

Bachelor Degree Project



Performance comparison of IPv4 and
IPv6 in open source router distributions

Bachelor Degree Project in Computer Science
15 ECTS
Spring term 2015

David Gometz

Supervisor: Jonas Mellin
Examiner: Jianguo Ding

Abstract

With IPv4 addresses running out there is a need for IPv6 compatible routers. This study aims to find open source routers that have support for IPv6 and compare it in terms of performance to IPv4 to see if there are any differences in performance.

In addition to this the chosen routers have also been evaluated in terms of security and other desired features.

An experiment and a theoretical study evaluating this was carried out to help companies and individuals wanting to use IPv6 make choices in what open source router to use.

Different performance factors were taken in to consideration as well as security features.

There were no significant differences between IPv6 and IPv4 with IPv4 slightly beating IPv6. Between the routers there were some differences with the VyOS router outperforming pfSense in terms of throughput but pfSense had lower latency values. Depending on the requirements for a specific network environment the results of this study could be used to pick an IPv6-enabled open source router distribution.

Keywords: Open Source, Routers, Performance, IPv4, IPv6, pfSense, VyOS

Contents

1	Introduction.....	1
2	Background	2
2.1	Routers.....	2
2.2	Open source software	2
2.3	IPv4 and IPv6	2
2.4	Performance and examples	3
2.5	Previous work	3
3	Problem definition.....	4
3.1	Purpose	4
3.2	Questions to be answered	4
3.3	Motivation	4
3.3.1	Objectives	5
3.4	Requirements	5
4	Methodology	6
4.1	Scope	6
4.2	Experiment	6
4.2.1	Throughput	7
4.2.2	Latency.....	7
4.2.3	Frame loss rate	7
4.3	Qualitative study.....	7
4.4	Validity	8
5	Implementation	9
5.1	Operating systems	9
5.1.1	pfSense	9
5.1.2	VyOS.....	9
5.1.3	Hosts	10

5.2	Commands used for tests	10
5.2.1	Throughput	10
5.2.2	Latency	11
5.2.3	Frame loss rate	11
6	Results	12
6.1	Throughput	12
6.2	Latency	17
6.3	Frame loss rate	20
6.4	Theoretical Study	20
6.4.1	NAT	20
6.4.2	DHCP	20
6.4.3	Firewall	20
6.4.4	VPN	21
6.4.5	Quality of Service	21
7	Analysis	22
8	Conclusion	24
9	Discussion	25
10	Future Work	26
	References	27
	Appendix 1 - Summary	1

1 Introduction

With IPv4 addresses running out there is a need for IPv6 compatible routers. This study aims to compare open source software routers in terms of performance between the IP protocols but also evaluating security and other desired features.

An experiment and a theoretical study evaluating this has been carried out to help companies and individuals make choices in what open source router to use using the results from the study.

2 Background

This chapter defines concepts that are essential for understanding the problem definition of this study.

2.1 Routers

A router is in the traditional sense a networking device which forwards data packets over a computer network (Hancock, 1995). A router connects at least two networks to each other in comparison to a switch which is a networking device that creates networks by connecting devices so that they can talk to each other. The most common scenario is an edge router which connects the local area network (LAN) to the Internet which is a wide area network (WAN).

Routers are usually sold as a device with pre-installed software ready to use out-of-the box from the manufacturer. The pre-installed software is proprietary and cannot always be replaced.

Open source developers have made it possible to turn a personal computer in to a router using operating systems specifically made for this purpose (Hoover, 2006). These systems are often based on Linux or BSD and are tailored to include software components that brings routing functionality to a PC.

2.2 Opensource software

Open source is software that free to distribute and not require any royalties or fees (Open Source Initiative, n.d.). The program must include source code and allow for distribution in source and compiled form (Open Source Initiative, n.d.). The license must allow modifications, derived works and allow them to be distributed under the same license and terms (Open Source Initiative, n.d.).

There exists many different open source licenses but they all comply with the Open Source Definition made by the Open Source Initiative.

There are some confusion about what is to be considered “open” and there are different opinions of the meaning (Cerri & Fuggetta, 2007). For this study any software that uses an open source license approved by the Open Source initiative is considered as open source.

2.3 IPv4 and IPv6

IPv4 the fourth and most commonly used version of the Internet Protocol and routes most of the Internet’s traffic at the time of writing this report. However the address space of IPv4 is not large enough to account for the growth of Internet users. There has been warnings of IPv4 address exhaustion as early as in the mid-1990s but there still hasn’t been any large changes (Dell, 2010, p.6). Therefore the new version 6 of the Internet Protocol has been developed with a much larger

address space which has enough addresses to not run out. There are also architectural inefficiencies to the IPv4 protocol (Bolla & Bruschi, 2013).

There exists many challenges in doing to the switch from IPv4 to IPv6 one of which is the devices that end users need to have. There are different transition mechanism which can be deployed but there must be hardware and software to support it (Mandic, 2014).

Cisco published a white paper in 2007 with a performance comparison in regards to throughput and latency comparing IPv4 and IPv6 on different Cisco router platforms (Cisco, 2007). The results showed small differences between the two protocols but the biggest difference was in the small packets sizes where IPv4 outperformed IPv6 in terms of throughput (Cisco, 2007).

2.4 Performance and examples

Performance is the action or process performing a task or a function and how successfully it is performed. In the context of computing and data transfer over networks, performance and scalability can for example be measured with these constructs: Throughput, Latency and Packet Loss.

These three are examples of measurements that show how well a network device performs in terms of transferring data which is one of its primary functions.

2.5 Previous work

Similar studies comparing open source software routers has been done in 2013 by Pär Fahlesson and in 2014 by Fredrik Jakobsson (Jakobson, 2014) (Fahlesson, 2013). None of these studies has taken IPv6 in to consideration but have instead been focused only on IPv4.

3 Problem definition

This part describes the purpose of the study and motivation behind the chosen subjects of evaluating open source software routers.

3.1 Purpose

The purpose of this study is to compare and contrast the results from evaluating the performance of IPv6 compared to IPv4 in open source software routers, taking security and other features in to account. The data and subsequent analysis of these tests may be used by individuals and companies when choosing router software.

3.2 Questions to be answered

The questions that this study aims to answer are:

- How do IPv4 and IPv6 compare to each other in terms of throughput, latency and frame loss rate in open source routers?
- How do open source routers compare to each other in terms of performance, security and other desired features?

3.3 Motivation

There are challenges arising from the exhaustion of IPv4 addresses and sooner rather than later a transition must be made from IPv4 to IPv6 (Levin & Schmidt, 2014). There must be both hardware and software to support it. As an alternative to pre-built routers with proprietary software there is the option to choose your own hardware and build a router with a router distribution using open source software. When choosing a router distribution one factor should be IPv6 support if one want to prepare and adapt for the future of networking.

There has been different tests and evaluations made between IPv4 and IPv6. One test in a made in a large-scale network using IPv6 shows that there are some differences including degradation in throughput compared to IPv4 (Shiau et al., 2006). This study examines the current state of open source router distributions seeing which of them have support for IPv6 and then performing an experiment comparing the performance of IPv4 and IPv6. Are there any significant performance differences between the protocols on the routers? How do the routers compare to each other? When companies and individuals are looking for an open source router with IPv6 functionality this study can be used as a source to see detailed data of the routers perform in different performance experiments. These results can hopefully aid them in choosing an open source router that fits their specific needs and network scenarios.

