TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.2 , Abril-Junio, 2021, p.63- 84 ISSN 1729-3804

LA GESTIÓN EN INTERNET DE LAS COSAS

Ing. Yoan Larry Cecilio Nuñez[1], Ing. Aileen Forte Moreno[2]

[1-2]Empresa de Telecomunicaciones de Cuba, ETECSA, Calle 19 esquina B, Plaza de la Revolución, La Habana, Cuba.

[1]e-mail: yoanlarry.cecilio@etecsa.cu
[2]e-mail: aileen.forte@etecsa.cu

RESUMEN

El crecimiento acelerado de la interconexión digital de los objetos cotidianos con Internet (Internet de las cosas o IoT por sus siglas en inglés) mediante múltiples tecnologías y sensores, hace necesario el definir un grupo de protocolos que permitan, de manera unificada, realizar las funciones de colección, almacenamiento, procesamiento y gestión de la información. Lo anterior es aún más necesario si se tiene en cuenta que dichos sensores permiten conectar el mundo físico con el digital, así como el desarrollo de computadores que permiten acceder a dicha información mediante plataformas web, donde se procesan y almacenan los datos. En esta investigación se analizan un grupo de variantes que permiten garantizar la gestión de IoT, teniendo en cuenta sus características y posibles campos de aplicación. Se hace énfasis en lo referido al intercambio de información entre terminales y la estandarización de los protocolos WBEM y SNMP.

PALABRAS CLAVES: IoT, protocolos, gestión.

MANAGEMENT IN INTERNET OF THINGS

ABSTRACT

The accelerated growth of the digital interconnection of everyday objects with the Internet (Internet of things or IoT) through multiple technologies and sensors, makes it necessary to define a group of protocols that allow, in a unified way, to perform the functions of collection, storage, information processing and management. The foregoing is even more necessary if one takes into account that these sensors allow connecting the physical world with the digital one, as well as the development of computers that allow access to said information through web platforms, where the data is processed and stored. This research analyzes a group of variants that allow guaranteeing the management of IoT, taking into account its characteristics and possible fields of application. Emphasis is made on the exchange of information between terminals and the standardization of the WBEM and SNMP protocols.

INDEX TERMS: IoT, protocols, management.

1. INTRODUCCIÓN

El crecimiento de Internet y su adaptación a nuestra vida cotidiana va más allá de las redes sociales y los buscadores de información. El alcance de Internet se ha introducido, en la vida completa de sus usuarios, en temas que hasta hace pocos años, no hubiésemos sido capaces de imaginar. El vertiginoso desarrollo de las redes de telecomunicaciones en los últimos 10 años ha traído consigo grandes oportunidades y retos. Ya el IPV6 (Internet versión 6) es una realidad y esto abre una gran brecha para que los más disímiles equipos puedan ser conectados a las redes y por supuesto, ser gestionados [1]. El Internet de las cosas (Internet of Things o IoT) y el Internet de todo (Internet of Things IoE) son los dos ejemplos prácticos más significativos que demuestran la afirmación anterior.

El IoT es el Internet que se utiliza por medio de diferentes dispositivos, como fotocopiadores, teléfonos, automóviles, televisores, etc. El objetivo de éste es seguir brindándole una experiencia en línea al usuario desarrollando nuevos y mejores “aparatitos online” que se encuentren en conexión permanente a través de Internet.

Manuscrito recibido: 2021-02-08, aceptado: 2021-02-08
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

Revista Telemática. Vol.20 No.2 ,Abril-Junio, 2021, p.63- 84 ISSN 1729-3804

Por otro lado, el IoE es el Internet que se aplica, por medio del uso de dispositivos interconectados en Internet, para una infinidad de usos y para toda una comunidad de usuarios. Básicamente, el "Internet del Todo" busca la integración de experiencias entre usuarios en línea para el propio beneficio de éstos. Tomando en cuenta esto, podemos decir que el IoT es una parte esencial de IoE; uno engloba al otro.

