Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 10, 2013

M. Ersue, Ed.
Nokia Siemens Networks
D. Romascanu, Ed.
Avaya
J. Schoenwaelder, Ed.
Jacobs University Bremen

July 9, 2012

Management of Networks of Constrained Devices: Use Cases and Requirements
draft-ersue-constrained-mgmt-00

Abstract

This document raises the questions on and discusses the use cases, requirements and the solutions required for the management of a network with constrained devices.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 10, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

1.1. Overview

Constrained networks usually consist of many small and low-power nodes, so called constrained devices (aka. sensor, smart object or M2M device), and one or more entities between the constrained devices and the Internet, which can act as a gateway or proxy. Constrained devices might be in charge of gathering information in diverse settings including natural ecosystems, buildings, and factories and send the information to one or more server stations. Constrained devices may work under severe resource constraints such as limited battery and computing power, little memory and insufficient wireless bandwidth, and communication capabilities. A central entity, e.g., a base station or controlling server, might have more computational and communication resources, which acts as a gateway between the constrained devices and the application logic in the core network.

Today diverse size of small devices with different resources and capabilities are becoming connected. Mobile personal gadgets, building-automation devices, cellular phones, M2M devices, and so on benefit from interacting with other "things" in the near or somewhere in the Internet. With this The Internet of Things becomes a reality build up of uniquely identifiable objects (things). And over the next decade, this could grow to trillions of constrained devices and will greatly increase the Internet's size and scope.

Network management is characterized by monitoring network status, detecting faults and inferring their causes, setting network parameters, and carrying out actions to remove faults and improve the performance. The traditional network management application periodically collects information from a set of elements that are needed to be managed, processes the data, and presents them to the network management users. Constrained devices, however, often have limited power, low transmission range, and might be unreliable. They might also need to work in hostile environments for long periods of time unsupervised. Due to such constraints, the management of a network with constrained devices offers different types of challenges compared to the management of a traditional IP network.

The IETF has already done a lot of standardization work to enable the communication in IP networks and to manage such networks as well as the manifold type of nodes in these networks [RFC6632]. However, the IETF so far has not developed any specific technologies for the management of constrained devices and the networks comprised by constrained devices. IP-based sensors or constrained devices in such an environment, i.e., devices with very limited memory and CPU resources, use today application-layer protocols in an ad-hoc manner

to do simple resource management and monitoring.

This document raises the questions on and aims to understand the use cases, requirements and the required solutions for the management of a network with constrained devices. Section 1.3 describes different options for the connectivity and management of constrained devices. Section 1.4 explains the classes with which constrained devices can be categorized. Section 2 aims to provide a problem statement on the issue of the management of networked constrained devices. Section 3 lists diverse use cases and scenarios for constrained management from the network as well as from the application point of view. Section 4 lists requirements on constrained networking and on management applications with constrained devices for discussion.

1.2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The following terms are used throughout this documentation:

Constrained Device: A device with resource constraints, e.g., limited amount of memory, limited processing capabilities, limited energy supply.

Constrained Network: A network constrained in resources, e.g., bandwidth, latency or data rate.

Network of Constrained Devices: A network to which constrained devices are connected. It may or may not be a Constrained Network.

Client: The originating endpoint of a request; the destination endpoint of a response.

Server: The destination endpoint of a request; the originating endpoint of a response.

1.3. Networks of Constrained Devices

We differentiate following options for the networking and management of networks of constrained devices:

Network topology options:

- a network of constrained devices which communicate with each other,

- Constrained devices which are connected directly to the Internet or a bigger IP network

- A network of constrained devices which communicate with a gateway or proxy with more communication capabilities

- Constrained devices which are connected to the Internet or a bigger IP network via the gateway/proxy

- A hierarchy of constrained devices, e.g., a network of C0 devices connected to one or more C1 devices - connected to one or more C2 devices - connected to one or more gateways - connected to some application servers or NMS system

- The possibility of device grouping (possibly in a dynamic manner) such as that the grouped devices can act as one logical device at the edge of the network and one device in this group can act as the managing entity

Management topology options:

- A network of constrained devices managed by one central manager. A logically centralized management might be implemented in a hierarchical fashion for scalability and robustness reasons. The manager and the management application logic might have a gateway/proxy in between or might be on different nodes in different networks, e.g., management application running on a cloud server.

