Study of IPv6 Protocol in the Data Model of the Smart Grid Distribution Domain

Estudio del protocolo IPv6 en el modelo de datos del Smart Grid Distribution Domai

Estudo do protocolo IPv6 no modelo de dados do domínio de distribuição de Smart Grid

Guillermo Adolfo David Nuñez[1]
Fabio German Guerrero[2]

Received: January 20th, 2020
Accepted: April 20th, 2020
Available: May 31th, 2020

How to cite this article:
G. A. David Nuñes, F. G. Guerrero, "Study of IPv6 Protocol in the Data Model of the Smart Grid Distribution Domain," *Revista Ingeniería Solidaria*, vol. 16, no. 3, 2020.
doi: https://doi.org/10.16925/2357-6014.2020.02.07

Artículo de investigación. https://doi.org/10.16925/2357-6014.2020.02.07

[1] Institución Universitaria Antonio José Camacho. Director Operativo Programa Ingeniería Electrónica.

ORCID: https://orcid.org/0000-0001-9446-2406

E-mail: gdavid@admon.uniajc.edu.co

[2] Escuela de Ingeniería Eléctrica y Electrónica. Universidad del Valle. Profesor Titular.

ORCID: https://orcid.org/0000-0002-5658-9497

E-mail: fabio.guerrero@correounivalle.edu.co

Abstract

Introduction: This article is the product of the research "Study of IPv6 Protocol in the Data Model of the Smart Grid Distribution Domain" developed at the Universidad del Valle and carried out during 2019, in which a description of the models and communication architectures for a Smart Grid in the domain of distribution is demonstrated. This description includes the definition of the communication requirements such as latency, bandwidth, traffic volume, and assignment of addresses for different applications.

Problem: There is an immediate need to establish standards and protocols for the Smart Grid, for both the electrical components and the component technologies of information and communication.

Objective: The objective of the research is to characterize the use of IPv6 in the context of the communications domain distribution of the Smart Grid.

Methodology: The work defines a virtualization environment in which the performance of IPv6 in the domain distribution of the Smart Grid will be evaluated; this evaluation includes the measurement and analysis of delays as well as traffic volumes, bandwidth, cyber-security conditions, and time allocation of network addresses.

Results: The IPv6 protocol is considered as a viable alternative in the Smart Grid communication model in order to comply with the communication requirements.

Conclusion: The implementation of Quality of Service QoS in IPv6, defined in RFC2474, is essential in the Smart Grid communication network in order to meet the communication requirements of the defined applications.

Originality: There is great expectation that networks based on the Internet Protocol will serve as a key element for communications within the Smart Grid.

Limitations: With the wide scope and dimensions involving Smart Grids, it is almost impossible to implement the communication network of a Smart Grid completely in a single simulation tool or emulation.

Keywords: Smart Grid, Internet Protocol, Latency, Throughput, Distribution Domain.

Resumen

Introducción: Este artículo es producto del proyecto de investigación "Estudio del Protocolo IPv6 en el modelo de datos del dominio de distribución de la Smart Grid" desarrollado en la Universidad del Valle en 2014 en el cual se muestra una descripción de los modelos y arquitecturas de comunicación para la Smart Grid en el dominio de distribución. Esta descripción incluye la definición de los requisitos de comunicación, como latencia, ancho de banda, volumen de tráfico y la asignación de direcciones para diferentes aplicaciones.

Problema: Existe una necesidad inmediata de establecer estándares y protocolos para Smart Grid tanto para los componentes eléctricos como para las tecnologías de la información y comunicación.

Objetivo: El objetivo de la investigación es caracterizar el uso de IPv6 en el contexto del dominio de distribución de comunicaciones de la Smart Grid.

Metodología: El trabajo define un entorno de virtualización en el que se evaluará el rendimiento de IPv6 en el dominio de distribución de la Smart Grid; Esta evaluación incluye la medición y el análisis de los retardos, así como los volúmenes de tráfico, el ancho de banda, las condiciones de seguridad informática y el tiempo de asignación de direcciones de red.

Resultados: El protocolo IPv6 se considera como una alternativa viable en el modelo de comunicación de la Smart Grid para poder dar cumplimiento a los requerimientos de comunicación.

Conclusión: La implementación de Calidad de Servicio (QoS) en IPv6 definida en el RFC2474, es fundamental en la red de comunicación de la Smart Grid para poder cumplir con los requerimientos de comunicación de las aplicaciones definidas.

Originalidad: Existe una gran expectativa de que las redes basadas en el Protocolo de Internet sirvan como un elemento clave para las comunicaciones dentro de Smart Grid.

Limitaciones: El amplio alcance y las dimensiones que involucran la Smart Grid, es casi imposible implementar la red de comunicación por completo en una sola herramienta de simulación o emulación.

Palabras clave: red inteligente, protocolo de internet, latencia, rendimiento, dominio de distribución.

Resumo

Introdução: Este artigo é o produto do projeto de pesquisa "Estudo do Protocolo IPv6 no modelo de dados do domínio de distribuição Smart Grid", desenvolvido na Universidade do Vale em 2014, no qual uma descrição dos modelos e arquiteturas de comunicação para uma Smart Grid no domínio da distribuição. Esta descrição inclui a definição dos requisitos de comunicação, como latência, largura de banda, volume de tráfego e atribuição de endereços para diferentes aplicativos.

Problema: Existe uma necessidade imediata de estabelecer padrões e protocolos para o Smart Grid, tanto para os componentes elétricos quanto para as tecnologias de componentes de informação e comunicação.

Objetivo: O objetivo da pesquisa é caracterizar o uso do IPv6 no contexto da distribuição do domínio das comunicações do Smart Grid.

Metodologia: O trabalho define um ambiente de virtualização no qual será avaliado o desempenho do IPv6 na distribuição de domínio do Smart Grid; essa avaliação inclui medição e análise de atrasos, bem como volumes de tráfego, largura de banda, condições de segurança cibernética e alocação de tempo dos endereços de rede.

Resultados: O protocolo IPv6 é considerado uma alternativa viável no modelo de comunicação Smart Grid para atender aos requisitos de comunicação.

Conclusão: A implementação da QoS da Qualidade de Serviço no IPv6 definida na RFC2474 é essencial na rede de comunicação do Smart Grid, a fim de atender aos requisitos de comunicação dos aplicativos definidos.

Originalidade: Há uma grande expectativa de que as redes baseadas no Protocolo da Internet sirvam como um elemento-chave para as comunicações dentro do Smart Grid.

Limitações: Com o amplo escopo e dimensões envolvendo as Smart Grids, é quase impossível implementar a rede de comunicação de uma Smart Grid completamente em uma única ferramenta de simulação ou emulação.

Palavras-chave: Rede Inteligente, Protocolo da Internet, Latência, Rendimento, Domínio de Distribuição.

