Performance Analysis of Dynamic Routing Protocols in IPv6 and IPv4 Networks

Ayoub Bahnasse
LIMIE Laboratory
Centre El Jadida,
Groupe ISGA
El Jadida, Morocco

Amine Taleb
LIMIE Laboratory
Centre El Jadida,
Groupe ISGA
El Jadida, Morocco

Sohaib Lamkadmi
LIMIE Laboratory
Centre El Jadida,
Groupe ISGA
El Jadida, Morocco

Achraf El Hassani
LIMIE Laboratory
Centre El Jadida,
Groupe ISGA
El Jadida, Morocco

ABSTRACT

The computer networks are increasingly imposed recently, all sectors currently rely on the protocol Internet Protocol to provide users with remote access, wherever and whenever. IP is currently involved in sensitive areas such as telemedicine, remote sensing, telepresence, electronic payment and so on. IP exists in two version version 4 (IPv4) and version 6 (IPv6), the difference between these two protocols is distinguished in terms of features, operation, and performance. In this article we will measure and evaluate the performance of the two IPv4 and IPv6 protocols in the networks of communicating companies. The study will be performed by varying the routing protocols RIP, RIPnG, OSPF, OSPFv3, IS-IS and IS-IS v6. Our study will be conducted under the OPNET Modeler simulators, the traffic we will exploit for evaluation is VoIP, videoconferencing, and FTP.

General Terms

Enterprise infrastructure deployment

Keywords

IPv6, IP Next Generation, IPv4, IPng, IETF, SIP

1. INTRODUCTION

With the success of the Internet, IP (Internet Protocol) has been exploited in a variety of sciences and disciplines that are constrained by security, availability, and real-time processing. The IP protocol has brought unparalleled flexibility by connecting all kinds of objects, hence the new Internet of Things (IoT) infrastructure [1], this infrastructure uses sensors to trace a large amount of data to controllers. IP exists in two versions, version 4 (IPv4) and version 6 (IPv6), the first despite its multiple weaknesses remains the most dominant in the sector of the telecommunications industry. These weaknesses can be detailed according to several sides, we quote mainly of security order [2], that is to say that IPv4 does not provide by default any mechanism of encryption, integrity, and authentication, the use of the IPsec protocol is optional. IPv4 suffers mainly from the saturation of the range of addresses, with the IoT infrastructures, the addresses are no longer sufficient, however with the mechanisms NAT [3] we can more or less answer on this problematic but in short terms. With 128-bit instead of 32-bit addresses, IPv6 has a much larger address space than IPv4 (nearly 100 trillion times more), so this huge amount of addresses allows for greater flexibility in assigning addresses. The benefits of IPv6 are multiple, but with a relatively complicated addressing scheme compared to IPv4, the IPv6 mechanism of stateless self-configuration of addresses is a considerable simplification compared to IPV4. Each node builds its IPv6 addresses without prior configuration, without additional DHCP server and therefore without configuring routers [4]. Other than the form, IPv6 supports the "Jumbograms" [5], that is to say that IPv4 packets are limited to 64 KB, this limit goes to 4 GB in IPv6 when the quality of links allows it. The simplicity of the routing, also, constitutes a point of major difference compared to IPv4, these tables are reduced and do not perform error control at the level of the headers of packets which makes it possible to reduce the transit time packets in the routers. Table 1 summarize some differences between two protocols IPv4 and IPv6.

Table 1. IPv4 versus IPv6

Criteria	IPv4	IPv6
Standard	IETF 1974	IETF 1998
Addressing	32 bits	128 bits
IPsec	Optional	Mandatory
Header length	Variable	Fixed
Flow	No	Packet Flow Label
Options	Yes	No (extensions)

The rest of the paper is organized as follows, in section 2 we will discuss dynamic routing protocols used in the simulations. In section 3 we will present some recent and relevant related works. In section 4 we will position clearly our contribution. In section 5 we will present the simulation environment. The presentation and discussion of obtained results will be performed in section 6. And we will conclude in section 7.