- Distributed management, where a constrained network is managed by more than one manager. Each manager controls a subnetwork and may communicate directly with other manager stations in a cooperative fashion. The distributed management may be weakly distributed, where functions are broken down and assigned to managers dynamically, or strongly distributed, where almost all managed things have embedded management functionality and explicit management disappears, which usually comes with the price that the strongly distributed management logic now needs to be managed.

- Hierarchical management, where a hierarchy of constrained networks are managed by the managers at their corresponding hierarchy level. I.e. each manager is responsible for managing the nodes in its sub-network. It passes information from its sub-network to its higher-level manager, and also disseminates management functions received from the higher-level manager to its sub-network. Hierarchical management is essentially a scalability mechanism, logically the decision making may be still centralized.

1.4. Constrained Device Classes

To organize the discussion, it is often useful to have some succinct terminology for different classes of constrained devices. Following [I-D.ietf-lwig-guidance], we distinguish the following classes:

Name	data size (e.g., RAM)	code size (e.g., Flash)
Class 0	<< 10 KiB	<< 100 KiB
Class 1	~ 10 KiB	~ 100 KiB
Class 2	~ 50 KiB	~ 250 KiB

Table 1: Classes of Constrained Devices

Class-0 (C0) devices are very constrained sensor-like motes. They will most likely not have the possibility to have a direct communications with the Internet in a secure manner. These class-0 devices will participate in Internet communications with the help of larger devices acting as proxy or gateways. It is assumed that C0 devices cannot be managed comprehensively in the traditional sense. They will be most likely preconfigured and if ever will be reconfigured rarely with a very small data set. At most they could answer keep-alive signals and send on/off or basic health indications.

Class-1 (C1) devices cannot easily talk to other Internet nodes with a full protocol stack using HTTP, TLS and related security protocols, and XML-based data representations. However, they have enough power to use a reduced or lightweight protocol stack (e.g., with CoAP over UDP) and participate in meaningful conversations without the help of a gateway node. So they can be integrated into an IP network in one way or the other but need to spare with memory for the protocol and application usage.

Class-2 (C2) can support mostly the same protocol stack as used on notebooks or servers. However, even these devices can benefit from lightweight and energy-efficient protocols and consuming less bandwidth on air. Furthermore, using less network resources would leave more resources available to applications. As such using the same protocol stack on Class 1 and 2 devices might reduce development costs and increase the interoperability.

For C1 devices it is indeed important to understand what type of applications they could run and which management mechanisms would be

most suitable. Even though they have some more functionality available, C2 devices need to be assessed for the type of applications they will be running and the management they would need. To be able to derive the requirements, the uses cases and the involvement of the devices in the management scenario need to be analyzed. The use cases where C1 or C2 devices build a cluster or are part of a hierarchy as well as the assumed degree of automation might be essentially important.

C1 and C2 devices are typically driven by 8-bit or 16-bit processors and they have in common that they are severely constrained by the amount of memory they can use. There are, however, also a number of devices that can afford to have 32-bit processors and memory sizes counted in MiB instead of KiB. While such devices are easily capable to run a complete IP protocol stack, they still can be constrained by a limited energy supply. We will call this class of devices power constrained devices.

2. Problem Statement

The terminology for the "Internet of Things" (IoT) is still nascent, and depending on the network type or layer in focus diverse technologies and terms are in use. Common to all these considerations is the "Things" or "Objects" are supposed to have physical or virtual identities using interfaces to communicate. In this context, we need to differentiate between the Constrained or Smart Devices identified by an IP address and virtual entities such as Smart Objects, which can be identified as a resource or a virtual object by using a unique identifier. Furthermore, the smart devices usually have a limited memory and CPU power as well as aim to be self-configuring and easy to deploy.

However, the tininess of the network nodes requires a rethinking of the protocol characteristics concerning power consumption, performance, memory, and CPU usage. As such, there is a demand for protocol simplification, energy-efficient communication, less CPU usage and small memory footprint.

On the application layer the IETF is already developing protocols like the Constrained Application Protocol (CoAP) [I-D.ietf-core-coap] supporting constrained devices and networks e.g., for smart energy applications or home automation environments. The deployment of such an environment involves in fact many, in some cases up to million smart meters or small devices, which produce a huge amount of data. This data needs to be collected, filtered, and pre-processed for further use in diverse services.

Considering the high number of nodes to deploy, one has to think on manageability aspects of the smart devices and plan for easy deployment, configuration and management. As a consequence, seamless monitoring and self-configuration of such network nodes becomes more and more imperative. Self-configuration and self-management is already a reality in the standards of some of the bodies such as 3GPP. To introduce self-configuration of smart devices successfully a device-initiated connection establishment might be useful.

