BS ISO 19080:2016

BSI Standards Publication

Intelligent transport systems — Communications access for land mobiles (CALM) — CoAP facility

bsi.

National foreword

This British Standard is the UK implementation of ISO 19080:2016.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2016

ISBN 978 0 580 86508 4

ICS 03.220.20; 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2016.

Amendments/corrigenda issued since publication

Date	Text affected

BS ISO 19080:2016

INTERNATIONAL STANDARD

ISO 19080

First edition
2016-10-01

Intelligent transport systems — Communications access for land mobiles (CALM) — CoAP facility

Systèmes intelligents de transport — Accès aux communications des services mobiles terrestres (CALM) — Équipements CoAP

Reference number
ISO 19080:2016(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 communications access for land mobile (CALM) focus on the specification of open interfaces regarding the functionality required by all relevant layers and entities of a Standard ITS station reference architecture.

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

The set of CALM 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 designed for safety of both life and property.

The fundamental advantage of the CALM concept with respect to traditional systems is the ability to support vertical handovers between the various media that can be included in a CALM system. Handover mechanisms are defined within the CALM architecture International Standard (ISO 21217), the CALM medium service access points International Standard (ISO 21218) and the CALM communication and station management International Standard (ISO 24102).

At network layer, CALM IPv6 networking ISO 21210 and CALM 6LoWPAN networking ISO 19079 determine the network protocols to support reachability at a global IPv6 address for Wireless Sensor Networks (WSNs) based on the IEEE 802.15.4 access medium.

CALM compliant 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 WSN to be dispatched to any ITS-Station. As WSNs are largely based on low-cost Component of The Shelf (COTS), IETF has started the standardization of a set of protocols at network and facility layer 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 application layer in this sense is the IETF Constrained Application Protocol (CoAP) (IETF RFC 7252), an optimized Representational State Transfer (REST) protocol built on top of the UDP transport protocol, and implementing a subset of HTTP specifications. This document specifies some facility protocols by leveraging the reachability of the WSN nodes guaranteed by the adoption of 6LoWPAN at the Network Layer, and describes how to use CoAP protocol specified by IETF in the context of C-ITS.

For a general introduction to CALM architecture, IPv6 networking and 6LoWPAN networking, the reader is referred to ISO 21217, ISO 21210 and ISO 19079, respectively.

INTERNATIONAL STANDARD ISO 19080:2016(E)

Intelligent transport systems — Communications access for land mobiles (CALM) — CoAP facility

1 Scope

This document describes the CoAP facilities 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) of individual CoAP and 6LoWPAN protocol blocks used within this document. This document does not define a new protocol, a new exchange of messages at the CoAP layer, or new data structures. It defines how protocols standardized by IETF are combined so that ITS stations can communicate with one another using CoAP. Procedures defined to share information between the CoAP layer and other components of the ITS station architecture are defined in ISO 24102 series (Management). In addition to the requirements specified within this document, a number of notes and examples are provided to illustrate CoAP main facilities.

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

ISO 24102-6[1)], *Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 6: Path and flow management*

IETF RFC 6690, *The Constrained RESTful Environments (CoRE) Link Format*

IETF RFC 7252:2014, *The Constrained Application Protocol (CoAP)*

IETF RFC 7641, *Observing Resources in the Constrained Application Protocol (CoAP)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 19079, ISO 21210, ISO 21217, ISO 21218, 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 http://www.iso.org/obp

NOTE Most of the definitions are taken from IETF RFC 7252, IETF RFC 7228 and IETF RFC 6690.

3.1
ITS-S CoAP node
device/node that implements CoAP protocol

[SOURCE: IETF RFC 7252]

1) To be published.

3.2
ITS-S CoAP Endpoint
entity participating in the CoAP protocol

Note 1 to entry: Colloquially, an endpoint lives on a "node", although "host" would be more consistent with Internet standards usage, and is further identified by transport-layer multiplexing information that can include a UDP port number and a security association.

[SOURCE: IETF RFC 7252]

3.3
ITS-S CoAP Client
originating endpoint of a request; the destination endpoint of a response

[SOURCE: IETF RFC 7252]

3.4
ITS-S Server
destination endpoint of a request; the originating endpoint of a response

[SOURCE: IETF RFC 7252]

3.5
confirmable message
message requiring an acknowledgement

Note 1 to entry: These messages are called "confirmable". When no packets are lost, each confirmable message prompts exactly one return message of type acknowledgement or type reset.

[SOURCE: IETF RFC 7252]

3.6
non-confirmable message
message not requiring an acknowledgement

Note 1 to entry: This is particularly true for messages that are repeated regularly for application requirements, such as repeated readings from a sensor.

[SOURCE: IETF RFC 7252]

3.7
acknowledgement message
message acknowledging that a specific confirmable message arrived

Note 1 to entry: By itself, an acknowledgement message does not indicate success or failure of any request encapsulated in the confirmable message.

[SOURCE: IETF RFC 7252]

3.8
reset message
message indicating that a specific message (confirmable or non-confirmable) was received, but some context is missing to properly process it

Note 1 to entry: This condition is usually caused when the receiving node has rebooted and has forgotten some state that would be required to interpret the message. Provoking a reset message (e.g. by sending an empty confirmable message) is also useful as an inexpensive check of the aliveness of an endpoint ("CoAP ping").

[SOURCE: IETF RFC 7252]

3.9
subject
resource in the namespace of an ITS-S CoAP server

Note 1 to entry: The state of the resource can change over time, ranging from infrequent updates to continuous state transformations.

[SOURCE: IETF RFC 7641]

3.10
observer
ITS-S CoAP client that is interested in having a current representation of the resource at any given time

[SOURCE: IETF RFC 7641]

4 Symbols and abbreviated terms

For the purposes of this document, symbols and abbreviated terms in ISO 21210, ISO 21217, IETF RFC 4944, IETF RFC 6282 apply.

5 Requirements

5.1 Categories

Clause 5 explains the relationship between the four categories of the requirements.

— The first category (see 5.2) contains requirements applying to all ITS-S CoAP nodes and it specifies requirements that are applicable to the different types of CoAP nodes in each ITS sub-system.

— The second category (see 5.3) contains the requirements that define the CoAP functional modules that are mandatory for the implementation of "ITS-S CoAP nodes". Two different modules are detailed.

— The third category (see 5.4) contains optional features and functions specified as one of the functional modules of the CoAP protocol block. These optional features could be combined to realize a set of ITS-S architecture depending on the specific application.

— The fourth category (see 5.5) contain requirements defining which of the CoAP functional modules specified in 5.3 and 5.4 are combined for each particular "ITS-S CoAP node" specified in 5.3.

