

**ISO/DTS 26048-1**

ISO/TC 204

~~ISO/AWI TS 26048-1(en)~~

Secretariat: -ANSI

Date: 2024-09-04

**Intelligent transport systems — Field device Simple Network  
Management Protocol (SNMP) data interface —**

**Part 1:  
Global objects**

iTeh Standards  
(<https://standards.itih.ai>)  
Document Preview

~~Systemes de transports intelligents — Interface de données SNMP pour les équipements en bord de route —~~

~~Partie 1: objets globaux~~

ISO/DTS 26048-1

<https://standards.itih.ai/catalog/standards/iso/f9dc43d2-f5b9-43e4-9206-9ca2f756a74b/iso-dts-26048-1>

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: + 41 22 749 01 11  
E-mail: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

ISO/DTS 26048-1

<https://standards.iteh.ai/catalog/standards/iso/f9dc43d2-f5b9-43c4-9206-9ca2f756a74b/iso-dts-26048-1>

## Contents

|  |      |
|--|------|
| Foreword.....  | viii |
| Part 1: Global objects .....                             | 1    |
| 1 — Scope.....   | 1    |
| 2 — Normative references.....                            | 1    |
| 3 — Terms and definitions.....                           | 2    |
| 4 — Symbols and abbreviated terms.....                   | 5    |
| 5 — Conventions and architecture.....                    | 6    |
| 5.1 — ISO maintenance portal.....                        | 6    |
| 5.2 — MIB files.....                                     | 6    |
| 5.3 — ASN.1.....   | 6    |
| 5.4 — Conformance.....                                   | 7    |
| 5.5 — SNMP terminology.....                              | 7    |
| 5.6 — Architecture.....                                  | 7    |
| 5.6.1 — ITS services.....                                | 7    |
| 5.6.2 — Functional view of interface.....                | 7    |
| 5.6.3 — Physical view.....                               | 7    |
| 5.6.4 — Communications view.....                         | 8    |
| 5.7 — Constraints.....                                   | 9    |
| 5.7.1 — Table design constraint.....                     | 9    |
| 5.7.2 — Access constraints.....                          | 9    |
| 5.8 — Outline.....                                       | 9    |
| 5.9 — Requirements pattern.....                          | 9    |
| 6 — User needs.....                                      | 11   |
| 6.1 — Authenticate users.....                            | 11   |
| 6.2 — Control access to data.....                        | 11   |
| 6.3 — Monitor failed access to the field device.....     | 11   |
| 6.4 — Manage the field device.....                       | 12   |
| 6.5 — Monitor field device components.....               | 12   |
| 6.5.1 — Monitor ambient environment.....                 | 12   |
| 6.5.2 — Monitor field device enclosure.....              | 12   |
| 6.5.3 — Manage enclosure climate control components..... | 12   |
| 6.5.4 — Monitor field device power.....                  | 13   |
| 6.5.5 — Manage auxiliary ports.....                      | 14   |
| 6.6 — Receive notification of triggers firing.....       | 14   |
| 6.7 — Manage device-specific notifications.....          | 14   |
| 6.8 — Log system events.....                             | 14   |
| 6.9 — Log user-defined data snapshots.....               | 14   |
| 6.10 — Record a series of data snapshots.....            | 15   |
| 6.11 — Issue trigger-based commands.....                 | 15   |
| 6.12 — Configure a complex device.....                   | 15   |
| 6.13 — Efficient exchange of data.....                   | 15   |
| 6.14 — Future user needs.....                            | 15   |
| 6.14.1 — Software update.....                            | 15   |
| 6.14.2 — Start-up configuration.....                     | 16   |
| 7 — High-level design.....                               | 16   |
| 7.1 — Authenticate users design overview.....            | 16   |
| 7.2 — Control access to data design overview.....        | 16   |
| 7.3 — Monitor failed access to the field device.....     | 17   |
| 7.4 — Manage the field device design overview.....       | 17   |