When choosing a router one can not only look at the pure performance. Security and other desired features play a big part when making a decision of what kind of router is best for the task at hand. Therefore this study also analyzes and summarizes typical features that could help in deciding between routers. These results can also aid companies and individuals that are looking for an open source router with specific functionality.

3.3.1 Objectives

1. Select routers from the specified requirements.
2. Examine the routers and their features to see if they have, if it works under IPv6 and then evaluate them by studying system documentation, resources made available on the Internet.
3. Compare and contrast the performance of the routers in an experiment using benchmarking tools to see their performance using IPv4 and IPv6 in:
 - a. Throughput
 - b. Latency
 - c. Packet loss rate
4. Compare results between routers too see how they perform in comparison to each other.
5. Compile the results of the two studies and produce an analysis that can aid in choosing between open source software routers.

3.4 Requirements

These are the requirements for the chosen routers in the study:

- The router must be open source
- The router must be possible to install on a x86 machine
- The router must have support for the IPv6 protocol
- The router must be in active development and updated within the last year.

In the choosing process other factors are taken in to consideration such as popularity, based on number of downloads. The source for this information is the website DistroWatch, a site that contains news, popularity rankings and other information about free software/open source Unix-like operating systems (DistroWatch, 2015a). DistroWatch describes their popularity rankings as a lighthearted way of measuring popularity (DistroWatch, 2015b).

Basic and advanced features such as DHCP, NAT, Quality of Service and other desired features. These features are not examined in a practical experiment like performance but are studied through examining systems documentation in the theoretical study and comparing the routers.

4 Methodology

4.1 Scope

From the delimitations two routers have been found that match the requirements:

- PfSense
- VyOS

The requirement for IPv6 was the hardest to meet because many of the routers only had partial support or required that you added support yourself which is not covered by this study. The chosen routers had full IPv6 support as well as the other requirements. Based on the delimitations, popularity rankings by DistroWatch and the aim to select a distribution focused primarily on acting as a router, the chosen routers were considered the most suitable routers for this study.

Other popular open source routers had to be omitted because of different reasons. One of the more popular open source according to DistroWatch rankings, ClearOS, had not support for IPv6 in their latest stable version (6.6.0). However according to a support representative that was contacted using the online chat on their website, it was planned for their next release. Another popular distribution according to DistroWatch rankings, Untangle NG Firewall, only has partial support for IPv6 and has completed two out three phases of IPv6 support where the third phase still has its status listed as “planning” with no update since 2013 (Untangle, 2013). A router distribution which has been around since 2003 called m0n0wall was also considered but while it had IPv6 support it had not been updated since 2014 and the author announced on February 15 that the project had officially ended (Manuel Kasper, 2015). One of the chosen routers, pfSense, is based on m0n0wall.

4.2 Experiment

The test is designed according recommendations published by the Internet Engineering Task Force (IETF) in their “Request for Comments” publications. Methodologies for carrying out and describing performance characteristics of a network interconnection device are defined in the publications RFC2544, Benchmarking Methodology for Network Interconnect Devices, and RFC5180, IPv6 Benchmarking Methodology for Network Interconnect Devices.

An experiment has been carried out in a lab using three computers per router. A number of computers with equal hardware configurations have been used for each of the software router distributions and a host computer. The computers have been set up as local networks with only the router and host connected to each other but isolated from any outside sources such as the Internet. The routers have been configured with IPv4 and IPv6 and the benchmarked using the tools Iperf and Ping to determine values for throughput, latency and packet loss rate. The tests

have been carried out on ten different occasions with ten trials per configuration and then min, max and mean values of all trials have been calculated.

The following frame sizes have been used in the tests: 64, 128, 256, 512, 1024, 1280 & 1518. These are the recommended frame sizes to use in performance experiments on the Ethernet standard (McQuaid & Bradner, 1999). The sizes include the minimum and maximum frame sizes and has a finer granularity among the smaller frame sizes (McQuaid & Bradner, 1999).

4.2.1 Throughput

Throughput is the maximum rate at which none of the offered frames are dropped by the device (Bradner, 1991).

In the throughput experiment a number of frames have been transmitted through the router at a specific rate and the frames have then been counted.

4.2.2 Latency

Latency is the time interval which starts when the last bit of the input frame reaches the input port and ends when the first bit of the output frame is seen on the output port (Bradner, 1991).

A stream of 120 frames of the aforementioned sizes have been sent from the host to the router measuring the time interval.

4.2.3 Frame loss rate

Frame loss rate is the percentage of frames that should be forwarded by a networks device under a steady state load but were not forwarded due to lack of resources (Bradner, 1991).

In the frame loss experiment a specific number of frames at a specific rate were sent through the router and counted to see how many that make it through. The results from the throughput experiment were used as the maximum rate for the different frame sizes. The throughput would then be reduced in 10% intervals until no frames were lost.

4.3 Qualitative study

Information was gathered from sources such as the system documentation, man-pages and official websites of the chosen routers.

The following features were examined and were ranked in a priority list:

1. NAT (Network Address Translation) and the IPv6 counterpart NPTv6
2. DHCP (Dynamic Host Configuration Protocol) and its' IPv6 version DHCPv6
3. Firewall

4. VPN (Virtual Private Network) and IPSec
5. Quality of Service

These features are ranked in order of importance and were examined in that order to prioritize due to the time constraint of this study.

4.4 Validity

There are numerous threats to validity that needs to be addressed when doing an experiment such as this according to Wohlin.

- Threats to the conclusion validity that need to be addressed are for one the threat of low statistical power, which according to (Wohlin et al., 2012) is the ability of statistical tests to reveal true patterns in the data. If the power is low there is risk of erroneous conclusions drawn from the results according to Wohlin. This threat is mitigated by running the practical experiments ten times on different occasions and establishing max, min and mean values from it.
Fishing for results is a threat to conclusion validity which is when the researcher is looking for a specific results and the analysis is no longer independent (Wohlin et al., 2012). This threat is mitigated by making the selection of routers a part of the method with no favoritism and by applying the exact same method to all test subjects.
- Threats to construct validity include inadequate preoperational explication of constructs which according to Wohlin et al. is when the constructs are not sufficiently defined. The constructs in this study are described in the methodology and based on already defined concepts.
The threat of Mono-method bias, which is when only a single method is used, is mitigated in this study by carrying out both a practical experiment to evaluate performance with quantitative results as well as a more qualitative study of security and other features.

Many validity threats that Wohlin et al. (2012) mentions are not applicable to this study such as internal and external validity threats related to social factors and other factors involving humans.

5 Implementation

All of the computers used in the experiment have the following hardware:

- Intel Core2 6400 CPU 2.13GHz
- 4 GB of RAM
- Network cards with speeds up to 1Gbit/s

5.1 Operating systems

The different router and host operating systems are installed on the local hard drive using images provided by the distribution websites.

5.1.1 pfSense

The pfSense router was installed using the following image file: pfSense-memstick-2.2.2-RELEASE-amd64.img.gz. The installation was completed using the guided installation with a *graphical user interface* (GUI). Standard options for install location, key map and such were selected. After the initial installation network interfaces were configured using the pfSense GUI which guides you through the choices of which network interface to use, what IP addresses to use, subnet mask and if it's IPv4 or IPv6. IPv4 was configured and then changed to IPv6 back and forth between the tests (See Appendix A and Appendix B). The following IP addresses and net masks was used for IPv4 and IPv6 respectively:

- 192.168.0.1/24
- fd85:a57c:289a:8c6b::/64

Using the webGUI, the package for the iperf tool was installed.

