Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2016, Vol. 8, No. 3

Comparative Study of a Router Performance with IPv4 and IPv6 Traffic

Nikola Dobrinov, Lorena Parra[1], Laura Garcia[2], Oscar Romero[3]

Polytechnic University of Valencia.

Camino de Vera, s/n 46022 Valencia, (Spain)

E-mail: [1]loparbo@doctor.upv.es, [2]laugarg2@teleco.upv.es, [3]oromero@dcom.upv.es

Received: September 11, 2016 Accepted: October 20, 2016 Published: October 31, 2016

DOI: 10.5296/npa.v8i3.10190 URL: http://dx.doi.org/10.5296/npa.v8i3.10190

Abstract

Because of the growth of the number of devices that use the internet, the number of available IPv4 addresses has run out in most parts of the world. IPv6 was created to solve this problem but the migration progress is proceeding at a slower pace that it was expected. This is mostly due to the cost of changing the equipment to one that supports IPv6 and the cost of configuring these devices. Knowing the aspects of a router configuration that are affected by the performance of IPv6 is very important in order to improve the efficiency of IPv6 end facilitate the migration process. In this paper we perform several measures to detect which aspects of the configuration of a bottom and medium range router are affected by IPv6. Two different topologies were used and different combinations of IPv4 and IPv6 traffic are sent. In different test Access Control Lists or IPv6 Routing Extension Headers are used. CPU usage and maximum traffic rate are some evaluated parameters. The router performance is clearly affected by the IPv6 traffic is used, CPU usage increases and the maximum traffic rate decreases.

Keywords: IPv4; IPv6; Router; Cisco; Performance

1. Introduction

The number of IP addresses available in all the world is practically exhausted [1]. Asia and Europe were the first continents to run out of IPv4 (Internet Protocol version 4) [2] addresses and ARIN (American Registry for Internet Numbers) reported on 2015 that the United States of America had used all of its free IPv4 addresses. The limited number of IPv4 addresses was a problem detected several years ago. It contributed to the creation of IPv6 (Internet Protocol version 6) [3] in 1999 [4] to guarantee the availability of IP addresses in the future. IPv4 was created with a total of 4.294.967.296 available addresses, however, IPv6 has approximately 340 undecillion addresses in order to avoid a future address exhaustion.

In order to employ IPv6, network devices must have the correct configuration. However, many devices are not prepared to support IPv6. The migration to IPv6 involves a great cost to telecommunication companies, because they have to buy new equipment and they have to train their employees how to operate them [5]. This fact and the possibility to reuse IPv4 addresses using private addressing and NAT (Network Address Translation) has led to a slower IPv6 migration than it was thought [6]. Even so, the use of IPv6 is spreading all over the world driven by big companies like Google or CDN providers [7]. According to Google statistics over the number of users that employ IPv6, the figure has reached the 14% of the users in a period of time of seven years [8]. Among the countries with the most implementation of the IPv6 protocol we can find Belgium with a 58.87 % of implementation, Switzerland with a 49.86%, Germany with a 49.55% and Equator with a 47.03%, among others [9].

Since the beginning of the deployment of IPv6 there have emerged several connectivity and compatibility problems with equipment and software designed to work with IPv4. Also, we assume that IPv6 will require a greater consumption of resources, which implies a greater energy consumption [10]. Because of these motives and to detect how the use of IPv6 affects routers of bottom and medium range routers, we have performed a series of measures. In these measures we obtain how the performance level of IPv6 affects routers such as the router 1841 from Cisco.

In the present paper we develop a comparison of Cisco Router 1814 performance under different type of unicast IPv4 and IPv6 traffic under different conditions. The studied router is the most used on the enterprises and it was created when the IPv4 was the 100% of traffic in the networks. Our objective is to evaluate the suitability of that router in a future scenario with IPv6 traffic.

The rest of the paper is organized as follows. Section 2 describes the related work.. In Section 3 is detailed the performed test bench. In section 4 the obtained results are explained. Finally, section 5 summarizes this paper.

2. Related work

Since IPv6 was released there have been several studies comparing how IPv6 and IPv4 worked as well as their performance with different aspects. Mohd.Kahiril Sailan et al. [11]

compare IPv6 and IPv4 to determine the advantages of IPv6. The main difference between them is the length of the address. IPv6 has a 128-bit address in order to guarantee the existence of addresses for an extended period of time. There are other differences such as the differences found in header options, QoS or ARP (Access Resolution Protocol). They point out that the advantages of IPv6 are the large address space, improved security due to the obligatory use of IPsec (IP Security protocol), enhanced QoS support with the included labeled flows, simplified auto configuration with DHCP (Dynamic Host Configuration Protocol) and upgraded mobility support with mobile IPv6, which allows to maintain the same IP address when switching from link to link. They also compare different routers on the grade of support of IPv6 they have.

In [12] Roman Yasinovskyy et al. compare the performance of VoIP in IPv6 and IPv4 networks. Their results show that there is hardly any difference in performance between IPv6 and IPv4 for the tests they completed. To do their study they used a softphone running on a PC with no operating system. They conclude that the reduction of the overheads of the system and the application improves the quality of the voice for both IPv6 and IPv4. Shaneel Narayan et al. compare in [13] the performance of IPv6 and IPv4 between two Windows operating systems. The systems they use to perform their metrics are Windows XP and Windows Server 2003. For small sized packets they have found that there is a difference of throughput of 54% approximately. For big sized packets the difference obtained is of 10.4% for Windows Server 2003 and 12% for Windows XP.

Some of the measures on different technologies for IPv4 and IPv6 where focused on the delay. In [14] Mariya Veruko et al. compare the performance of Access Control List (ACL) implemented in IPv4 and IPv6 networks. They also measure the delay when ACLs are implemented over IPv6 and compare it with the delay results obtained after utilizing an IPv6-IPv4-IPv6 tunnel. The results show that the percentage of the increased delay is a 67% for IPv4 networks with either NAT or ACLs. For IPv6 network it starts with a 317% increased delay without any additional security and 367% with ACLs. For IPv6-IPv4-IPv6 tunnels the difference is a 60% with no ACLs and a 630% of increased delay with ACLs. Xiaoming Zhou et al. performed delay measured as well in [15]. They compare the delay and packet loss between IPv6 and IPv4 analyzing over 600 end to end pats. They conclude that native IPv6 has more delay that IPv4. IPv6 in IPv4 tunnels are the ones with more delay, so the authors determine that only native IPv6 should be used instead of IPv6 in IPv4 tunnels.

There are not any articles that compare the differences of a router performance between IPv6 and IPv4 and propose the optimal configuration. Other articles propose optimal configuration for other technologies such as [16], where Wei Jiang et al. propose an automatic router configuration to access control. They use DC and RDC method to configure border routers of an ISP (Internet Service Provider) to send an unsafe IP address through a null route. They also have created a comprehensive NACS (Network Access Control System) management system to decrease the network management load in large scale networks. In our article we perform several measures to determine the performance of Cisco 1841 routers with IPv6 and IPv4.

3. Test bench

In this section, we are going to describe at first the used equipment, both software and hardware features. The details of the performed test, as topology or specific configurations are also explained.

First, the description of the employed devices is detailed. Two computers were used as a host to send and receive traffic. Both devices have the same features, they are dual core computers with 4Gb of RAM and Windows 7 operative system, their characteristics are described in Table 1. The other employed devices are two routers Cisco 1841 [17] with two10/100Mbps Ethernet ports and the following Cisco IOS C1841-ADVENTERPRISEK9-M Version 12.4(25d). The specifications of the routers are detailed in Table 1. It is important to know that the employed router, Cisco 1841, use different procedures to process traffic. Unicast IPv4 traffic is processed at hardware level while multicast IPv4 and all IPv6 traffic are processed at software level.

Different software was used to generate traffic in one host, to measure the received traffic in the other host and to observe the traffic along the network. The software IP Traffic – Test and Measure version 2.7 from ZTI Communications has been used to generate different traffic in the majority of the test. It can generate UDP and TCP traffic at different velocities as 10/100/1000Mbps for up to 16 simultaneous connexions. IP Traffic also gives statistics of a set of parameters at the source and destination as: instant traffic rate, volume of data transmitted so far, rate of packets per second (pps), number of packets sent and loss rate at destination host. To calculate the loss rate the program considers the sequence number of the sent packets. The second employed program is the Xcap version 1.0.2 even though it has low capacity to generate large volumes of traffic it supports extension headers for IPv6 protocol. This program was utilized when we work with any extension headers. Finally Wireshark was used as a sniffer to monitor the generated traffic of the previous programs and ensure that they are working correctly. It has been used also to record the reception times of some packets.