|        |   |    |
|--------|---|----|
| 7.5    | Monitor field device components                         | 17 |
| 7.6    | Receive notification of triggers firing design overview | 17 |
| 7.6.1  | General   | 17 |
| 7.6.2  | Triggers  | 18 |
| 7.6.3  | Action selection  | 18 |
| 7.6.4  | Notification Factory                                    | 19 |
| 7.6.5  | Notification channel                                    | 19 |
| 7.7    | Manage device-specific notifications design overview    | 19 |
| 7.8    | Log system events design overview                       | 19 |
| 7.9    | Log user-defined data snapshots design overview         | 20 |
| 7.10   | Record a series of data snapshots design overview       | 20 |
| 7.11   | Issue trigger-based commands design overview            | 21 |
| 7.12   | Configure a complex device design overview              | 22 |
| 7.13   | Efficient exchange of data design overview              | 23 |
| 7.14   | Triggers  | 23 |
| 7.14.1 | General   | 23 |
| 7.14.2 | Scheduled triggers design overview                      | 23 |
| 7.14.3 | Day plan triggers design overview                       | 24 |
| 7.14.4 | Condition-based triggers design overview                | 24 |
| 8      | Requirements  | 25 |
| 8.1    | Action feature  | 25 |
| 8.1.1  | Action feature definition                               | 25 |
| 8.1.2  | Action feature data exchange requirements               | 26 |
| 8.1.3  | Action feature functional requirements                  | 27 |
| 8.2    | Clock feature   | 27 |
| 8.2.1  | UTC Clock   | 27 |
| 8.2.2  | Local clock   | 29 |
| 8.2.3  | Daylight saving time                                    | 30 |
| 8.3    | Command feature   | 30 |
| 8.3.1  | Command feature definition                              | 30 |
| 8.3.2  | Command feature data exchange requirements              | 31 |
| 8.3.3  | Command feature capability requirements                 | 32 |
| 8.3.4  | Command feature functional requirements                 | 32 |
| 8.4    | Conditional trigger feature                             | 32 |
| 8.4.1  | Conditional trigger feature definition                  | 32 |
| 8.4.2  | Conditional trigger feature data exchange requirements  | 32 |
| 8.4.3  | Conditional trigger feature functional requirements     | 33 |
| 8.4.4  | Conditional trigger feature capability requirements     | 33 |
| 8.5    | Controller feature                                      | 39 |
| 8.5.1  | Controller feature definition                           | 39 |
| 8.5.2  | Controller feature data exchange requirements           | 39 |
| 8.5.3  | Controller feature capability requirements              | 41 |
| 8.5.4  | Controller performance requirements                     | 41 |
| 8.6    | Day plan feature  | 41 |
| 8.6.1  | Day plan feature definition                             | 41 |
| 8.6.2  | Day plan feature data exchange requirements             | 41 |
| 8.6.3  | Day plan feature functional requirements                | 43 |
| 8.7    | Dynamic object feature                                  | 43 |
| 8.7.1  | Dynamic object feature definition                       | 43 |
| 8.7.2  | Dynamic object feature data exchange requirements       | 43 |
| 8.7.3  | Dynamic object feature capability requirements          | 44 |
| 8.7.4  | Dynamic object feature performance requirements         | 45 |
| 8.8    | Field device feature                                    | 46 |
| 8.8.1  | Field device definition                                 | 46 |

