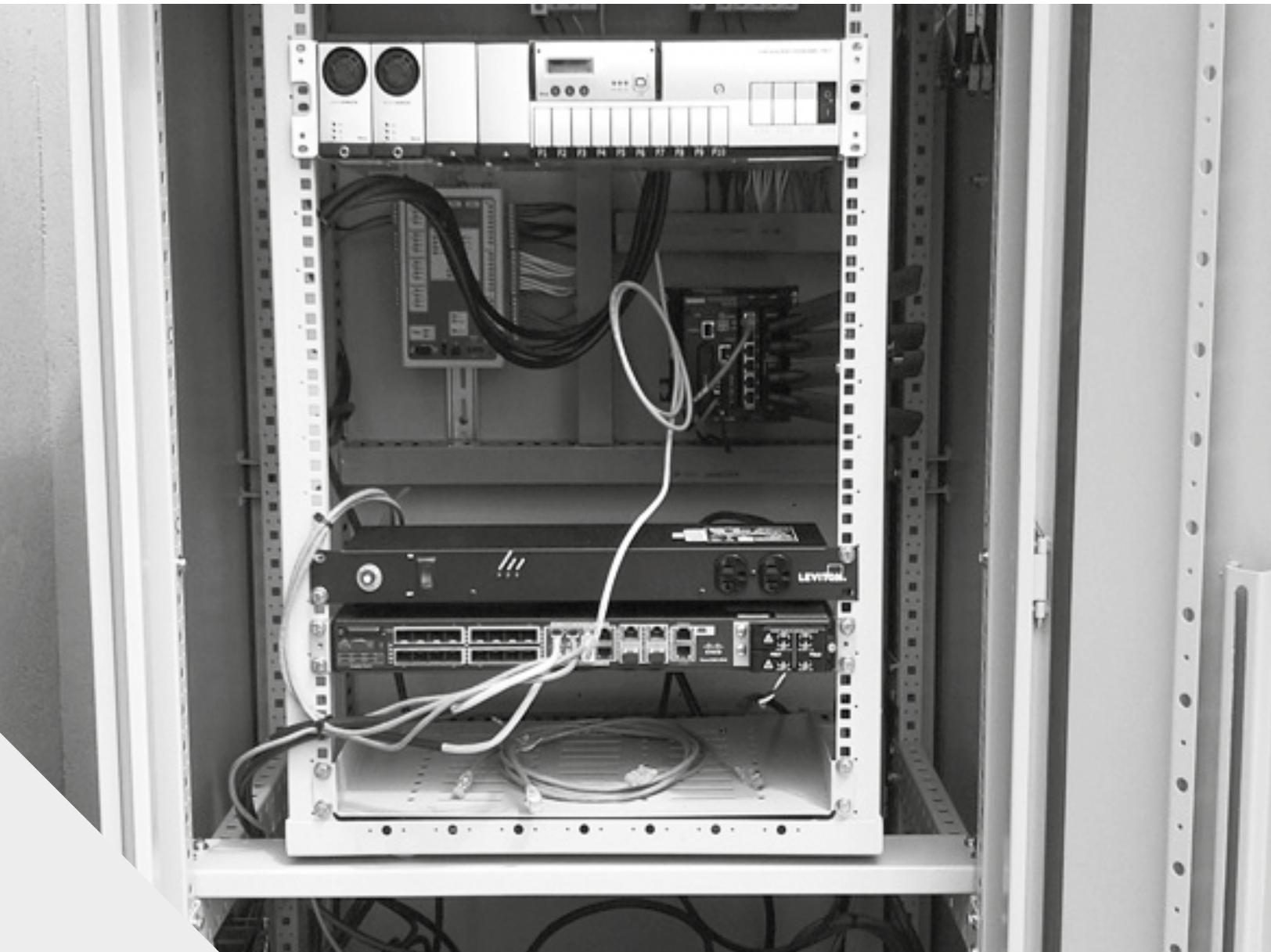


Evaluación de la arquitectura de comunicaciones en subestaciones MT para asegurar su operación

MT substations communication architecture evaluation to guarantee the operation quality



Evaluación de la arquitectura de comunicaciones en subestaciones MT para asegurar su operación¹

MT substations communication architecture evaluation to guarantee the operation quality