Table 1. Features of employed devices

Features of Host	IOS	Windows 7 Professional Service Pack 1 (32 bits)
	Processor	Intel(R) Core(TM) i3-2120 @ 3.30GHz
	Number of Processors	2
	RAM Memory	4.00 GBytes
	Grafic card	Intel(R) HD Graphics
	Hard Disc	112 GBytes (63GBytes available)
	Network Interface Controller	Realtek PCIe GBE Family Controller
Features of Router	DRAM Memory	DIMM 256 MBytes default (384 MBytes maximum)
	Flash Memory	64 MBytes default (128 MBytes maximum)
	Ethernet Ports	Two 10/100 Mbps
	Processor	RM5261A-256H @ 250 MHz, Controlador Marvell GT96103A
	IOS	Cisco IOS Software C1841-ADVENTERPRISEK9-M, Version 12.4(25d)

Two different topologies were employed. Topology A has two hosts and one router 1841, the host generates or receives traffic or both. The connections between the hosts and router were done with Ethernet cable from the Network Interface Card (NIC) of each host to the Fast Ethernet (Fa) connection of the router. The topology is shown in Fig. 1 and the IP information is detailed in Table 2. Topology B is composed by two hosts and two routers, as in topology A all the connections are done with Ethernet cable. The topology is shown in Fig. 2 and the IP information is detailed in Table 3. The routing tables of both topologies can be seen in Table 4 and Table 5.

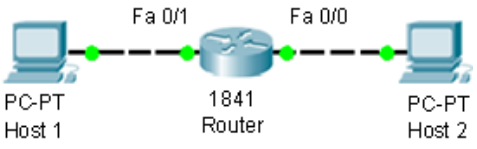

Figure 1. Topology A

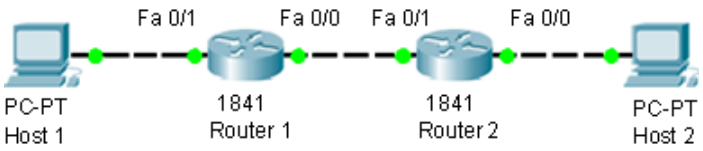

Figure 2. Topology B

Table 2. IP information of topology A

		IP	Subnet Mask
Host 1	IPv4	192.168.1.7	255.255.255.0
	IPv6	2001:200:0:2::2	/64
Host 2	IPv4	192.168.0.5	255.255.255.0
	IPv6	2001:200:0:1::2	/64
Router: Fa 0/0	IPv4	192.168.0.1	255.255.255.0
	IPv6	2001:200:0:1::1	/64
Router: Fa 0/1	IPv4	192.168.1.1	255.255.255.0
	IPv6	2001:200:0:2::1	/64

Table 3. IP information of topology B

		IP	Subnet Mask
Host 1	IPv4	192.168.1.7	255.255.255.0
	IPv6	2001:200:0:2::2	/64
Host 2	IPv4	192.168.0.5	255.255.255.0
	IPv6	2001:200:0:1::2	/64
Router 1: Fa 0/0	IPv4	192.168.3.1	255.255.255.252
	IPv6	2001:200:0:3::1	/64
Router 1: Fa 0/1	IPv4	192.168.1.1	255.255.255.0
	IPv6	2001:200:0:2::1	/64
Router 2: Fa 0/0	IPv4	192.168.0.1	255.255.255.0
	IPv6	2001:200:0:1::1	/64
Router 2: Fa 0/1	IPv4	192.168.3.2	255.255.255.252
	IPv6	2001:200:0:3::2	/64

Table 4. Routing table Router 1 and 2 Topology B

	IP	Subnet Mask	Next hop	Interface
Router 1	192.168.0.0	255.255.255.0	192.168.3.2	Fa 0/0
	192.168.1.0	255.255.255.0	Direct	Fa 0/1
	192.168.3.0	255.255.255.252	Direct	Fa 0/0
	2001:200:0:1::	/64	2001:200:0:3::2	Fa 0/0
	2001:200:0:2::	/64	Direct	Fa 0/1
	2001:200:0:3::	/64	Direct	Fa 0/0
Router 2	192.168.0.0	255.255.255.0	Direct	Fa 0/0
	192.168.1.0	255.255.255.0	192.168.3.1	Fa 0/1
	192.168.3.0	255.255.255.252	Direct	Fa 0/0
	2001:200:0:1::	/64	Direct	Fa 0/0
	2001:200:0:2::	/64	2001:200:0:3::1	Fa 0/1
	2001:200:0:3::	/64	Direct	Fa 0/0

Table 5. Routing table Router 1 Topology A

IP	Subnet Mask	Next hop	Interface
192.168.0.0	255.255.255.0	Direct	*Fa* 0/0
192.168.1.0	255.255.255.0	Direct	*Fa* 0/1
2001:200:0:1::	/64	Direct	*Fa* 0/0
2001:200:0:2::	/64	Direct	*Fa* 0/1

Now the considerations about the measures are detailed. Different combinations of IPv4 and IPv6 traffic were sent, 100% IPv4 and 0% IPv6 (100/0), 90% IPv4 and 10% IPv6 (90/10), 50% IPv4 and 50% IPv6 (50/50), 10% IPv4 and 90% IPv6 (10/90) and 0% IPv4 and 100% IPv6 (0/100). The padding used on frames UDP went from 1 Byte to 1472 Bytes and are composed by hexadecimal values of 5 and A, 0101 and 1010 that avoids Bit Stuffing. All the traffic is sent in unidirectional flow unless otherwise is indicated for a specific test. The Maximum Transfer Unit (MTU), on Ethernet networks this value is 1500 Bytes plus the Ethernet Heather, 18 Bytes. For our test the MTU is 1518 Bytes. One of the used parameters to evaluate the effects of different traffic on the router is the use of CPU (%) of the router. It is obtained from the Command Line Interface (CLI) using the command *show processes cpu history*. It gives information about the use of CPU at the last 60s, 60min and 72h, only the data related with the last 60s is used. With the values of the last 60s the arithmetic mean was calculated and this is the value of CPU usage. In the following test other of the studied parameters is the maximum traffic, traffic is expressed in Mbps and it represents the traffic on the Application layer.

Several test were done, first are detailed the test performed with Topology A. The tests were aimed to find the limit of the router capacity under different traffic conditions. In the first test frames of different length from 64 Bytes for IPv4 or 67 Bytes for IPv6 until 5958 Bytes were transmitted and the maximum routing traffic is recorded. The test is done with different combinations of IPv4 and IPv6 traffic. Frames up to 1518 Bytes were fragmented. The second test is aimed to evaluate the use of CPU using a frame of 1518 Bytes and different throughput, from 10% to 95%. This scenario is repeated for different combinations of IPv4 and IPv6 traffic. The evaluation of differences on packets per second (pps) and CPU usage with packets of IPv4 and IPv6 are send together is detailed in third test. Frames of different size were used and different combinations of IPv4 and IPv6, 100/0, 50/50 and 0/100, traffic were generated. The forth test evaluates the frame loss rate. The previous tests were aimed to evaluate the capacity of the Router Cisco 1841 but in this test the aim is to evaluate the performance after this limit, where the appearance of frame loss is expected. With this purpose 4 different size of frame from 64 bytes to 1518 bytes were used with throughput varying from 10 Mbps to 95Mbps with traffic of IPv4 and IPv6. The frame loss rate and the CPU usage were analysed. The evaluation of router performance under bidirectional throughput rate with different frame size and different combination of IPv4 and IPv6 traffic is shown in sixth test. The maximum traffic and the CPU usage were evaluated and compared with the same test on unidirectional traffic. The sixth test was performed with Topology A to study if there was any difference between resetting the router from the software or from the hardware. Host 1 sent IPv4 traffic to host 2. On host 2 during the transmission the router was reset from the CLI, software reset, and from the switch, hardware reset. The transmission stops during the time that the router needs to reset; this time is measured using Wireshark to monitor the traffic that arrives to the host 2. Five repetitions were done of each reset procedure. The seventh test is focused on the effect of different IPv4 and IPv6 traffic on the inter packet delay. Frames of 1518 Bytes were transmitted from host 1 to host 2, on host 2 Wireshark is used to capture data. More than 10,000 packets were captured and the

frame.time_relative data were analysed. It has information about the reception time of each packet, assuming 0s as the reception time of the first packet. Comparing the time between the reception of packet *x* and the reception of packet *x-1* is possible to calculate the inter packet delay. The transmission is repeated with different throughput, from 10 Mbps to 95 Mbps and with IPv4 traffic, IPv6 traffic and with a combination of them 50/50. The last test entails the use of ICMP protocol and the forwarding of "*Echo Request*" from host 2 to router and the reception of "*Echo Reply*" is recorded by Wireshark at host 2. Different throughputs were tested, from 100pps to 4000pps, and different sizes of ICMP Data, from 100 Bytes to 1472 Bytes for ICMPv4 [18] and ICMPv6 [19]. The CPU usage was the evaluated parameter.

Other tests were done to evaluate the effects of the Access ACL. Frames of 1518 were sent from host 2 to host 1. The tests of ACLs were done without any ACL, with only two ACLs (one for IPv4 and one for IPv6) of a single line that permits the traffic and finally with two ACLs of 25 lines. At the ACL with 25 lines, the first 24 lines deny traffic to the IPs that do not contain the assigned IP, the last line permits traffic to the destination IP to ensure that the router must read all the 25 ACL lines. In the cases with ACLs they can be applied at Fa0/0 in, at Fa0/1out or at both interfaces. These entire tests were done with combinations of traffic of IPv4 and IPv6 of 100/0, 50/50 and 0/100.

