INTERNATIONAL STANDARD

ISO 15784-2

First edition
2015-11-01

Intelligent transport systems (ITS) — Data exchange involving roadside modules communication —

Part 2: Centre to field device communications using SNMP

Systèmes intelligents de transport (SIT) — Échange de données impliquant la communication de modules en bordure de route —

Partie 2: Communications par dispositif du centre au terrain en utilisant le protocole simple de gestion de réseau (SNMP)

Reference number
ISO 15784-2:2015(E)

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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

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

ISO 15784 consists of the following parts, under the general title *Intelligent transport systems (ITS) — Data exchange involving roadside modules communication*:

— *Part 1: General principles and documentation framework of application profiles*

— *Part 2: Centre to field device communications using SNMP*

— *Part 3: Application profile-data exchange (AP-DATEX)*

This part of ISO 15784 deals with the use of SNMP based communications between traffic management centres and roadside modules for the purpose of configuring, controlling, and monitoring their operation.

Introduction

Background

The need for standardized communication with ITS field devices is growing around the world. A number of countries have adopted SNMP-based field device communication standards.

There is a growing view and empirical evidence that standardizing this activity will result in improved ITS performance, reduced cost, reduced deployment time, and improved maintainability. This part of ISO 15784 creates a standard for ITS field device communications based on several simple concepts:

a) maximize the use of the SNMP standards which are widely used in the management of network devices;

b) provide for the transport of data by means of serial communication, TCP/IP, UDP/IP, and other transport mechanisms used by the Internet community;

c) provide security by the various mechanisms used in the Internet community;

d) provide data definitions using the MIB format defined by the SNMP community. The MIBs for ITS device information will not be part of this part of ISO 15784 as these MIBs will be application, locale, and jurisdiction specific to meet local needs. However, a basic set of management information common to all implementations of this protocol is included.

By using this approach, agencies can specify open procurements and systems can be expanded geographically in an open and non-proprietary manner which reduces the costs, speeds the deployment, and simplifies the integration.

Overview

SNMP is a collection of well thought-out and well-proven concepts and principles. SNMP employs the sound principles of abstraction and standardization. This has led to SNMP being widely accepted as the prime choice for communication between management systems and devices on the Internet and other communications networks.

The original implementation of SNMP was used to manage network devices such as routers and switches. Since then, the use of SNMP has grown into many areas of application on the Internet and has also been used successfully over various serial communications networks.

This part of ISO 15784 includes references to four variants of the network management protocol. Three of these are versions of SNMP as defined by the Internet Engineering Task Force and the fourth is defined in this part of ISO 15784 and is based on work in the U.S.

This part of ISO 15784 does not specify any requirements that contradict or cause non-conformance to the base standards.

Document approach and layout

This part of ISO 15784 defines the following:

a) an overview of this part of ISO 15784, including conventions and architecture (Clause 6);

b) the major capabilities of this part of ISO 15784 (Clause 7);

c) the technical details of STMP (Clause 8);

d) performance requirements for entities claiming conformance to this part of ISO 15784 (Clause 9);

e) a protocol requirements list (Annex A);

f) the formal ASN.1 module for STMP (Annex B);

g) the formal definition of SNMP objects defined by this part of ISO 15784 (Annex C);

h) a primer for understanding the protocols defined in this part of ISO 15784 (Annex D);

i) example encodings of messages defined in this part of ISO 15784 (Annex E).

Intelligent transport systems (ITS) — Data exchange involving roadside modules communication —

Part 2:
Centre to field device communications using SNMP

1 Scope

1.1 General

This part of ISO 15784 specifies a mechanism to exchange data and messages in the following cases:

a) between a traffic management centre(s) and roadside modules for traffic management;

b) between roadside modules used for traffic management.

The scope of this part of ISO 15784 does not include the communication between traffic management centre and in-vehicle units, between roadside modules and in-vehicle units, in-vehicle communication, in-cabinet communication, or motion video transmission from a camera or recorded media.