Carlos Andrés Ruiz Zea², Anderson Salazar Zuluaga³, Germán Darío Zapata Madrigal⁴, Rodolfo García Sierra⁵

^{2,3,4} Universidad Nacional, sede Medellín, Colombia

⁵Codensa S. A. ESP Grupo Enel, Bogotá, Colombia

Artículo recibido en junio de 2016; artículo aceptado en agosto de 2016

Citación del artículo: Ruiz, C., Salazar, A., Zapata, G. & García, R. (2017). Evaluación de la arquitectura de comunicaciones en subestaciones MT para asegurar su operación. I+D Revista de Investigaciones, 9(1), pp. 6 - 13

Resumen

En este trabajo se expone un concepto acerca del funcionamiento de los equipos utilizados en topologías de redes de comunicaciones para subestaciones eléctricas de media tensión (MT). Se proponen también unas pruebas de transporte de información para los equipos que componen la arquitectura LAN del sistema. Posteriormente, se presentan los resultados obtenidos al someter los dispositivos a alto tráfico de información, evaluando arquitecturas WAN y LAN para asegurar la calidad en la operación de los equipos y la transmisión de los datos. Estas pruebas permiten verificar la disponibilidad de la red y se establecen *firewalls* que permiten implementar estrategias de seguridad básicas para garantizar la disminución de vulnerabilidades en la información que se desea enviar.

Palabras clave: Automatización de la distribución, comunicación GPRS, pruebas de desempeño, seguridad de acceso, vulnerabilidad en comunicaciones.

Abstract

This paper presents a concept about the operation of the equipment used in communications networks topologies for medium voltage (MV) electrical substations. Some tests for information transportation for the equipment that make up the LAN system architecture is also proposed. Subsequently the results obtained in the tests of the devices working with high traffic information are presented, evaluating WAN and LAN architectures to ensure quality in the operation

1. Investigación tecnológica, enfoque cualitativo, resultado de un proyecto de investigación culminado, perteneciente al área de automatización de la distribución, subárea de sistemas de comunicación, desarrollado en el grupo de investigación T&T. Dirección Carrera 80 65-223 Lab. M7-408, Tel.: 4255020. Fecha de inicio: junio de 2014, fecha de terminación: diciembre de 2014.

2. Ingeniero de control, Universidad Nacional de Colombia. Investigador del grupo: T&T. Universidad Nacional de Colombia, Medellín (Colombia): Dirección Carrera 80 65-223 Lab. M7-408, Tel: 4255020. Correo institucional: caaruize@unal.edu.co.

3. Ingeniero de control, Universidad Nacional de Colombia. Estudiante de maestría en Ingeniería Eléctrica, Universidad Nacional de Colombia. Investigador del grupo T&T. Universidad Nacional de Colombia, Medellín (Colombia): Dirección: Carrera 80 65-223 Lab. M7-408, Tel.: 4255020. Correo institucional: asalazaz@unal.edu.co.

4. Ingeniero electricista, Universidad Nacional de Colombia. Doctor en Ciencias Aplicadas, Universidad de Los Andes, Venezuela. Docente, Universidad Nacional de Colombia. Director del grupo: T&T. Universidad Nacional de Colombia, Medellín (Colombia): Dirección Carrera 80 65-223 Lab. M7-408, Tel.: 4255020. Correo electrónico institucional: gdzapata@unal.edu.co.

5. Ingeniero electricista, Universidad Nacional de Colombia. Magíster en Economía, Universidad Nacional de Colombia, Bogotá. Profesional experto, Gerencia técnica Codensa S.A. ESP de la ciudad de Bogotá (Colombia). Correo institucional: rodolfo.garcia@enel.com.

of the equipment and the transmission of the data. These tests can verify network availability and implement firewalls that allow setting basic safety strategies to ensure the reduction of vulnerabilities in the information to be sent.

Keywords: Access security, communication vulnerability, distribution automation, GPRS communication, performance testing.

