REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TELEM@TICA
Revista Telem@tica. Vol. 12. No. 3, septiembre-diciembre, 2013, p. 49-60 ISSN 1729-3804

Arquitectura y Gestión de la IoT

Dana Rodríguez González

ETECSA. Ingeniería en Telecomunicaciones y Electrónica. dana.rodriguez@etecsa.cu

RESUMEN / *ABSTRACT*

Los avances realizados en la nueva era de la Internet, denominada Internet de las cosas (IoT), han sido desarrollados de forma vertical y fragmentada, desplegados más bien por áreas específicas de la industria como la salud, el transporte, la producción, el hogar, entre otras. Es por ello el número tan elevado de arquitecturas y mecanismos de gestión propuestos, los cuales a su vez están conformados por tecnologías, protocolos y estándares diferentes. En aras de consolidar una propuesta única tanto de arquitectura como de gestión en este trabajo se realiza un estudio que abarca las principales tendencias hacia la estandarización en el mercado actual de la IoT. A partir del estudio realizado se propone un esquema de arquitectura de la IoT así como se selecciona la plataforma WBEM para la gestión Web de los dispositivos.

Palabras claves: Arquitectura de IoT, IoT, gestión Web, WBEM

IoT Network Management / Abstract

The advancement made in the new Era of the Internet, which is known for the term: Internet of Things, have been made in a vertically and fragmented way. The changes have been introduced on specific industry fields, like for example on Health, Transport area, Home environment, among others. That is why there exist a huge number of architectures and management proposals, including different technologies, protocols and standards. Trying to find a unique and standard proposal suitable for all the IoT network this work present an study of the main tendencies of the standardization process and select the technologies and protocols that best suited for the bigger picture of the IoT. Architecture is proposed and the standard WBEM for the web management is selected as well.

Key words: IoT, Web management, WBEM

INTRODUCCIÓN

Los avances alcanzados en los últimos años en la circuitería embebida con la miniaturización de los chips y sus Sistemas Micro-eléctrico-Mecánicos (MEMS), los avances alcanzados en la Internet con el surgimiento de la computación en la nube, los servicios Web y los grids, y en las comunicaciones inalámbricas con la tecnología de sensores RFID (Radio Frecuency-ID) y la aceptación de la tecnología UPnP (Universal Plug and Play) en el hogar, han propiciado el surgimiento de una nueva era: "La era de la Internet de las cosas", aquella donde todo dispositivo electrónico o mecánico se convierte en un ente inteligente, capaz de comunicarse, compartir información y tomar decisiones de forma autónoma empleando la comunicación inalámbrica y la propia Internet como base para la comunicación.

Para poder implementar esta nueva era tecnológica de la IoT en la red actual de Internet, tal y como se conoce, será necesario resolver el problema asociado a la concurrencia de un número muy elevado de dispositivos de naturaleza heterogénea sobre la Internet, lo que es conocido como el paradigma de la futura existencia de 7 trillones de dispositivos por 7 billones de personas[1]. En base a ello, variadas organizaciones y proyectos, pertenecientes la mayoría a sectores específicos en la industria han propuesto protocolos y estándares. Esto, a su vez, tiene la limitante de que provoca la existencia de una IoT muy fragmentada y desarrollada de forma vertical, por sectores independientes de la industria. De manera que queda conformada una arquitectura de la IoT diferente para cada área especifica de la industria, medicina, hogar, producción, transporte, etc.

Debido a la necesidad existente de encontrar una arquitectura y un mecanismo de gestión estándar que permitan la interoperabilidad y convergencia entre todos los elementos que conformen la IoT, este trabajo se propone realizar un análisis del estado del arte de todos los protocolos y estándares existentes relacionados a esta nueva era para a partir de ello poder dejar propuestos una única arquitectura y mecanismo de gestión para la IoT.

Para la realización de esta investigación se emplearon los métodos de trabajo teórico y valorativo, a través de los cuales se pasó a revisar, analizar y comparar las diferentes propuestas para la arquitectura y gestión de los elementos de la Internet de las cosas referentes a gran parte de la bibliografía existente.

Arquitectura de la IoT

La estandarización de una arquitectura para la IoT es aún un proceso en desarrollo. La tendencia ha estado inclinada a darles solución a dos problemas fundamentales: buscar una forma estándar de acceso al medio y a los dispositivos, y buscar la forma de integrar los dispositivos a la Internet. Tomando como base el estudio realizado en el proyecto IOT-A[2], en la tabla 1 se hace un resumen de las principales organizaciones, proyectos, protocolos y arquitecturas propuestas correspondientes al mencionado proceso de estandarización.