1 INTRODUCTION

At present, there is a widespread global effort to modernize the electrical grid in order to increase reliability and power quality, as well as to achieve the inclusion and subsequent transition to renewable energy sources, reduction of greenhouse gases, and development of sustainable economies to ensure the prosperity of future generations. As a consequence of these efforts, the idea of the Smart Grid as an advanced network that converges on the integration of multiple computer technologies, digital communications, and services available for delivery to power users has been conceived. Therefore, there is an immediate need to establish standards and protocols for the Smart Grid for both the electrical components [1] (generation, transmission, and distribution) and the component technologies of information and communication.

Within the framework of the requirements of telecommunications defined for the Smart Grid, there is currently neither an established communication model nor a definition of standards and protocols that together meet the needs and requirements of communication for the Smart Grid, and thus Internet Protocol version 6 (IPv6) has been proposed as a communication platform for the Smart Grid. The integration of the IPv6 protocol with the Smart Grid is the main focus of this article.

In the national and international research context, there is growing interest worldwide in supporting the integration of new technologies and applications that will achieve the development and sustainability of the electricity networks of the future, including the implementation of renewable energy sources, distributed energy resources, electric vehicle integration, and demand management of electricity consumption, among others [2]. In order to support these technologies and applications, it is necessary to have a communication network that is modern, advanced, flexible, and scalable, with a bidirectional flow of information that meets the basic needs of monitoring and controlling the Smart Grid. The support of these applications requires the development of new recommendations and improvement of already existing ones to cover the basic aspects of communication from the physical layer to the application layer of the Open System Interconnection (OSI), as well as the definition of the architecture and communication model of the Smart Grid.

2. RESEARCH BACKGROUND

A. SMART GRID

It has already been recognized in the academic, research, and industrial arenas that the Smart Grid is a new power grid which fully integrates advanced technologies of sensing and measurement, information and communication technologies (ICT) for analysis and decision making, and automatic control technology with the infrastructure of the electric network [3] [4]. The definition for Smart Grid, provided by the U.S. Department of Energy, is an energy supply network that supports bi-directional power flow, distributed and automated, and permits real-time balancing of demand-supply via high speed computing and communications [5]. The fundamental goal of the Smart Grid is to ensure the operation of the energy system in a transparent, sustainable, environmentally friendly, cost-efficient, and mainly safe way [6] [7]. In Colombia, the development of the Smart Grid is led by the initiative called “Colombia Inteligente”, which has defined working groups in the areas of smart metering by Advanced Metering Infrastructure (AMI), ICTs, and the development of a maturity model that collects the context of the Colombian electricity sector. The strategy of this initiative provides coverage for Equity, Energy Security, Penetration of Clean Energy, Energy Efficiency, Competitiveness, Productivity, and Knowledge Generation [8].

B. COMMUNICATION IN SMART GRIDS

Communication, in the Smart Grid, refers to the information infrastructure and networking that allow the flow of information between the services/applications and the elements that are part of the physical equipment [3]. In the communication network, it is necessary to consider both the network architecture and performance metrics in order to meet the requirements of the applications and services, including aspects such as Quality of Service (QoS) and security in the transmission of information on the network. In [9], five kinds of applications are defined to facilitate the understanding of the communication architecture of the Smart Grid, and qualitative characterization is performed, taking into account the required network topology, amount of data, permitted latency, security, and reliability. Applications are: Smart metering, also known as AMI, Automatic Demand Response (ADR), Remote protection (Tele-protection), automated distribution and Management of micro-networks.

The data network for the Smart Grid must support a variety of communication technologies, starting from wired systems with copper, fiber, or Power Line Communications (PLCs) through wireless networks. The IP (Internet Protocol) has been devised as the fundamental protocol at the network layer for implementing applications beyond AMI (Advanced Metering Infrastructure) for the Smart Grid. In reference [10], a comprehensive list of potential applications for the Smart grid using the IP protocol in the distribution domain is presented. PLC (Power Line Communications) is one of the most important technologies for data transmission for the Smart Grid in the distribution domain. In reference [11], a state-of-the-art review of PLC technologies and applications for the Smart Grid is presented. Several works report the use of simulation in the study of different aspects of the Smart Grid. For instance, in reference [12], a comprehensive overview of simulation tools for power system simulators, communication network simulators, and combined power and communication simulators is presented. In reference [13], a PLC channel simulator implemented with the network simulator-3 (ns-3) is presented. There are several works oriented to evaluate the performance of PLC technologies at the data link layer, taking into account the impairments of the physical layer, such as in reference [14], where a simulation of the PRIME technology by means of Matlab and OMNeT+ simulations is presented. Our work is fundamentally different because it is oriented toward performance analysis at the network layer, considering different conditions of the underlying infrastructure by using a virtual environment.

In Table I, the specific communication requirements for the Smart Grid are specified.

Table I. Communication Requirements of the Smart Grid

Parameter	Description
Number of devices	As networks expand on a large scale, it is expected that the number of devices connected to the network will increase substantially and, as a consequence, the number of addresses needed to unambiguously identify these devices will also tend to grow considerably.
QoS	Different metrics should be considered, such as end-to-end latency, bandwidth, and reliability, with regard to the different types of applications.
Security and privacy	This covers the confidentiality, integrity and availability of electronic information systems necessary for the management, operation, and protection of the Smart Grid.
Traffic volume	Since new devices will be added in the Smart Grid, the network must carry more messages simultaneously without diminishing the latency requirements.
Latency	This is one of the most stringent requirements for the Smart Grid. For example, if a substation loses any input data, it can replace that entry with any value from another sensor, producing undesired control actions which generate erroneous results.
Dynamic network	Most Smart Grid nodes are static; however, it should be considered that electric vehicles and some nodes will have mobility.
Heterogeneity of media	Data transmission will occur over multiple media, from copper cabling systems and fiber or PLCs to wireless and cellular network technologies.
Routing	Due to the heterogeneity of devices, links, and node types, achieving interoperability requires different routing techniques.

Source: [15]

The current communication network is inadequate, inflexible, and costly. The insufficiency lies in several factors: First, the current networks provide coverage only to the domains of generation and transmission, but there is no coverage for domain distribution, which is expected to present many changes to the Smart Grid. Second, the capacity and speed of installed communication networks are insufficient to accommodate the future capacity and speed requirements of Smart Grid applications. Third, modifications to existing networks are difficult and cumbersome, and the addition of new participants to the network may require installations or modifications that are not only costly in terms of design, hardware, and programming, but also increase the latency in sending data [15]. However, the IEEE 2030-2011 standard has been broadly accepted as the first industry standard with a SG architecture, and configuration and inter-operability requirements [16] [17]. Among the stakeholders in the development of the Smart Grid, there is great expectation that networks based on the Internet Protocol (IP) will serve as a key element for communications within the Smart Grid. Although the IP cannot address all the requirements of communication, there are a series of important aspects that make it a fundamental technology for the Smart Grid [18] [19]. In [20] and [21], it is proposed that the communication solution for the Smart Grid is an IP-based network supported by optical fibers. Table II indicates the typical values of delay and bandwidth recommended in the data transmission of the most important applications of the Smart Grid [22].