Los operadores del sistema de distribución de energía eléctrica requieren de información que les brinde conocimiento sobre el comportamiento de sus sistemas con el fin de tomar decisiones sobre el proceso eléctrico mediante los datos suministrados desde diferentes sectores de la infraestructura. Comportamientos históricos del sistema, programación de mantenimientos, manipulación de protecciones, entre otros, son datos que se transmiten mediante redes de comunicaciones que son implementadas por las compañías del sector, permitiendo un flujo bidireccional de datos de las variables entre los dispositivos que interactúan en el medio con su centro de control (Kuzlu, Pipattanasomporn & Rahman, 2014). Esto permite brindar un mejor servicio al consumidor, ya que se facilita la monitorización de los equipos y variables del sistema, y, además, brinda la posibilidad de programar mantenimientos, detectar fallas a tiempo y gestionar los equipos fácilmente. Los sistemas de comunicaciones en este sector han adquirido una importante complejidad (Figura 1); estos manejan alto tráfico de datos necesarios para establecer continuamente el estado del sistema, por lo que se requiere equipos de alta calidad, que soporten interferencia electromagnética, manejen protocolos de redundancia, protocolos de sincronización de tiempo y seguridad de redes. El manejo de todas estas funciones es necesario a la hora de establecer la debida comunicación entre equipos para realizar su gestión y control, cuidando en todo momento la disponibilidad de la red (Gungor et al., 2013).

Este trabajo está dividido en tres secciones. Inicialmente, se describe la infraestructura de comunicaciones utilizada por Codensa y los equipos usados de un gabinete de comunicaciones basado en tecnología GPRS para subestaciones de media tensión; luego, se presentan las pruebas implementadas a la infraestructura disponible y los respectivos resultados en los que se analizan disponibilidad y seguridad. Finalmente, se presentan las conclusiones acerca de la implementación de estas topologías en el sector eléctrico, y se plantean algunos trabajos futuros a desarrollar.

Infraestructura

La arquitectura de comunicaciones del gabinete disponible en las subestaciones de media tensión de Codensa cuenta con una infraestructura que se encarga

de enviar y recibir todo el tráfico de datos desde y hacia el centro de control de la compañía. Los equipos tienen diseños especiales para ambientes agrestes y con funciones específicas para este tipo de condiciones. En la Figura 2 se presenta el aspecto interior del gabinete con los equipos de comunicación utilizados. A estos equipos se les realizaron pruebas de tráfico de información para las topologías presentadas en la sección de pruebas implementadas. En la Tabla 1 se presenta una descripción corta de cada uno de los equipos con las funcionalidades más relevantes.

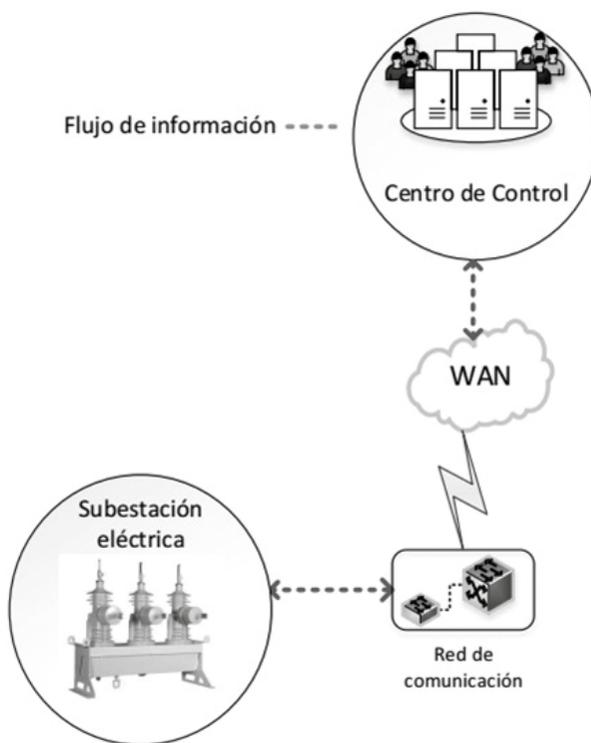


Figura 1. Comunicaciones en las subestaciones eléctricas. Esta gráfica muestra la arquitectura de comunicaciones que se usa en las subestaciones eléctricas de media tensión. Usualmente, se implementan soluciones basadas en conexiones GPRS. Este diseño particular se usa en Codensa. Fuente: Elaboración propia.

