INTERNATIONAL STANDARD

ISO 19079

First edition
2016-10-01

Intelligent transport systems — Communications access for land mobiles (CALM) — 6LoWPAN networking

Systèmes intelligents de transport — Accès aux communications des services mobiles terrestres (CALM) — Gestion de réseau 6LoWPAN

Reference number
ISO 19079:2016(E)

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

Introduction

The set of International Standards that collectively refer to CALM (Communications Access for Land Mobile) focus on the specification of open interfaces regarding the functionality required by all relevant layers and entities of a standard communication architecture for Intelligent Transport Systems (ITS). This communication is known as the ITS station reference architecture (ISO 21217).

These International Standards are designed to allow interoperable instantiations of ITS stations (ITS-S), which are based on the concept of abstracting applications and services from the underlying communication layers. This abstraction makes the ITS station architecture ideally suited to the development and deployment of Cooperative ITS applications and services.

The set of ITS station International Standards include specifications for security in ITS communications, ITS-S management, distributed ITS-S implementations, legacy communication media interfaces, legacy application interfaces, and new communication interfaces specifically designed for ITS applications such as those targeted to safety of both life and property.

The fundamental advantage of the ITS station with respect to traditional systems is the ability to support vertical handovers between the various access technologies that can be included in an ITS station. Handover mechanisms are defined within the ITS station reference architecture, the ITS station medium service access points International Standard (ISO 21218) and the ITS station management International Standard (ISO 24102).

The ITS station IPv6 networking International Standard (ISO 21210) determines the network protocols to support reachability at a global IP address, continuous Internet connectivity, and the handover policies between session performed by infrastructure mobile routers (MR) using the same media or using different access technologies.

ITS station compliant internal networks (both in-vehicle and off-vehicle) are expected to interact with each other to seamlessly exchange information. This should be true also for information retrieved from Wireless Sensor Networks (WSN) to be dispatched to any ITS station. As WSNs are largely based on low-cost Component of The Shelf (COTS), IETF has promoted the standardization of a set of protocols at the network and facility layers suited for constrained devices (in terms of capability of processing, storage or communication) based on low-rate wireless personal area networks (LR-WPANs) technologies. An important candidate at network layer in this sense is the IETF IPv6 over Low power Wireless Personal Area Networks (6LoWPAN), an adaptation layer for IPv6 that addresses device limitations by means of header compression and protocol optimizations.

This document identifies network protocols that are needed to support global reachability at a global IP address for Wireless Sensor Networks (WSNs) based on the IEEE 802.15.4 access medium; in particular, this document states how to use the set of 6LoWPAN protocols specified by IETF in the context of ITS.

Intelligent transport systems — Communications access for land mobiles (CALM) — 6LoWPAN networking

1 Scope

This document describes the networking protocol functionality related to 6LoWPAN networking between two or more ITS stations communicating over the global Internet communication network.

It is assumed that the reader is familiar with IETF specifications found in "Request for Comments" (RFCs) 4944, 6282 and 2460 for 6LoWPAN and IPv6 protocols respective blocks used within this document. This document does not define a new protocol, neither does it define new abstraction for exchange of messages at the 6LoWPAN layer nor does it define new data structures. It, however, illustrates how the IETF protocols are combined to allow seamless communication among both heterogeneous and homogeneous ITS stations using 6LoWPAN. The 6LoWPAN family of protocols defined in this document as the Internet of Things Management Service Entity (IoT MSE) is integrated within the ITS station reference architecture as a new protocol block of the ITS station Networking and Transport layer. The procedures defined to share information between the IoT MSE block of the ITS station networking and transport protocols and other components of the ITS station architecture will be defined in the ISO 24102 series. ISO 24102 series includes the specifications for ITS station management, which are standardized to be compliant with the ITS station reference architecture and related standards.

In addition to the requirements described within this document, a number of notes and examples are provided to illustrate the IoT MSE block and its configuration.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 21210:2012, *Intelligent transport systems — Communications access for land mobiles (CALM) — IPv6 Networking*

ISO 21217:2014, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

ISO 21218:2013, *Intelligent transport systems — Communications access for land mobiles (CALM) — Access technology support*

ISO 24102-3:2013, *Intelligent transport systems — Communications access for land mobiles (CALM) — Management- Part 3: Service access points*

ISO 24102-6, *Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 6: Path and flow management*

ETSI/TS 102 760-1 V1.1.1 (2009-11), *Intelligent Transport Systems (ITS); Test specifications for Intelligent Transport Systems; Communications Access for Land Mobiles (CALM); Medium Service Access Points (ISO 21218); Part 1: Implementation Conformance Statement (ICS) proforma*

IETF RFC 2460 *Internet Protocol Version 6*

IETF RFC 4861 *Neighbor Discovery for IP version 6 (IPv6)*

IETF RFC 4301 *Security Architecture for the Internet Protocol*

IETF RFC 4302 *IP Authentication Header*

IETF RFC 4303 *IP Encapsulating Security Payload (ESP)*

IETF RFC 4835 *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*

IETF RFC 3566 *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*

IETF RFC 7228 *Terminology for Constrained-Node Networks*

IETF RFC 4919 *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*

IETF RFC 4944 *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*

IETF RFC 6282 *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*

IETF RFC 6347 *Datagram Transport Layer Security Version 1.2*

IETF RFC 6775:2012 *Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)*

IETF RFC 6550 IPv6 *Routing Protocol for Low-Power and Lossy Networks (RPL)*

IETF RFC 6568 *Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)*

IETF RFC 6957 *Duplicate Address Detection Proxy*

IEEE 802.15.4-2006*Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 21210, ISO 21217, ISO 21218 and ISO 24102-3 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp/

3.1
IoT management service entity
IoT MSE
collection of modules required for a specific instantiation of 6LoWPAN

Note 1 to entry: The 6LoWPAN network comprises of a set of 6LoWPAN protocols, of which some are already standardized (see IETF RFC 6282and IETF RFC 6775, etc.).

3.2
6LoWPAN address
address including the network prefix and the host address

Note 1 to entry: The network-prefix set-up determines if the device can be addressed globally whereas the host address should be unique within the 6LoWPAN.

3.3
6LoWPAN prefix
prefix corresponding to a node’s address

3.4
link-local address
6LoWPAN address corresponding to a “link-local 6LoWPAN unicast address” and being used to communicate with devices in the same PAN

3.5
6LoWPAN global address
6LoWPAN address for communicating with devices globally

3.6
6LoWPAN node
device that implements 6LoWPAN

Note 1 to entry: See IETF RFC 4944, IETF RFC 6282 and IETF RFC 6775.

3.7
6LoWPAN host
ITS-S 6LoWPAN node comprising of ITS-S IoT MSE functionality other than those of a 6LoWPAN router or 6LoWPAN gateway

3.8
6LoWPAN internal interface
interface of a 6LoWPAN node in an ITS station used to connect with other 6LoWPAN nodes

3.9
6LoWPAN external interface
6LoWPAN interface of an ITS-S 6LoWPAN router node in an ITS station used to connect to the Internet or to other ITS-Stations

3.10
6LoWPAN ad-hoc router
device that implements 6LoWPAN and a layer-3 ad-hoc routing protocol internally to an ITS-S

Note 1 to entry: IETF RFC 4944, IETF RFC 6282, and IETF RFC 6775.

3.11
6LoWPAN access router
6LoWPAN AR
6LoWPAN router residing in an ITS-S at the edge of an Access Network and connected to one or more access points

3.12
6LoWPAN-IPv6 border router
6LoWPAN-IPv6 BR
6LoWPAN router residing in an ITS-S at the edge of an Access Network and connected to the Internet

Note 1 to entry: This router could perform additional functions related to IPv6 networking as defined in ISO 21210.

3.13
ITS-station unit
ITS-SU
physical instantiation of an ITS-S

Note 1 to entry: This could be a distributed instantiation in a 6LoWPAN/IPv6 Border router and 6LoWPAN Hosts. An ITS-SU contains one or more ITS-SCUs, and hence one or more communication interfaces (CIs). See Annex A for guidelines on CI.

3.14
ITS-S communication unit
ITS-S CU
physical unit in an ITS-SU containing a part or all of the functionality of an ITS-S

Note 1 to entry: In case an ITS-SU consists of a single physical unit, the ITS-SU and the ITS-SCU are identical. In case an ITS-SU consists of more than one ITS-SCU, then these ITS-SCUs are interconnected via the ITS station-internal network of the ITS-SU.

