International Standard

ISO 15784-2

Second edition
2024-06

Intelligent transport systems — Data exchange involving roadside modules communication —

Part 2: Centre to field device communications using Simple Network Management Protocol (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 15784-2:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

This second edition cancels and replaces the first edition (ISO 15784-2:2015), which has been technically revised. It also incorporates the Amendment ISO 15784-2:2015/Amd 1:2020.

The main changes are as follows:

— support for Simple Network Management Protocol (SNMP) versions other than SNMP version 3 have been removed;

— support for the Simple Transportation Management Protocol (STMP) has been removed;

— the security stack has been updated to support Transport Layer Security (TLS) version 1.3.

A list of all parts in the ISO 15784 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 Background

The need for standardized communication with intelligent transport system (ITS) field devices is growing around the world. A number of countries base their field device communications on the Simple Network Management Protocol (SNMP).

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 document creates a standard for ITS field device communications based on several simple concepts:

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

b) provision of a consistent definition of the transport and networking layers;

c) promotion of the adoption of recommended security features; and

d) promotion of the use of interoperable data definitions for the management of field devices, such as those defined in the ISO 26048 series and regional standards while also supporting vendor and project-specific data.

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

0.2 Overview

SNMP is a collection of planned and proven concepts and principles. SNMP employs the principles of abstraction and standardization. This has led to SNMP being widely adopted for communication between management systems and devices on the internet, and other communications networks.

This document requires the use of SNMP version 3 (SNMPv3), as defined by the Internet Engineering Task Force (IETF). SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure, previous versions of SNMP permit access control based on the unauthenticated contents of the SNMP message, rather than using the authenticated identity from the lower layers.

This document does not specify any requirements that contradict or cause non-conformance to the standards listed in the normative references section of this document.

The data to be exchanged by SNMP is defined in Management Information Bases (MIBs), which are defined separately in the firewall MIB, RFCs, the ISO 26048 series, regional standards, vendor specifications and project specifications.

0.3 Document approach and layout

This document provides:

a) an overview of the content of SNMP, including conformance and conventions (Clause 5);

b) a description of the reference architecture for systems that implement this document (Clause 6);

c) technical requirements for entities claiming conformance to this document (Clause 7);

d) performance requirements for entities claiming conformance to this document (Clause 8);

e) a primer for understanding the protocol defined in this document (see Annex A);

f) example encodings of messages conforming to this document (see Annex B);

g) an electronic profile requirements list for implementations to use (available at: https://standards.iso.org/iso/15784/-2/ed-2/en/);

h) an electronic management information base (MIB) that defines the firewall objects (available at: https://standards.iso.org/iso/15784/-2/ed-2/en/).

Intelligent transport systems — Data exchange involving roadside modules communication —

Part 2: Centre to field device communications using Simple Network Management Protocol (SNMP)

1 Scope

This document specifies a mechanism for exchanging data and messages in the following cases:

a) exchange between a traffic management centre and ITS roadside equipment for traffic management;

b) exchange between ITS roadside equipment used for traffic management.

This document is not applicable to:

— communication between traffic management centres and in-vehicle units;

— communication between ITS roadside equipment and in-vehicle units;

— in-vehicle communication;

— in-cabinet communication;

— motion video transmission from a camera or recorded media.

This document is suitable for use when both of the following conditions apply:

1) The data to be exchanged can be defined as one or more elements that can be retrieved or stored – SNMP 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 ITS roadside equipment. 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 regions to control devices such as dynamic message signs.

2) Guaranteed, deterministic, real-time exchange of data is not critical – SNMP operations typically require less than 100 ms, but the underlying network can cause multi-second delays in delivering messages or even lost messages; thus, SNMP is not intended for applications that require reliable sub-second communications.

This document can be used 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);

— repeated, frequent exchanges of the same message structure (with potentially different values), even on relatively low-bandwidth links;

NOTE 1 The dynamic object feature, defined in ISO/TS 26048-1, can be used to eliminate a considerable amount of overhead that is normally associated with SNMP communications to make it more suitable for low-bandwidth links.

