Monitoreo SNMP y VPN sobre WAN para prevención de caída de transmisores de televisora

Guillermo Navarro Gonzalez, Centro de Enseñanza Técnica y Superior.
Ramón Alejandro Guzmán, Centro de Enseñanza Técnica y Superior.

Abstract Las televisoras cuentan con dispositivos de transmisión críticos para la operación y a través de las generaciones hay equipos que permiten el monitoreo inteligente y otros que son legado, sin embargo, dada su inversión no son fáciles de reemplazar. Esta investigación muestra los dispositivos de legado y los dispositivos inteligentes comunicándose mediante el protocolo SNMP a un servidor Zabbix como unidad central de monitoreo encargada de registrar toda la información de los dispositivos, así como el uso de la red social Telegram para alertar al personal de trabajo y una conexión VPN para acceso remoto. Obteniendo registros de tendencias en las lecturas de los dispositivos para la prevención de caídas y reduciendo tiempos de detección de anomalías y recorridos hacia las locaciones de los dispositivos.

I. Introduccion

Una televisora en Baja California distribuye su señal mediante tres estaciones repetidoras con cinco equipos, tres transmisores y dos aires acondicionados y una estación principal, ubicados en Tijuana además de una repetidora en Tecate, también con tres transmisores y dos aires acondicionados. A su vez la estación principal cuenta con cien equipos aproximadamente, de los cuales cinco son aires acondicionados. Si cualquiera de estos equipos falla, la señal puede interrumpirse parcial o totalmente dependiendo de su ubicación, por lo que el monitoreo es clave para la continuidad de la transmisión de la señal de la televisora.

II. Antecedentes

El análisis de fallas en resumen de 2018 permitió identificar los siguientes antecedentes, sobre historial, tiempos de respuesta, monitoreo actual y recorridos humanos para el monitoreo de los equipos de transmisión.

A. Historial de fallas en equipos remotos

El historial de fallas mostró las siguientes alarmas por daño total en 2018, ver tabla I

TABLA 1
Historial de fallas de transmisor remoto

Equipo	Periodo	Alarmas de baja potencia	Ultimo reemplazo por daño total
1	06-Abr-2018 a 24-Abr-2018	212	05-Abr-2018
2	29-Mar-2018 a 18-Abr-2018	3	28-Mar-2018

TABLA 2
Parámetros de transmisor

Parámetro	Mínimo	Máximo	Unidades
Corriente de amplificador.	6	12	A
Fuente de voltaje.	40	46	V
Temperatura de circuitería.	0	45	°C

Desde 2013 el parámetro principal para detectar anomalías ha sido la corriente de amplificador, ver Tabla II.

Sin embargo, una prueba térmica a los equipos en reparación, observamos temperaturas de hasta 110 °C, en las resistencias disipadoras de potencia, en comparación a la temperatura obtenida en los equipos funcionando correctamente de entre 30 y 35 °C, y con esta muestra identificamos un segundo parámetro para el monitoreo de anomalías en los equipos transmisores. Aunque para los

equipos transmisores de la estación central no cuentan con un historial de fallas registrado.

B. Tiempos de respuesta al identificar una alerta o falla.

Los equipos transmisores de la estación central cuentan con un sistema de alertas interno; normalmente el operador detecta anomalías en los equipos inspeccionando visualmente el equipo o en su aplicación web. Ver Tabla III.

TABLA 3
TIEMPOS DE RESPUESTA DEL OPERADOR

Gravedad	**Mínimo**	**Máximo**	**Unidades**
Advertencia	10	120	Minutos
Desastre	0	10	Segundos

El nivel de gravedad "Advertencia" está relacionado a fallas como anomalías en las lecturas de los equipos y el nivel "Desastre" a fallas totales del equipo dejándolo incapacitado. La única falla de nivel desastre registrada en los equipos de la estación central fue registrada en 2011 con una pérdida total de 120 transistores amplificadores.

