

PERFORMANCE EVALUATION OF OSPF AND RIP ON IPV4 & IPV6 TECHNOLOGY USING G.711 CODEC

Mabubur Syed and Isaac Yerima Ambore

Department of Computer Information Science, Minnesota State University, Mankato.
Minnesota, USA

ABSTRACT

Migration from IPv4 to IPv6 is still visibly slow, mainly because of the inherent cost involved in the implementation, hardware and software acquisition. However, there are many values IPv6 can bring to the IP enabled environment as compared to IPv4, particularly for Voice Over Internet Protocol (VoIP) solutions. Many companies are drifting away from circuit based switching such as PSTN to packet based switching (VoIP) for collaboration. There are several factors determining the effective utilization and quality of VoIP solutions. These include the choice of codec, echo control, packet loss, delay, delay variation (jitter), and the network topology. The network is basically the environment in which VoIP is deployed. State of art network design for VoIP technologies requires impeccable Interior Gateway routing protocols that will reduce the convergence time of the network, in the event of a link failure. Choice of CODEC is also a main factor. Since most research work in this area did not consider a particular CODEC as a factor in determining performance, this paper will compare the behaviour of RIP and OSPF in IPv4 and IPv6 using G.711 CODEC with riverbed modeller17.5.

KEYWORDS

IPv4, IPv6, Network topology, VoIP, CODEC

1. INTRODUCTION

VoIP refers to transmission of voice over an IP based network. VoIP involves sending voice information in digital form using packet based switching rather than using the traditional protocols of the Public Switched Telephone Network (PSTN). PSTN is an aggregation of circuit switching telephony. This form of transmission is superior to conventional circuit switched communication in many ways. However, VoIP technology is an emerging technology and a plethora of security issues are associated with it [1]. Companies are gradually moving away from PSTN into either a total Implementation of VoIP or a hybrid model of PSTN and VoIP. This is a result of increased cost associated with placing long distance calls using PSTN. Telecom companies using VoIP save money by utilizing the internet's data bandwidth. The allocation of bandwidth for the VoIP environment also presents a problem. VoIP requires low delay and low packet loss rates so as to not impair the interaction among talking parties and the delivered content quality [2]. However, IP networks offer a best-effort service and do not meet stringent Quality of Service (QOS) requirement [6]. Although most VoIP implementation ensures the right QOS be applied on switches and routers, still there are many other factors that may affect phone call quality, including the choice of codec, echo control, packet loss, delay, delay variation (jitter), and the network design. [3]. VoIP requires a robust environment to thrive, every VoIP

solution rides on an IP enabled network environment. Most networks use the Internet Protocol version 4 (IPv4) standard that features IP addresses four bytes (32 bits) in length. This creates a shortage of IPv4 addresses, as every device on the Internet that uses IPv4 needs a unique address. The new Internet Protocol version 6 (IPv6) standard features addresses, which is 16 bytes (128 bits) in length to resolve shortage of IPv4 addresses [4].

However, to resolve the problem of limited address range in IPv4, a method called Network Address Translation (NAT) is used to map private addresses to public IP addresses [5]. Although NAT is an important technique for mapping IP addresses, it does not support standard network layer security and also creates complicated barriers to VoIP, and other services. Another problem is that IPv4 has limited security features integrated in it and additional security is implemented by means of external security protocols. One example is the use of IPsec as an encrypting mechanism for IPv4 traffic [5]. IPv6 presents a solution for some of the challenges posed by IPv4 enabled environment for VoIP services.

IP Routing is an essential component of data network that provides the efficient real-time data delivery that VoIP requires. Best effort networks leverage interior gateway protocol (IGP) technologies to determine paths for routing packets between hosts on IP networks [6]. Route convergence can be detrimental to VoIP users, as it impacts both latency and jitter [6].

The ability for a network to converge addresses the manner in which networks recover from problems and network changes. This is possible with the features embedded in dynamic network protocols [7]. It takes a robust routing protocol to provide this efficiency; one of the greatest challenge continues to be making the right choice for an efficient routing protocol for VoIP and selecting an appropriate IP technology between IPv4 and IPv6.

2. INTERNET PROTOCOLS

2.1. IPv4 and IPv6

One of the greatest limitations of IPv4 is the deficit in the number of IP addresses for customers and also the secured services that consumers need to access applications such as VoIP [7]. IPv6 has solved some of these problems by expanding the packet header size which increases routing efficiency and provides more IP addresses than IPv4. This might sound good, but it also has its demerit because VoIP traffic has smaller packet sizes, so the expansion of the packet header will increase the bandwidth requirement for the traffic, consequently increasing total bandwidth requirement of IPv6 network compared to IPv4. IPv6 also provides a higher performance, particularly for real time traffic, which requires quality of service (QoS), and the overall processing time is reduced [7].

With the emergence of IPv6 VoIP technology internet is likely going to run on IPv6 networks. However, the IPv4 to IPv6 transition is expected to last for several years due to the vast base of installed IPv4 networks and the high cost involved in the transition. During this period, communication between many IPv6 networks will only be possible using existing IPv4 connectivity. The recommended interim measure to address this issue is 6to4 encapsulation, which embed security into IPv4. IPsec is encapsulated into it [9]. IPv6 makes the global routing simpler than IPv4. There is lesser impact on resources and memory, which helps to improve performance and be more efficient. The security is provided end to end by encryption, which is

integrated within IPv6 [8]. In IPv6 the presence of the traffic class flag set helps to prioritize traffic with QoS from 0-7. This will reduce congestion. The quality of service is provided by the flow label, which is 20 bits [8]. Payload length, which is 16 bits, is used to detect the length of data and is able to transfer up to 64 KB [8].