The last test with the Topology A is focused on the effects of IPv6 Extension Headers. For this test the Xcap software is used for IPv6 traffic generation with different extension headers. Frames of a fixed length are used, 1280 Bytes, in order to add extension headers of different size without exceeding the 1518 Bytes. The traffic is sent from 100 pps to the higher rates until the router reaches the 100% of CPU usage. To route the packet the router just needs to read the principal header and there is no need to read the extension headers. To force the router to read all the extension headers an ACL is used. The ACL only permits the pass of UDP traffic, and then the router must read all the extension headers until the camp Next Header where the value associated to UPV is placed. Different extension headers were used, four cases are examined. In the first case, one extension header (Hop-by-Hop) without ACL is used and after with the ACL. Next, traffic with four extension headers in the next order Options Header, Routing Header, Fragment Header, Destination Options Header and the ACL is used. The last case is the use of 20 extension headers of the type Destination Options Header in combination with the use of ACL. The traffic is sent from 100 pps to the higher rates until the router reaches the 100% of CPU usage.

Two main different tests were done with the Topology B, the first one aimed to evaluate the packet fragmentation. The second one is focused on IPv6 Routing Extension Header. Firstly, for the packet fragmentation test, IPv4 traffic is used. With IPv6 traffic the packets are fragmented in the host while in IPv4 the packets are fragmented in the router. With the 1841 Router is not possible to configure the MTU, but it is possible to set a MTU at network level. Levels of 1500, 1000, 500 y 68 Bytes are set as MTU, with the highest level no fragmentation will be done. The lowest level, 68 Bytes, is the minimum that can be set on Cisco devices. For this test the traffic was sent from host 1 to host 2 and the MTU limitation was established from router 1 to router 2. Different sizes of frames were used to generate the traffic. The CPU

usage and the pps in router 1 were measured to find when the packets were fragmented and when they were not. After this test, a new assay was done to measure the Fragments per Second (fps). The aim was to measure the cost of fragmenting the entering frames. A constant rate of 5000pps was stablished at the router entrance in order to have a constant cost of packets processing. Hence, the changes on the CPU usage will be related only to fragmentation. A MTU of 100 Bytes was set to force the high fragmentation. Different traffic was generated, from frames of 118 Bytes to 918 Bytes. The usage of CPU and the fps were the evaluated parameters. The second test is aimed to study the effects of IPv6 Routing Extension Headers (REH), Xcap was used for unidirectional or bidirectional traffic generation. The routing header was used to define the route of the packets. The employed routing header is shown in Table 6. The traffic was sent from host 1 to host 2 with different frame size. For this test the minimum frame size was 128 Bytes. The frame of 67 Bytes was not used because it does not allow having the extension header. The maximum frame size used was 1514 Bytes, instead of 1518 like in the previous test because of the Xcap software limitations. Three different cases were analysed, first with unidirectional traffic with 1000pps rate, second with 5000pps rate and third with bidirectional traffic and 1000pps. These cases are repeated with the routing header and without it as a reference. The measured parameter was the CPU usage.

Table 6. Routing Header used for IPv6 Routing Extension Header tests

Principal Header IPv6		*Routing Header*	
Version	6	Next Header	11 = UDP
Traffic Class	0	Hdr Ext Len	32
Flow Label	0	Routing Type	0
Payload Length	70	Segments Left	2
Next Header	43 = Routing Header	Reserved	0
Hop Limit	64	Address[1]	2001:200:0:3::2
Source Address	2001:200:0:2::2	Address[2]	2001:200:0:1::2
Destination Address	2001:200:0:2::1		

4. Results

In this section the results of the different test are detailed. The section is divided into two subsections first subsection presents the results obtained with the test performed with Topology A. Second subsection presents the data of the tests with Topology B.

4.1 Tests with Cisco Router 1841

This subsection presents all the obtained data from the different test with the topology of two hosts and one Cisco Router 1841. First, the data about the maximum traffic routed at different frame size is analyzed. The results are shown in Fig. 3. As the frame size increases, the maximum traffic that the router is able to route increases. This is caused because the router must read the header for each packet. For the same traffic, the higher the packet size, the lesser time is consumed by the router reading headers. This relation is maintained until

packets of 1518 Bytes. For frames with higher size, 1522 and higher, the router needs to fragment the frames in the case of IPv4 traffic or by the host in the case of IPv6 traffic. From this point each packet is divided into two or more packets. The first one with the maximum frame size accepted in Ethernet technology, and another with the rest of Bytes.. Comparing the traffic with frame size of 1518 and 1522 Bytes we can see the downgrade of the routing capacity when almost the same information has the double of headers. The reduction is about 5.31% and 5.28% with 100/0 and 90/10, 37.63% with 50/50 and 34.59% and 33.33% with 10/90 and 0/100. The reduction is higher when the IPv6 traffic represents more than 10% of the traffic.

For the entire frame size is possible to see that the maximum traffic is the highest when the sent traffic corresponds to IPv4. As more IPv6 traffic is included the reduction on maximum traffic routed is higher. This is caused because the 1841 Router is prepared to work with IPv4 protocol and it has clear difficulties to work with IPv6 traffic. The headers of IPv6 traffic are longer that IPv4 headers. Next, the data of the test aimed to evaluate the use of CPU while router is routing frames under different throughputs. The data can be seen in Fig. 4, it is possible to see that the higher the throughput, the greater the CPU usage. The higher the traffic with the same frame size is, the higher number of packets must be processed and higher number of headers must be read by the router. By the other side, the use of IPv6 traffic increases the use of CPU. Again, the data illustrates that Router 1841 costs more to process IPv6 packets. The use of CPU to transmit IPv4 frame at 90Mbps (12%) is lower than to transmit 10Mbps of mixed 50% IPv4 and 50% IPv6 traffic (12.5%).

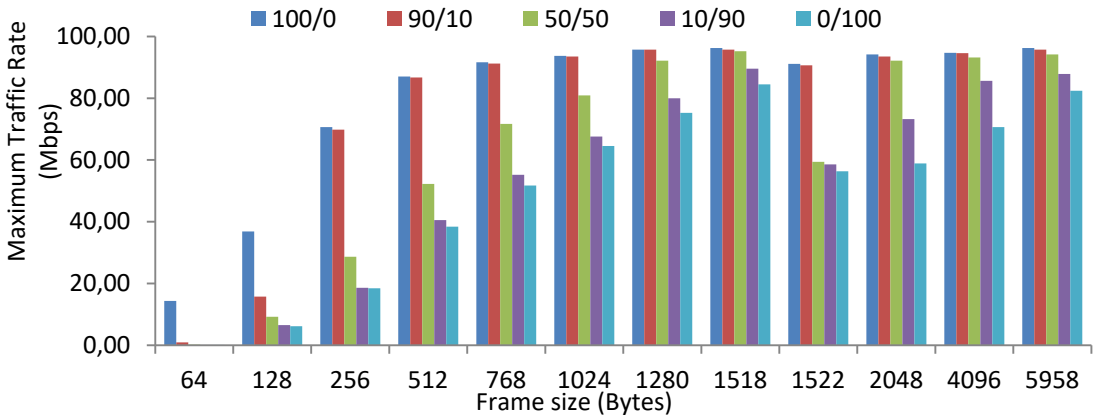

Figure 3. Maximum traffic with different frame size

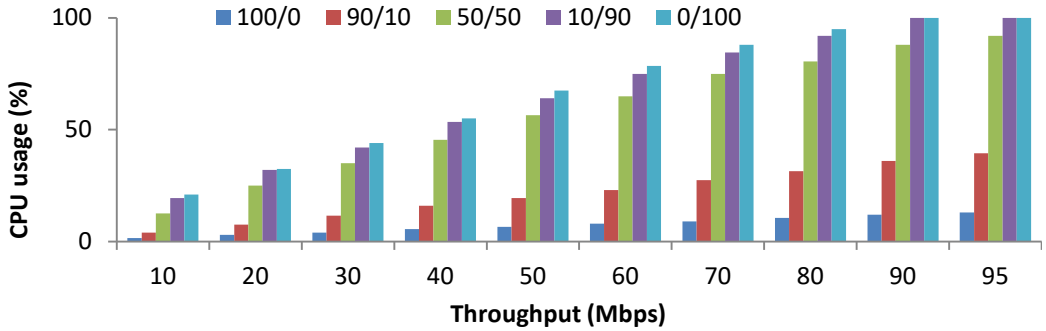

Figure 4. CPU usage (%) for different throughputs.