C. Monitoreo Actual

Los equipos remotos son monitoreados a través de su aplicación web integrada y visualizados en distintos monitores. Los equipos de la estación central también son monitoreados con su aplicación web y de forma visual.

D. Áreas de estación y distancia entre bunkers repetidores

La estación principal cuenta con un área de aproximadamente 7,206 m^2, el equivalente aproximado a 87% de un campo de futbol FIFA [9] en sus máximas dimensiones, los equipos transmisores y sus periféricos están en las secciones resaltadas de la Figura 1.

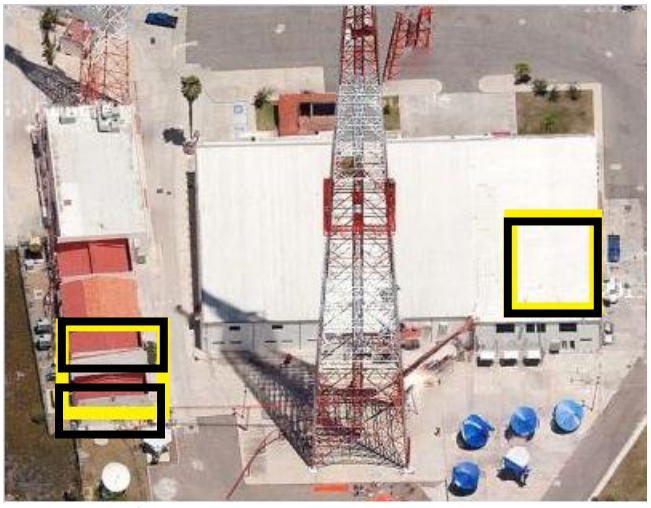

Fig. 1. Ubicación de equipos transmisores en televisora

Dentro del edificio principal, los equipos están distribuidos en cuatro salas con aproximadamente 180 m^2. Existen dos edificios adjuntos de aproximadamente 85 m^2, la distancia entre la sala de monitoreo y los edificios adjuntos es de 142 m aproximadamente.

Un recorrido habitual entre las salas dentro del edificio principal es de 48 metros aproximadamente. Partiendo desde la sala de monitoreo, el operador viaja diariamente para ajustar un equipo en uno de los edificios adjuntos.

Teniendo en cuenta las distancias anteriores, en un día normal con un recorrido el operador en turno recorrería 190 metros, con un equivalente anual de 48 km sin contar los recorridos por averías o interrupciones en la transmisión.

E. Enlaces de comunicación

La televisora cuenta con los siguientes enlaces y/o redes de comunicación:

- Un enlace IP vía microonda entre estación principal y bunker repetidor. Este enlace permite monitorear el estatus de los equipos transmisores con aplicación web integrada, pero solo una estación repetidora cuenta con esta comunicación.
- Un enlace IP vía microonda entre estación principal y estación de Tecate. Este enlace permite enviar señal de video a la estación de Tecate.
- Una red satelital para comunicación de todas las estaciones a nivel nacional (Intranet). En esta red están conectados la mayoría de los equipos utilizados en la estación principal, y es administrada desde la Ciudad de México para dar soporte técnico a los equipos en red, acceso a información para los trabajadores y comunicación telefónica sobre IP (VoIP).
- Una red local de internet. Con dos proveedores de internet comerciales (Telmex e Izzi) para el uso cotidiano de correo de la televisora y acceso a información en internet.

III. MARCO TEÓRICO

Un análisis documental permitió identificar aplicaciones previas en redes y protocolos utilizados para la conexión de dispositivos, sensores y algún tipo de aplicación de cómputo para desplegar información en como agricultura [10], donde Sisyanto, Suhardi y Kurniawan desarrollaron un sistema inteligente de agricultura de hidroponía para monitorear parámetros importantes vía sensores conectados a una Raspberry Pi y visualizar la información en la red social Telegram, así como casos de monitoreo del medio ambiente y control de riego en el cultivo de vegetales utilizando microcontroladores y el protocolo ZigBee, desplegando la información en un sitio web [13]. También el monitoreo de dispositivos médicos [11], y uno para servidores [14], cercano a la aplicación de este caso, sin embargo, este implica el monitoreo de dispositivos de transmisión.