Dentro de los principales aportes realizados por las organizaciones se destacan la IEEE (Institute of Electrical and Electronics Engineers) en grupos de trabajo 802.15 y el protocolo 802.15.4 que permite la comunicación con bajas tasas de transmisión para poder trabajar con dispositivos de bajo coste y recursos limitados. La IETF (Internet Engineering Task Force) con variadas propuestas, como el protocolo CoAP (Constrained Application Protocol) protocolo de la capa de aplicación que corre sobre UDP especializado en la transferencia de datos a través de la Web y que se destaca por permitir a los dispositivos con recursos limitados comunicarse; el protocolo RPL (IPv6 Routing Protocol for Lower and

Lossy Networks), protocolo de capa de red que permite trabajar igualmente con dispositivos de recursos limitados, el 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) que actualmente es un grupo de trabajo independiente enfocado en el protocolo que lleva por nombre el mismo del grupo. También, se destacan la organización W3C (World Wide Web Consortium) con el protocolo SOAP (Simple Object Access Protocol) que define cómo los objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML. El grupo OMG (Object Management Group) con el framework CORBA (Common Object Request Broker Architecture) que brinda interoperabilidad entre elementos software de naturaleza diferente, y el DMTF (Distributed Management Task Force) con sus propuestas también, entre las que se destaca WBEM (Web Based Enterprise Managment) con los protocolos CIM-XML (Common Information Model-Extensible Markup Language), WS-MAN (Web-Service Management) y WSDM (Web Service Distribution Management).

Tomando como base a las propuestas anteriores listadas en la tabla 1 y haciendo una analogía a los conocidos modelos OSI y TCP/IP, esta tendencia a la estandarización puede quedar resumida como se muestra en la figura 1.

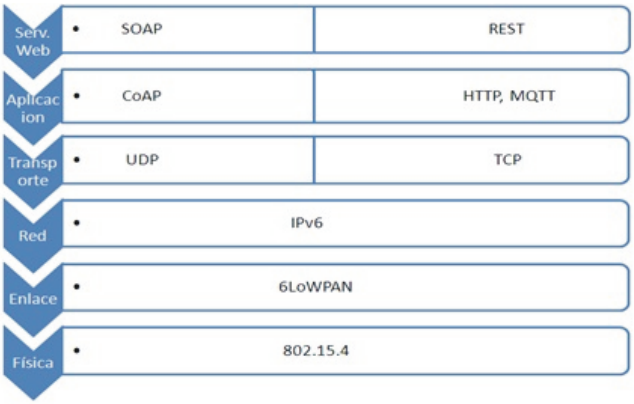

Figura 1. Stack de Protocolos de la Arquitectura de la IoT

Como se puede observar, queda definido en la capa física o de acceso al medio el estándar 802.15.4. Esta decisión se tomó basada en las ventajas de este estándar para la IoT, principalmente debido a que permite trabajar con dispositivos de recursos limitados, como es el caso de la mayoría de los elementos de la IoT y porque además permite el consumo eficiente de energía por parte de los dispositivos al cubrir cortas distancias y emplear tasas de transmisión bajas. Dentro de este estándar se destacan el protocolo de comunicación ZigBee y la tecnología de sensores RFID caracterizadas ambas por bajo un costo de implementación y por favorecer aún más el bajo consumo.

En la capa de enlace se propone el estándar 6LoWPAN, puesto que permite emplear como medio físico el estándar 802.15.4 y a IPv6 como estándar de comunicación, a partir de la definición de mecanismos de compresión y encapsulación de la cabecera de los paquetes IPv6 sobre el ya seleccionado 802.15.4.

La selección de IPv6 como protocolo de comunicación se debe a que es el único estándar que permite interoperabilidad con la infraestructura de red existente a la vez que permite asignarle una dirección única a cada uno de los miles de millones de dispositivos que se prevén que conformen la IoT. Cabe destacar que actualmente se está empleando en muchos sistemas, el direccionamiento mediante las RFID-tags, empleando el estándar EPC, pero esta tecnología no es escalable, ni concibe la

intercomunicación de todos los dispositivos de la IoT empleando la infraestructura de Internet como base.

En la capa de transporte pueden seleccionarse UDP si se va a emplear el protocolo de capa de aplicación CoAP, y TCP para el resto, que representa la mayoría de aplicaciones Web que corren sobre HTTP o el nuevo MQTT, aún no estandarizado.