4 Symbols and abbreviated terms

Symbols and abbreviated terms specified in ISO 21210, ISO 21217, ISO 21218, ISO 24102-3, IETF RFC 4944, IETF RFC 6282, IETF RFC 6775, IETF RFC 4301, IETF RFC 4302, IETF RFC 4303, IETF RFC 6347 apply.

5 Requirements: ITS-Station 6LoWPAN Nodes

5.1 Categories

This subclause describes the relationship between the five categories of requirements.

— The first category (see 5.2) contains requirements applying to a specific instantiation of an ITS-S 6LoWPAN node and the requirements applying to different types of 6LoWPAN nodes in each ITS sub-system.

— The second category (see 5.3) contains requirements that define the IoT MSE (6LoWPAN networking) modules, which are specific to the “ITS-S 6LoWPAN nodes”. The five different modules are detailed under this category and they may be combined in different ways according to the functions of the 6LoWPAN nodes that is defined in 5.2.

— The third category (see 5.4) contains requirements defining which of the IoT MSE modules specified in 5.3 are combined for each particular “ITS-S 6LoWPAN node” specified in 5.2 and it further provides an example instantiation for an ITS-SU distributed in one or more ITS-SCUs.

— The fourth category (see 5.5) contains 6LoWPAN addressing requirements that are applicable to “ITS-S 6LoWPAN nodes” according to the functions listed in 5.2.

— The fifth category (see 5.6) contains optional features and functions. Their actual specification is currently out of the scope of this document.

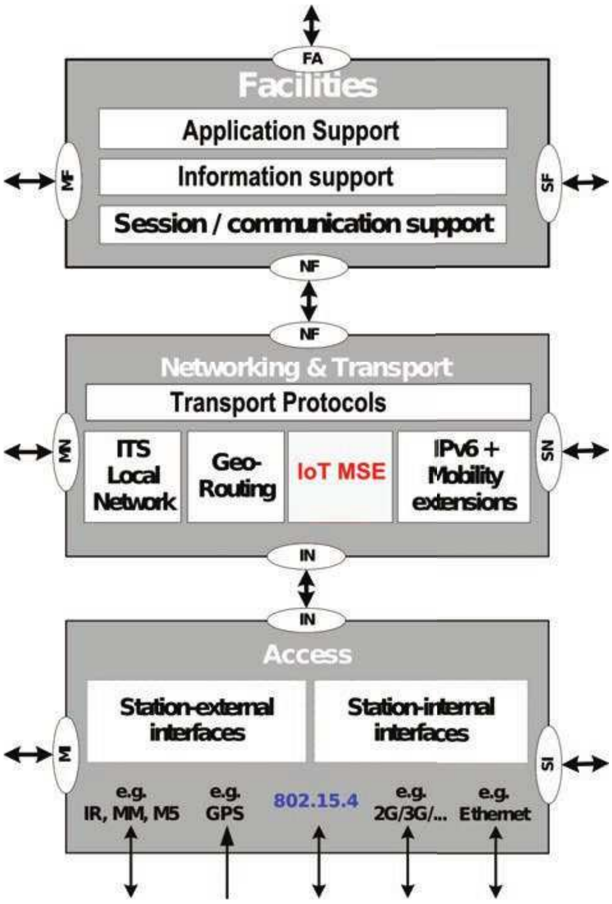

Figure 1 — Scope of IoT MSE (6LoWPAN Networking) within the ITS station reference architecture

In Annex A, the general usage for MAC-PHY interface is provided.

5.2 ITS-S nodes implementing 6LoWPAN

Figure 1 illustrates the scope of IoT MSE within the ITS station reference at the Network and Transport (NT) layer. A station implementing 6LoWPAN(in a PAN) is pictorially represented in Figure 2 together with its (eventual) connectivity to ordinary Internet peers (in a LAN) making use of a special node (i.e. an “Access Router”) equipped with at least two MAC interfaces.

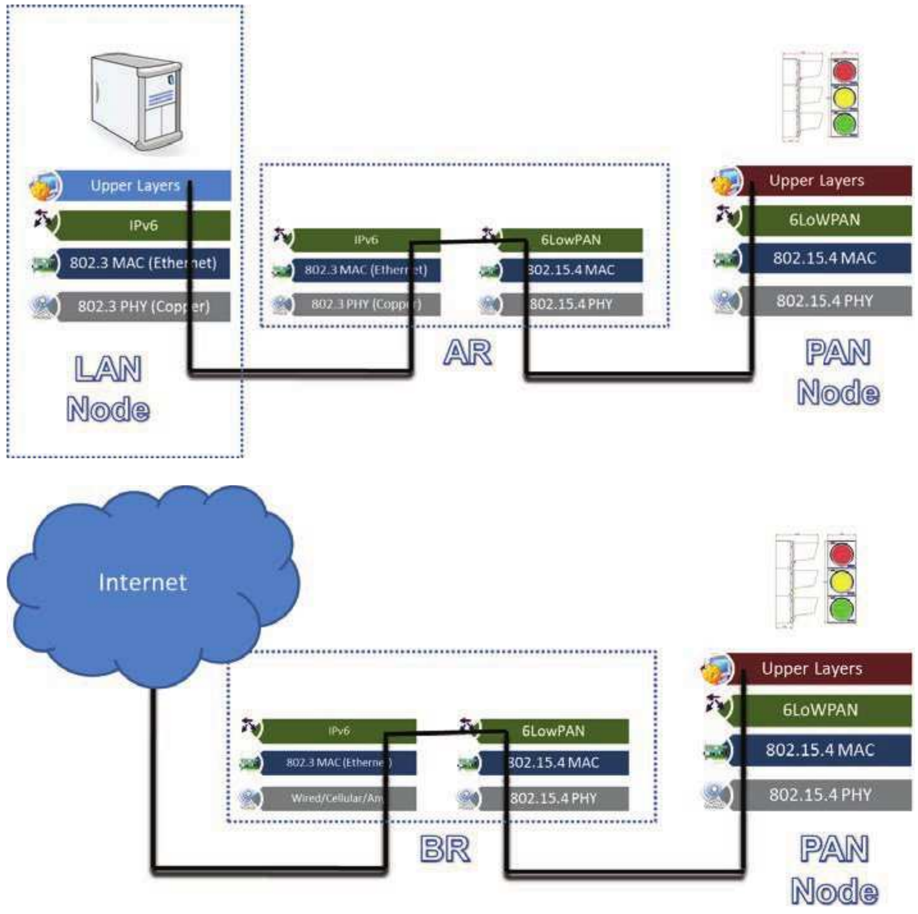

Figure 2 — 6LoWPAN subsystem

If the router device connects the PAN to the Internet, the device is called "Border Router".

The 6LoWPAN-based ITS stations can notably take part in the "Road-side" and "Vehicular" subsystems as pictorially shown in ISO 21217:2014, Figure 16. The other scenarios will not be discussed in this document due to the reduced impact they provide on the C-ITS general architecture.

5.2.1 Requirements for all ITS-S 6LoWPAN nodes

5.2.1.1 General

This subclause specifies the functional requirements of all ITS stations implementing 6LoWPAN networking. A Personal Area Network in an ITS station implemented according to these specifications is referred to as an "ITS-S 6LoWPAN".

5.2.1.2 Specific Instantiation of 6LoWPAN nodes

Additional features may be required according to the role played by the ITS-S 6LoWPAN node, which in this instance could be an ITS-S 6LoWPAN host, an ITS-S 6LoWPAN (ad-hoc) router as well as a multi-MAC device such as ITS-S IPv6 mobile router, ITS-S IPv6 access router, ITS-S IPv6 border router (see ISO 21210) regardless of the deployment scenarios such as the "Road-side" and "Vehicular" subsystems, etc. as pictorially shown in Figure 3.