Regarding to the test where the pps and CPU usage were analysed under different types of traffic, the results can be seen in Fig. 5 and Fig. 6. Figure 5 shows the CPU usage. Two different tendencies can be observed, first the CPU usage when the traffic is composed only by packets with IPv4 protocol is lower than with IPv6 protocol or mixed traffic in all the cases. There are no differences on CPU usage when the traffic is only composed by IPv6 packets or with mixed traffic 50/50, in both cases the CPU usage is close to the maximum CPU capacity. The second tendency is the increase of CPU usage with the decrease of the frame size in IPv4 traffic; this effect is not seen in IPv6 traffic or mixed traffic. When the size of packets increase, fewer packets can be send before reaching the limit of maximum traffic. Traffic with fewer packets entails fewer headers that router must read and less CPU usage. This relation between frames size and CPU usage is not present with IPv6 traffic or mixed traffic. In Fig. 6 the pps reached with different frame size can be seen. As frame size increases the number of pps decreases. As it is explained above, the higher the frame size, the fewer the packets that can be routed before reach the maximum traffic limit for a certain frame size and no more packets are sent to avoid packets loss. This trend can be seen in all traffic, from IPv4 protocol, IPv6 protocol or mixed traffic 50/50. However, the reduction on pps is not the same for IPv4 and IPv6 traffic. We are going to compare the pps for a frame size of 128 Bytes and 1280 Bytes, 10 times higher. For IPv4 protocol to increase 10 times the frame size represents a drop of 83.5% of the traffic, while for IPv6 the reduction of the traffic is only a 35% and 50% for mixed traffic. The reduction is higher for IPv4 traffic. On the other hand, comparing frames of the same size with different protocols, the IPv4 traffic presents higher transfer rates in pps than mixed traffic or IPv6 traffic. It is because the headers of IPv6 are more complex than headers of IPv4 and the router needs more time to read them. This reduction is greater when the frame size is smaller, because the smaller frame size the more packets arrive to the router, therefore, more headers and more time spend reading them. For packets of 128 Bytes mixed traffic suppose a reduction of 66% of traffic rate on pps respect IPv4 traffic and IPv6 implies a drop of 38%. Nevertheless, with a frame size of 1024 Bytes the reduction is 6% with mixed traffic and 20% with IPv6 traffic.

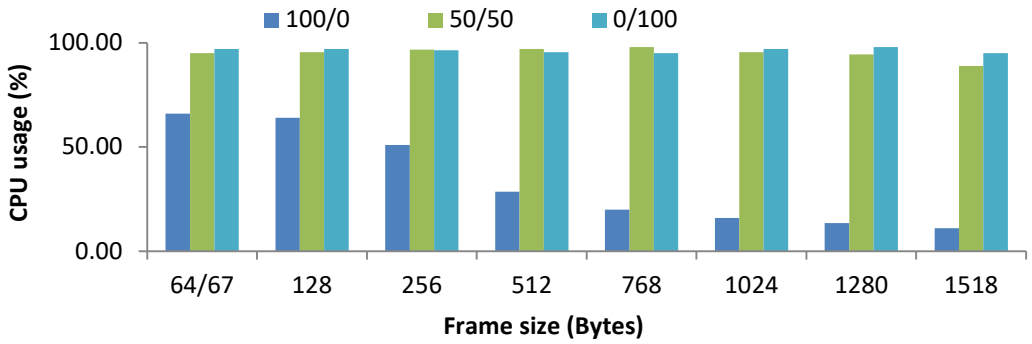

Figure 5. CPU usage (%) for different frame size

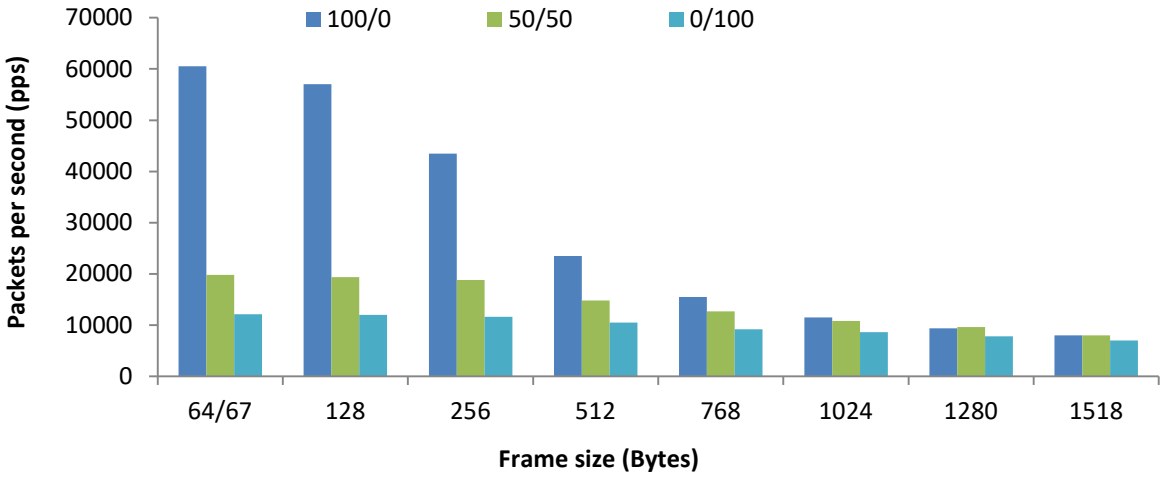

Figure 6. Traffic rate in pps for different throughputs.

Now, the results of tests aimed to evaluate the frame loss under different conditions are presented. This is the only test where there is frame loss. The CPU usage with different traffic can be seen in Fig. 7. Firstly, is possible to see that smaller frame size requires higher CPU usage. If we pay attention to the throughput of 10Mbps from frame size of 256 Bytes to 1518 Bytes we can see that the usage of CPU is 7%, 3.5% and 2% For IPv4 and 62.5%, 38% and 21.5% for IPv6. When the frame size is twice the CPU usage, it is increased by 50% and 57% in IPv4 and 60% and 56.5% in IPv6. Secondly, the CPU usage also increases linearly with the throughput until certain point, where the maximum traffic is reached, at this moment the router does not accept more traffic. From this point, there is frame loss and even though more traffic is sent from the host, no more traffic is read by the router and no more CPU is required. This point is reached for frames of 64 Bytes of IPv4 at 20Mbps and earlier for IPv6 at 10Mbps. From this point the CPU usage for IPv4 is set to 68% and 98% for IPv6. For frames of 256 Bytes is reached at 80 Mbps and at 20 Mbps for IPv4 and IPv6 respectively. From this point the CPU usage for IPv4 is set to 54% and 97% for IPv6. This limit is reached at 90 Mbps and 40 Mbps for IPv4 and IPv6 frames of 512 Bytes. From this point the CPU usage for IPv4 is set to 30% and 98% for IPv6. Finally, the highest frames, 1518 Bytes, are reached only in IPv6 at 90 Mbps and the CPU usage is 98%.

In all the cases IPv6 traffic reaches the maximum traffic before IPv4.These points represent the start of frame loss in Fig. 8. From these points forward the excess of traffic represents the frame loss, representing higher frame loss rate. Finally in this graphic is possible to see again that IPv4 traffic routing demands less processor capacity than IPv6 traffic. We are going to compare the CPU usage for all the traffics between IPv4 and IPv6, excluding the ones where CPU usage is higher than 95% in IPv4 or IPv6. The cost of sent IPv4 traffic, from the point of view of CPU usage, compared with IPv6 is approximately 10% (9.84%).