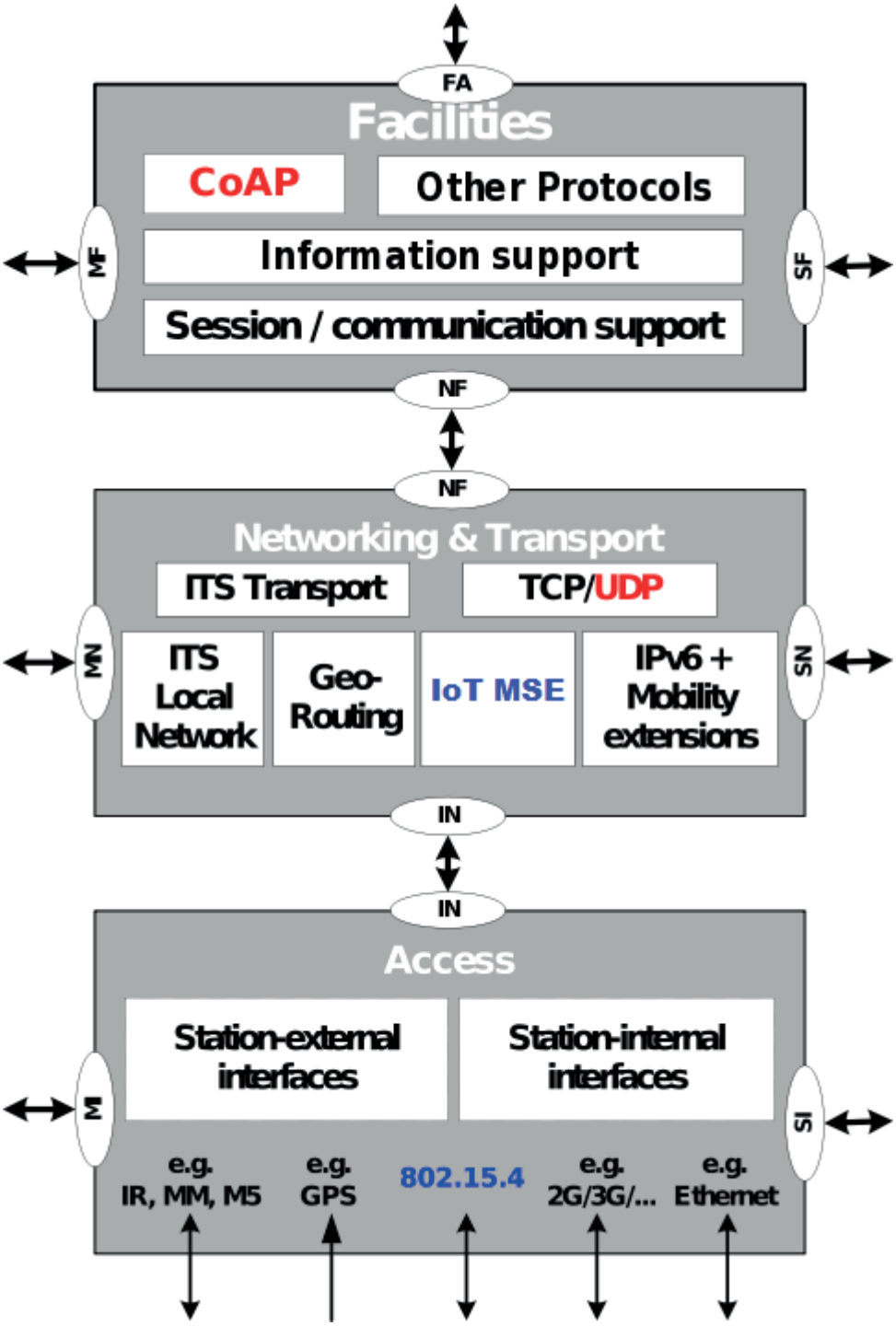


Figure 1 — Scope of this document within the architecture of an ITS-S

5.2 ITS-S nodes implementing CoAP

5.2.1 General

As CoAP was designed according to the REST architecture, it thus exhibits functionality similar to that of the HTTP protocol, it will support web style transactions originated or directed to 6LoWPAN nodes in ITS stations (ISO 19079).

For a better understanding of CoAP, the terminologies are specified in IETF RFC 7252 and the "Terminologies behind constrained-node networks" in IETF RFC 7228. These documents shall serve as the normative references for how to apply "CoAP" to ITS CALM.

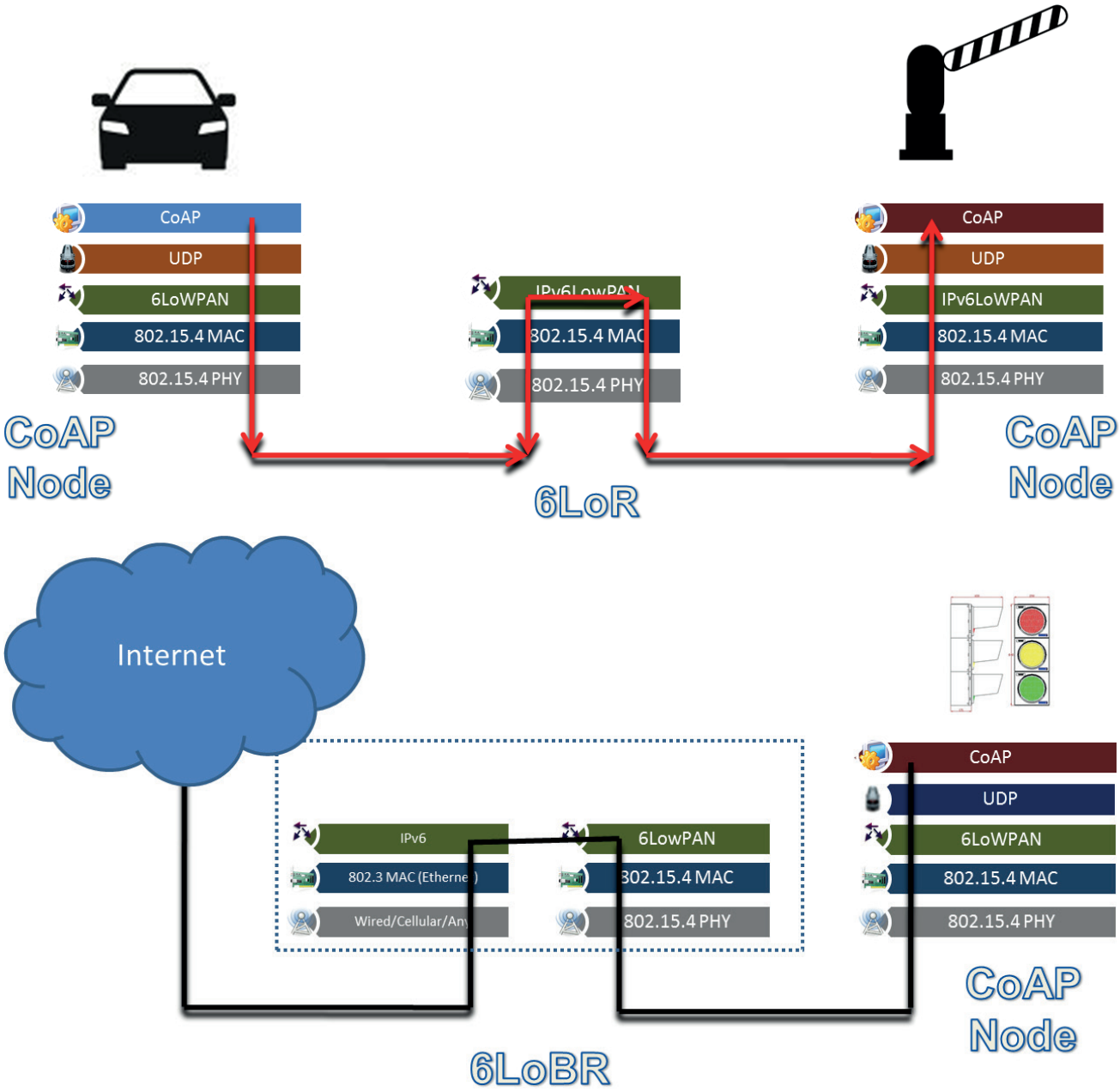


Figure 2 — CoAP based subsystem

A station implementing CoAP (in a PAN) is pictorially represented in Figure 2 together with its connections with other CoAP nodes in the same 6LoWPAN (IETF RFC 4919, IETF RFC 4944, IETF RFC 6282), eventually exploiting the multi-hop forwarding module featured by ad-hoc routers. The forwarding service established with peers of the Internet is also shown leveraging the functionality provided by a "6LoWPAN Border Router" equipped with at least two MAC interfaces.

The CoAP-based ITS stations can notably take part in the "road-side" and "vehicular" subsystems as pictorially shown in ISO 21217:2014, Figure 16, although this protocol instantiated at the facility layer does not depend on the actual network topology. The other scenarios will not be discussed in this document due to the reduced impact they provide on the C-ITS general architecture.