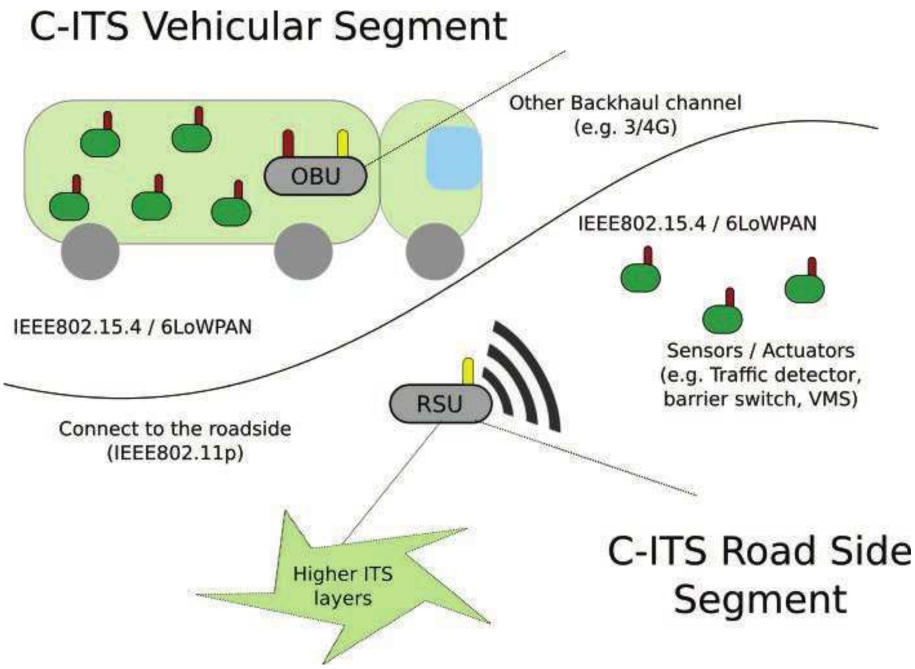

Figure 3 — Example of 6LoWPAN nodes in ITS deployment

ITS-S 6LoWPAN deployed in ITS stations shall be part of the global public Internet.

ITS-S 6LoWPAN shall all be 6LoWPAN islands of inter-connected networks over the public Internet by using either the native IPv6, or tunnelled in IPv4 networks or a combination of both.

Transition mechanisms may be deployed to facilitate the communication between the 6LoWPAN entities and the public Internet entities that are not yet able to communicate using the IPv6 protocol International Standard.

The functions of an ITS subsystem may be distributed among various nodes on an ITS-S 6LoWPAN. There shall be at least one ITS-S 6LoWPAN (ad-hoc) “Router” on the ITS-S 6LoWPAN to guarantee the connectivity among nodes.

If the ITS-S functionality is spread over a set of nodes in a PAN and a LAN, the ITS-S 6LoWPAN router shall have an ITS-S internal interface in order to forward messages coming or directed to any node in the ITS-S IPv6 LAN (see Figure 2).

Any ITS-S 6LoWPAN shall have at least one external 6LoWPAN interface (implementing the “Border Router” functionality) to guarantee the addressability and connectivity to the Internet.

5.2.1.3 Communications directed to other Internet peers

Being part of the global Internet, 6LoWPAN nodes deployed within ITS-S 6LoWPAN can communicate with IPv6 third parties that are not located in the same ITS. It is necessary that the 6LoWPAN in ITS stations are backward compatible with all legacy IPv6 nodes connected to the ITS station either in the “ITS-S 6LoWPAN” or anywhere in the Internet.

5.2.1.4 ITS-S 6LoWPAN host instantiation

An ITS-S 6LoWPAN host deployed in an ITS-S 6LoWPAN shall implement the modules of an ITS-S 6LoWPAN host as indicated in 5.4.1.

5.2.1.5 ITS-S 6LoWPAN ad-hoc router instantiation

An ITS-S 6LoWPAN ad-hoc router deployed in an ITS-S 6LoWPAN shall implement the modules of an ITS-S 6LoWPAN ad-hoc router in accordance with 5.4.2. If desired in a particular implementation, the functions of the ITS-S 6LoWPAN host can be performed by an ITS-S 6LoWPAN ad-hoc router.

5.2.1.6 ITS-S 6LoWPAN access router instantiation

An ITS-S 6LoWPAN access router deployed in an ITS-S 6LoWPAN shall implement the modules of an ITS-S 6LoWPAN access router in accordance with 5.4.3. If desired in a particular implementation, the functions of the ITS-S 6LoWPAN ad-hoc router can be performed by an ITS-S 6LoWPAN access router.

5.2.1.7 ITS-S 6LoWPAN border router instantiation

An ITS-S 6LoWPAN border router deployed in an ITS-S 6LoWPAN and connected to the Internet shall implement the modules of an ITS-S 6LoWPAN border router in accordance with 5.4.4. If desired in a particular implementation, the functions of the ITS-S 6LoWPAN access router can be performed by an ITS-S 6LoWPAN border router.

5.2.1.8 ITS-S 6LoWPAN gateway instantiation

An ITS-S gateway acting as a firewall isolating non-6LoWPAN devices from other devices that are reachable over 6LoWPAN can be implemented as an ITS-S 6LoWPAN host (in accordance with 5.4.1) or as an ITS-S 6LoWPAN router (in accordance with 5.4.2, 5.4.3 or 5.4.4).

5.2.1.9 Consideration on central and personal ITS-Station subsystems

As discussed in 5.2, while the provisions for the ITS-S 6LoWPAN nodes deployed in both central and personal ITS subsystems are not specified in this document, nothing prevents the adaptation of 6LoWPAN networking to these subsystems.

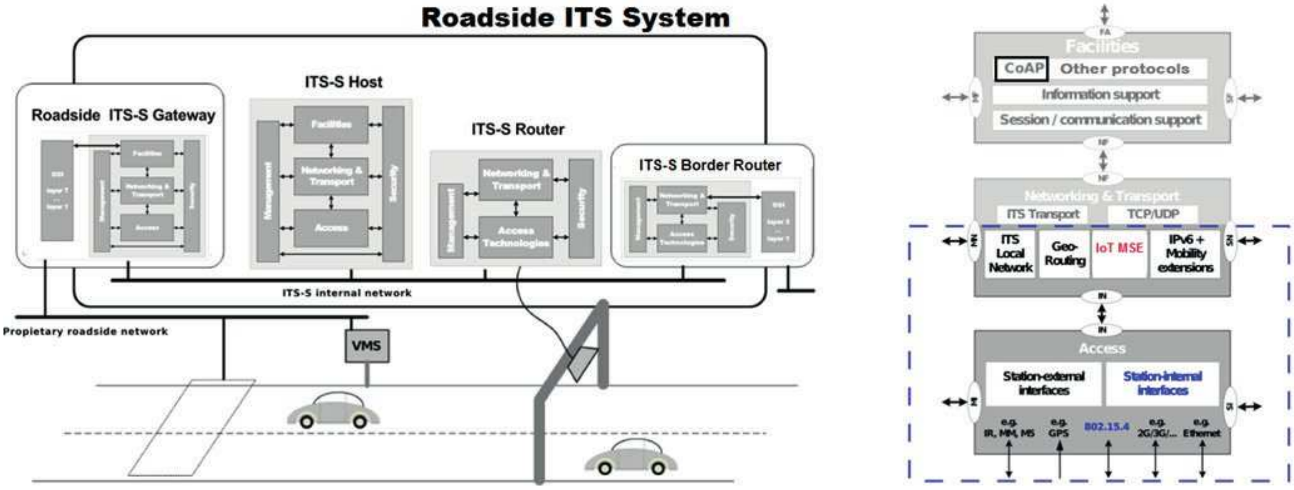

Figure 4 — Extended road-side sub-systems (ISO 21210 and ISO 21217) including 6LoWPAN

5.2.2 ITS-S 6LoWPAN nodes deployed in roadside ITS sub-systems

In addition to 5.2.1, which applies to all ITS sub-systems the provisions in 5.2.2 apply to roadside ITS sub-systems. Figure 4 illustrates the extension of the roadside subsystem in consideration to ITS-S 6LoWPAN nodes.

A roadside ITS station may contain one or more 6LoWPAN networks.

The “ITS-S 6LoWPAN border router” will provide access to the Internet in accordance with 5.4.4. See example instantiation in ITS-SU in 5.4.

An “ITS-S 6LoWPAN access router” implemented following the provisions in 5.4.3, will eventually provide access to the roadside IPv6 LAN and the vehicular ITS sub-systems if it is also implementing the ITS-S IPv6 Access Router (ISO 21210) functions in that specific instantiation.

