University of Porto
Faculdade de Engenharia

Traffic monitoring tools PGRE

Lab work 2

Alena Tesařová
Rodrigo Caldas
Tiago Ribeiro

March 25, 2020

Contents

1 Introduction

The purpose of this assignment is to get familiar with the tools for monitoring the traffic of systems and services in a network, with particular relevance in the web-based tools, freeware. It is proposed to use two tools that provide a HTML monitoring data interface from the management variables in the equipment in the case of "The Multi Router Traffic Grapher" tool (MRTG), or traffic analysis on the network, as in the case of “Network TOP” (ntop). The work consists of using MRTG and ntop to monitor a network and in particular the routers and services running on it.

2 MRTG

The Multi Router Traffic Grapher (MRTG) is a free software for monitoring and measuring the traffic load on network links. It allows the user to see the traffic load on a network over time in graphical form.

It was developed to monitor router traffic, but has developed into a tool that can create graphs and statistics for almost anything.

MRTG is written in Perl and can run on Windows, Linux, Unix, Mac OS and NetWare. Example of a MRTG graph is shown in Figure 1.

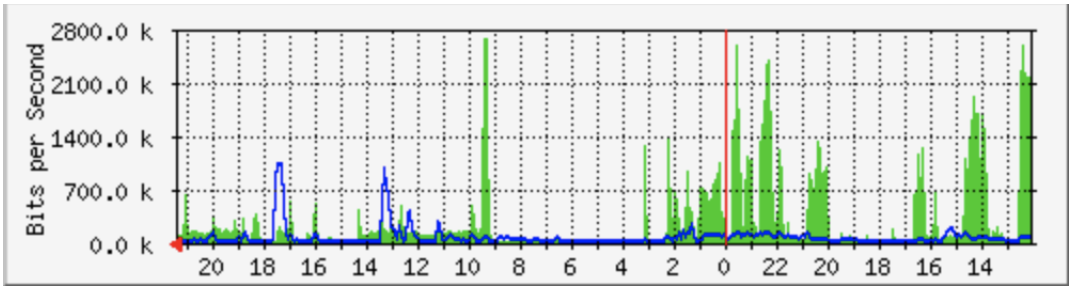


Figure 1: MRTG graph

2.1 SNMP

MRTG uses the Simple Network Management Protocol (SNMP) to send requests with two objects identifiers to a device. The device, which must be SNMP-enabled, will have a management information base to look up the object identifiers specified. After collecting the information it will send back the raw data encapsulated in an SNMP protocol. MRTG records this data in a log on the client along with previously recorded data for the device. The software then creates an HTML document from the logs, containing a list of graphs detailing traffic for the selected devices in the server. [1]

MRTG features

- works on most UNIX and Windows NT platforms
- is written in Perl and comes with all available source code
- typically collects data every five minutes (it can be configured to collect data less frequently).
- comes with a toolkit suitable for your configuration
- creates an HTML page per target that features four graphs (GIF or PNG images)

3 NTOP

Ntop is computer software that probes a computer network to show network use in a way similar to what the program top does for processes. In interactive mode, it displays the network status on the user's terminal. In Web mode, it acts as a web server, creating a HTML dump of the network status. It supports a NetFlow-sFlow emitter-collector, a Hypertext Transfer Protocol (HTTP) based client interface for creating ntop-centric monitoring applications, and RRDtool for persistently storing traffic statistics.

Common usage on a Linux system is to start the ntop daemon (*/etc/init.d/ntopd* start), then it is possible to use the web interface to ntop via visiting *http://127.0.0.1:3000* provided the loopback device has been started (*/etc/init.d/net.lo* start) and the listening port for ntop is 3000 (look out for the -w option in grep ntop). [2]