Although CoAP is a UDP-dependent standard applicable to every layer-3 protocol, its most popular implementation is the one connected with 6LoWPAN. The latter will be considered in the remainder of this document.

5.2.2 Requirements on all ITS-S CoAP nodes

This subclause specifies the functional requirements of all ITS stations implementing CoAP in an "ITS-S 6LoWPAN" as shown in the scenario of Figure 3. This figure depicts two possible ITS-S subsystems that utilize CoAP protocol to realize communication between constrained devices, e.g. WSNs and the internet.

An "ITS-S CoAP node" shall implement CoAP in accordance with IETF RFC 7252 and IETF RFC 6690.

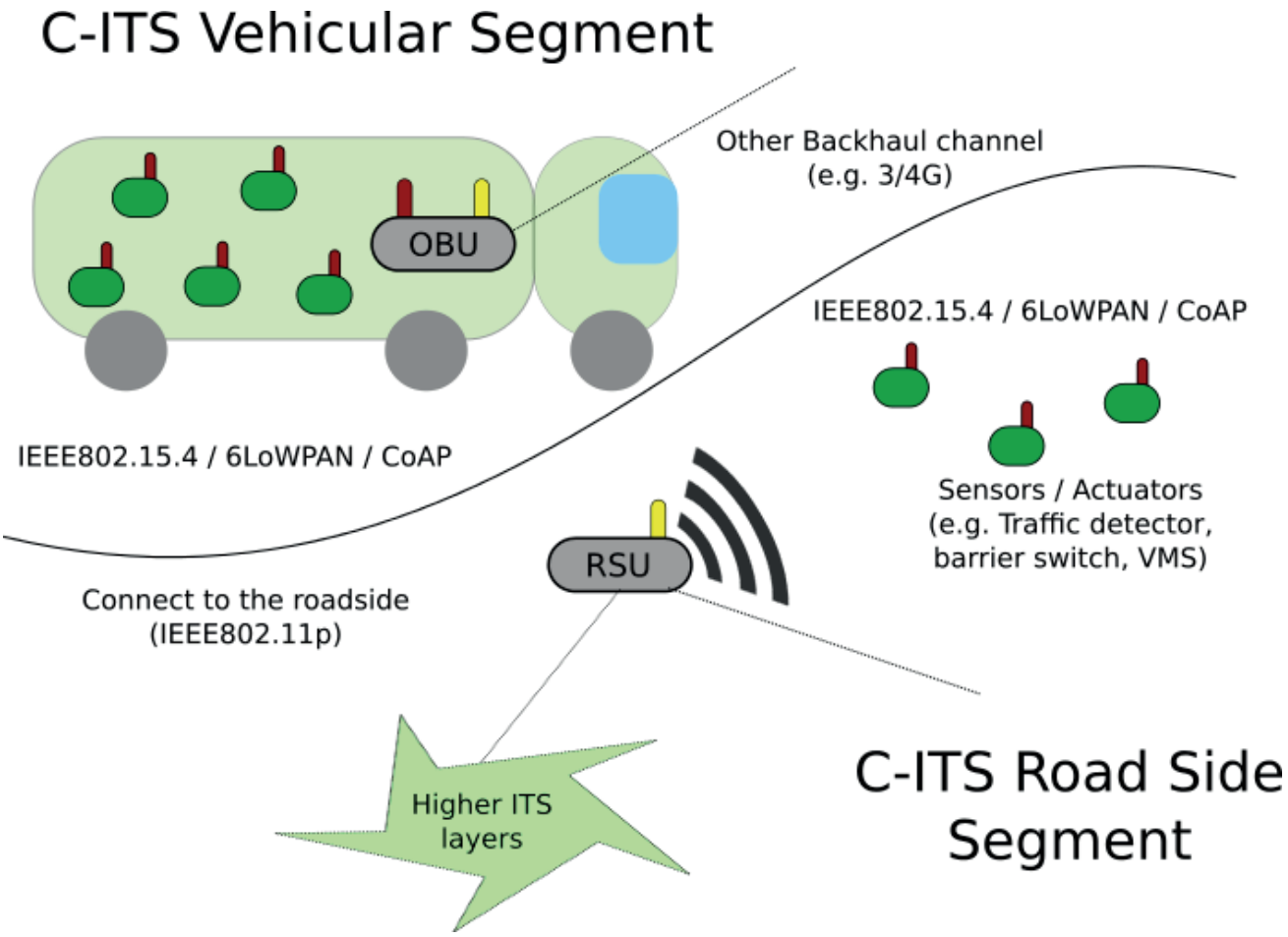


Figure 3 — Example CoAP nodes in ITS

ITS-S CoAP nodes could be used in Traffic variable message systems (VMSs), ITS weather stations and transportation and logistics applications. The network of wireless sensor nodes deployed in these categories shall be prescribed as ITS-S CoAP nodes.

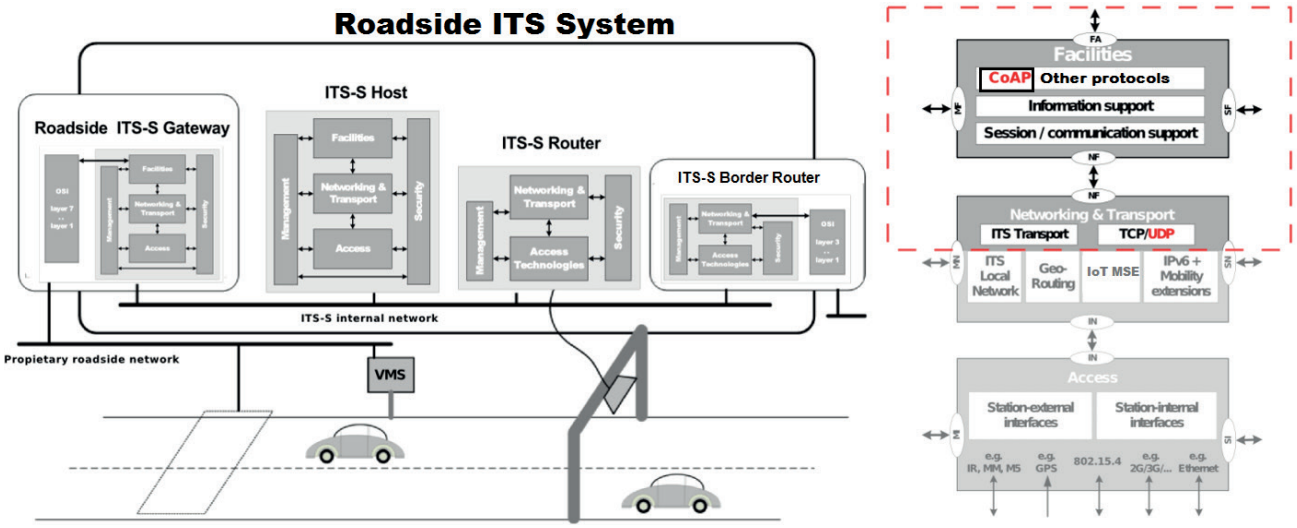


Figure 4 — Extended road-side sub-systems (ISO 21210 and ISO 21217) including CoAP