Por su parte, la capa de aplicación está representada fundamentalmente por los protocolos CoAP, HTTP y MQTT aunque cabe mencionar, también la posibilidad de poder emplear los conocidos protocolos FTP, SMTP y JMS. El protocolo CoAP es un protocolo de poca complejidad, baja sobrecarga y de fácil traducción a HTTP para simplificar su integración con la Web. Como su nombre lo indica este protocolo fue desarrollado, fundamentalmente para entornos con recursos limitados, como es el caso de los WSN (Wirereless Sensor Networks) dentro de la IoT. Por su parte, el MQTT es un protocolo del tipo publish/subscribe muy simple y ligero, diseñado específicamente para redes y dispositivos de recursos limitados y con bajas tasas de transmisión. El HTTP es el protocolo más difundido en la actualidad y es el empleado para cada transacción de datos que se hagan sobre la Internet y por tanto considerado pieza fundamental para el transporte de los servicios Web en esta nueva arquitectura de la IoT.

La última capa propuesta no corresponde a ninguna capa del modelo OSI o TCP/IP, sino quees una nueva capa que se añade para permitir la comunicación entre los dispositivos sobre la Internet: La capa de servicios Web. Los servicios Web son basados en estándares como SOAP y en arquitecturas REST para intercambiar datos entre aplicaciones de software desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma. Esta interoperabilidad la consiguen mediante la adopción de estándares abiertos.

Cabe destacar que el empleo de los servicios Web como nueva capa de la arquitectura de la IoT trae ciertos beneficios, entre los que se encuentran:

- Los servicios Web van a constituir el método, por defecto de comunicación entre los dispositivos (M2M) empleando como base la Internet.
- El uso de estándares abiertos basados en HTTP como base da el poder de desarrollar independientemente del dispositivo, es decir de la plataforma o lenguaje de programación de la aplicación.
- El empleo de esta tecnología para la comunicación permite consumir menos recursos de cómputo en los dispositivos, ya que los servicios Web trabajan directamente con los datos puros, al contrario de las aplicaciones Web.

Entre las principales plataformas existentes basadas en servicios Web que se emplean para gestionar la información de determinados sensores ubicados en dispositivos inteligentes empleando la tecnología de computación en la nube se encuentran Pachube, Nimbits, ThingSpeak y SensorCloud. Estos servicios permiten recoger datos en tiempo real de varios dispositivos y mantener el control de los mismos.

A manera de conclusión, sobre el tema de estandarización de la arquitectura se puede plantear que la arquitectura propuesta permite resolver el problema de la interoperabilidad entre las arquitecturas de IoT existentes en sectores específicos de la Industria, al emplear la Web como medio de comunicación entre los dispositivos. Además, logra resolver el problema de intercomunicación de los elementos de la

IoT con la infraestructura de red existente, por medio del empleo de protocolos de Internet estandarizados.

Mecanismos de gestión de IoT

La literatura existente relativa a las formas de implementación de la gestión de la IoT se puede dividir en cuatro grupos de acuerdo al mecanismo o estándar de gestión empleado: SNMP (Simple Network Management Protocol), TMN (Telecomunication Network Management), WBEM (Web Based Enterprise Management), y PBM (Policy Based Management) que corresponde a la gestión autonómica. A continuación se realiza un breve resumen de cada una de las propuestas que conciernen estos estándares para gestionar los elementos de la IoT.

1- Gestión de IoT haciendo uso del protocolo SNMP modificado

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, entre los que sobresalen[3, 4, 5]. Estas propuestas 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 limitantes del protocolo SNMP se pueden consultar en la RFC3512[6].

Una de las propuestas del empleo de SNMP para la gestión de IoT que más aceptación ha tenido fue 6LoWPAN-SNMP[3]. 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.

- 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.

2- Gestión de IoT usando CORBA-TMN

La característica fundamental de este tipo de arquitectura en la que se basan varias propuestas[7, 8, 9] 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 existen 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.

3- Gestión de IoT usando WBEM

La gestión Web basada en empresas (WBEM) es una iniciativa del DMTF[10] para proveer un conjunto de estándares y tecnologías para la gestión de Internet desarrollados con el fin de unifica 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, como se puede observar en la figura 2.