A simple application layer protocol, such as CoAP, is essential to address the issue of efficient object-to-object communication and information exchange. Such an information exchange should be done based on interoperable data models to enable the exchange and interpretation of diverse application and management related data.

In an ideal world, we would have only one network management protocol for monitoring, configuration, and exchanging management data, independently of the type of network (e.g., Smart Grid, wireless access or core network). Furthermore, it would be also desirable to

derive the basic data models for constrained devices from the core model we use today to enable reuse of functionality and end-to-end information exchange. However, the current management protocols seem to be too heavyweight compared to the capabilities the constrained devices have and are not applicable directly for the use in a network of constrained devices. Furthermore, the data models addressing the requirements of such smart devices need yet to be designed.

The IETF so far has not developed any specific technologies for the management of constrained devices and the networks comprised by constrained devices. IP-based sensors or constrained devices in such an environment, i.e., devices with very limited memory and CPU resources, use today, e.g., application-layer protocols to do simple resource management and monitoring. This might be sufficient for some basic cases, however, there is a need to reconsider the network management mechanisms based on the new, changed as well as reduced requirements coming from smart devices and the network of such constrained devices. Albeit it is questionable whether we can take the same comprehensive approach we use in an IP network also for the management of constrained devices. Hence the management of a network with constrained devices might become necessary to design as much as possible simplified and less complex.

3. Use Cases

This section discusses some application scenarios where networks of constrained devices are expected to be deployed. For each application scenario, we first briefly describe the characteristics followed by a discussion how network management can be provided, who is likely going to be responsible for it, and on which time scale management operations are likely carried out.

3.1. Environmental Monitoring

Environmental monitoring applications are characterized by the deployment of a number of sensors to monitor emissions, water quality, or even the movements and habits of wildlife. Other applications in this category include earth quake or tsunami early-warning systems. The sensors often span a large geographic area, they can be mobile, and they are often difficult to replace. Furthermore, the sensors are usually not protected against tampering.

Management of environmental monitoring applications is largely concerned with the monitoring whether the system is still functional and the roll-out of new constrained devices in case the system looses too much of its structure. The constrained devices themselves need to be able to establish connectivity (auto-configuration) and they need to be able to deal with events such as loosing neighbors or being moved to other locations.

Management responsibility typically rests with the organization running the environmental monitoring application. Since these monitoring application must be designed to tolerate a number of failures, the time scale for detecting and recording failures is for some of these applications likely measured in hours and repairs might easily take days. However, for certain environmental monitoring applications, much tighter time scales may exist and might be enforced by regulations (e.g., monitoring of nuclear radiation).

3.2. Medical Applications

Constrained devices can be seen as an enabling technology for advanced health monitoring and emergency notification systems, ranging from blood pressure and heart rate monitors to advanced devices capable to monitor implanted technologies, such as pacemakers or advanced hearing aids. Medical sensors may not only be attached to human bodies, they might also exist in the infrastructure used by humans such as bathrooms or kitchens. Medical applications will also be used to ensure treatments are being applied properly and they might guide people losing orientation.

Constrained devices that are part of medical applications are either managed by the users of those devices or by an organization providing medical (monitoring) services for physicians. In the first case, management must be automatic and or easy to install and setup by average people. In the second case, it can be expected that devices are controlled by specially trained people. In both cases, however, it is crucial to protect the privacy of the people to which medical devices are attached. Even though the data collected by a heart beat monitor might be protected, the pure fact that someone carries such a device may need protection. As such, certain medical appliances may not want to participate in discovery and self-configuration protocols in order to remain invisible.

Many medical devices are likely used (and relied upon) to provide data to physicians in critical situations since the biggest market is likely elderly and handicapped people. As such, fault detection of the communication network or the constrained devices becomes a crucial function that must be carried out with high reliability and, depending on the medical appliance and its application, within seconds.

3.3. Industrial Applications

Industrial Applications and smart manufacturing refer to not only production equipment, but also to a factory that carries out centralized control of energy, HVAC (heating, ventilation, and air conditioning), lighting, access control, and so on via a network. For the management of a factory it is becoming essential to implement smart capabilities. From an engineering standpoint, industrial applications are intelligent systems enabling rapid manufacturing of new products, dynamic response to product demand, and real-time optimization of manufacturing production and supply chain networks. Potential industrial applications e.g. for smart factories and smart manufacturing are:

- Digital control systems with embedded, automated process controls, operator tools, and service information systems optimizing plant operations and safety.