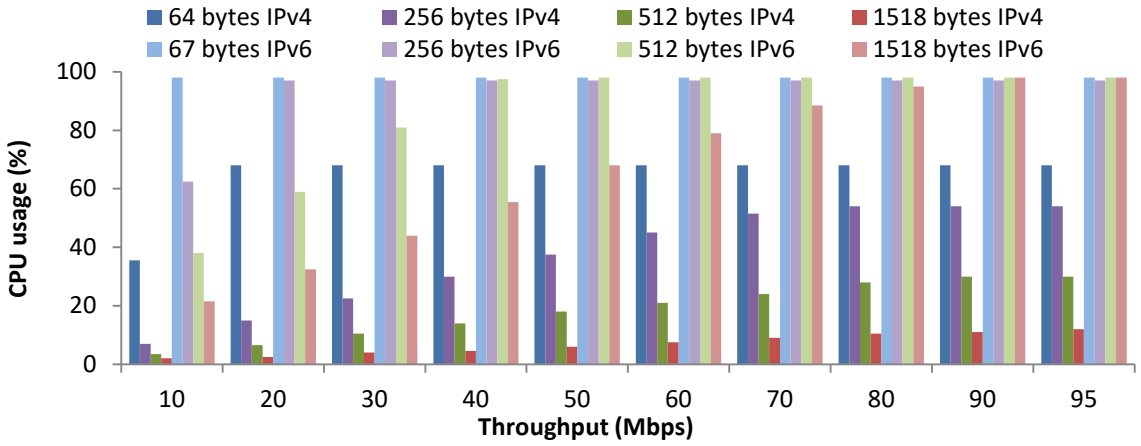

Figure 7. CPU usage (%) for different frame size and load lines

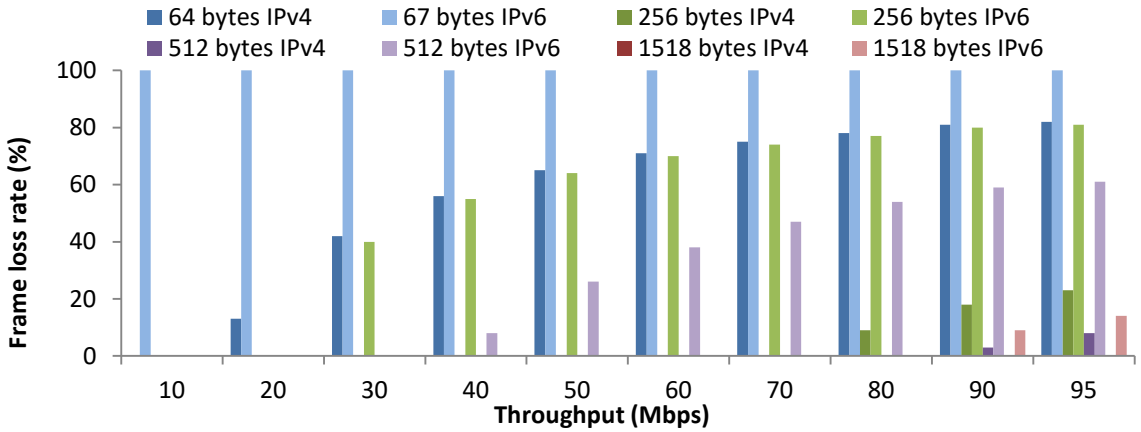

Figure 8. Frame loss rate for different frame size and load lines

The test with bidirectional traffic is analysed now. This is a very important test because in normal conditions the network transport data in both directions and the router must route traffic from and to both directions. When bidirectional traffic is generated the amount of traffic generated is the same for both directions. Fig. 9 and Fig. 10 represent the CPU usage and Maximum traffic (Mbps) for different frame size and for unidirectional and bidirectional traffic. The CPU usage decrease with the frame size and increase with the percentage of IPv6 traffic. Regarding to the maximum traffic, as in previous tests, higher frame size implies higher maximum traffic because of the fewer number of headers.

Comparing unidirectional traffic with bidirectional traffic, bidirectional traffic requires higher use of CPU when IPv4 protocol is used. This increase of CPU usage represents the 20% of the CPU because of it the router is able to archive the traffic, as can be seen in Fig. 10.

By the other side, with IPv6 protocol and mixed traffic in both cases, unidirectional and bidirectional, the CPU usage is near the 100%, see Fig. 9. Nevertheless the maximum traffic that the router can route for mixed traffic is lower with bidirectional traffic than for unidirectional traffic. The reduction in bidirectional traffic is near 50% of the traffic in unidirectional conditions.

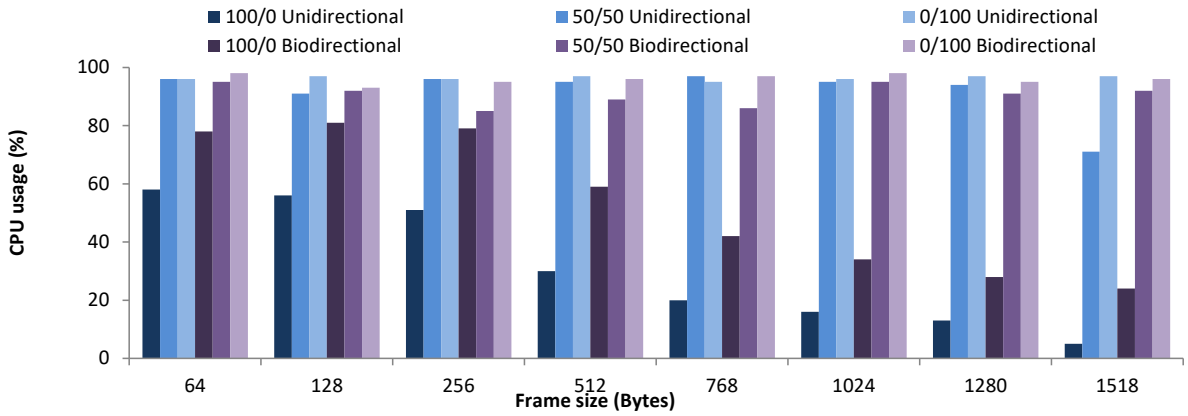

Figure 9. CPU usage (%) for different frame size and throughputs.

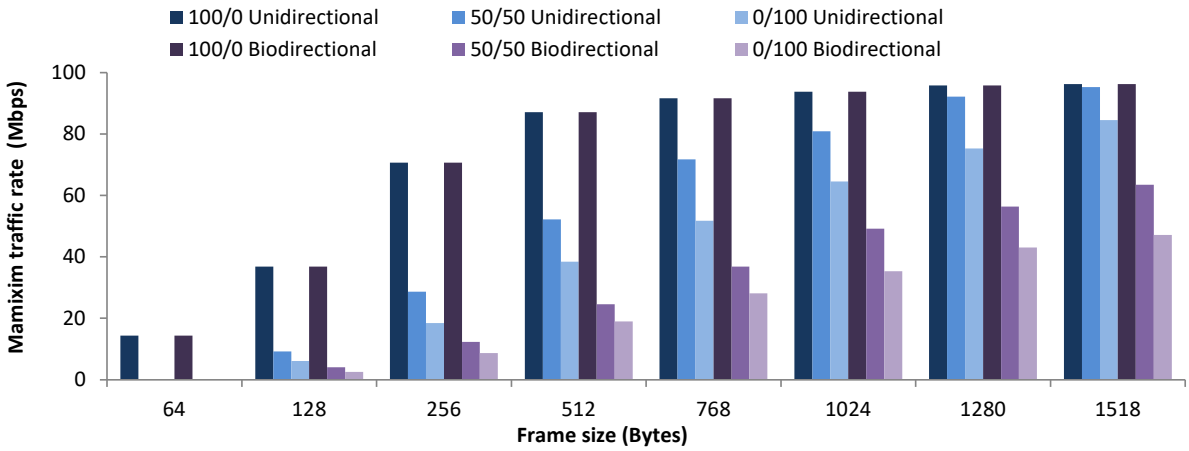

Figure 10. Maximum traffic for bidirectional and unidirectional data flow

The results of the sixth test, where the difference Software Reset Time (SRT) and Hardware Reset Time (HRT) was studied, are show in next. In this test 5 repetitions were done, that can be seen in Table 7. The mean reset time was 67.3s for software reset and 66.86s for hardware reset. However some statistical analyses have been done in order to know if the observed difference in the means is because of the different reset modes or it is because of the aleatory of the data. The statistical test employed is the ANOVA, before doing the ANOVA it is necessary to ensure that our data follows a normal distribution. A descriptive analysis of our data confirms that the kurtosis and skewness coefficients are between ±2, thus the data follows a normal distributions. The ANOVA result, see Table 8, is a p-value higher than 0.05 hence the observed differences is not statistically significant. It is possible to conclude that, there is no difference on resetting the router from CLI or from the switch button.

Table 7. Data of reset time for different trials

Trial	**1**	**2**	**3**	**4**	**5**
SRT (s)	67.5	67.8	66.9	67.5	66.8
HRT (s)	66.3	67.2	67.4	66.5	67

Table 8. ANOVA statistical test

Source	***Sum. of Squares***	***Df***	***Mean Square***	***F-Ratio***	***P-Value***
Inter groups	0.47524	1	0.47524	2.29	0.1684
Intra groups	1.6576	8	0.2072		
Total (Cor.)	2.13284	9			

Now the results of inter packet delay (IPD) tests are shown. First, it is important to mention that for the IPv6 traffic at 90Mbps and 95Mbps some packets were lost and this data is not considered for the analysis. As the frame size is fixed to 1518 bytes the time to transmit a packet at line rate will be fixed as well. The packets are transmitted uniformly, keeping the same delay between packets. The higher the throughput, the higher number of packets is transmitted in less time, therefore less IPD is observed. At low throughputs, 10 Mbps the IPD is 1.2ms. For higher throughputs, as 95 Mbps, the IPD is 10 times lower, 0.12ms. By the other side, no effects are found considering the different used protocols and the IPD.

The results of ICMP test are shown below in Fig. 12. The CPU usage increases with the packet size and with the increase of packets per second. For ICMPv4 small size as 100 Bytes the CPU usage is less than 10%, with frame size of 1000 Bytes the CPU usage is around 50% but for 4000 Bytes the CPU reaches up to 90%. However for ICMPv6 the increase is less pronounced, the CPU usage is approximately 5%, 30% and 60% for frames of 100 Bytes, 1000 Bytes and 4000 Bytes. The high CPU usage in relation with ICMP protocol can be used as a weak point for router security, for this reason the use of ICMPv6 can reduce this weakness. The use of ICMPv6 instead of ICMPv4 supposes a reduction of 33% of CPU usage.