Además de los equipos descritos en la Tabla 1, para las pruebas desarrolladas en este trabajo se utilizó un dispositivo para sincronización de tiempo GPS LANTIME / M600 / MRS / PTP, el cual es utilizado como servidor NTP de toda la red (Meinberg, 2015). Estos equipos son fundamentales en este tipo de implementaciones ya que imprimen la estampa de tiempo en todos los mensajes de control desde el centro de control, y de los mensajes de alerta y de acuse de recibo enviados desde la subestación.

Cada dispositivo está adaptado al medio, lo cual permite la integración de otros IED en este tipo de ambiente industrial, donde la infraestructura de comunicaciones

se basa en tecnología GPRS. El equipo que cuenta con esta capacidad es el conmutador y enrutador Ruggedcom Rx1512 (*switch/router*, en inglés), que permite la comunicación bidireccional desde y hacia el centro de control. Esta característica posibilita la gestión de los diferentes dispositivos, y activa o lee puertos de salida para diversas maniobras en el caso de la RTU. Cabe aclarar que, como es una comunicación inalámbrica, la seguridad de la información, por medio de redundancia de datos y *firewalls* básicos que permitan un desarrollo adecuado del tráfico de datos, es de suma importancia. En la siguiente sección se habla de esto por medio de las pruebas implementadas a toda la arquitectura del gabinete de comunicaciones.

Tabla 1
Equipos que componen la arquitectura de comunicaciones de subestaciones MT

Etiqueta	Nombre	Descripción
1	RTU-Semi	Unidad remota de telecontrol que permite configurar entradas y salidas digitales, según las necesidades. Usa el protocolo IEC 60870-5-104* (SEMI, 2014).
2	Ruggedcom Rx1512	Dispositivo de capa 2 y 3 del modelo OSI (switch y router, en inglés). En la arquitectura de red es el encargado de soportar el tráfico de datos para telegestión y telecontrol de los dispositivos dentro de la subestación MT (Siemens, 2014).
3	Cisco CGS2520	Dispositivo conmutador Cisco (o switch, en inglés) diseñado para soportar ambientes agrestes con gran interferencia electromagnética. Está diseñado para apoyar la infraestructura de comunicaciones en los diferentes sectores de la energía eléctrica (Cisco, 2013).

* IEC: International Electrotechnical Commission.

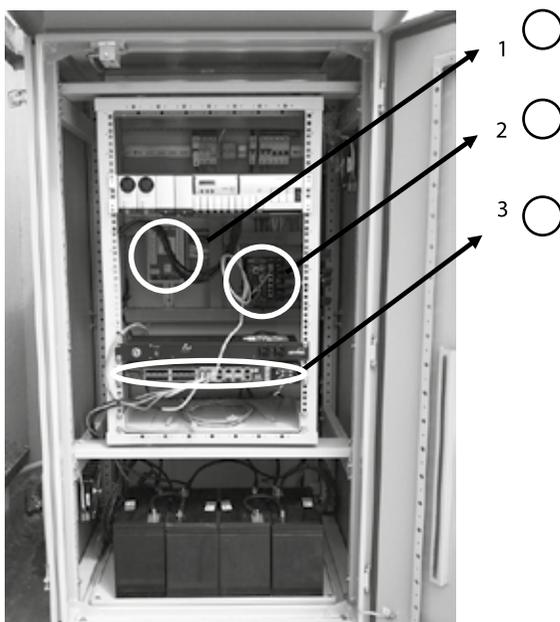


Figura 2.
Gabinete de comunicación subestación MT.

Pruebas implementadas

Probar la capacidad de todos los equipos involucrados en la red que ejecutan funciones de enrutamiento (*routing*, en inglés) y conmutación (*switching*), permite observar el comportamiento cada uno de estos en la gestión de sus recursos. Es por esto que es importante monitorizar el estado de todos los puntos de red por medio de herramientas avanzadas de análisis de tráfico y estado de la red. En estas pruebas, específicamente, se usaron las herramientas de software Solarwinds y Wireshark. Estas herramientas entregan estadísticas de los paquetes de datos enviados y perdidos, además del tiempo de respuesta promedio de cada uno de los equipos involucrados en la red.

