2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing

Challenges of the Internet of Things: IPv6 and Network Management

Hanane Lamaazi[1], Nabil Benamar[1], Antonio J. Jara[2], Latif Ladid[3] and Driss El Ouadghiri[1]
[1]University Moulay Ismail, Faculty of Science, Meknes
Laboratory of Modeling Analysis and Control System, Meknes, Morocco
{Lamaazi.hanane; benamar73; dmelouad}@gmail.com
[2]University of Applied Sciences Western Switzerland (HES-SO)
Sierre, Vallais, Switzerland
jara@ieee.org
[3]IPv6 Forum and University of Luxembourg
Luxembourg
latif@ladid.lu

***Abstract*— Nowadays, many researchers are interested in the concept of Internet of Things (IoT). IoT is evolving our knowledge and conception of the world. IoT aims to offer a common communication paradigm for all objects via the Internet and its protocols. For that reasons, it is being applied in all areas of life, such as environmental monitoring, healthcare, military, cities management, and industry. One of the major challenges of the IoT is to integrate IPv6, and its related protocols, into the constrained capabilities offered by Wireless Sensor Networks, building automation, and home appliances. One of the design considerations, for the success of the IoT, is to integrate what exists from IPv6, before creating novel protocols, in order to promote and ensure the interoperability, homogeneity, openness, security, flexibility, and heritage of all existing hardware, tools, and applications of IPv6. This work presents how to integrate the management protocols in IPv6 into the emerging IoT networks based on protocols such as 6LoWPAN. An overview of the different management protocols for IPv6 is presented. Network Management Protocol (SNMP), and the considerations for IoT management from works such as Lightweight Network Management Protocol (LNMP), and the COnstrained networks and devices MAnagement (COMAN) Group from the IETF are discussed. COMAN is presenting solutions such as simplified MIB, new SNMP consideration, and CoAP-based management.**

Keywords*— *IoT, IPv6, SNMP, COMAN, 6LoWPAN, WSN, management protocol, LNMP.

I. INTRODUCTION

For a long time, the concept of Internet of Things was just a metaphor, but with time it has become a reality. Nowadays, the number of devices connected to Internet is increasing continuously; it is expected to reach from 30 to 80 billion devices by 2020 [1]; evolving from an “Intranet of Things” from industrial and insolated environments, to an “Internet of Everything” [2].

IPv6 addressing space is making possible to connect unlimited number of devices with Internet [3]. The IoT is based on Low-Power Wireless Personal Area Networks (LoWPAN), which are intelligent devices that have low and constrained performance. For this purpose, the IETF defined IPv6 on LoWPAN networks to extend these smart devices on the Internet. This definition has given birth to the protocol: 6LoWPAN [3], thereby, integrating IPv6 into Wireless Sensor Networks (WSN) [4]. For IoT, the challenges to offer IPv6 communication imposed WSN to apply IPv6 [5]. Given the constrained environments in which they are implemented, WSN gains the benefit of IPv6 and allow a computerized maintenance and management compatible with these networks, to facilitate maintenance and provide the most suitable service user [5].

IoT networks needs tools and resources to carry out the management given its complexity in order to ease of deployment and provide optimal service to the end-users [6]. For this purpose, several management protocol have been proposed, to reach this need, such as LNMP (LoWPAN Network Management Protocol) which is based on the 6LoWPAN protocol, SNMP (Simple Network Management Protocol) is a protocol designed for the management and control devices connected to the IP network.

A. Problem Statement

The new concept “Internet of things" in its use depends on the type of layer or network on which it is based. The common notions in these considerations are the 'thing' or 'objects' that must have physical or virtual identities, using interfaces to communicate. In our studies, we should make a difference between smart objects and constrain and smart devices. The latter is identified by an IP address, while smart objects considered as virtual resource, use unique identifiers. Furthermore, constrain devices have a low memory capacity and a low power processor. Their goal is to make self-configurable devices for ease of deployment [7].

For smart energy applications, and home automation, the IETF has developed a protocol at the application layer, which is the CoAP designed to constrain devices. It is necessary for the exchange of information and the treatment of an object-object communications, which allow interoperability of the various applications and data [7].