— allowing ITS roadside equipment to issue exception reports when special conditions arise.

NOTE 2 Exception reporting uses SNMP notifications in combination with the notification management features defined in ISO/TS 26048-1.

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/TS 14812, *Intelligent transport systems — Vocabulary*

ISO/TS 26048-1, *Intelligent transport systems — Field device SNMP data interface — Part 1: Global objects*

RFC 2578, *Structure of Management Information Version 2 (SMIv2), April 1999*

RFC 2579, *Textual Conventions for SMIv2, April 1999*

RFC 2580, *Conformance Statements for SMIv2, April 1999*

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

RFC 3412, *Message Processing and Dispatching, December 2002*

RFC 3413, *SNMP Applications, December 2002*

RFC 3414, *User-based Security Model, December 2002*

RFC 3415, *View-based Access Control Model, December 2002*

RFC 3416Version 2, *of SNMP Protocol Operations, December 2002*

RFC 3417, *Transport Mappings, December 2002*

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

RFC 3430, *Simple Network Management Protocol (SNMP) over Transmission Control Protocol (TCP) Transport Mapping, December 2002*

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

RFC 4001, *Textual Conventions for Internet Network Addresses, February 2005*

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

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

RFC 6353, *Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), July 2011*

RFC 7860, *HMAC-SHA-2 Authentication Protocols in User-Based Security Model (USM) for SNMPv3, April 2016*

RFC 8446, *The Transport Layer Security (TLS) Protocol Version 1.3, August 2018*

RFC 9147, *The Datagram Transport Layer Security (DTLS) Protocol Version 1.3, April 2022*

RFC 9456, *Updates to the TLS Transport Model for SNMP, November 2023*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/TS 14812 and the following apply.

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

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

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

3.1
agent
Simple Network Management Protocol (SNMP) entity that can respond to SNMP `get` and `set` requests

Note 1 to entry: An agent may also issue `report`, `trap` and/or `inform` messages.

3.2
datagram
self-contained unit of data transmitted independently of other units of data

3.3
deprecated
still valid, but not to be used for new designs

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

3.4
encoding
complete sequence of octets used to represent a data value

3.5
field device
infrastructure-based ITS component located outside of a data centre that is designed to provide local processing or routing services while stationary

Note 1 to entry: This concept is described in ISO/TS 14812 using the term "field system". However, this document uses the term "field device" due to the use of the latter term in management information base (MIB) modules that pre-date the ISO/TS 14812 definition.

3.6
manager
Simple Network Management Protocol (SNMP) entity that can generate SNMP `get` and `set` requests and/or can receive `report`, `trap` and/or `inform` messages

3.7
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]

3.8
object type
specific, defined piece of data, registered for public use on the international object identifier tree

3.9
protocol
set of message formats (semantic, syntactic and symbolic rules) and the rules for message exchange between peer layer entities (which messages are valid when)

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

3.10
protocol data unit
unit of information communicated between network peers

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

3.11
proxy forwarder
agent that acts on behalf of a target entity

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

3.12
SNMP entity
implementation of the Simple Network Management Protocol (SNMP) that resides in an entity

3.13
SNMP object
instance of an object type

4 Abbreviated terms

AES	Advanced Encryption Standard
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
DTLS	Datagram Transport Layer Security
HMAC	hash-based message authentication code
IANA	Internet Assigned Numbers Authority
Ipv4	Internet Protocol – version 4
Ipv6	Internet Protocol – version 6
ITS	intelligent transport systems
MIB	management information base
PDU	protocol data unit
PRL	profile requirements list
SHA	secure hash algorithm
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3, as defined by IAB STD 62 NOTE The term “SNMP” is used in informal statements or when referring to the general concepts of the protocol; “SNMPv3” is used in formal requirements and other statements where the version needs to be emphasized.
TLS	Transport Layer Security
TSM	Transport Security Model

UDP	User Datagram Protocol
USM	User-based Security Model
UTMC	Urban Traffic Management and Control

5 Conformance and Conventions

5.1 ASN.1

This document contains references to ASN.1 data concepts 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`) to distinguish these terms from normal English.