2.2. OSPFv2 and OSPFv3

Open shortest Path First (OSPF) version 2 is used by IPv4 while OSPF version 3 is used by IPv6. It is one of the interior gateway routing protocols we will focus on. OSPF is a dynamic routing protocol that quickly detects topological changes in the Autonomous System (AS) number (such as router interface failures) and calculates new loop-free routes after a period of convergence [9]. It is a link state protocol which functions based on the status of links. It divides the entire internetwork or autonomous system into areas, making a hierarchy [10]. In 1999, OSPFv3 was published as RFC2740 to support IPv6 [11]. It was reviewed in RFC5523, and updated in RFC5340 [12]. OSPFv3 has some similarities with OSPFv2, although OSPFv3 is not backward compatible with OSPFv2. OSPFv3, which is described in RFC 5340, expands on OSPFv2 to support IPv6 routing prefixes and the larger size of IPv6 addresses [13]. OSPFv3 still uses the Dijkstra algorithm to calculate shortest path and lowest cost to each destination [13]. Convergence time is a critical factor in the deployment of VoIP solution. A network with a minimal convergence time is a major requirement for shortest path. Cost computation is dynamic, and it is essential to reduce every aberration so as to minimize its impact on the network. There are various formulae for calculating cost in OSPF, because each network has a unique characteristic and cost component can change. Below is a formula for OSPFv3 cost calculation The overall link cost is computed using the formula shown below [13].

$$\text{LinkCost} = A + BW * (\text{Throughput_weight}/100) + \text{RESOURCES} * (\text{Resources_weight}/100) + \text{Latency} * (\text{Latency_weight}/100) + L2_factor * (L2_factor_weight/100) \quad (1.1)$$

Where,

$$A = [\text{ospf_reference_bw}/(\text{MDR}) * (1000)].$$

A is the cost for OSPFv3, using its reference bandwidth, by default the OSPF reference bandwidth for OSPF is 10⁸ Mbps, but the type of interface can influence this value.

$$BW = ((65535) * (100 - (\text{CDR}/\text{MDR}) * 100)) / 100$$

$$\text{RESOURCES} = \text{Percentage that can represent the remaining amount of resource: } (65535) * (100 - \text{Resources})^3 / 1000000.$$

$$\text{Throughput} = (\text{Current-data-rate}) / (\text{maximum-data-rate})$$

$$L2_factor = ((100 - \text{RLQ}) * (65535)) / 100.$$

Latency = Transmission delay that packets encounter in milliseconds

RLQ = Numeric value (0-100) representing Relative Link Quality (RLQ)

65535 is the maximum OSPF link cost of a 64k link.

Weight = This is a keyword used to tune down the cost range of a layer 2 feedback which is usually between 0 – 65535, it is used with throughput, L2 factor, latency and resources keyword with the ospfv3 cost command.

In today's networks, it is essential that we consider service interruption time with respect to traffic type. For example, an interruption of a half-second would be unnoticed in a web page download, while unacceptable in a VoIP call. It is for this reason that convergence is indispensable when planning for any VoIP solution. Edge and core networks are moving from

average convergence times of 100-150 milliseconds to 50 milliseconds, which is a standard used in SONET Networks for decades [7].

OSPFv3 addressing semantics have been removed from the OSPF protocol packets and the main Link state advertisement (LSA) types, leaving a network protocol independent core. In particular [14]:

- IPv6 addresses are not present in OSPF packets, except in LSA payloads carried by the Link State Update packets.
- Router-LSAs and network-LSAs no longer contain network addresses, but simply express topology information.
- OSPF Router IDs, Area IDs, and LSA Link State IDs remain at the IPv4 size of 32 bits. They can no longer be assigned as (IPv6) addresses.
- Neighboring routers are now always identified by Router ID. Previously, they had been identified by an IPv4 address on broadcast, NBMA (Non-Broadcast Multi-Access), and point-to-multipoint links.

2.3. RIPv2 and RIPv6

Routing Information Protocol Next Generation (RIPv6) was designed to work as an Interior Gateway Protocol (IGP) in moderate-size AS's. It is not intended for use in complex environments. It uses the same algorithm with RIPv2 known as Distance Vector algorithm. The basic algorithms used by this protocol were used in computer routing as early as 1969 in the ARPANET. However, the specific ancestry of this protocol is within the Xerox network protocols [15].

It should be noted that RIPv6 is not intended to be a substitute for OSPFv3 in large autonomous systems. The restrictions on AS diameter and complexity which applied to RIPv2 also apply to RIPv6 [18].

To ensure a future for the Routing Information Protocol, a new IPv6-compatible version had to be developed. This new version was published in 1997 in RFC 2080, RIPv6 for IPv6, where the 'ng' stands for next generation (IPv6 is also sometimes called "IP next generation") [16]. There is also a negligible difference between RIPv2 and RIPv6. Basically, RIPv6 is just an adjustment made on RIPv2 to suite IPv6. Just like OSPF, RIPv6 is not backward compatible to RIPv2.

The RIPv6 IGP uses the Bellman-Ford distance vector algorithm to determine the best route to a destination, using hop count as the metric [19]. RIPv6 works basically the same way as RIPv2 but has the following differences in terms of packets [17];

- **Different IP address lengths:** RIPv6 uses 128-bit IP addresses, compared with RIPv2's 32-bit addresses.
- **Different packet lengths:** a RIPv2 message carries up to 25 route entries, while the maximum number of route table entries (RTEs) in a RIPv6 packet depends on the IPv6 MTU of the sending interface.
- **Different packet formats:** like a RIPv2 packet, a RIPv6 packet consists of a header and multiple RTEs.