|  |    |
|--|----|
| 8.8.2—General field device features.....                         | 46 |
| 8.8.3—Ambient air temperature.....                               | 47 |
| 8.8.4—Ambient light.....   | 48 |
| 8.8.5—Ambient relative humidity.....                             | 48 |
| 8.8.6—Auxiliary bi-directional port.....                         | 48 |
| 8.8.7—Auxiliary input port.....                                  | 48 |
| 8.8.8—Auxiliary output port.....                                 | 48 |
| 8.8.9—Field device air conditioner.....                          | 49 |
| 8.8.10—Field device battery.....                                 | 49 |
| 8.8.11—Field device dehumidifier.....                            | 50 |
| 8.8.12—Field device doors.....                                   | 50 |
| 8.8.13—Field device fans.....                                    | 50 |
| 8.8.14—Field device generator.....                               | 51 |
| 8.8.15—Field device heaters.....                                 | 51 |
| 8.8.16—Field device humidity.....                                | 52 |
| 8.8.17—Field device mains power.....                             | 52 |
| 8.8.18—Field device power supply.....                            | 52 |
| 8.8.19—Field device processor temperature.....                   | 53 |
| 8.8.20—Field device solar power.....                             | 53 |
| 8.8.21—Field device temperature.....                             | 53 |
| 8.8.22—Field device thermostat.....                              | 53 |
| 8.8.23—Field device wind power.....                              | 54 |
| 8.9—File feature.....  | 54 |
| 8.9.1—File feature definition.....                               | 54 |
| 8.9.2—File feature data exchange requirements.....               | 54 |
| 8.10—Logging feature.....  | 54 |
| 8.10.1—Logging feature definition.....                           | 54 |
| 8.10.2—Logging feature data exchange requirements.....           | 54 |
| 8.10.3—Logging feature functional requirements.....              | 56 |
| 8.10.4—Logging feature capability requirements.....              | 56 |
| 8.11—Notification feature.....                                   | 57 |
| 8.11.1—Notification channel.....                                 | 59 |
| 8.11.2—Notification factory.....                                 | 68 |
| 8.11.3—Independent notification.....                             | 69 |
| 8.11.4—Notification aggregator.....                              | 70 |
| 8.12—Owner feature.....  | 73 |
| 8.12.1—Owner feature definition.....                             | 73 |
| 8.12.2—Owner feature data exchange requirements.....             | 73 |
| 8.13—Recording feature.....                                      | 74 |
| 8.13.1—Recording feature definition.....                         | 74 |
| 8.13.2—Recording feature data exchange requirements.....         | 74 |
| 8.13.3—Recording feature capability requirements.....            | 76 |
| 8.13.4—Recording feature functional requirement.....             | 76 |
| 8.14—Scheduled trigger feature.....                              | 76 |
| 8.14.1—Scheduled trigger feature definition.....                 | 76 |
| 8.14.2—Scheduled trigger feature data exchange requirements..... | 76 |
| 8.14.3—Scheduled trigger feature functional requirements.....    | 77 |
| 8.14.4—Scheduled trigger feature capability requirements.....    | 77 |
| 8.15—Secure communications feature.....                          | 77 |
| 8.15.1—Secure communications feature definition.....             | 77 |
| 8.15.2—Secure communications protocol requirements.....          | 77 |
| 8.15.3—Secure communications conformance requirements.....       | 78 |
| 8.16—SNMP target feature.....                                    | 78 |
| 8.16.1—SNMP target feature definition.....                       | 78 |