5.2 SNMP Terminology

Terminology between the different versions of SNMP is slightly different. This document uses the terminology of SNMPv3.

5.3 Format

This document conforms to ISO 15784-1.

5.4 Conformance

Conformance to this document is defined by the requirements contained in Clauses 7 and 8. The profile requirements list, available at https://standards.iso.org/iso/15784/-2/ed-2/en/, summarizes these requirements in a table format that can be used to document the conformance of implementations. In case of conflict between the PRL and the main body of this document, the main body of this document shall take precedence.

This document 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 document for convenience. The omission of a feature in this document shall not be interpreted as a prohibition of its use.

6 Architecture

6.1 ITS services

This document defines the underlying mechanisms by which ITS field devices can be monitored, configured and controlled. ITS field devices may be used to support almost any ITS service defined in ISO 14813-1, with a roadside component.

6.2 Physical view

Figure 1 depicts the physical view of this interface using the graphical conventions defined by the architecture reference for cooperative and intelligent transportation (ARC-IT, http://arc-it.net) and also documented in ISO 14813-5:2020, Annex B.

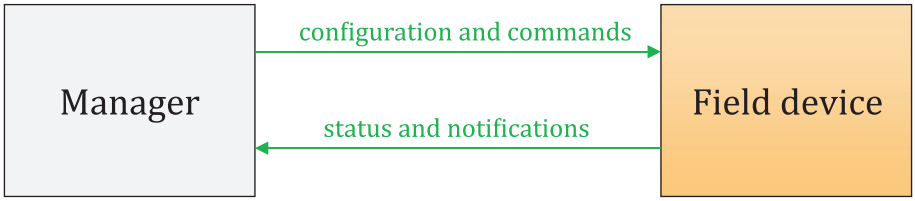

Figure 1 — Physical view of interface

The manager of the field device is shown in grey indicating that it can be any type of physical object, such as a central system, another field device, a maintenance laptop or any other device that supports the defined interface.

The field device is shown in orange, indicating that it is located in the field (e.g. along the roadside). This document addresses the information flows exchanged between these two components over a connection. A field device can have any number of connections to other ITS stations or external systems.

The figure indicates two information transfers between these physical objects. The first is the "configuration and commands" information flow from the manager to the field device. The second is "status and notifications" information flow from the field device to the manager. Both flows are shown in green indicating that authentication is required, and both are shown with a single arrowhead indicating a unicast transfer.

This document specifies the requirements for the underlying SNMP interface. ISO/TS 26048-1 defines a core set of data that can be managed using this SNMP interface. Other documents containing MIBs (e.g. RFCs, the remainder of the ISO 26048 series, regional standards, vendor specifications or project specifications) can specify additional data that can be managed using the SNMP interface.

NOTE SNMP uses a get/set paradigm where there is a manager and an agent. However, a single field device can act as both a manager (e.g. sending requests to other field devices) and as an agent (e.g. responding to requests from a centre or other field device) simultaneously.

6.3 Communications view

Figure 2 depicts how this document is intended to relate to other documents using the ITS Station architecture, as defined in ISO 21217.