This part of ISO 15784 is complimentary to ISO 15784-3, but uses a different application layer for the information exchanges to configure, control, and monitor the field traffic control roadside modules. Where ISO 15784-3 is based on the DATEX standards, this part of ISO 15784 uses an alternative approach based on SNMP with an optional extension for more efficient transmission over low bandwidth media. Both of these standards conform to the application profile requirements set forth in ISO 15784-1.

1.2 Overview

This application profile is suitable for usage when the following conditions apply:

a) when the data to be exchanged can be defined as one or more elements that can be retrieved or stored. The protocol can support a wide variety of devices and has adopted the concept of a management information base (MIB) which identifies the configuration, control, and monitoring parameters for the roadside module. This standardized approach is commonly used for network management applications for devices such as routers, switches, bridges, and firewalls. It is also used in many countries to control devices such as dynamic message signs;

b) when guaranteed, deterministic, real time exchange of data are not critical. SNMP operations are typically fairly fast, but the underlying network can cause delays in delivering messages or even lost messages; thus, the protocol is not appropriate for applications that require reliable sub-second communications;

c) for intermittent exchange of any defined data. Normal SNMP operations allow messages to be structured by combining any group of elements into a retrieval or storage request;

d) for repeated, frequent exchanges of the same message structure (with potentially different values) on even low bandwidth links. This profile supports both an efficient variant of SNMP known as STMP which allows the run-time definition of 13 messages that can be repeatedly exchanged as needed with minimal overhead;

e) for allowing a roadside module to issue exception reports when special conditions arise. This profile includes the concept of an inform message that allows an agent to notify the manager of special conditions even though the manager did not specifically request the information at the time.

Note that this part of ISO 15784 does not address the data required for each specific type of ITS device. Subsequent device communications standards are to be developed to identify the functionality of the device and the objects to manage and monitor that functionality. This part of ISO 15784 is similar to NTCIP 2301 that defines the protocols along with the objects required for controlling, operating, monitoring, and diagnosing those protocols. Other standards define device-specific objects. It is anticipated that regions will develop device MIB's that meet their specific needs.

This part of ISO 15784 will allow for open systems deployment using devices from many manufacturers providing a variety of services in a shared network environment. With such open protocols, public MIB's, and conformance to the standards, roadside modules can become interoperable among vendors and a variety of vendors can provide product in a systems environment.

2 Conformance

Conformance to this part of ISO 15784 is defined in Annex A through the definition of each feature as mandatory, optional, or conditional. Every effort has been made to make these conformance tables consistent with the body of the text, but in the case of a conflict between the Annex and the main body of this part of ISO 15784, Annex A shall take precedence.

This part of ISO 15784 explicitly identifies a number of options that an implementation may support. These are options that are likely to be encountered in deployments and are listed in this part of ISO 15784 as a convenience. The omission of a feature in this part of ISO 15784 should not be interpreted as a prohibition of its use.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 15784-1, *Intelligent transport systems (ITS) — Data exchange involving roadside modules communication — Part 1: General principles and documentation framework of application profiles*

ISO/IEC 8825-7, *Information technology — ASN.1 encoding rules — Part 7: Specification of Octet Encoding Rules (OER)*

IETF RFC 1157, *A Simple Network Management Protocol (SNMP)*

IETF RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*

IETF RFC 1910, *User Based Security Model for SNMPv2*

IETF RFC 2578, *Structure of Management Information Version 2 (SMIv2)*

IETF RFC 3411:2002, *An Architecture for Describing SNMP Management Frameworks*

IETF RFC 3412:2002, *Message Processing and Dispatching*

IETF RFC 3413:2002, *SNMP Applications*

IETF RFC 3414:2002, *User-based Security Model*

IETF RFC 3415:2002, *View-based Access Control Model*

IETF RFC 3416, *Version 2 of SNMP Protocol Operations*

IETF RFC 3417:2002, *Transport Mappings*

IETF RFC 3418:2002, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

IETF RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

IETF RFC 3826:2004, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

IETF RFC 5590:2009, *Transport Subsystem for the Simple Network Management Protocol (SNMP)*

IETF RFC 5591:2009, *Transport Security Model for the Simple Network Management Protocol (SNMP)*

IETF RFC 6353, *Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)*

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

4.1
agent
SNMP entity (4.20) that can respond to SNMP `get` and `set` requests

Note 1 to entry: An agent can also issue `report`, `trap`, and/or `inform` *messages* (4.10).