Table II. Smart Grid Applications and Network Requirements

Application	Network Requirement	
	Bandwidth	**Latency**
AMI	10–100 kbps/node, 500 kbps backhaul	2–15 s
Demand response	14–100 kbps per node/device	500 ms to several minutes
Wide-Area Situational Awareness (WASA)	600–1500 kbps	20–200 ms
Distributed energy resources and storage	9.6–56 kbps	20 ms–15 s
Electric transportation	9.6–56 kbps, 100kbps	2 s – 5 min
Distribution grid management	9.6–100 kbps	100 ms–2 s

Source: [22]

3. METHODOLOGY

In Figure 1, a basic scheme of a communication network in the distribution domain for the Smart Grid is displayed. In this case, the collector devices are modeled through routers and relay devices are modeled by switches. The Electrical Service Interface (ESI) and smart meters are modeled by hosts [23].

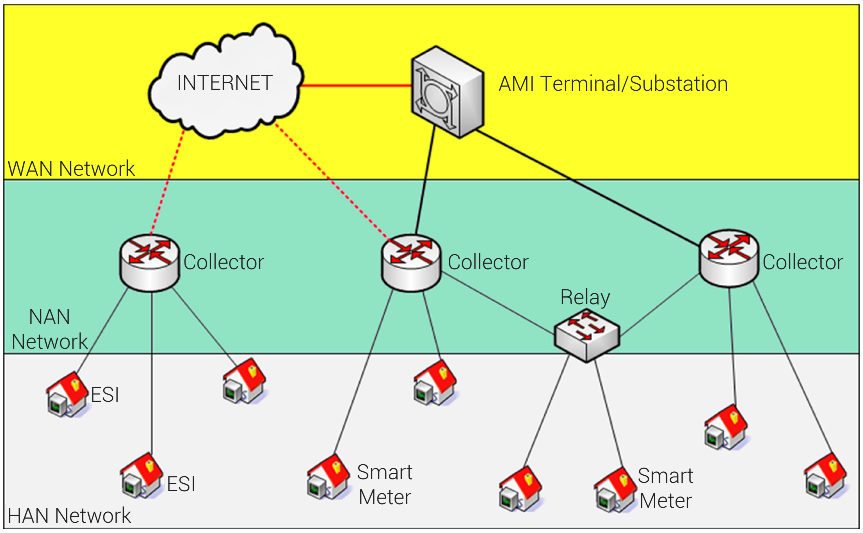

Figure 1. Basic architecture used in the simulation
Source: own work

Figure 2 shows the architecture implemented in software GNS3 with a maximum of only 6 of the 128 ESI nodes that can be used in the virtualization environment. Routers, identified as C1 to C5, represent collecting devices as mentioned above. One of the main objectives of the GNS3 virtualization environment is to measure the maximum bandwidth available (throughput) per node and the latency between the ESI nodes and the AMI terminal/substation.

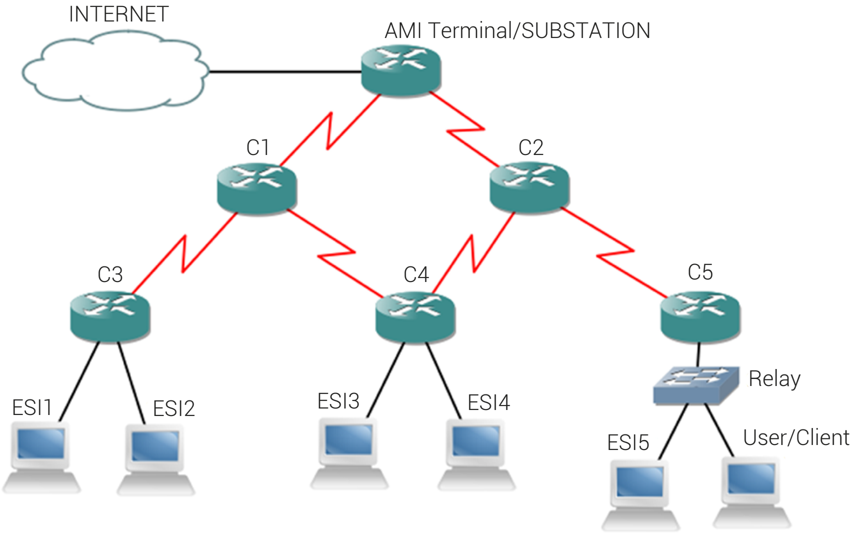

Figure 2. Architecture implemented in GNS3
Source: own work

These measurements were performed using the Distributed Internet Traffic Generator (D-ITG) version 2.6.1 software and the graphical user interface (GUI) D-ITG version 2.7 [24], [25]. The emulation is carried out by varying the number of nodes or ESI interfaces, from 1 to 128, with the aim of recreating several traffic situations and characterizing the conditions of bandwidth, latency and jitter based on the number of active nodes. In the emulation environment, seven cases were taken depending on the number of active nodes, which was 2, 4, 8, 16, 32, 64, and 128, where each one generates an average traffic of 100 kbps. Once the test scenario had been defined, different features offered by IPv6 and that are of special interest in the Smart Grid environment were simulated, such as: addressing, computer security, and QoS, which are described in the next section.

4. RESULTS

A. ADDRESS ASSIGNMENTS

The IPv6 network address allocation to Smart Grid end devices was assigned through collectors. There are two mechanisms provided by IPv6 for automatic address assignment: auto-configuration and DHCPv6 [26]. Both mechanisms were used in the virtualization environment in conjunction with DHCP. The measurement of the addresses' allocation times was done using the debugger available from the IOS of the router; the sniffer software Wireshark was also used. Figure 3 shows the results obtained when measuring the average bytes required by each allocation method.

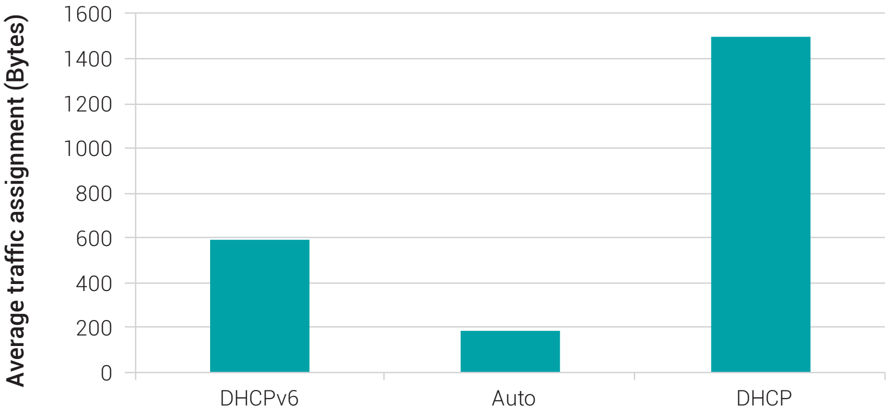

Figure 3. Average data volume assignment
Source: own work

Figure 4 shows the results obtained for the network address assignment times using the auto-configuration, DHCPv6, and DHCP methods.