For the IoT, the use of a huge number of devices offers a large amount of data that must be collected, filtered and treated to make them less complicated to use. This has made rethink giving these smart devices, the self-configuration and self-management features, these features can be satisfied if connection establishment devices. This idea has already became a reality in some standards organization such as 3GPP [7].

Here the main aim for an ideal world is to create a single management protocol, which allows at the same time, monitoring, configuration, and management of any network: basic network, wireless, Smart Grid...

978-1-4799-4331-9/14 $31.00 © 2014 IEEE
DOI 10.1109/IMIS.2014.43

For network management and constrain devices the IETF has not yet developed technologies to meet this need, taking into account their low power processor and limited memory capacity. To make the resource management and monitoring of data, these devices use protocols in the application layer, but which remain satisfactory only for some cases [7].

This work is focused on the analysis of the different mechanisms for management in constrained networks based on IPv6. This paper is structured as follows: Section 2 gives a concept of IoT communication. Section 3 presents the use cases of COMAN. Then, Section 4 identifies the candidate technologies of COMAN. After that, we treated some protocols of management, such as LNMP, SNMP which are analyzed in the Section 5. Section 6 discussed the different options available, a finally Section 7 concludes this work.

II. INTERNET OF THINGS

Each author defines IoT according to a particular aspect that he wants to put forward. Thus, we have found many definitions, each reflecting a particular point of view [8].

Here we propose a definition of IoT by S. Bortzmeyer AFNIC (French Association for Internet Naming in Cooperation): "*give the ability to communicate on the Internet to objects that are not considered, from near or far, as computers*" [8]. IoT is also defined as "virtually custom objects and identified that can connect and communicate in space and with intelligent interfaces". Following these definitions, it can be concluded that, the IoT attribute to objects of human qualities, such as smart and communication ability, also gives them a ubiquitous dimension [9].

Generally IoT is based on independent systems, each one with its own infrastructure that sits on an existing Internet infrastructure, and which starts in relationship to services. The IoT enables communications from Object to person; from object to object, and from Machine to machine (M2M).

IoT is a gathering of several domains, but before that it is a gathering of innovative ideas that gave birth to this technology that will change our lives completely. The following diagram illustrates the different stages of development of the idea of the IoT, taking into account the different nature of transactions and interactions.

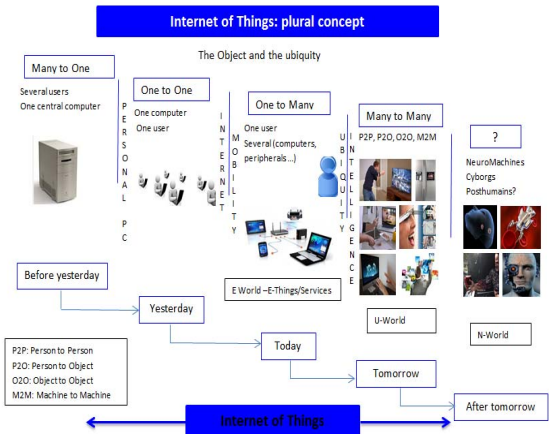

Fig. 2. Internet of Things: Plural Concept [10]

III. USE CASE OF COMAN (MANAGEMENT OF COSTRAINED NETWORK AND DEVICES)

The characteristics of network management is monitoring network status, setting network parameters, detecting faults and their causes, and maintain normal operation of network, to improve network efficiency and application performance. However, constrained devices, might be unreliable, have limited power, and low transmission range. Compared to the management of traditional IP network, the management of a network with constrained devices offers different challenges [11]. In this section we discussed some use cases for the management of a constrained network [11]:

a. Environmental Monitoring

The characteristic of the environmental monitoring is the use of a number of sensors, which are not protected against falsification and used to monitor the movements and habits of wildlife, emissions, and qualities water. Other use is focused on climate change, earthquakes, systems preventions tsunami... [11]. Concerning the management of applications environmental monitoring, it stays relating the operation of the devices, or in the case of breakdowns or destruction, it must be replaced by a new constrained device, which re-enters the management of these applications, these devices were forced to be self-configurable, taking into account the loss of neighbors, or change the places where they apply [11].