4.2
component
any equipment connected to the ITS infrastructure

Note 1 to entry: Components can be either management centre components or field components. Components in an ITS system can be supplied by more than one manufacturer.

4.3
datagram
self-contained unit of data transmitted independently of other units of data

4.4
deprecated
still valid, but is not to be used for new designs

Note 1 to entry: This is a term that is used in the `STATUS` field of MIBs to indicate that the associated *object* (4.12) no longer represents the preferred design, but the object may still be useful for backwards compatibility with legacy implementations. A deprecated object can be made *obsolete* (4.14) with the next or subsequent release of the standard.

4.5
encoding
complete sequence of octets used to represent a data value

4.6
entity
device or "thing" that will become part of an intelligent transportation system

4.7
instance
specific object implementation that is based on a definition in the component's MIB

4.8
interoperable
ability of two or more systems, or *components* (4.2) to exchange information and then to be able to use the information that has been exchanged

4.9
manager
SNMP entity (4.20) that can generate SNMP `get` and `set` requests and/or can receive `report`, `trap`, and/or `inform` *messages* (4.10)

4.10
message
structured grouping of data elements or data frames into a package of information that has been created for the purpose of communicating between *components* (4.2) or between applications

4.11
MIB view
subset of the complete set of object instances in a device MIB

Note 1 to entry: Each subset of *objects* (4.12) is associated with an SNMP community name.

4.12
object
specific, defined piece of data registered for public use on the international object identifier tree

Note 1 to entry: Objects may be defined to several different standards for use by different technology systems.

4.13
object identifier
ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node

[SOURCE: ISO/IEC 9834-1:2012, 3.5.11]

4.14
obsolete
no longer valid

Note 1 to entry: This is a term that is used in the `STATUS` field of MIBs to indicate that the associated object no longer represents the preferred design and should not be used. An obsolete object can be removed from the next or subsequent release of the standard.

4.15
protocol
set of message formats (semantic, syntactic, and symbolic rules) and the rules for message exchange between peer layer entities (which *messages* (4.10) are valid when)

[SOURCE: ISO/IEC 16500-1:1999, 3.56]

4.16
protocol data unit
unit of information communicated between network peers

[SOURCE: ISO/IEC 24791-5:2012, 4.10]

4.17
proxy agent
agent (4.1) that acts on behalf of a target entity

Note 1 to entry: A proxy agent is typically used as a translator to allow a device that does not conform with the network protocol to participate on the network.

4.18
roadside module
group of *components* (4.2) or applications installed at the roadside and that can be controlled and/or monitored by a remote entity

Note 1 to entry: Each roadside module may be subject to separate procurement against specifications which define the required functionality and interfaces.

4.19
SNMP application
internal architectural component of the SNMP architecture as defined in IETF RFC 3411

Note 1 to entry: Defined SNMP applications include the command generator, command responder, notification originator, notification receiver, and proxy forwarder.

4.20
SNMP entity
implementation of SNMP that resides in an *entity* (4.6)

4.21
tag
means of denoting the type of each ASN.1 type

5 Symbols and abbreviated terms

AES	Advanced Encryption Standard
ASN.1	Abstract Syntax Notation One
BCP	Best Current Practice
BER	Basic Encoding Rules
CBC	Cipher Block Chaining
DES	Data Encryption Standard
DTLS	Datagram Transport Layer Security
IAB	Internet Architechture Board
IPv4	Internet Protocol — version 4
ITS	Intelligent Transport Systems
MD5	Hash-based Message Authentication Code — Message Digest 5
MIB	Management Information Base
MPD	Message Processing and Dispatching
OER	Octet Encoding Rules
OID	Object Identifier
OSI	Open Systems Interconnect
PDU	Protocol Data Unit
PRL	Profile Requirements List

RFC	Request for Comments

NOTE Specifically, RFCs published by the Internet Engineering Task Force.

SHA-1	Hash-based Message Authentication Code — Secure Hash Algorithm 1
SMIv2	Structure of Management Information version 2
SNMP	Simple Network Management Protocol
`snmp`	SNMP MIB

NOTE When shown in the lower case and fixed-width font, the acronym refers specifically to the set of objects defined underneath the "`snmp`" arc of the international object identifier tree as defined in IETF RFC 3418.