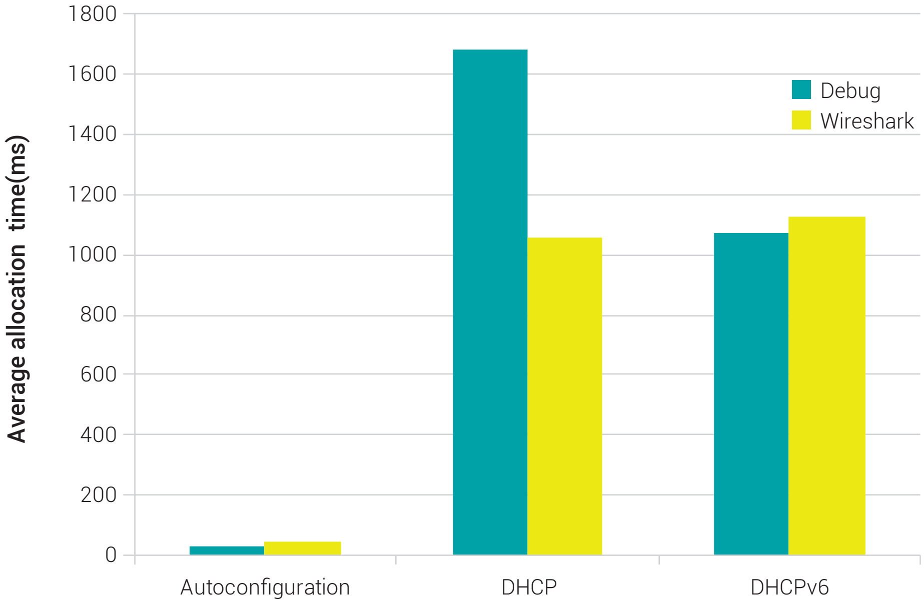

Figure 4. Time for IPv6 Address Assignment.
Source: own work

B. CYBER SECURITY

The implementation of security in IPv6 is performed through the implementation of the Internet Security Protocol (IPSec). For the purpose of the emulation, the network segment comprising communication between HAN networks and NAN-associated networks is taken [26]. An IPSec mode tunnel is then implemented through the Encapsulating Security Payload (ESP) protocol on a point-to-point HDLC link with a bandwidth of 1544 kbps supporting three different encryption algorithms: Data Encryption Standard (DES), Triple DES or 3DES, and Advanced Encryption Standard (AES). Figure 5 shows the results of the throughput measurement obtained without security and with IPsec IPv6 with the different encryption algorithms mentioned above.

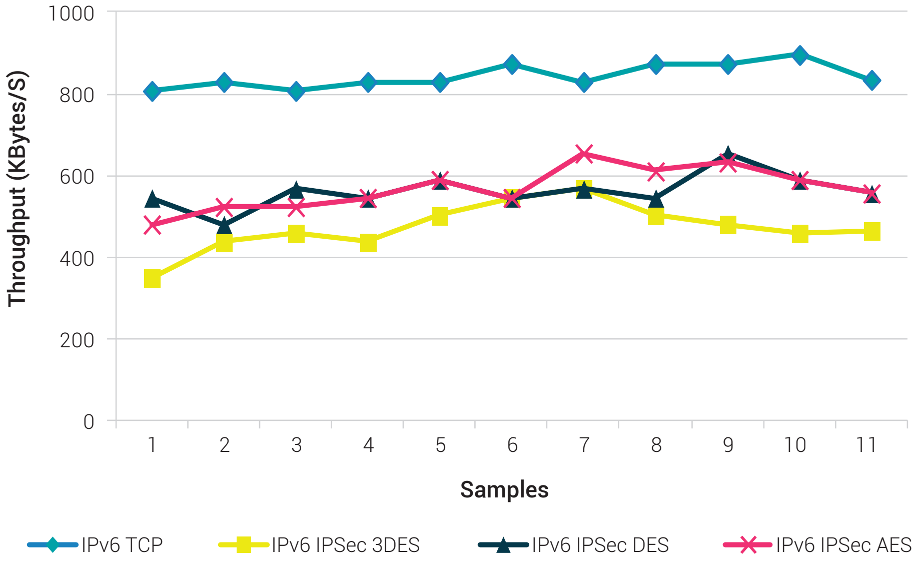

Figure 5. IPv6 link throughput comparison with and without IPSec
Source: own work

Figure 6 shows the mean delay obtained in the link analyzed, which was simulated initially without security and then with IPSec and different encryption algorithms.

C. QUALITY OF SERVICE

To implement QoS in IPv6, the use of Differentiated Services Code Points (DSCPs) defined in RFC2474 was contemplated and this code point is found in the header of the IPv6 packet in a field of eight bits called "Traffic Class".

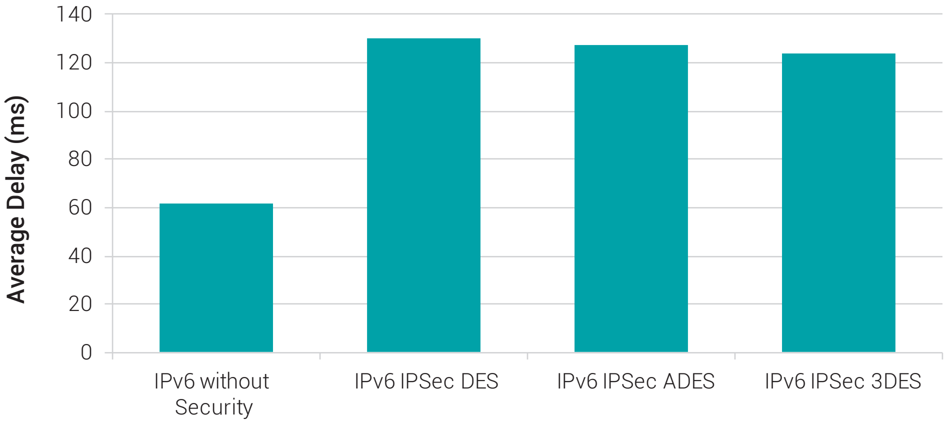

Figure 6. Average latency on IPv6 link with and without IPSec.
Source: own work

For data traffic generated by the "Customer" node, QoS policies were implemented, specifically defining three classes of traffic, in particular, of the 64 available according to RFC2474, which are detailed below: *Expedited Forwarding* (EF), which is defined in RFC3246 and characterized by low latency and low jitter, *Class Selector* CS3, which provides the highest effective bandwidth or throughput of the traffic labeled in this class and *Assured Forwarding* AF31, defined in RFC 2597 and updated in RFC 3260, whose characteristic is to ensure the data is forwarded with the least packets discarded.

Figure 7 shows the measurement result in the network latency between the "client" node located in the HAN network and a server acting as an AMI terminal located in the WAN network, based on the architecture in Figure 1.