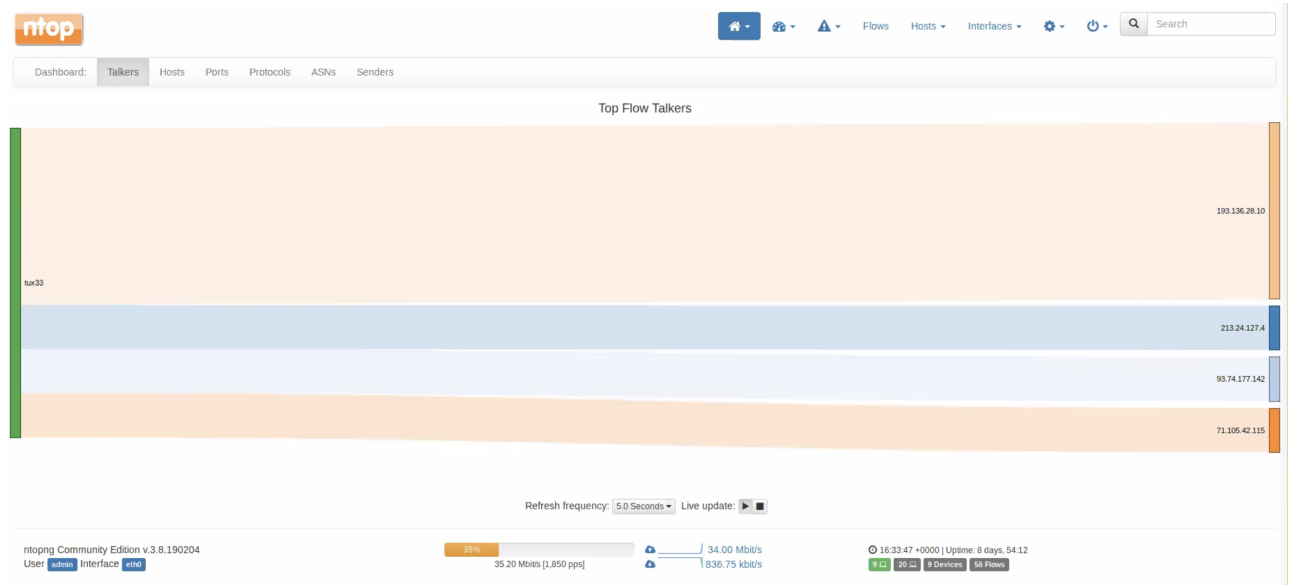


Figure 2: NTOP Web view

NTOP features

- show realtime network traffic and active hosts
- geolocate and overlay hosts in a geographical map
- report IP protocol usage sorted by protocol type
- full support for IPv4 and IPv6
- analyse IP traffic and sort it according to the source/destination

4 MRTG versus NTOP

Although both are quite powerful tools we can find several differences between them.
MRTG collects information from a much larger variety of sources (over SNMP) and from a larger number of devices. But, the information available is less exact than detailed packet-parsing.

On the other hand, **Ntop** is designed to watch network traffic at the packet level on interfaces. It can only collect information from hosts that have the ability to run Ntop and process the packets.

5 Server configuration and preparing the environment

Our first task was to create a right environment to better demonstrate monitoring tools. Our configuration can be seen in Table 1. We put main servers on computer one, FTP works on computer two and the rest of computers will be used as clients that will be sending requests. Using two clients we can better compare results on monitoring tools. Results will be presented in section 6.

Computer 1	WebServer, NTPserver, Mailserver e DNS server
Computer 2	FTP
Computer 3	Client1
Computer 4	Client2

Table 1: Used configuration on four different computers

5.1 Web Server

Web server is a server that can satisfy client by replying on this requests on the World Wide Web. It receives HTTP Requests and send HTTP Responses to the browser. To demonstrate working web server on our first computer, we used a software called *curl* that provides transferring data with URLs (in Figure 3). [4]