5.1.2 VyOS

VyOS was installed using the following image file: vyos-1.1.5-amd64.iso. The installation was completed using the guided *command line interface* (CLI) installation using default options. After the installation configuration of the interfaces was made using the CLI and these commands:

- set interfaces ethernet eth0 address '192.168.0.1/24'
- set interfaces ethernet eth0 description 'INSIDE'

IPv4 was configured and then changed to IPv6 back and forth between the tests. The following IP addresses and net masks was used for IPv4 and IPv6 respectively (See Appendix A and Appendix B):

- 192.168.0.1/24
- fd85:a57c:289a:8c6b::/64

The iperf tool was installed using the apt-get command.

5.1.3 Hosts

For the hosts a minimal Debian Linux system was installed using the following image: debian-8.1.0-amd64-netinst.iso. No additional software was installed except for basic networking tools. The hosts were then respectively configured to use the networks provided by the router computers (See Figure 1). Only one host was connected to the router at one time.

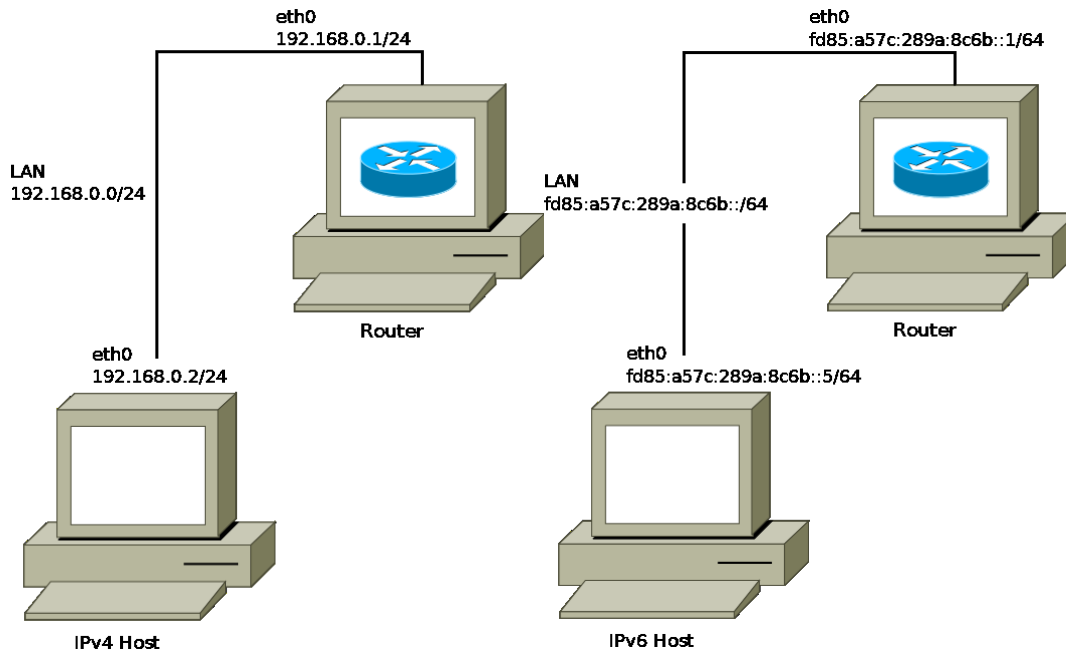


Figure 1 Network topology

5.2 Commands used for tests

Here are the different commands used for performing the performance tests.

5.2.1 Throughput

Command on used on router:

IPv4	IPv6
<code>iperf -s</code>	<code>iperf -s -V</code>

Iperf is started in server mode with `-s` flag which makes the router listen for TCP-traffic on the default iperf port which is 5001. The `-V` flag is used to bind iperf to an IPv6 address and is used on all subsequent iperf commands when using IPv6.

Command on host:

```
iperf -c ipaddress -l framesize -t 600 -i 10 > results
```

Iperf is used with `-c` flag which takes an IP address as argument and connects to that server. The `-l` flag specifies the frame size to be used and is changed according to the different Ethernet frame sizes. The `-t` flag specifies the time in seconds and `-i` specifies the interval between tests. This sets the test to run 60 times during a period of 600 seconds. The results are then written to a file specified after the `>`. For IPv6 the `-V` flag is added.

5.2.2 Latency

Command on host:

```
ping -c 120 -s framesize -8 ipaddress > results
```

The ping command is used on the host specifying number of requests to send using the `-c` flag, frame size with the size of the ICMP head subtracted (8 bytes) and the router IP address. This command is run for each frame size and the results are then written to a file specified after the `>`. For IPv6 the tool ping6 is used with same options.

5.2.3 Frame loss rate

Command on server:

```
iperf -s -u
```

Iperf is started in server mode with the `-s` and `-u` flag which makes the router listen for UDP-traffic on the default iperf port which is 5001. The `-V` flag is used to bind iperf to an IPv6 address and is used on all subsequent iperf commands when using IPv6

Command on host:

```
iperf -c ip -u -b throughput -l framesize -t 600 -i 10 > results
```

Iperf is again used with `-c` flag which takes an IP address as argument and connects to that server. The `-u` flag specifies that it should send UDP-traffic to be able to specify bandwidth using the `-b` flag. The argument for the `-b` flag is set to the throughput corresponding to the throughput measured on the frame size. The `-l` flag specifies the frame size to be used and is changed according to the different Ethernet frame sizes. The `-t` flag specifies the time in seconds and `-i` specifies the interval between tests. This sets the test to run 60 times during a period of 600 seconds. The results are then written to a file specified after the `>`. For IPv6 the `-V` flag is added.

6 Results

In this section the results from the experiment and theoretical study are presented.

6.1 Throughput

The figures in this section shows the minimum, average and maximum values for the throughput of each of the frame sizes. There are charts for each router, each of the IP protocols and a chart comparing the average values of the IP protocols side by side.

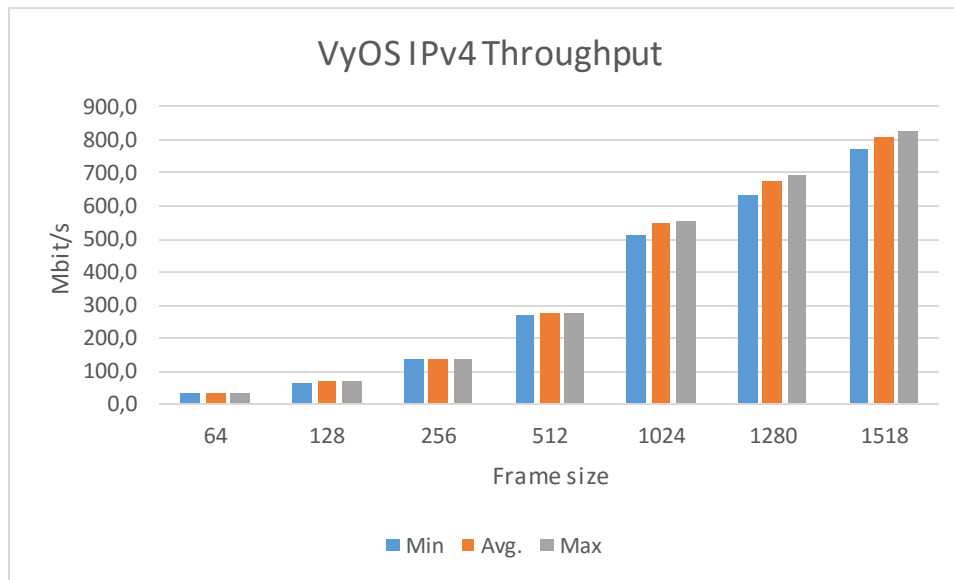


Figure 2 VyOS IPv4 Throughput

Figure 2 shows the throughput for VyOS IPv4 where the difference between minimum and max values is not very high in the lower frame sizes but in the larger frame sizes it goes as high as 51 Mbit/s.