Se estima que, en un día común es posible encontrar a cualquier ser humano rodeado por entre 1000 y 5000 objetos. Sería interesante imaginar lo que se podría llegar a hacer si se consiguiera desarrollar una tecnología que conectara a cada uno de estos objetos a Internet. Asimismo, según Forbes, en 2020 se espera que las industrias de transporte y logística, fabricación discreta y servicios públicos gasten 40 mil millones de dólares (cada una) en plataformas, servicios y sistemas de IoT en todo el mundo [4]

La necesidad de estandarizar los protocolos para la gestión de los terminales IoT, así como la información que estos tributan, constituyen aspectos claves en el desarrollo de este artículo. Para esto se realiza un estudio de los más utilizados en la actualidad por los diferentes fabricantes de dispositivos, se muestran sus características más significativas, así como la factibilidad de utilizar uno u otro.

Para lograr lo anterior se realiza incialmente una breve explicación teórica de los conceptos más importantes relacionados con IoT, lo que incluye también su arquitectura por capas y sus características. Posteriormente se describen los protocolos de gestión más utilizados, señalando sus apsectos más significativos y lo que hace que estos sean adoptados por los fabricantes, lo que permite llegar a conclusiones de cuales son los más difundidos y el porqué.

2. IOT, CONCEPTO Y ARQUITECTURA

El internet de las cosas (IoT), se refiere a la interconexión digital de los objetos cotidianos con Internet, conformado de múltiples tecnologías como sensores que permiten conectar el mundo físico con el digital, computadores que permiten procesar esa información y plataformas web donde se procesan y almacenan los datos [1]. Dicha tecnología nos permite llevar a la implementación una idea, lo que no hace enfocarnos en definir correctamente el concepto de la idea y abrir nuestra imaginación hacia proyectos que en otro momento se hubiesen transformados en temas perfectos para filmes de ciencia ficción. IoT abre las puertas a la innovación y alienta a implementar nuevas soluciones [2].

¿Cuál es la arquitectura propuesta para IoT? ¿Qué capas podemos definir?

Por arquitectura entendemos la infraestructura para la especificación de una red de componentes físicos y su configuración y organización funcional, sus principios y procedimientos operacionales, y los tipos de datos que se intercambian entre ellos. Es decir, se describe cómo los componentes físicos del IoT, recogen los datos, cómo se procesan e intercambian, y en qué formatos lo hacen [3]. Según se define en la web Hindawi, en el artículo relacionado con las arquitecturas de IoT [4], estas pueden ser representadas de dos formas (Ver Fig.1).

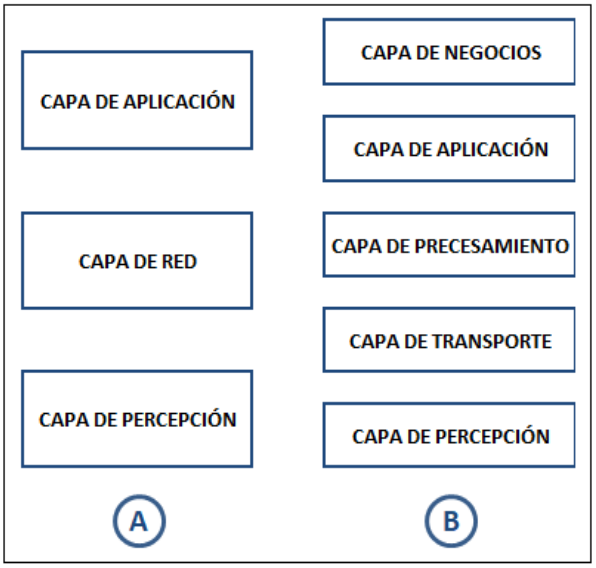

Figura 1: Arquitectura IOT. (A: Tres niveles)(B: Cinco niveles).

La de la izquierda es la más sencilla, y resulta perfecta desde el punto de vista conceptual, porque describe completamente la lógica de la tecnología: los datos recabados por los dispositivos físicos se transmiten hacia otros dispositivos, servidores o elementos de la red y se procesan en las aplicaciones finales para un uso concreto. Consta de tres capas: la capa de Percepción, que se corresponde al nivel físico, el de los dispositivos, y a la adquisición de datos por medio de sensores; la capa de Red, que se encarga del transporte de los datos de las capa superior a la inferior y viceversa y la capa de aplicación. Todas estas capas deben garantizar que el usuario acceda al servicio sin preocuparse por el funcionamiento del sistema.

