coman
Internet-Draft
Intended status: Informational
Expires: January 04, 2014

B. Greevenbosch
K. Li
Huawei Technologies
P. van der Stok
vanderstok consultancy

July 03, 2013

Candidate Technologies for COMAN
draft-greevenbosch-coman-candidate-tech-03

Abstract

This draft identifies candidate technologies and considerations for the COMAN use cases and requirements.

Note

Discussion and suggestions for improvement are requested, and should be sent to coman@ietf.org.

Status of This Memo

This Internet-Draft will expire on January 04, 2014.

Copyright Notice

Table of Contents

1. Requirements notation

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].

2. Introduction

In [I-D.ersue-constrained-mgmt], several use cases and associated requirements are defined for the management of constrained devices, in a possibly constrained network.

This document identifies possible technologies associated with the use cases and requirements.

In addition, this document includes several considerations associated with the requirements, that are relevant for choosing proper technologies.

The goal of this document is to identify what has been done, and what still needs to be done. Especially, it aims at establishing a clearer view of the scope and work in COMAN.

3. Identified candidate technologies for the requirements

3.1. OMA-LwM2M

OMA Lightweight M2M [OMA-LwM2M-TS] aims at providing an underlying layer agnostic protocol to allow M2M service enablement and management between the LwM2M Server and the LwM2M Client, which is placed in the resource constrained devices. The first version of enabler is currently being specified. The enabler provides a light and compact protocol and a flat data structure, and can satisfy various management requirements for constrained devices.

OMA-LwM2M has overlap with the following COMAN requirements:

- 4.2.002 Compact encoding of management data

- 4.4.001 Device status monitoring

- 4.4.002 Energy status monitoring

- 4.4.012 Logging

- 4.6.001 Authentication on management system and devices

- 4.6.002 Support suitable security bootstrapping mechanisms

- 4.6.003 Access control on management system and devices

Because of the overlap and early stage of OMA-LwM2M, good coordination between COMAN and OMA-LwM2M is advisable.

3.2. OMA Device Management

OMA Device Management [OMA-DM] provides various functions for mobile device management. OMA-DM specifies and depends heavily on the SyncML language, which uses XML. The typical underlying transport protocol is HTTP. This makes OMA-DM in unaltered form infeasible for constrained devices. Especially, it violates the following requirements:

- 4.1.001 Support multiple device classes within a single network

- 4.2.002 Compact encoding of management data

Nevertheless, there is much overlap between OMA-DM functionality and COMAN requirements. As such, OMA-DM MAY be used as inspiration for the COMAN solution.

OMA-DM defines a general data model for management purpose, which is called a Management Object (MO). MOs are stored on the device and can be manipulated by management actions carried over the OMA-DM protocol. For each management purpose, a specific MO has been defined. MOs relevant to the COMAN requirements include "FUMO" for firmware update requirements, "DiagMon MO" for diagnostic and monitoring requirements and the "Scheduling MO" for scheduling requirements. The various MOs are discussed in Section 3.2.1 and its subsections.

Apart from requirements covered by MOs, the following COMAN requirements intersect with the general OMA-DM functionality:

- 4.1.007 Network-wide configuration - Use broadcast capability from OMA-DM 1.3 - Sessionless specification.

3.2.1. OMA-DM Management Objects

3.2.1.1. OMA DiagMon MO

OMA DiagMon MO builds on and leverages the OMA DM v1.x protocol. It provides standard DM Management Objects and associated client-side and server-side behaviour necessary to conduct diagnostics and monitoring activities on mobile devices.

Requirements related to OMA DiagMon MO:

- 4.4.003 Monitoring of current and estimated device availability: can be achieved by DiagMon functions MO.

- 4.4.004 Network status monitoring: can be achieved by DiagMon functions MO.

- 4.4.006 Performance monitoring: can be achieved by DiagMon functions MO.

- 4.4.007 Fault detection monitoring: can be achieved by Trap MO.

- 4.4.011 Notifications: can be achieved by reporting functions in DiagMon MO.

- 4.4.008 Passive and reactive monitoring: can be achieved by Trap MO.

- 4.5.001 Self-management - Self-Healing: device events can be captured by Trap MO, also periodically, to achieve self-management.