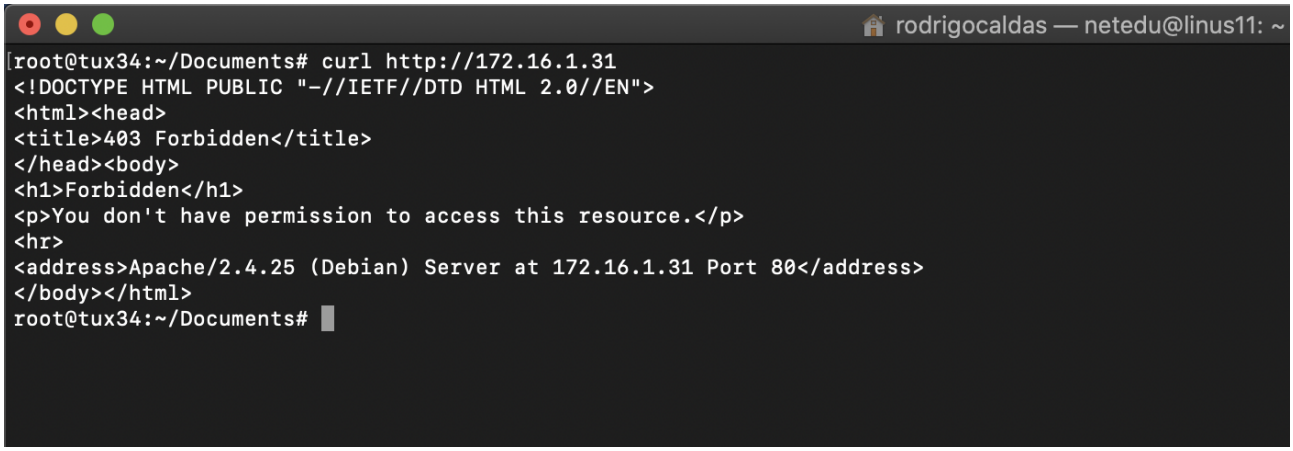


Figure 3: Web Server sends the HTTP Response to client

5.2 NTP server

Network time protocol is used to synchronize time between computers over the world according to the Coordinated Universal Time. It sends and receives timestamps using UDP diagrams on port number 123. The current protocol version is 4. The most common command is *ntpdate* to sync time from the server – in our case server *172.16.1.31* as shown in Figure 4. To install NTP server we used this link as a main reference: `https://linuxconfig.org/how-to-setup-ntp-server-and-client-on-debian-9-stretch-lin` [3, 5]

Figure 4: NTP server sends the timestamp to sync the time on client

5.3 Mail server

Mail servers care about sending an email to the right client. There are two types of mail servers – income and outcome mail servers. The most common outcome server is SMTP (Simple Mail Transfer Protocol) and the most known income servers are IMAP or POP3. We installed the mail server with Postfix using this guide `https://www.tecmint.com/install-postfix-mail-server-with-webmail-in-debian/`.

In Figure 5 there is an example of client-server communication where computer 4 sends an email to computer 1 where the mail server is running. [6]

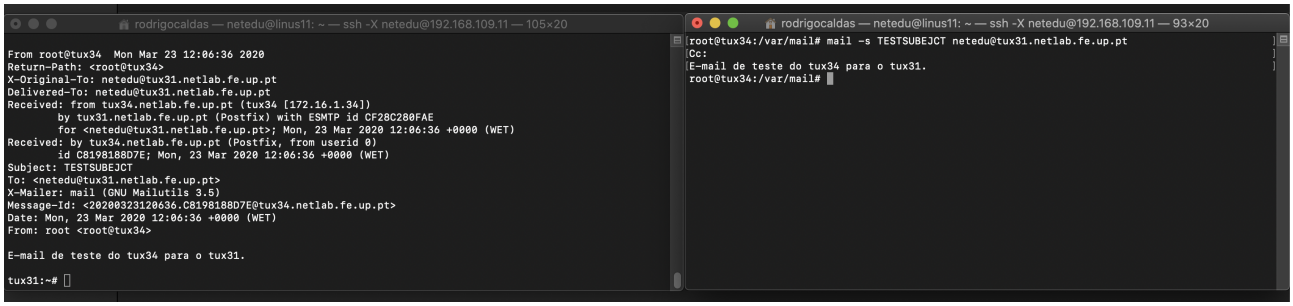


Figure 5: Client-server communication

5.4 DNS server

Domain name server is a hierarchical and decentralized naming system that is mainly responsible to find the correct IP address, but it has many other usage. In Figure 6 we used a tool *dig* to query the DNS running on first computer.