Capa de Percepción: En ella se encuadran los diferentes sensores encargados de recoger información del entorno. Aquí se "sienten" parámetros físicos, o bien se identifican otros dispositivos inteligentes del entorno.

Capa de Red: Se encarga de conectar el dispositivo a otras "cosas inteligentes", o bien a dispositivos de red o servidores. Dispone de las herramientas necesarias para transmitir datos entre dispositivos (o servidores y dispositivos de red), y también para realizar cierto grado de procesamiento de los mismos.

Capa de Aplicación: Es en la que se enmarcan las aplicaciones del usuario. Desde las aplicaciones domésticas sobre uso de recursos (agua, gas, electricidad), hasta las aplicaciones logísticas para las empresas, que optimicen los recursos y el tiempo de procesado. Cualquier aplicación, doméstica o industrial, que haga uso de dispositivos conectados (IoT) se incluye en esta "capa" (por ejemplo, las que hacen posible la smart home, smart cities, eHealth…).

La arquitectura de la derecha es más compleja pero con más detalles que se ajustan mejor a un diseño real, esta dispone de dos capas que funcionan igual, que son la capa de Percepción y la de Aplicación, a continuación se describen las tres restantes:

Capa de Transporte: se encarga de todo lo necesario para transmitir información de la capa inferior (percepción) a la superior (procesamiento). Esto significa que resuelve la comunicación entre dispositivos a nivel de red (ya sea red 3G/4G, WiFi, Bluetooth,…).

Capa de Procesamiento: se encarga de tomar los datos de la capa inferior y los procesa. En esta capa se situarían todos los servicios de procesamiento de datos como bases de datos, cloud computing o big data, así que podemos decir que es una de las capas principales de la arquitectura.

Capa de Negocio: se concentra la solución de todos los "problemas" de más alto nivel de abstracción, como los modelos de negocio, la privacidad de los datos de usuario, y se gestionan las aplicaciones y en general todo el modelo IoT.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.2 ,Abril-Junio, 2021, p.63- 84 ISSN 1729-3804

El sincronismo es un requisito indispensable para el correcto funcionamiento de las redes y la integridad de los datos. A diferencia de las redes de multiplexación por división de tiempo (TDM, del inglés *Time Division Multiplexing*) heredadas, las redes de paquetes no son deterministas con respecto al retardo y la variación de retardo. Por lo tanto, el rendimiento de la sincronización debe ser monitoreado y asegurado [2].

La migración del transporte basado en TDM a una red de transporte de paquetes ha cambiado significativamente los esquemas de sincronismo. La distribución de la información de temporización para la sincronización constituye un nuevo desafío para los operadores de telecomunicaciones [2].

Han surgido protocolos de sincronismo de próxima generación orientados a infraestructura de redes por naturaleza asíncrona, con el objetivo de garantizar la entrega de servicios en tiempo real y con la calidad requerida. Estos son: Protocolo de tiempo de red (NTP, del inglés *Network Time Protocol*), Ethernet síncrono (SyncE, del inglés *Synchronous Ethernet)* y Protocolo de precisión de tiempo (PTP, del inglés *Precision Time Protocol*). A continuación se describen las principales características de los mismos, haciendo énfasis en el último de los mencionados.

3. GESTIÓN DE IOT

Mantenimiento, control de estado, actualizaciones de software y firmware, reparaciones, en resumen, gestionar una red de unas decenas de ordenadores puede parecer trabajoso, pero no debe ser gran cosa en comparación con responsabilizarse de cientos y cientos de dispositivos que, además, pueden estar diseminados en un muy extensa. Así que por una parte hacen falta sistemas bien diseñados y que permitan realizar la mayor parte de las tareas posibles de manera remota y, por otra parte, profesionales capaces de acometer el desafío de gestionar una red de ese tamaño y con esas peculiaridades.

Una preocupación común por los fabricantes y consumidores de IoT es la interoperabilidad general de estos. Muchos expresan su preocupación de que las plataformas IoT son difíciles de gestionar debido a la falta de estándares y la gran diversidad en dispositivos e implementaciones. La adopción de estándares permitiría plataformas de gestión uniformes y evitaría silos tecnológicos.