3.2.1.2. OMA Scheduling MO

The OMA-DM Scheduling MO enabler [OMA-Scheduling-MO] specifies the scheduling framework as well as its Management Objects that can be layered on top of OMA-DM v1.x, to seamlessly add the common scheduling capability to the OMA-DM based management infrastructure. With this capability, the OMA-DM system is able to schedule management operations on the device, and have them executed offline when the schedule - time-based or event-based - matches.

Requirements related to OMA Scheduling MO:

- 4.5.001 Self-management - Self-Healing: time-based scheduled task can achieve periodic self-management.

3.2.1.3. OMA-FUMO

OMA-FUMO provides information on management objects associated with firmware updates in OMA-DM based mobile devices and the behaviour associated with the processing of the management objects.

3.2.2. ACL mechanism in OMA-DM

OMA-DM [OMA-DM] defines the Access Control List (ACL) mechanism to control the access to the Management Objects. ACL is a property associated with the Management Object nodes, and is used to grant access permissions to the server identifiers.

Related requirements:

- 4.6.002 Support suitable security bootstrapping mechanisms

- 4.6.003 Access control on management system and devices

3.3. CoAP

The Constrained Application Protocol (CoAP) [I-D.ietf-core-coap] is defined by the IETF. It provides an application layer protocol especially designed for constrained devices. It is binary and easy to parse.

CoAP is especially suitable on top of IPv6 and UDP. However, other lower level protocols are possible too.

In addition, several drafts have been specified to target specific issues.

3.3.1. CoAP main specification

The following requirements are met by the CoAP main specification:

- 4.1.001 Support multiple device classes within a single network - the low complexity of CoAP allows usage in all device classes.

- 4.1.004 Minimise state maintained on constrained devices - CoAP has been designed to keep servers stateless.

- 4.1.006 Support for lossy links and unreliable devices - through the CoAP CON retransmission mechanism.

- 4.2.004 Mapping of management protocol interactions - CoAP provides HTTP/Coap Mapping.

- 4.2.007 Protocol extensibility - mainly provided by options mechanism.

- 4.3.003 Asynchronous transaction support - CoAP supports separate response and piggy-backed response.

- 4.4.007 Fault detection monitoring (partly) - CoAP pinging allows verification if a device is online.

3.3.2. CoAP capability discovery specifications

Various CoAP drafts cover different aspects of capability discovery.

- RFC 6690 [RFC6690] defines a link format, which provides information on resources a server is offering.

- The draft [I-D.greevenbosch-core-profile-description] allows signalling a CoAP server profile.

- The draft [I-D.shelby-core-resource-directory] allows acquiring information about resources from another server, called the "Resource Directory".

- The draft [I-D.lynn-core-discovery-mapping] provides a mapping between the resource directory and a DNS lookup. This allows usage of DNS lookup for the discovery of CoAP servers.

- The informational draft [I-D.vanderstok-core-dna] discusses mapping between IP address and a Fully Qualified Domain Name (FQDN), proposing DNS for lookup of the IP address. In addition, it discusses possible naming conventions, group communication and resource discovery. Towards the latter, registration of new devices to the resource directory is discussed.

Related COMAN requirement:

- 4.3.002 Capability discovery

3.3.3. CoAP group communication

The informational CoAP group communication draft [I-D.ietf-core-groupcomm] discusses various aspects of group communication through IP multicast [RFC4604] in CoAP.

Another informational draft discussing group communication is [I-D.vanderstok-core-dna]. This draft gives detailed examples, and discusses multicast, naming and DNS mapping of groups.

Related COMAN requirement:

- 4.8.001 Group-based provisioning

3.3.4. CoAP energy saving technology

The draft [I-D.rahman-core-sleepy] provides a mechanisms for sleepy devices. These mechanisms include informing an intermediate resource directory (defined in [I-D.shelby-core-resource-directory]) of its waking up or intent to fall asleep. Through these two drafts, clients can use the observe mechanism [I-D.ietf-core-observe] to be informed of whether a device is sleeping or active.