|        |  |    |
|--------|--|----|
| 8.16.2 | SNMP target feature data exchange requirements             | 78 |
| 8.16.3 | SNMP target feature capability requirements                | 79 |
| 8.17   | Start-up feature   | 79 |
| 8.17.1 | Start-up feature definition                                | 79 |
| 8.17.2 | Start-up feature data exchange requirements                | 79 |
| 8.18   | Supplemental roadside sensors and actuators (SRSA) feature | 80 |
| 8.18.1 | SRSA feature definition                                    | 80 |
| 8.18.2 | SRSA feature data exchange requirements                    | 80 |
| 8.18.3 | SRSA feature capability requirements                       | 81 |
| 8.18.4 | SRSA feature performance requirements                      | 81 |
| 8.18.5 | SRSA feature supplemental requirements                     | 82 |
| 8.19   | System log feature   | 82 |
| 8.19.1 | System log feature definition                              | 82 |
| 8.19.2 | System log feature data exchange requirements              | 82 |
| 8.19.3 | System log feature capability requirements                 | 83 |
| 8.20   | System log filter feature                                  | 83 |
| 8.20.1 | System log filter feature definition                       | 83 |
| 8.20.2 | System log filter data exchange requirements               | 84 |
| 8.21   | Transaction feature  | 84 |
| 8.21.1 | Transaction feature definition                             | 84 |
| 8.21.2 | Transaction feature data exchange requirements             | 84 |
| 8.21.3 | Transaction feature functional requirements                | 85 |
| 8.22   | View-based access control model (VACM) feature             | 85 |
| 8.22.1 | VACM feature definition                                    | 85 |
| 8.22.2 | VACM feature data exchange requirements                    | 85 |
| 9      | Dialogues  | 86 |
| 9.1    | General dialogue rules                                     | 86 |
| 9.1.1  | Management station initiated                               | 86 |
| 9.1.2  | SNMP agent performance requirements                        | 86 |
| 9.1.3  | Generic and custom dialogues                               | 86 |
| 9.2    | Generic dialogues  | 86 |
| 9.2.1  | Get elemental data   | 86 |
| 9.2.2  | Set elemental data   | 86 |
| 9.2.3  | Walk data  | 86 |
| 9.2.4  | Get bulk data  | 87 |
| 9.2.5  | Get tabular data   | 87 |
| 9.2.6  | Set tabular data   | 87 |
| 9.2.7  | Get data column  | 87 |
| 9.2.8  | Get counters   | 87 |
| 9.2.9  | Get data from dynamic table entry                          | 88 |
| 9.2.10 | Get row status of dynamic table entry                      | 88 |
| 9.2.11 | Configure entry of a dynamic table                         | 88 |
| 9.2.12 | Configure entry of a dynamic table with TestAndIncr        | 90 |
| 9.2.13 | Toggle active status of a dynamic table entry              | 90 |
| 9.2.14 | Delete entry from a dynamic table                          | 91 |
| 9.2.15 | Send a notification  | 91 |
| 9.2.16 | Retrieve dynamic object data in one step                   | 91 |
| 9.2.17 | Retrieve dynamic object data in two steps                  | 91 |
| 9.2.18 | Set dynamic object in one step                             | 92 |
| 9.2.19 | Set dynamic object data in two steps                       | 92 |
| 9.2.20 | Retrieve a file  | 93 |
| 9.2.21 | Generate a file  | 93 |
| 10     | Security   | 93 |

|              |   |     |
|--------------|---|-----|
| 10.1         | Vulnerabilities .....                           | 93  |
| 10.2         | Authentication and access control .....         | 94  |
| 10.3         | Encryption .....                                | 94  |
| 10.4         | Security recommendation .....                   | 94  |
| Annex A      | Conformance .....                               | 95  |
| A.1          | Overview .....                                  | 95  |
| A.1.1        | General .....                                   | 95  |
| A.1.2        | Conformance tables .....                        | 96  |
| A.1.3        | Conformance table references .....              | 96  |
| A.2          | Conformance codes .....                         | 96  |
| A.3          | Parent items .....                              | 96  |
| A.4          | Qualifiers .....                                | 97  |
| A.5          | Option groups .....                             | 97  |
| Annex B      | Management information base (MIB) summary ..... | 98  |
| B.1          | Included MIBs .....                             | 98  |
| B.2          | Referenced MIBs .....                           | 98  |
| Bibliography | .....   | 115 |

|          |   |    |
|----------|---|----|
| Foreword | .....   | ix |
| 1        | Scope .....                                     | 1  |
| 2        | Normative references .....                      | 1  |
| 3        | Terms and definitions .....                     | 2  |
| 4        | Symbols and abbreviated terms .....             | 5  |
| 5        | Conventions and architecture .....              | 7  |
| 5.1      | ISO maintenance portal .....                    | 7  |
| 5.2      | MIB files .....                                 | 8  |
| 5.3      | ASN.1 .....                                     | 8  |
| 5.4      | Conformance .....                               | 8  |
| 5.5      | SNMP terminology .....                          | 8  |
| 5.6      | Architecture .....                              | 8  |
| 5.7      | Constraints .....                               | 11 |
| 5.8      | Outline .....                                   | 11 |
| 5.9      | Requirements pattern .....                      | 11 |
| 6        | User needs .....                                | 13 |
| 6.1      | Authenticate users .....                        | 13 |
| 6.2      | Control access to data .....                    | 13 |
| 6.3      | Monitor failed access to the field device ..... | 14 |
| 6.4      | Manage the field device .....                   | 14 |
| 6.5      | Monitor field device components .....           | 14 |
| 6.6      | Receive notification of triggers firing .....   | 16 |
| 6.7      | Manage device-specific notifications .....      | 16 |
| 6.8      | Log system events .....                         | 16 |
| 6.9      | Log user-defined data snapshots .....           | 16 |
| 6.10     | Record a series of data snapshots .....         | 17 |
| 6.11     | Issue trigger-based commands .....              | 17 |
| 6.12     | Configure a complex device .....                | 17 |
| 6.13     | Efficient exchange of data .....                | 17 |
| 6.14     | Future user needs .....                         | 18 |
| 7        | High-level design .....                         | 18 |