Una vez analizadas las distintas aplicaciones previas fue necesario enfocarse en la documentación de los protocolos

de comunicación en redes utilizados para la interoperabilidad entre dispositivos, donde toman como base el modelo Open Systems Interconnection (OSI). El modelo es separado en una serie de siete capas, en las cuales cada una define protocolos dependiendo de la función desempeñada.

Esta investigación está enfocada en la capa 7, capa de aplicación.

La capa de aplicación es la responsable de definir la presentación del servicio para el usuario final. Los protocolos varían dependiendo de la información requerida para ser transmitida por el usuario [Alani M.M.].

Para el sistema de monitoreo propuesto, lo esencial es mostrar cierta información al operador en turno y con ella poder identificar anomalías en los equipos. Entonces es necesario saber cuáles protocolos pueden usarse para adquirir el estado de los equipos y prevenir fallas o caídas. Rayes y Salam [5] y Alani [6] mencionan algunos de los protocolos comúnmente utilizados en la capa de aplicación como Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3), Telnet, Domain Name Service (DNS), Secure Shell (SSH), Simple Network Managment Protocol (SNMP). Sin embargo, esta investigación selecciono SNMP como el protocolo como el protocolo de comunicación para el monitoreo remoto.

Ya que SNMP es el protocolo de mayor uso para el monitoreo de dispositivos acoplados a una red [1]. Un sistema de manejo de red (Network Managment System, NMS) ejecuta aplicaciones para el monitoreo y control de dispositivos en la red. Los componentes básicos para un NMS son:

- SNMP Manager: Es la entidad responsable de entablar la comunicación con el agente SNMP.
- Managed Devices: Son los dispositivos en la red que requieren de manejo o monitoreo de datos.
- SNMP Agent: Es el programa integrado en el dispositivo de monitoreo, encargado de recopilar la información para su manejo por el SNMP Manager.

El protocolo SNMP actúa en la capa de aplicación del modelo OSI.

El agente está localizado dentro del dispositivo a manejar (Managed Device), lo cual accede a la configuración y estadísticas de este dispositivo para compartirla una estación controladora. El SNMP Manager en el dispositivo controla la red. El manager envía solicitudes encapsuladas en SNMP a los distintos agentes, esto con el fin de recibir la información accesible de los agentes. Cabe destacar que el mismo agente puede enviar información de carácter crítico sin que el manager lo solicite, denominados trampas.

Cada agente SNMP mantiene una base de datos (Managment Information Base, MIB) con la información recabada de los dispositivos controlados, ver Figura 2.

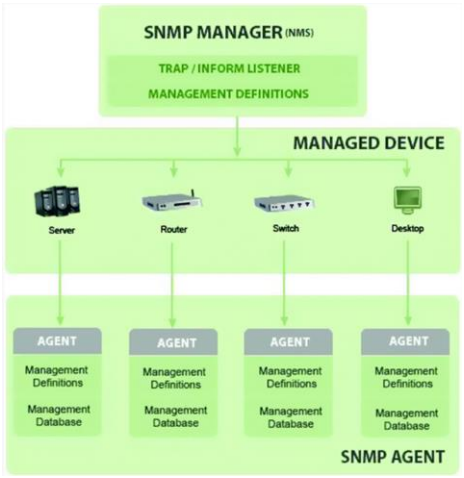

Fig. 2. Diagrama básico de comunicación SNMP. [2, Iqbal A., Pattinson C., Kor AL., 2017]

El protocolo SNMP utilizado para este caso puede funcionar en redes locales (LAN) y redes de área amplia (WAN). Para tener un acceso local y remoto al sistema de monitoreo, se realizó un análisis de la tecnología Vitual private network (VPN), la cual extiende una red privada a través de una red pública y permite a los usuarios enviar y recibir información a través de la red pública [15]. La tecnología VPN establece un túnel de comunicación encriptado dándole seguridad a los usuarios a la hora de conectar 2 sitios remotos [16].