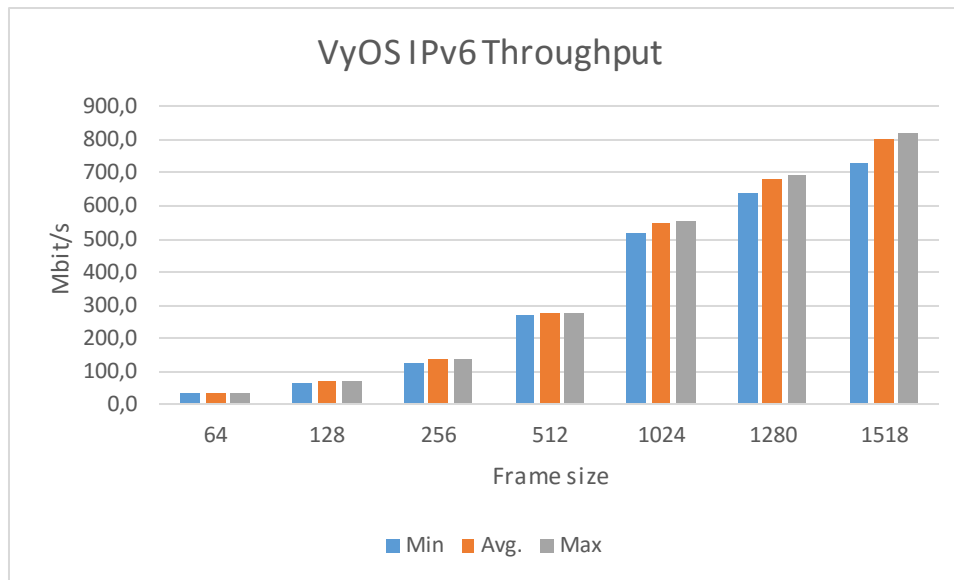


Figure 3 VyOS IPv6 Throughput

Figure 3 shows the throughput for VyOS IPv6 where the difference between minimum and max values in the lower frame sizes are not high but slightly higher than IPv4. In the larger frame sizes the difference is much higher going up to as high as 90 Mbit/s difference in the 1518 byte frame size

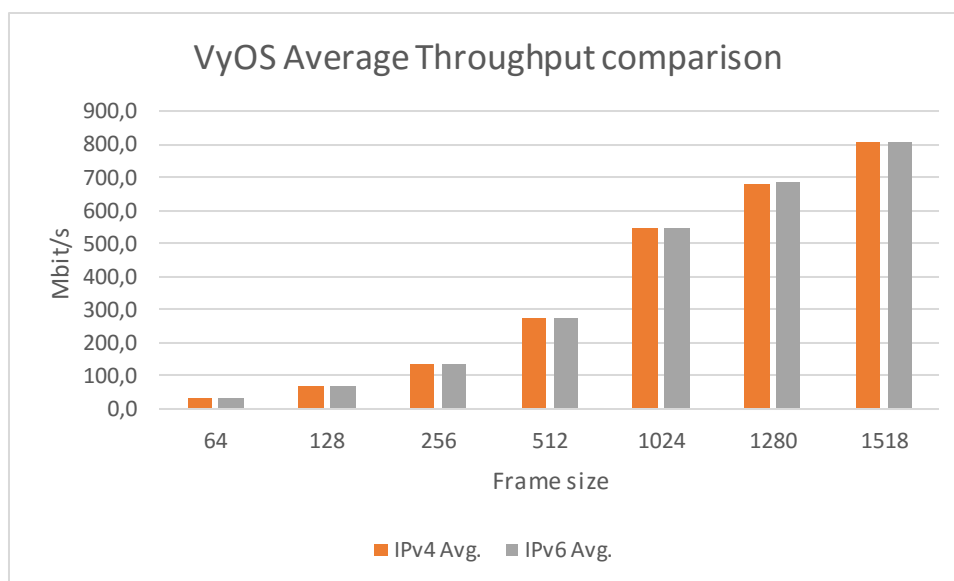


Figure 4 VyOS Average Throughput comparison

Figure 4 shows the average throughput for VyOS where the average values are quite close with IPv4 having slightly higher values on frame sizes 256 bytes, 512 bytes, 1024, bytes and 1518

bytes. IPv6 beats IPv4 with higher values at frame sizes 128 bytes and 1280 bytes. At 64 bytes frame size both are equal.

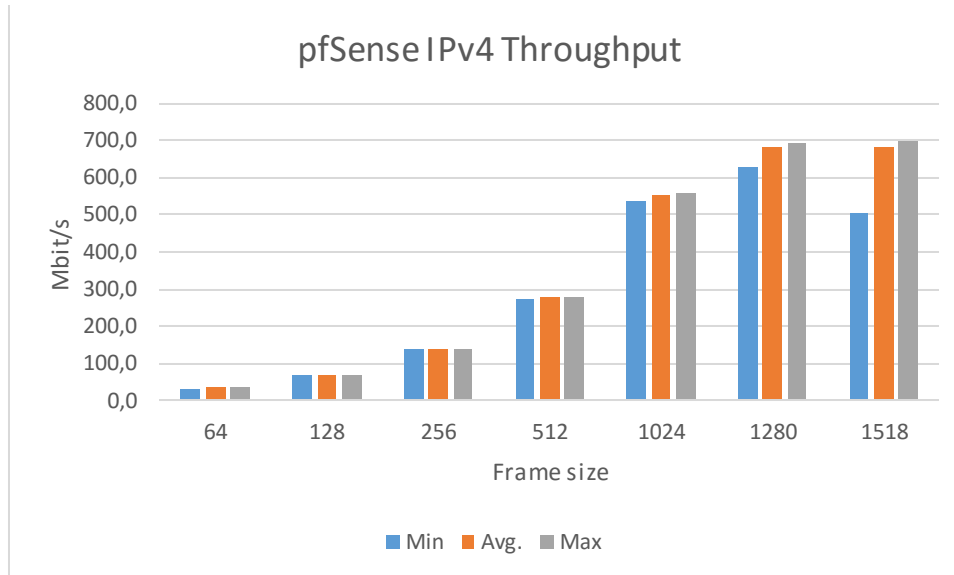


Figure 5 pfSense IPv4 Throughput

Figure 5 shows the throughput for IPv4 where PfSense has minor difference between minimum and maximum throughput in the smaller frame sizes but there are some substantial differences in the higher ones with the 1518 byte frame size difference being at 195 Mbit/s. However the minimum values of both 1280 bytes and 1518 bytes could be seen as anomalies since recordings that low are not common in the data.

The average value of 1518 byte frame size is actually lower than the average value of 1280 byte frame size.