Para las pruebas propuestas se utilizan dos topologías diferentes (véase Figura 3 y Figura 4), esto con el fin de observar las capacidades técnicas de los equipos cuando son sometidos a alto tráfico de información. En estas configuraciones se utiliza el dispositivo Ruggedcom

RX1512 como enrutador, sin utilizar la interfaz celular y analizando su gestión de recursos en dicha función (véase Figura 3). Posteriormente, se utiliza como conmutador (o switch), se activa su interfaz celular y se envía a través de esta todo el tráfico que no está destinado para la LAN.

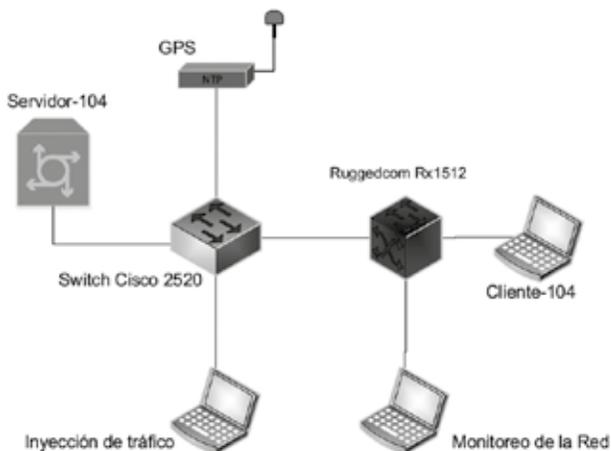


Figura 3.
Topología para pruebas en red LAN. Este esquema muestra la topología lógica de conexión entre equipos para el desarrollo de las pruebas LAN.
Fuente: Elaboración propia.

Esto permite establecer una conexión por medio de internet con el Centro de Control para visualizar las variables y comandos de interés, y para verificar la implementación de seguridades mediante *firewalls* en los dispositivos que se conectan a internet. Así entonces, se puede asegurar la información que transita por esta red (véase Figura 4).

Las topologías implementadas se basan en una capa de enlace de datos, donde, por medio de conmutación y enrutamiento, se envían datos por la interfaz celular hacia el centro de control. Sin embargo, como en este tipo de sistemas hay tráfico de datos alto, y la información que se extrae del sistema es de suma importancia, es necesario conocer cómo se comportan la red y los equipos que la componen. Por lo tanto se deben realizar pruebas de estrés, las cuales simulan tráfico de datos alto atravesando la red. Luego, se establece la comunicación por medio del protocolo IEC-60870-5-104, y se observan los recursos consumidos por cada equipo, tanto el equipo Cisco CGS2520 como el equipo Ruggedcom RX1512. También es importante el tiempo de respuesta y la pérdida de paquetes.

El objetivo de la prueba de estrés es generar un tráfico en la red simulando una avalancha de información de los equipos conectados a la infraestructura presentada en la Figura 3 y Figura 4, con la idea de hacer que el equipo

Cisco CGS 2520 use más sus recursos en memoria, procesador, temperatura y uso de los puertos. Para esto, se sobrecarga la red de forma incremental y se verifica cada uno de los recursos del equipo y el comportamiento del tiempo del dato transferido. Es otras palabras, se trata de verificar que a medida que se va incrementando el tráfico el tiempo que demora el dato en atravesar toda la red esté dentro de unos tiempos aceptables para la empresa.

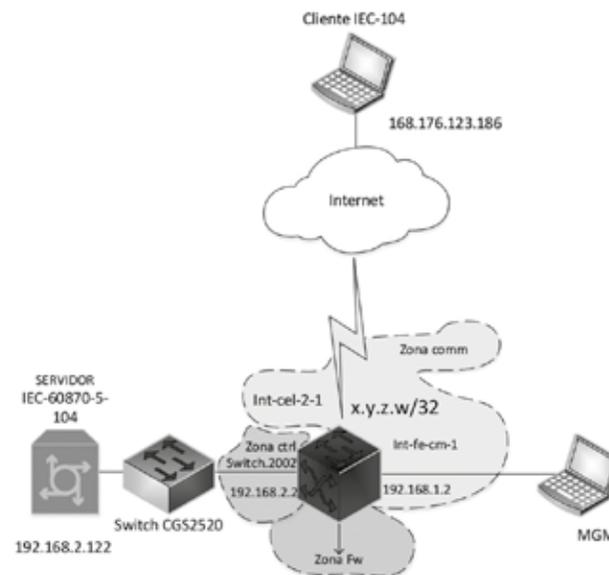


Figura 4.
Topología para las pruebas de la interfaz GPRS. Este esquema muestra la topología lógica de conexión del equipo Ruggedcom RX1512 para la ejecución de las pruebas de transporte por GPRS.