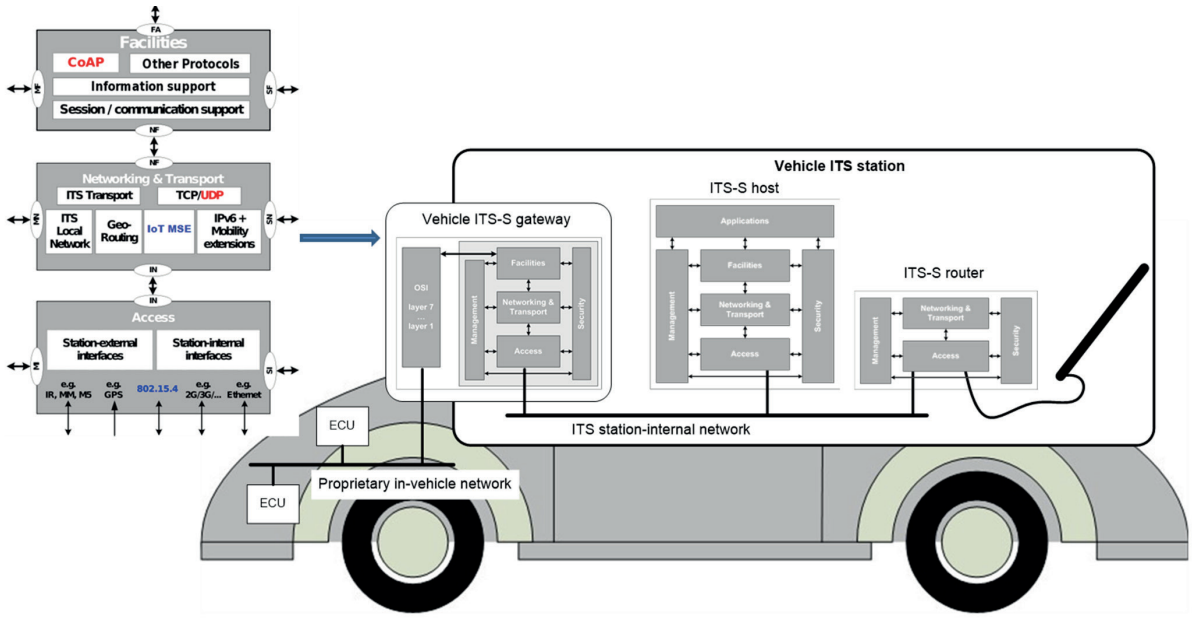


Figure 5 — Extended vehicular ITS sub-system including CoAP

In all setups (see Figures 4 and 5), the deployment will include a set of ITS CoAP nodes addressable from the internet through a ITS 6LoWPAN border router (or mobile router in the case of vehicles), as specified in ISO 19079.

5.3 CoAP functional modules

5.3.1 General

This subclause specifies what CoAP functions are required by an ITS-S CoAP node. These functions are put together in three different modules. 5.5 specifies which of these modules are required for each type of ITS-S CoAP node specified in 5.2. This separation into modules simplifies the specification of CoAP functions.

Figure 6 illustrates how these functional modules are mapped to the CoAP facilities functional block of the ITS station reference architecture.

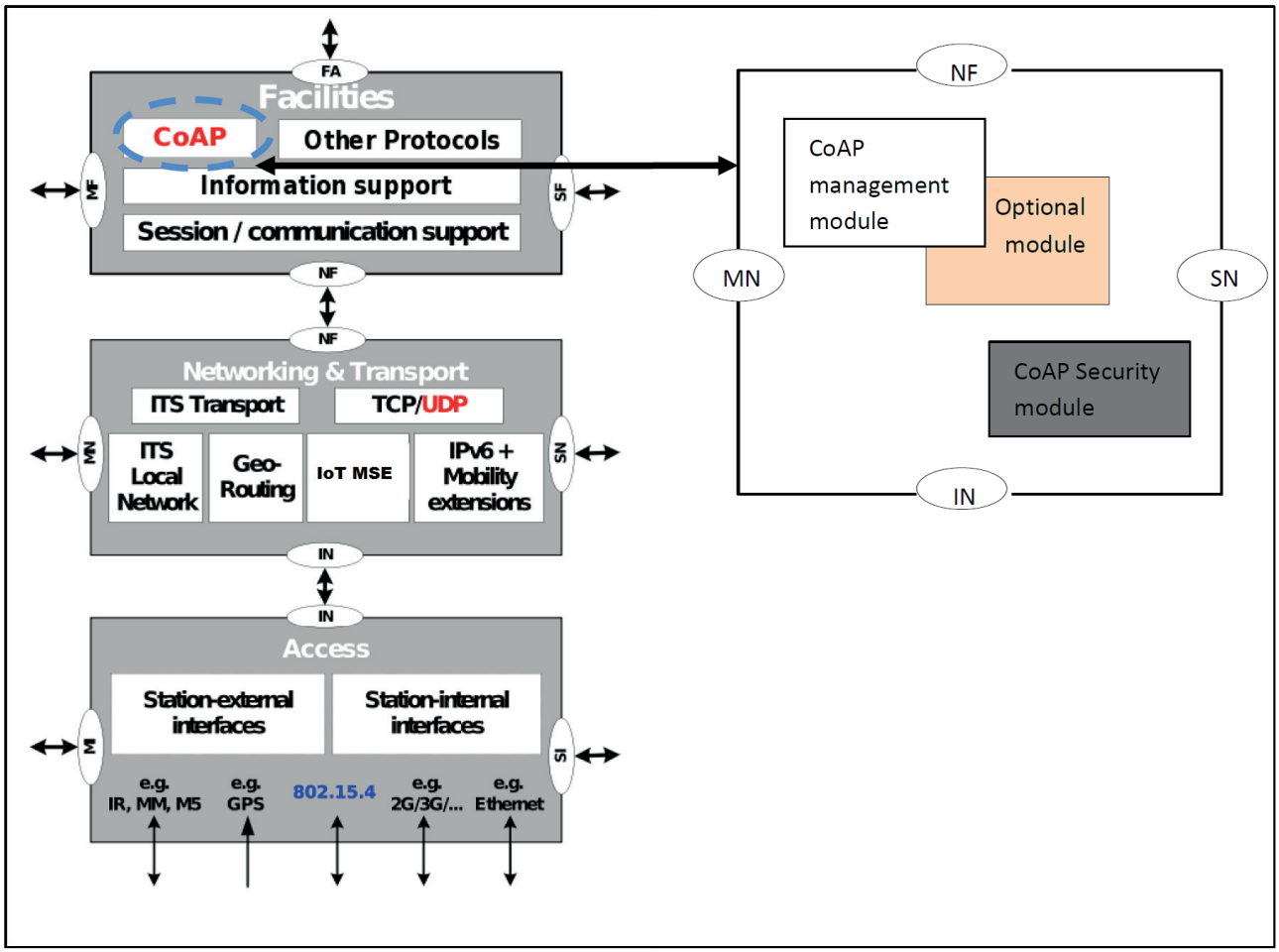


Figure 6 — CoAP functional modules

5.3.2 CoAP management module

5.3.2.1 General

The CoAP management module shall implement some functions defined in the CoRE Link Format (IETF RFC 6690) and the CoAP (IETF RFC 7252).

These functions are used by an ITS-S CoAP node to enable resource discovery, resource directory and resource observation of the available resources on an ITS-S CoAP node.

With the aim of offering generic services performing similar common actions at the ITS-S facilities layer to all applications, as standardized in ISO 21217 the CoAP management module shall:

a) request default settings from the ITS station management entity through the MF-SAP using MF-COMMAND.request instructions as specified in ISO 24102-6;

b) use the procedures defined in ISO 17429 for the exchange of information between the ITS station facilities layer and the ITS-S application processes.

5.3.2.2 Message formatting

For clarity, the mechanism of message formatting is included below.

Message Formatting: The CoAP message definition used in an ITS-S system shall be encoded in a simple binary format, which by default are transported over UDP i.e., every CoAP message occupies the data section of one UDP datagram. The CoAP message starts with a fixed-size of 4-byte header that is followed by a variable-length token value, which can be between 0 and 8 byte long. Following the Token value comes a sequence of zero or more CoAP Options in Type-Length-Value (TLV) format, optionally followed by a payload that takes up the rest of the datagram. Figure 6 shows an example message format (see IETF RFC 7252).