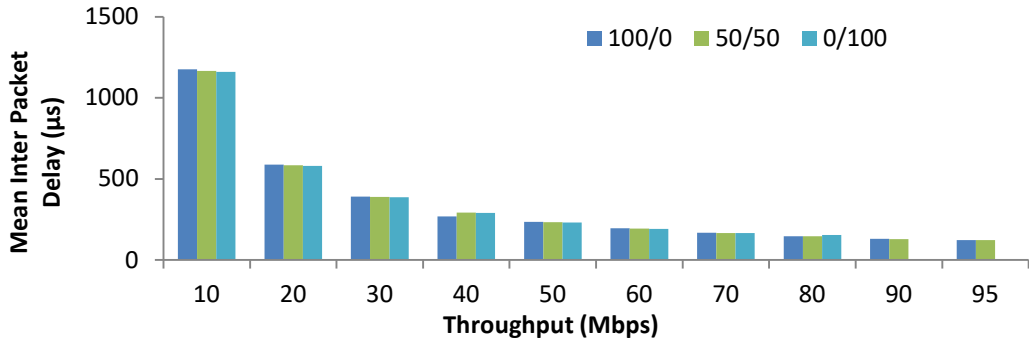

Figure 11. Mean Inter Packet Delay for different throughputs.

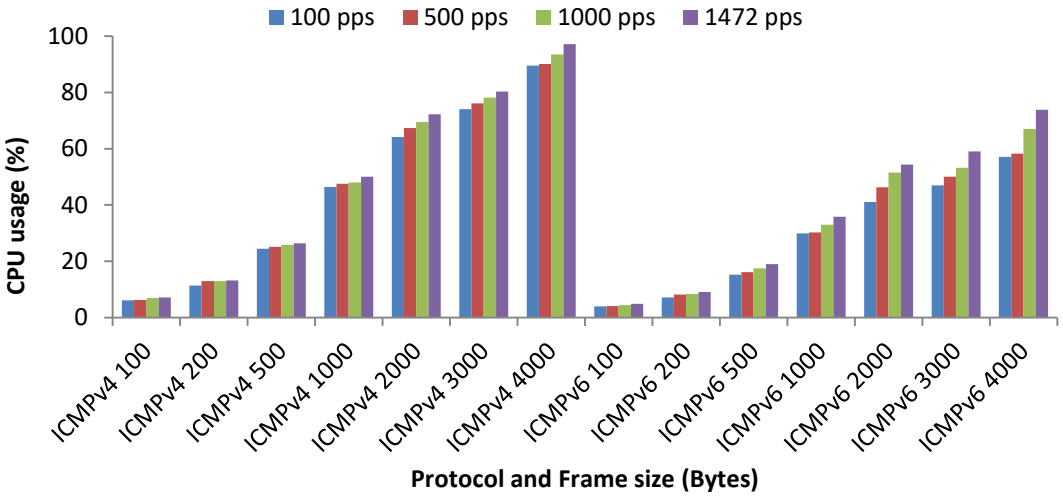

Figure 12. The CPU usage for different ICMP messages

The results of the tests aimed to evaluate the use of ACL with different IPv4 and IPv6 traffic are shown below. The CPU usage is shown in Fig. 13 and the maximum traffic rate in Fig. 14. First, as it was seen before, the CPU usage increases with the percentage of IPv6 traffic in all the cases. Second, the CPU usage increases with the use of ACL compared with the traffic without ACL. Nevertheless, the use of ACL with 1 line or with 25 lines does not suppose a considerable increase on the CPU usage, the differences are less than 2%. By the other side, the use of ACL in Fa0/0 in or in Fa0/1 out do not represent any increase of CPU usage. But, comparing the use of ACL in Fa0/0 in with the use of ACL in Fa0/0 in and Fa 0/1 out it presents a difference. In the second case there is an increment of more than 3% and this increase is greater as the IPv6 traffic increases. The use of CPU of IPv6 traffic without ACL (67.5%) is almost the same CPU usage than with mixed traffic 50/50 with ACL of 1 line Fa0/0 in Fa0/1 out (68%). Regarding to the maximum traffic rate it is possible to see that, as in previous test, the use of IPv6 traffic reduces the maximum traffic rate. The use of ACL reduces the maximum traffic rate only when the IPv6 traffic is higher than 50%, for traffic 100/0 and 90/10 no great differences on maximum traffic rate when ACL are used. The reduction of traffic when the ACL are employed is caused because of the router needs to check the ACL for each packet before send it. We also can conclude that traffic reduction is only accurate when the IPv6 traffic represents the 50% of traffic or more because of the router 1841 costs more to process the ACL with IPv6 traffic that with IPv4 traffic. Concerning to the effect of different point of application of the ACL, Fa0/0 in, Fa0/1 out or both some data can be deduced. The maximum traffic rate is higher when ACL is applied at Fa0/1 out, follow by Fa0/0 in and it is lower when the ACL are applied in both interfaces because for each packet the router must check two times the ACL.

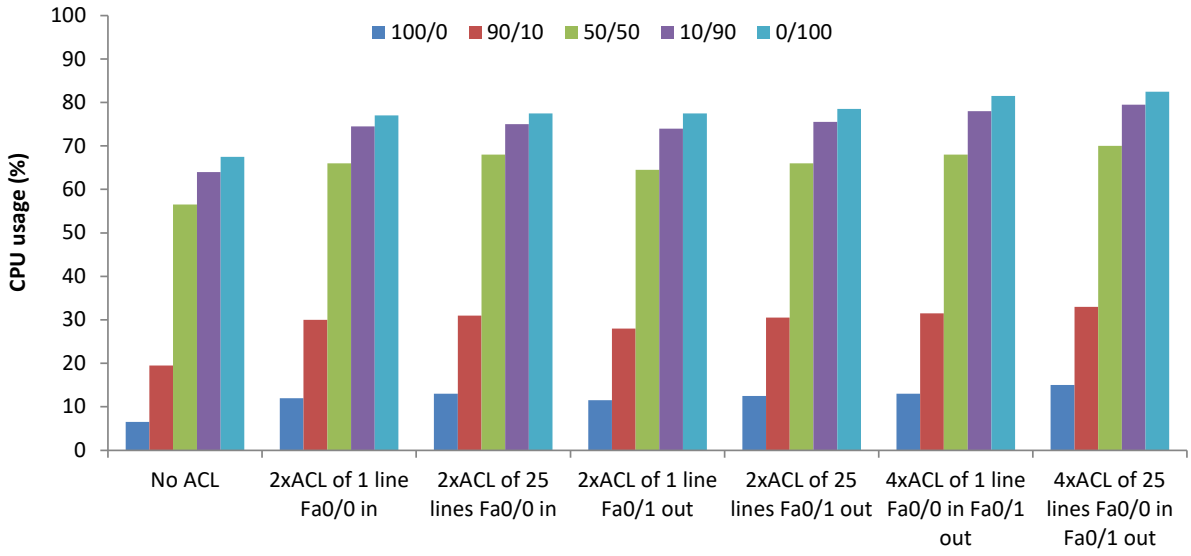

Figure 13. CPU usage (%) for different ACL use

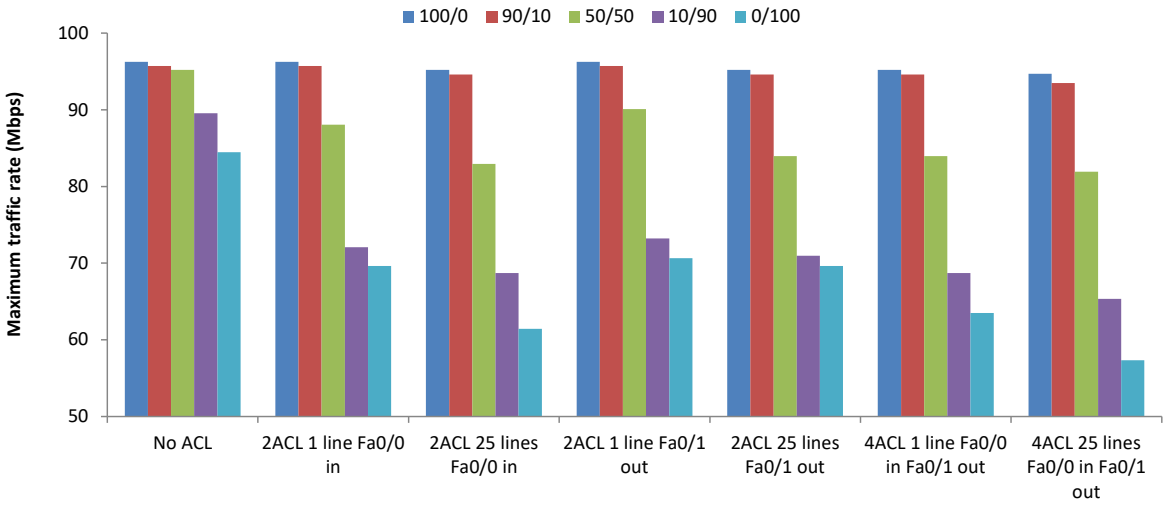

Figure 14. Maximum traffic for different ACL use

Finally, the results of the test where different IPv6 extension headers were used are presented in Fig. 15. First, the CPU usage is higher as higher is the data flow in pps, because of the need of process more packets in less time. When the traffic is low, as 100pps, no big differences are found in CPU usage with different traffic, with and without headers or ACL, it is 2% approx. But with high traffic, as 6000 pps, the CPU usage is different for different traffic typology. It is lower when no ACL are used (around 80%) and maximum for Hop-by-Hop with ACL (94%) for other situations the CPU usage is almost 92%. No differences are found on the use of 4 extension headers or 20 extension headers. Nevertheless, the use of ACL as it was seen in the previous tests, causes an increase of CPU usage.

