internet connectivity.

Q3/ Write a command that filters only the packets with destination IP address of your default gateway. Do you see any packet captured if you navigate to a webpage through your browser? If yes/no, explain the reason behind your observation?

[A3] We utilized the following filter for this question: ip.dst == 128.179.184.1 . However, we do not observe any traffic when we navigate to a webpage because communication between gateway and our computer happens in MAC layer

2.3 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`. Which exchanges of messages is happening after first ping command according to the theory? Now find these messages in the Wireshark output. 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?

[A4] In theory, first a request to DNS server should be made to extract the ip address of the destination host. After getting the ip address of the destination, source computer sends ICMP packet. If the host is up and does not block ICMP packets, we expect to get a response with ICMP protocol. If the destination host is blocking ICMP packets or it is down or does not exist, we expect to get a request time out error since our packets does not reach to the destination.

Q5/ In a browser open `www.swisscom.ch`. Next, try pinging it. Does it work? Explain the result.

[A5] In browser we observed that the host is reachable since our browser successfully displayed the webpage hosted by the destination host. However, when we pinged the destination host, we did not get any response. Reason is that the destination host blocked the ICMP packets.

Q6/ Ping `www.canterbury.ac.nz` and `www.newzealand.com`. What are Round-trip times (RTTs) for each ping? Based on your observation, can you identify which server can be located in New Zealand?

[A6] For the canterbury.ac.nz, RTT is 357ms in average, which is probably far away from Europe. On the other hand, for the www.newzealand.com RTT is 33ms in average. This indicates even if the domain name looks like it is hosted somewhere in New Zealand, actually it is hosted somewhere near Switzerland. We checked from geoiplookup.net and verified that it is hosted in Germany and the first one is hosted in New Zealand.

2.4 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
```

Q7/ Start Wireshark and do `traceroute` to `www.facebook.com`. How did you filter the packets that are coming from your machine during `traceroute`? Which OS (Linux, MacOSX, or Windows) are you running? Does your system uses ICMP, TCP or UDP protocol for `traceroute`? Write down the result of the traceroute.

[A7] At first we did not use any filter to observe the traffic. Then we realized that traceroute in our computer utilizes ICMP and UDP protocols. So we used the filter : dns or icmp in wireshark.

We use Windows 10 OS. Following output is our result:

```
Tracing route to facebook.com [31.13.64.35]
over a maximum of 30 hops:
```

netstat is a tool for displaying TCP connections, routing table, interfaces and network statistics. On Linux, netstat (part of net-tools) is superseded by **ss** (part of iproute2).

Open a web browser, go to `www.epfl.ch`, and leave the browser open for the moment.

Look at the active TCP connections.

In MacOS and Windows:

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

In Linux:

```
# ss -t -n
```

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

Q8/ Identify the TCP connections where destination IP address is IP address of `www.epfl.ch` webpage. Is there one, or are there several such connections?

We used the following command:

```
sudo ss -t -n | grep 104.20.229.42
```

where the given IP address is the IP address of the EPFL server. The output is:

```
ESTAB  0        0            128.179.132.5:44284        104.20.229.42:443
```

Yes, there is only one connection with that given IP address.

[A8]

2.5 MAC addresses

A MAC address (media access control address) of a device is a unique identifier assigned to a network interface controller (NIC). MAC addresses are linked to the hardware of network adapters. A MAC address is given to a network adapter when it is manufactured. It is hardwired or hard-coded onto your computer's network interface card (NIC) and is unique to it.

Q9/ What is the MAC address of your wireless interface? How can you find a MAC address of your default gateway?

From ifconfig, we see that the MAC address of our wireless interface is:
54:27:1e:5c:d0:12
We can find the MAC address of our default gateway by using arp command. ARP stands for " Address Resolution Protocol".
sudo arp -n gives:

```
128.179.128.1            ether   00:08:e3:ff:fc:04   C                    wlp2s0
```

[A9]

Q10/ Are your and your lab partner's machines in the same subnet? Can you find a MAC address of your lab partner's machine from your machine? How?

We opened a hotspot and we connected to the same network. While we are in the same network, I used arp -n command and I see that my partner's MAC address is c0:b5:d7:df:04:d7. But before, when we were connected to EPFL access point, we were not in the same network since our default gateway IP addresses were different.

[A10]

Q11/ Ping `www.facebook.com`. What is the MAC address of the packet received from facebook while pinging? Is this the MAC address of the facebook server?

[A11] The IP packets do not contain any information about the MAC address of the destination host, because remote server and our computer are in different Local Area Networks. We can observe the MAC address only inside the same network.

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 before changing them to `1.2.3.4`.

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`

Q12/ Try pinging Facebook and observe the traffic with Wireshark. What happens?

[A12] Our computer tries to resolve the domain name of facebook.com, but it does not get any answer, because it is asking to a non-existing DNS server. We see "destination unreachable" in Wireshark for ICMP packets.

Q13/ Try pinging the IP address of Facebook that you discovered in Sections 2.3 and 2.4. Does it work?

[A13] Yes, this time it worked. Since we provided the IP address, it did not need to resolve any domain name.

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
```

Q14/ 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

[A14] IPv4 address is: 128.179.33.39
IPv6 address is: 2001:620:618:521:1:80b3:2127:1

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
```

Q15/ Filter the DNS packets in Wireshark. 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.

[A15] The usual DNS queries during pinging is asking for the type A (IPv4) record to resolve the name of the domain. However, in traceroute, it asks for type PTR record to perform a reverse DNS operation, i.e., it gives the IP address of the domain, detected by the ICMP packets with specific TTL values, and then it asks for the name of the domain. We observed that some DNS records do not contain PTR records, and for those particular DNS records, we did not see any

4 The IPv6 Internet

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

Find access to an IPv6 network and **disable IPv4 on your machine**.

To disable IPv4:

On MacOSX, you can execute the following command from the *Terminal* app

```
# networksetup -setv4off "InterfaceName"
```

You can also turn an interface off without using *Terminal* app. Go to System Preferences and then click on Network. Next, click on the interface you want to change its configuration. Then, select Advanced button. In the new window, go to tab TCP/IP. Now, in the configuration of IPv4, you can turn off IPv4 or select Using DHCP for automatic IPv4 assignment.

On Red Hat-based Linux, following commands can be used from the *Terminal* app

```
# sudo sysctl -w net.ipv4.conf.all.disable_ipv4=1
# sudo sysctl -w net.ipv4.conf.default.disable_ipv4=1
```

On Debian-based Linux, add the following in `/etc/sysctl.conf` file and reboot the machine.

```
net.ipv4.conf.all.disable_ipv4 = 1
net.ipv4.conf.default.disable_ipv4 = 1
net.ipv4.conf.lo.disable_ipv4 = 1
```

On Windows, Click Start, and then click Control Panel. Click Network and Sharing Center. In the View your active networks area, click Local Area Connection, and then click Properties. On the Networking tab, clear the Internet Protocol Version 4 (TCP/IPv4) check box, and then click OK.

If IPv6 networking is disabled (which might be the case if you used the same interface as for second section of the TP), enable it before accessing an IPv6 network.

To re-enable IPv6 for a network interface (if not already enabled):

On MacOSX, you can execute the following command from the *Terminal* app

```
# networksetup -setv6automatic "InterfaceName"
```

On Red Hat-based Linux, following commands can be used from the *Terminal* app

```
# sudo sysctl -w net.ipv6.conf.all.disable_ipv6=0
# sudo sysctl -w net.ipv6.conf.default.disable_ipv6=0
```

On Debian-based Linux, remove the lines you added in `/etc/sysctl.conf` file while disabling IPv6 connectivity and reboot the machine.

On Windows, Click Start, and then click Control Panel. Click Network and Sharing Center. In the View your active networks area, click Local Area Connection, and then click Properties. On the Networking tab, mark the Internet Protocol Version 6 (TCP/IPv4) check box, and then click OK.

IPv6 access is provided in or around INF019 room via a wireless access point (`SSID: lca2-tcpip-labs`, the password is announced on Moodle).

Use wireshark to observe the traffic. On your computer type

```
# ping www.facebook.com
```

Note that if it is not pinging with IPv6 by default, instead of `ping` command, you should use `ping6` on MacOSX and `ping -6` on Windows.

Q16/ 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.

[A16] There are usual ICMPv6 packets, which we send and receive. But additionally, we see Neighbor Solicitation, Neighbor Advertisement, Multicast Listener Report Messave v2, and Router Advertisement packets also with the ICMPv6 protocol. The IPv6 address sizeis 128 bits whereas the IPv4 address size is 32 bits. Echo ping request type 8 is used in IPv4 whereas Echo ping request type 128 is used in the IPv6. The average RTT we get is 18.963

Repeat the test with the `traceroute` command from Section 2.4. Use:

In Linux or MacOS:

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

Note that if the `traceroute` command is not done by default with IPv6, you should use `traceroute6` command.

In Windows:

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

Note that if the `tracert` command is not done by default with IPv6, you should use `tracert -6` command.

Q17/ Write the result. Does the path to Facebook in the IPv6 Internet cross the same routers as in IPv4?

[A17]