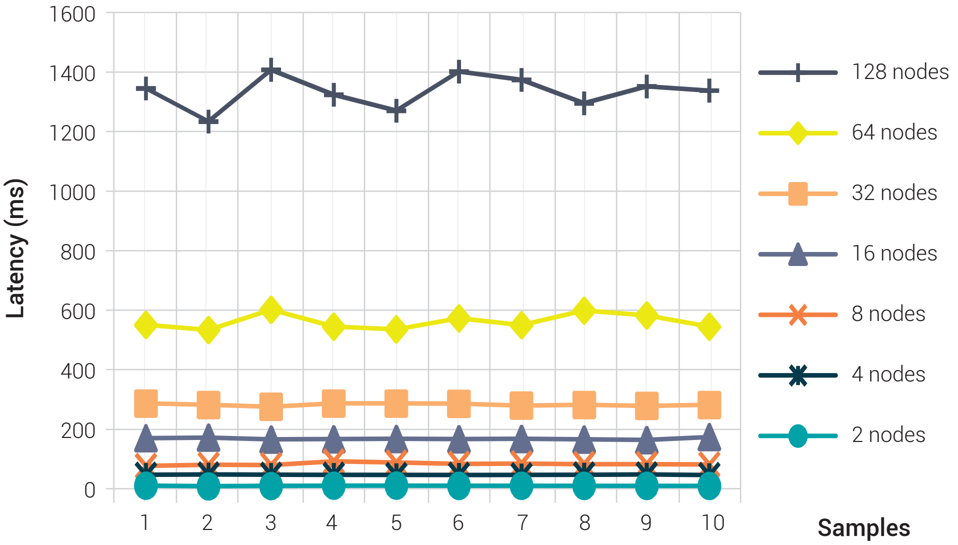

Figure 7. Latency measurement without QoS
Source: own work

Subsequently, traffic was tagged with the EF class, and routers acting as collectors were configured so that traffic tagged in this class had a priority of 70% of the other untagged traffic. The same previous measurement was performed and the results are shown in Figure 8.

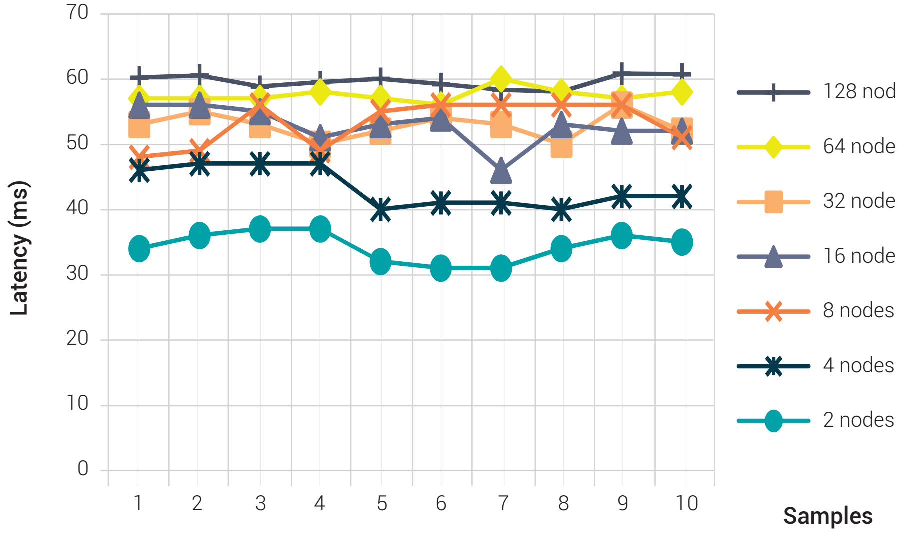

Figure 8. Latency measurement with QoS
Source: own work

By employing network architecture and traffic conditions similar to the previous case, the measurements of throughput were made on the same network segment used to measure latency. The results obtained from the emulation are shown in Figure 9, where the measurement of throughput for the analyzed traffic is presented; initially without traffic and subsequently considering the congestion caused by the other nodes in the network and without activating QoS policies.

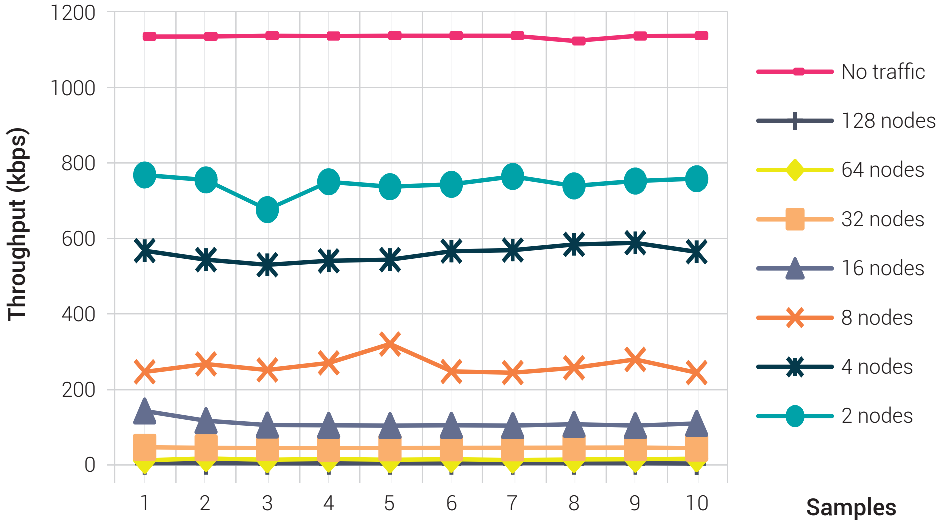

Figure 9. Throughput measurement without QoS
Source: own work

Subsequently, the QoS policy that was applied was the Class Selector 3 (CS3) and the class was configured to ensure throughput of 70% over the rest of the untagged traffic. The measurement results are shown in Figure 10.

5. DISCUSSION OF RESULTS

This section provides a discussion of the results obtained in relation to the requirements of latency, throughput, and security of each of the Smart Grid applications. In Figure 11, the measurement of latency is shown compared with the minimum threshold for applications of ADR and Distribution Grid Management.