Resultados

Los resultados de las pruebas están basados en las siguientes definiciones:

Average response: cantidad de tiempo que tarda en devolver un resultado a una solicitud, el cual se ve afectado por el ancho de banda de la red, la cantidad de solicitudes y los recursos del equipo.

Packet loss: paquetes perdidos que hacen referencia a los datos que viajan a través de la red que no llegan a su destino.

Luego de estas definiciones, se presentarán los resultados obtenidos para cada uno de los equipos que componen la arquitectura de comunicaciones de las subestaciones MT. A continuación, se describen dichos resultados para cada uno de los equipos evaluados.

Ruggedcom Rx1512

En la Figura 5 se presentan los resultados obtenidos por medio del *software* Solarwinds. Esta herramienta monitorizó la red sometida a alto tráfico de datos. En la primera gráfica se observa el tiempo medio de respuesta, el cual estuvo situado alrededor de los 0.07ms. La segunda gráfica da cuenta del porcentaje de paquetes perdidos en la prueba, cuyo resultado fue de 0%. Lo anterior indica que el desempeño de la red es satisfactorio para el escenario desarrollado.

Ahora, en la Figura 6 se puede observar el estado general del equipo en cuanto a la carga impuesta a la CPU y a la memoria RAM. Allí se puede ver que el Ruggedcom RX1512 no sufrió sobrecargas en estos dos recursos y se concluye que este equipo pudo manejar de forma correcta todo el tráfico que se le impuso.

Switch Cisco CGS2520

En cuanto al conmutador (o *switch*) Cisco CGS 2520, en la Figura 7 se presentan los resultados obtenidos por medio del *software* Solarwinds para este caso. Allí se puede ver, en la primera gráfica, que el tiempo medio de respuesta estuvo situado alrededor de los 1.93ms. Por otro lado, la segunda gráfica da cuenta del porcentaje de paquetes perdidos en la prueba, cuyo resultado también fue de 0%. Así entonces, es válido señalar que el desempeño de la red es satisfactorio para el escenario desarrollado.

Finalmente, en la Figura 8 se muestra el rendimiento de la CPU del equipo Cisco CGS2520 durante las pruebas ejecutadas. Allí se puede observar que el valor máximo de carga impuesta a este equipo fue de 86%. Este valor da cuenta de la importancia que tiene este equipo dentro de la infraestructura de comunicaciones