|                       |   |     |
|-----------------------|---|-----|
| 7.1                   | Authenticate users design overview.....                         | 18  |
| 7.2                   | Control access to data design overview.....                     | 18  |
| 7.3                   | Monitor failed access to the field device .....                 | 19  |
| 7.4                   | Manage the field device design overview.....                    | 19  |
| 7.5                   | Monitor field device components .....                           | 19  |
| 7.6                   | Receive notification of triggers firing design overview.....    | 19  |
| 7.7                   | Manage device-specific notifications design overview .....      | 22  |
| 7.8                   | Log system events design overview .....                         | 22  |
| 7.9                   | Log user-defined data snapshots design overview.....            | 22  |
| 7.10                  | Record a series of data snapshots design overview.....          | 23  |
| 7.11                  | Issue trigger-based commands design overview .....              | 25  |
| 7.12                  | Configure a complex device design overview.....                 | 27  |
| 7.13                  | Efficient exchange of data design overview .....                | 28  |
| 7.14                  | Triggers .....  | 28  |
| 8                     | Requirements.....   | 34  |
| 8.1                   | Action feature.....   | 34  |
| 8.2                   | Clock feature.....  | 36  |
| 8.3                   | Command feature .....   | 39  |
| 8.4                   | Conditional trigger feature.....                                | 40  |
| 8.5                   | Controller feature .....  | 47  |
| 8.6                   | Day plan feature .....  | 49  |
| 8.7                   | Dynamic object feature.....                                     | 51  |
| 8.8                   | Field device feature.....                                       | 54  |
| 8.9                   | File feature .....  | 62  |
| 8.10                  | Logging feature .....   | 62  |
| 8.11                  | Notification feature .....                                      | 65  |
| 8.12                  | Owner feature .....   | 82  |
| 8.13                  | Recording feature .....   | 83  |
| 8.14                  | Scheduled trigger feature .....                                 | 85  |
| 8.15                  | Secure communications feature.....                              | 86  |
| 8.16                  | SNMP target feature .....                                       | 87  |
| 8.17                  | Start-up feature .....  | 88  |
| 8.18                  | Supplemental roadside sensors and actuators (SRSA) feature..... | 89  |
| 8.19                  | System log feature .....  | 91  |
| 8.20                  | System log filter feature .....                                 | 92  |
| 8.21                  | Transaction feature.....  | 93  |
| 8.22                  | View-based access control model (VACM) feature .....            | 94  |
| 9                     | Dialogues.....  | 94  |
| 9.1                   | General dialogue rules.....                                     | 94  |
| 9.2                   | Generic dialogues.....  | 95  |
| 10                    | Security.....   | 103 |
| 10.1                  | Vulnerabilities .....   | 103 |
| 10.2                  | Authentication and access control .....                         | 103 |
| 10.3                  | Encryption .....  | 103 |
| 10.4                  | Security recommendations .....                                  | 103 |
| Annex A (informative) | Conformance .....   | 104 |
| Annex B (informative) | Management information base (MIB) summary.....                  | 107 |
| Bibliography          | .....   | 109 |



## 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~~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](http://www.iso.org/directives)).