SNMPv1	Simple Network Management Protocol version 1
SNMPv2	Simple Network Management Protocol version 2
SNMPv3	Simple Network Management Protocol version 3
STMP	Simple Transportation Management Protocol
STD	IAB Standard
TLS	Transport Layer Security
TSM	Transport Security Model
UDP	User Datagram Protocol
USM	User-based Security Model
UTMC	Urban Traffic Management and Control

6 Overview

6.1 Conventions

6.1.1 ASN.1

This part of ISO 15784 contains ASN.1 modules, MIBs (which are written in the form of ASN.1), and references to and explanations of ASN.1 data concepts within its text. In all cases, the ASN.1 terms are presented in a fixed width font (e.g. `such as this`) in order to distinguish these terms from normal English.

6.1.2 SNMP terminology

Terminology between the different versions of SNMP is slightly different. For the purposes of this part of ISO 15784, we adopt the terminology of SNMPv3.

6.1.3 Format

This application profile conforms to ISO 15784-1.

6.2 ASN.1 modules and MIBs

All ASN.1 modules for this part of ISO 15784 have been grouped into Annex B for easy reference. All MIB modules have been grouped into Annex C for easy reference.

6.3 Logical architecture

This application profile is suitable for usage in the following architectures, as depicted in Figure 1:

1) communications between a traffic management centre (TMC) and roadside modules;

2) communications between another (non-traffic management) centre and roadside modules;

3) communications between two roadside modules. Note that this part of ISO 15784 is based on the use of SNMP which implements a SET/GET paradigm where there is a manager and an agent. However, a roadside module may act as both a manager (e.g. sending requests to other roadside modules) and as an agent (e.g. responding to requests from the TMC) simultaneously.

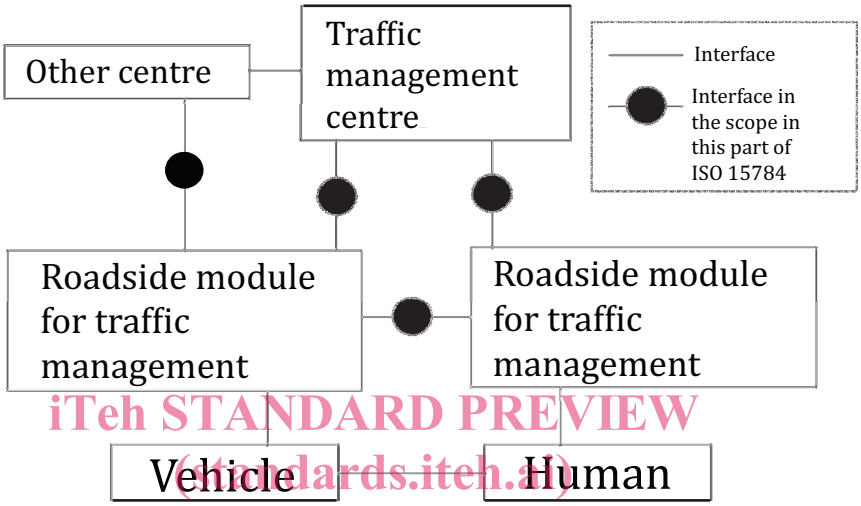

Figure 1 — Example of this AP-scenario

6.4 Relationship to the OSI model

The Open Systems Interconnect (OSI) reference model defines seven layers, each performing a particular role in the transmission of data over a medium. This part of ISO 15784 defines a particular combination of standards for the upper three layers.

The top layer of the OSI seven-layered model, ***the application layer***, handles issues such as network transparency, resource allocation, and problem partitioning. The application layer is concerned with the user's view of the network.

The second highest layer in the OSI seven-layered model, also known as layer 6 or the ***presentation layer***, performs functions such as text compression, code conversion, or format conversion to try to smooth out differences between hosts.

Layer 5, the ***session layer***, handles security and creation of the session.

The specific protocols defined by this part of ISO 15784 for each layer are shown in Table 1.