IV. Definición del Problema

Debido a la ubicación de la instalación de tres estaciones repetidoras remotas y una central en la ciudad de Tijuana, y una en Tecate. El monitoreo de prioridad es la estación central y el monitoreo a los estatus de los equipos remotos es limitado. La cantidad de equipos por estación remota es de cinco por ubicación, y alrededor de unos cien en la estación principal, si alguno de los equipos en las estaciones remotas falla la señal quedaría interrumpida en el área de cobertura por dicha estación. Teniendo en cuenta lo anterior y que el personal de monitoreo solo cuenta con una persona por turno, es complicado detectar anomalías en los equipos, esto es para todas las ubicaciones. Por lo que el problema de esta investigación es:

¿Puede recibirse de manera remota y centralizada el estado y temperaturas de los equipos transmisores y sus periféricos?

Hi_1

Las hipótesis para el problema son:

Ho_1 = Puede recibirse remotamente el estado básico y temperaturas de dispositivos de forma centralizada.

Hi_1 = No puede recibirse remotamente el estado básico y temperaturas de dispositivos de forma centralizada.

V. Metodología

La metodología consistió en una investigación

documental para identificar alternativas de comunicación y sensores para el monitoreo y una investigación de campo para integrar un prototipo para aceptar o rechazar las hipótesis.

A. *Investigación Documental*

La estrategia para definir un prototipo colección de información básica y temperatura de dispositivos remotos considero:

1. Investigar soluciones de software comerciales para telemetría.
2. Investigar protocolos para entablar comunicación entre estaciones remotas y estación central.
3. Investigar los sensores necesarios para obtener datos de los dispositivos remotos.
4. Investigar interfaces para centralizar la obtención de datos de los dispositivos.

En base a los antecedentes, los criterios para seleccionar los componentes del diseño del prototipo serian: la infraestructura necesaria para integrarlo, costo y escalabilidad.

B. *Investigación de Campo*

La investigación de campo consistió en el diseño de un prototipo para monitorear parámetros de operación de los transmisores y sus temperaturas en ubicaciones remotas a el operador desde la comodidad de la oficina o el hogar sin necesidad de trasladarse a las ubicaciones remotas; Además de equipos periféricos alertando de anomalías y sus temperaturas. El propósito de la información recabada por el prototipo para el operador es detectar anomalías en los equipos y tomar acciones correspondientes para prevenir la interrupción de las operaciones.

VI. Desarrollo

Un comparativo de los protocolos HTTP, FTP, SMTP, POP3. Telnet, DNS, SSH Y SNMP de la capa de aplicación permitió identificar tres candidatos para un sistema de monitoreo, HTTP, SSH y SNMP. La implementación de una aplicación en HTTP implicaba diseñar una aplicación desde cero, y el protocolo SSH era una opción viable para enviar y recibir la información de forma segura, pero también requería diseñar desde cero. Sin embargo, el protocolo SNMP implementado en la mayoría de los dispositivos en red [1] cuenta con aplicaciones de software especializadas para obtener información a través de la red. Además, la capacidad de comunicación vía SNMP de los equipos en la televisora caso de aplicación de este proyecto es del 81% y llevó a la elección de este protocolo para el desarrollo del prototipo de monitoreo centralizado.