~~Attention is drawn~~ISO draws attention to the possibility that ~~some of the~~ ~~elements~~implementation of this document may ~~be involve~~ the ~~subject~~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](http://www.iso.org/patents). 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](http://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~~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 ~~the following URL:~~ [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

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

~~This is the first edition of ISO/TS 26048-1.~~

A list of all parts in the ISO 26048 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](http://www.iso.org/members.html) ~~www.iso.org/members.html~~.



# Intelligent transport systems — Field device ~~SNMP~~Simple Network Management Protocol (SNMP) data interface —

## Part 1: Global objects

### 1 Scope

Field devices are a key component in intelligent transport systems (ITS). Field devices include traffic signals, message signs, weather stations, traffic sensors, roadside equipment for connected ITS environments, etc.

The ISO 26048 series defines data that can be used to manage field devices, including device configuration, control, and monitoring. Field devices can be quite complex, necessitating the standardization of many data concepts for exchange. As such, the ISO 26048 series is divided into several individual parts. This document (~~Part ISO 26048-1~~) introduces the ISO 26048 series, provides ~~normative~~ content that ~~applies to all~~is normatively referenced in subsequent parts, and defines data that is applicable to the management of a wide range of field devices.

The scope of the ISO 26048 series does not define the logic used by the management station, the underlying protocols used to exchange the defined data elements, or internal design of the field device. However, the ISO-26048-series does define functional requirements on the interface and assumes an interface based on an SNMPv3 environment as specified by ISO/~~DIS~~-15784-2.

NOTE Many of the concepts defined in this document were derived from ~~[1]~~NTCIP 1103<sup>[1]</sup> and ~~[2]~~NTCIP 1201<sup>[2]</sup>, however, the design has been updated to better address security concerns. It is expected that future versions of NTCIP will migrate to the design defined in this document.

### 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 5345:2022~~, *Intelligent transport systems — Identifiers*

~~ISO/DIS-ISO 15784-2~~, *Intelligent transport systems (ITS) — Data exchange involving roadside modules communication — Part 2: Centre to field device communications using ~~SNMP~~Simple Network Management Protocol (SNMP)*

ISO/IEC-~~8825-1:2021~~, *Information technology — ASN.1 encoding rules — Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC-~~8825-7:2021~~, *Information technology — ASN.1 encoding rules — Part 7: Specification of Octet Encoding Rules (OER)*

ISO/IEC/IEEE-~~24765:2017~~, *Systems and software engineering — Vocabulary*

ISO/TS-~~14812:2022~~, *Intelligent transport systems — Vocabulary*

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

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

~~RFC 2580, Conformance Statements for SMIPv2, April 1999~~

~~RFC 3411, Simple Network Management Protocol (SNMP) Management Frameworks, December 2002.~~

~~RFC 3413, Simple Network Management Protocol (SNMP) Applications, December 2002.~~

~~RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), December 2002.]~~

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

~~RFC 4133, Entity MIB (Version 3), August 2005.~~

~~RFC 4217, Securing FTP with TLS, October 2005.~~

~~RFC 5424, The Syslog Protocol, March 2009.~~

~~RFC 5676, Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications, October 2009.~~

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

### 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC/IEEE ~~24765:2017~~, ISO/TS ~~14812:2022~~, as well as and the following apply.

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

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

~~<https://standards.iteh.ai/catalog/standards/iso/19dc43d2-15b9-43e4-9206-9ca2f756a74b/iso-dts-26048-1>~~

— ISO Online browsing platform: available at ~~<http://www.iso.org/obp>~~<https://www.iso.org/obp>

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

#### 3.1

##### command generator

Simple Network Management Protocol (SNMP) application (3.19) that monitors and manipulates management information

#### 3.2

##### command responder

Simple Network Management Protocol (SNMP) application (3.19) that provides access to management information

#### 3.3

##### control object

writable Simple Network Management Protocol (SNMP) object (3.23) used to request ~~immediately activate~~ immediate activation of a feature or state of the field device (3.5)

Note 1 to entry: Although control objects are writable, they are not considered part of the agent configuration and are therefore not database parameters (3.4).