b. Medical Applications

For medical applications, the constrained devices remains an enabling technology very advanced, which are used for emergency notification systems and remote health monitoring, from simple applications such as blood pressure and monitors heart rate, has advanced features, which may use technologies implemented, such as advanced hearing aids and pacemakers. The management of these devices constrain used for medical applications, is done by the organization that offers medical services and employing specially trained person to control these devices, or users of these devices, which requires that the management should be easy installed and configured by them, or it is done in a manner automatic [11].

c. Infrastructure Monitoring

Infrastructure monitoring aims detect any changes or events that could affect the safety these infrastructures. It includes several infrastructures such as bridges, windmills, railway tracks, as it allows defining a cost effective manner, planning of repair and maintenance activities. The network uses the monitoring infrastructure is based on a combination of fixed and wireless technologies, since its use could be in near or difficult to access areas[11].

d. Automated Metering Infrastructure (AMI)

The AMI network uses an electric utility, allowing recovering the data of uses of each electricity meter, and receive immediate notifications in case of power failure. Furthermore, AMI networks could communicate distribution devices and automation such as circuit breakers and transformers, if their use was designed to be extensible and open [11].

IV. COMAN CANDIDATE TECHNOLOGIES

On this section we identify some candidate technologies for use cases and requirements COMAN. The goal of this section is to identify what has been done, and what still needs to be done, and give a clear view of the scope and work in COMAN [12]:

	Description	Some overlap with COMAN requirements
OMA-LwM2M	OMA Open Mobile Alliance Lightweight M2M enables the management of M2M services through the protocol that it provides placed in resources constrain devices	-Authentication on management system and devices - Energy status monitoring - Access control on management system and devices
OMA-DM	OMA Device Management [OMA-DM] provides various functions for mobile device management. OMA-DM specifies and depends heavily on the SyncML language. The typical underlying transport protocol is HTTP. This makes OMA-DM in unaltered form infeasible for constrained devices.	-Support multiple device classes within a single network -Compact encoding of management data
CoAP	Constrained Application Protocol is an application protocol layer, designed to constrain devices	- Capability discovery - Group-based provisioning - Support for lossy links and unreachable devices - Support of energy-optimized communication protocols
SNMP	The Simple Network Management Protocol is the most widely used protocol for managing networks seen its simplicity, it allows the monitoring and management of different network entities.	- Multiple device classes - Management scalability - Protocol Extensibility - Notifications - Authentication of management system and devices - Access control on management system and devices
BACnet	BACnet protocol has been maintained by the organization ASHRAE (American Society of Heating, Refrigeration and Air-Conditioning Engineers). BACnet allows a specified control system, a number of object on which they are composed	- Management scalability - Distributed Management - Hierarchical management - Protocol extensibility - Self-configuration capability

V. MANAGEMENT PROTOCOL

More the network becomes huge, more management becomes difficult, and since the IoT is interested have a huge number of connected devices. Therefore its necessity to have a management networks is important, to provide good quality service to the end customer, and make it more reactive network face to change. Network management includes a set of means implemented, such as techniques, knowledge, and tools that allows network administration and supervision, order to: monitor the systems, retrieve information, perform operations control and configuration management, and especially treatment of operational problems on the network such as: the maintenance, technical assistance...
In our case we will treat some protocols that enable management [6].

A. LNMP

LNMP LoWPAN Network Management Protocol is management architecture for 6LoWPAN networks. To increase the lifetime of the network, LNMP architecture focuses on reducing the cost of communication. One of the objectives of LNMP is interoperability with SNMP. However, SNMP was considered quite large both in terms of communication and complexity for devices has limited resources [13]. LNMP comprises two architectures: an operational architecture and informational architecture that we describe in what follows [14]:

1. Operational architecture:

In this architecture is the 6LoWPAN entity that performs management operations. First, and before performing the task of management must be a network discovery, through which performs the collection and detection devices, after this discovery comes the stage management device available [14].