2. ROUTING PROTOCOLS

Network convergence is a term that means that all routers in the same autonomous system or zones have the same routing table. This convergence can be achieved by using dynamic or static routing protocols [6], static routing protocols are actually deployed only in the case of small-scale networks since convergence depends mainly on the human factor, any incorrect parameterization is translated by the lack of accessibility of certain destinations. However, static routing can be used to interconnect remote sites, provided that the intermediate network is convergent, the general use of this type of routing is in virtual private network (VPN) connections [7] [8] or default routes for ADSL lines. Dynamic routing protocols are illustrated in two broad categories: Interior Gateway Protocols (IGP) and Exterior Gateway Protocols (EGP). IGP routing protocols are classified into three families: distance vectors, link state, and hybrids. In this section we will deal with three routing protocols with which we conducted our study.

2.1 RIP

Routing Information Protocol (RIP) [9] is a remote vector routing protocol, exists in two version for IPv4, it is RIPv1 and RIPv2. RIPv1 is a classful version, that is to say it only takes into consideration the default mask, this can cause several problems among the black hole. RIPv1 is based on the delivery of routing updates, and therefore provides a vulnerability in the disclosure of the routing table to unwanted users. RIPv1 also suffers from source checking mechanisms for updates, however, this version as for version 2 is vulnerable to spoofing attacks, overflowing routing table, and falsification of announced routes. The second version solved the problem of broadcasting, the updates are sent to the multicast address 224.0.0.9 with UDP as transport protocol, the advantage indeed of this version compared to the first version, lies in the fact that the original masks are announced in the updates, and thus the problem of the black hole is no longer posed. RIPv1 and RIPv2 have common weaknesses, these weaknesses are in their operating types, these protocols periodically send all the routing tables, and therefore sometimes abusively consume the bandwidth of the links. The RIPng version for IPv6 networks [10] is based on the IPSec security mechanisms [11] available in IPv6. The RIPng packets are sent to the multicast address all-rip-router FF02 :: 9 and encapsulated in a UDP packet with the port number 521.

2.2 OSPF

Open Shortest Path First [12], is a link-state protocol, which is based on three table to achieve the convergence state, which are in order: the neighbor table, topology table, and the routing table . The neighbor table contains the identifier directly connected routers, and their roles (DR, BDR, DROthers). The topology table contains the complete network architecture with all alternate paths to reach all destinations. The routing table that contains only the best path to reach a specific destination, depending on the metric that is the cost. OSPF for IPv4 (OSPFv2) or IPv6 (OSPFv3) have the same operating principle, the network is structured as multiple areas, the backbone area (Area 0) and the standard area (Area> 0). Two standard areas can communicate only via a backbone area, or through virtual links. In a broadcast or multi-access network, the election of a designated router and Backup is carried by area, and the election is made according to the highest priority or router identifier.

The difference between OSPFv2 and OSPFV3 can be summarized in the following criteria:

- Announcements - OSPFv2 announces IPv4 routes, while OSPFv3 announces routes for IPv6.
- Source Address - OSPFv2 messages come from the IPv4 address of the output interface. In the OSPFv3 protocol, OSPF messages are provided using the link-local address of the output interface.
- Multicast addresses all OSPF routers - OSPFv2 uses 224.0.0.5; while OSFFv3 uses FF02 :: 5.
- Multicast address DR / BDR - OSPFv2 uses 224.0.0.6; while OSFFv3 uses FF02 :: 6.

2.3 IS-IS

IS-IS (Intermediate System to Intermediate System) is a link-state internal routing protocol. It has been standardized by ISO (ISO 10589). An IS-IS router can be either: level-1 (intra-area routing), level-2 (inter-area routing), level-1-2 (intra and inter-area routing). In order to build its topology, IS-IS uses 3 types of messages: HELLO messages to build adjacencies; Link State Protocol (LSP) messages for exchanging link state information; Sequence Number Packet (SNP) messages to confirm the topology. To develop these messages, IS-IS relies on the use of independent pieces of information called TLVs (Type, Length, Value). The message thus consists of a header followed by a list of TLVs. Each TLV carries its own information, and is therefore standardized.