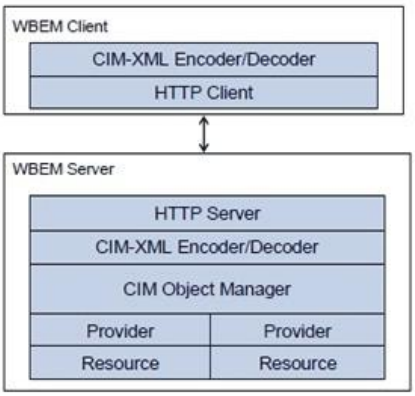

Figura 2. Arquitectura WBEM[11]

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 enrutar 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 [12]. Cisco hizo uso del modelo de información común CIM en su herramienta de gestión CiscoWorks 2000 [13]. HP provee soluciones que incluyen WBEM-Services, WBEM-Providers, HP-WBEM-Client y HP-WBEM-SDK[14], 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[15] (Windows Management Instrumentation).

4- Gestión de IoT haciendo uso de PBM

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).

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

Hasta el momento no se cuenta con un sistema de gestión autonómico estandarizado para los elementos de la IoT, solo se destacan algunas propuestas de software en sectores específicos del sistema de gestión autonómico, como las que se destacan: el uso de DPSW (Device Profile for Web Service) usando JMEDS (Java Multi Edition DPWS) [16] para implementar los gestores autonómicos. El empleo del framework SAF (Symtom Automatation Framework) [17] el cual es basado en XML y a su vez

permite el tratamiento y diagnóstico de sistemas complejos. Y GAMF (Generic Autonomic Management Framework) [18] que tiene como objetivo habilitar gestores autonómicos en desarrollo en cualquier sistema especifico sin necesidad de re-implementarlo.

Selección de Plataforma de Gestión: WBEM

Para pasar a seleccionar el método de gestión de los elementos de la IoT se trazaron los siguientes requerimientos:

- El mecanismo seleccionado debe ser capaz de brindar Interoperabilidad con la infraestructura de red existente y todos los elementos inteligentes que conforman la red.
- Debe ser capaz de no sobrecargar por procesamiento a los dispositivos, que se caracterizan por tener recursos limitados.
- Debe permitir configuración remota y autoorganización.
- Debe existir la facilidad de que cualquier dispositivo pueda añadirse a la red sin importar la plataforma o hardware que emplee.
- Tomando en cuenta la arquitectura propuesta, donde los servicios Web constituyen un componente esencial para la comunicación entre los objetos de la IoT, el estándar de gestión a seleccionar debe ser capaz de permitir gestionar los servicios Web.

Luego de analizados los mismos como se muestra en la tabla 2, es evidente que los beneficios recaen sobre WBEM. Note que no se incluyó la gestión autonómica debido a la escasez de implementaciones de propuestas existentes.

Tabla 1. Proceso de Estandarización de la IoT

Organizaciones	Proyectos	Plataformas	Protocolos
Comité Técnico M2M ETSI	FlexWare	Interdigital	SCADA
3GPP TSG Service & System Aspects	SIRENA	Orange Labs Digital Home	Modbus
TIA TR-50 Comité de Ingeniería	SODA	EDF R&D Smart Gris Experimental Platform	UPnP
IETF	UseNet	Wuxi Instituto de las cosas (China)	NAT-PMP
Global ICT, forum de estandarización de la India	EXALTED	Trangram (Japón)	DPWS
ITU	AIM	HP CenSe	CoAP
Open Mobile Alliance	eSENSE	EMMON	6LoWPAN
DMTF, M2M Standarization Task Force	OpenWSN	Alcatel Home Sensor Gateway Prototype	SOAP
W3C	Berkeley's Local	AIM Gateway Prototype	MQTT
OMG	Intel Iris Net	BOSP	JXTA
EPCGlobal	Berkeley's WEBS	Intel Framework	Zigbee

Tabla 2. Comparativa de los mecanismos de gestión

	SNMP	CORBA/TMN	WBEM
Confiabilidad	Poco	Confiable	Confiable
Cobertura	Hasta nivel de red	Hasta nivel de servicio y negocio	Hasta nivel de servicio y negocio
Enfoque de lenguaje	Orientado a variables ASN.1	Orientado a objetos (OO) ASN.1	Técnicas de modelamiento OO UML (MOF)
Complejidad	Simple dispositivo Complejo en gestor	Muy complejo	Distribuida

CONCLUSIONES

Tomando como base los aportes realizados en los últimos años por diferentes organizaciones y en sectores específicos de la industria dirigidos a encontrar una forma estándar de integrar los dispositivos inteligentes a la Internet, este trabajo deja propuestos una arquitectura y mecanismo de gestión que permiten contemplar la implementación sobre la IoT de todas estas tecnologías y protocolos propuestos y a su vez mantener la interoperabilidad con los elementos de la existente Internet. Como parte de esta propuesta se destaca el empleo de IEEE 802.15.4 y del estándar 6LoWPAN para adaptarse a un medio restringido y de bajas tasas de transmisión típico de la IoT, y el protocolo IPv6 como forma de solucionar el problema del direccionamiento de los miles de millones de dispositivos. Por su parte, los servicios Web quedaron seleccionados como lenguaje por defecto para la comunicación entre los elementos de la IoT.