Related COMAN requirements:

- 4.1.006 Support for lossy links and unreachable devices

- 4.7.002 Support of energy-optimized communication protocols

3.3.5. Congestion avoidance in CoAP

The considerations in this section relate to:

- 4.9.001 Congestion avoidance

- 4.9.003 Traffic delay schemes

The draft [I-D.bormann-core-cocoa] provides general background information about CoAP congestion control, and its challenges.

The draft [I-D.li-core-conditional-observe] defines a mechanism to signal minimum time between CoAP observations.

The draft [I-D.greevenbosch-core-minimum-request-interval] defines a mechanism to restrict the speed in which a CoAP client sends requests to the CoAP server.

Other ways to delay the traffic in CoAP is by sending delayed ACKs. However, this has limitations as too much delay will lead to retransmits from the client side. In addition, this method requires the server to maintain bookkeeping of the delayed ACKs.

3.4. Cryptography considerations

4.6.001 Authentication of management system and devices

- The raw public key as defined in [I-D.ietf-tls-oob-pubkey] can be used for establishing security and authentication.

- OCSP-lite as defined in [I-D.greevenbosch-tls-ocsp-lite] can be used for revocation checking of the raw public key.

4.6.002 Support suitable security bootstrapping mechanisms

- The draft [I-D.jennings-core-transitive-trust-enrollment] describes a system in which a Device is introduced to a Controller by a Introducer. In this draft, it is suggested that the Device symmetric key is coded as a QR code on the box, which can be read by the Controller, which may be a mobile phone with internet access.

4.6.004 Select cryptographic algorithms that are efficient in both code space and execution time

- Candidates for asymmetric cryptography:

  - RSA

  - ECC

  Keysize TBD.

- Candidates for symmetric cryptography:

  - AES (keysize 128/192/256)

  Keysize TBD.

- Candidates for hashing:

  - SHA-1

  - SHA-256

  - SHA-512

- For CoAP [I-D.ietf-core-coap], the following choices have been made:

  - Cipher suite: TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 specified in [I-D.mcgrew-tls-aes-ccm-ecc], [RFC5246], [RFC4492]

  - Hash: SHA-256

  - ECC with curve secp256r1 (equivalent to NIST P-256) [RFC4492]

  - AES-128 in CCM mode [RFC5116], [CCM]

4.6.008 Select cryptographic algorithms that are to be supported in hardware

- TBD

3.5. MANET

TBD.

3.6. BACnet

BACnet exists under the auspices of the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). BACnet is an American national standard, a European standard, a national standard in more than 30 countries, and an ISO global standard. The protocol is supported and maintained by ASHRAE Standing Standard Project

Committee (SSPC) 135. BACnet is the most deployed communications standard for building control in the USA. It consists of a number of working groups. Their results are published in one BACnet specification document: International ISO standard 16484-5 [ISO16484-5]. It defines a network architecture on top of several PHYs (ARCnet, MS/TP, Ethernet, P2P, LONTalk) and IP. It specifies a number of object types from which a control system can be composed. Central is the device objects (unique per device) that maintains all organization information for a given devices. Object types are defined for scheduling, grouping, alarm handling, object and device management, and service discovery. The BACnet specification includes an extensive Alarm and Event service, and object access service for system configuration purposes, and remote device management services.

The following requirements are met by the BACnet specification:

o 4.1.001 Support multiple device classes within a single network - the BACnet standard has an open source implementation that fits on the smallest devices and can also be deployed on larger devices

o 4.1.002 Management scalability - the BACnet standard defines a hierarchical management structure where data are collected from all devices with support from information in the device object. Group objects can be defined which aggregate information from multiple objects within the same device. A working group, BACnet/ WS, is dedicated to defining the architecture for storing historical data of the control system in a central repository using the ATOM Publishing standard and exploiting the xml modeling facilities.

o 4.1.003 Hierarchical management - hierarchical management is supported by the device and object structure, the independent structure in alarm management, and the group object which supports the grouping of commands.

o 4.1.004 Minimize state maintained on constrained devices - state is minimized by selecting relevant objects in the control devices.

o 4.1.008 Distributed Management - BACnet does provide the possibility to export management to multiple managers, however, no atomic write and read is specified, although there is a transaction concept at network level.

o 4.2.001 Modular implementation of management protocols - BACnet encourages and prescribes a modular implementation by segmenting the management functions and distributing them over different objects.