3. RELATED WORKS

Assessing the performance of IPv4 and IPv6 routing protocols and their impact on business services is a very active area of research. The work [13] evaluated by simulation the performance of the IPv4 and IPv6 routing protocols by increasing the load of the packets. The simulation was performed under the GNS3 simulator, with the RIP, EIGRP, and OSPF protocols. The authors found that RIP provides better results compared to other protocols in terms of latency and convergence time. In general, the authors showed the effectiveness of IPv6 over IPv4. In an essay [14], the author evaluated VoIP quality of service (QoS) performance in an IPv4 and IPv6 network. The author has shown that IPv4 offers better results compared to IPv6, and this is due to the reduced size of the IPv4 header (20 bytes) compared to IPv6 (40 bytes). In another work [15] the authors performed a comparative study between the performances of EIGRPv6, RIPng, and OSPFv3 on real-time applications. The study was conducted under the OPNET Modeler simulator, the authors showed that the EIGRPv6 protocol is the fastest protocol in terms of convergence, and the protocol provides the best QoS levels for real-time applications.

4. POSITIONING OF CONTRIBUTION

Our contribution is in the context of:

1. Performance evaluation of IPv4 and IPv6 protocols,
2. Evaluation of the performance of the routing protocols in both versions,
3. Measuring the impact of previous protocols on different types of applications (VoIP, Video Conferencing, and FTP),
4. Measuring the impact of the escalation in terms of the number of customers per site.

The study will be carried out on the protocols of routing RIPv2, RIPng, OSPFv2, OSPFv3, ISISv4 and ISISv6

5. NETWORK TESTBED

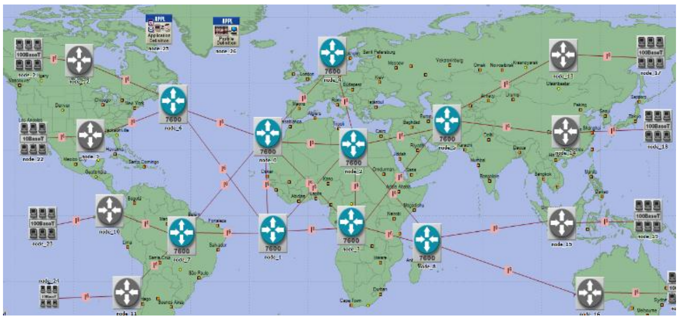

Fig 1: Network testbed

Figure 1 illustrates the network testbed on which all our simulations was carried. The goal of this performance analysis is to stress this network on every protocol, ISIS, RIP and OSPF on both IP version 4 and 6. As the topology explain itself, we have total of 17 routers and 80 end-user workstations with three applications:

- Voice over IP (VoIP) with GSM Codec
- Video Conferencing, medium resolution
- FTP, medium load