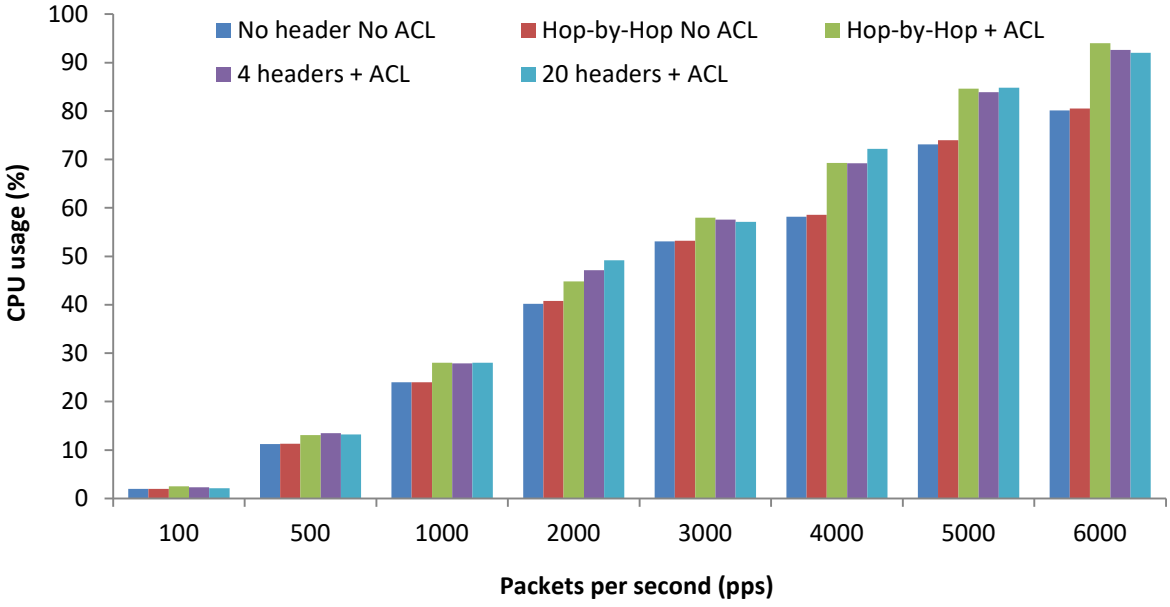

Figure 15. Maximum traffic for different IPv6 extension headers

4.2 Tests with two Cisco Router 1841

In this subsection the data of the test with two routers are shown. First the test focused on

the effects of packet fragmentation, see Fig. 16. The CPU usage and the PPS in router 1 were measured to find when the packets were fragmented and when they were not. It is possible to see that while the UDP data (frame size – 46 Bytes) is lower than the MTU the PPS and CPU usage are the same for all the frame size. In this conditions the PPS and CPU usage decrease with the frames size. It has been explained before, higher frame sizes imply less headers to process for the same amount of data. By the other side, with the same data flow, smaller frame size contains less data and more packets can be sent. Nevertheless once the UPD data is higher than MTU there is a peak on CPU compared with the CPU usage of traffic that do not exceed the MTU the use of CPU is 2.7 times higher. This increase on CPU usage is due to the need of fragmentation. The frames need to be fragmented, Router 1 must pack new packets with corresponding headers and route them to their destination. After this peak the CPU usage decreases because the number of packets decreases. The PPS of traffic that exceeds the MTU suffers a reduction; this reduction is maximum with MTU of 68 Bytes. For MTU, 68 Bytes, only the traffic with frame size of 64 Byte is sent without fragmentation. From traffic with frame size of 128 to 1024 Bytes the CPU usage decreases because fewer packets are processed. But from traffic of 1280 Bytes and higher, the CPU usage increases again. This increase of the CPU usage is caused because of the high fragmentation rate. For a frame of 1518 Bytes 31 new frames must be created by the router, it supposes an enormous amount of work for the processor.

Now the results of the test that studied the fps are shown, see Fig. 17. It is possible to see that the higher fragmentation implies higher CPU usage. Fragmentation and CPU usage have a lineal correlation. An increment of fragmentation of one more fragment per packet supposes an increment of CPU usage of 4.5%. This small increment can be critical when traffic of high frame size is used with a network with low MTU, see frame size of 918, one packet is fragmented into 11 packets. At this point the increase of CPU usage supposes that the use of CPU rise to 51.2%, while sending packets without fragmentation supposes a CPU usage of 6%.

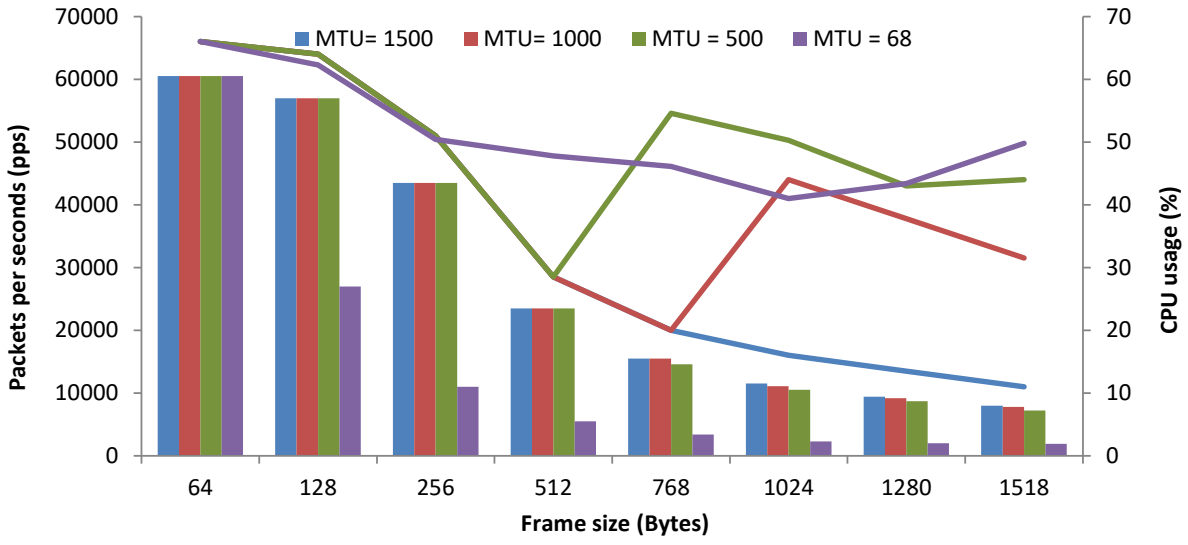

Figure 16. CPU usage and packets per second during fragmentation

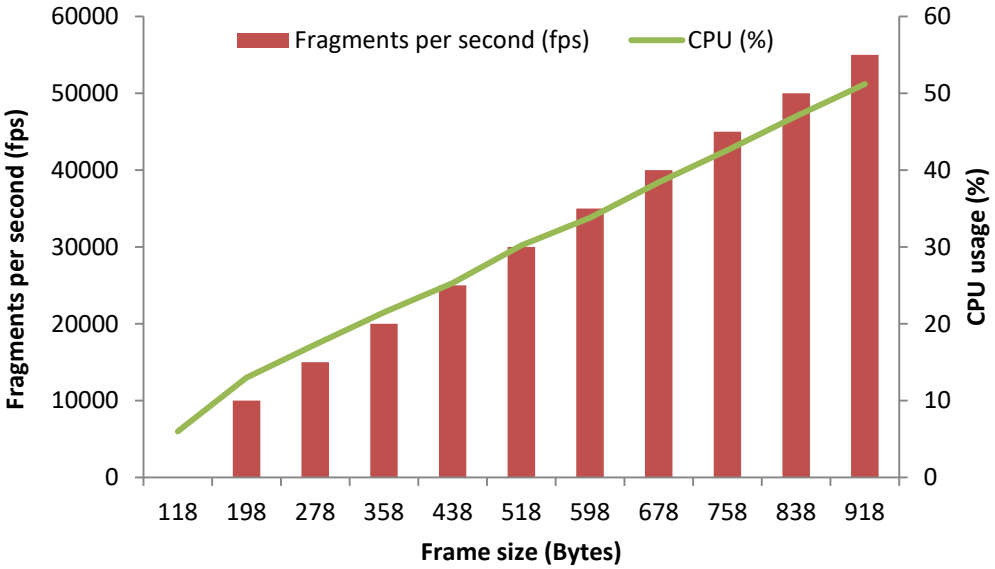

Figure 17. CPU usage with different fragmentations

In Fig. 18 the results of the test with REH are shown. First, we can see that the CPU usage increases when the traffic contains REH. It is caused because of the need to read the REH. This increase is lower as lower is the data flow in pps. For 1000 pps the increase of CPU usage when REH are employed is less than 2% of CPU capacity, while for 5000 pps the increase of packets implies an increase of CPU usage of 6%. The increase on CPU usage caused by the use of REH is the same for bidirectional and unidirectional traffic. As in other test, the CPU usage increases with the bidirectional traffic.