- 4.2.002 Compact encoding of management data - BACnet transports binary data encoded according to ASN.1, reduces storage space as much as feasible given the specified functionality.

- 4.2.005 Consistency of data models with the underlying information model - BACnet has an information model based on the ATOM publishing protocol. The BACnet Annex N standard prescribes the mapping between the information model and the data model present in the nodes.

- 4.2.007 Protocol extensibility - the BACnet model encourages extensibility, as proven by the constant backwards compatible standards updates. The standards extension process is slow and sets the extension pace.

- 4.3.001 Self-configuration capability - BACnet supports discovery of devices, their objects and properties via WHO-HAS, I-AM and similar messages.

- 4.3.002 Capability Discovery - See 4.3.001.

- 4.3.004 Network reconfiguration - BACnet knows the concept of BACnet routers. Routers declare themselves to network segments, and can be allocated started, stopped. No automatic procedures are described for full auto-configuration.

- 4.4.001 Device status monitoring - BACnet provides extensive tools for network and device status monitoring, specified in the Alarm and Event services section. BACnet supports a very flexible event and alarm reporting. Clients can subscribe to generators of events and alarms, which can be changes of values in objects or status changes. Classes of events can be specified with appropriate handling by the clients.

- 4.4.002 Energy status monitoring - This can be provided in BACnet by creating a binary value object type connected to the energy c.q. power attributes to monitor and specify a change of state with an appropriate client.

- 4.4.003 Monitoring of current and estimated device availability - See text in 4.4.002.

- 4.4.004 Network status monitoring - BACnet provides facilities to configure and install routers on the BACnet network. BACnet specifies the MS/TP and PTP link protocols with the possibility to monitor link status.

- 4.4.006 Performance Monitoring - BACnet defines a set of application layer objects. Dependent on their function, performance measures are monitored and events or alarms are generated to be monitored by an alarm handling service.

- 4.4.007 Fault detection monitoring - BACnet includes fault detection monitoring at network level.

- 4.4.009 Recovery - BACnet provides functions for network recovery and object, device recovery without specifying how these functions must be used in case of given errors.

- 4.4.010 Network topology discovery - this is a rather basic capability of a BACnet network.

- 4.4.011 Notifications - the BACnet alarm and event services are dedicated to this topic.

- 4.4.012 Logging - BACnet annex N specifies how logged values can be stored in a server using the ATOM publishing protocol.

- 4.6.001 Authentication of management system and devices - BACnet security service provides authentication of peers, operators and data source.

- 4.10.002 Reliable unicast transport - BACnet provides a transaction service over the network.

- 4.10.003 Best-effort multicast - BACnet goes to great pains to provide a broadcast facility which is essential for its configuration purposes.

- 4.11.001 Avoid complex application layer transactions requiring large application messages - BACnet has a finite set of application message constructs in which application messages should fit.

- 4.11.002 Avoid reassembly of messages at multiple layers in the protocol stack - BACnet avoids reassembly by contruction.

3.7. SNMP

The Simple Network Management Protocol (SNMP) can be used to monitor and manage various network entities. It is the most popular network management protocol today based on IETF standards. In [RFC3410] an introduction and overview of SNMP is presented. The architecture of the Internet Standard management framework consists of:

- A data definition language, referred to as Structure of Management Information (SMI), is defined in [RFC2578], [RFC2579], [RFC2580].

- The Management Information Base (MIB) which contains the information to be managed and is defined for each specific function to be managed [RFC3418].

- A protocol definition referred to as Simple Network Management Protocol. Version 3 (SNMPv3) is defined in [RFC3411], [RFC3412], [RFC3413], [RFC3416], and [RFC3417].

- Security and administration that provides SNMP message based security on the basis of the user-based security model, discussed in [RFC3414] and [RFC3415].

Separation in modules was motivated by the wish to respond to the evolution of Internet. The protocol part (SNMP) and data definition part (MIB) are independent of each other. The separation has enabled the progressive passage from SNMPv1 via SNMPv2 to SNMPv3. The SNMP protocol supports seven types of access supported by as many Protocol Data Unit (PDU) types. Two types of message exchange are used:

- The SNMP client sends out a request message after which the SNMP server returns a Response message.