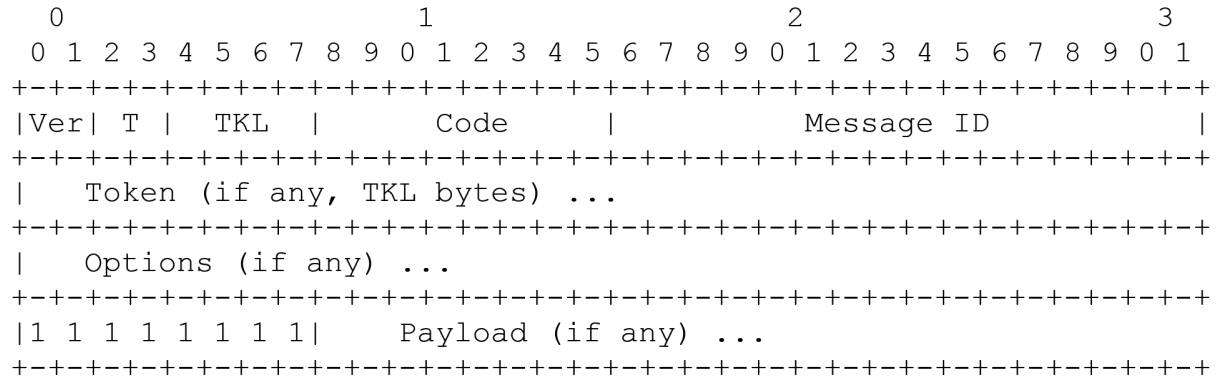


Figure 7 — Message format

The fields in the header are defined as follows:

Version (Ver): 2-bit unsigned integer indicates the CoAP version number. Implementations of this specification MUST set this field to 1 (01 binary). Other values are reserved for future versions. Messages with unknown version numbers MUST be silently ignored.

Type (T): 2-bit unsigned integer indicates if this message is of type Confirmable (0) (CON), Non-confirmable (1) (NON), Acknowledgement (2) (ACK), or Reset (3) (RST). The semantics of these message types are defined in IETF RFC 7252:2014, Clause 4.

Token Length (TKL): 4-bit unsigned integer, indicates the length of the variable-length Token field (0-8 bytes). Lengths 9-15 are reserved, MUST NOT be sent, and MUST be processed as a message format error.

Code: 8-bit unsigned integer, split into a 3-bit class (most significant bits) and a 5-bit detail (least significant bits), documented as “c.dd” where “c” is a digit from 0 to 7 for the 3-bit subfield and “dd” are two digits from 00 to 31 for the 5-bit subfield. The class can indicate a request (0), a success response (2), a client error response (4), or a server error response (5). (All other class values are reserved.) As a special case, Code 0.00 indicates an empty message. In case of a request, the code field indicates the request method; in case of a response, a response code. The semantics of requests and responses are defined in IETF RFC 7252:2014, Clause 5.

Message ID: 16-bit unsigned integer in network byte order. Used to detect message duplication and to match messages of type acknowledgement/reset to messages of type confirmable/non-confirmable. The rules for generating a message ID and matching messages are defined in IETF RFC 7252:2014, Clause 4.

5.3.2.3 Resource Discovery

With this service an ITS-S CoAP node will discover on-line resources using the CoRE Link Format (IETF RFC 6690). An ITS-S CoAP node (end-point) could be implemented either as a server or a client node. This CoAP node shall implement a resource discovery as either a unicast or multicast. When an ITS-S CoAP server node’s IP address is known unicast discovery is used to locate the entry point to the interested resource. This function is performed using a GET to “/.well-known/core” (shown in Figure 8) on the ITS-S server node, which returns a payload in the CoRE Link Format. An ITS-S CoAP node as a

client would then match the appropriate URI, resource type, interface description, content-type and media type, etc. with the specific directives of the final application.

A multicast resource discovery is useful if the ITS-S CoAP node needs to discover a resource within a limited scope, which supports a multicast. The GET request to "/.well-known/core" on the ITS-S server node is made. Same as with the unicast, the multicast resource discovery is located based on the resource type, interface description and other ITS-S specific attributes. An example implementation of a CoAP server and client targeted for logistic transportation is described in Reference [12].

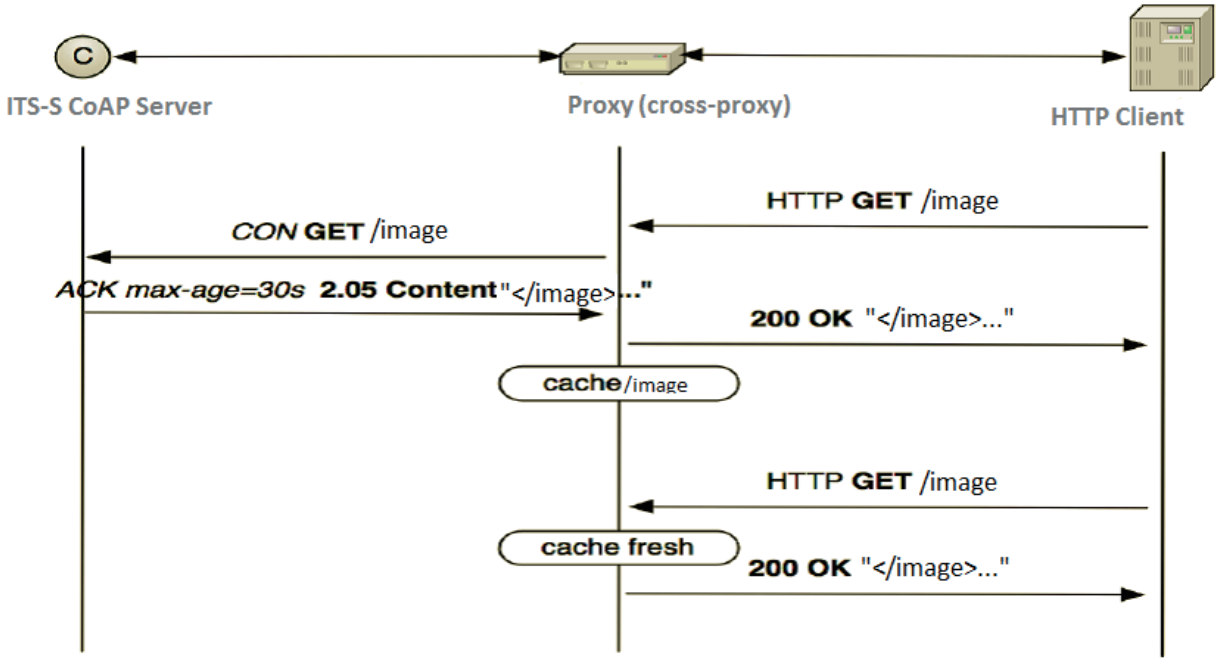


Figure 8 — Resource discovery

To increase interoperability in a CoRE environment, a CoAP endpoint shall support the CoRE Link Format of discoverable resources as described in IETF RFC 6690, except where fully manual configuration is desired.

5.3.2.4 Resource observe

The ITS-S CoAP node shall implement the CoAP core protocol specified in IETF RFC 7641 with a mechanism for an ITS-S CoAP client to "observe" a resource on an ITS-S CoAP server. The ITS-S CoAP client retrieves a representation of the resource and requests this representation be updated by the ITS-S server as long as the ITS-S client is interested in the resource.