**3.4****database parameter**

writable [Simple Network Management Protocol \(SNMP\)](#) object used to configure an *SNMP agent* [\(3.18\)](#) and that can be set and validated using a single SNMP SetRequest-PDU

**3.5****field device**

fixed or portable roadside module that includes ~~an SNMP agent~~ [Simple Network Management Protocol \(SNMP\) agent \(3.18\)](#)

**3.6****fire**

~~to~~ start a process when a *trigger* (~~Error! Hyperlink reference not valid.~~[3.28](#)) value transitions from false to true

**3.7****inform**

*notification* [\(3.11\)](#) sent with an expectation of an acknowledgement

**3.8****interrelated parameter**

writable [Simple Network Management Protocol \(SNMP\)](#) object [\(3.23\)](#) used to configure an *SNMP agent* [\(3.18\)](#) and that is designed to require the use of multiple SNMP SetRequest-PDUs prior to validating and implementing a new value

Note 1 to entry: The need for multiple SetRequest-PDUs is typically due to the number of other SNMP objects that are associated with the object. For example, a table can contain a column indicating a percent value where all rows of the table are supposed to equal 100. Configuring all rows within the table at once can exceed the size limitations on a single PDU. In this case, the designer can declare the SNMP object to be an interrelated parameter.

Note 2 to entry: Interrelated parameters are set using the transaction feature defined in [8.21](#).

**3.9****log**

registry of data *snapshots* [\(3.17\)](#) within ~~an a~~ [Simple Network Management Protocol \(SNMP\) agent \(3.18\)](#) that can be retrieved by an *SNMP manager* [\(3.22\)](#)

**3.10****management station**

system that manages one or more *field devices* [\(3.5\)](#) with ~~an a~~ [Simple Network Management Protocol \(SNMP\) manager \(3.22\)](#)

**3.11****notification**

[Simple Network Management Protocol \(SNMP\)](#) message from ~~an a~~ *SNMP agent* [\(3.18\)](#) that is generated independently from any explicit request

Note 1 to entry: While a notification is not generated in response to any explicit request, it can be generated based on configured parameters stored within the *SNMP agent* [\(3.18\)](#).

**3.12****notification originator**

[Simple Network Management Protocol \(SNMP\)](#) application [\(3.19\)](#) that initiates asynchronous messages

### 3.13

#### notification receiver

Simple Network Management Protocol (SNMP) application (3.19) that processes asynchronous messages

### 3.14

#### principal

entity on whose behalf services are provided or processing takes place

EXAMPLE 1 An individual.

EXAMPLE 2 An application.

### 3.15

#### proxy forwarder

Simple Network Management Protocol (SNMP) application (3.19) that forwards messages between entities

Note 1 to entry: Proxy forwarder applications typically change the protocol or message model as a part of ~~its~~their functionality.

### 3.16

#### response time

time from the receipt of a Confirmed Class pduType by the *command responder (3.2)* to the sending of the response PDU by the command responder

Note 1 to entry: For this document, the response time is measured at the application programming interface of the command responder. Any delays imposed within the lower layers are network delays and are not included in the response time.

### 3.17

#### snapshot

#### data snapshot

information captured when a *trigger (3.28)* fires (3.6) within ~~an~~a Simple Network Management Protocol (SNMP) agent (3.18)

Note 1 to entry: A snapshot can be used in the generation of an SNMP *notification (3.11)* or the creation of a new entry within a *log (3.9)*.

### 3.18

#### SNMP agent

Simple Network Management Protocol (SNMP) entity (3.20) containing one or more *command responder (3.2)* and/or *notification originator (3.12)* applications

### 3.19

#### SNMP application

application that provides specific functional processing of Simple Network Management Protocol (SNMP) management data

### 3.20

#### SNMP entity

implementation of one or more Simple Network Management Protocol (SNMP) message processing models with one or more associated *SNMP applications (3.19)*

Note 1 to entry: An SNMP entity may also support one or more security models.