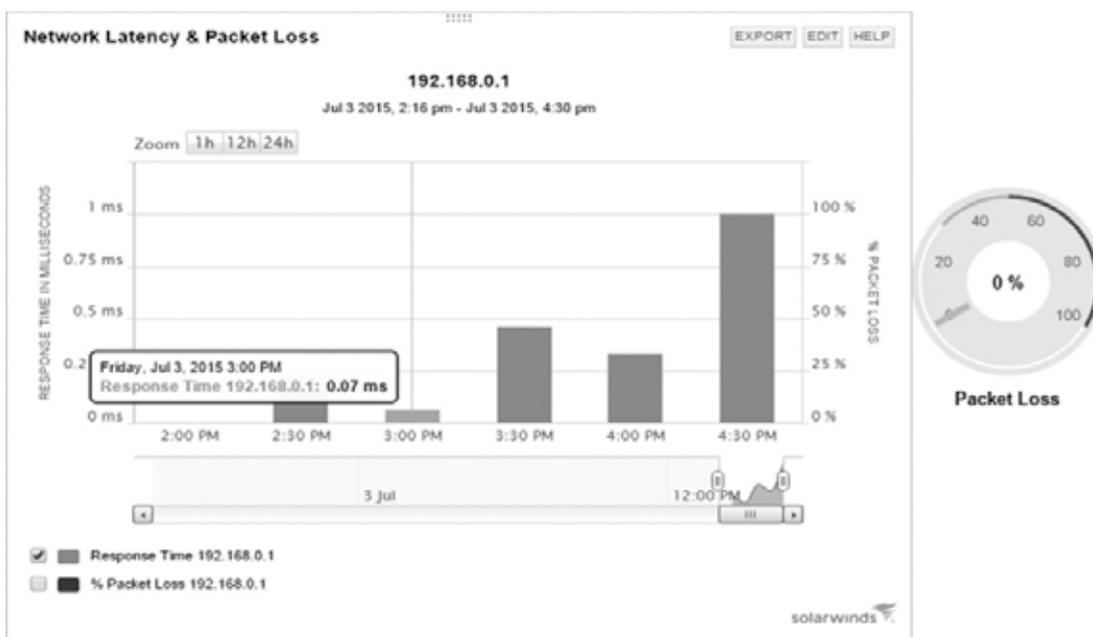


Figura 5. Tiempo medio de respuesta y paquetes perdidos en RX1512. Estas gráficas muestran los resultados obtenidos en las pruebas de transporte para el equipo Ruggedcom RX1512. Se presenta el tiempo medio de respuesta y el porcentaje de paquetes perdidos en la transmisión de información.

Slot	Detected-module	CPU load(%)	RAM Avail(%)	RAM Low(%)
main	RX1512 8 Gigabit Layer 3 w/ 2 LM slots and no PM slot	57	56	56

Figura 6. Rendimiento del equipo Ruggedcom RX1512. Esta gráfica muestra el rendimiento del equipo Ruggedcom RX1512 obtenido durante las pruebas ejecutadas. Se pueden observar datos acerca de la carga de trabajo impuesta a la CPU y a la memoria RAM.

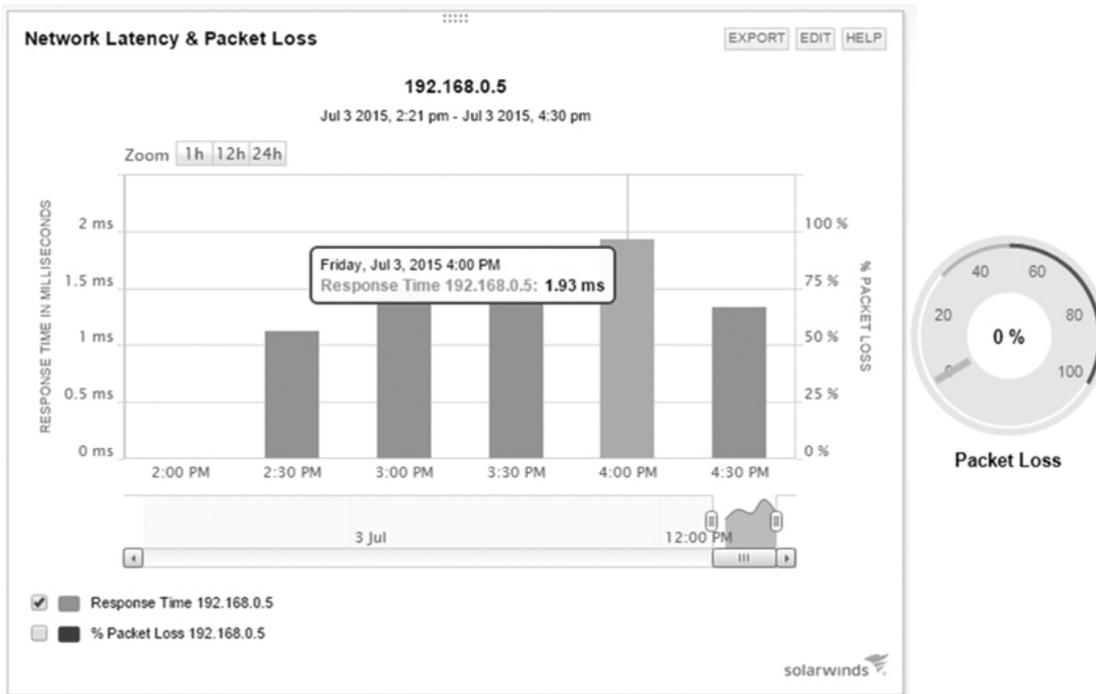


Figura 7. Tiempo medio de respuesta y paquetes perdidos en CGS2520. Estas gráficas muestran los resultados obtenidos en las pruebas de transporte para el equipo Cisco CGS 2520. Se presenta el tiempo medio de respuesta y el porcentaje de paquetes perdidos en la transmisión de información.