Los protocolos de administración estándar han permitido que los sistemas de soporte operativo brinden nuevos servicios e información de muchos proveedores en una plataforma unificada. El protocolo principal que habilita esta capacidad es el Protocolo simple de administración de redes (SNMP) (Ver Fig.2 y 3).

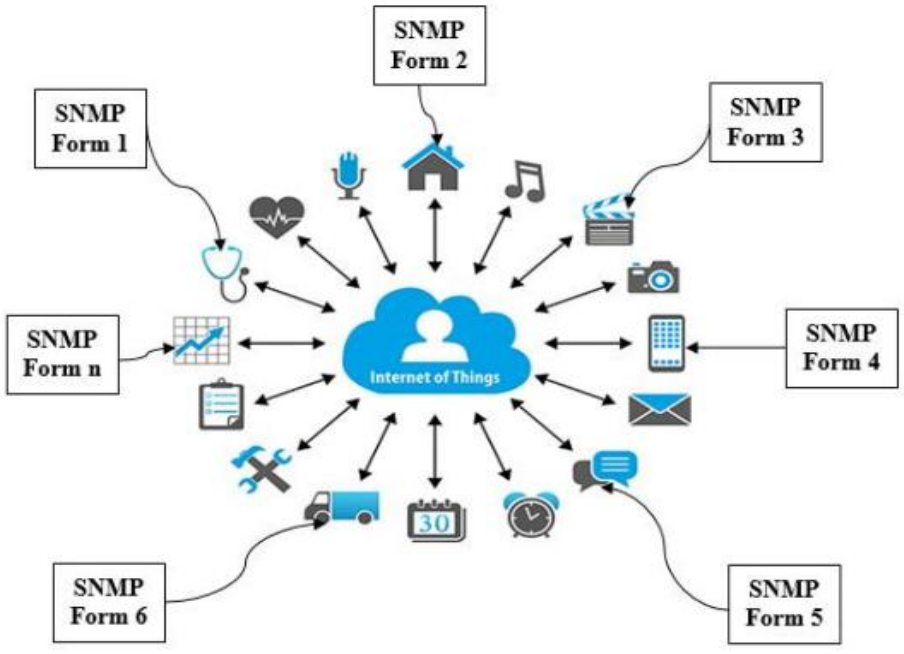

Figura 2: Idea para la gestión utilizando SNMP.

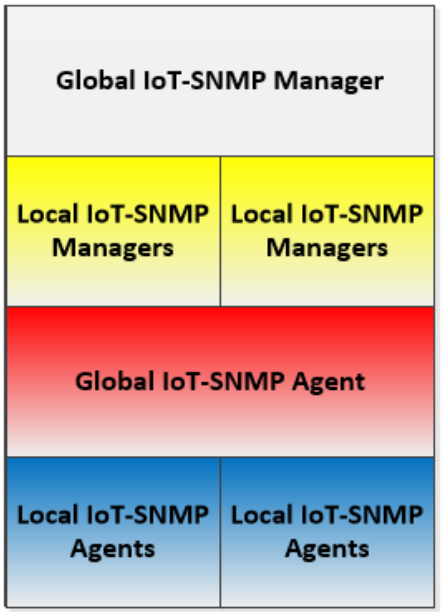

Figura 3: Jerarquía SNMP.

Sus capacidades habilitadas para flexibilidad nunca fueron concebidas originalmente por los vendedores. Un ejemplo es el descubrimiento de redes que permitió a los sistemas de gestión construir relaciones de redes. Los estándares SNMP entre los proveedores de hardware han permitido a los proveedores de software ofrecer esta capacidad. Según la experiencia, la verdadera razón por la cual los protocolos de administración dominados por SNMP radica en lo siguiente [5]:

Ubicuidad. Todos los dispositivos de red son compatibles con SNMP y al igual que el software de monitoreo. Proporciona un estándar genérico que todos los dispositivos deben admitir.

Documentación. Los humanos y las máquinas pueden procesar la documentación en lo que se llama una Base de información de administración (MIB).

Extensibilidad. Los vendedores pueden extender el esquema de sus productos.

Activo y pasivo. Activo: los eventos se pueden generar en tiempo real desde el dispositivo hasta el sistema de gestión. Pasivo, permite que muchos sistemas de gestión recopilen métricas del dispositivo según lo necesiten. Estos dos métodos de gestión brindan flexibilidad para adaptarse a las restricciones de monitoreo y redes.