1.1 Network Discovery:

The requirements of WSN focus in their use in a constrained environment, which makes them very difficult to manage, and discover the devices manually remain an almost impossible function, hence the need to develop an automated procedure that allows the monitoring of network status [14].
The operational architecture distributes the tasks between the 6LoWPAN that performs the task of discovering the network monitored his status, and the coordinators that allow discovering the devices; the goal of this distribution task is to reduce the cost of communication, because for sensor networks, bandwidth is an important element [14].

a. End devices

When the coordinator wants to check the status of the device, the devices takes care of sending state in a periodic manner [14].

b. Coordinators

The coordinator for its part, it keeps the information of the state of devices, it is composed of two tables, the first contains a list of devices notification, and the second contains a list of status of all devices, these two tables is filled to the phase of initiation network [14].
During operation if a new device is associated with the coordinator, an entry will be added to both tables, and even in the absence of a device, the coordinator stops receiving status information of the devices, when they send a request, and if it does not receive a response on the other hand, then the coordinator deletes the devices from its list of table and then performs the update [14].

c. Bridge

For filtering state information that receives the coordinator, this is the bridge that takes care. This gateway allows filling the status table, in database management information (MIB) that the SNMP protocol makes available in the form of IP address. With the network management station (NMS), this allows obtaining the available nodes on the network. The information contained in the gateways can be treated, while the network latency and the reporting interval allow defining the accuracy of the data [14].

1.2 Monitoring device

Within 6LoWPAN, it is preferable to use the SNMP protocol, with queries of device status monitoring, given its simplicity. But the constraint is that the SNMP protocol is quite cumbersome for 6LoWPAN networks in terms of complexity and communication. But the purpose of 6LoWPAN is to reuse existing protocols [14]. The work proposed by [14] is that SNMP will be used on the IPv6 side only; in this case the gateway acts as a proxy between SNMP and the local management framework. For packets, they use a simplified format to and from SNMP on a 6LoWPAN gateway. SNMP requests are converted to UDP request, containing object identifiers, also when the gateway receives the responses; they are converted into SNMP format [14].

2. The information architecture

As already mentioned, the 6LoWPAN tries to reuse existing protocols such as SNMP, it is also important to support the database of management information (MIB). The purpose is to define for each base layer data management, taking into account the constraints on the availability of bandwidth and sensor nodes to optimize the 6LoWPANs [14].

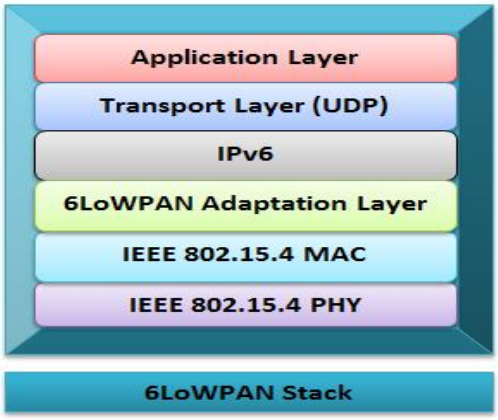

Fig 3. 6LoWPAN Stack Architecture [14]

a. PHY and MAC layer

➢ 6LoWPAN Physical Layer

The 6LoWPAN PHY layer provides two services: the PHY data service, which provides across the physical radio channel, transmission and reception of data packets between MAC and PHY, and the PHY management service interfacing to the physical layer management entity (PLME), which maintains a database of information on related personal area networks and offers access to every layer management function [15].

➢ 6LoWPAN Data Link Layer

The 6LoWPAN Data Link Layer, which is the MAC sub-layer, provides two services: the MAC data service that allows letting the transmission and receiving of MAC protocol data units (MPDU) across the PHY data service, and the MAC management service interfacing to the MAC sub-layer management entity (MLME) [15].

b. 6LoWPAN: Adaptation Layer

The main component of 6LoWPAN is the adaptation layer. For adaptation layer, the first major function is TCP/IP header compression. With this compression, 802.015.4 can transmit a payload effectively.
IEEE 802.15.4 has a maximum frame size of 128 bytes, while IPv6 requires a maximum transmission unit (MTU) of 1280 bytes. For this, the adaptation layer allows both fragmentation and reassembling.
Other functions of the adaptation layer are routing, neighbor discovery and multicast support [16].

c. Network layer

The network layer has like main considerations, addressing, routing and mapping protocols. This layer provides to sensor nodes, internetworking capability.
On one hand, the 6LoWPAN adaptation layer allows mesh-under routing decision; on the other hand, 6LoWPAN network layer allows route-over routing decision [15].