- Asset management using predictive maintenance tools, statistical evaluation, and measurements maximizing plant reliability.

- Smart sensors detecting anomalies to avoid abnormal or catastrophic events.

- Smart systems integrated within the industrial energy management system and externally with the smart grid enabling real-time energy optimization.

Sensor networks are an essential technology used for smart manufacturing. Measurements, automated controls, plant optimization, health and safety management, and other functions are be provided by large numbers of networked sectors. Data interoperability and seamless exchange of product, process, and project data is being enabled through interoperable data systems used by collaborating divisions or business systems. Intelligent automation and learning systems are vital to smart manufacturing but must be effectively integrated with the decision environment. Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. Inaccessible locations, rotating machinery, hazardous areas, and mobile assets can be reached with wireless sensors. WSNs can provide today wireless link reliability, real-time capabilities, and quality-of-service and enable industrial and related wireless sense and control applications.

Management of industrial and factory applications is largely focused on the monitoring whether the system is still functional, real-time continuous performance monitoring and optimization as necessary. The factory network might be part of a campus network or connected to the Internet. The constrained devices in such a network need to be able to establish configuration themselves (auto-configuration) and might need to deal with error conditions as much as possible locally. Access control has to be provided with multi-level administrative access and security. Support and diagnostics can be provided through remote monitoring access centralized outside of the factory.

Management responsibility is typically owned by the organization running the industrial application. Since the monitoring applications must handle a potentially large number of failures, the time scale for detecting and recording failures is for some of these applications likely measured in minutes. However, for certain industrial applications, much tighter time scales may exist, e.g. in real-time, which might be enforced by the manufacturing process or the use of critical material.

3.4. Home Automation

Home automation includes the control of lighting, heating, ventilation, air conditioning, appliances, and entertainment devices to improve convenience, comfort, energy efficiency and security. It can be seen as a residential extension of building automation.

Home automation networks need a certain amount of configuration (associating switches or sensors to actors) that is either provided by electricians deploying home automation solutions or done by residents by using the application user interface to configure (parts

of) the home automation solution. Similarly, failures may be reported via suitable interfaces to residents or they might be recorded and made available to electricians in charge of the maintenance of the home automation infrastructure.

The management responsibility lies either with the residents or it may be outsourced to electricians providing management of home automation solutions as a service. The time scale for failure detection and resolution is in many cases likely counted in hours to days.

3.5. Building Automation

Building automation comprises the distributed systems designed and deployed to monitor and control the mechanical, electrical and electronic systems inside buildings with various destinations (e.g., public and private, industrial, institutions, or residential). Advanced Building Automation Systems (BAS) may be deployed concentrating the various functions of safety, environmental control, occupancy, security. In some cases the deployment of the various functional systems may be made atop of the same communication infrastructure, which may involve wired or wireless communications networks inside the building.

Building automation requires the deployment of a large number of sensors that monitor the status of devices, and parameters inside the building and controllers with different specialized functionality for areas with or the totality of the building. Examples of functions performed by such controllers are the regulating the quality, humidity and temperature of the air inside the building and lighting. Other systems may report the status of the machinery inside the building like elevators, or inside the rooms like projectors in meeting rooms. Security cameras and sensors may be deployed and operated on the same or on separate dedicated infrastructures. The deployment area of a BAS is typically inside one building (or part of it) or several buildings geographically grouped in a campus.

Some of the sensors in Building Automation Systems (for example fire alarms or security systems) register, record and transfer critical alarms information and must to be resilient to events like loss of power or security attacks. This leads to the need that some components and subsystems operate in constrained conditions. Also in some environments the malfunctioning of a control system (like temperature control) needs to be reported in the shortest possible time. Complex control systems can misbehave, and their critical status reporting and safety algorithms need to be basic and robust and perform even in critical conditions.

3.6. Energy Management

[I-D.ietf-eman-framework] defines a framework for providing Energy Management for devices within or connected to communication networks. This document observes that one of the challenges of energy management is that a power distribution network is responsible for the supply of energy to various devices and components, while a separate communication network is typically used to monitor and control the power distribution network. Devices that have energy management capability are defined as Energy Devices and identified components within a device (Energy Device Components) can be monitored for parameters like Power, Energy, Demand and Power Quality. If a device contains batteries, they can be also monitored and managed.