Flexibilidad. TCP o UDP son compatibles dependiendo de los problemas de recursos. Es decir. Se puede tolerar el uso de UDP para un ancho de banda bajo y pérdida. TCP si no. El cifrado está disponible si es necesario.

IOT se aparta de los dispositivos tradicionales debido a sus limitaciones de recursos. Esto ha llevado a la adopción de protocolos alternativos como CoAP (Protocolo de aplicación restringida) y MQTT (Transporte de telemetría de mensajes en cola).

CoAP: es un "protocolo de transferencia web especializado para usar con nodos restringidos y redes restringidas (por ejemplo, de baja potencia, con pérdida)".

MQTT (y su variante MQTT-SN): según lo define un estándar OASIS, es un protocolo de transporte de mensajería orientado a la publicación / suscripción orientado a servidores cliente ligero, abierto y simple, muy similar conceptualmente al funcionamiento de muchas herramientas de chat.

Otros protocolos que se han ido estandarizando para lograr la gestión de dispositivos IoT son:

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.2 ,Abril-Junio, 2021, p.63- 84 ISSN 1729-3804

OMA Lightweight M2M (LwM2M), creado por la Open Mobile Alliance es un protocolo rápido, ligero y estructurado, ideal para dispositivos de baja capacidad.

OMA-DM, creado también por la Open Mobile Alliance, pero orientado a aplicaciones móviles. Es ideal para cosas en movimiento (que cambian de IP, por ejemplo). Es más complejo y estructurado que LwM2M.

TR-069, creado por el Broadband Forum (la primera versión es de 2004) y usado en cientos de millones de dispositivos en el mundo, al ser un protocolo ampliamente utilizado por los operadores de telecomunicaciones para provisionar routers, etc. Por ello, es muy complejo, pesado y estructurado, pero funciona muy bien para gateways y equipamiento de telecomunicaciones. Como curiosidad, casi ningún producto TR069 está certificado.

Estos protocolos proporcionan ventajas en velocidad, simplicidad, bajo uso y limitaciones de recursos. Sin embargo, debido a su naturaleza muy flexible, carecen de la capacidad de integrarse a las pilas de gestión existentes, ya que están destinadas a ser utilizadas para la transferencia de datos, no para la gestión. Además, un problema continuo con estos protocolos es que pueden prestarse fácilmente a un bloqueo patentado en lugar de SNMP. Algo a considerar, tal vez, es que los protocolos de gestión y transferencia de datos pueden no ser los mismos. MQTT como ejemplo es bueno para respaldar la recopilación de conjuntos de datos desbloqueados por los dispositivos de IoT, pero no necesariamente para la administración de los dispositivos (a menos que tenga la intención de utilizar los datos que se recopilan como un indicador de disponibilidad / estado del dispositivo).

Se ha desarrollado una solución para cerrar la brecha en el monitoreo con la introducción de estos nuevos protocolos IoT al permitir el acceso SNMP a los datos de monitoreo obtenidos de dispositivos con recursos limitados que no pudieron o no puede soportar SNMP. Desarrollaron un servidor SNMP de prueba de concepto que serviría como puente entre los protocolos MQTT y CoAP que podrían ser aprovechados por los sistemas habilitados para SNMP [5] .

El empleo de SNMP para la gestión de los elementos de la IoT es una variante muy atrayente debido a la popularidad que ha alcanzado este estándar de gestión entre los fabricantes y proveedores y a la amplia difusión que ha tenido el mismo. En base a esto se han realizado varios estudios durante los últimos años, los cuales no dejan de ser interesantes, pero hasta que no se suplan las limitantes del protocolo SNMP no podrán ser implementadas eficazmente para gestionar la IoT. Estas limitantes se deben, fundamentalmente a deficiencias propias del protocolo SNMP, que no estaba destinado a ser una norma internacional (las mismas se pueden ver en la RFC35126).