A. *Modelo propuesto*

El prototipo desarrollado utilizó el protocolo SNMP para el monitoreo de los equipos, aprovechando los enlaces IP con las estaciones remotas para obtener la información requerida y centralizarla en un servidor en la estación principal. Los equipos en la estación principal fueron conectados a una red local del servidor, facilitando la interconexión de todos los equipos. Para tener un mayor control de la actividad de los equipos, implementamos un sistema de alarmas dirigidas a un grupo de mensajes en Telegram, para los empleados del área encargada de transmisores.

La red de monitoreo quedo de la siguiente manera. Ver Figura 3.

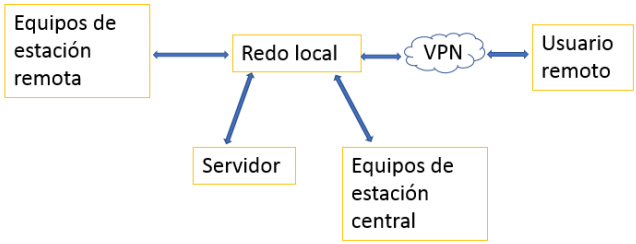

Fig. 3. Diagrama de conexión entre estación remota, estación principal y usuario remoto.

B. *Selección de software*

La selección del software basó su criterio en el costo, escalabilidad y documentación disponible.

TABLA 4
ADMINISTRADORES SNMP POR COSTO

Administrador SNMP	Sistema Operativo	Versión de prueba	Costo US$
Solarwinds NPM	Windows	30 días	2955
PRTG	Windows	30 días y versión limitada	1600
Nagios Core	Linux	NA	Gratis
Spiceworks	Windows	NA	Gratis
Zabbix	Linux	NA	Gratis

La aplicación Solarwinds tiene un costo de varios miles de dólares. PRTG cuenta con una interfaz amigable y soporte por parte de la empresa, sin embargo, implica un costo mayor a mil dólares y su versión gratuita está limitada para el monitoreo de este caso. Spiceworks es gratuita, pero limita la operación con equipos personalizados SNMP. Nagios Core tiene documentación limitada. Zabbix cumple con todos los criterios mencionados. Por lo que Zabbix fue seleccionado para el desarrollo.

C. *Diseño de prototipo*

El mercado ofrece una variedad de productos comerciales capaces de actuar como transductor y enviar la información vía protocolo SNMP. Como los listados en la Tabla V.

TABLA 5
ALTERNATIVAS PARA EL PROTOTIPO SNMP

Producto	Marca	Costo US$
AlertWerks sensor de temperatura	AKCP	46.87
INV-Temp	ServersCheck	65
Raspberry Pi 3	Raspberry pi	39
Arduino UNO	Replica	17

En base al entorno de costos la opción más económica es el Arduino UNO. Sin embargo, las características técnicas del Raspberry Pi3 lo superan, ver tabla VI. El prototipo con Raspberry Pi utilizó el sensor de temperatura DS18B20 con un costo en el mercado de entre $70 y $150 pesos, ofreciendo comunicación de un puerto con los dispositivos e integrando varios sensores en paralelo, limitado por el dispositivo en el que es conectado.

TABLA 6
COMPARATIVO ENTRE ARDUINO UNO Y RASPBERRY PI 3

	Arduino UNO	Raspberry Pi 3
CPU	Microcontrolador ATmega328P	1.4 GHz 64-bit quad-core ARMv8
GPIO	20	40
Wireless	Modulo por separado	2.4 GHz 5 GHz IEEE 802.11.b/g/n/ac, Bluetooth 4.2
USB	Modulo por separado	4 USB 2.0
Multi tarea	N/A	Si
Voltaje de entrada	7-12V	5V
Memoria	32 KB	Micro SD 8 a 32GB

Fig. 4. Raspberry pi3 con sensores DS18B20

Un script en Python fue diseñado para la obtención de temperatura de los sensores y para la comunicación SNMP se implementó un script en BASH, el cual colecta los datos del script en Python y los transmite vía SNMP.