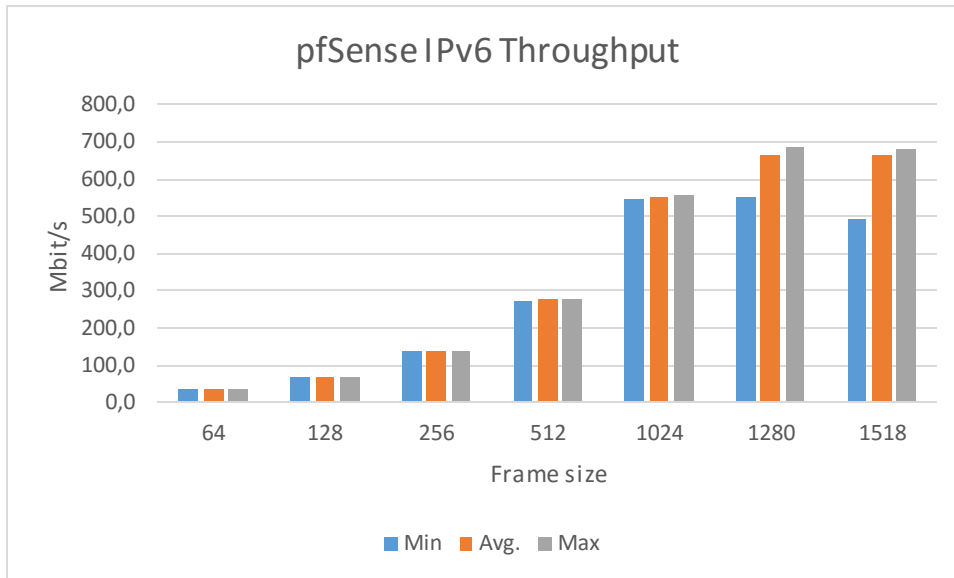


Figure 6 pfSense IPv6 Throughput

Figure 6 shows the throughput for pfSense IPv6 where there are minor differences between minimum and maximum but like IPv4 there are big differences in 1280 bytes and 1518 bytes which in this also are anomalies and not common in the result data.

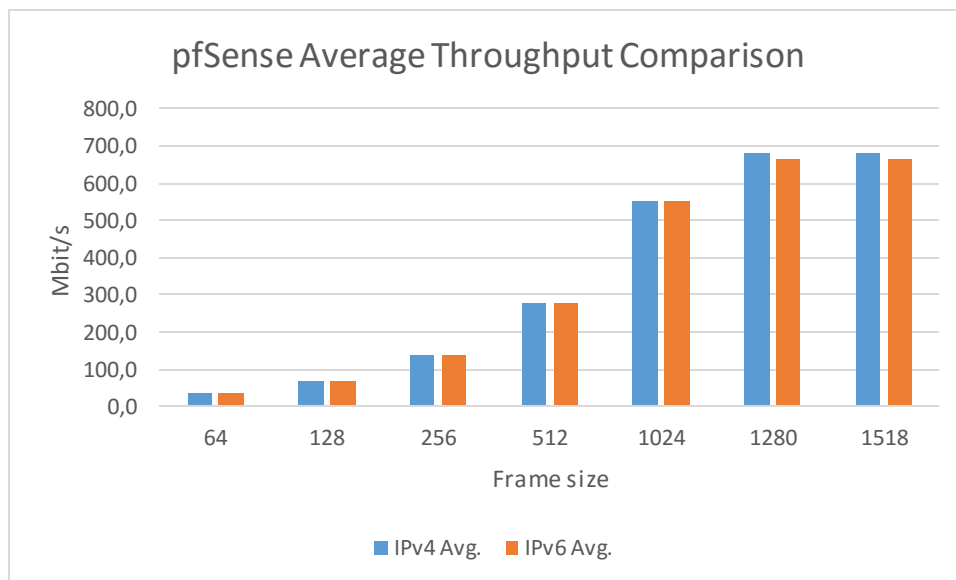


Figure 7 pfSense Average Throughput Comparison

Figure 7 shows the average throughput for pfSense where the average values are quite similar in the 64 though 1024 byte frame sizes with minor differences of 0,1-0,3 Mbit/s with IPv4 being

superior or equal in all frame sizes except 1024. In the 1280 byte and 1518 byte frame sizes IPv4 beats IPv6 by 15 Mbit/s.

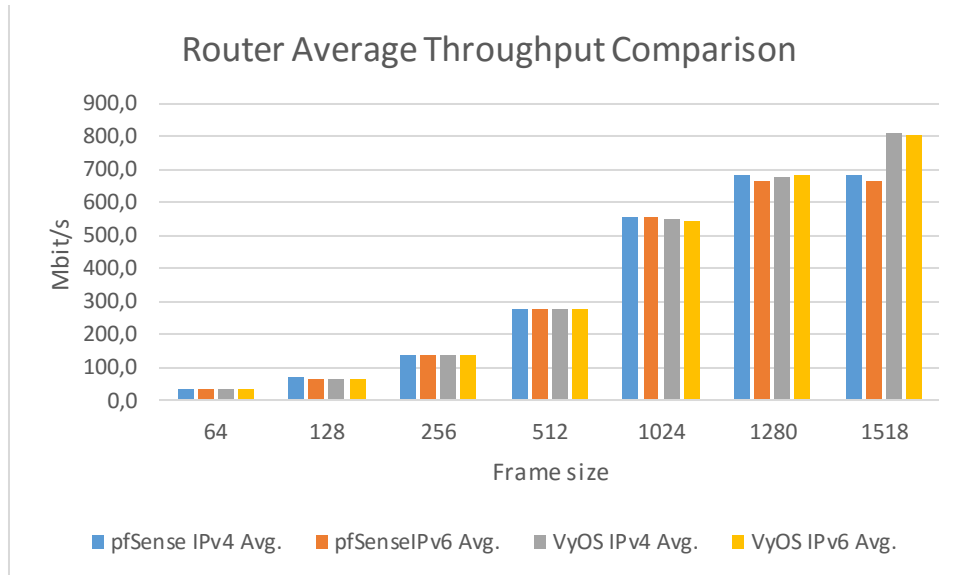


Figure 8 Router Average Throughput Comparison

Figure 8 shows the average throughput for both routers where the routers perform more or less equal on most frame sizes with minor differences except for the 1518 byte frame size where VyOS outperforms pfSense with a difference of 129-139 Mbit/s.

6.2 Latency

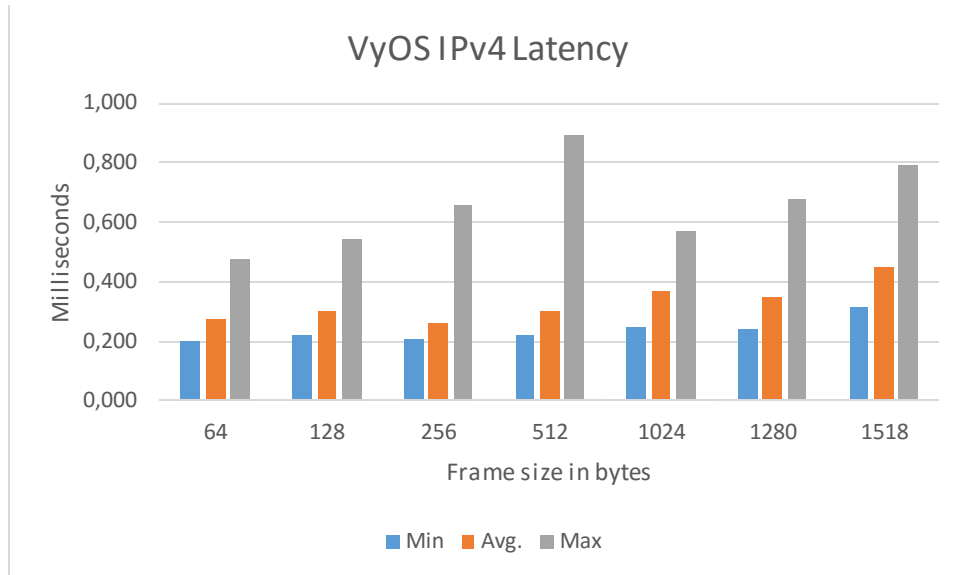


Figure 9 VyOS IPv4 Latency

Figure 9 shows the latency for VyOS IPv4 where the latency varies between frame sizes with no consistent pattern but with an overall increase with the frame size. There are quite high maximum values and differences between minimum and maximum which are caused anomalies of high latency readings which are not common.