RIPng relies on the authentication mechanism of IPv6 to ensure integrity and validity. RIPng uses UDP port 521, rather than RIP's UDP port 520. The destination multicast address used for RIPng packets is FF02::9, which is the IPv6 equivalent of RIPv2's 224.0.0.9 [20]. Although it is easier to deploy RIPng, it has its limitations. One limitation is its inability to detect routing loops in more complex network topologies, which also makes it converge slowly in some situations [21]. This attribute is detrimental to the implementation of VoIP technologies, because it has one metric which is the hop count. The RIPng message format contains following fields [22]: Below is the structure for RIPng [12, 13];

| | | |
|---------------------------|-------------|------------------|
| Command (1) | Version (1) | Must be zero (2) |
| Router table entry 1 (20) | | |
| Router table entry 2 (20) | | |

Figure 1: RIPng format

3. RELATED WORKS

The greatest determinant in call quality is the design, implementation, and use of the network that VoIP solution will be deployed on. A typical VoIP call will start on a LAN at a Customer Premises Equipment, go through a WAN connection to a provider, and then go back out the other end [26]. This means voice traffic can be forwarded from one router to the other using either static routes or dynamic routing protocols or a combination of both. In hindsight, the technique used to route voice traffic across a network has a tremendous influence on the call quality. Singh et al [23] concluded that signal quality in VoIP systems depends on several factors, including routing protocols used in a network, coding processes, speech content and error correction schemes. Their work was basically a review of factors affecting VoIP traffic and a review of modern VoIP systems and its improvement over the years. Consequently, there needs to be a critical study on how different dynamic routing protocols can affect VoIP performance in both IPv4 and IPv6 technologies in a small network.

Che & Cobley [24] studied how VoIP performance can be affected by the routing behaviours of protocols such as OSPF, RIP and EIGRP all in IPv4 technology. Their simulation was implemented with OPNET modeller. They configured a link to fail and recover in order to evaluate how the route will converge, as well as monitor the effect on latency and jitter in call quality. They evaluated the VoIP performance of three routing protocols using three different scenarios for each protocol respectively. The metrics for the evaluation includes: Mean Opinion Score(MOS), Delay, Jitter and de-jitter. The results show that during the failure and recovery process of their links, OSPF is more consistent in terms of the route convergence and route computation. This makes OSPF a better option for VoIP services compared to EIGRP and RIP on IPv4 technology. However, when Hussain & Jamwal [25] Carried out a comparative analysis between RIP, EIGRP and OSPF with a hybrid topology (combination of Ring and Star) using riverbed 17.5 modeller, they concluded that RIP has more convergence time and EIGRP has less convergence time in a larger network during link failures.

Following the trend in transition from IPv4 to IPv6, Narula & Pallarvi [26] evaluated the performance of RIP and OSPF for IPv6 using OPNET 14.5 simulation tool. They had three scenarios configured to simulate video conferencing: Voice, database query and HTTP. The first was configured for RIPng, the second was OSPFv3 and the third was a combination of both

RIPng and OSPFv3. They compared and analysed simulation results in terms of Database query response time, page response, object response time in HTTP, IPv6 traffic dropped, jitter, end to end delay, traffic sent in voice packet delay variation, traffic received and sent in video conference. They concluded that the response time in HTTP is better in a network where OSPFv3 and RIPng is running as to a network where they had either only OSPFv3 or RIPng.

They also observed that for real time applications traffic received and sent in video conferencing, response time in database query performs better in OSPFv3 than RIPng and a combination of both RIPng and OSPFv3. Basically, this research was done using IPv6 technology. Ahmed et al [27] looked at the performance of VoIP in IPv4 and IPV6 environments. They critically analysed the result as they compared the performance. Their simulation was done with the OPNET simulation tool. They didn't consider any protocol as such. Nevertheless, their results show that jitter for VoIP running in an IPv6 environment is very insignificant. The MOS value for IPv6 was also more consistent than the IPv4 technology. Based on their research, they concluded that IPv6 is more efficient for deploying VoIP without considering any dynamic routing protocol. On the other hand, Kaur & Singh [28] compared two routing protocols theoretically without any experiment. They focused on the flaws in using IPv6 based protocol. They compared IS-IS and OSPF in IPv6 technology. Kaur & Singh conducted a study using OPNET 14.5 to evaluate and compare the performance of IS-IS, OSPF and a combination of IS-IS and OSPF all in IPv6 for real time applications. Their assertion was that video end to end delay in IS-IS was better than OSPFv3 alone and a combination of both OSPFv3 and IS-IS in IPv6.

Whitefield & Zhhu [29] compared two dynamic protocols in IPv6 that includes OSPFv3 and EIGRPv6. They used Cisco equipment to compare these protocols and accessed the performance of each protocol when implementing some security mechanism. They had two scenarios with encryption and authentication as their security mechanism introduced to the networks. They also compared their convergence rate and found out that EIGRPv6 was faster than OSPFv3. Their study also shows that MD5 authentication mechanism used by EIGRPv6 affected its performance and IPsec improved OSPFv3's performance.

Additionally, a recent study was done by Sirika & Mahajine that analysed the performance of VoIP and videoconferencing based on convergence time, jitter, packet loss, end to end delay and throughput. They had two situations for the failure and recovery process. The first situation had shorter failure and recovery time while the second situation had a larger time. They concluded that for both video conferencing and VoIP, RIPv2 is suitable for smaller networks compared to EIGRP. They also stated that OSPF was better for a very large network.

Most study in this area did not consider CODEC as a factor in determining call quality. The choice of CODEC is the first factor in determining the quality of a call. Generally, the higher the Bit rate used for the CODEC, the better the voice quality. Higher bit rate CODECs, however, take up more space on the network and also allow for fewer total calls on the network [11]. JDS Uniphase corporation believe G.711 is considered the highest quality. That is why in this paper we configured G.711 as the CODEC for this VoIP evaluation. Therefore, all our analysis and results are based on G.711 CODEC.

4. SIMULATION AND DESIGN

It is very expensive and time consuming to deploy a complete test bed containing multiple networked computers, routers and data links to validate and verify network protocols or a specific

network algorithm in network research area, although this is feasible [30]. The design process for this work is achieved via network simulation. A lot of study has been done about the need for simulations in computer networks. Obiniyi et al [31] described network simulation as one of the three broad techniques currently used in performance analysis and evaluation of computer networks compared to the analytical modelling and measurements technique which they carefully studied.