D. *Servidor VPN*

El mismo prototipo Raspberry Pi3 fue utilizado como servidor VPN para el acceso en cualquiera parte.

VII. RESULTADOS

El prototipo permitió la generación de un historial de lecturas en los equipos transmisores de la estación remota y la principal. Ver Figura 5 y Figura 6.

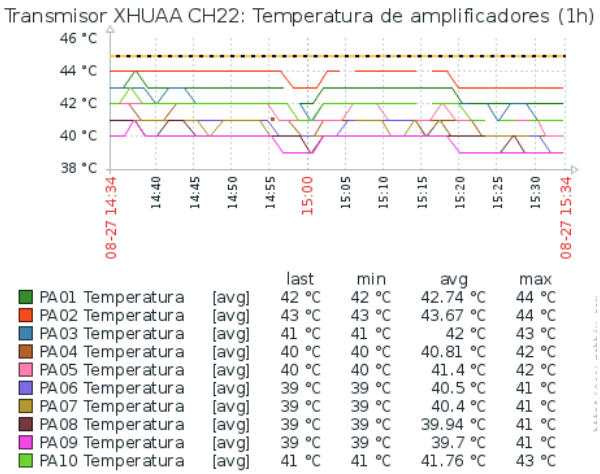

Fig. 5. Historial de temperaturas de una hora de los amplificadores del transmisor de canal 22.

Las gráficas 5 y 6 de los historiales muestra una línea punteada como nivel de alerta en base a las pruebas de instalación realizadas en los equipos. Y para tener un mayor control en la prevención de caída de equipos, se integró en dos niveles de alerta para la respuesta calificada como advertencia o desastre.

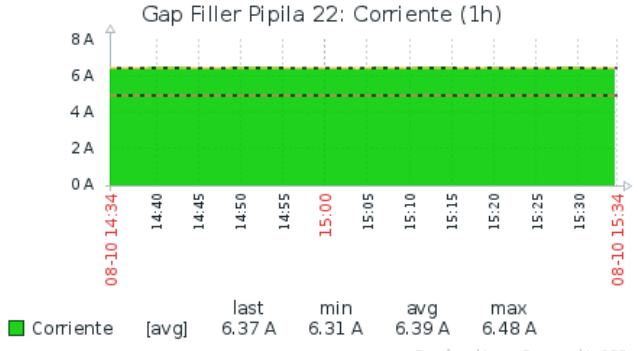

Fig. 6. Historial de corrientes de una hora de transmisor repetidor de canal 22.

Las alertas fueron enviadas a equipos de telefonía celular y él envió de los mensajes de alerta directo permitió informar a todos los empleados del área, aun cuando no estaban monitoreando el equipo directamente o estaban ocupados en otras áreas de la estación. Ver Figura 7.

Fig. 7. Mensajes de alarma recibidos en grupo de Telegram.

Una prueba de recepción de mensajes con una muestra de treinta alertas forzadas mostró los siguientes tiempos para el mensaje de alerta y el mensaje de recuperación. Ver Tabla VII y VIII.

TABLA 7
TIEMPOS DE RECEPCIÓN PARA MENSAJE DE ALERTA.

Mínimo (Seg)	Promedio (Seg)	Máximo (Seg)
33	109.6	184

TABLA 8
TIEMPOS DE RECEPCIÓN PARA MENSAJE DE RECUPERACIÓN.

Mínimo (Seg)	Promedio (Seg)	Máximo (Seg)
53	89.5	157

El operador tarda entre diez minutos a una hora en identificar una alarma en los transmisores de la estación principal y en las estaciones puede tardar hasta un día o más.

Inicialmente las gráficas obtenidas dejaban pequeños espacios sin información, ver Figura 8. Logramos disminuir las omisiones de datos aumentando el tiempo de espera para para recibir los datos en el servidor de tres segundos a seis segundos, ver Figura 9. Estos espacios en blanco solo logran verse en los periodos de cero a doce horas, a partir de un día la aplicación interpola los datos obtenidos previniendo la discontinuidad de la gráfica, ver Figura 10.