6. OBTAINED RESULTS

In this section we will discuss the obtained results for each application

6.1 Voice over IP

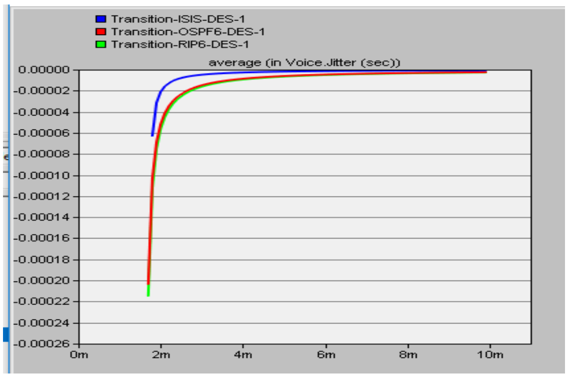

Fig 2: Jitter of VoIP in IPv6

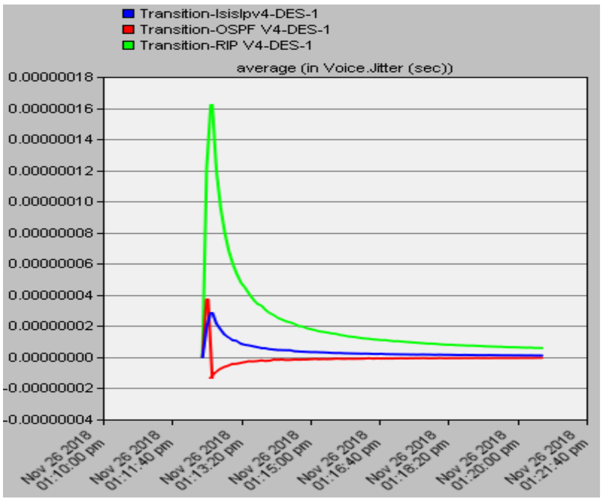

Fig 3: Jitter of VoIP in IPv4

Above in figure 2 and 3, charts shows the comparison of VOIP jitter between IPv4 and IPv6 and shows that IPv4 have higher Jitter than IPv6.

The MOS score quantifies the quality actually perceived by a certain population. In particular, it takes into account psychoacoustic effects.

In the case of vocoders, the MOS score also shows the differences in quality related to the language of the speaker and the listener. A vocoder can be noted 3.9 in English and 1.9 in Mandarin Chinese. Finally, the MOS is an indispensable tool when developing a new type of codec. The complex algorithms that a modern codec uses often have a number of parameters that make it more or less specific to a particular type of application. The choice of parameter values is very difficult (sometimes impossible) to do rationally. In this case, the MOS comes to the aid of researchers by providing a quantitative answer based on a real perceptual experience.

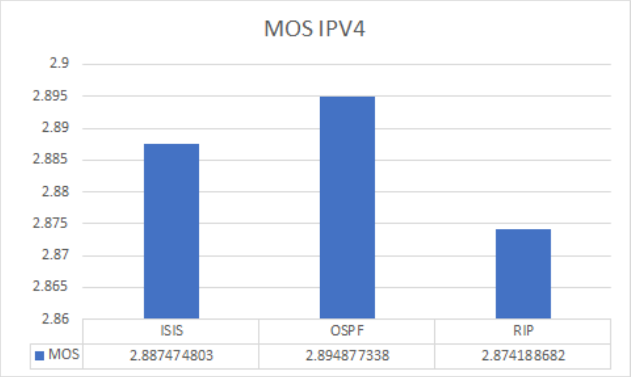

Fig 4: MOS in IPv4

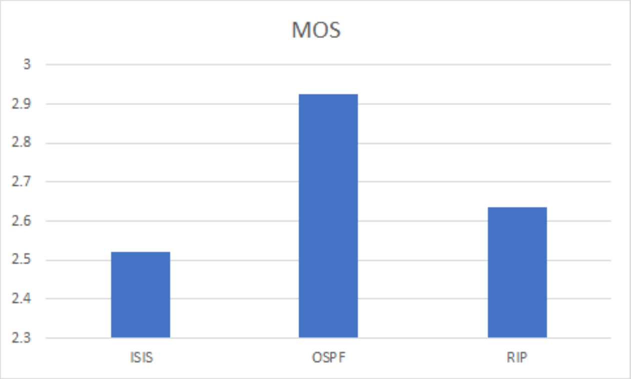

Fig 5: MOS in IPv6

Charts above (Figure 4 and figure 5) shows the comparison of IPV4 and IPV6 voice MOS. As we see below, RIP is the most efficient protocol in IPv4, while in IPv6 we could say that ISIS is performing better with a lot of improvement compared to other protocols.