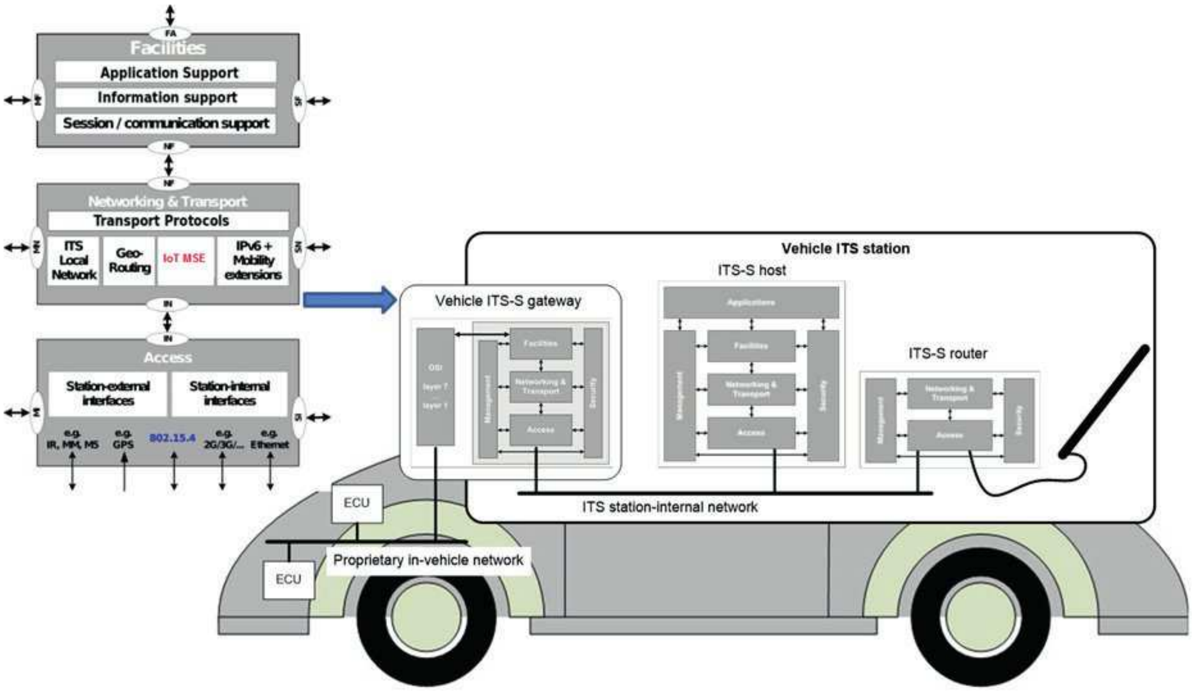

Figure 5 — Extended Vehicular ITS sub-system including 6LoWPAN

5.2.3 ITS-S 6LoWPAN LAN nodes deployed in vehicle ITS sub-systems

In addition to 5.2.1 which applies to all ITS sub-systems, the provisions of 5.2.3 apply to vehicle ITS sub-systems. Figure 5 illustrates the extension of the vehicular subsystem in consideration to ITS-S 6LoWPAN nodes.

A vehicular ITS station may contain one or more 6LoWPAN networks.

The “ITS-S 6LoWPAN border router” will provide access to the Internet in accordance with 5.4.4. See example instantiation in ITS-SU in 5.4.

An “ITS-S 6LoWPAN access router” implemented following the provisions in 5.4.4, will eventually provide access to the roadside IPv6 LAN if it is also implementing the ITS-S IPv6 Access Router (ISO 21210) functions in that specific instantiation.

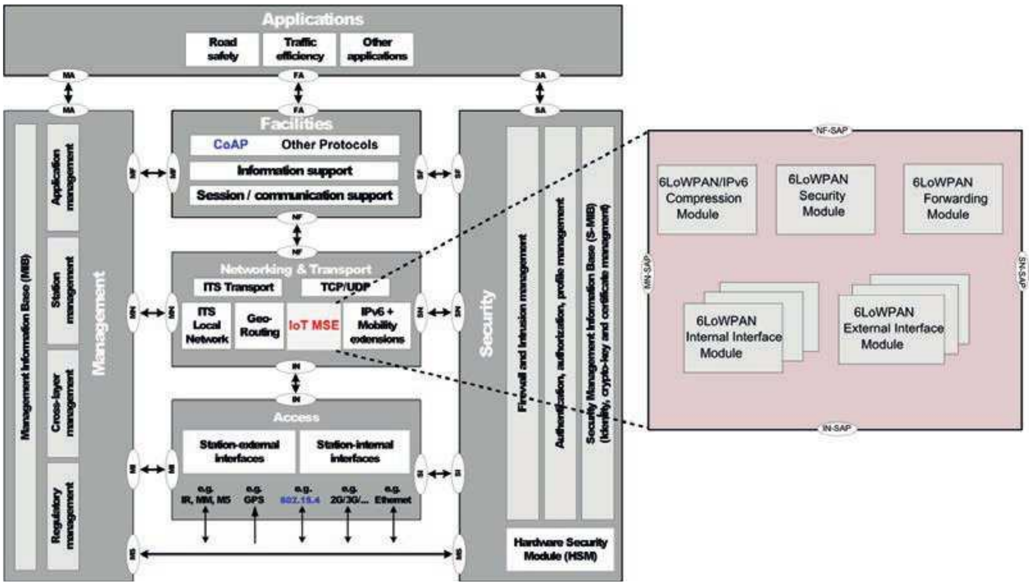

Figure 6 — IoT MSE functional modules

5.3 The IoT management service entity

5.3.1 The 6LoWPAN forwarding module

6LoWPAN Packet forwarding at the ITS Network and Transport layer permits to transmit data packets generated at higher layers in the ITS-S to other nodes in the PAN, IPv6 connected LAN(s) or the Internet.

The forwarding module is also required to receive incoming data packets from the internal/external interfaces and forward them to the next destination, either to the higher layers of the node itself or other nodes in the network.

The 6LoWPAN forwarding module consists of some adopted IP features (Stateless Address Auto-Configuration, Neighbor Discovery) needed to acquire IP parameters such as 6LoWPAN address and IP next hop determination. The packets can be forwarded either to

— the NF-SAP as defined in ISO 24102-3 if the 6LoWPAN address belongs to the receiving node,

— the 6LoWPAN internal interface module if the next hop to the destination 6LoWPAN address belongs to the ITS station itself,

— the IPv6 LAN Interface module if the next hop to the destination IPv6 address belongs to the ITS station itself, or

— the External 6LoWPAN Interface module if the next hop to the destination 6LoWPAN address does not belong to the ITS station itself.

The 6LoWPAN forwarding module receives 6LoWPAN packets from its External Interface(s), 6LoWPAN and IPv6 LAN Interface(s) or the layer above through the NF interface.

— The 6LoWPAN forwarding module shall maintain the information necessary about 6LoWPAN and IPv6 neighbors (in case of "access" and "border" routers) in order to determine the next hop towards a destination reachable through an interface to perform the forwarding function.

— Whenever the 6LoWPAN forwarding module receives a 6LoWPAN packet, it shall perform next hop determination and address resolution and forward the packet to the appropriate interface (or the layer above if intended for itself) as specified in its forwarding table.

The forwarding table shall be updated by the ITS station management entity of the ITS station reference architecture (ISO 21217).

Implementations supporting path and flow management shall

a) request default settings of the forwarding table from the ITS station management entity through the MN-SAP using MN-COMMAND.request instructions as specified in ISO 24102-6, and

b) modify the forwarding table upon the reception of MN-COMMAND.request instructions from the ITS station management entity through the MN-SAP as specified in ISO 24102-6.

NOTE 1 The default settings are particularly important so that the 6LoWPAN forwarding module can route flows originated from “non CALM-Aware” applications. Rules are configurable by stakeholders, e.g. users, device vendors, service providers, OEMs, car manufacturers. These rules are competitive factors among stakeholders, so the definitions of these policies are outside the scope of this document. The default routing procedures can be pre-registered in any manner the manufacturer wishes to implement or can be performed based on the source and destination addresses indicated in the 6LoWPAN header. Methods to define rules binding Flow Ids to applications are outside the scope of this document.

NOTE 2 The 6LoWPAN Forwarding module exchanges packets with the above layer if the 6LoWPAN source or destination address in the packet belongs to the ITS-S 6LoWPAN node. According to the ITS station reference architecture (ISO 21217), traditional OSI network and transport layers are merged into a single layer. No transport layer functions specific to CALM are necessary. If any is needed, its specification is out of the scope of this document.

In usual deployments, 6LoWPAN devices implement UDP at Transport Layer following the specifications of CoAP (depending on UDP) at Facility Layer.

All packets should be transmitted to some transport layer functions before they are transmitted through the NF interface.

5.3.2 Internal ITS-S 6LoWPAN interface module

This module aims at interconnecting all devices belonging to the same ITS station. For the communication with IPv6 peers in the LAN, the same provisions of ITS-S IPv6 LAN interface module apply (see ISO 21210:2012, 5.3.2).