The simulation for this work is done with the new Riverbed Modeller Academic Edition 17.5 PL6. This replaces IT Guru Academic Edition for Educational users. It contains tools for all phases of study, model design, simulation, data collection and analysis [32].

4.1. Network Topology

The topology used is a small network, which consists of four 7200 routers labelled *R1*, *R2*, *R3* and *R4*, two Ethernet switch labelled *switch1* and *switch2*, and two IP Phone 1 and Phone 2. All the devices are connected together with the routers connecting to each other using point to point (PPP) Digital Signal 3 (DS3) link model and is shown in Figure 2 and Figure 3.

For proper comparison, we are going to have four scenarios configured with the same network model. These scenarios will be subdivided based on the IP technology used, the first and second scenario will be configured for IPv4, and then the third and fourth will be configured on IPv6. Subsequently, each IP technology will be configured using their respective routing protocols for both RIP and OSPF.

The Application definition, profile definition and failure recovery object was configured from the object palette using similar parameter for VoIP, including the encoding technology which was PCM with G.711 CODEC. This is used because of its simplicity and it is considered the highest quality [26]. G.711 is known for its toll quality as well [25].

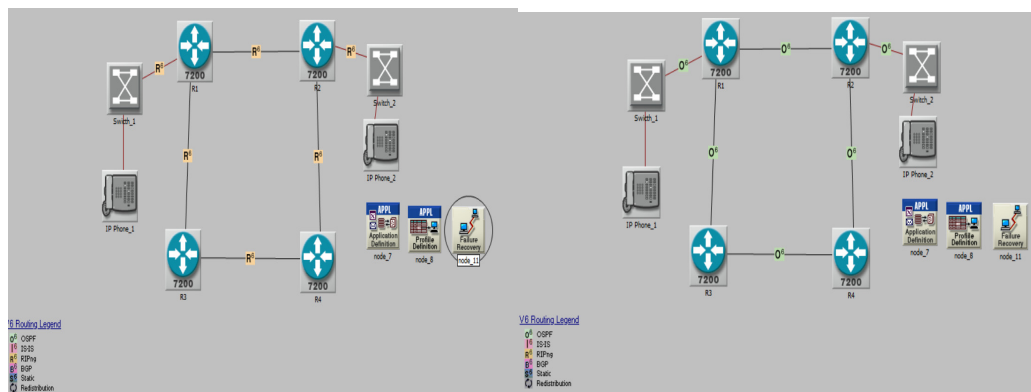


Figure 2. IPv6 environment with RIPng and OSPFv3

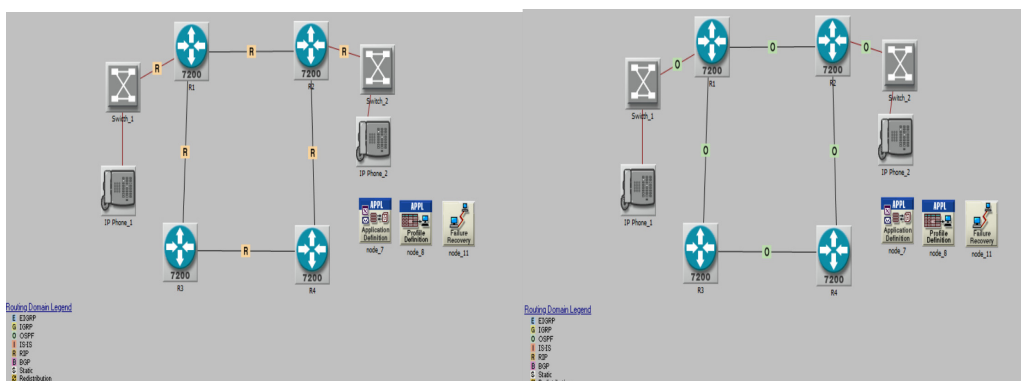


Figure 3. IPv4 environment with OSPF

The failure recovery process is configured between R1 and R2 based on the information in Table 1. The link fails and recovers after 300secs (5 minutes). However, the simulation will run for 35 minutes.

Table 1. Link Recovery/Failure.

| Time (Second) | Status |
|---------------|---------|
| 300 | Fail |
| 600 | Recover |
| 900 | Fail |
| 1200 | Recover |
| 1500 | Fail |
| 1800 | Recover |

The Comparison is between two routing protocols and two IP technologies. These will be evaluated based on their effect on some VoIP metrics. The VoIP environment could either be a network running on IPv4 or IPv6.

5. EVALUATION OF PERFORMANCE AND RESULTS

There are a lot of factors which can affect the performance of Voice quality. These include Jitter, packet end to end delay, packet end to end variation and packet loss and echo [30]. The factors including other parameters will serve as the functional metrics for comparing the routing protocols for this experiment. Tangential, to the simulations below are the results.

5.1. Traffic Sent

This is the total voice traffic sent from the source IP Phone to the destination IP phone across the simulated network. Based on the result in Figure 4, OSPFv3 sends less traffic compared to RIPng in an IPv6 environment. This also happens in the IPv4 environment, except that we have more traffic sent using OSPFv3 than OSPFv2. When the traffic sent is less, this means the performance for OSPF is better in both IPv6 and IPv4 environments. This will reduce congestion as well as latency. We can see that OSPF sent 14600 bytes/sec compared to RIP which sends 1500 bytes/sec just to send the same voice traffic from Phone 1 to Phone 2 at a given time.