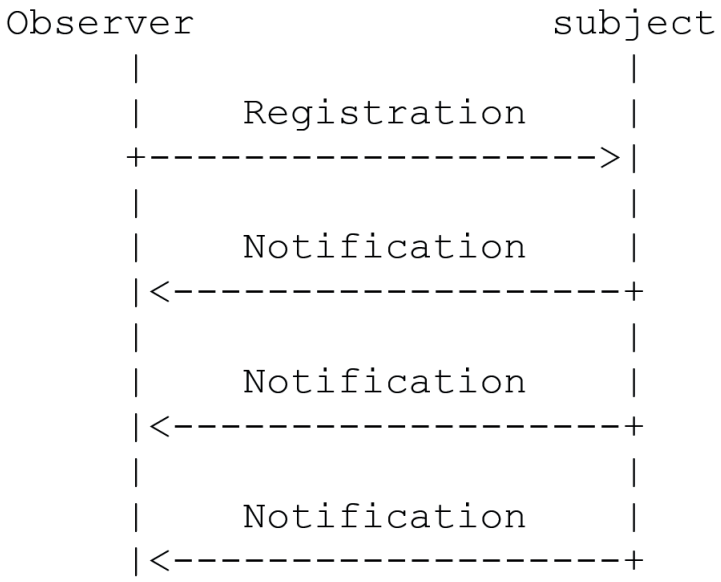


Figure 9 — Observer design pattern

As shown in Figure 9, the observer design pattern shall be realized in an ITS-S CoAP network as follows:

Subject: In the context of CoAP, the subject is a resource in the namespace of an ITS-S CoAP server. The state of the resource can change over time, ranging from infrequent updates to continuous state transformations.

Observer: An observer is an ITS-S CoAP client that is interested in having a current representation of the resource at any given time.

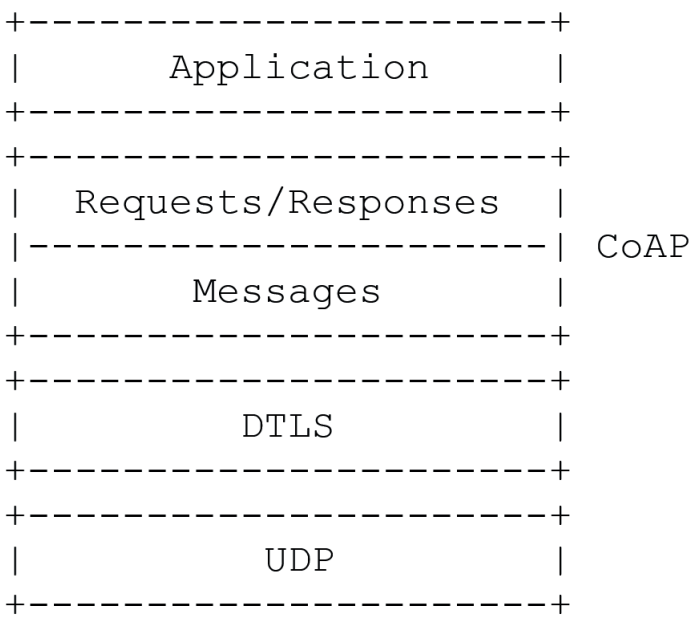
Registration: An ITS-S CoAP client registers its interest in a resource by initiating an extended GET request to the server. In addition to returning a representation of the target resource, this request causes the ITS-S CoAP server to add the client to the list of observers of the resource.

Notification: Whenever the state of a resource changes, the ITS-S CoAP server shall notify each client in the list of observers of the resource. Each notification is an additional CoAP response sent by the ITS-S CoAP server in response to the GET request and this includes a complete, updated representation of the new resource state.

NOTE **Responses sent by ITS-S CoAP server**: As notifications are just additional responses sent by the ITS-S CoAP server in response to a GET request, they are subject to caching as defined in IETF RFC 7252:2014, 5.6 (see 5.5).

5.3.3 CoAP security module

The ITS-S CoAP security module has the same security considerations as described in IETF RFC 7252:2014, Clauses 9 and 11. Just as HTTP is secured using transport layer security (TLS) over TCP, CoAP is secured using datagram TLS (DTLS) (IETF RFC 6347) over UDP (see Figure 10). DTLS is TLS with added features to deal with the unreliable nature of the UDP transport.



NOTE As shown in IETF RFC 7252.

Figure 10 — DTLS-secured CoAP

In some ITS constrained nodes (limited flash and/or RAM) and networks (limited bandwidth or high scalability requirements), and depending on the specific cipher suites in use, all modes of DTLS may not be applicable. Some DTLS cipher suites can add significant implementation complexity, as well as some initial handshake overhead needed when setting up the security association. Once the initial handshake is completed, DTLS adds a limited per-datagram overhead of approximately 13 bytes, not including any initialization vectors/nonce (e.g. 8 bytes with TLS_PSK_WITH_AES_128_CCM_8, see IETF RFC 6655), integrity check values and padding required by the cipher suite. Whether the use of a given mode of DTLS is applicable for an ITS CoAP-based application should be carefully weighed considering the specific cipher suites that may be applicable, whether the session maintenance makes it compatible with application flows, and whether sufficient resources are available on the constrained nodes and for the added network overhead.

The "/.well-known/core" resource MAY be protected, e.g. using datagram transport layer security (DTLS) following the approach of IETF RFC 6347, when hosted on an ITS-S CoAP server as per IETF RFC 7252:2014, 9.1. Some ITS-S CoAP servers might provide resource discovery services to a mix of clients that are trusted to different levels.

For a better understanding of CoAP security, the CoAP bindings are specified in IETF RFC 7252, i.e. "defining DTLS binding to CoAP" in Clause 9. This document shall serve as the normative reference on how to apply "CoAP security" to CoAP nodes in ITS CALM.

5.4 Optional module

5.4.1 General

This module specifies other features and functions that could be realized by an ITS-S CoAP node. Features such as CoAP/HTTP interoperability, resource directory and blockwise transfer could be implemented as optional features depending on the network type.

5.4.2 CoAP/HTTP interoperability

5.4.2.1 General

In an ITS-S network where information would increasingly converge to the HTTP, one important optional feature of CoAP implementation would be the HTTP interoperability. This interoperability shall ensure that:

— the URI does not change between CoAP and HTTP;

— HTTP/CoAP mapping is performed by a proxy.

HTTP shall access available resources on an ITS-S CoAP node using the same URI. For example, the ITS-S CoAP resource "//itsnode.coap.monitor.net/temperature", shall be accessed using CoAP at the URI "coap://itsnode.coap.monitor.net/temperature", and similarly using HTTP the resource would be accessed at http://itsnode.coap.monitor.net/temperature. And this mapping shall be performed by using the proxy option.