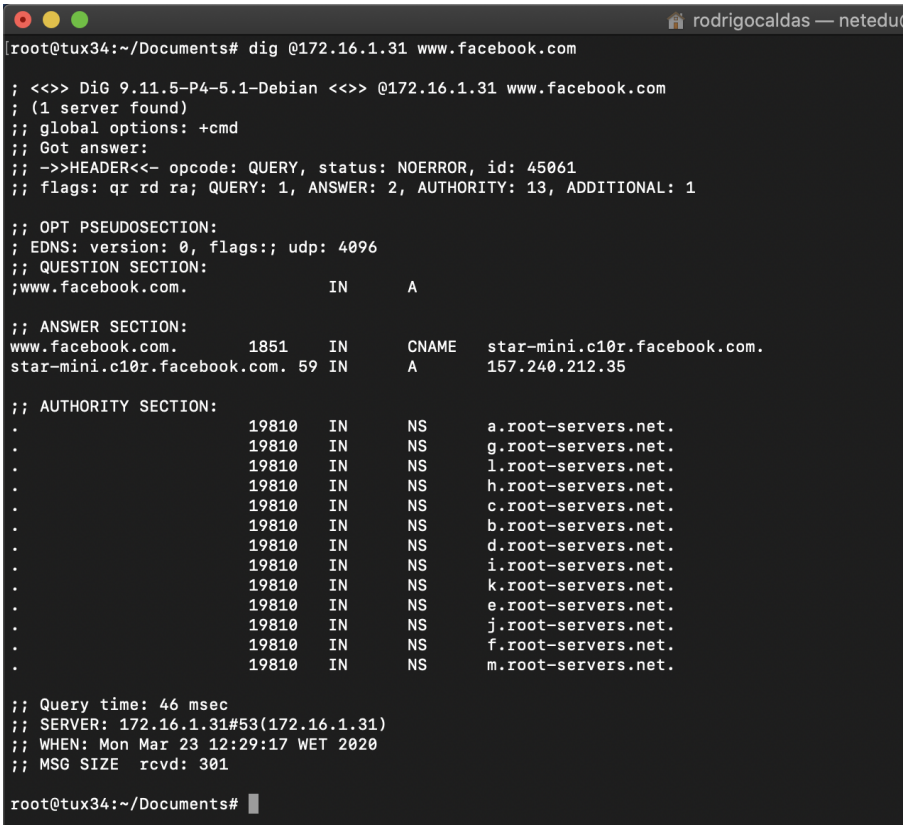


Figure 6: DNS server

5.5 FTP server

File transfer protocol is as standard computer that is used for transferring files between client and a server. We created a script (Figure 7) that downloads a file through FTP, requested by the client to the server that is running on computer number 2.

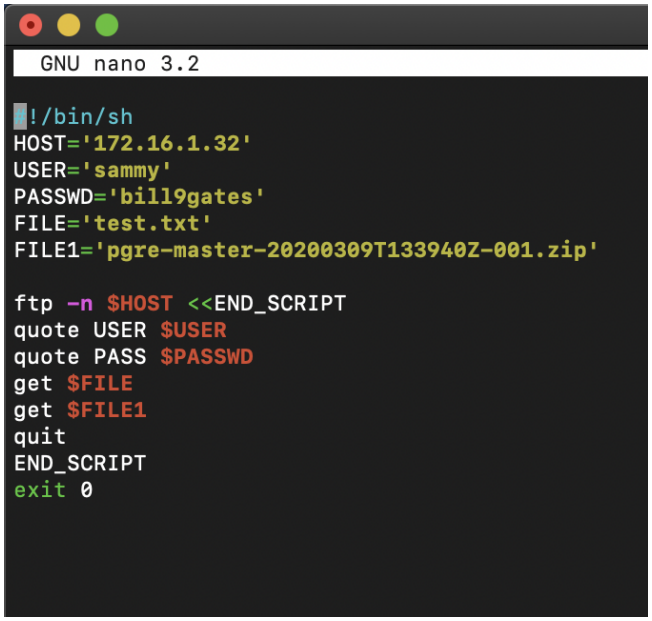


Figure 7: Script to download a file through FTP to server

5.6 Crontab

Crontab is a Unix program that is used to view or edit the table of commands that are executed by cron on a given schedule. To configure cron, we use the command **crontab -e**. In the configuration file it is necessary to enter all the commands we want to execute and also schedule of the time they should be executed.

The configuration of Crontab is shown in Listing 1 where we can see the commands that we want to execute and the time. In this case, Crontab is configured on the client side to request a query for each service every 5 minutes.

Listing 1: Crontab

```
*/5 * * * * ntpdate -u 172.16.1.31
*/5 * * * * /root/Documents/ftp_d.sh
*/5 * * * * dig @172.16.1.31 www.facebook.com > /dev/null 2>&1
*/5 * * * * curl http://172.16.1.31 > /dev/null 2>&1
*/5 * * * * echo 'E-mail p 31' | mail -s 'teste' netedu@tux31.netlab.fe.up.pt
```

6 Monitoring tools results

We have been measuring flows for 14 days using 2 tools – *MRTG* and *NTOP* on computer tux34. Results are presented below in section 6.1 and 6.2.