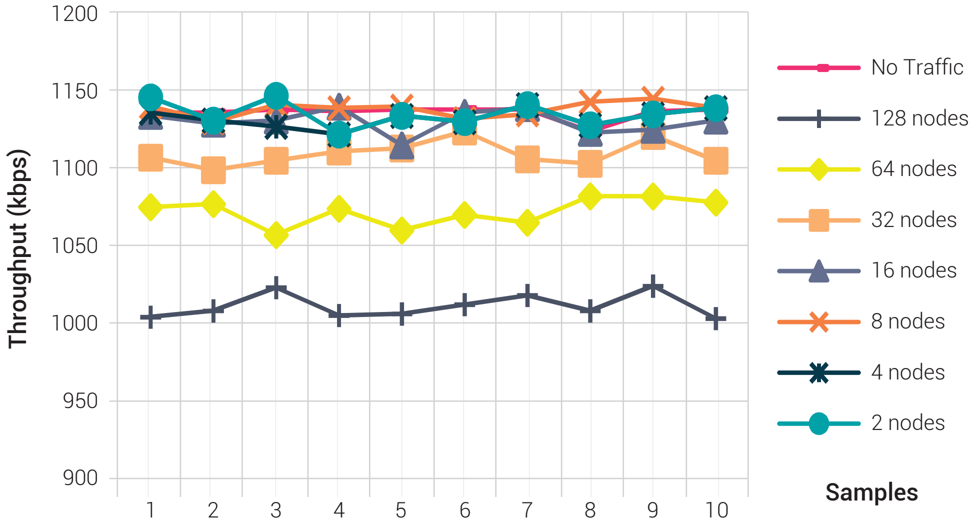

Figure 10. Throughput measurement with QoS
Source: own work

As observed in the figure, for ADR applications with 64 and 128 nodes without QoS policies, the minimum threshold defined in 500 ms was not met. Similarly, for applications in Distribution Grid Management with 32, 64, and 128 nodes without QoS policies, the minimum latency threshold set to 200 ms is not met. It is also noted that the implementation of QoS, in all cases, ensures compliance with minimum latency; however, this does not mean that the use of QoS is required for a high number of nodes, because the maximum thresholds are set at 2 s for Distribution Grid Management applications and several minutes for ADR applications. Figure 12 shows the delays obtained compared to latency thresholds for WASA and Tele-protection, which are the most demanding applications with regard to delays in the Smart Grid.

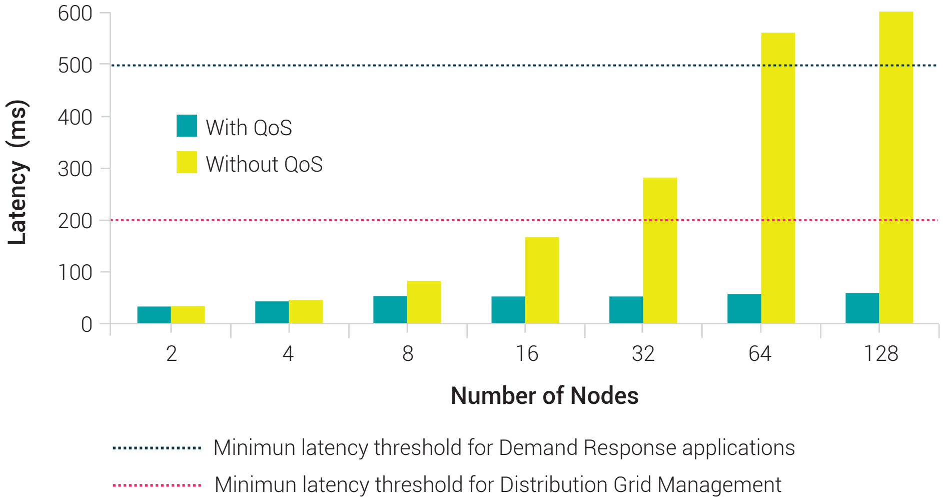

Figure 11. Latencies with respect to the threshold for ADR and Distribution Grid Management
Source: own work

As seen in Figure 12, the recommended requirements for latency in WASA applications of 20 to 200 ms are met, up to a maximum value of 16 active nodes. If more than 16 nodes are required, then it will be necessary to implement QoS policies. There is also evidence that for Tele-protection applications, whose recommended latency should not exceed 10 to 8 ms, it is not possible to comply with this delay requirement, even with the implementation of QoS policies. This result suggests that for Tele-protection, the implementation of protocols and technologies, on not only the network layer but also the link and physical layer, should be considered, ensuring the suggested latencies.

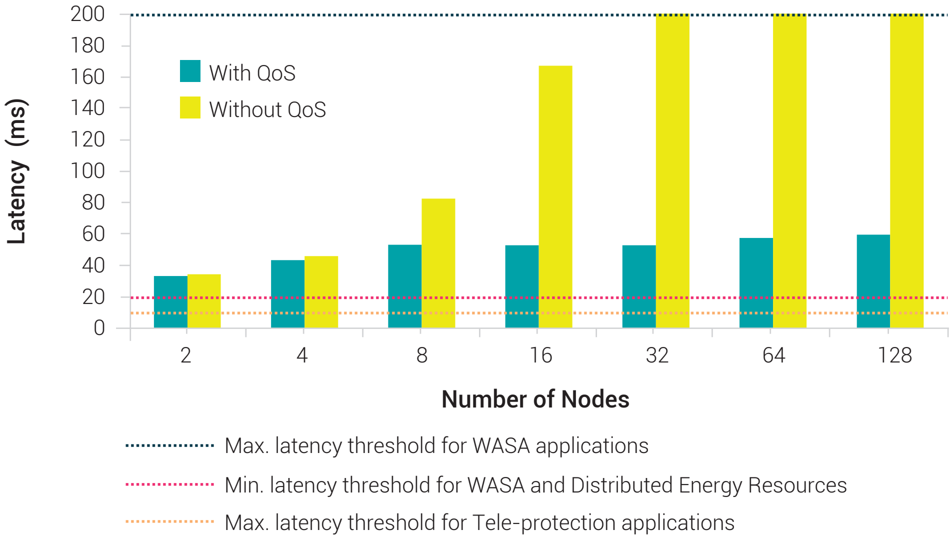

Figure 12. Latencies with respect to the threshold for WASA, Distributed Energy Resources, and Tele-protection applications
Source: own work

For analysis of the throughput results, compared with the minimum and maximum thresholds recommended in Table II, a procedure similar to that described above for the analysis of the latency measurements was performed. In Figure 13, the throughput measurement for 2, 4, and 8 nodes is shown in comparison with the recommended maximum and minimum throughput thresholds for WASA applications (between 600 and 1500 kbps). The recommended backhaul throughput threshold for AMI applications in 500 kbps. The recommended throughput threshold for Electric Transportation applications is 100 kbps and finally, the recommended maximum throughput threshold for ADR, AMI, Distribution Grid Management, and Tele-protection is 100 kbps.

As can be seen in Figure 13, most of the throughput requirements for the applications mentioned there, for 2, 4 and 8 active nodes on the network, are met; even before activating QoS policies. For WASA applications with more than four nodes and without QoS policies, there is no guarantee that the minimum recommended throughput will be met. With the above, and considering the small number of active nodes in the network, it is concluded that it will be necessary to implement QoS policies for WASA applications with special emphasis on the guaranteed bandwidth. Another case, in which no effect is given to recommended throughput, is that of "Backhaul" traffic generated by the AMI applications for more than four nodes, unless QoS policies are applied.

In Figure 14, the throughput measurement is shown for 16, 32, 64, and 128 nodes compared to the maximum recommended throughput thresholds defined for AMI, ADR, Electric Transportation, Distribution Grid Management and Tele-protection (100 kbps). The maximum recommended threshold for Distributed Energy Resources and Storage is 56 kbps. The minimum recommended threshold for ADR is 14 kbps and the minimum recommended threshold for AMI, Distributed Energy Resources, and Storage, Distribution Grid Management, and Tele-protection is 9.6 kbps.