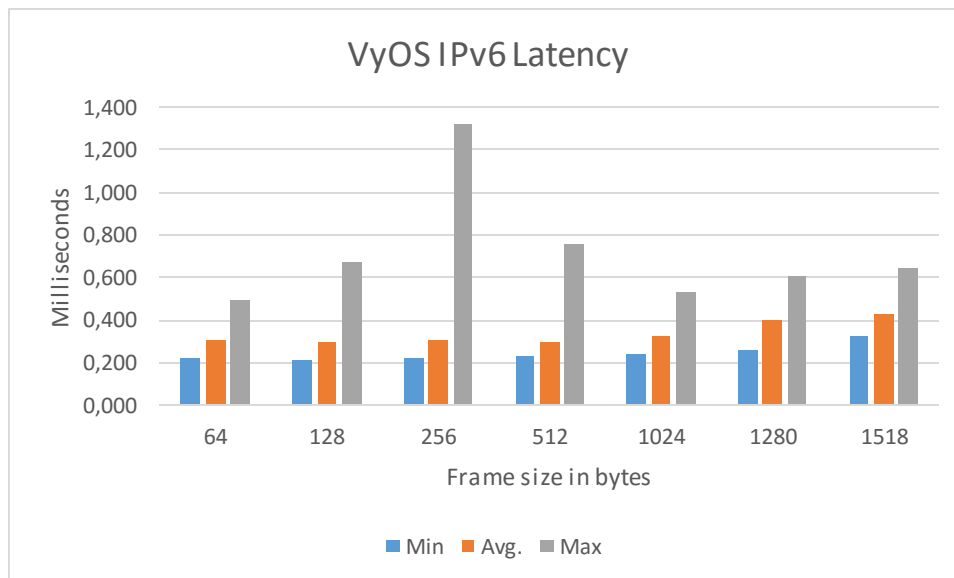


Figure 10 VyOS IPv6 Latency

Figure 10 shows the latency for VyOS IPv6 where the data of IPv6 is similar but has even bigger anomalies in terms of high values.

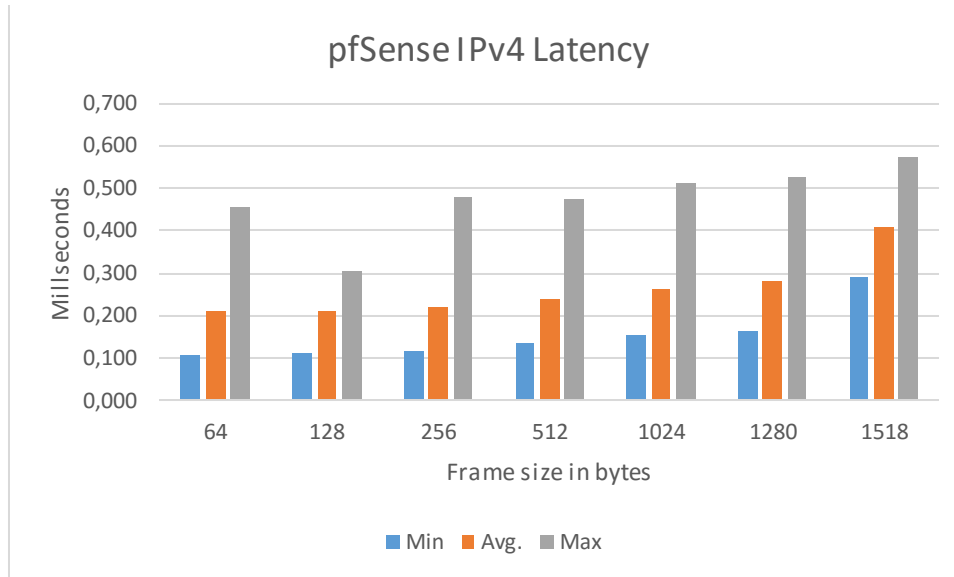


Figure 11 pfSense IPv4 Latency

Figure 11 shows the latency for pfSense IPv4 where there is a constant rise in latency in the increase of frame size. There is also the occurrence of high value anomalies.

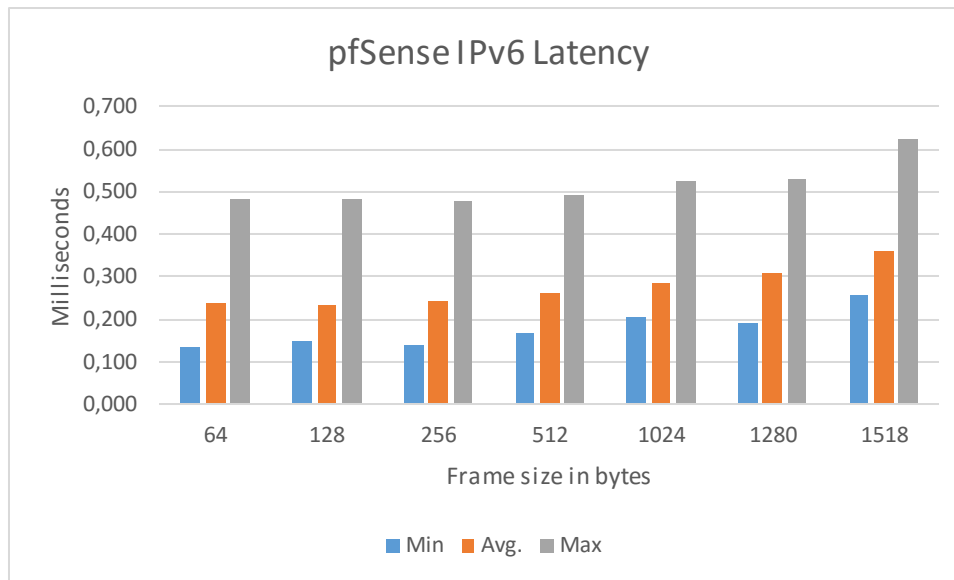


Figure 12 pfSense IPv6 Latency

Figure 12 shows the latency for pfSense IPv6 where similar to IPv4 there is a constant rise in latency in the increase of frame size. There is also the occurrence of high value anomalies which are generally higher than on IPv4.