de las subestaciones MT, ya que este se encarga de conmutar todo el tráfico dentro la red. Dentro de estas subestaciones la red recibe datos de diversos tipos, como medición, control y alarmas, entre otros. A primera vista, este equipo puede significar un punto de falla adicional, sin embargo, es necesario señalar que a este equipo no solo se conecta el servidor IEC 60870-5-104 mostrado en la Figura 3 y la Figura 4, sino otros equipos como medidores de calidad de potencia, reconectores, interruptores de cabecera de circuitos de distribución, relés, entre otros. Por lo tanto, es un equipo neurálgico para la comunicación entre el centro de control y la subestación MT.

Conclusiones

Tradicionalmente, las empresas del sector eléctrico presentan topologías de red encargadas de transportar la información de diferentes equipos, los cuales adquieren datos de variables como corrientes, voltajes y potencia, entre otras. Adicionalmente, estos equipos manejan datos de reconectores, seccionadores y demás dispositivos que interactúan día a día en este ambiente. Por esta razón, es de suma importancia considerar dispositivos de red adecuados, los cuales soporten y respalden la operación crítica dentro de las subestaciones y sean capaces de procesar altos tráficos de datos en todo momento.

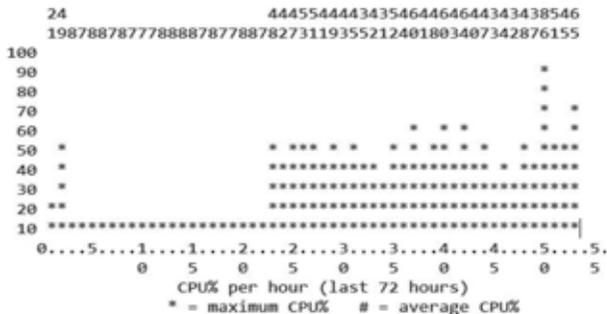


Figura 8. Rendimiento del equipo Cisco CGS2520. Esta gráfica muestra el rendimiento del equipo Cisco CGS2520 obtenido durante las pruebas ejecutadas. Se pueden observar datos acerca de la carga de trabajo impuesta a la CPU.

En el trabajo desarrollado se pudo observar que las topologías de red implementadas son acertadas en cuanto a la infraestructura utilizada, ya que no hay ninguna pérdida de información y se presenta poco consumo de recursos. Sin embargo, hay errores en cuanto al sistema físico que pueden interferir en el tráfico de información para el telecontrol y la telegestión, pues la arquitectura de red presentada depende de un solo enlace entre el conmutador Cisco CGS2520 y el Ruggedcom Rx1512. Esto conlleva que cualquier error físico de conexión o alimentación deje incomunicados los equipos de la arquitectura de comunicaciones con el centro de control. En este informe se muestra un avance de

lo que se ha realizado hasta ahora en la implementación de este tipo de topologías generando datos, usándolos en interfaces sencillas y visualizando la comunicación de las variables creadas. A futuro, será posible incorporar nuevos equipos como reconectores, indicadores de falla, indicadores de tensión, seccionadores, medidores de calidad de potencia o medidores de energía, que posibiliten la adquisición de estos datos y la interacción con los equipos para automatización de circuitos de distribución.

Referencias

- Cisco. (2013). Cisco 2520 Connected Grid Switch. San Jose, CA: Autor. Recuperado de <http://goo.gl/ksOEal>
- Gungor, V., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2013). A Survey on smart grid potential applications and communication requirements. *IEEE Transactions on Industrial Informatics*, 9(1), 28–42. Recuperado de <http://doi.org/10.1109/TII.2012.2218253>
- Kuzlu, M., Pipattanasomporn, M., & Rahman, S. (2014). Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks*, 67, 74–88. Recuperado de <http://doi.org/10.1016/j.comnet.2014.03.029>
- Meinberg. (2015). LANTIME M600/MRS/PTP Time Server. Recuperado de <http://goo.gl/obD4VT>
- SEMI. (2014). Unidades Remotas de Telecontrol Setis. España: Autor. Recuperado de <http://goo.gl/5sBZFs>
- Siemens. (2014). Ruggedcom RX1512 Switch and Router. Recuperado de <https://goo.gl/8aFYnI>