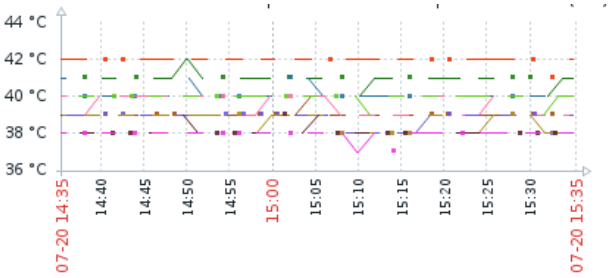

Fig. 8. Grafica con espacios en blanco antes de cambio de tiempo de espera de 3 segundos.

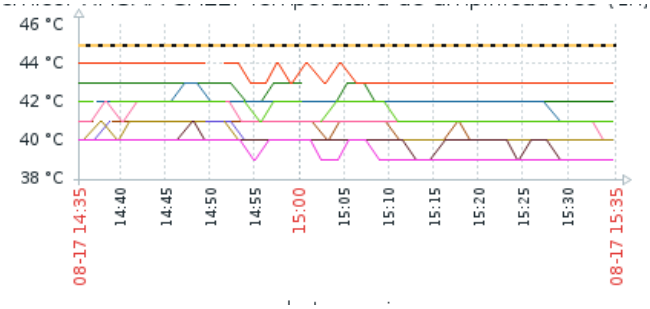

Fig. 9. Gráfica con espacios en blanco antes de cambio de tiempo de espera de seis segundos.

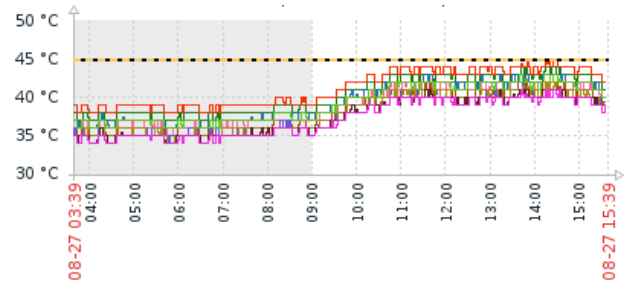

Fig. 10. Grafica con valores interpolados.

El prototipo de toma de temperaturas instalado en los racks mostró las siguientes temperaturas. Ver figura 11.

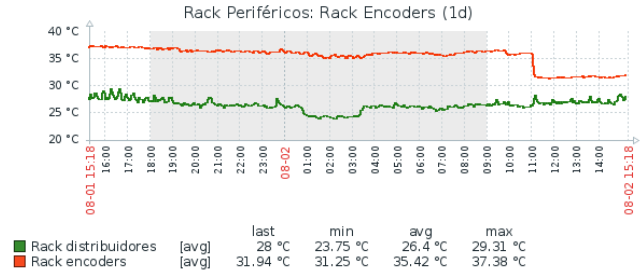

Fig. 11. Grafica con temperaturas de racks

El nuevo sistema de monitoreo redujo el recorrido habitual para el operador en turno de madrugada de 190 m a 145 m, para los demás turnos el recorrido se redujo a casos de tener que atender emergencias. La detección de anomalías no graves en los transmisores se redujo a un promedio obtenido por los mensajes de Telegram de 109.6 segundos. Con los historiales generados por el servidor Zabbix, ahora se pueden identificar tendencias en las lecturas de los transmisores y actuar antes de que ocurra una falla grave. El monitoreo centralizado redujo a un equipo la cantidad necesaria para el monitoreo de los transmisores en la estación. La conexión VPN permitió acceder a toda la información monitoreada de forma remota sin necesidad de encontrarse en la estación.

Con lo anterior mencionado podemos concluir lo siguiente.