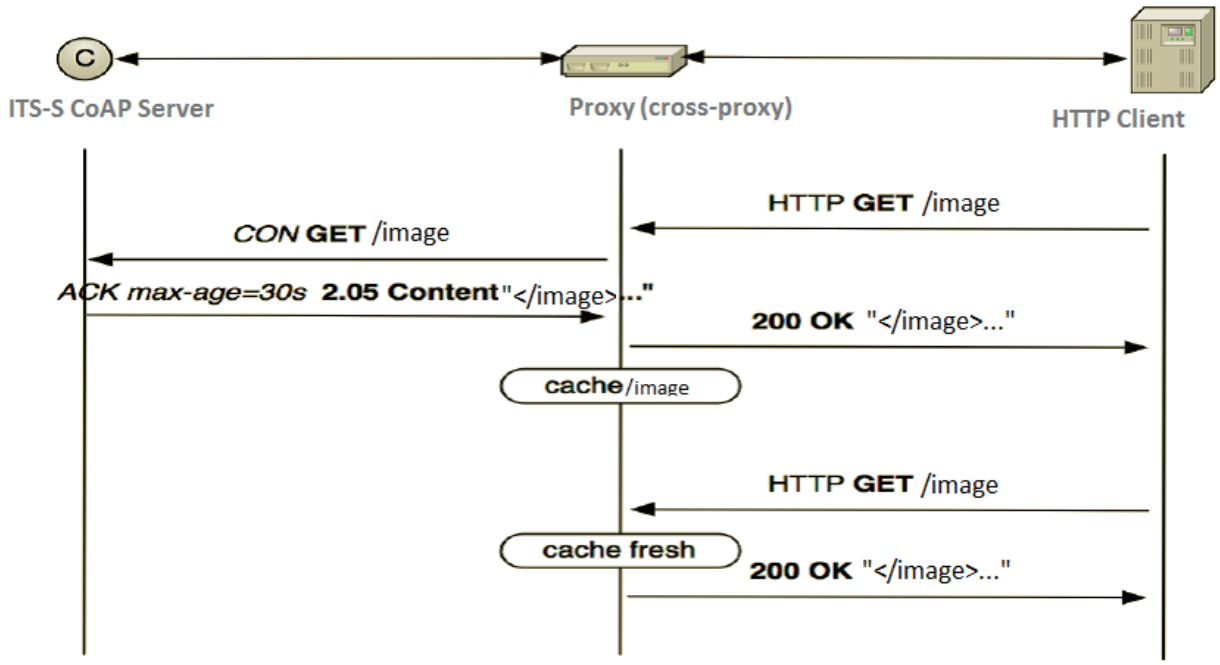


Figure 11 — Proxying and caching features

5.4.2.2 Proxy feature

As CoAP was designed according to the REST architecture it thus exhibits functionality similar to that of the HTTP protocol, it is quite straightforward to map from CoAP to HTTP and from HTTP to CoAP. Such a mapping may be used to realize an HTTP REST interface using CoAP or to convert between HTTP and CoAP. This conversion can be carried out by a cross-protocol proxy ("cross-proxy"), which converts the method or response code, media type, and options to the corresponding HTTP feature. A proxy is a CoAP endpoint (see Figure 11) that can be tasked by CoAP/HTTP clients to perform requests on their behalf. IETF RFC 7252:2014, Clause 5 more details about HTTP mapping.

The proxy referred to HTTP-CoAP cross-protocol proxy (HC)[13] shall provide a cross-protocol mapping between the HTTP-CoAP. Two kinds of HC proxies may exist:

— 1-way proxy: This proxy shall map from a client of a protocol, e.g. CoAP to a server of another protocol, e.g. HTTP and not vice versa.

— 2-way proxy (bidirectional): This proxy shall map from a client of both protocols (in this case CoAP and HTTP) to a server of the other protocol, e.g. CoAP or HTTP.

These proxies shall be realized using the below general types of proxies:

— Forward proxy (F): It is a type of proxy known by an ITS-S client (either CoAP or HTTP) used to access a specific cross-protocol server (respectively HTTP or CoAP). Main feature: server(s) do not require to be known in advance by the proxy [zero server configuration (ZSC)].

— Reverse proxy (R): It is known by the client to be the server, however for a subset of resources it works as a proxy, by knowing the real server(s) serving each resource. When a cross-protocol resource is accessed by a client, the request will be silently forwarded by the reverse proxy to the real server (running a different protocol). If a response is received by the reverse proxy, it will be mapped, if possible, to the original protocol and sent back to the client. Main feature: client(s) do not require to be known in advance by the proxy [zero server configuration (ZSC)].

— Transparent (or Intercepting) proxy (I): This proxy can intercept any origin protocol request (HTTP or CoAP) and maps it to the destination protocol, without any kind of knowledge about the client or server involved in the exchange. Main feature: client(s) and server(s) do not require to be known in advance by the proxy (ZCC and ZSC).

The HC proxy shall be placed at the edge of the constrained network in various logical locations, e.g. on the Server-side or the client-side or on the external-side.

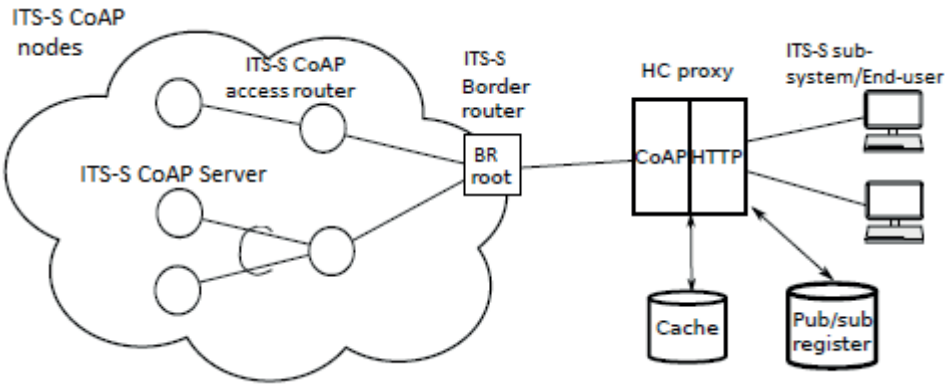


Figure 12 — Example caching architecture in ITS-S

5.4.2.3 Caching feature

Figure 12 depicts a possible use-case of the caching feature specified in IETF RFC 7252. This scheme supposes a number of ITS-S CoAP server nodes exposing a set of resources, e.g. traffic counts being queried from another ITS-S sub-system or end-user. The set of resources is gathered by the ITS-S border router. The HC proxy as discussed previously will then forward to the ITS-S sub-system or end-user the request. When HC proxy is used, any request from the end-user is intercepted by the HC proxy which handles also the eventual response from the given ITS-S CoAP server. If the proxy has a stored value which is fresh enough that is, whose lifetime is smaller than a given threshold it directly replies to the request from a remote client, without forwarding it to the ITS-S CoAP nodes. Otherwise, if the required value is not present or violates the threshold, it transfers the request to the applicable ITS-S CoAP server. Additionally, the proxy stores the sensor responses in the cache, in order to make them available for other eventual incoming requests[14].

An ITS-S CoAP node may implement the caching option in order to efficiently fulfil requests. Simple caching is enabled using freshness and validity information carried with CoAP responses as specified in IETF RFC 7252. The cache operation preserves the semantics of CoAP transfers while eliminating the transfer of information already held in the cache. Although caching is an entirely OPTIONAL feature of CoAP, we assume that reusing the cached response is desirable in ITS-S and that such reuse is the

default behaviour when no requirement or locally-desired configuration prevents it. Therefore, CoAP cache requirements are focused on preventing a cache from either storing a non-reusable response or reusing a stored response inappropriately.

5.4.3 Resource directory

In many deployment scenarios of the ITS-S system where there are constrained networks with sleeping servers or large M2M deployments with bandwidth limited access networks, it makes sense to deploy resource directory entities that store links to resources stored on other ITS-S CoAP node (servers). For example, in Figure 13, ITS-S CoAP node A and B are POSTing (registering) their link format to another ITS-S CoAP server node that supports a resource directory.

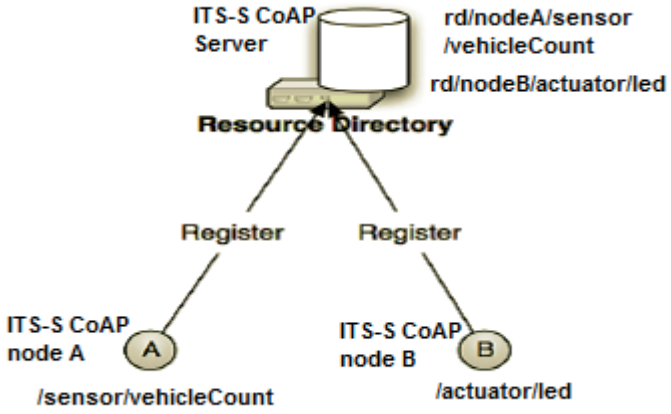


Figure 13 — Resource directory

For a better understanding of CoRE Link Formats, the terminologies are specified in IETF RFC 6690. This document shall serve as the normative reference on how to apply CoRE Link to the necessary CoAP optional features in ITS CALM.