B. SNMP

SNMP (Simple Network Management Protocol) is a protocol designed to manage and control connected to the IP network devices. SNMP can be applied to various devices: routers, switches, workstations, servers, etc. It was standardized by the IETF (Internet Engineering Task Force) and is composed of a set of norm: a database schema, an application protocol layer, and a set of data objects [17]. SNMP enables communication between two entities, this is a protocol application level; it relies on:

- UDP for transport of their packages via 2 standard ports 161 for orders and 162 traps
- ASN.1 (Abstract Syntax Notation One) [18].

1. Architecture SNMP

The architecture of the SNMP protocol consist entities following [19] :

- Management stations NMS (Network Management Station)
- Agents
- MIBs (management information base)

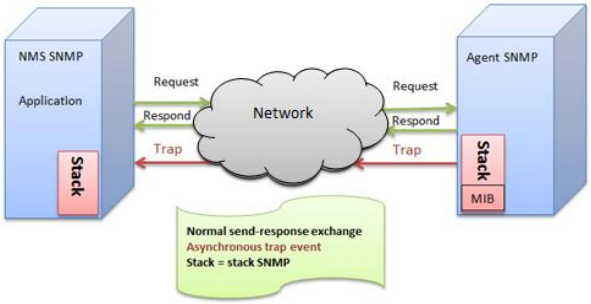

Fig. 4. SNMP Architecture: Information Exchange between NMS and MIB via network [19]

1.1. Agent

The architecture of SNMP defines an Agent as the active element management system. SNMP agent allows the NMS management station to administer a network component, responding to its requests, and can also send unsolicited messages asynchronously; agent contains a simple database MIB which in turn contains data network components [19].

1.2. Manager (NMS)

NMS is the SNMP management station which can receive unsolicited messages (trap) sent by the agent, it can also read and write values retained by agent in its MIB [19].

1.3. Management Information Base (MIB)

A MIB is a database which contains information collected and organized a hierarchical manner, and through SNMP we can access it, it comprises a set of objects characterized that all of them the given terminal. MIB defined a set of concept: naming, type, size of the given object, it is a data-oriented specification [18].

2. Adapting SNMP for IPv6

Our objective was to make network management using IoT and adapt them with the new version of Internet Protocol that is IPv6, thereby the SNMP protocol which is widely used for the network management given its simplicity, it too was adapted to operate with IPv6. In conducting its architecture does not depend on IP since it is at the application layer, its evolution to IPv6 does not impose major problem. One of the most responded SNMP implementations for IPv6 is the NET-SNMP [20]. NET-SNMP formerly UCD-SNMP is maintained by the American University ''University of California Davis (UCD)''. Previously it has been developed by the American College Carnegie Mellon University (CMU) [21].
NET- SNMP is a suite of application that uses both IPv4 and IPv6, this suite includes:

- Command-line applications to [22]:
  - Retrieve information from an SNMP-capable device, either using single requests (snmpget, snmpgetnext), or multiple requests (snmpwalk, snmptable, snmpdelta).
  - Manipulate configuration information on an SNMP-capable device (snmpset).
  - Retrieve a fixed collection of information from an SNMP-capable device (snmpdf, snmpnetstat, snmpstatus).
  - Convert between numerical and textual forms of MIB OIDs, and display MIB content and structure (snmptranslate).
- A graphical MIB browser (tkmib), using Tk/perl.
- A daemon application for receiving SNMP notifications (snmptrapd).
- An extensible agent for responding to SNMP queries for management information (snmpd).
- A library for developing new SNMP applications, with both C and perl APIs

NET-SNMP can be applied on different operating systems such as Linux (kernels 2.4 to 1.3), NetBSD (1.5alpha 1.0), Solaris (2.8 to 2.3), Win32 ... [21]