The Internal ITS-S 6LoWPAN interface module shall provide a mechanism for transmitting 6LoWPAN packets between the 6LoWPAN forwarding module and the layer below through the Access and Network (IN) interface with the constraint of selecting IEEE 802.15.4-2006 as the only compatible channel for MAC technology. A detailed description on how to use the IEEE 802.15.4 access technology with ITS is provided in Annex A.

The ITS-S 6LoWPAN internal interface module shall configure its 6LoWPAN addresses according to 5.5 “6LoWPAN Address Configuration”. Neighbor discovery (as optimized from the IPv6 corresponding protocol, standardized in IETF RFC 4861) is discussed in IETF RFC 6775. The example included in 5.5 is also applicable to the Neighbor Discovery function.

5.3.3 External 6LoWPAN interface modules

The “external 6LoWPAN interface” module shall provide a mechanism for transmitting 6LoWPAN packets to the Internet. The same provisions of ITS-S IPv6 external LAN interface module apply (see ISO 21210:2012, 5.3.3).

5.3.4 6LoWPAN/IPv6 Compression module

Apart from compressing/decompressing the IPv6 packet being transmitted in accordance to IETF RFC 6282, the 6LoWPAN compression module shall also implement a routing strategy such as in IETF RFC 6550. All routing functionalities are performed within this module.

5.3.5 6LoWPAN/IPv6 security module

Generally speaking, communication security must ensure confidentiality, integrity and authentication between two peers interconnected through the Internet.

When one of the peers is part of a 6LoWPAN, there can be issues related to the constraints both at node (i.e. RAM footprint, computational overhead) and network levels (i.e. increased number of packets exchanged through the network).

Although IEEE 802.15.4-2006 guarantees host-to-host integrity and confidentiality with hardware-implemented protocols (e.g. AES-CCM-128), there can be security breaches when end-to-end transmissions in multi-hop topologies must be considered. Moreover, the IEEE standard does not consider how to secure MAC headers and does not detail how the keys will be distributed to all nodes.

Therefore, in 6LoWPAN, the adoption of security protocols at networking layer has been considered. To fulfil the full interoperability with the conventional Internet, solutions based on IPsec (IETF RFC 4301, which turns to be mandatory in IPv6) have been explored as candidate IETF standards for LoWPANs[1].

The ITS-S security module shall carry out the following actions:

a) communicates with the security entity through the SN-SAP interface;

b) communicates with other modules in the IoT MSE functional block;

c) enables the security protocols for the required security services;

d) reports available 6LoWPAN security capabilities to the security entity through the SN-SAP.

In this document, it is assumed that symmetric cryptography (with pre-shared set of keys) is suited to the set of applications and services which can be accomplished by a 6LoWPAN definitely not providing the ITS with safety-critical services.

5.3.5.1 Addressing security issues in 6LoWPAN Networks

The 6LoWPAN security module could utilize the IP security (IPsec) technological solution. The security module implementation must support an End-to-End (E2E) communication between an ITS-6LoWPAN node and other nodes. In 6LoWPAN, this is achieved using the Next Header Compression (NHC) mechanism described in IETF RFC 6282. If the IPsec solution is adopted, the security module shall be implemented to support either the IPsec's Authentication Header (AH, defined in IETF RFC 4302) and/or the Encapsulation Security Payload (ESP, defined in IETF RFC 4303). The first protocol allows for authentication and integrity, whereas the latter enables for confidentiality (and optionally integrity and authentication if AH is not adopted).

5.3.5.2 6LoWPAN with compressed IPsec

Considering that 6LoWPAN is an adaptation layer of IPv6 in low-rate PANs, IPsec could be a technological solution suited to be ported to 6LoWPAN. In order to link IPsec header compression with 6LoWPAN, IETF RFC 6282 defines the general format of NHC that can be used to encode IP extension headers. IETF RFC 6282 defines an NHC encoding for IPv6 Extension Headers (NHC_EH) shown in Figure 7 that can be used to link uncompressed AH and ESP headers to the 6LoWPAN header compression.

```
  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| 1 | 1 | 1 | 0 |     EID     |NH |
+---+---+---+---+---+---+---+---+
```

Figure 7 — LOWPAN NHC encoding for IPv6 Extension Header

The working draft[1] suggests making use of the two unassigned values of EID to consider compressed security header like AH (see NOTE) and ESP.

NOTE LoWPAN NHC for AH.

Example Authentication Header using the LoWPAN_NHC.

6LoWPAN can be used to compress a significant number of bits in AH as shown in the example in Figure 7. The next header is decided based on the value of NH bit in the IPv6 Extension Header Encoding in IETF RFC 6282. The compressed IPsec draft proposes to always elide the length field. The payload length field (the length of AH header in 32-bit words units minus “2” as in IETF RFC 4302 in the AH header is always elided, as it can be inferred from the lower layers: either from the IEEE 802.15.4-2006 header or the 6LoWPAN header. The size of the Integrity Check Value (ICV) can be obtained from the security parameter index (SPI) value because the length of the authenticating data depend on the algorithm used and are fixed for any input size. The RESERVED field in the AH header is also always elided. The SPI and sequence number (SN) are compressed using the proposed NHC encoding for the AH header shown in Figure 8 and are explained below.

```
  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| 1 | 1 | 0 | 1 |  SPI  |  SN   |
+---+---+---+---+---+---+---+---+
```

Figure 8 — LOWPAN NHC encoding for AH

— The first four bits in the NHC AH represent the NHC ID is defined for AH. These are set to 1101.

— If SPI = 00: the default SPI for the IEEE 802.15.4 network is used and the SPI field is omitted. The default SPI value could be set to 1. This does not mean that all nodes use the same security association (SA), but that every node has a single preferred SA, identified by SPI 1. If SPI = 01: the least significant 8 bits of the SPI are carried inline; the remaining 24 bits are elided. If SPI = 10: the least significant 16 bits of the SPI are carried inline; the remaining 16 bits are elided. If SPI = 11: All 32 bits of the SPI are carried inline.

— If SN = 00: the least significant 8 bits of sequence number are carried inline. The remaining bits are elided. If SN = 01: the least significant 16 bits of the SN are carried inline; the remaining 16 bits are elided. If SN = 10: the least significant 24 bits of the SN are carried inline; the remaining 8 bits are elided. If SN = 11: All 32 bits of the SN are carried inline.

When used in 6LoWPAN, AH calculates the ICV on the uncompressed IP header, thus allowing authenticated communication with Internet hosts. The minimum length of a standard AH, supporting the mandatory HMAC-SHA1-96 (*IETF RFC 4835*), consists of 12 bytes of header fields plus 12 bytes of ICV. Figure 9 shows a sample NHC compressed IP/UDP packet secured with AH. Using NHC encoding for the AH it is possible to reduce the AH header overhead from 24 bytes to 14 bytes: 1 byte of next header, 1 byte of length, 2 bytes of Reserved field, 4 bytes of SPI, and 2 bytes of sequence number. However, two additional bytes are used to define NHC_EH and NHC_AH. Therefore, in the best case, with AES-XCBC-MAC-96 (*IETF RFC 3566*) or HMAC-SHA1-96 ciphers (when 12 bytes are used for ICV), applying NHC encoding for AH saves 8 bytes in each data packet secured with IPsec AH.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   octet 1      |   octet 2      |    octet 1     |    octet 1    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         LOWPAN_IPHC             |  Hop Limit     | Source Address|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Source Address|      Destination Address         | LOWPAN_NHC_EH |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| LOWPAN_NHC_AH |       Sequence Number            |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                +
|                                                                 |
|         Integrity Check Value-ICV (Variable)  +-+-+-+-+-+-+-+-+
|                                                | LOWPAN_NHC_UDP|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Source Port    |  Dest Port     |    Checksum    |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                +
|                                                                 |
+                                                                 +
|                     UDP Payload (Variable)                      |
+                                                                 +
|                                                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9 — Sample NHC compressed IP/UDP packet secured with AH

Similar to AH, the LoWPAN NHC encoding for ESP is possible; the security parameter index, the sequence number, the next header fields and the NHC ID for ESP can be encoded. The minimum ESP overhead without authentication is 10 bytes (IETF RFC 4303), after optimal compression this header overhead can be reduced to 6 bytes, considering that two bytes are used for NHC_EH and NHC_ESP. ESP also includes an Initialization Vector(IV), which is equal to the size of an encryption block; 16 bytes in the case of AES. If authentication is enabled in the ESP, additional 12 bytes of ICV are also required.