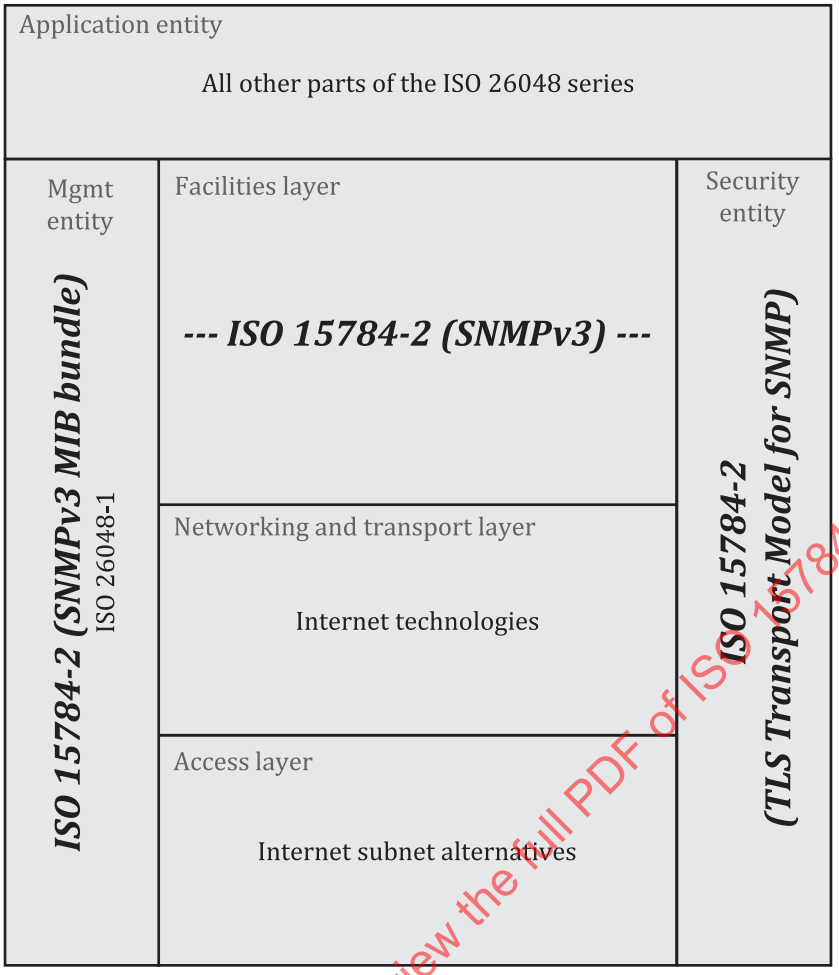

Figure 2 — Typical communications stack

This document defines the Facilities Layer and portions of the Security Entity and Management Entity. The ISO 26048 series defines aspects related to the Management and Application Entities.

The protocol data units defined by this document are intended to be exchanged using well-known internet protocols, such as DTLS/UDP/IP or TLS/TCP/IP over any number of access layers to media.

7 Requirements

7.1 Overview

The high-level requirements and options presented in this document follow the modular architecture adopted by SNMP. As such, this clause covers the following topics, which correspond approximately to RFC 3411 to RFC 3418, followed by additional requirements:

a) terminology and internal architecture;

b) message processing and dispatching;

c) applications;

d) security models;

e) view-based access control;

f) protocol operations;

g) transport mappings;

h) management information bases;

i) additional requirements.

7.2 Terminology and internal architecture

The terminology and internal architecture used for SNMP discussions shall be as defined in RFC 3411 and RFC 5590.

NOTE The internal architecture includes a definition of various components and abstract service interfaces that can exist within an SNMP entity. While implementations are encouraged to adopt this style of architecture for their internal design, they are not required to do so. This document only requires conformance at the external interface of the SNMP engine and does not impose any requirements on the internal design. Nonetheless, the terms defined in this architecture are important for understanding the intended operation of the overall protocol.

7.3 Message Processing and Dispatching

The message processing and dispatching rules shall conform to RFC 3412.

An implementation of this document shall support the SNMPv3 message processing model defined in Section 6 of RFC 3412:(2002).

NOTE 1 SNMPv3 is the most current version of SNMP.

Deployment of SNMP versions prior to SNMPv3 is not recommended.

Operators should disable any earlier version of SNMP supported by a device prior to its deployment.

NOTE 2 SNMP versions prior to SNMPv3 did not include adequate security. With previous versions of SNMP, there is no authentication of who is attempting to access (read/change/create/delete) SNMP objects within the agent, even if the network itself is secure.

7.4 Applications

7.4.1 Entity type

An implementation of this document shall be an agent, a manager, or both.

7.4.2 Command generator

A manager shall support a command generator application, as defined in RFC 3413.