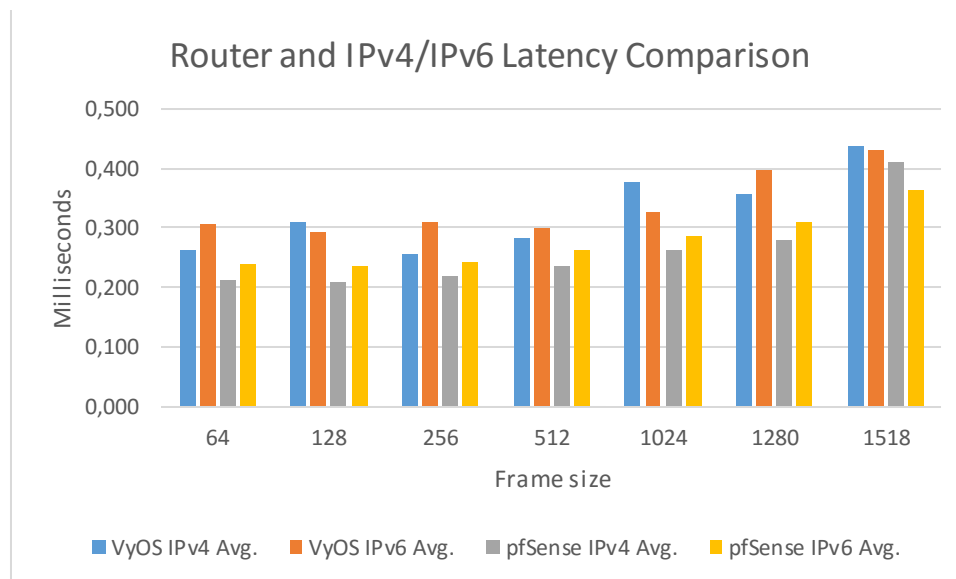


Figure 13 Router and IPv4/IPv6 Latency Comparison

Figure 13 shows average latency for both routers where the latency of pfSense is lower in all frame sizes an IP protocol variations compared to the latency of VyOS. Genereally IPv4 has lower latency than IPv6 except for the frame size of 1518 bytes for both routers and 128 byte and 1024 byte frame size for VyOS.

6.3 Frame loss rate

The results of the frame loss experiment were all at 0% frame loss between all tests and are therefore not presented in graphical form.

6.4 Theoretical Study

Here are the results of the theoretical study of security and other desired features.

6.4.1 NAT

VyOS has support for NAT and also the IPv6 counterpart NPTv6. NPTv6 (Network Prefix Translation) is a form of NAT for IPv6 that can be used for example multihoming (VyOS, 2015b).

Both source and destination NAT is supported (VyOS, 2015a). Specific rules for source NAT can be set per network and interface by setting the internal IP address that are to be translated, the outgoing interface and the external address what are to be translated to. Destination NAT can be set up using similar methods by defining incoming interface, protocol and port and the internal address of which the traffic should be forwarded to. All of the configuration of the NAT and NPTv6 is done via entering specific commands in to a CLI (Command Line Interface) according to the VyOS configuration syntax.

PfSense support both source and destination NAT but has no mentioning of the IPv6 counterpart NPTv6 (pfSense, 2014). The NAT configuration is done via a web interface. If an address pool is used for translating internal addresses there are different options on how the different addresses are chosen including: Round Robin, Random and limited by Bitmask.

6.4.2 DHCP

DHCP is present both as a server service and the option to forward DHCP packages as a relay. Both routers have this feature and it is configured through command line on VyOS and through the web GUI on pfSense. Both routers also have the IPv6 equivalent DHCPv6 which can be enabled.

6.4.3 Firewall

The firewall in VyOS uses the netfilter firewall for Linux for packet filtering. The firewall has support for groups of ports, addresses as well as interface or zone based filtering. However the group feature only works on IPv4 and not on IPv6. Firewall rules are written as commands and are evaluated from top to bottom.

The firewall in pfSense are configured by the web GUI and has more alternatives as to how to apply the rules such as date and time ranges. The firewall rules can be applied to groups and interfaces. It can also be specified if the rule applies to IPv4 or IPv6. The rule settings can be inverted and provides many other options to specify a rule.

6.4.4 VPN

VyOS and pfSense both have the option of configuring a VPN over IPsec. They both have specific rulesets which can be configured for the VPN.

6.4.5 Quality of Service

VyOS uses tc (Traffic Control), a Linux command part of iproute2, as the backend of its quality of services features (VyOS, 2015c). It provides different choices of network scheduling algorithms for shaping the network traffic including hierarchical token bucket and hierarchical fair-service curve.

7 Analysis

Looking at the throughput of VyOS Ipv4 (Figure 1) there is constant rise of throughput with increasing frame sizes but also a drastic increase in difference between minimum and maximum values. This difference is even higher when looking at the throughput of VyOS IPv6 (Figure 2) with a difference of 90Mbit/s in the largest frame size. When comparing the two IP versions there is not a clear superior version looking at the data. IPv4 outperforms or equal IPv6 in all frame sizes except two, 128 and 1280, at which IPv6 outperforms IPv4. The differences are not that big and not enough to draw a conclusion of which is the better protocol in terms of throughput.

The throughput of pfSense has major anomalies of low values in throughput of the higher frame sizes 1280 bytes and 1518 bytes. This is seen on both IPv4 and IPv6. These low values are not common and can therefore be considered anomalies and since values that low are not frequent in the results there are not any major impacts on the average values. There is not much of an increase in throughput between 1280 and 1518 in either of the IP versions. When comparing the IP versions one can see that IPv4 is superior or equal to IPv6 in all frame sizes except 1024 bytes. In the larger frame sizes IPv4 is substantially better than IPv6 beating it by 15 Mbit/s. Overall IPv4 outperforms IPv6 in terms of throughput using pfSense.

Comparing the two routers average throughput values one can see that they are quite equal until you reach the larger frame sizes where on 1518 bytes VyOS beats pfSense with values as high as 139 Mbit/s. Considering this one can declare that VyOS performs better than pfSense with large frame sizes under these conditions.

The latency of VyOS IPv4 increases with frame size and suffer from high max values which are not consistent and also not frequent in the data. The result of IPv6 is similar but the high anomalies are even greater. When comparing IPv4 and IPv6 there is no consistent winner in terms of low latency. The protocol with the lowest latency differs between frame sizes and no protocol version seems superior to the other

Pfsense latency has similar problems with high value anomalies with the ones in IPv6 being generally higher. When comparing IPv4 and IPv6 the IPv4 protocol has overall lower latency between frame sizes except for on 1518 bytes on which IPv6 has the lower latency of the two. But overall IPv4 can be seen as the superior protocol version in terms of latency on pfSense.

Comparing the two routers there is a clear difference with pfSense having overall lower latency on all frame sizes and protocol versions. The superior router under these conditions in terms of latency is clearly pfSense.

When looking at the values of frame loss rate which was a consistent 0% across both routers on both protocols one cannot draw any clear conclusions. Under these conditions they performed equally but it might have been the way the experiment was designed or other factors. No superior router or protocol can be declared. However, frame loss is not something that is desired so the results should be seen as positive for the different protocols and routers.

Looking at the different features they both have all of the desired features but with different options and limitations. VyOS has support for NPTv6 which pfSense has not. DHCP features are equal. Basic firewall settings are equal on both routers but when you start to look at more advanced rules pfSense has a better selection of options than VyOS has without installing extra software.

8 Conclusion

The aim of this study was to evaluate performance and compare IPv4 and IPv6 as well as security and other features that can aid someone when choosing an open source software router. The experiment was carried out and produced results from both routers and both protocols. The theoretical study was also carried out and produced a compiled summary of desired features.

The results of the performance experiment shows that there are no huge difference between IPv4 IPv6. There are some differences and IPv4 still outperforms IPv6 by small margins but not by much. It's not big enough margins to reject the use of IPv6. Between the routers the VyOS router outperformed pfSense in terms of throughput but pfSense had lower latency values than VyOS. There is not enough basis to say that one router outperformed the other looking at these results. There were some differences but no router outperformed the other in all of the tests.