VI. DISCUSSION

In this paper, our work has as objective, to analyze different research focuses on the concept of IoT, this analysis allowed us give approach and simplify study of IoT concept from the point of view use, implementation, and requirements.
All first, after giving a general idea of the IoT, taking into account the definition, estimates of future [1] [2], we focused on the implementation of the new protocol on IoT Internet is IPv6 [3], and the adaptation of different types of networks such as WSN and LoWPAN on where IoT is based, with IPv6, this adaptation protocol had the advantage of allowing an unknown number of device to connect to the Internet, also enjoy the advantage of IPv6, taking into account mobility, reliability, manageability and security, which is confirmed by [3] [4] [5] [6]. Also we drew attention to the concept of network management and device constraints, thanks to COMAN, as well we talked about the different problems of networks and devices constraints, and we presented use cases of this type of networks and devices and which allows to make our lives easier and safer and that is what is was confirmed by [7] [11]. Then we put the focus on the candidate technologies for requirements and use cases COMAN as OMA-LwM2M, OMA-DM, CoAP, SNMP, and BACnet. The goal is to identify the work that has been done and continues to do in COMAN, which was mentioned in [12]. But finally we focus on management protocols such as LNMP and SNMP, their convenience to the needs of the IoT, and their integration in the structure of IPv6 [14] [18] [19] [20] [21] for the protocol LNMP has the advantage of giving efficiency and reducing load on the network, so it can increase the life of the network by reducing the cost of communication. The LNMP aims to have interoperability with SNMP. This is seen both in terms of communication and complexity as large enough for a resource limited devices [13]. For SNMP, it is designed for the management and control of devices connected to the IP network, the main quality of this protocol is its simplicity and ease of deployment, as it applies to various device such as routers, the switch etc.. And this is what has been confirmed in [9].

VII. CONCLUSION

In this article, we presented the Internet of Things as a technology that will change our daily lives, as is interested in combining all areas of life, to ease their use and development that meets all the needs of these users. But before going into details, we made a simple definition for Internet of Things. So we gave a detailed view of WSNs in which, based the IoT, we also presented solutions for the implementation of WSN with the IP protocol. Also we introduced the 6LoWPAN solution, which is a solution for sensor networks with low power to connect via the Internet.
As IoT tends to connect all devices to the Internet, it also takes into account the networks and devices constrain, and their management, and that is what we presented with COMAN (Management of Constrained Networks and Devices) through which we have recognized the type of network and use cases Constrain networks and devices. View network complexity of the IoT, which is increasing day by day, taking into account

the devices connected to the Internet, their management becomes an essential need, for it we studied two management protocol, which are LNMP and SNMP, which will allow ease of deployment and a more comfortable use for the end user with the best quality service.

REFERENCES

[1] Pierre-Marie Mateo, '' L'Europe et surtout la France, prêtes à se saisir du potentiel de l'internet des objets ?'',(online) Atelier 27 November 2013, consulted 15 January 2014, 1p. Available on the Internet : http://www.atelier.net/trends/articles/europe-surtout-france-pretes-se-saisir-potentiel-de-internet-objets_425725

[2] Jara, A. J., Ladid, L., Skarmeta, A. The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol. 4, No. 3, pp. 97-118, September 2013

[3] Antonio J. Jara, David Fernandez, Pablo Lopez, Miguel A. Zamora and Antonio F. Skarmeta " Lightweight MIPv6 with IPSec support ,A mobility protocol for enabling transparent IPv6 mobility in the Internet of Things with support to the security, "

[4] Aurélien Jacquot, ''Supervision de réseaux d'objets intelligents communicants sans fil'', No d'Ordre : 2019, EDSPIC : 477

[5] Fabricio A. Silva, Linnyer B. Ruiz, Thais R. M. Braga, José Marcos S. Nogueira, and Antonio A. F. Loureiro, ''Defining a Wireless Sensor Network Management Protocol''

[6] NGUYEN Manh Tuong, Victor MORARU '' Les protocoles pour la gestion des réseaux Informatiques'' Institut de la Francophonie pour l'Informatique.