VIII. Conclusión

La integración de un módulo Raspberry Pi3 con Zabbix para los dispositivos sin el protocolo SNMP y los dispositivos con SNMP nativo con la red social Telegram permitió un monitoreo centralizado de los estados básicos de los equipos transmisores y sus temperaturas. El uso de la VPN permitió tener acceso a toda la información centralizada desde cualquier parte remota.

Referencias

[1] Deng H., Liu G., Zhang L. (2011) Analysis and Implementation of Embedded SNMP Agent. In: Li D., Liu Y., Chen Y. (eds) Computer and Computing Technologies in Agriculture IV. CCTA 2010. IFIP Advances in Information and Communication Technology, vol 347. Springer, Berlin, Heidelberg

[2] Iqbal A., Pattinson C., Kor AL. (2017) Introducing Controlling Features in Cloud Environment by Using SNMP. In: Kharchenko V., Kondratenko Y., Kacprzyk J. (eds) Green IT Engineering: Concepts, Models, Complex Systems Architectures. Studies in Systems, Decision and Control, vol 74. Springer, Cham

[3] Hosek, J., Molnar, K., Rucka, L. et al. Telecommun Syst (2013) 52: 1595. https://ebiblio.cetys.mx:4083/10.1007/s11235-011-9516-2

[4] da Silva I.N., Hernane Spatti D., Andrade Flauzino R., Liboni L.H.B., dos Reis Alves S.F. (2017) Computer Network Traffic Analysis Using SNMP Protocol and LVQ Networks. In: Artificial Neural Networks. Springer, Cham

[5] Rayes A., Salam S. (2017) The Internet in IoT—OSI, TCP/IP, IPv4, IPv6 and Internet Routing. In: Internet of Things From Hype to Reality. Springer, Cham

[6] Alani M.M. (2014) TCP/IP Model. In: Guide to OSI and TCP/IP Models. SpringerBriefs in Computer Science. Springer, Cham

[7] Halsey M., Ballew J. (2017) TCP/IP Networking. In: Windows Networking Troubleshooting. Apress, Berkeley, CA

[8] De Soete M. (2011) SSH. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA

[9] Futbolia.com. (2014). Medidas oficiales de los campos de fútbol según FIFA. [online] Available at: http://www.futbolia.com/opinion/medidas-oficiales-de-los-campos-de-futbol-segun-fifa.

[10] R. E. N. Sisyanto, Suhardi and N. B. Kurniawan (2017), Hydroponic smart farming using cyber physical social system with telegram messenger, International Conference on Information Technology Systems and Innovation (ICITSI), Bandung.

[11] N. Lasierra, Á. Alesanco and J. García (2012), An SNMP-Based Solution to Enable Remote ISO/IEEE 11073 Technical Management, IEEE Transactions on Information Technology in Biomedicine.

[12] Andrea Dalle Vacche. (2015). Mastering Zabbix - Second Edition. Packt Publishing Ltd: Birmingham B3 2PB, UK.

[13] N. Kaewmard and S. Saiyod (2014), Sensor data collection and irrigation control on vegetable crop using smart phone and wireless sensor networks for smart farm, IEEE Conference on Wireless Sensors (ICWiSE), Subang.

[14] W. Zeng and Y. Wang (2009), Design and Implementation of Server Monitoring System Based on SNMP, International Joint Conference on Artificial Intelligence, Hainan Island.

[15] Zhang S., Li A., Zhu H., Sun Q., Wang M., Zhang Y. (2018) Research on the Protocols of VPN. In: Xhafa F., Patnaik S., Zomaya A. (eds) Advances in Intelligent Systems and Interactive Applications. IISA 2017. Advances in Intelligent Systems and Computing, vol 686. Springer, Cha

[16] Belimpasakis, P. & Stirbu, V. Multimed Tools Appl (2014) 70: 1899. https://ebiblio.cetys.mx:4083/10.1007/s11042-012-1221-y