Energy devices differ in complexity and may include basic sensors or switches, specialized electrical meters, or power distribution units (PDU), and also subsystems inside network devices (routers, network switches) or home or industrial appliances. An Energy Management System is a combination of hardware and software used to administer a network with the primary purpose being Energy Management. The operators of such systems are either the utility providers or customers that aim to control and reduce the energy consumption and the associated costs. The topologies differ and the radius of deployment can cover areas from small surfaces (individual homes) to large geographical areas.

A smart grid is an electrical grid that uses data networks to gather and act on information, in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. As such Smart Grid provides sustainable and reliable generation, transmission, distribution, storage and consumption of electrical energy based on advanced energy and ICT solutions and enables e.g. following specific application areas: Smart transmission systems, Blackout Prevention Systems, Advanced Metering Infrastructure (AMI), Advanced Distribution Management, Smart Substation Automation, Smart Metering, Demand Response/Load Management, Smart Home and Building Automation, E-mobility, etc.

Smart Metering is a good example for an M2M application and can be realized as one of the vertical applications in an M2M environment. Many different type of possibly wireless small meters produce all together a huge amount of data which is collected and processed by a central entity and an application server. The M2M infrastructure can be provided by a mobile network operator as the meters in urban areas will have most likely a cellular or WiMAX radio.

Smart Grid is a distributed and heterogeneous network and might have been built based on diverse networking technologies, such as wireless Access Technologies (WiMAX, Cellular, and Microwave), wireline and Internet Technologies (e.g., Ethernet, IP/MPLS, SDH/PDH over Fiber optic, and xDSL) as well as other technologies including ZigBee, Z-Wave, 6LoWPAN, Wi-Fi, PLC/BPL over power-line. The operational effectiveness of the smart grid is highly dependent on a robust, two-way, highly secure, and reliable communications network with suitable availability.

The management of a distributed system like smart grid requires an end-to-end management of and information exchange through different type of networks. However, as of today there is no integrated smart grid management approach nor a common smart grid information model available. Specific smart grid applications or network islands use their own management mechanisms. For example, the management of smart meters depends very much on the M2M service enablement or AMI environment they have been integrated to and the networking technologies they are using. In general smart meters do only need seldom reconfiguration and they send a small amount of redundant data to a central entity. For a discussion on management needs in Smart Home and Building Automation see Section 3.4 and Section 3.5.

3.7. Transport Applications

Transport application is a generic term for the integrated application of communications, control and information processing in a transportation system. Transport telematics or vehicle telematics are used as a term for the group of technologies that support transportation systems. Transport applications running on such a transportation system cover all modes of the transport and consider all elements of the transportation system, i.e. the vehicle, the infrastructure, and the driver or user, interacting together dynamically. The overall aim is to improve decision making, often in real time, by transport network controllers and other users, thereby improving the operation of the entire transport system. As such transport applications can be seen as one of the important M2M service scenarios with the involvement of manifold small devices.

The definition encompasses a broad array of techniques and approaches that may be achieved through stand-alone technological applications or as enhancements to other transportation communication schemes. Examples for transport applications are inter and intra vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistic and fleet management, vehicle control, and safety and road assistance.

As a distributed system transport systems require an end-to-end

management of and information exchange through different types of networks. It is likely that constrained devices in a network (e.g. a moving in-car network) have to be controlled by an application running on an application server in the network of a service provider. Such a network might be a wireless access network using diverse wireless technologies. As a result the management of constrained devices in the transport system might be necessary to plan top-down and might need to use data models obliged from and defined on the application layer.

Management responsibility typically rests within the organization running the transport application. The constrained devices in a moving transport network might be initially configured in a factory and a reconfiguration might be needed only rarely. New devices might be integrated in an ad-hoc manner based on self-management and -configuration capabilities. Monitoring and data exchange might be necessary to do via a gateway entity connected to the back-end transport infrastructure. The devices and entities in the transport infrastructure need to be monitored more frequently and can be able to communicate with a higher data rate. The connectivity of such entities does not necessarily have to be wireless. The time scale for detecting and recording failures in a moving transport network is likely measured in hours and repairs might easily take days. It is likely that a self-healing feature would be used locally.

3.8. **Infrastructure Monitoring**

Infrastructure monitoring is concerned with the monitoring of infrastructures such as bridges, railway tracks or (offshore) windmills. The primary goal is usually to detect any events or changes of the structural conditions that can impact the risk and safety of the infrastructure being monitored. Another secondary goal is to schedule repair and maintenance activities in a cost effective manner.