An agent may support a command generator application, as defined in RFC 3413.

7.4.3 Command responder

A manager may support a command responder application, as defined in RFC 3413.

An agent shall support a command responder application, as defined in RFC 3413.

7.4.4 Notification originator

A manager may support a notification originator application, as defined in RFC 3413.

An agent may support a notification originator application, as defined in RFC 3413.

If the implementation supports a notification originator, it shall only send notifications in accordance with the provisions of ISO 26048-1.

7.4.5 Notification receiver

A manager may support a notification receiver application, as defined in RFC 3413.

An agent may support a notification receiver application, as defined in RFC 3413.

7.4.6 Proxy forwarder

A manager may support a proxy forwarder application, as defined in RFC 3413.

An agent may support a proxy forwarder application, as defined in RFC 3413.

7.5 Security models

7.5.1 User-based security model

7.5.1.1 General

An implementation of this document shall support the user-based security model (USM) defined in RFC 3414.

Operators should:

a) configure USM to require authentication and privacy;

b) manage and maintain their USM private key credentials;

c) limit USM access to a minimal set of operations that can potentially be critical during periods of network stress (e.g. a denial-of-service attack); and

d) avoid using USM, except when the network is under stress.

NOTE While TLSTM is more up-to-date than USM and offers several advantages over USM, USM can enhance integrity and reliability of network operations when the network is under stress. Minimizing the use of USM except when a network is under stress minimizes the need to update USM security keys, which has been reported to be rather burdensome.

7.5.1.2 SHA-2 authentication

USM shall support HMAC-SHA-2 (SHA-2) as defined in RFC 7860.

As computer processor speeds increase, authentication schemes need to be improved to provide adequate protection against automated attacks. At the time of publication of this document, SHA-2 is the recommended level of authentication for protecting against automated attacks.

7.5.1.3 AES encryption

USM shall support Advanced Encryption Standard (AES) cipher algorithm as defined in RFC 3826.

Operators should update security keys for authentication and encryption at regular intervals.

As computer processor speeds increase, encryption schemes need to be improved to provide adequate protection against automated attacks. At the time of publication of this document, AES is the recommended level of encryption for protecting against automated attacks.

7.5.2 Transport security model

An implementation of this document shall support the transport security model (TSM) defined in RFC 5591.

An implementation of this document shall support the Transport Layer Security (TLS) Transport Model for SNMP as defined in RFC 6353 and updated by RFC 9456.

7.6 View-based access control

An implementation of this document shall follow the view-based access control rules defined in RFC 3415.

7.7 Protocol operations

7.7.1 General

An implementation of this document shall support the protocol operations defined in RFC 3416.

7.7.2 Request ID variation

When issuing SNMP requests, managers shall vary the value of `request-id`.

NOTE A common approach is to increment the `request-id` for each request issued, but this is not a requirement.

7.8 Transport mappings

7.8.1 Port numbers

An SNMP entity should use either the assigned well-known port number, as assigned by the Internet Assigned Numbers Authority (IANA), or a private port number.

NOTE 1 UDP and TCP use a common set of well-known port numbers, which apply to both Ipv4 and Ipv6. The well-known port number for SNMP is 161. The well-known port number for SNMP notifications is 162.

NOTE 2 Private port numbers span the range from 49152 to 65535, inclusive.

7.8.2 UDP over IPv4

An implementation of this document may support SNMPv3, as defined in 7.1 through 7.7, over the UDP over IPv4 transport mapping defined in Section 3 of RFC 3417:(2002).

NOTE 1 This is the typical deployment environment for this document.

NOTE 2 The RFC requires BER encoding and support of packets of at least 484 octets.

7.8.3 UDP over IPv6

7.8.3.1 General

An implementation of this document may support SNMPv3, as defined in 7.1 through 7.7, over the UDP over IPv6 transport mapping defined in 7.8.3.2 through 7.8.3.3.

7.8.3.2 Serialization

Each instance of a message shall be serialized (i.e. encoded) according to the rules of BER using the algorithm specified in Section 8 of RFC 3417:(2002). The resulting BER-encoded message shall be placed into a single UDP datagram and sent using a single IPv6 packet.