5.4 Modules implemented in ITS-S 6LoWPAN nodes

5.4.1 to 5.4.4 identify which of the modules specified in 5.3 shall be implemented for each type of "ITS-S 6LoWPAN node" ("6LoWPAN Access router", "6LoWPAN Ad-hoc router'', "6LoWPAN Border router", "6LoWPAN Host", note that the term "Host" and "Router" are as defined in ISO 21217). The basic 6LoWPAN functions (such as 6LoWPAN addressing or transmission over IEEE 802.15.4) are omitted because these are features with which all 6LoWPAN nodes shall conform in order to be in accordance with IETF RFC 4944 and IETF RFC 6282.

In order to simplify the description of the modules implemented in an ITS-SCU, a new protocol block called the Internet of Things Management Service Entity (IoT-MSE) is defined as shown in Figure 10. This new protocol block shall inherit all the IPv6 functionalities (i.e. IPv6 functional modules) specified in ISO 21210 for the Internet Management Service Entity (I-MSE). As an example supposing an instantiation of an ITS-SCU in a border router that is residing on the edge of a 6LoWPAN network and connected to the Internet or to other ITS-S, the BR in this specific instantiation shall perform all the required functions specified within the I-MSE together with the necessary IoT MSE related functions. If on the other hand the ITS-SCU is instantiated in a 6LoWPAN Host, this reduced function device shall only be required to perform a few selected functionalities defined in the IoT MSE.

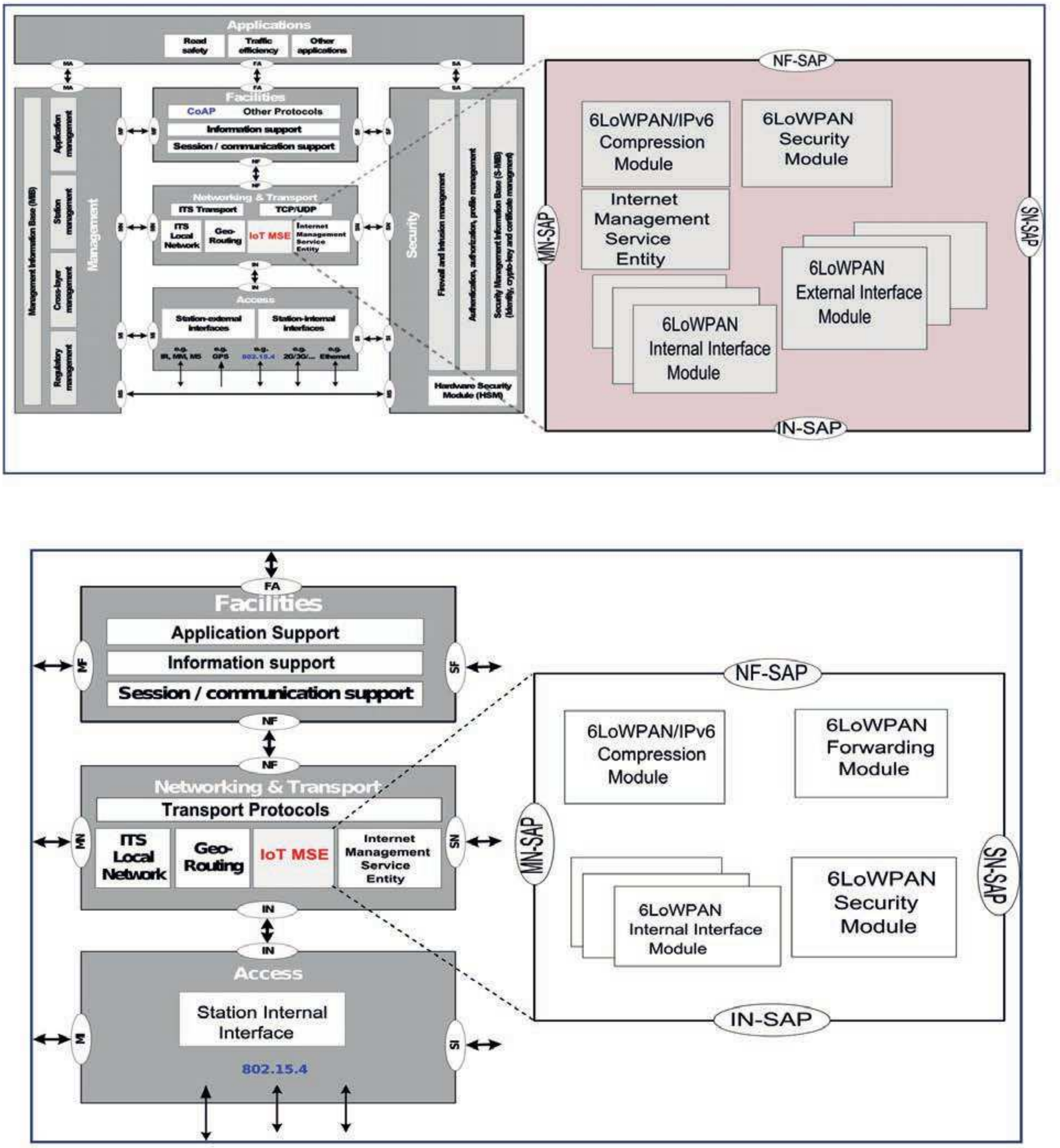

Figure 10 — ITS Station Unit: Modules implemented in BR (ITS-SCU) and Host (ITS-SCU)

Figure 10 depicts an example ITS Station, which includes an ITS-SCU as a Host and an ITS-SCU as a border router. Note that this configuration may include one or more ITS-SCUs and altogether making up an ITS-Station Unit (ITS-SU). The BR functionality may provide connectivity to other ITS communication nodes over both its internal and external networks.

In addition to the IoT MSE functionality, all other IPv6 and mobility extension related functions needed by a BR are described in ISO 21210, these sets of functions are divided into various modules that may be specific to a particular instantiation of a BR depending on what network it is connected or attached to. In this document, the BR shall be capable of performing all the IoT MSE (6LoWPAN networking) functions and shall use the 6LoWPAN internal interface module to connect with any attached 6LoWPAN

Host. It will use the 6LoWPAN external interface module to connect with the internet or any other external ITS-SUs or CUs if required.

5.4.1 ITS-S 6LoWPAN host modules

"ITS-S 6LoWPAN hosts" (i.e. "Vehicle Hosts", "Roadside Hosts", "Central Hosts", as referred to in ISO 21217) shall implement only the non-routing capabilities of an ITS station and shall include the following modules:

— 6LoWPAN forwarding module;

— 6LoWPAN compression module;

— 6LoWPAN internal interface module(s);

— 6LoWPAN security module.

5.4.2 ITS-S 6LoWPAN ad-hoc router modules

The "ITS-S 6LoWPAN ad-hoc router" shall include the following modules:

— 6LoWPAN forwarding module;

— 6LoWPAN compression module;

— 6LoWPAN internal interface module(s);

— 6LoWPAN security module.

5.4.3 ITS-S 6LoWPAN access router modules

The "ITS-S 6LoWPAN access router" shall include the following modules:

— 6LoWPAN forwarding module;

— 6LoWPAN internal interface module(s);

— 6LoWPAN external interface module(s);

— 6LoWPAN security module.

There shall be a "6LoWPAN external interface" module for each communication interface.

5.4.4 ITS-S 6LoWPAN-IPv6 border router modules

5.4.4.1 General

The "ITS-S 6LoWPAN border router" shall include the following modules:

— 6LoWPAN compression module;

— 6LoWPAN internal interface module(s);

— 6LoWPAN external interface module(s);

— 6LoWPAN security module.

This node will include the Internet Service Management Entity functional block and feature a 6LoWPAN external interface module for each communication interface.

5.4.4.2 Implementation of border router

If desired in a particular implementation, the functions of the ITS-S BR can be performed by an ITS-S mobile router as described in ISO 21210. An ITS-S mobile router deployed in an ITS-S 6LoWPAN network and connected to the Internet shall implement the modules of an ITS-S 6LoWPAN-IPv6 border router in accordance with 5.4.4.

5.4.4.3 Additional IPv6 functions of border router

Any other functions required to be performed by the BR that are not specific to the 6LoWPAN network is out of the scope of this document. In addition to the IoT MSE functionalities, all other extensions to IPv6 and mobility related functions that may be required by a router and that are not specific to 6LoWPAN networking are described within the I-MSE.

5.5 The 6LoWPAN address configuration

5.5.1 General

All “ITS-S 6LoWPAN nodes” shall configure a “link-local 6LoWPAN address” on each of their 6LoWPAN interfaces following the methods specified in IETF RFC 4944. Moreover, all “ITS-S 6LoWPAN nodes” shall configure a “global 6LoWPAN address” following the methods specified in IETF RFC 4944 and IETF RFC 6282.