- The SNMP server sends a confirmed or unconfirmed notification message with a list of (OBJECT-IDENTIFIERs, value) pairs to a notification requesting end-point.

The MIB objects are defined in ASN.1, for various protocols, at different layers. For example, [RFC4113] defines a MIB for UDP, whereas the draft [I-D.schoenw-6lowpan-mib] defines a MIB module for 6LoWPAN [RFC4944].

The interesting part of SNMP is that it provides a framework that enables request/response and notification type message exchanges. The purpose of the message exchange is defined by the contents of the MIBs which are declared independently for many different purposes. Related requirements are:

- 4.1.001 Multiple device classes, SNMP and MIB are class independent.

- 4.1.002 Management scalability, SNMP can be the basis for extended management functionality.

- 4.2.001 Modular implementation, Separation between MIB and SNMP provides basic modularity. Separation in MIBs and SNMP entities provides a second level of modularity.

- 4.2.005 Consistency between data and information model, Encouraged by separation of MIBs.

- 4.2.007 Protocol Extensibility, Supported by design, but lacks in message PDU type extensibility.

- 4.3.004 Network reconfiguration, Several MIBs support network configuration but not in an automatic network state driven fashion.

- 4.4.001 Device status monitoring, Appropriate MIB is specified.

- 4.4.002 Energy state monitoring, MIB specified by Eman.

- 4.4.004 Network status monitoring, Appropriate MIB is specified

- 4.4.006 Performance monitoring, Appropriate MIBs may be specified outside IETF

- 4.4.007 Fault detection monitoring, Appropriate MIBs are specified.

- 4.4.011 Notifications, Basic SNMP function.

- 4.6.001 Authentication of management system and devices, supported by SNMPv3.

- 4.6.003 Access control on management system and devices, supported by SNMPv3.

- 4.7.001 Management of Energy Resources, supported by Eman MIBs.

- 4.11.001 Avoid large messages, SNMP supports progessive transport of data in self contained chunks.

- 4.11.002 Avoid reassembly at multiple layers, SNMP request specifies data size per message.

Since much MIB creation effort can be done offline through macros, and BER encoding is not extremely complex, it is feasible to implement SNMP in constrained environments. Sharing the security code between SNMP and DTLS/CoAP makes the inclusion of SNMP even more attractive.

3.8. NETCONF

Cover at least:

- The NETCONF protocol is defined in [RFC6241]

- The YANG module is defined in [RFC6022]

- NETCONF is based on XML

3.9. Other requirements and candidate technologies

4.1.005 Automatic re-synchronisation with eventual consistency

4.1.006 Support for lossy links and unreachable devices

- Mechanisms for devices that are not sleepy, but have unstable network connections (e.g. mobile devices) are needed.

4.1.008 Distributed management

4.2.006 Loss-less mapping of management data models

4.3.002 Capability discovery

4.3.004 Network reconfiguration

4.4.009 Recovery

4.4.010 Network topology discovery

4.7.001 Management of energy resources

4.7.002 Support of energy-optimized communication protocols

- 6LoWPAN [RFC4944] provides IPv6 functionality for IEEE 802.15.4 networks.

4.7.003 Support for layer 2 energy-aware protocols

- IEEE 802.15.4 [IEEE-802.15.4] provides wireless low power communication on short distance.

4.7.004 Dying gasp

4.9.002 Redirect traffic

4.10.001 Scalable transport layer

4.10.002 Reliable unicast transport

4.10.004 Secure message transport

4.11.001 Avoid complex application layer transactions requiring large application layer messages

4.11.002 Avoid reassembly of messages at multiple layers in the protocol stack

4. High level requirements that need to be observed continuously

4.1.001 Support multiple device classes within a single network

4.1.002 Management scalability

4.1.004 Minimise state maintained on constrained devices

4.1.006 Support for lossy links and unreachable devices

4.2.002 Compact encoding of management data

- A binary format would be most compact.

- TLV could be considered.

- XML would be counter productive.

- JSON may be counter productive.

4.2.003 Compression of management data or complete messages

- When the messages are designed compact enough, compression will be unnecessary.