Sobre la gestión de todos los elementos de la IoT se analizaron las limitantes de SNMP y de la arquitectura TMN-CORBA y se seleccionó a la tecnología WBEM para la gestión de los servicios Web integrados en los dispositivos. De los mecanismos de gestión propuestos quedó pendiente y abierta la variante de emplear la gestión autonómica para los dispositivos de la IoT.

REFERENCIAS

1. Kraemer, R., & Katz, M. (Eds.). (2009). Short-range wireless communications: Emerging technologies and applications. Wiley (pp 14).

2. IOT-A project: disponible en www.iot-a.eu/public/public-documents/d3.1.

3. Choi, H., Kim, N., & Cha, H. (2009, Junio). 6lowpan-snmp: "Simple network management protocol for 6lowpan. In High Performance Computing and Communications, 2009. HPCC'09. 11th IEEE International Conference on (pp. 305-313). IEEE.

4. Ning, H., Ning, N., Qu, S., Zhang, Y., & Yang, H. (2007, Diciembre). "Layered structure and management in internet of things. In Future Generation Communication and Networking" (Fgcn 2007) (Vol. 2, pp. 386-389). IEEE.

5. Chen, C. Y., Chao, H. C., Wu, T. Y., Fan, C. I., Chen, J. L., Chen, Y. S., & Hsu, J. M. (2011). "IoT-IMS Communication Platform for Future Internet. International Journal of Adaptive, Resilient and Autonomic Systems (IJARAS)", 2(4), 74-94.

6. MacFaden, M. (2003) "Configuring Networks and Devices With SNMP-RFC3512". The Internet Engineering Task Force (IETF).

7. JEONG, Moon-Sang, et al. "CORBS/CMIP: gateway service scheme for CORBA/TMN integration". Knom Review, 1999, vol. 2, no 1, p. 55-62.

8. Chen, G., Neville, M., & Kong, Q. (1996, Octubre). Distributed network management using CORBA/TMN. In Proceedings of the 7th IFIP/IEEE International Workshop on Distributed Systems Operation and Management (DSOM).

9. Jae-Young, K. I. M., Hong-Taek, J. U., Hong, J. W. K., Seong-Beom, K. I. M., & Hwang, C. K. (1999). "Towards TMN-based integrated network management using CORBA and java technologies". IEICE transactions on communications, 82(11), 1729-1741.

10. Estándar WBEM del DMTF: http://www.dmtf.org/standards/wbem. Visitado el 15 de abril 2013.

11. Chris Hobbs (11 febrero 2004): "A Practical Approach to WBEM/CIM Management" (pp 18-20)

12. Boss, G., Malladi, P., Quan, D., Legregni, L., & Hall, H. (2007). "Cloud computing". IBM white paper, 1369.

13. YOO, Sun-Mi, et al. "Performance evaluation of wbem implementations". KNOM Review, 2006, vol. 8, no 2,

(pp. 7)

14. HP WBEM: http://h71028.www7.hp.com/enterprise/cache/9920-0-0-225-121.aspx. Visitado el 3 de abril 2013

15. Tunstall, C., & Cole, G. (2003). Developing WMI solutions: a guide to Windows management instrumentation. Addison-Wesley Professional.

16. Karnouskos, S., & Izmaylova, A. (2009, Junio). “Simulation of web service enabled smart meters in an event-based infrastructure. In Industrial Informatics”, 2009. INDIN 2009. 7th IEEE International Conference on (pp. 125-130). IEEE.

17. Isaiadis, S., Lee, V., Snelling, D., Lipton, P., & Vaught, J. (2010, Noviembre). “Symptoms Automation Framework for Cloud Business Alignment: A Collaborative and Responsive Architecture for Knowledge Sharing”. En Intelligent Networking and Collaborative Systems (INCOS), 2010 2nd International Conference (pp. 161-168). IEEE.

18. Tauber, M. (2010). “A Generic Autonomic Management Framework” (GAMF).