The CoRE Link Format specified in IETF RFC 6690 can be utilized to build resource directory[15] on an ITS-S CoAP server. An ITS-S CoAP node may perform the following operations below provided the resource directory (RD) is supported by the particular implementation as used in Figure 13:

— an ITS-S CoAP node (sleeping server) can POST (register) their link format to the RD hosted on another ITS-S CoAP server;

— an ITS-S CoAP node (sleeping server) can PUT (refresh) to the RD hosted on another ITS-S CoAP server periodically;

— an ITS-S CoAP node (sleeping server) may DELETE (remove) their entry on the RD hosted on another ITS-S CoAP server;

— an ITS-S CoAP node (sleeping server) may GET (lookup) the RD hosted on another ITS-S CoAP server or lookup the resource of other ITS-S CoAP node;

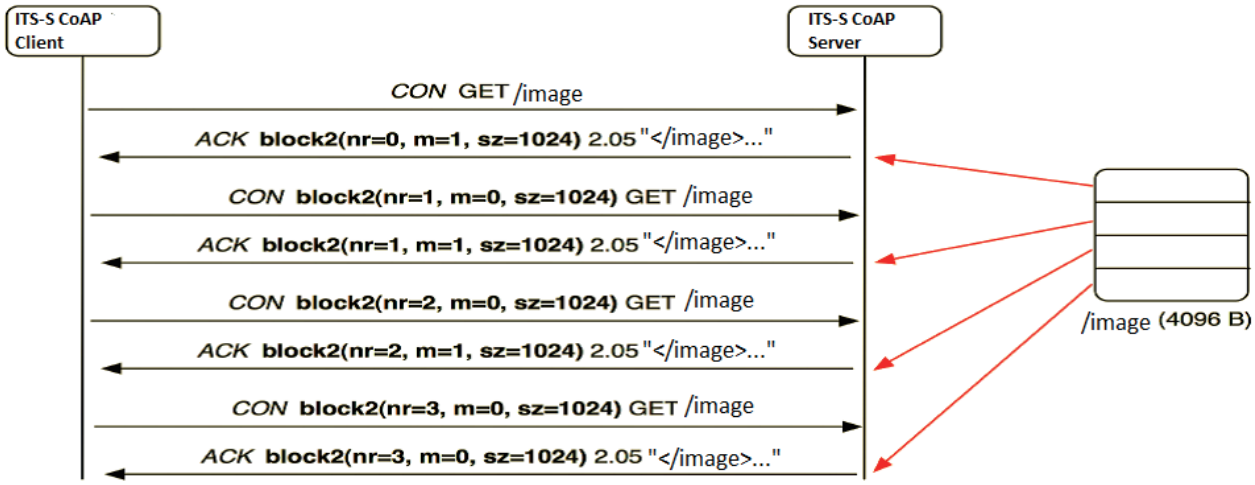


Figure 14 — Simple blockwise GET transfer

5.4.4 Blockwise transfers

The CoAP protocol is based on the datagram transport protocols such as the UDP. The UDP is limited on the maximum size of resource representation that can be transferred on the network without incurring huge IP fragmentation. However, the payload support of the UDP is still limited to 64 KiB and this is a bottleneck for constrained devices/network. An ITS-S CoAP node implemented within a constrained network inherits this payload limit offered by UDP. To avoid huge IP fragmentation or the adaptation layer fragmentation (i.e. 60 bytes to 80 bytes for 6LoWPAN) in an ITS-S the ITS-S CoAP node shall implement a blockwise transfer for transferring multiple blocks of information from a resource representation in multiple request-response pairs as defined in the internet draft of blockwise transfers in CoAP[16]. This block option allows the ITS-S server node to be truly stateless. ITS-S server node is thus able to handle each block transfer separately without a need for connection setup and in addition this function present a pair of CoAP options that enables _block-wise_access to resource representation in the ITS-S systems. Thus, allowing a minimal way to transfer large resource representation in a block-wise fashion within an ITS-S system.

In an ITS-S system when a resource representation is larger than can be comfortably transferred in the payload of a single CoAP datagram, a block option can be used to indicate a block-wise transfer as defined in RFC internet draft of blockwise transfers in CoAP. Figure 14 depicts how this feature can be implemented in an ITS. The figure consists of an ITS-S CoAP client node performing a GET operation on a resource located on another ITS-S CoAP server, the sequence of GET operation is performed using a blockwise transfer for the multiple request-response pairs.

Important statement on security consideration on blockwise transfers: Providing access to blocks within a resource may lead to surprising vulnerabilities. Where requests are not implemented atomically, an attacker may be able to exploit a race condition or confuse a server by inducing it to use a partially updated resource representation. Partial transfers may also make certain problematic data invisible to intrusion detection systems; it is RECOMMENDED that an Intrusion Detection System (IDS) that analyses resource representations transferred by CoAP implement the Block options to gain access to entire resource representations. Still, approaches such as transferring even-numbered blocks on one path and odd-numbered blocks on another path, or even transferring blocks multiple times with different content and obtaining a different interpretation of temporal order at the IDS than at the server, may prevent an IDS from seeing the whole picture.

These kinds of attacks are well understood from IP fragmentation and TCP segmentation; CoAP does not add fundamentally new considerations. Where access to a resource is only granted to clients making use of specific security associations, all blocks of that resource MUST be subject to the same

security checks; it MUST NOT be possible for unprotected exchanges to influence blocks of an otherwise protected resource.

As a related consideration, where object security is employed, PUT/POST should be implemented in an atomic fashion, unless the object security operation is performed on each access and the creation of unusable resources can be tolerated. A stateless server might be susceptible to an attack where the adversary sends a Block1 (e.g. PUT) block with a high block number: A naive implementation might exhaust its resources by creating a huge resource representation. Misleading size indications may be used by an attacker to induce buffer overflows in poor implementations, for which the usual considerations apply.

5.5 Modules implemented in ITS-S CoAP nodes

5.5.1 General

5.5.1 and 5.5.2 identify which of the modules specified in 5.3 shall be implemented for each type of "ITS-S CoAP node" ("full function device" and "reduced function device").

5.5.2 ITS-S CoAP full function device modules

The "ITS-S CoAP full function device" shall include the following modules:

— CoAP management module;

— CoAP security module;

— CoAP optional module.

This is the usual set of modules implemented in routers, namely ITS-S 6LoWPAN access routers and ITS-S 6LoWPAN border routers.

5.5.3 ITS-S CoAP reduced function device modules

The "ITS-S CoAP reduced function device" shall include the following modules:

— CoAP management module;

— CoAP security module.

This is the usual set of modules implemented in hosts, namely ITS-S 6LoWPAN hosts.

Bibliography

[1] ISO 17429, *Intelligent transport systems — Cooperative ITS — ITS station facilities for the transfer of information between ITS stations*

[2] ISO 19079, *Intelligent transport systems — Communications access for land mobiles (CALM) — 6LoWPAN networking*

[3] ISO 21210, *Intelligent transport systems — Communications access for land mobiles (CALM) — IPv6 Networking*

[4] ISO 21218, *Intelligent transport systems — Communications access for land mobiles (CALM) — Access technology support*

[5] ISO 24102-3, *Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 3: Service access points*

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

[7] IETF RFC 4944, *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*

[8] IETF RFC 6282, *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*

[9] IETF RFC 6347, *Datagram Transport Layer Security Version 1.2*

[10] IETF RFC 6655, *AES-CCM Cipher Suites for Transport Layer Security (TLS)*

[11] IETF RFC 7228, *Terminology for Constrained-Node Network*

[12] Kuladinithi K., Bergmann O., Pötsch T., Becker M., Görg C. Implementation of CoAP and its Application in Transport Logistics. In Proc.IP+SN, Chicago, IL, USA, 20111

[13] https://datatracker.ietf.org/doc/draft-ietf-core-observe/, Observing Resources in CoAP

[14] https://datatracker.ietf.org/doc/draft-ietf-core-http-mapping/, Map HTTP to CoAP

[15] Leone R., Medagliani P., Leguay J. Optimizing QoS in Wireless Sensor Networks using a Caching Platform, SENSORNETS, Barcelona, Spain, February 2013

[16] https://datatracker.ietf.org/doc/draft-ietf-core-resource-directory/, CoRE Resource Directory

[17] https://datatracker.ietf.org/doc/draft-ietf-core-block/, Blockwise transfers in CoAP

ICS 35.240.60; 03.220.20

Price based on 18 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.