4.2.007 Protocol extensibility

5. Table of requirements and related technologies

The Table 1 summarises the requirements and related or possible candidate technologies.

Requirement number	Name	Associated technology
4.1.001	Support multiple	[I-D.ietf-core-coap], [ISO16484-5], [RFC3410]

	device classes within a single network	
4.1.002	Management scalability	[ISO16484-5], [RFC3410]
4.1.003	Hierarchical management	[ISO16484-5]
4.1.004	Minimise state maintained on constrained devices	[I-D.ietf-core-coap], [ISO16484-5]
4.1.005	Automatic re-synchronisation with eventual consistency	
4.1.006	Support for lossy links and unreachable devices	[I-D.ietf-core-coap] [I-D.rahman-core-sleepy], [I-D.shelby-core-resource-directory], [I-D.ietf-core-observe]
4.1.007	Network-wide configuration	[OMA-DM], [ISO16484-5]
4.1.008	Distributed management	[ISO16484-5]
4.2.001	Modular implementation of management protocols	[ISO16484-5], [RFC3410]
4.2.002	Compact encoding of management data	[OMA-LwM2M-TS], [ISO16484-5]
4.2.003	Compression of management data or complete messages	

4.2.004	Mapping of management protocol interactions	[I-D.ietf-core-coap]
4.2.005	Consistency of data models with the underlying information model	[ISO16484-5], [RFC3410]
4.2.006	Loss-less mapping of management data models	
4.2.007	Protocol extensibility	[I-D.ietf-core-coap], [ISO16484-5], [RFC3410]
4.3.001	Self-configuration capability	[ISO16484-5]
4.3.002	Capability discovery	[RFC6690], [I-D.greevenbosch-core-profile-description], [I-D.shelby-core-resource-directory], [I-D.lynn-core-discovery-mapping], [I-D.vanderstok-core-dna], [ISO16484-5]
4.3.003	Asynchronous transaction support	[I-D.ietf-core-coap]
4.3.004	Network reconfiguration	[ISO16484-5], [RFC3410]
4.4.001	Device status monitoring	[OMA-LwM2M-TS], [ISO16484-5], [RFC3410]
4.4.002	Energy status monitoring	[OMA-LwM2M-TS], [ISO16484-5], [RFC3410]
4.4.003	Monitoring of current and estimated device availability	[OMA-DiagMon-MO], [ISO16484-5]

4.4.004	Network status monitoring	[OMA-DiagMon-MO], [ISO16484-5], [RFC3410]
4.4.005	Self-monitoring	[OMA-DiagMon-MO], [ISO16484-5]
4.4.006	Performance monitoring	[OMA-DiagMon-MO], [ISO16484-5], [RFC3410]
4.4.007	Fault detection monitoring	[I-D.ietf-core-coap], [OMA-DiagMon-MO], [ISO16484-5], [RFC3410]
4.4.008	Passive and reactive monitoring	[OMA-DiagMon-MO]
4.4.009	Recovery	[ISO16484-5]
4.4.010	Network topology discovery	[ISO16484-5]
4.4.011	Notifications	[OMA-DiagMon-MO], [ISO16484-5], [RFC3410]
4.4.012	Logging	[OMA-LwM2M-TS], [ISO16484-5]
4.5.001	Self-management - Self-healing	[OMA-DiagMon-MO], [OMA-Scheduling-MO]
4.6.001	Authentication of management system and devices	[OMA-LwM2M-TS], [I-D.ietf-tls-oob-pubkey], [I-D.greevenbosch-tls-ocsp-lite], [ISO16484-5], [RFC3410]
4.6.002	Support suitable security bootstrapping mechanisms	[OMA-LwM2M-TS], [OMA-DM], [I-D.jennings-core-transitive-trust-enrollment]
4.6.003	Access control on management system and devices	[OMA-LwM2M-TS], [OMA-DM], [RFC3410]