[7] M. Ersue, Ed, D. Romascanu, J. Schoenwaelder, Management of Networks with Constrained Devices: Problem Statement and Requirements draft-ersue-opsawg-coman-probstate-reqs-00, (online) Internet Engineering Task Force 25 Octobre 2013, consulted 3 December 2013, 56p. Available on the Internet: http://tools.ietf.org/html/draft-ersue-opsawg-coman-probstate-reqs-00#page-5

[8] Benoît PONSARD (Fondateur de Kimeggi) , '' LE « MACHINE TO MACHINE », PREMIER PAS VERS L'INTERNET DES OBJETS'', FLUX No 269 – MARS-AVRIL 2012

[9] Pierre-Jean Benghozi, Sylvain Bureau, Françoise Massit-Folléa '' L'Internet des Objets : Quels enjeux pour les Européens ?''

[10] Marie-George Clouet, ''Internet des Objets : Definition et Premiere Approche'',(online) Graphemeride 20 novembre 2013, consulted 15 January 2014, 1p. Available on the Internet: http://www.graphemeride.com/blog/internet-des-objets-definition-et-premiere-approche#.UsqrB9J5Me

[11] M. Ersue, Ed, D. Romascanu, J. Schoenwaelder, Management of Networks with Constrained Devices: Use Cases draft-ersue-opsawg-coman-use-cases-00, (online) Internet Engineering Task Force 25 Octobre 2013, consulted 3 December 2013, 33p. Available on the Internet: http://www.ietf.org/id/draft-ersue-opsawg-coman-use-cases-00.txt

[12] B. Greevenbosch, K. Li, P. van der Stok, Candidate Technologies for COMAN draft-greevenbosch-coman-candidate-tech-03, (online) Internet Engineering Task Force 3 july 2013, consulted 6 December 2013, 26p. Available on the Internet: http://tools.ietfs.org/html/draft-greevenbosch-coman-candidate-tech-03

[13] Siarhei Kuryla, ''Implementation and Evaluation of the Simple Network Management Protocol over IEEE 802.15.4 Radios under the Contiki Operating System'', 52p, Master of Science in Smart Systems, School of Engineering and Science Jacobs University Bremen gGmbH, July 22nd, 2010.

[14] Hamid Mukhtar, Kim Kang-Myo, Shafique Ahmad Chaudhry, Ali Hammad "LNMP- Management Architecture for IPv6 based lowpower Wireless Personal Area Networks (6LoWPAN)"

[15] Nurul Halimatul Asmak Ismail , Rosilah Hassan, Khadijah W. M. Ghazali, '' A Study on Protocol Stack in 6LoWPAN Model'', Journal of Theoretical and Applied Information Technology, Vol. 41, No.2 , 10p 31st July 2012.

[16] ''6LoWPAN Technical Overview'', Mindteck 17p. Available on the Internet: http://ms11.voip.edu.tw/~jryan/ref/6LoWPAN%20Technical%20Overview.pdf

[17] ''Simple Network Management Protocol'' , (online) Dbpedia, consulted 2 January 2014, 1p. Available on the Internet: http://fr.dbpedia.org/page/Simple_Network_Management_Protocol

[18] ''SNMP: *Simple Network Management Protocol''*, 72p. Available on the Internet: http://deptinfo.cnam.fr/new/spip.php?pdoc6723

[19] Fabien Reichenbach, ''Service SNMP de détection de faute pour des systèmes répartis'', Laboratoire de Systèmes Répartis, Ecole Polytechnique Fédérale de Lausanne EPFL Fbruary 2002, 66p. Available on the Internet: http://infoscience.epfl.ch/record/49953/files/Rei02.pdf

[20] ''La supervision des réseaux IPv6'' http://www.renater.fr/IMG/pdf/recommendations_supervision_IPv6.pdf

[21] Blaise LUSIKILA LUAMBASU, ''Chapitre3 : Mise en Œuvre de Net-snmp sous linux'', (online) memoireonline 2007, consulted 23 december 2013, Available on the Internet : http://www.memoireonline.com/05/09/2078/m_Conception-Implementation-dune-Base-de-Donnees-pour-la-Gestion-dun-Organisme-et-Administration13.html

[22] (online) net-snmp Last modified: Tuesday, 26-Feb-2013, consulted 17 december 2013, 1p. Available on the Internet : http://www.net-snmp.org/