In terms of features both routers had all of the desired functionality declared in this study. The degree of options of customization varied with pfSense often having more options handy and easily accessed than VyOS which required a bit more tinker to get to the same level of functionality. With the two routers having different user interfaces it, in the end, comes down to personal preference when choosing which router fits the need of interested party.

As a company or individual looking for an open source router with IPv6 functionality either of these router would be a good choice. Both routers state that they support IPv6 and has documentation on their websites on how to use it. Compared to many other popular open source router distributions which do not have full IPv6 support these two routers had good support without sacrificing other features. IPv6 performed okay compared to IPv4 on both routers so there is not a huge sacrifice in performance if you want to use IPv6 before IPv4. Depending on specific demands on network performance such as low latency or high throughput a company or individual can using these results make an educated choice of an IPv6 ready open source router distribution.

9 Discussion

This study was carried out as both an experiment and a theoretical study. The experiment delivered some results which can be used in different ways depending on what kind of requirements you have on your network environment. The theoretical study would have benefited from some hands-on experiments to evaluate the features more in-depth. As the experiment took more time than expected, less time were left to perform the theoretical study.

The frame loss experiment would've needed more evaluation before being carried out. The topology could've been expanded with more devices and performing the experiment during non-optimal situations to get data when frame loss would occur.

10 Future Work

In the future a more thorough test with more routers, number of tests, and a more in-depth analysis of desired features could be performed. The experiment could benefit from being run more times and under different circumstances to find more comparable results.

Many routers evaluated when making the choice of which routers to the study of there were many that only had partial support for IPv6 and therefore had to be omitted. In a future study, when these routers has full IPv6 support, new studies with similar performance experiments can be performed to how well their implementation of IPv6 compares to their implementation of IPv4. These results can then be compared to the routers in this study and see if there are any performance differences among the routers.

References

- Bolla, R. & Bruschi, R. (2013). An open-source platform for distributed Linux Software Routers. *Computer Communications*. 36 (4). p.pp. 396–410. Available from: [Accessed: 15 June 2015].
- Bradner, S. (1991). *Benchmarking Terminology for Network Interconnection Devices*. [Online]. 1991. Available from: <https://tools.ietf.org/html/rfc1242>. [Accessed: 8 April 2015].
- Cerri, D. & Fuggetta, A. (2007). Open standards, open formats, and open source. *Journal of Systems and Software*. 80 (11). p.pp. 1930–1937. Available from: [Accessed: 15 June 2015].
- Cisco (2007). *Performance-Comparison Testing of IPv4 and IPv6 Throughput and Latency on Key Cisco Router Platforms*. [Online]. 2007. Cisco. Available from: http://www.cisco.com/web/strategy/docs/gov/IPv6_Performance_AB.html. [Accessed: 15 June 2015].
- Dell, P. (2010). Two economic perspectives on the IPv6 transition. *Info : the Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media*. 12 (4). p.pp. 3–14. Available from: [Accessed: 15 June 2015].
- DistroWatch (2015a). *DistroWatch.com: About DistroWatch*. [Online]. 2015. Available from: <http://distrowatch.com/dwres.php?resource=about>. [Accessed: 14 June 2015].
- DistroWatch (2015b). *DistroWatch.com: DistroWatch Page Hit Ranking*. [Online]. 2015. Available from: <http://distrowatch.com/dwres.php?resource=popularity>. [Accessed: 14 June 2015].
- Fahlesson, P. (2013). *ROUTERMJUKVAROR BASERADE PÅ ÖPPEN KÄLLKOD : Jämförelsestudie mellan open source routrar*. [Online]. Available from: <http://his.diva-portal.org/smash/record.jsf?pid=diva2:630522>. [Accessed: 15 June 2015].
- Hancock, B. (1995). Attacking network routers. *Network Security*. 1995 (9). p.pp. 11–12. Available from: [Accessed: 15 June 2015].
- Hoover, J.N. (2006). Open Source The Network. *InformationWeek*. (1079). p.p. 67. Available from: [Accessed: 15 June 2015].
- Jakobson, F. (2014). *Open source routing software : A comparative study of open source software routers*. [Online]. Available from: <http://his.diva-portal.org/smash/record.jsf?pid=diva2:726337>. [Accessed: 5 March 2015].
- Levin, S.L. & Schmidt, S. (2014). IPv4 to IPv6: Challenges, solutions, and lessons. *Telecommunications Policy*. 38 (11). p.p. 1059.

- Mandic, D. (2014). *IPv6: Övergångsmekanismer och relaterade säkerhetsproblem*. [Online]. Skövde: University of Skövde. Available from: <http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-9568>. [Accessed: 5 March 2015].
- Manuel Kasper (2015). *m0n0wall - End of the m0n0wall project*. [Online]. 15 February 2015. Available from: http://m0n0.ch/wall/end_announcement.php. [Accessed: 14 June 2015].
- McQuaid, J. & Bradner, S. (1999). *Benchmarking Methodology for Network Interconnect Devices*. [Online]. 1999. Available from: <https://tools.ietf.org/html/rfc2544>. [Accessed: 6 April 2015].
- Open Source Initiative (n.d.). *The Open Source Definition*. [Online]. Available from: <http://opensource.org/osd>. [Accessed: 5 March 2015].
- pfSense (2014). *Introducing pfSense - PFSenseDocs*. [Online]. 2014. Available from: https://doc.pfsense.org/index.php/Introducing_pfSense. [Accessed: 27 May 2015].
- Shiau, W.-L., Li, Y.-F., Chao, H.-C. & Hsu, P.-Y. (2006). Evaluating IPv6 on a Large-scale Network. *Comput. Commun.* 29 (16). p.pp. 3113–3121.
- Untangle (2013). *IPv6 - UntangleWiki*. [Online]. 2013. Available from: <http://wiki.untangle.com/index.php/IPv6>. [Accessed: 14 June 2015].
- VyOS (2015a). *Feature list - VyOS*. [Online]. 2015. Available from: http://vyos.net/wiki/Feature_list#Firewall_and_NAT. [Accessed: 27 May 2015].
- VyOS (2015b). *How to do NPTv6 - VyOS*. [Online]. 2015. Available from: http://vyos.net/wiki/How_to_do_NPTv6. [Accessed: 27 May 2015].
- VyOS (2015c). *QoS - VyOS*. [Online]. 2015. Available from: <http://vyos.net/wiki/QoS>. [Accessed: 15 June 2015].
- Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B. & Wesslén, A. (2012). *Experimentation in Software Engineering*. 2012 edition. New York: Springer.

Appendix 1 - Summary

This study compares two routers, a networking device used to forward packages on computer networks which are open source distributions and can be freely downloaded and distributed. The routers were compared in terms of performance of the current Internet Protocols IPv4 and IPv6. IPv4 is the most widely used version today but there is a need to start using IPv6 in the future. The study aims to make the choosing process for companies and individuals seeking a open source router distribution with IPv6 support easier.

The routers were chosen based on specific delimitations with IPv6-support and being open source being the most important ones. Two routers, VyOS and pfSense, were selected based on the delimitations. The routers were then compared in an experiment as well as a theoretical study comparing security and other features.

The results of the experiment showed small differences between IPv4 and IPv6 on both routers with IPv4 performing slightly better. Between the routers there some differences with the VyOS router outperforming pfSense in terms of throughput but pfSense had lower latency values. Depending on the requirements for a specific network environment the results of this study could be used to pick an IPv6-enabled open source router distribution that fits a specific scenario.