4.6.004	Select cryptographic algorithms that are efficient in both code space and execution time	
4.7.001	Management of energy resources	[IEEE-802.15.4], [I-D.rahman-core-sleepy], [RFC3410]
4.7.002	Support of energy-optimized communication protocols	[I-D.ietf-core-coap], [RFC4944], [I-D.rahman-core-sleepy], [I-D.ietf-core-observe], [I-D.shelby-core-resource-directory]
4.7.003	Support for layer 2 energy-aware protocols	[IEEE-802.15.4]
4.7.004	Dying gasp	
4.8.001	Group-based provisioning	[I-D.ietf-core-groupcomm], [I-D.vanderstok-core-dna], [RFC4604]
4.9.001	Congestion avoidance	[I-D.ietf-core-coap], [I-D.li-core-conditional-observe], [I-D.bormann-core-cocoa], [I-D.greevenbosch-core-minimum-request-interval]
4.9.002	Redirect traffic	
4.9.003	Traffic delay schemes	[I-D.ietf-core-coap], [I-D.li-core-conditional-observe], [I-D.bormann-core-cocoa], [I-D.greevenbosch-core-minimum-request-interval]
4.10.001	Scalable transport layer	
4.10.002	Reliable	

	unicast transport	
4.10.003	Best-effort multicast	[ISO16484-5]
4.10.004	Secure message transport	
4.11.001	Avoid complex application layer transactions requiring large application layer messages	[RFC3410]
4.11.002	Avoid reassembly of messages at multiple layers in the protocol stack	[ISO16484-5], [RFC3410]

Table 1: Requirements and technologies

6. Conclusion and recommendations

In this document, we have identified technology standards that currently cover many of the COMAN use cases. COMAN should consider referencing these technologies when appropriate. In addition, this document points at technologies that are not deployed in a standard, and hence need new standardisation. We recommend to write a document in COMAN that describes the overall envisaged management system and suggests standardisation topics for IETF.

7. Security Considerations

TBD

8. IANA considerations

TBD

9. Change Log

v00 -> v01:

- Added text about BACnet.

v01 -> v02:

- Updated text about BACnet.
- Updated to match new requirements numbering in I-D.ersue-constrained-mgmt v04.

v02 -> v03:

- Added text about SNMP.
- Added bullets about security choices in CoAP.

10. References

10.1. Normative References

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

10.2. Informative References

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[RFC2580] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[RFC3412] Case, J., Harrington, D., Presuhn, R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, December 2002.

[RFC3413] Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, December 2002.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[RFC3415] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002.

[RFC3416] Presuhn, R., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, December 2002.

[RFC3417] Presuhn, R., "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, December 2002.

[RFC3418] Presuhn, R., "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3418, December 2002.

[RFC4113] Fenner, B. and J. Flick, "Management Information Base for the User Datagram Protocol (UDP)", RFC 4113, June 2005.

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006.

[RFC4604] Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", RFC 4604, August 2006.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC6022] Scott, M. and M. Bjorklund, "YANG Module for NETCONF Monitoring", RFC 6022, October 2010.

[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, April 2011.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC6690] Shelby, Z., "Constrained RESTful Environments (CoRE) Link Format", RFC 6690, August 2012.

[I-D.ietf-core-coap] Shelby, Z., Hartke, K., and C. Bormann, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-18 (work in progress), June 2013.

[I-D.ietf-core-groupcomm] Rahman, A. and E. Dijk, "Group Communication for CoAP", draft-ietf-core-groupcomm-09 (work in progress), May 2013.

[I-D.ietf-core-observe] Hartke, K., "Observing Resources in CoAP", draft-ietf-core-observe-08 (work in progress), February 2013.

[I-D.ietf-tls-oob-pubkey] Wouters, P., Tschofenig, H., Gilmore, J., Weiler, S., and T. Kivinen, "Out-of-Band Public Key Validation for Transport Layer Security (TLS)", draft-ietf-tls-oob-pubkey-07 (work in progress), February 2013.

[I-D.bormann-core-cocoa] Bormann, C., "CoAP Simple Congestion Control/Advanced", draft-bormann-core-cocoa-00 (work in progress), August 2012.

[I-D.ersue-constrained-mgmt] Ersue, M., Romascanu, D., and J. Schoenwaelder, "Management of Networks with Constrained Devices: Problem Statement, Use Cases and Requirements", draft-ersue-constrained-mgmt-03 (work in progress), February 2013.