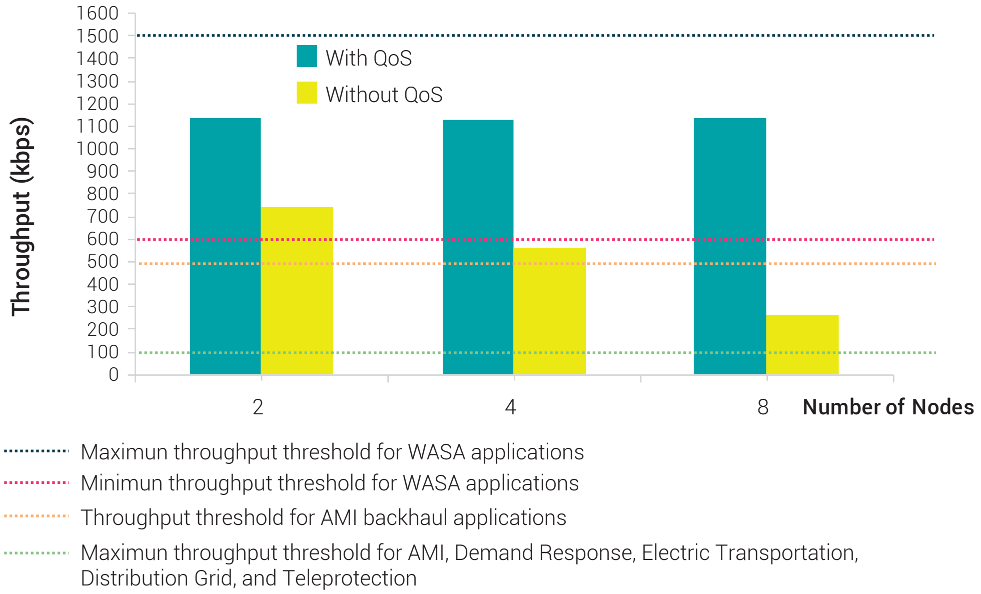

Figure 13. Throughput with respect to the threshold for Smart Grid applications with 2, 4, and 8 active nodes
Source: own work

As can be seen in Figure 14, for up to 16 nodes, the threshold is met for maximum throughput for AMI, ADR, Electric Transportation, Distribution Grid Management, and Tele-protection without the application of QoS policies. For a number of nodes greater than 16, the implementation of QoS policies will be needed to guarantee the recommended throughput in the applications mentioned. Figure 14 also shows that for 64 nodes, compliance is given to the minimum throughput thresholds for Demand Response, AMI, Distributed Energy Resources, and Storage, Distribution Grid Management and Tele-protection without the application of QoS policies. This last situation is probably the most critical in the simulations presented because it includes the largest number of applications in the distribution of the Smart Grid.

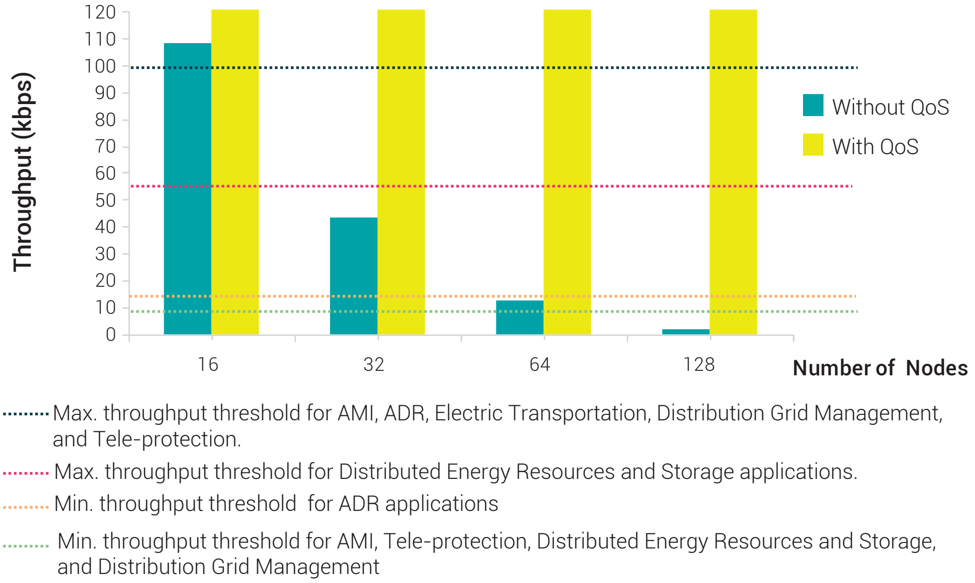

Figure 14. Throughput with regard to the threshold for Smart Grid applications with 16, 32, 64, and 128 nodes

Source: own work

6. CONCLUSIONS

- Because of its large coverage, the architecture of the Smart Grid communication network can be split into smaller coverage networks based on the actors involved and their applications, such as HAN and NAN networks. Similarly, the typical topologies, devices such as relays, collectors, AMI terminals, and ESI interfaces, and their interactions within the different types of networks in the Smart Grid were defined.
- A communication model for the distribution domain was defined in which HAN, FAN, WAN Networks and the Internet are integrated. The model is based on the architecture proposed by ITU-T and the reference model proposed by NIST. The model was proposed with the aim of integrating the IPv6 protocol and concludes that according to the results obtained and the level of compliance of the communication requirements, the IPv6 protocol is suitable for information transport in the distribution domain of the Smart Grid.
- A virtualization environment was created to integrate and validate the features of IPv6 with the communication model of the Smart Grid, and it was

concluded that due to the wide scope and dimensions involving Smart Grids, it is almost impossible to implement the communication network of a Smart Grid completely in a single simulation tool or emulation.

- Smart Grid applications will require a large number of network addresses to identify all devices that are expected to be installed in different user scenarios, service providers, and the entities of regulation and control. Therefore, the use of IPv6 with its massive address space widely meets this need for identification of Smart Grid demand. Similarly, the allocation of IPv6 network addresses using the auto-configuration mechanism is quite useful for addressing the devices on HAN and NAN networks.
- The security and integrity of information in the Smart Grid can be implemented with IPv6 by activating IPSec. Using IPSec increases delays and decreases network throughput dramatically, which may prevent compliance with the requirements of some applications of the Smart Grid. Therefore, security mechanisms must be implemented in the network segments that carry critical information that may compromise the stability of the power systems.
- The characteristics of communication in the Smart Grid, such as delays and throughput, are highly sensitive to the number of devices in the network. For AMI, ADR, Distributed Energy Resources and Storage, and Electrical Transportation, an approximate number of up to 64 active nodes without QoS meets the requirements of throughput and latency. For a larger number of nodes, it is essential to implement QoS policies.