6.1 MRTG

In Figure 8 there is a main page of MRTG tool. We measured the data on computer 4 and the last update was on March 23. The green part of graph represents the total traffic leaving the server and entering our network. This part can be barely seen because there was almost no traffic going in our network. The blue line on the graph represents all traffic coming in to the server. The graphs are read right to left with the most recent traffic displayed on the left side of the graph.

On the left side of the graph there will be a list of numbers that represent the bandwidth usage. The numbers at the bottom of the graph show either the hour, the day of the week, the last 4 weeks, or the months of the year depending on the type of the graph (monthly, yearly, daily).

In week view graph in Figure 9b we can for example get an information about maximum bandwidth usage that was 3927.5 kB/s.

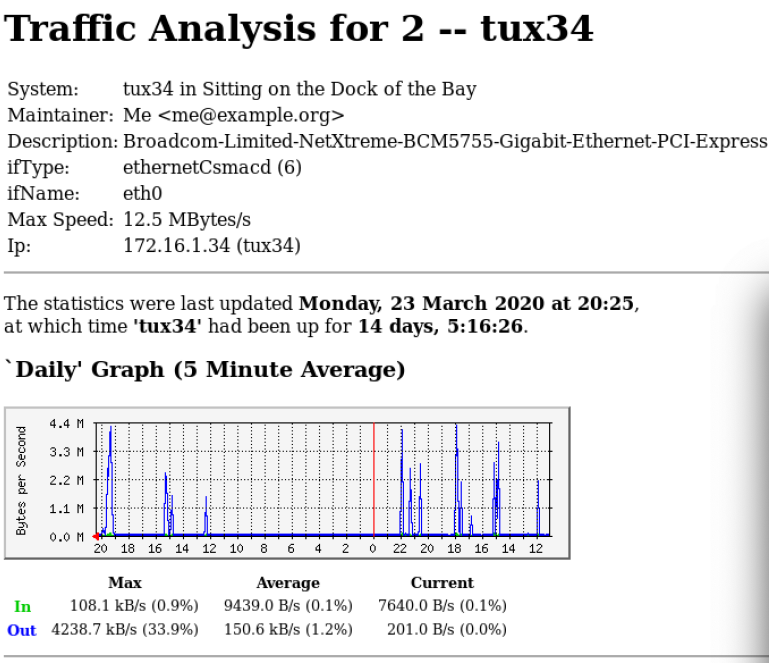
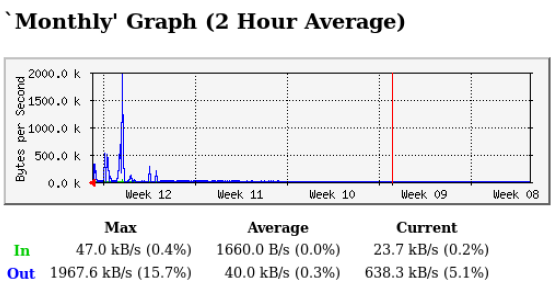
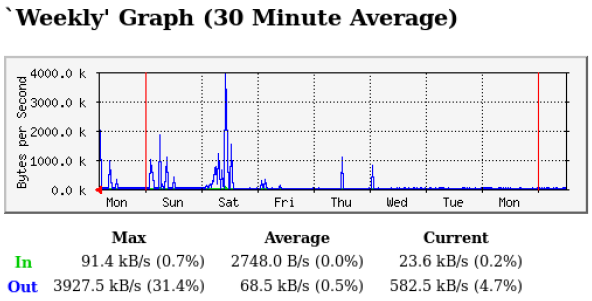