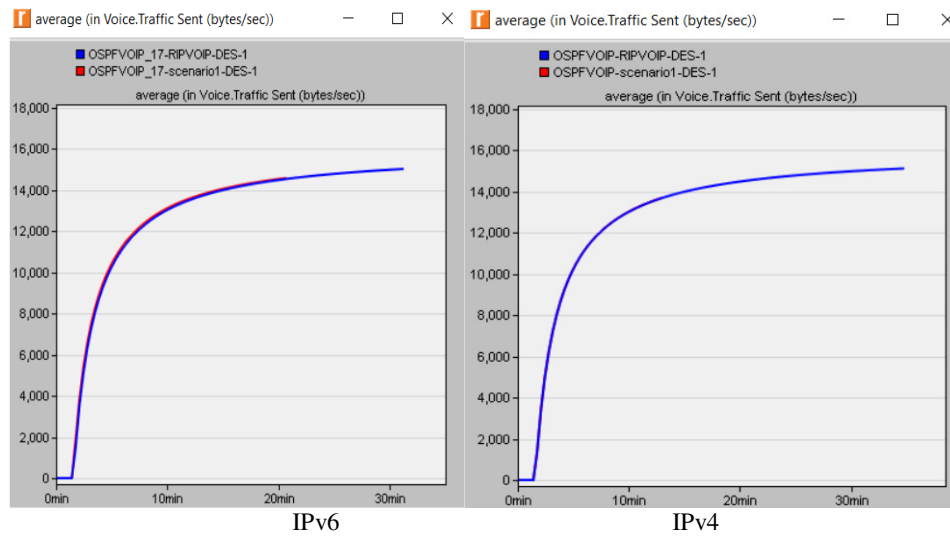


Figure 4. Voice Traffic Sent in bytes vs Time

5.2. Received Traffic

This is the total voice traffic received when a phone call was placed from Phone 1 to Phone 2. The IPV6 environment with OSPFv3 running on the network received less traffic than RIPng. OSPF in IPV4 also received less traffic than OSPFv3.

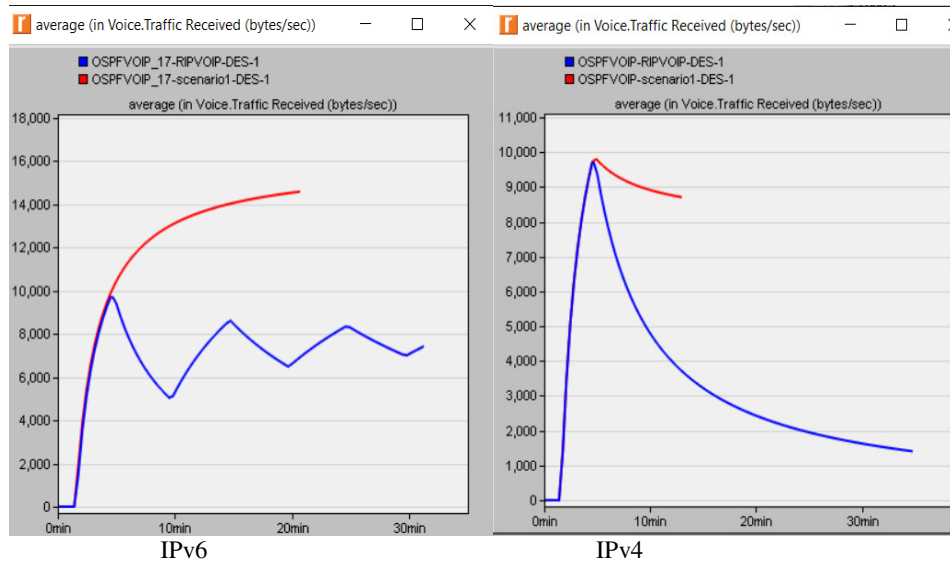


Figure 5: Voice Traffic received vs Time

5.3. Packet Delay Variation

The performance metric, Packet Delay Variation(PDV) is based on the difference in the One-Way-Delay (OWD) of selected packets. This difference in delay is called "IP Packet Delay Variation (IPDV)." This was defined in a draft of the IETF [33]. When the average IPDV is higher, there is usually low performance [34]. From our result in Figure 6, OSPF has a lower PDV with an average voice PDV of 0.3 microseconds. This situation is the same with the IPv4 environment.

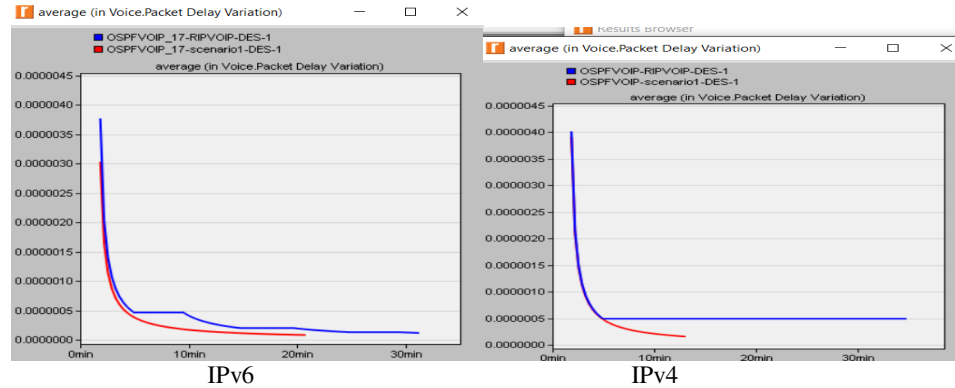


Figure 6. Packet Delay Variation.

5.4. Jitter

The variation in the arrival time of the packets at the receiver end leads to jitter. This will affect the quality of conversation. The sender is expected to transmit each voice packet at a regular interval. But jitter affects the speech in such a way that all the voice packets do not get to the decoder at the right time, thereby making the reconstructed speech sporadic [33/23]. From this result, RIPng and RIPv2 have a lower jitter compared to OSPF in both IPv6 and IPv4.