As an example, we will consider a message exchange as described in IETF RFC 6775 also considering Neighbor Discovery as a further service.

5.5.2 Consideration on address configuration

Rules are required to determine how addresses are allocated (either dynamically or statically), by whom, for what use, and with what lifetime. It is necessary that the uniqueness of the address and location privacy of the user be guaranteed. These are operational considerations that are outside the scope of this document.

5.5.3 Address configuration and Optimized Neighbor Discovery

Neighbor Discovery (ND) function according to IETF RFC 6775:

a) a neighbor discovery option to distribute 6LoWPAN header compression context to hosts;

b) a host address registration feature using a new option in unicast Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages;

c) multihop distribution of prefix and 6LoWPAN header compression context;

d) multihop Duplicate Address Detection (DAD), which uses two new ICMPv6 message types. DAD is not necessary if EUI-64-based IPv6 addresses are used, since they are unique.

NOTE Functions c) and d) could be substituted or performed by any routing protocol that provides good alternative mechanism to achieve the same overall effect.

5.5.4 Examples: Message Exchange

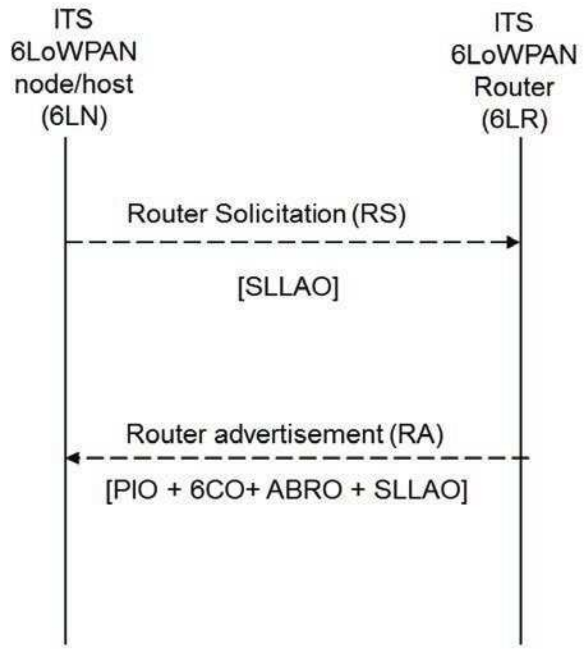

Figure 11 — Basic router solicitation/router advertisement exchange between a node and a 6LR

Figure 11 and Figure 12 show example message exchanges between an ITS 6LoWPAN node (6LN) and ITS 6LoWPAN (ad-hoc) router (6LR) and 6LoWPAN border router (6LBR). The exchanges use the ND Message options defined in IETF RFC 6775:

a) address Registration Option (ARO), 6LoWPAN Context Information option (6CO), and Authoritative Border Router option (ABRO);

b) duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC).

In Figure 11, the steps listed below describe the message sequence:

— 6LN interface initializes with link-local address based on EUI-64, next it multicasts a RS message to specify its source link-layer address;

— all 6LR within direct connectivity reply with a unicast RA message for available IPv6 prefix(es);

— Host-Router interaction as described in of IETF RFC 6775:2012, Clause 3; ABRO + 6CO + Prefix information option (PIO) + other options;

— when ARO is used by hosts, an SLLAO (Source Link-Layer Address Option) as in IETF RFC 4861 must be included, and the address that is to be registered MUST be the IPv6 source address of the NS message;

— ARO and ABRO are specifically used to achieve multihop distribution of prefix and 6LoWPAN header compression context.

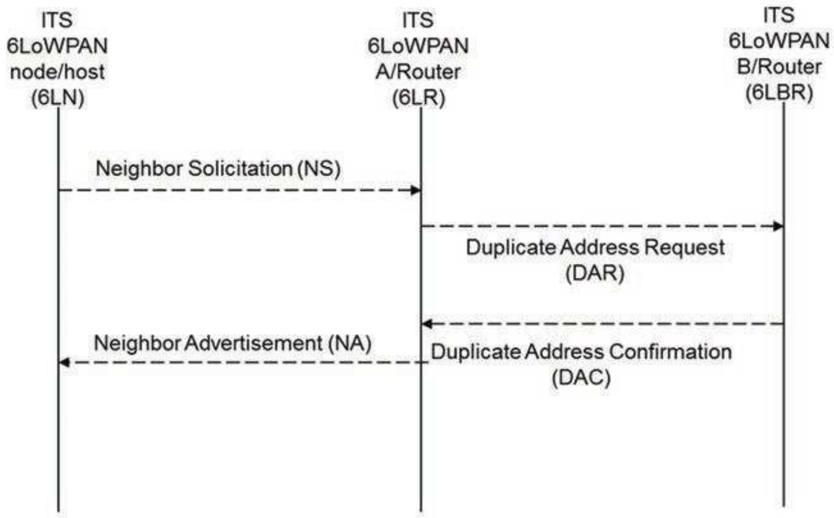

Figure 12 — Basic Router Solicitation/Router Advertisement Exchange between a Node, a 6LR and a 6LBR

In Figure 12, the steps listed below describe the message sequence.

a) After address configuration as shown in Figure 11, a unicast NS is sent to the 6LR to register its configured address.

b) Then, the 6LR sends a unicast DAR message to the 6LBR to check the status of the IPv6 address if available.

c) The 6LBR replies to the 6LR with a DAC message indicating the status of the registration. The status indicates a successful registration or a failure due to a duplicated address.

d) Finally, the 6LR sends a unicast NA message to the 6LN indicating the same status received from the 6LBR in the DAC message.

5.6 Optional features and functions

5.6.1 IPv6-IPv4 interoperability

While all ITS sub-systems are required to support IPv6 for TCP/IP-based communications, 6LoWPAN nodes deployed in an “ITS-S 6LoWPAN” can be required to communicate with legacy IPv4 nodes that will continue to operate in the Internet for several years. In addition, some access networks will remain accessible using IPv4 only, whereas existing legacy ITS services or non-ITS services, such as web servers can remain accessible in IPv4 only.

“ITS-S 6LoWPAN border routers” shall provide IPv4/6LoWPAN transition mechanisms to transmit packets over IPv4 networks.

5.6.2 IPv6 priority

The ITS-S 6LoWPAN router may implement mechanisms to ensure 6LoWPAN packets with higher priority (time critical, safety, etc.) are sent prior to packets of lower priority as instructed by the management entity. The specification of these methods is outside the scope of this document.

NOTE Consideration on Flow Label: The “Flow Label” field in the 6LoWPAN header can be set by CALM-aware applications to differentiate flows with higher priorities and to match flows to particular interfaces based on preferences exchanged between the CALM-aware applications running on “ITS-S IPv6 hosts” and the “ITS-S 6LoWPAN-IPv6border router” serving the ITS-S 6LoWPAN.

Annex A
(normative)

General usage for MAC-PHY interface: IEEE 802.15.4 Communication and Management Interface Adaptation for IoT MSE

A.1 General

This specific guideline enables the usage of the IEEE 802.15.4-2006 technology as an ITS access technology in an ITS station. It specifies the details of the "Communication Adaptation Layer" (CAL) and the "Management Adaptation Entity" (MAE) of communication interfaces specified in ISO 21218.

Wherever practicable, this guideline has been developed by referencing suitable existing standards, adopted by selection.

A.1.1 Terms and definitions

CI	Communication interface
VCI	Virtual communication interface
BC-VCI	VCI for reception from and transmission to a broadcast MAC address
UC-VCI	VCI for reception from and transmission to a unicast MAC address
CAL	Communication adaptation layer
MAE	Management adaptation entity
CIAC	Communication interface access class
TX-VCI	VCI for unicast transmission

A.2 Communication interface

The concept of a communication interface (CI) is introduced in ISO 21217 as part of the ITS station reference architecture. Interfaces, management, behavior, and parameters of CIs are specified in ISO 21218. In particular, the adaptation of a CI access technology:

— to the communication service access point IN-SAP;

— to the management service access point MI-SAP, with reference to ISO 24102-3.

Such adaptation enables a common definition of IN-SAP and MI-SAP service primitives for all kinds of access technologies. Equipment and systems complying with this document shall operate in the environment of, and to the parameters defined in ISO 21218 with additional details of this adaptation functionality dedicated to the access technology as specified in IEEE 802.15.4-2006, 1.1 and 1.2.