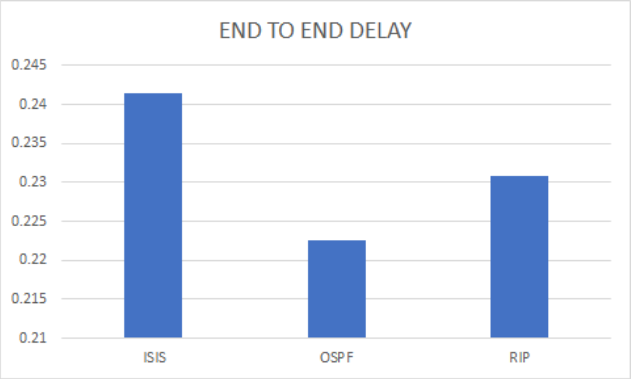

Fig 6: End to end Delay in IPv6

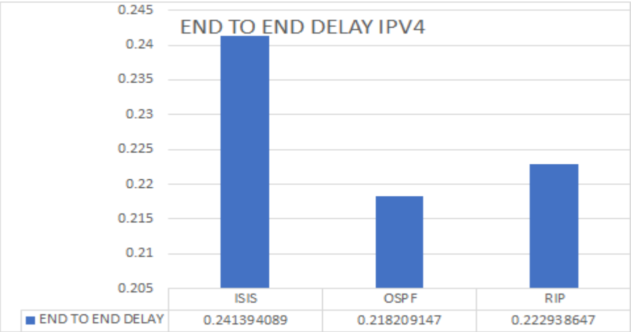

Fig 7: End to end delay in IPv4

The end-to-end delay is the time required for the packet to be transferred to a network from source to destination. It is the sum of the delay of transmission, the delay of propagation, the delay of treatment and timeout. The end to end delay makes a real difference in VoIP calls. Charts below (Figure 6 and Figure 7) show that IPv6 offers better performances especially with OSPF with a smaller end to end delay compared to ISIS and RIP in both IPv4 and IPv6.

6.2 Video conference

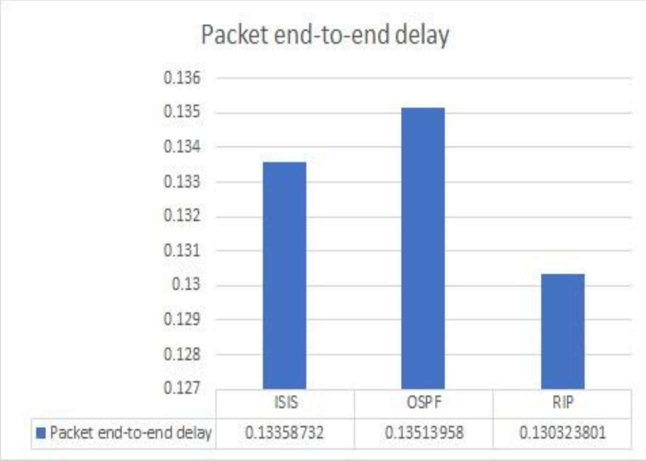

Fig 8: Video Conferencing Packet end to end delay

Figure 8 illustrates the video conference packet end to end delay on IPv6 routing protocols. Obtained results shows that RIP perform better than ISIS and OSPF.

6.3 FTP

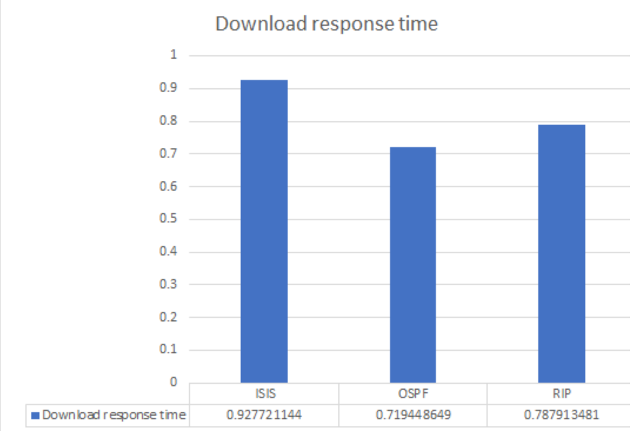

Figure 9: Download response time IPv4

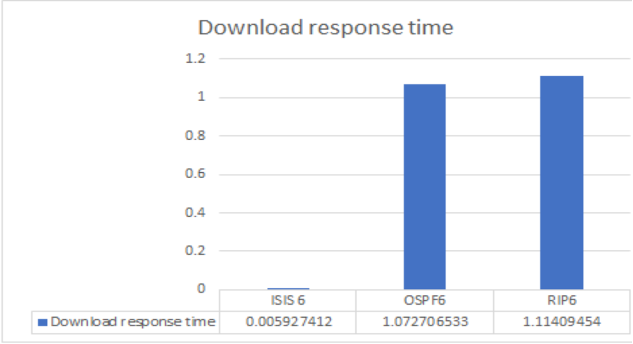

Figure 10: Download response time IPv6

According to figure 9 and figure 10, we notice that in an IPv4 architecture the download response time is approximately the same for the OSPF and RIP, ISIS protocols, the latter takes a little more time. But in an Ipv6 architecture we noted that the download response time for OSPF and RIP is so high and the response time for ISIS is almost 0.