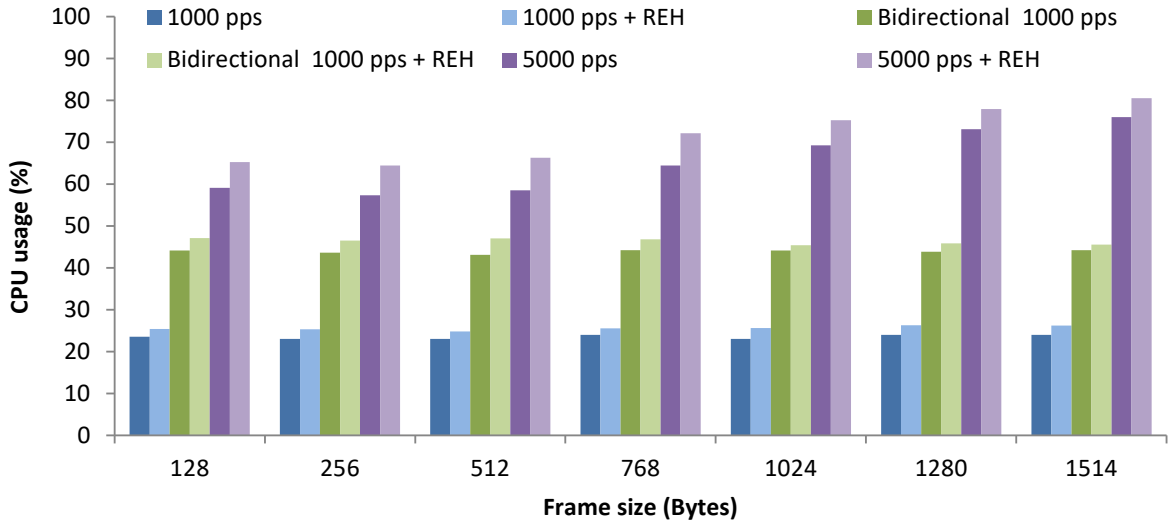

Figure 18. CPU usage (%) with different REH use

5. Conclusions

In this paper an exhaustive study of Cisco Router 1841 performance with IPv6 traffic is shown. Different topologies were tested and different traffic is used with and without ACL, extension headers among others. The CPU usage, throughput, packets per second and inter

packet delay are some of the evaluated parameters. The maximum traffic rate was reached with packets of 1518 Bytes and IPv4 protocol, and it decreases with the use of IPv6 protocol. The router reaches higher performance when work with IPv4 traffic. The CPU usage increases with the increase of IPv6 traffic. The use of ACL in IPv4 traffic the CPU usage rises from 6.5% without ACL to 15% with ACL (8.5%) while for IPv6 goes from 67.5% to 82.5%, 15%, the double. The maximum traffic rate falls 1.54 Mbps by the use of ACL in IPv4 and 27.14 Mbps in IPv6. With IPv4 the router is able to support bidirectional traffic without decrease the maximum traffic rate, compared with unidirectional traffic. But for IPv6 in bidirectional traffic the maximum traffic rate is lower than for unidirectional traffic in the same conditions. The use of REH in the traffic supposes an increment of the CPU usage; this increment depends on the packets per second of the data flow. The presented results and conclusions are valid only for the Cisco Router 1841. We can expect that other devices with the same limitation to process IPv6 compared with IPv4 traffic at hardware level will show similar reductions.

We can summarize that the usage of IPv6 traffic supposes a reduction of the Cisco Router 1841 compared with IPv4 traffic as it is shown in the manufacturer indicates [20]. In this paper we have quantified this reduction. It is caused because of the different header sizes and the different processing of IPv4 and IPV6. We can expect that in the next years when the IPv6 increase the enterprises needs to change their Router 1841 to new devices that process the IPv6 traffic at hardware level if they pretend to maintain the maximum traffic rate or avoid the increase of CPU usage. The acquisition of devices that can process IPv6 traffic at hardware level suppose an investment too high to be assumed by the medium and small size enterprises. An increase on CPU usage implies an increase of energy consume that can be considerable when several devices are working.

As future work we will test the energy consumption of different devices with IPv4 and IPv6 traffic in more complex topologies and transmitting high flow rates. We will also test other devices from other manufacturers with other characteristics. We need to consider that nowadays the multimedia streaming supposes an increasing percentage of the traffic.

Acknowledgement

This work has been supported by the pre-doctoral student grant “Ayudas para contratos predoctorales de Formación del Profesorado Universitario FPU (Convocatoria 2014)” Reference: FPU14/02953 by the “Ministerio de Educación, Cultura y Deporte”.

References

[1] Hardzone, “El tiempo de vida del estándar IPv4 ya llega a su final”. Available at http://hardzone.es/2015/09/27/nos-quedamos-sin-direcciones-ipv4/. Last accessed on October 17, 2016.

[2] Internet Protocol, Version 4 (IPv4) Specification. Available at:

https://tools.ietf.org/html/rfc791. Last accessed on October 17, 2016.
[3] Internet Protocol, Version 6 (IPv6) Specification. Available at: https://tools.ietf.org/html/rfc2460. Last accessed on October 17, 2016.
[4] Tech Times, "IPv4 addresses run out: What's the backup plan?". Available at http://www.techtimes.com/articles/88190/20150925/ipv4-addresses-run-out-whats-the-backup-plan.htm. Last accessed on October 17, 2016.
[5] Ramon Millan, ¿Qué ha pasado con IPv6? Available at http://www.ramonmillan.com/tutoriales/estadoipv6.php. Last accessed on October 17, 2016.
[6] Smartcio, "El estado actual de IPv6". Available at http://smartcio.es/estado-actual-ipv6/. Last accessed on October 17, 2016.
[7] Sucuri blog, "What is the status of IPv6 adoption?". Available at http://smartcio.es/estado-actual-ipv6/. Last accessed on October 17, 2016.
[8] Google statistics on IPv6. Available at https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption. Last accessed on October 17, 2016.
[9] Cisco 6lab. Available at http://6lab.cisco.com/stats/. Last accessed on October 17, 2016.
[10] Andrade-Morelli S., Ruíz-Sánchez E., Sendra S. and Lloret J., "Router Power Consumption Analysis: Towards Green Communications", Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 113, pp. 28-37, 2012. http://dx.doi.org/10.1007/978-3-642-37977-2_3
[11] Mhod.Khairil S., Rosilah H. and Ahmed P., "A Comparative Review of IPv4 and IPv6 for Research Test Bed", ICEEI '09 International Conference on Electrical Engineering and Informatics, Malaysia, 5-7 August, 2009. http://dx.doi.org/10.1109/ICEEI.2009.5254698
[12] Yasinovskyy R., Wijesinha A., and Karne R., "A Comparison of VoIP Performance on IPv6 and IPv4 networks", IEEE/ACS International Conference on Computer Systems and Applications (AICCSA 2009), Rabat, Morocco, 10-13 May, 2009. http://dx.doi.org/10.1109/AICCSA.2009.5069388
[13] Narayan S., Kolahi S., Sunarto Y., Nguyen D. and Mani P., "Performance Comparison of IPv4 and IPv6 on Various Windows Operating Systems", 11th International Conference on Computer and Information Technology (ICCIT 2008), Khulna, Bangladesh, 24-27 December, 2008. http://dx.doi.org/10.1109/ICCITECHN.2008.4803056
[14] Verovko M., Verovko O., Kazymyr V., Davies J. and Grout V., "Performance Concerns When Implementing Infrastructure Security in IPv4/IPv6 networks", Internet Technologies and Applications (ITA), Wrexham, UK, 8-11 September, 2015. http://dx.doi.org/10.1109/ITechA.2015.7317393
[15] Zhou X., Jacobsson M., Uijterwaal H., Van Mieghem P., "IPv6 delay and loss performance evolution", International Journal of Communication Systems, Volume 21, Issue 6, pp. 643-663, June 2008. http://dx.doi.org/10.1002/dac.916
[16] Jiang W., Fang B., Tian Z. and Zhang H., "Design and Research of a Large-scale Network Access Control System with Hybrid Router Configuration", 3rd International Conference on Innovative Computing Information and Control (ICICIC '08), USA, 18-20 June, 2008. http://dx.doi.org/10.1109/ICICIC.2008.216

[17] Cisco 1841 Router Datasheet. Available at http://www.cisco.com/c/en/us/products/collateral/routers/1800-series-integrated-services-routers-isr/product_data_sheet0900aecd8016a59b.html. Last accessed on October 20, 2016.
[18] Internet Control Message Protocol. Available at https://tools.ietf.org/html/rfc792. Last accessed on October 17, 2016.
[19] Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. Available at https://tools.ietf.org/html/rfc4443. Last accessed on October 17, 2016.
[20] Portable Product Sheets – Routing Performance. Available at https://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf. Last accessed on October 20, 2016.

Copyright Disclaimer