Figure 8: MRTG main page view



(a) Monthly graph that MRTG generated

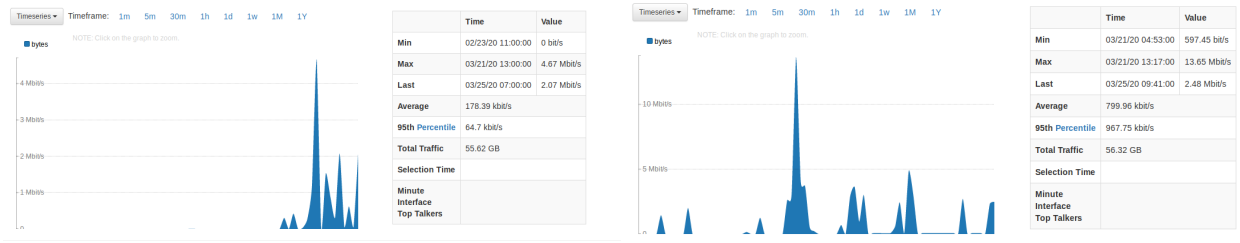


(b) Weekly graph that MRTG generated

Figure 9: Results of MRTG

6.2 NTOP

We managed to get to the results of NTOP by remote access through ssh. In Figure 10 there are 2 graphs showing traffics. Because of a bad remote access to the client we could not get the title of x-axis and the rest of information. The graphs are read left to right with the most recent traffic displayed on the right side of the graph. If we compare results of MRTG with NTOP we can notice that the shapes are very similar (it is necessary to turn the MRTG graph to be able to see it). The peak in both was measured on Saturday, March 21.



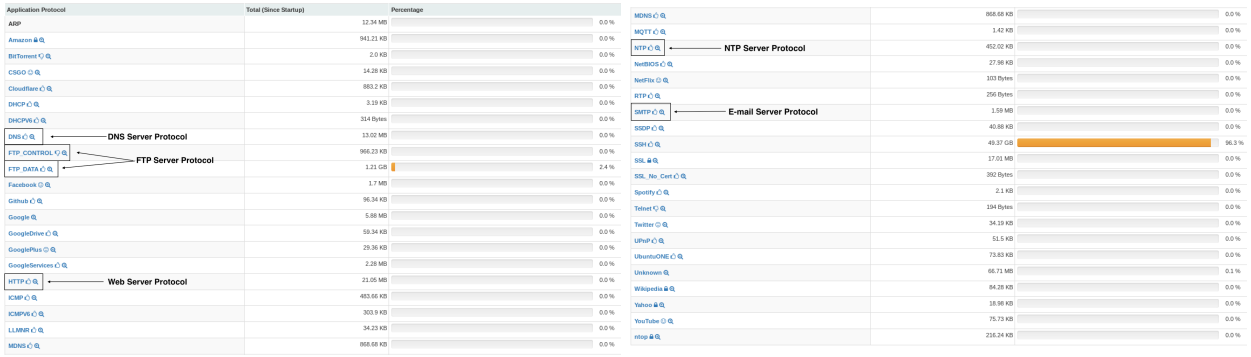
(a) NTOP month view traffic

(b) NTOP week view traffic

Figure 10: Results of NTOP

6.2.1 Tabular view

Tabular view (in Figure 11) shows historical data for the specified time in a tabular format. In Figure 11a on the left side there are flows for DNS, FTP and Web server protocols. On the right side (Figure 11b) there are flows for NTP and SMTP protocols.



(a) NTOP tool shows DNS, FTP and HTTP queries.

(b) NTOP tool shows NTP and SMTP queries.

Figure 11: Results of NTOP

7 Conclusion

In this protocol we described two very useful tools to monitor traffic on router. Than, we prepared an appropriate environment to be able to monitor different type of services as DNS, FTP, NTP, SMTP or HTTP requests. The distribution of different protocols is nicely shown in NTOP interface in comparison with MRTG. The biggest difference of this tools is the type of information they display – NTOP is designed to watch network traffic at the packet level on interfaces, it collects information from hosts that runs NTOP, but MRTG, on the other hand, collects information from a much larger variety of sources, typically over SNMP, and from a larger number of devices. From our point of view, we would choose NTOP because of its friendly user interface and amount of information it gives us about a monitored device. Unfortunately, we were not able to profit fully from the power of this tool because of a slow access through ssh client.

References

[1] *MRPG. [Online, last update 23.2. 2018]. URL* https://en.wikipedia.org/wiki/Multi_Router_Traffic_Grapher

[2] *NTOP. [Online, last update 11.1. 2020]. URL* https://en.wikipedia.org/wiki/Ntop

[3] *Network Time Protocol. [Online, last update 11.3. 2020]. URL* https://en.wikipedia.org/wiki/Network_Time_Protocol

[4] *What is a web server?. [Online, last update 18.6. 2019]. URL* https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_web_server

[5] *How to Synchronize Time with NTP in Linux. [Online, last update 20.4. 2018]. URL* https://www.tecmint.com/synchronize-time-with-ntp-in-linux

[6] *Mail Server. [Online, visited 23.3.2020]. URL* https://whatismyipaddress.com/mail-server