References

[1] L. T. Berger and K. Iniewski, *Smart Grid Applications, Communications and security,* pp. 5-44, New Jersey: John Wiley & Sons, INC., 2012.

[2] P. A. Owusu and S. Asumadu-Sarkodie, “A review of renewable energy sources, sustainability issues and climate change mitigation,” *Cogent Engineering,* pp. 3-9, 2016. [Online]. doi: https://doi.org/10.1080/23311916.2016.1167990

[3] A. Pieroni, S. Noemi, D. Nunzio, F. Francesca and R. Mario, “Smarter City: Smart Energy Grid based on Blockchain Technology,” *International Journal on Advanced Science, Engineering and Information Technology*, pp. 298-302, 2018. [Online]. doi: 10.18517/ijaseit.8.1.4954

[4] C. Wei, “A Conceptual Framework for Smart Grid,” *2010 Asia-Pacific Power and Energy Engineering Conference*, Chengdu, China, pp. 1-4, 2010. [Online]. doi: 10.1109/APPEEC.2010.5448786

[5] U.S. Department Of Energy (DOE), “The Smart Grid: An Introduction”, pp. 8-43, 2010. [Online]. Available: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf. [Accessed 23 02 2017].

[6] National Institute of Standards and Technology NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*, pp. 14-147, September 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r3.pdf.

[7] N. S. Nafi, K. Ahmed, M. A. Gregory and M. Datta, “A Survey of Smart Grid Architectures, Applications,” *Journal of Network and Computer Applications,* pp. 23-33, 2016. [Online]. doi: https://doi.org/10.1016/j.jnca.2016.10.003

[8] Colombia Inteligente, *Antecedentes y marco conceptual del analisis, evaluacion y recomendaciones para la implementacion de redes inteligentes en Colombia*, pp. 25-55, 2016. [Online]. Available: http://www.upme.gov.co/Estudios/2016/SmartGrids2030/1_Parte1_Proyecto_BID_Smart_Grids.pdf

[9] Ye, Feng, Qian, Yi and Hu, Rose, *Smart Grid Communication Infrastructures*, pp. 205-228, 2018. [Online]. doi: 10.1002/9781119240136

[10] Noelia Uribe-Pérez, Itziar Angulo, David De la Vega & Txetxu Arzuaga «Smart grid applications for a practical implementation of IP over narrowband power line communications,» *Energies,* vol. 10, nº 11, pp. 3-9, 2017, doi: 10.3390/en10111782

[11] G. López, J. Matanza, D. De La Vega, M. Castro, A. Arrinda, “The Role of Power Line Communications in the Smart Grid Revisited: Applications, Challenges, and Research Initiatives,” *IEEE Access,* vol. 7, pp. 117346-117368, 2019. [Online]. doi: 10.1109/ACCESS.2019.2928391

[12] K. Mets, J. Aparicio Ojea, C. Develder, “Combining Power and Communication Network Simulation for Cost-Effective Smart Grid Analysis,” *IEEE Communications Surveys & Tutorials,* vol. 16, no. 3, pp. 1771-1796, 2014. [Online]. doi: 10.1109/SURV.2014.021414.00116

[13] F. Aalamifar, A. Schlögl, D. Harris, L. Lampe, “Modelling power line communication using network simulator-3,” de *2013 IEEE Global Communications Conference (GLOBECOM)*, Atlanta, GA, pp. 2970-2973, 2013. [Online]. doi: 10.1109/GLOCOM.2013.6831526

[14] J. Matanza, S. Alexandres, C. Rodriguez-Morcillo, "Automatic Meter-Reading Simulation through Power Line Communication," *IEEE 21st International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems*, San Francisco, CA, pp. 284-287, 2013. [Online]. doi: 10.1109/MASCOTS.2013.36

[15] A. Sheraz, S. M. Farhan, G. Sajjad A., Q. I.M. y A. Naveed, "Cognitive radio based Smart Grid Communication Network," *Renewable and Sustainable Energy Reviews,* pp. 535-548, 2017. [Online]. doi: https://doi.org/10.1016/j.rser.2017.01.086

[16] IEEE, *2030-2011 - IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads*, IEEE, pp. 21-27, 2011. [Online]. doi: 10.1109/IEEESTD.2011.6018239

[17] X. Fang, S. Misra, G. Xue y D. Yang, "Smart Grid - The New and Improved Power Grid: A Survey," *Communications Surveys & Tutorials,* vol. 14, no. 4, pp. 944-980, 2012. [Online]. doi: 10.1109/SURV.2011.101911.00087

[18] F. Lobo, A. Cabello, A. Lopez, D. Mora y R. Mora, "Distribution Network as communication system," *SmartGrids for Distribution, 2008,* Frankfurt, Germany , pp. 1-4, 2008. [Online]. doi: 10.1049/ic:20080448

[19] I. P. Solano Benítez, G. A. Méndez, N. M. Agredo Salazar, D. Cabezas Burbano, and C. I. Uribe Guirales, "Análisis comparativo de los Protocolos IPV6 e IPV4," *Ing. Solidar*, vol. 5, no. 9, pp. 42-53, Jan. 2010.

[20] A. Amit, K. Swathi y V. Pramode K., "A Proposed Communications Infrastructure for the Smart Grid," *2010 Innovative Smart Grid Technologies (ISGT)*, Gothenburg, Sweden , pp. 2-4, 2010. [Online]. doi: 10.1109/ISGT.2010.5434764

[21] J. Gao, Y. Xiao, J. Liu y W. Liang, "A survey of communication/networking in Smart Grids,» *Future Generation Computer Systems,* pp. 391-404, 2012. [Online]. doi: https://doi.org/10.1016/j.future.2011.04.014

[22] S. Nico; A. Kemal; U. Suleyman, "*A survey of routing protocols for smart grid communications*", pp. 2745-2771, 2012. [Online]. doi: https://doi.org/10.1016/j.comnet.2012.03.027

[23] International Telecommunication Union ITU-T, "Deliverable on Smart Grid Architecture", pp. 6-40, 2011. [Online]. Available: http://www.itu.int/en/ITU-T/focusgroups/smart/Pages/Default.aspx.

[24] A. Botta, A. Dainotti and A. Pescapé, “A tool for the generation of realistic network workload for emerging networking scenarios,” *Computer Networks,* pp. 3531-3547, 2012. [Online]. doi: https://doi.org/10.1016/j.comnet.2012.02.019

[25] S. Kolahi, S. Narayan, D. D. T. Nguyen and Y. Sunarto, “Performance Monitoring of Various Network Traffic Generators,” *13th UKSim-AMSS International Conference on Computer Modelling and Simulation*, Cambridge UK, pp. 501-504, 2011. [Online]. doi: 10.1109/UKSIM.2011.102

[26] R. Sangam y J. Daniel, “IPv6 Introduction and Configuration”, pp. 1-23, May 2012. [Online]. Available: https://www.redbooks.ibm.com/redpapers/pdfs/redp4776.pdf.