```
traceroute to star-mini.c10r.facebook.com (2a03:2880:f127:283:face:b00c:0:25de) from 2001:
470:26:40b::ffff:8, 30 hops max, 24 byte packets
 1  2001:470:26:40b::bbbb:1 (2001:470:26:40b::bbbb:1)  14,25 ms  7,885 ms  36,604 ms
 2  tunnel496810.tunnel.tserv23.zrh1.ipv6.he.net (2001:470:25:40b::1)  39,026 ms  43,471 ms
7,679 ms
 3  10ge2-16.core1.zrh3.he.net (2001:470:0:11d::1)  80,081 ms  16,51 ms  10,438 ms
 4  100ge8-1.core1.zrh2.he.net (2001:470:0:3fc::1)  18,57 ms  6,158 ms  6,094 ms
 5  100ge12-2.core1.par2.he.net (2001:470:0:3ff::2)  20,279 ms  21,386 ms  19,814 ms
 6  100ge14-1.core1.nyc4.he.net (2001:470:0:33b::1)  89,972 ms  90,353 ms  90,867 ms
 7  100ge4-1.core2.chi1.he.net (2001:470:0:270::2)  113,426 ms  111,008 ms  111,538 ms
 8  equinix.br01.ord1.tfbnw.net (2001:504:0:4:0:3:2934:1)  114,527 ms  114,051 ms  121,792
ms
 9  po131.asw01.ord3.tfbnw.net (2620:0:1cff:dead:beef::16c2)  161,945 ms  138,523 ms
110,357 ms
```

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

Q18/ 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?

[A18] Web server is responsible for displaying HTML pages. We observed that an iframe embedded in the HTML page of lca.epfl.ch website accepts only IPv4 connection. When we tried to access it with IPv6 connection, we would get an error. The name is the site is: widget.routerank.com

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.

Yes, both cases work fine. In traceroute6, we have fewer nodes than the nodes in traceroute. In traceroute6, the packets are of size 24 byte, whereas in traceroute, the packets are of syze 60 byte.

[A19]

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

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

It is done in IPv6.

[A20]

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

It does a DNS lookup for both IPv4 and IPv6 addresses, denoted by A and AAAA. If only one of them is present, then the machine continues that way. If both are present, then the machine prefers IPv6 to IPv4, and the communication continues in IPv6 protocol.

[A21]

Research Exercises (Optional)

6 Wireshark vs tshark

You already have experience of Wireshark usage (2.2). There also exists a command line version of wireshark, called tshark. Depending on one's needs, abilities, and familiarity, one may sometimes find tshark more handy than wireshark or vice-versa. In the research exercise you will compare tshark and wireshark and see in which cases one tool is better than the other.

In the next section, we introduce you with tshark.

6.1 tshark

tshark lets you capture packet data from a live network, or read packets from a previously saved capture file. The captured packets are decoded by tshark and then, can either be printed to the standard output or written to a file. tshark's native capture file format is pcap format, which is also the format used by wireshark and tcpdump.

6.1.1 A short tutorial on tshark

To capture all the traffic passing through a certain interface and save it in `captured_packets.pcap` file, the following command can be used.
On Windows:
1. In powershell navigate to the folder where Wireshark installed using `cd` command
2. Run the following command

```
#./tshark.exe -i interface_name -w captured_packets.pcap
```

On Linux/Mac

```
# tshark -i interface_name -w captured_packets.pcap
```

where `-i` should be followed by the name of the interface and `-w` with the name of the file for captured data. In order to get the names of interfaces you can use the `-D` option:

```
# tshark -D
```

Now, using a web browser, visit few web pages like facebook.com or cnn.com. Once you're done, stop the packet capture by pressing Ctrl + C.

To read the packets captured in `captured_packets.pcap` file, use the `-r` option. Following should read all the packets captured in the `captured_packets.pcap` file:

```
# tshark -r captured_packets.pcap
```

If you want only http request packets to be displayed, please do:

```
# tshark -r captured_packets.pcap -Y http.request
```

where `-Y` option lets you specify display filters (using the same syntax as in Wireshark).

Now, let's display the hosts you connected through http. To specify that, you need to use `-T` option to specify that we want to extract fields and `-e` option to specify the field you want to be displayed. Therefore, the whole commands becomes:

```
# tshark -r capture.pcp -Y http.request -T fields -e http.host
```

If you want to check whole list of available options in tshark, you can do:

```
# tshark -help
```

or the help page can be accessed through web with this link

`https://www.wireshark.org/docs/man-pages/tshark.html`

The capture and display filters used in tshark are the same as in Wireshark and can be accessed with below links.

Capture Filters: `https://wiki.wireshark.org/CaptureFilters`

Display Filters: `https://wiki.wireshark.org/DisplayFilters`

6.1.2 Exercise 1

Alice is soon going to have her holidays. She is searching for holiday offers on the web. She finds a very interesting and inexpensive offer at a website and therefore, she hurries up to book it. She enters all her details in a html form, including her name, date of birth, phone numbers, email addresses, home address, and registers for this offer. After registration, when she wants to pay for this offer, she realizes that her connection to this website (until now) is not encrypted. So she stops the online payment.

The pcap file, named alice.pcap, stores all the above-mentioned activities of Alice, captured by tshark at her network interface. Now, your job is find the packet in the pcap file that contains all her information. You should use tshark command to get hold of all her details she typed in for reserving this trip.

Hint: The details are filled by Alice in a html form. Therefore, an http post request body should contain her details.

Q22/ Please write below all the commands you tried in the order you typed in, even if you did not succeed to get her details. We are interested in your thought process, how did you proceed, the commands you tried, and how close you finally could come to the solution even if you did not succeed.

We used the following command:

```
tshark -r alice.pcap -Y "http.request.method==POST" -d tcp.port==80,http -T fields -e ip.src -e ip.dst -e text
```

HTTP traffic is running on port 80. We also wanted to filter only the post requests. The output is given below:

```
128.178.151.55 5.39.15.179  Timestamps,POST /ajax/sra/search.php HTTP/1.1\r\n,\r\n,Form item: "type" = "2383"
128.178.151.55 5.39.15.179  Timestamps,POST /ajax/sra/fiche_produit_desktop.php HTTP/1.1\r\n,\r\n,Form item: "tarifs" = "<form class="price-form">
    <p class="label">
        Nombre de voyageurs :
    </p>
    <div class="row">
        <div class="small-2 column">
            <label for="adults" class="right inline">
         ,Form item: "descriptif" = "<div id="detail_descriptif" class=" details_produit">
 Durée du voyage : <span id="regime_descriptif">8 jours
   / 7 nuits</span><br/><br/>
  <b>SITUATION </b><br />
Niché au milieu d'un magnifique jardin v
```

[A22]

6.1.3 Exercise 2

In this exercise you will compare the usage of Wireshark and tshark.

Q23/ How can you identify the TCP connections opened by visiting the `www.epfl.ch` webpage **using Wireshark**? Which filter you will use? Describe the steps that you have done and write the filter command that you used. Also write down the connections that you have found. Is there one, or are there several such connections?

We used the following filter: tcp.connection.fin && ip.dst==104.20.229.42 (We checked the IP of the website)
There is only one connection. Now, the machines have acknowledged each other by doing a 3-way handshake. The FIN flag indicates that the TCP connection is now ready.

[A23]

Now assume that you do not have access to GUI and only command line is available. It means that both browser and tshark should be opened from the command line.

Q24/ How can you identify the TCP connections opened by visiting the `www.epfl.ch` webpage **using tshark**? Describe the steps that you have done and write the command that you use. ***Hint:*** *In this case you will need to know how to run tshark and browser with predefined url simultaneously. Also, how run tshark* *capture for a certain amout of time.*

[A24] We used the following command: sudo tshark -i wlp3s0 -w captured_packets.pcap -a duration: 10 & firefox -headless -url www.epfl.ch
What it does is that it starts tshark, capturing the packets from the wireless adaptor, for a duration of 10 seconds. The "&" command in Linux puts the process to the background, and it prints its outputs to the bash terminal. Then, we started the Firefox internet browser in