[I-D.greevenbosch-core-minimum-request-interval]

Greevenbosch, B., "CoAP Minimum Request Interval", draft-greevenbosch-core-minimum-request-interval-01 (work in progress), April 2013.

[I-D.greevenbosch-core-profile-description]
Greevenbosch, B., Hoebeke, J., Ishaq, I., and F. Abeele, "CoAP Profile Description Format", draft-greevenbosch-core-profile-description-02 (work in progress), June 2013.

[I-D.greevenbosch-tls-ocsp-lite]
Greevenbosch, B., "OCSP-lite - Revocation of raw public keys", draft-greevenbosch-tls-ocsp-lite-01 (work in progress), June 2013.

[I-D.jennings-core-transitive-trust-enrollment]
Jennings, C., "Transitive Trust Enrollment for Constrained Devices", draft-jennings-core-transitive-trust-enrollment-01 (work in progress), October 2012.

[I-D.li-core-conditional-observe]
Li, S., Hoebeke, J., Abeele, F., and A. Jara, "Conditional observe in CoAP", draft-li-core-conditional-observe-04 (work in progress), June 2013.

[I-D.lynn-core-discovery-mapping]
Lynn, K. and Z. Shelby, "CoRE Link-Format to DNS-Based Service Discovery Mapping", draft-lynn-core-discovery-mapping-02 (work in progress), October 2012.

[I-D.mcgrew-tls-aes-ccm-ecc]
McGrew, D., Bailey, D., Campagna, M., and R. Dugal, "AES-CCM ECC Cipher Suites for TLS", draft-mcgrew-tls-aes-ccm-ecc-06 (work in progress), February 2013.

[I-D.rahman-core-sleepy]
Rahman, A., "Enhanced Sleepy Node Support for CoAP", draft-rahman-core-sleepy-02 (work in progress), February 2013.

[I-D.schoenw-6lowpan-mib]
Schoenwaelder, J., Sehgal, A., Tsou, T., and C. Zhou, "Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", draft-schoenw-6lowpan-mib-03 (work in progress), February 2013.

[I-D.shelby-core-resource-directory]

Shelby, Z., Krco, S., and C. Bormann, "CoRE Resource Directory", draft-shelby-core-resource-directory-05 (work in progress), February 2013.

[I-D.vanderstok-core-dna]
Stok, P., Lynn, K., and A. Brandt, "CoRE Discovery, Naming, and Addressing", draft-vanderstok-core-dna-02 (work in progress), July 2012.

[CCM] , "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality ", National Institute of Standards and Technology SP 800-38C, May 2004.

[IEEE-802.15.4]
IEEE Computer Society, ., "IEEE std. 802.15.4-2003", October 2003.

[ISO16484-5]
, "Building automation and control systems -- Part 5: Data communication protocol", ISO 16484-5, 2012.

[OMA-DM] , "OMA Device Management 1.3", OMA-ERP-DM-V1_3-20121213-C , December 2012.

[OMA-DiagMon-MO]
, "OMA Diagnostics and Monitoring Management Object", OMA-ERP-DiagMon-V1_0-20120313-A , March 2012.

[OMA-FUMO]
, "Firmware Update Management Object", OMA-TS-DM-FUMO-V1_0-20070209-A , February 2007.

[OMA-Scheduling-MO]
, "OMA DM Scheduling Management Object", OMA-ERP-DM_Scheduling-V1_0-20110614-C , June 2011.

[OMA-LwM2M-TS]
, "OMA Lightweight M2M", OMA-TS-LightweightM2M-V1_0-20130123-D (work in progress), January 2013.

Authors' Addresses

Bert Greevenbosch
Huawei Technologies Co., Ltd.
Huawei Industrial Base
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: bert.greevenbosch@huawei.com

Kepeng Li
Huawei Technologies Co., Ltd.
Huawei Industrial Base
Bantian, Longgang District
Shenzhen 518129
P.R. China

Phone: +86-755-28971807
Email: likepeng@huawei.com

Peter van der Stok
vanderstok consultancy

Phone: +31-492474673 (Netherlands), +33-966015248 (France)
Email: consultancy@vanderstok.org
URI: www.vanderstok.org