7.8.3.3 Message size

An implementation claiming conformance to this transport mapping shall accept messages up to and including 484 octets in size. It is recommended that implementations accept messages up to 1 472 octets in size. Implementation of larger values is encouraged when possible.

7.8.4 TCP over IPv4

An implementation of this document shall support SNMPv3, as defined in 7.1 to 7.7, over the TCP over IPv4 transport mapping defined in RFC 3430.

7.8.5 TCP over IPv6

An implementation of this document may support SNMPv3, as defined in 7.1 through 7.7, over the TCP over IPv6 transport mapping defined in RFC 3430.

7.8.6 Secure transport

7.8.6.1 Support for DTLS

An implementation of this document that supports UDP shall support Datagram Transport Layer Security (DTLS) version 1.3 as defined in RFC 9147.

7.8.6.2 Support for TLS

An implementation of this document shall support the Transport Layer Security (TLS) Protocol Version 1.3, as defined in RFC 8446.

7.8.6.3 Cipher suites

An implementation of this document shall support the TLS_AES_128_GCM_SHA256 cipher suite, as defined in RFC 8446.

7.8.6.4 Deployment guidance

There are cryptographic limits on the amount of plaintext which can be safely encrypted under a given set of keys. An analysis (see Reference [12]) of these limits, assuming the underlying primitive has no weaknesses, indicates that the keys for the TLS_AES_128_GCM_SHA256 cipher suite should be updated, as described in Section 4.6.3 of RFC 8446:(2018), prior to exchanging $2^{28,5}$ (about 376 million) packets with an average size of 1 024 bytes per packet. At one request and one response per second, the key would remain valid for 6 years. Most ITS devices do not exchange this much data, allowing the keys to remain valid for a longer period.

The actual frequency of updating the keys should be based on a careful analysis of multiple factors as described in NIST 800-57 Part 1.

7.9 Management information base (MIB)

7.9.1 Agent MIBs

An SNMP agent claiming conformance to this document shall support the following MIBs:

a) `SNMP-FRAMEWORK-MIB`, as defined in Section 5 of RFC 3411:(2002);

b) `SNMP-MPD-MIB`, as defined in Section 5 of RFC 3412:(2002);

c) `SNMP-USER-BASED-SM-MIB`, as defined in Section 5 of RFC 3414:(2002);

d) `SNMP-USM-AES-MIB`, as defined in Section 2 of RFC 3826:(2004);

e) `SNMP-VIEW-BASED-ACM-MIB`, as defined in Section 4 of RFC 3415:(2002);

f) `SNMPv2-MIB`, as defined in Section 2 of RFC 3418:(2002);

g) `SNMP-TSM-MIB`, as defined in Section 7 of RFC 5591:(2009);

h) `SNMP-TLS-TM-MIB`, as defined in Section 4 of RFC 9456:(2023);

i) `FD-FIREWALL-MIB`, as defined in https://standards.iso.org/iso/15784/-2/ed-2/en/. The firewall MIB is defined as a part of this document and requires conformance to portions of RFC 2578, RFC 2579, RFC 2580 and RFC 4001.

7.9.2 Notification originator MIBs

An SNMP entity claiming support for the notification originator application shall support the following MIBs:

a) `SNMP-TARGET-MIB`, as defined in Section 4.1 of RFC 3413:(2002);

b) `SNMP-NOTIFICATION-MIB`, as defined in Section 4.2 of RFC 3413:(2002);

c) `ISO 26048-1-Notification`, as defined in ISO/TS 26048-1.

7.9.3 Proxy forwarder MIBs

An SNMP entity claiming support for the proxy forwarder application shall support the following MIBs:

a) `SNMP-TARGET-MIB`, as defined in Section 4.1 of RFC 3413:(2002);

b) `SNMP-PROXY-MIB`, as defined in Section 4.3 of RFC 3413:(2002).