A.2.1 Communication Adaptation

The "Communication Adaptation Layer" (CAL) specified in ISO 21218 provides the IN-SAP towards the ITS-S networking & transport layer. The CAL can be interpreted as an extension of an existing LLC or MAC protocol.

An IEEE 802.15.4-2006 implementation according to this specification shall support both BC-VCIs, UC-VCIs and all the related procedures specified ISO 21218. The Link-ID shall be constructed as specified in ISO 21218:2014, 6.3 and C.3.

A.2.2 Management Adaptation

A.2.2.1 Management Adaptation Entity

The “Management Adaptation Entity” (MAE) specified in ISO 21218 provides the MI-SAP towards the ITS-S management entity. The MI-SAP services, service primitives and service primitive functions are specified in ISO 24102-3.

The following MI-COMMANDs presented in Table A.1 shall be supported.

Table A.1 — MI-Commands

&MXParam	Comments
CIstateChng	Allows the ITS-S management entity to request a change of CI-state.
VciCmd	Allows the ITS-S management entity to request creation of a UC-VCI, to reset a UC-VCI, and to delete a UC-VCI.

The MI-REQUESTs presented in Table A.2 shall be supported.

Table A.2 — MI-REQUESTs

&MXParam	Comments
Events21218	Allows the CI to report events to the ITS-S management entity.

A.2.2.2 Mapping of IEEE 802.15.4-2006 connection states to ISO 21218 CI states

A CI with IEEE 802.15.4 access technology according to this specification shall support all the CI states; not-existent (0), existent (1), registered (4), active (8), connected (16), suspended (64) and inactive (128) and follows the procedure of CI state machine in ISO 21218:2014, Figure 4.

A.2.2.3 Connection and disconnection procedure

a) Connection of a CI is a process that depends on the CI access class. The IEEE 802.15.4-2006 shall conform to the CI access class “CIAC-1” specified in ISO 21218:2014, Table 2. For CI access class “CIAC-1”, connection is automatically established upon first usage of a TX-VCI or upon reception of a frame from a peer station.

b) Disconnection of a CI is a process that depends on the CI access class. See the state machine in ISO 21218:2014, Figure 4. For CI access class “CIAC-1”, disconnection is performed upon the situation that no more TX-VCI with a relation to a peer station are known.

A.2.3 CI parameters

A.2.3.1 General

IEEE 802.15.4-2006 CIs shall support the I-Parameters presented in Table A.3 and Table A.4, and all I-Parameters identified in ETSI TS 102 760-1 V1.1.1 (2009-11) as mandatory.

NOTE In the above sentence, the term “support” means that the parameters can be accessed by the ITS-S management entity, and contain the information as specified in ISO 21218.

A.2.3.2 IEEE 802.15.4 specific parameters

Table A.3 — IEEE 802.15.4 Specific I-Parameters

I-Parameter name/ ASN.1 Type	Description and detail specification
CommProfile/ `CommProfile`	See Table A.4
CIclass/ `CIclass`	Communication interface class with value CIC-I1
CIaccessClass/ `CIaClass`	CI access class with value CIAC-1
MedType/ `MedType`	Identifies the type of access technology, i.e. IEEE 802.15.4. The value assigned by the ISO 21218 registry and published on http://standards.iso.org/iso/21218/ is"ISO 19079" = 11.

A.2.3.3 Communication profile parameters

The I-Parameters specified in ISO 21218 and presented in Table A.4 shall be used as communication profile parameters of the IEEE 802.15.4-2006 access technology to be considered in I-Parameter CommProfile.

Table A.4 — IEEE 802.15.4 Communication profile parameters

I-Parameter name/ASN.1 Type	Description and detail specification
CIclass/ `CIclass`	Identifies communication interface class.
CIaccessClass/ `CIaClass`	Identifies communication interface access class.
MedType/ `MedType`	Identifies the type of access technology, i.e. IEEE 802.15.4.
Connect/ `Connect`	Identifies whether a CI connects to the network service automatically or manually upon request by the user. Default value shall be automatic (0).
CommRangeRef/ `Distance`	Estimate of size of communication zone. NOTE Value is derived from TXpower, RXsensitivity and the properties of the reference station. To be calculated by the MAE.
RXsensitivity/ `RxSens`	Threshold to detect incoming communication (in dBm). The representation considers the highest sensitivity of 0 dBm presented by the value 0, and the lowest sensitivity of -255 dBm presented by the value 255.
TXpower/ `TxPower`	Transmission power (in dBm). The representation considers the lowest power level of -128 dBm presented by the value 0, and the highest power level of +127 dBm presented by the value 255.
TXpowMax/ `TxPowMax`	Medium-specific reference number of maximum allowed transmit power. Regional regulations may prevent to use large amplified transmissions.
PeerRXpower/ `PeerRXpower`	Medium-specific reference number of RX power as estimated at the peer station.
DataRate/ `DataRate`	Identifies the data rate in the link in units of 100 bit/s.
DataRateNW/ `DataRateNW`	Identifies an estimate of average data rate available at the IN-SAP in 100 bit/s
DataRatesNW/ `DataRatesNW`	Identifies minimum and maximum values of I-parameter DataRateNW
BlockLength/ `INTEGER(0..65535)`	Identifies the maximum supported length of LPDUs in integer multiples of an octet. It is equal to 127.

Table A.4 *(continued)*

I-Parameter name/ASN.1 Type	Description and detail specification
TotalBatteryEnergy/ `TotalBatteryEnergy`	Identifies the amount of energy of the prescribed battery pack. xx = c-totalBatteryEnergy
FrequencyBand/ `FrequencyBand`	Identifies the frequency band in the ISM: 2 stands for the 2.4GHz band, 1 stands for the 915MHz band, and 0 stands for the 868MHz band. xx = c-frequencyBand
ChannelParam/ `ChannelParam`	ChannelParam presents k (see below): Fc = 868.3 (MHz) for k = 0; Fc = 906 + 2 (k – 1) (MHz) for k = 1, 2, ..., 10; Fc = 2405 + 5 (k – 11) (MHz), for k = 11, 12, ..., 26 xx = c-channelParam

Annex B
(normative)

ASN.1 module

B.1 Overview

The following ASN.1 module is specified in this annex:

— **CALM6lowpan** `{ iso (1) standard (0) 6lowpan (19079) asnm-1 (1) }`

In case the ASN.1 specifications given in this annex are not compliant with illustrations or specifications provided elsewhere in this document, the specifications given in this annex shall prevail.

B.2 Module CALMfntp

This module specifies ASN.1 type definitions together with useful ASN.1 value definitions.

It imports ASN.1 definitions from the module specified in ISO 21218.

```
CALM6lowpan { iso (1) standard (0) 6lowpan (19079) asnm-1 (1) }
DEFINITIONS AUTOMATIC TAGS::=BEGIN
IMPORTS
IPARAM, I-ParamNo FROM CALMllsap {iso(1) standard(0) calm-ll-sap(21218) asnm-1 (1)
version1 (1)}
;
TotalBatteryEnergy ::= SEQUENCE{
   maxEnergy        MaximumBatteryCapacity,
   actualStatus     BatteryEnergyStatus
   }
MaximumBatteryCapacity ::= INTEGER{
   zeroAmpHour               (0),
   oneHundredMilliAh         (1),
   twoHundredMilliAh         (2),
   oneAh                     (10),
   tenAh                     (100),
   twentyfiveAh             (250)
   } (0..255) -- max capacity in steps of 100 mAh
BatteryEnergyStatus ::= INTEGER{
   zeroPercent               (0),
   halfPercent               (1),
   onePercent                (2),
   hundredPercent            (200),
   chargeFailure             (201)
   } (0..255) -- any value above 200 indicates a battery problem
FrequencyBand ::= INTEGER{
   c-866MhzBand              (0),
   c-915MHzBand              (1),
   c-2400MHzBand             (2)
   } (0..255)
ChannelParam ::= INTEGER(0..255) -- values k=0 .. 26 are currently in use.
totalBatteryEnergy  IPARAM::={&paramRef c-totalBatteryEnergy, &Parameter
TotalBatteryEnergy}
frequencyBand       IPARAM::={&paramRef c-frequencyBand, &Parameter FrequencyBand}
channelParam        IPARAM::={&paramRef c-channelParam, &Parameter ChannelParam}
END
```


Bibliography

[1] https://datatracker.ietf.org/doc/draft-raza-6lowpan-ipsec, Compression of IPsec AH and ESP Headers for Constrained Environments

ICS 35.240.60; 03.220.20
Price based on 25 pages