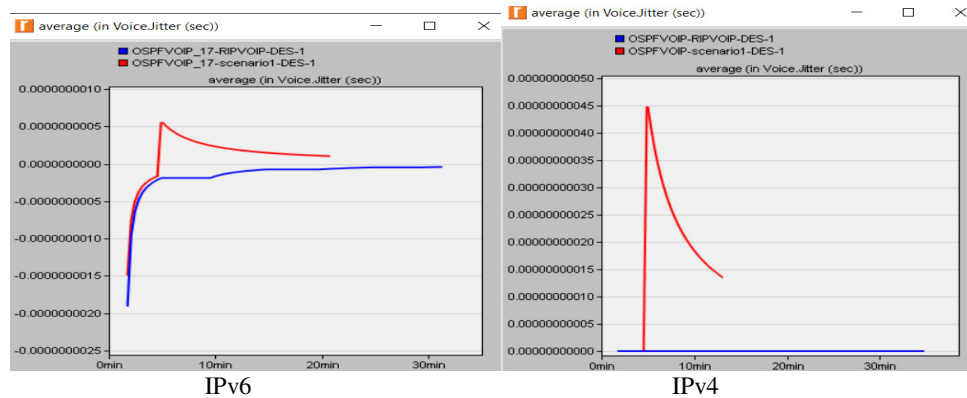


Figure 7. Voice Jitter vs Time

5.5. Dropped Traffic

Packet loss in VoIP will typically have a slowly degrading impact on speech communications. The human ear is very good at handling the short gaps that are typical of packet loss. Therefore, it may take a significant amount of packet loss to occur before a user can notice this loss in the form of speech degradation [26]. When a packet travels from source to destination and is not able to find a next hop address, it drops the packets. A consistent drop in traffic leads to speech degradation. Traffic dropped can also be called packet loss. This can be seen as the failure of one or more packets to reach their destination across the network. The maximum allowable packet loss is less than 1% for WANs and less than 0.05% for LANs [35]. From our result, RIPng has less traffic dropped compared to OSPFv3. Despite all the link failures and recoveries, RIPng isn't really disturbed by this. This is because of the Bellman Ford algorithm, which gives RIPng/RIP greater resilience and lower convergence time in a small network compared to OSPFv3/OSPF. However, we also notice that after the first link failure, OSPF in IPv4 drops lesser traffic, while RIPv2 causes more traffic loss.

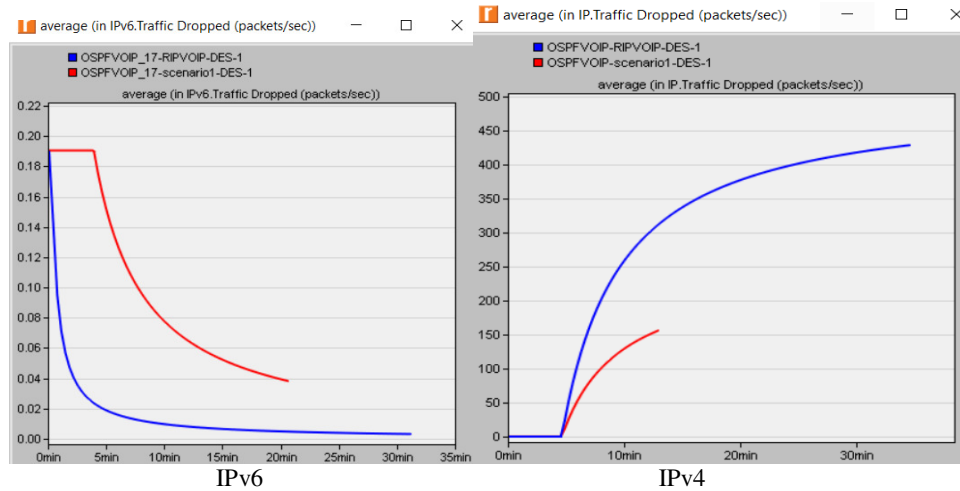


Figure 8. Traffic Dropped

5.6. Mean Opinion Score (MOS)

This is a subjective test that is usually on a scale from 1 to 5. A 5 denotes excellent and a 1 denotes unacceptable. MOS is used for individual opinion scores. Therefore, there is a great relationship between MOS and user experience [36].

Figure 9 shows that in the IPv6 environment, when the link failed and recovered for the first time, the MOS value for both OSPFv3 and RIPng was the same. However, as soon as the link failed again after 5 minutes, MOS for RIPng started reducing while the MOS for OSPFv3 remained stable. On the other hand, the MOS value for RIPv2 in the IPv4 environment was constantly at 4 while OSPF reduced to about 4.03254. Based on these variations, we conclude that RIP has more resilient to link failure in a small network than OSPF both in IPv6 and IPv4 environment.

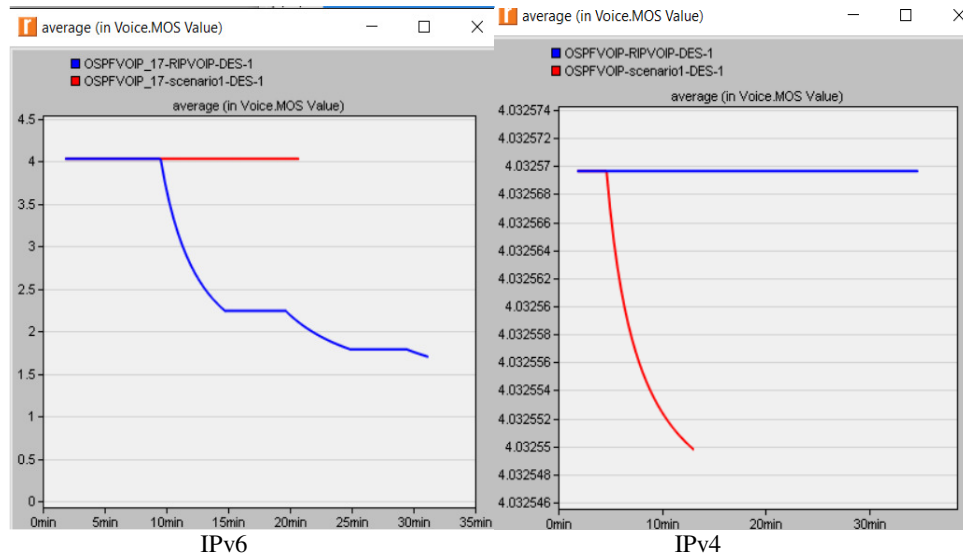


Figure 9. MOS Values

5.7. End to End Delay

This is the average time taken by the voice traffic to travel from one phone to the other. This includes all the delays caused by the route discovery process and queue in data packet transmission. Only the data packets that successfully delivered to the destination are counted. The lower the value of end to end delay, the better the performance of the protocol [37]. From our results, we can see that from both the IPv6 and IPv4 environments, RIPng and RIPv2 have a lower end to end delay value. One of the reasons is because RIP converges faster as it goes through fewer hops to get to its destination.