Una de las propuestas del empleo de SNMP para la gestión de IoT que más aceptación ha tenido fue 6LoWPAN-SNMP3. Esta plantea una forma óptima de gestionar los elementos de la IoT por medio de la implementación del protocolo SNMP con algunas modificaciones, entre las que se encuentra poder gestionar los elementos instalando un agente por cada dispositivo, un gestor local en cada Gateway y un gestor remoto en la infraestructura de red IP existente. Las modificaciones propuestas al protocolo SNMP fueron las siguientes [7]:

- Emplear el broadcast o multicast para la transmisión del mensaje de control y configuración de los dispositivos. Esto lo proponen en aras de ahorrar potencia y para el caso de que se gestionen dispositivos similares.
- Incorporar un GETRequest PDU y StopGETRequest PDU de forma periódica, de manera tal que se pueda optimizar el uso eficiente de la energía, factor clave en los dispositivos inteligentes. Este PDU periódico permite que el reporte solo sea pedido una vez por el gestor.
- Comprimir el mensaje SNMP para igualmente reducir el consumo de energía.

Otra propuesta para la gestión de IoT es la utilización de CORBA-TMN. La característica fundamental de este tipo de arquitectura radica en que permite combinar la robustez de CMIP con la interoperabilidad de CORBA.

CMIP es el protocolo que define la información de gestión para la comunicación entre las aplicaciones de gestión y agentes del modelo de gestión OSI. CORBA, por su parte es un framework que entra en el grupo de sistemas de gestión distribuída conocidos como Distributed Object Technology o DOT por sus siglas en inglés. Estos sistemas se destacan por aportar modularidad, abstracción, posibilidad de reutilización del software, de nombrado de recursos y de localización. Empleando CORBA por tanto se posibilita la interoperabilidad de comunicación entre los diversos componentes de software escritos en diferentes lenguajes que van estar integrados en los dispositivos de la IoT.
Las razones fundamentales que detuvieron el desarrollo de este mecanismo en gestión son:

- No existencia de normas para el soporte e implementación de CORBA.
- El stack de protocolos de la arquitectura TMN es muy complejo para ser implementado en la nueva era de la Internet.

La gestión Web basada en empresas (WBEM) es una iniciativa del DMTF para proveer un conjunto de estándares y tecnologías para la gestión de Internet desarrollados con el fin de unificar los sistemas de gestión de redes, de usuarios y aplicaciones existentes. Esto lo logra fundamentalmente gracias a su trabajo en conjunto con el modelo de información común: CIM. Se puede destacar como principal ventaja del empleo de WBEM en la gestión de IoT que la misma aprovecha el poder de la Web para facilitar las tareas de gestión. Los componentes fundamentales que forman parte de la arquitectura del sistema de gestión Web basada en empresas son la aplicación de gestión (WBEM-Client) y el intermediario entre el gestor y el hardware del dispositivo, el WBEM-Server, el cual es comúnmente instalado en los dispositivos (Ver Fig. 4).

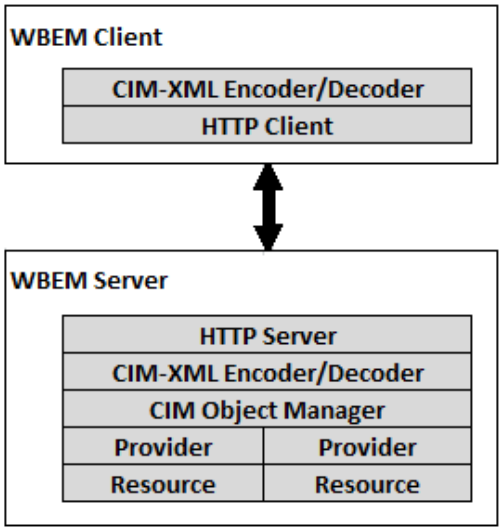

Figura 4: Arquitectura WBEM.

Una de las principales características del WBEM-Client es que obtiene la información de gestión a partir de una comunicación directa con el CIMOM empleando los mensajes Request, en vez de acceder directamente a los proveedores asociados a los dispositivos. Esta característica le brinda interoperabilidad al modelo. Por su parte, el WBEM-Server permite ocultar los detalles de comunicación entre el gestor y los proveedores que interactúan directamente con el hardware del dispositivo.