7.9.4 Other supported data

All SNMP objects accessible by the agent shall be defined in an MIB module according to the rules defined in RFC 2578.

7.10 Context engine ID discovery

An SNMP entity claiming to be a manager may support context engine ID discovery as defined by RFC 5343.

8 Performance

8.1 Overview

The use of SNMP to retrieve SNMP objects implies a required response time for the field device to commence transmission to the management station. The performance requirements will depend on the complexity of the device and the specific data being retrieved, which also depends on the specific ITS device type.

The procuring agency should identify the specific performance requirements that are needed to ensure reliable operation within their network environment.

8.2 Default response time

In the absence of any other specification, the response time, defined as the time from the receipt of the last byte of a Confirmed Class `pduType` to the start of the transmission of the first byte of the response message (when access is allowed by lower layers) shall not exceed the maximum of 100 ms or the response time explicitly defined within the standard MIB definition of one of the SNMP objects contained in the response.

NOTE This default response time is based on experimental data from deployments of existing systems with requests of limited processing complexity. Users can alter these response times, but increasing response times will result in longer timeouts, which can slow the performance of real-time systems while shorter response times can be difficult to achieve for requests that require much processing. It is expected that most exceptions to the default response time will relate to a small number of defined object types. A conformant implementation can always respond before the expiration of the response time, unless explicitly stated otherwise.

EXAMPLE 1 A certain system needs to poll many devices for a specific set of information on a frequent basis. The procurement for that system can require response times for that specific information of 70 ms rather than the default 100 ms.

EXAMPLE 2 A standard defines an object type that requires the agent to perform significant processing prior to responding. In this case, the object type definition can indicate a maximum response time of 200 ms.

EXAMPLE 3 A standard can limit the number of SNMP objects that can be retrieved in a single request while still meeting the 100 ms response time.

Annex A
(informative)

Primer for SNMP

A.1 Overview

This annex contains information that is intended to assist with understanding some of the concepts presented in the rest of the document.

This document is based on the internet standard SNMP "get-set" paradigm. In this paradigm, SNMP allows a management system (i.e. a "manager") to issue messages to monitor (i.e. "get") and alter (i.e. "set") one or more specific pieces of data (i.e. "SNMP objects") within a target device (i.e. "agent").

NOTE Within this terminology, alterations can include the creation of new instances of data within the limits of the agent (i.e. a manager can set the value of an object with a syntax "read-create", even if that object did not previously exist, as long as the device is able to support such an object).

A.2 Object types

All the information within an agent that is accessible via SNMP is defined in a file called a management information base (MIB), which is both human-readable and machine-interpretable. Within this file, a separate object type is defined for each type of elemental information, which is called an SNMP object. An example object type definition is provided below:

```
exampleObject OBJECT-TYPE
   SYNTAX       INTEGER (1..255)
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "A value used as an example."
::= { exampleNode 1 }
```

The textual name of the object type is "`exampleObject`". The "`SYNTAX`" field indicates the types of values that can be stored by instances of the object type. The "`SYNTAX`" field is a primary factor that determines how the information will be encoded. The "`MAX-ACCESS`" field indicates the maximum level of access allowed by any operation. An object type whose instances can be remotely changed will have a `MAX-ACCESS` of "`read-write`" or "`read-create`", but as some user groups can have limited rights, a read-writable object type can appear as read-only to some users.

The "`STATUS`" field indicates whether this object type still represents best practice or whether it has been deprecated in some way. The "`DESCRIPTION`" field provides the textual definition of the object type and may also include informative text associated with the object type. Finally, the last line indicates the globally-unique identifier of the object type, known as the object identifier (OID). The OID is registered on the international object identifier tree.

NOTE 1 Within SNMP specifications, the globally-unique identifier is called the "name" of the object whereas the textual name is called the "descriptor".

The international object identifier tree was jointly created by ISO and ITU-T to provide a way to provide a globally unique reference to any identifiable concept through a mechanism that uses a distributed set of registration authorities. The identifier consists of a set of integral identifiers, each of which can be associated with a name.