Management of infrastructure monitoring applications is primary concerned with the monitoring of the functioning of the system. Infrastructure monitoring devices are typically rolled out and installed by dedicated experts and changes are rare since the infrastructure itself changes rarely. However, monitoring devices are often deployed in unsupervised environments and hence special attention must be given to protecting the devices from being modified.

Management responsibility typically rests with the organization owning the infrastructure or responsible for its operation. The time scale for detecting and recording failures is likely measured in hours and repairs might easily take days. However, certain events

(e.g., natural disasters) may require that status information is obtained much more quickly and that replacements of failed sensors can be rolled out quickly (or redundant sensors be activated quickly).

4. Requirements per Device Class and Applications

The structure of this section is subject for discussion on the maillist.

4.1. Requirements Template

Following is the requirements template proposed to use.

Req-ID: An ID uniquely identified by a three-digit number

Title: The title of the requirement.

Requirement Type: Functional Requirements (FR), Non-Functional Requirements (NFR), Design Constraints (DC);

Description: The rational and description of the requirement.

Source: The origin of the requirement and the matching use case or application.

Device type: The device type(s) to which this requirement applies to.

Priority: The priority of the requirement showing the importance. Mandatory (M), Optional (O), Conditional (C).

4.2. Requirement Examples

Following are two examples for the use of the requirements template.

Req-ID: R-001

Title: Constrained devices must support auto-configuration capability.

Requirement Type: FR

Description: Auto-configuration or self-configuration is the automatic configuration and re-configuration of devices without manual intervention. Compared to the traditional management of devices where the management application is the central entity configuring the devices, in the auto-configuration scenario the device is the active part and initiates the configuration process. Auto-configuration in general simplifies the deployment, initial operation and the maintenance of the constrained devices and becomes indispensable if there are a huge number of devices to configure or a plug&play behavior is desired.

Source: Diverse use cases requiring easy deployment and plug&play behavior as well as easy maintenance of many constrained devices.

Device type: C1 and C2.

Priority: M

Req-ID: R-002

Title: The system must support secure network management access.

Requirement Type: FR

Description: Access control is a security feature provided by the management system allowing an administrator to restrict access to a subset of the management operations and data using various criteria. There is a need for standard mechanisms to restrict the access for particular users to a pre-configured subset of all available management operations and content. Usually a conceptual access control model is used to configure and monitor the access control procedures desired by the administrator to enforce a particular access control policy and authorization of the administrative users. It is unlikely that constrained devices would need multiple identities with different access control policies. Access privileges (access control rules) and the policy might be hard wired in a C1 device. It is assumed that C2 devices can provide a better granularity of the access control feature. However, access control needs to be defined modular to enable choosing between particular functionality and a lightweight implementation.

Source: Diverse use cases providing access to management operations and data on constrained devices.

Device type: C1 and C2.

Priority: M

5. IANA Considerations

This document does not introduce any new code-points or namespaces for registration with IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

6. Security Considerations

This document discusses the use cases and requirements on the network of constrained devices. If specific requirements for security will be identified, they will be described in future versions of this document.

7. Acknowledgments

The editors would like to thank participants on the maillist for their valuable contributions and comments.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[RFC6632] Ersue, M. and B. Claise, "An Overview of the IETF Network Management Standards", RFC 6632, June 2012.

[I-D.ietf-lwig-guidance]
Bormann, C., "Guidance for Light-Weight Implementations of the Internet Protocol Suite", draft-ietf-lwig-guidance-00 (work in progress), June 2012.

[I-D.ietf-core-coap]
Shelby, Z., Hartke, K., Bormann, C., and B. Frank, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-10 (work in progress), June 2012.

[I-D.ietf-eman-framework]
Claise, B., Parello, J., Silver, L., Quittek, J., and B. Nordman, "Energy Management Framework", draft-ietf-eman-framework-04 (work in progress), March 2012.

[I-D.ietf-eman-requirements]
Quittek, J., Winter, R., Dietz, T., Claise, B., and M. Chandramouli, "Requirements for Energy Management", draft-ietf-eman-requirements-07 (work in progress), July 2012.

Authors' Addresses

Mehmet Ersue (editor)
Nokia Siemens Networks

Email: mehmet.ersue@nsn.com

Dan Romascanu (editor)
Avaya

Email: dromasca@avaya.com

Juergen Schoenwaelder (editor)
Jacobs University Bremen

Email: j.schoenwaelder@jacobs-university.de