Como se puede observar en la figura, la diferencia fundamental en los dos componentes radica en que el WBEM-Server está compuesto por el CIMOM y los proveedores asociados a los recursos. CIMOM es considerado la pieza clave del WBEM-Server ya que es el encargado de encaminar la información acerca de los objetos y eventos entre el que la solicita (WBEM-Client) y el que la brinda (Provider), además se encarga de comunicarse con el repositorio que contiene la información de gestión asociada a los dispositivos, el CIM-Schema. El resto de los elementos claves de la arquitectura con los protocolos empleados para la comunicación, el protocolo CIM-XML, que se encarga de la codificación/descodificación de la información y el protocolo HTTP para el transporte de los datos.

Este estándar de gestión es empleado en la actualidad por varios líderes de la industria entre los que se destacan IBM, con su conocido sistema de gestión Tivoli. Cisco hizo uso del modelo de información común CIM en su herramienta de gestión CiscoWorks 2000. HP provee soluciones que incluyen WBEM-Services, WBEM-Providers, HP-WBEM-Client y HP-WBEM-SDK, y Microsoft provee un sistema de gestión basado en WBEM embebido en el propio sistema operativo de Windows, a partir del Windows 2000 llamado WMI (Windows Management Instrumentation).

La cuarta tendencia propuesta para gestionar los elementos de la Internet consiste en hacer uso de la gestión autonómica. Este tipo de gestión se destaca por modificar el rol del operador, el cual en vez de controlar el sistema directamente, pasa a realizar funciones asociadas a la descripción de políticas. Es por ello que este tipo de gestión es conocida como PBNM (Policy-Based Network Management).

Revista Telemática. Vol.20 No.2 ,Abril-Junio, 2021, p.63- 84 ISSN 1729-3804

La gestión autonómica ha sido propuesta al igual que WBEM para solventar el problema de gestión de dispositivos complejos. Esto lo logra a partir del cumplimiento de las cuatro funcionalidades prefijadas de la gestión autonómica: auto-configuración, auto-reparación, auto-optimización y auto-protección. Estas funcionalidades se plantea que pueden ser configuradas e implementadas además de las políticas definidas por el hombre a través de ontologías. Una de las principales ventajas del empleo de este mecanismo de gestión en la IoT radica en que el mismo permite automatizar el trabajo del hombre, con lo cual se cumple con la primera hipótesis de la IoT; otra ventaja es que brinda la posibilidad de gestionar entornos tan distribuídos y complejos como los de la IoT.

Debido a que el contexto en que se desenvuelve la IoT tiene implícitas características muy específicas y diferentes de los sistemas para los cuales se concibió la gestión autonómica, va a ser necesario adaptar nuevas técnicas de gestión autonómica con especificidades para el entorno de la IoT. Las especificidades a tener en cuenta son la adaptación a:

- Un elevado dinamismo y distribución
- Una naturaleza en tiempo real
- Dispositivos de recursos limitados
- Medios con pérdidas.

4. CONCLUSIONES

La utilización de Internet de las cosas ha comenzado a ser estratégico para los negocios y será fundamental en los procesos toma de decisiones, otorgando más agilidad a las acciones, mejorando procedimientos y logrando empresas más innovadoras y productivas, pero también consiguiendo ahorrar costes y mejorar la seguridad.

Un punto trascendental en IOT es la gestión de sus terminales y de la información que los mismos brindan, la misma se ha visto frenada en gran medida por la necesidad de estandarizar los protocolos que utiliza los dispositivos, aunque de manera general se percibe que la misma se ha enfocado con mayor fuerza a utilizar:

- WBEM con el objetivo de aprovechar poder de la Web para facilitar las tareas de gestión.
- SNMP debido a la popularidad que ha alcanzado este estándar de gestión entre los fabricantes y proveedores y a la amplia difusión que ha tenido el mismo.