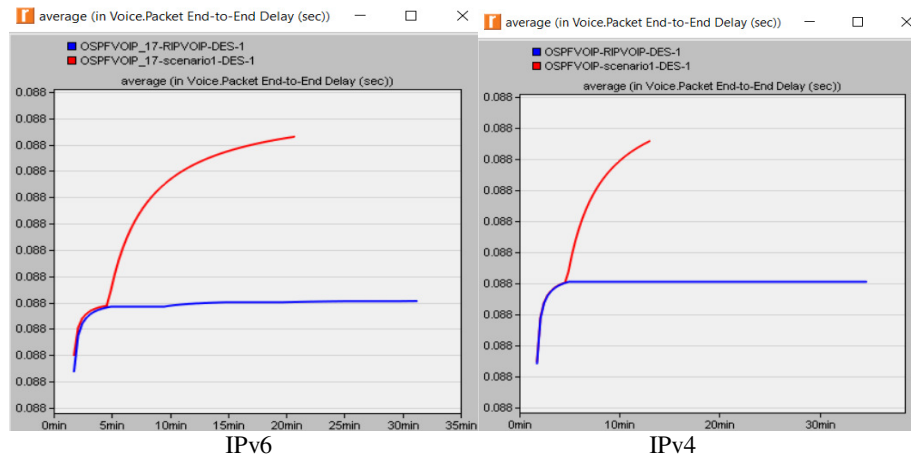


Figure 10. Packet End to End Delay

6. CONCLUSIONS

Selecting an appropriate CODEC for any VoIP deployment is a major factor in determining its voice quality. The VoIP simulation and result analysis for this paper is based on G.711 CODEC.

Currently, G.711 is the best CODEC available for voice encoding. Another consideration for VoIP deployment is the network topology and the routing involved. This study has successfully compared two routing protocols, RIP and OSPF. We analysed them in IPv4 and IPv6 using G.711 CODEC to measure the performance of VoIP in a small network using seven metrics. The result shows OSPFv3 sent less traffic than RIPng when a call is placed from one end to the other, although OSPFv3 sent more traffic than OSPFv2. Considering packet delay variation, the higher the packet delay variation the lower is the performance. From the results, we noticed that OSPFv3 has a better packet delay variation than OSPFv2, RIPv2 and RIPng. However, RIPng has less traffic dropped, less end to end delay, and less jitter experience compared to RIPv2, OSPFv3 and OSPFv2. Because MOS is subjective, both IPv4 and IPv6 had a stable MOS value, but after the link failure we noticed a decline in the MOS value for RIPng and OSPFv2. Our future work will include analysing other protocols like IS-IS from a similar perspective and comparing other CODECs for this simulation.

REFERENCES

- [1] Kuhn, D. Richard, Walsh, J. Thomas & Fries, G. Steven. (2005). Security Considerations for Voice over IP Systems. Special Publication (NIST SP) - 800-58(). Retrieved 25 May, 2016, from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=150222
- [2] Pravda, I & Vodrazka, J. (2007). Voice Quality Planning for NGN Including Mobile Networks. 12th International Conference on Personal Wireless Communications, 245(1),376–383.
- [3] Lin, S.J & Yang, D.L. (2015). Capability measure for VoIP Performance. Journal of Testing and Evaluation, 43(5),
- [4] Mitchell, B. (2016). IP - Internet Protocol. Retrieved 26 May, 2016, from http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm
- [5] Dutta, N, Pokhrel K, Biradar S.R, Gautam, K, Abusafi, Md, Pradhan,S, Chakraborty, K, Bhattacharyee S. (2014). Analysis of Packet Transmission Overhead of IPv4 and IPv6 through simulation. International journal of computer applications, (), pp 20-21.
- [6] Che, X & Cobley, L.J. (2009). “VoIP performance over different interior gateway protocols.” International journal of communication network and security, Vol. 1, No.1.pp 34-41
- [7] Rev.C. (2014) Measuring Network Convergence Time. Retrieved 25 May, 2016, White paper from <https://www.ixiacom.com/sites/default/files/resources/whitepaper/convergence.pdf>
- [8] Albkerat, A & Isaac, B. (2014). Analysis of IPv6 Transition technologies. International journal of Computer network & communications, 6(5),
- [9] Moy, J. (1994). OSPF Version 2. Request for Comments: 1583, Retrieved 25 May, 2016, from <https://www.ietf.org/rfc/rfc1583.pdf>
- [10] Lammle, T. (2007). Cisco Certified Network Associate Study Guide. (6th ed.). Indiana: Sybex.
- [11] Chipps, K.M. (2016). Kenneth M Chipps PhD. Retrieved 25 May, 2016, from www.chipps.com
- [12] Berger, L. (April 2009).OSPFv3 Based Layer 1 VPN Auto-Discovery. IETF. RFC: 5523. Retrieved 25 May, 2016, from <https://tools.ietf.org/html/rfc5523>
- [13] Cisco. (2012). IPv6 Configuration Guide, Cisco IOS Release 124T. Retrieved 26 May, 2016, from <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/12-4t/ipv6-12-4t-book/ip6-ospf.html>
- [14] Coltun, R, Ferguson, D, Moy, J, (July 2008). OSPF for IPv6.IETF. STD1. RFC:5340 Retrieved 25 May, 2016, from <https://tools.ietf.org/html/rfc5340>
- [15] Javvin Technologies Inc. (2005). RIPng: Routing information protocol next generation for IPv6. In Javvin (Ed), Network Protocol Handbook (pp. 76-77). California: Javvin Technologies.
- [16] Kozierok, C.M. (2005). RIPng. [Weblog]. Retrieved 26 May 2016, from http://www.tcpipguide.com/free/t_RIPngRIPv6MessageFormatandFeatures.htm