7. CONCLUSION

Although the current trend is migration to the new IPv6 standard, this article has performed an evaluation of the performance of IPv4 and IPv6-based networks. The study touched on several different aspects; measuring the scalability of the two protocols, evaluating the IGP routing protocols in both protocols, and measuring the impact of these elements on the performance of the transported applications. The simulations were performed under OPNET Modeler. The results obtained showed the effectiveness of the IPv6 protocol compared to IPv6 in almost all the results obtained

8. ACKNOWLEDGMENT

This work is a validation of a mini project carried out by the engineering students Amine Taleb, Sohaib Lamkadmi, and Achraf El Hassani in ISGA El Jadida, supervised by Dr A. Bahnasse. We address our sincere thanks to the director Dr A. Outzourhit for encouraging us to lead this work and to our school for providing us necessary tools to success this experience.

We would like to thank the editor and the anonymous reviewers for their comments that contributed to the improvement of the work.

9. REFERENCES

[1] Khiat, A., Bahnasse, A., Bakkoury, J., El Khaili, M., & Louhab, F. E. (2019). New approach based internet of things for a clean atmosphere. International Journal of Information Technology, 11(1), 89-95.

[2] Bahnasse, A., Talea, M., Louhab, F. E., Laafar, S., Harbi, A., & Khiat, A. (2017, July). SAS-IMS for smart mobile security in IP multimedia subsystem. In Proceedings of the 2017 International Conference on Smart Digital Environment (pp. 35-41). ACM.

[3] Tsirtsis, G., & Srisuresh, P. (2000). Network address translation-protocol translation (NAT-PT) (No. RFC 2766).

[4] Chown, T., Loughney, J., & Winters, T. (2019). IPv6 Node Requirements (No. RFC 8504).

[5] Borman, D., Deering, S., & Hinden, R. (1999). IPv6 Jumbograms (No. RFC 2675).

[6] Bahnasse, A., & El Kamoun, N. (2015). Study and Analysis of a Dynamic Routing Protocols' Scalability over a Dynamic Multi-point Virtual Private Network. International Journal of Computer Applications, 123(2).

[7] Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017). Evaluation of tunnel layer impact on VOIP performances (IP-MPLS-MPLS VPN-MPLS VPN IPsec). International Journal of Computer Science and Network Security (IJCSNS), 17(3), 87.

[8] Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017). Analytical performance and evaluation of the scalability of layer 3 tunneling protocols: case of voice traffic over IP. IJCNS International Journal of Computer Science and Network Security, 17(4), 361-369.

[9] Hedrick, C. L. (1988). Routing information protocol (No. RFC 1058).

[10] Malkin, G., & Minnear, R. (1996). Ripng for ipv6 (No. RFC 2080).

[11] Khiat, A., Bahnasse, A., Bakkoury, J., & El Khaili, M. (2017). Study, evaluation and measurement of IEEE 802.16 e secured by dynamic and multipoint VPN IPsec. International Journal of Computer Science and Information Security, 15(1), 276.

[12] Moy, J., "OSPF Version 2", RFC 2178, DOI 10.17487/RFC2178, July 1997, <https://www.rfc-editor.org/info/rfc2178>.

[13] Al-Ani, D. R., & Al-Ani, A. R. (2018). The performance of IPv4 and IPv6 in terms of Routing Protocols using GNS 3 Simulator. Procedia computer science, 130(C), 1051-1056.

[14] Mohamed, H. H. A. (2018). QoS Measurement for Real-Time Voice Traffic Over IPv4 and IPv6 (Doctoral dissertation, Sudan University of Science and Technology).

[15] Samaan, S. S. (2018). Performance Evaluation of RIPng, EIGRPv6 and OSPFv3 for Real Time Applications. Journal of Engineering, 24(1), 111-122