REFERENCIAS

[1] «¿ Qué es IOT? », feb. 15, 2019. https://www.iac.com.co/que-es-iot/ (Accedido: nov. 1, 2019).
[2] «Monitoriza el hardware para el internet de las cosas y sácale todo el partido», oct. 13, 2019 https://www.muutech.com/monitoriza-el-hardware-para-el-internet-de-las-cosas-y-sacale-todo-el-partido/ (Accedido: nov. 1, 2019).
[3] «¿Cómo se resuelve la conectividad masiva que trae el IoT?, oct. 31, 2019», https://www.t-systemsblog.es/como-se-resuelve-la-conectividad-masiva-que-trae-el-iot/ (Accedido: nov. 1, 2019).
[4] «Internet of Things: Architectures, Protocols, and Applications», ene. 26, 2017. https://www.hindawi.com/journals/jece/2017/9324035/ (Accedido: nov. 2, 2019).
[5] «Comparativa entre MQTT y OPC-UA», ago. 20, 2019. https://www.muutech.com/comparativa-entre-mqtt-y-opc-ua/ (Accedido: nov. 2, 2019).
[6] Mihjlo Savić, «Bridging the SNMP GAP: Simple Network Monitoring the Internet of Things», Series: Electronics and Energetics Vol. 29, No 3, September 2016, pp. 475 – 487.
[7] «Arquitectura y Gestión de la IoT», Dana Rodríguez González. Revista Telem@tica. Vol. 12. No. 3, septiembre-diciembre, 2013, p. 49-60.
[8] «Adaptive Protocol for Management Internet of Things Systems: Analysis, Design and Performance Evaluation», Omar Said. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 8 (2018) pp. 6125-6137.
[9] «Design and Testing of SNMP/MIB based IoT Control API», Muhammad Zeeshan, National University of Sciences and Technology (NUST), Islamabad, Pakistan, 2019.
[10] L. Zhao, S. Qu, J. Zeng, and Q. Zhao, "Energy-saving and Management of Telecom Operators' Remote Computer Rooms using IoT Technology," IEEE Access, pp. 1–1, 2020, doi: 10.1109/ACCESS.2020.3022641.

[11] H. Zhang, M. Babar, M. U. Tariq, M. A. Jan, V. G. Menon, and X. Li, "SafeCity: Toward Safe and Secured Data Management Design for IoT-Enabled Smart City Planning," IEEE Access, vol. 8, pp. 145256–145267, 2020, doi: 10.1109/ACCESS.2020.3014622.
[12] N. C. Narendra, N. Deb, and S. Das, "Dynamic Contextual Goal Management in IoT-based Systems," IEEE Internet of Things Journal, pp. 1–1, 2020, doi: 10.1109/JIOT.2020.3013643.
[13] G. Lee, B. Kim, S. Song, S. Heo, and H. Kim, "ComFlex: Composable and Flexible Resource Management for the IoT," IEEE Internet of Things Journal, pp. 1–1, 2020, doi: 10.1109/JIOT.2020.3022873.

SOBRE LOS AUTORES

Yoan Larry Cecilio Nuñez. Ingeniero en Telecomunicaciones. En la actualidad es Especialista B en telemática. Departamento de Soporte Especializado en la Vicepresidencia de Operaciones de la Red (VPOR) en la Empresa de Telecomunicaciones de Cuba SA (ETECSA Es profesor Instructor de la Universidad Tecnológica de La Habana (CUJAE). Número de ORCID 0000-0002-2850-0379.

Aileen Forte Moreno, Ingeniera en Telecomunicaciones y Electrónica. En la actualidad es Especialista A en Informática. Departamento de Plataformas en Vicepresidencia de Operaciones de la Red (VPOR) en la Empresa de Telecomunicaciones de Cuba SA (ETECSA). Es profesora Instructora de la Universidad Tecnológica de La Habana (CUJAE). Su número de ORCID es 0000-0003-2877-7084

CONFLICTO DE INTERESES

No existe conflicto de intereses entre los autores en relación al contenido del artículo aquí reflejado, aunque dos pertenecen a ETECSA y otro a la Universidad Tecnológica de La Habana José Antonio Echeverría (CUJAE). Tampoco existe conflicto de intereses entre los autores y las instituciones a las que están afiliados, ni con ninguna otra institución.

CONTRIBUCIONES DE LOS AUTORES

Yoan Larry Cecilio Nuñez:
Conceptualización, preparación, creación y desarrollo del artículo y aprobación de la versión final a publicar.

Aileen Forte Moreno:
Conceptualización, preparación, creación y desarrollo del artículo y aprobación de la versión final a publicar.

Ambos autores contribuyeron con las ideas que se plasman en el artículo.