- [17] H3c. (2016). IP routing technology. Retrieved 25 May, 2016, from http://h3c.com/portal/Products___Solutions/Technology/IP_Routing/Technology_White_Paper/200811/619458_57_0.htm
- [18] Malkin, G. (January 1997). IETF. RIPng. RFC:2081. Protocol Applicability Statement Retrieved 25 May, 2016, from <https://www.ietf.org/rfc/rfc2081.txt>
- [19] Juniper. (2016). RIPng Overview. Retrieved 25 May, 2016, from https://www.juniper.net/documentation/en_US/junos13.3/topics/concept/routing-protocol-rip-ng-security-overview.html
- [20] Allied Telesis (2016). RIPng. Retrieved 25 May, 2016, from http://www.alliedtelesis.com/userfiles/file/RIPng_Feature_Overview_Guide.pdf
- [21] Crankshaft. (). RIPng Message format. [Weblog]. Retrieved 26 May 2016, from <http://what-when-how.com/ipv6-advanced-protocols-implementation/introduction-to-ripng-ipv6-unicast-routing-protocols/>
- [22] Malkin, G.; Minnear, R. (January 1997), IETF.RFC: 2080.RIPng for IPv6. Retrieved 25 May, 2016, from <https://tools.ietf.org/html/rfc2080>
- [23] Singh H. Pal, Singh, S, Singh, J, Khan, S.A. (2014). VoIP: State of art for global connectivity-A critical review. *Journal of Network and computer Applications*, 37(), 365-379.
- [24] Che, X & Cobley, L.J. (2009). VoIP performance over different interior gateway protocols. *International journal of communication network and security*, 1(1),
- [25] Hussein,W.M & Jamwal, S (2016). Comparative analysis of various routing protocols. *International Journal of modern Engineering Research*.
- [26] Narula, R & Pallarvi, A. (2014). Performance evaluation of RIP and OSPF in IPv6 using OPNET 145 simulator. *International journal of technical research and applications*, Volume 2(6), 37-41.
- [27] Ahmed M, Litchfield T, Alan, Ahmed, S,. (2014). VoIP Performance Analysis over IPv4 and IPv6. *International journal of computer Network and Information Security*, 11(), 43-48.
- [28] Kaur, J & Singh, E.P. (2014). Comparative Analysis of IPv6 Based IS-IS and OSPF-v3 Protocols. *International journal of engineering sciences & research technology*, 3(7),
- [29] Whitefield, R.J & Zhu, S.Y. (2015). A comparison of OSPFv3 and EIGRPv6 in a small IPv6 enterprise network. *International journal of Advanced computer science and Application*, 6(1),.
- [30] JDS Uniphase Corporation, VoIP Overview (2010) Retrieved 23 May, 2016, White paper from <http://www.viavisolutions.com/sites/default/files/technical-library-files/voipterm-wp-acc-tm-ae-0210.pdf>
- [31] Obiniyi, A.A, Abur, M & Soroyewun, M.B. (2014). New innovations in performance analysis of computer Networks: A review. *International journal of Applied information systems*, 6(2249-0868).
- [32] Riverbed. (2016). Riverbed Academic Modeler Release Edition. Retrieved 26 May, 2016, from <https://splash.riverbed.com/community/product-lines/steelcentral/university-support-center/blog/2014/06/11/riverbed-modeler-academic-edition-release>
- [33] Hagen, S. (2006). Routing protocols. In Apandi, T & Loukides, M (Eds), 23 IPv6 essentials (pp. 156). Paris: Oreily publishers.
- [34] Demichelis, C. & Chimento, P. "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)," RFC 3393 (Proposed Standard), Internet Engineering Task Force, Nov. 2002. [Online]. Available: <http://www.ietf.org/rfc/rfc3393.txt>.
- [35] Sevone. (2015). A Guide to Ensuring Perfect VoIP Calls. Retrieved 26 May, 2016, from <https://www.sevone.com/content/guide-ensuring-perfect-voip-calls>
- [36] Slattery, T. (2013, 26th November). Troubleshooting VoIP Packet Loss. [Weblog]. Retrieved 26 May 2016, from <http://www.nojitter.com/post/240164279/troubleshooting-voip-packet-loss>
- [37] Telkemy, A, Clark, Huawie, Q, Wu, Schott, R, Zorn G, "RTP Control Protocol (RTCP) Extended Report (XR) Blocks for Mean Opinion Score (MOS) Metric Reporting.," RFC 7266(Proposed Standard), Internet Engineering Task Force, Jun. 2014. [Online]. Available: <https://tools.ietf.org/html/rfc7266>

Authors

Mahbubur Syed is currently a professor and chair of Computer Information Science Department at Minnesota State University, Mankato USA. He also taught at the North Dakota State University in USA, Monash University in Australia, Bangladesh University of Engineering and in Bangladesh, and also worked at Ganz Electric Works in Hungary. He has more than 100 papers published in journals and conference proceedings. He has been serving in different roles such as co-editor-in chief, associate editor, editorial review committee, member of editorial board in several international journals. He has been involved in international professional activities including organizing conferences and serving as conference and program committee chair.



Isaac Yerima Ambore worked as Graduate research assistant in Computer Information Science department at Minnesota State University Mankato. He received his Bachelor's degree in Computer Science from Ahmadu Bello University Zaria, Nigeria and is currently pursuing his masters in Information Technology in MSU with Dr Syed as his advisor. He is a CISCO certified Network Professional (CCNP) and also a CISCO certified Design Professional (CCDP). His current research interests include VoIP Performance and information security risk.

